T.C.
İSTANBUL ÜNİVERSİTESİ-CERRAHPAŞA
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

DOKTORA TEZİ

MOBİL ÖDEME SİSTEMLERİNDE KİŞİSEL VERİLERİN GÜVENLİ SAKLANMASI için MODEL TASARIMI ve PERFORMANS ANALİZİ

Öznur ŞENGEL

DANIŞMAN
Prof. Dr. Ahmet SERTBAŞ

II. DANIŞMAN
Doç. Dr. Muhammed Ali AYDIN

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği Programı

İSTANBUL-2020

Bu çalışma, 19.10.2020 tarihinde aşağıdaki jüri tarafından Bilgisayar Mühendisliği Anabilim Dalı, Bilgisayar Mühendisliği Programında Doktora tezi olarak kabul edilmiştir.

Tez Jürisi

Prof. Dr. Ahmet SERTBAŞ(Danışman)
İstanbul Üniversitesi-Cerrahpaşa
Mühendislik Fakültesi

Doç. Dr. Atakan KURT
İstanbul Üniversitesi-Cerrahpaşa
Mühendislik Fakültesi

Doç. Dr. Berk CANBERK
İstanbul Teknik Üniversitesi
Bilgisayar ve Bilişim Fakültesi

Doç. Dr. Şerif BAHTİYAR
İstanbul Teknik Üniversitesi
Bilgisayar ve Bilişim Fakültesi

Dr. Öğr. Üyesi Özgür Can TURNA
İstanbul Üniversitesi-Cerrahpaşa
Mühendislik Fakültesi

20.04.2016 tarihli Resmi Gazete'de yayımlanan Lisansüstü Eğitim ve Öğretim Yönetmeliğinin 9/2 ve 22/2 maddeleri gereğince; Bu Lisansüstü teze, İstanbul Üniversitesi-Cerrahpaşa'nın abonesi olduğu intihal yazılım programı kullanılarak Lisansüstü Eğitim Enstitüsü'nün belirlemiş olduğu ölçütlere uygun rapor alınmıştır.

ÖNSÖZ

Bu çalışma İstanbul Üniversitesi-Cerrahpaşa Lisansüstü Eğitim Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda yapılan "Mobil Ödeme Sistemlerinde Kişisel Verilerin Güvenli Saklanması için Model Tasarımı ve Performans Analizi" adlı doktora tez çalışmasını içermektedir.

Bu tez çalışma konusunun belirlenmesinde ve çalışmanın her aşamasında bilgilerini, tecrübelerini ve değerli zamanlarını esirgemeyerek bana her fırsatta yardımcı olan çok değerli danışman hocalarım Sayın Prof. Dr. Ahmet SERTBAŞ ve Sayın Doç. Dr. Muhammed Ali AYDIN'a en içten dileklerimle teşekkür ederim.

Tez izleme komitesi üyelerim Sayın Doç. Dr. Atakan Kurt ve Sayın Doç. Dr. Berk CANBERK'e tezimin gelişimi boyunca verdikleri değerli yönlendirme ve bilgilendirmeleri için teşekkür ederim.

Lisans, yüksek lisans ve doktora eğitimim boyunca kazandırdıkları her şey için ve beni gelecekte söz sahibi yapacak bilgilerle donattıkları için üniversite hocalarımın hepsine teker teker teşekkürlerimi ve saygılarımı sunuyorum.

Doktora eğitimim süresince manevi olarak her zaman yanımda olan, desteğini hiçbir zaman esirgemeyen, uyum içerisinde aynı odayı paylaştığım iş arkadaşlarım Melike GÜNAY ve Özge GÜNAYDIN'a çok teşekkür ederim.

Tüm hayatım boyunca her daim yanımda olup, eğitim hayatım boyunca maddi ve manevi desteklerini esirgemeyen, beni bu günlere sevgi ve saygı kelimelerinin anlamlarını bilecek şekilde yetiştirerek getiren bu hayattaki en büyük şansım olan anne ve babama sonsuz teşekkürler. Her zaman yanımda olup hayalimi gerçekleştirmemde beni cesaretlendiren, kendimden şüphe ettiğimde bana inanan, anne ve babamın bana en değerli hediyesi olan kardeşlerim Özlem ve Özge'ye tüm kalbimle teşekkür ederim.

Ekim 2020 Öznur ŞENGEL

İÇİNDEKİLER

Sayfa No

ÖNSÖZ ..... **iv**
İÇİNDEKİLER ..... **v**
ŞEKİL LİSTESİ ..... **viii**
TABLO LİSTESİ ..... **xi**
SİMGE VE KISALTMA LİSTESİ ..... **xiii**
ÖZET ..... **xvii**
SUMMARY ..... **xix**
1. GİRİŞ **1**
2. GENEL KISIMLAR **5**
2.1. MOBİL ÖDEME SİSTEMLERİ 5
2.2. BİYOMETRİK VERİ 10
2.3. ŞİFRELEME 17
2.3.1. SEZAR ŞİFRELEME 19
2.3.2. YERİNE KOYMALI ŞİFRELEME 20
2.3.3. VIGENERE ŞİFRELEME 21
2.3.4. VERNAM ŞİFRELEME 21
2.3.5. PLAYFAIR ŞİFRELEMESİ 22
2.3.6. HILL ŞİFRELEME 23
2.3.7. PERMÜTASYON ŞİFRELEME 23
2.3.8. AÇIK ANAHTARLI ŞİFRELEME (BAKIŞIMSIZ ŞİFRELEME) 24
2.3.8.1 RIVEST-SHAMIR-ADLEMAN ALGORİTMASI *24*
2.3.9. GİZLİ ANAHTARLI ŞİFRELEME (BAKIŞIMLI ŞİFRELEME) 25
2.3.9.1. VERİ ŞİFRELEME STANDARDI *26*
2.3.9.2. ÜÇLÜ VERİ ŞİFRELEME STANDARDI *30*
2.3.9.3. GELİŞMİŞ ŞİFRELEME STANDARDI *31*
2.4. ŞİFRELEME MODELİ 37
2.4.1. SİYAH KUTU ŞİFRELEME MODELİ 37
2.4.2. GRİ KUTU ŞİFRELEME MODELİ 37
2.4.3. BEYAZ KUTU ŞİFRELEME MODELİ 38
2.5. YERİNE KOYMALI KUTU (S-KUTU) 41

2.5.1. İNDİRGENEMEZ POLİNOMLU S-KUTULAR....45
2.5.2. KAOTİK S-KUTULAR....47
2.5.3. BİYOMETRİK S-KUTULAR....53
3. MALZEME VE YÖNTEM....56
3.1. MODELİNİN TANIMLANMASI....56
3.2. ŞİFRELEME ALGORİTMASININ YAPISI....58
3.3. BİYOMETRİK VERİ (NEDEN PARMAK İZİ?)....64
3.3.1. PARMAK İZİ VE ÖZELLİKLERİ....67
3.4. ÖNERİLEN ETKİN BİYOMETRİK S-KUTU ALGORİTMASI....68
3.4.1. PARMAK İZİ İLE S-KUTU OLUŞTURMA....73
3.4.2. PARMAK İZİ İLE TERS S-KUTU OLUŞTURMA....83
3.5. GÜVENLİK PERFORMANS METRİKLERİ....84
3.5.1 DOĞRUSAL OLMAMA....85
3.5.2. KATI ÇIĞ KRİTERİ....85
3.5.3. DOĞRUSAL OLASILIK....88
3.5.4. DİFERANSİYEL OLASILIK....90
3.5.5. BİT BAĞIMSIZLIK KRİTERİ....93
3.5.6. BÜTÜNLÜK....94
3.5.7. RASTGELELİK....96
3.5.8. GÜVENİLİRLİK ARALIĞI....96
3.5.9. YÜRÜTME SÜRESİ....97
4. BULGULAR....98
4.1. ÖNERİLEN PARMAK İZİ S-KUTULARINA AİT BULGULAR....98
4.1.1. DOĞRUSAL OLMAMA SONUÇLARI....100
4.1.2. KATI ÇIĞ KRİTERİ SONUÇLARI....102
4.1.3. DOĞRUSAL OLASILIK SONUÇLARI....103
4.1.4. DİFERANSİYEL OLASILIK SONUÇLARI....105
4.1.5. BİT BAĞIMSIZLIK KRİTERİ SONUÇLARI....107
4.1.6. BÜTÜNLÜK SONUÇLARI....108
4.1.7. RASTGELELİK SONUÇLARI....111
4.1.8. GÜVENİLİRLİK ARALIĞI SONUÇLARI....114
4.1.9. YÜRÜTME SÜRESİ SONUÇLARI....115
4.2. ÖNERİLEN PARMAK İZİ S-KUTULARIN MEVCUT S-KUTULAR İLE KARŞILAŞTIRILMASI....119
4.2.1. POLİNOMLU S-KUTULAR İLE KARŞILAŞTIRILMASI....121

4.2.2. KAOTİK S-KUTULAR İLE KARŞILAŞTIRILMASI 123
4.2.3. BİYOMETRİK S-KUTULAR İLE KARŞILAŞTIRILMASI 130
5. TARTIŞMA VE SONUÇ 135
KAYNAKLAR 140
EKLER 152
A. ÖNERİLEN ETKİN BİYOMETRİK S-KUTU VE TERS S-KUTU OLUŞTURMA ALGORİTMASINI KULLANARAK ELDE EDİLEN PARMAK İZİ S-KUTU ÖRNEKLERİ 152
ÖZGEÇMİŞ 155

ŞEKİL LİSTESİ

Sayfa No

Şekil 2.1: Mektupla/telefonla sipariş ve internette yapılan kartlı ödeme işlemleri adeti (Bankalararası Kart Merkezi, 2020). 5

Şekil 2.2: Yakın Alan İletişimine sahip mobil telefon yapısı. 8

Şekil 2.3: Biyometrik veri örnekleri. 11

Şekil 2.4: Biyometrik teknolojisi kategorileri. 12

Şekil 2.5: Şifreleme sistemi. 17

Şekil 2.6: Şifreleme teknikleri. 18

Şekil 2.7: Açık anahtarlı şifreleme algoritmalarının çalışma yapısı. 24

Şekil 2.8: Gizli anahtarlı şifreleme algoritmalarının çalışma yapısı. 26

Şekil 2.9: Veri şifreleme standardının çalışma yapısı. 27

Şekil 2.10: Veri şifreleme standardında yer alan f fonksiyonunun çalışma yapısı. 28

Şekil 2.11: Veri şifreleme standardında anahtarın elde edilmesi. 29

Şekil 2.12: Üçlü veri şifreleme standardının çalışma şeması. 30

Şekil 2.13: Bayt değiştirme işlemi. 32

Şekil 2.14: Ters bayt değiştirme işlemi. 32

Şekil 2.15: Satır kaydırma işlemi. 33

Şekil 2.16: Ters satır kaydırma işlemi. 33

Şekil 2.17: Sütun karıştırma işlemi. 34

Şekil 2.18: Ters sütun karıştırma işlemi. 34

Şekil 2.19: Döngü anahtarını ekleme işlemi. 35

Şekil 2.20: Döngü anahtarını oluşturma adımları. 36

Şekil 2.21: Siyah kutu şifreleme modeli. 37

Şekil 2.22: Gri kutu şifreleme modeli. 38

Şekil 2.23: Beyaz kutu şifreleme modeli. 38

Şekil 2.24: NxN s-kutu yapısı. 42

Şekil 3.1: Mobil ödeme uygulaması. 56

Şekil 3.2: Kullanılacak platformun sağladığı olanaklar. 58

Şekil 3.3: Şifreleme algoritmalarının ortalama yürütme süreleri. 63

Şekil 3.4: AES algoritmasının anahtar boyutuna göre şifreleme ve şifre çözme süreleri. 64

Şekil 3.5: Mobil ödeme sistemindeki biyometrik tanımlayıcı özellikleri. 67

Şekil 3.6: Parmak izi ayrıntıları. 68

Şekil 3.7: Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasının blok diyagramı. 69

Şekil 3.8: Önerilen parmak izi s-kutu algoritmasının işlevsel akış diyagramı. 73

Şekil 3.9: Parmak izi görüntüsü. 74

Şekil 3.10: Ölçeklendirilmiş ikili formattaki parmak izi görüntüsü. 74

Şekil 3.11: Hatları inceltilmiş parmak izi görüntüsü. 75

Şekil 3.12: Parmak izinde çatallanma özelliğinin bulunduğu yerler. 77

Şekil 3.13: Parmak izinde hat sonu özelliğinin bulunduğu yerler. 78

Şekil 3.14: S-kutu değerinden ters s-kutunun satır ve sütun bilgisini bulma. 83

Şekil 3.15: S-kutunun satır-sütun bilgisinden ters s-kutunun değer bilgisini oluşturma. 84

Şekil 3.16: S-kutudan ters s-kutunun oluşturulması. 84

Şekil 3.17: Katı çığ kriteri metriğinin işleyişine örnek. 87

Şekil 3.18: Fark işleminin sonucunun fark matrisine işlenmesine örnek. 87

Şekil 3.19: Denklemin elde edilmesi. 89

Şekil 3.20: Bire bir fonksiyon. 94

Şekil 3.21: Örten fonksiyon. 95

Şekil 3.22: Bire bir ve örten fonksiyon. 95

Şekil 4.1: Çatallanma parmak izi özelliğinin yürütme süreleri. 115

Şekil 4.2: Hat sonu parmak izi özelliğinin yürütme süreleri.....116

Şekil 4.3: Çatallanma-hat sonu parmak izi özelliğinin yürütme süreleri. 117

TABLO LİSTESİ

Sayfa No

Tablo 2.1: Literatürde kullanılmış diğer teknikler. 16

Tablo 2.2: Sezar şifreleme veri tablosu. 20

Tablo 2.3: Tablo yöntemi şifreleme veri tablosu. 20

Tablo 2.4: Vernam şifreleme ile modüler toplama işlemi. 22

Tablo 2.5: Playfair şifreleme matrisi örneği. 23

Tablo 2.6: Gelişmiş şifreleme standardının değişken değerleri. 31

Tablo 2.7: AES algoritmasının RCON değerleri. 36

Tablo 2.8: AES s-kutusu. 43

Tablo 2.9: AES ters s-kutu. 44

Tablo 2.10: GF(2^8)'de asal ve/veya indirgenemez polinomlar. 46

Tablo 3.1: Şifreleme algoritmalarının özellikleri. 61

Tablo 3.2: Şifreleme algoritmaların güvenlik saldırıları açısından karşılaştırması. 62

Tablo 3.3: Şifreleme yürütme süreleri. 62

Tablo 3.4: Biyometrik verilerin tanımlayıcı özellikleri. 66

Tablo 3.5: Parmak izinde bulunan çatallanma özelliğinin koordinat bilgileri. 76

Tablo 3.6: XOR işleminin sonucu. 79

Tablo 3.7: Tekrar eden değerlerin silinmesi. 80

Tablo 3.8: 0-255 arası eksik olan değerler. 82

Tablo 3.9: S-kutuya değerlerin yerleştirilmesi. 82

Tablo 3.10: 4x4 s-kutu. 88

Tablo 3.11: Denklemin tüm s-kutunun girdi-çıktı eşlemesine uygulanması. 89

Tablo 3.12: Verilen giriş farklılıkları için çıkış farklılığının hesaplanması. 91

Tablo 3.13: Elde edilen giriş-çıkış farklarının XOR dağılım tablosuna işlenmesi. 92

Tablo 3.14: 4x4 s-kutu örneği.....96

Tablo 4.1: Önerilen parmak izi s-kutuların güvenlik metriklerinin sonuçları.....98

Tablo 4.2: Parmak izi özelliklerine göre önerilen parmak izi s-kutularının doğrusal olmama sonuçları.....101

Tablo 4.3: Parmak izi özelliklerine göre önerilen parmak izi s-kutularının katı çığ kriteri sonuçları. 102

Tablo 4.4: Parmak izi özelliklerine göre önerilen parmak izi s-kutularının doğrusal olasılık sonuçları.....104

Tablo 4.5: Parmak izi özelliklerine göre parmak izi s-kutularının diferansiyel olasılık sonuçları. 105

Tablo 4.6: Parmak izi özelliklerine göre parmak izi s-kutularının bit bağımsızlık kriteri sonuçları. 107

Tablo 4.7: Parmak izlerinden biri ile oluşturulmuş s-kutu. 109

Tablo 4.8: Parmak izlerinden biri ile oluşturulmuş ters s-kutu. 110

Tablo 4.9: Parmak izinden çatallanma özelliği kullanılarak elde edilen s-kutu.....112

Tablo 4.10: Parmak izinden hat sonu özelliği kullanılarak elde edilen s-kutu.....113

Tablo 4.11: Parmak izinden hem çatallanma hem de hat sonu özelliği kullanılarak elde edilen s-kutu. 114

Tablo 4.12: Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasının yürütme süreleri.....117

Tablo 4.13: Parmak izi özelliklerine göre önerilen algoritmanın ortalama yürütme süreleri. 119

Tablo 4.14: Parmak izi özelliklerine göre elde edilen ortalama sonuçlar.....120

Tablo 4.15: Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile elde edilen bir s-kutu ve sonuçları.....121

Tablo 4.16: İndirgenemez polinom ile oluşturulan s-kutuların sonuçları. 122

Tablo 4.17: Kaotik s-kutuların sonuçları.....125

Tablo 4.18: Mevcut biyometrik s-kutuların sonuçları. 131

Tablo 4.19: Biyometrik s-kutu ve ters s-kutu algoritmalarının yürütme süreleri.....133

SİMGE VE KISALTMA LİSTESİ

Simgeler **Açıklama**

B : Parmak izinin ikili formattaki hali
B1 : Parmak izinin hatlarının belirlenmiş hali
B[] : Parmak izindeki çatallanma özelliğine ait bilgilerin saklandığı matris
C : Şifreli metin
$\mathbf{C_a}$: Şifreli metnin a. karakteri
$\mathbf{C_i}$: DES algoritmasında i. döngüde şifreli metin
D : Şifre çözme algoritması
$\mathbf{D_i}$: DES algoritmasında i. döngüde düz metin
{d, n} : RSA algoritması için gizli anahtar
E : Şifreleme algoritması
E() : DES algoritmasında genişletme fonksiyonu
{e, n} : RSA algoritması için açık anahtar
F : Parmak izi okuyucusundan alınan veri
IP() : İlk yer değiştirme fonksiyonu
IS[] : Ters s-kutu matrisi
K : Gizli anahtar
$\mathbf{K_{00}}$: Blok şifrelemede anahtarın 0.satır 0.sütunun kesişimindeki değer
$\mathbf{K_a}$: Anahtarın a. karakteri
$\mathbf{K_i}$: DES algoritmasında i. döngüde anahtar
$\mathbf{K_{açık_B}}$: B kullanıcısının açık anahtarı
$\mathbf{K_{gizli_B}}$: B kullanıcısının gizli anahtarı
$\mathbf{L_0}$: DES algoritmasında 0. döngüde düz metnin 32 bitlik sol bölümü
$\mathbf{L_i}$: DES algoritmasında i. döngüde düz metnin 32 bitlik sol bölümü
$\mathbf{LS_i()}$: DES algoritmasında i birim sola öteleme
n : s-kutunun girdisindeki bit sayısı
$\mathbf{n_g}$: Güvenlik aralığında gözlem sayısı
N : s-kutunun bir boyutu
P : Düz metin
$\mathbf{P_a}$: Düz metnin a. karakteri
PC() : DES algoritmasında sabit yer değiştirme fonksiyonu

(p,q) : RSA algoritması için asal sayı çifti

R[] : Parmak izindeki hat sonu özelliğine ait bilgilerin saklandığı matris

RB[] : Parmak izindeki hat sonu ve çatallanma özelliğine ait bilgilerin saklandığı matris

R_0 : DES algoritmasında 0. döngüde düz metnin 32 bitlik sağ bölümü

R_i : DES algoritmasında i. döngüde düz metnin 32 bitlik sağ bölümü

s : Standart sapma

S_{00} : s-kutunun 0.satır 0.sütunun kesişimindeki değer

S[] : s-kutu matrisi

S() : s-kutu fonksiyonu

$S_i()$: s-kutu çıktısının i. biti

$S_j()$: s-kutu çıktısının j. biti

T : Parmak izinin hatlarının inceltilmiş hali

x : Yatay piksel değeri

X : Güvenlik aralığında gözlemlenen verilerin ortalaması

x_0 : DES algoritmasında 0. döngüde düz metin

x^i : s-kutunun üretildiği polinomun i. bitini

y : Düşey piksel değeri

Z : Güvenlik aralığında güvenilirlik seviyesi

Γ_a : Girdi maskesi

Γ_b : Çıktı maskesi

Δx : Giriş farkı

Δy : Çıkış farkı

Kısaltmalar **Açıklama**

A : Adaenin

AES : Advanced Encryption Standard (Gelişmiş Şifreleme Standardı)

API : Application Programming Interface (Uygulama Programlama Arayüzü)

ATM : Automated Teller Machine

BEK : Biyometrik Şifreleme Anahtarı

BGE : Billet, Gilbert and Ech-Chatbi

BIC : Bit Independence Criterion (Bit Bağımsızlık Kriteri)

BIC-NL : Bit Independence Criterion-Nonlinearity (Bit Bağımsızlık Kriteri-Doğrusal Olmama)

BIC-SAC : Bit Independence Criterion-Strict Avalanche Criterion (Bit Bağımsızlık Kriteri-Katı Çığ Kriteri)

BKM : Bankalararası Kart Merkezi

C : Sitozin

CEJO : Chow, Eisen, Johnson, and Oorschot

CPU : Central Process Unit (Merkezî İşlem Birimi)

DCT : Discrete Cosine Transform

DEA : Data Encryption Algoritm (Veri Şifreleme Algoritması)

DES : Data Encryption Standard (Veri Şifreleme Standardı)

DH : Deffie-Helman

DNA : Deoksiribo Nükleik Asit (Deoxyribonucleic acid)

DP : Differential Probability (Diferansiyel Olasılık)

DTI : Delaunay triangulation indexing

DU : Differential Uniformity (Diferansiyel Dağılım)

ECC : Elliptic Curve Cryptography (Eliptik Eğri Şifreleme)

EFT : Elektronik Fon Transferi

EMV : Europay Mastercard Visa

FCM : Firebase Cloud Messaging

FIPS : Federal Information Processing Standard (Federal Bilgi İşleme Standardı)

G : Guanin

GB : Gigabyte

GF : Galois Field (Galois alanı)

GHz : Gigahertz

GSM : Global System for Mobile Communication (Mobil İletişim için Küresel Sistem)

HCE : Host Card Emulation (Ana Kart Emulatörü)

HSM : Hardware Security Module (Donanım Güvenlik Modülü)

IBM : International Business Machines

ICOs : I-Ching operators

IDE : Integrated Development Environment

IDEA : International Data Encryption Algorithm (Uluslararası Veri Şifreleme Algoritması)

IP : Initial Permutation (İlk Yer Değiştirme)

IPs : Isomorphism of Polynomials

KBio : Biyometrik Anahtar

LAT : Lineer Approximation Table (Doğrusal Yaklaşım Tablosu)

LDA : Linear Discriminant Analysis (Doğrusal Ayırteden Analizi)

LP : Lineer Probability (Doğrusal Olasılık)

NFC : Near Field Communication (Yakın Alan İletişimi)

NIST : National Institute of Standards and Technology (Ulusal Standartlar ve Teknoloji Enstitüsü)

NL : Nonlinearity (Doğrusal Olmama)

PCA : Principal component analysis (Temel Bileşenler Analizi)

PIN : Personal Identification Number

POS : Point of Sales Terminal (Satış Noktaları Terminali)

RAM : Random Access Memory (Rastgele Erişimli Hafıza)

RC5 : Rivest Cipher 5

RCON : Round CONstant (Döngü Sabiti)

RFID : Radio Frequency Identification (Radyo Frekanslı Tanımlama)

RNA : Ribo Nükleik Asit (Ribonucleic Acid)

RSA : Rivest-Shamir-Adleman

SAC : Strict Avalanche Criterion (Katı Çığ Kriteri)

SAFER : Secure and Fast Encryption Routine (Güvenli ve Hızlı Şifreleme Rutini)

SIM : Subscriber Identity Module(Abone Kimlik Modülü)

s-kutu : Yerine koymalı kutu (Substitution box, s-box)

T : Timim

U : Urasil

WBC : White Box Cryptography Model (Beyaz Kutu Şifreleme Modeli)

Wi-Fi : Wireless Fidelity (Kablosuz Bağlantı Alanı)

XOR : eXclusive-OR (dışlayan veya)

YAİ : Yakın Alan İletişimi

ÖZET

DOKTORA TEZİ

MOBİL ÖDEME SİSTEMLERİNDE KİŞİSEL VERİLERİN GÜVENLİ SAKLANMASI İÇİN MODEL TASARIMI VE PERFORMANS ANALİZİ

Öznur ŞENGEL

İstanbul Üniversitesi-Cerrahpaşa

Lisansüstü Eğitim Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

Danışman : Prof. Dr. Ahmet SERTBAŞ

II. Danışman : Doç. Dr. Muhammed Ali AYDIN

Günümüzde mobil ödeme sistemlerinin kullanımı artmış ve bilgi ve güvenliği çok önemli konular haline gelmiştir. Mobil ödeme sistemi, kullanıcıların mobil uygulama para hesaplarını veya Mobil İletişim için Küresel Sistem faturasını kullanılarak güvenli ve hızlı bir ödeme kanalı üzerinden kişisel verilerinin iletildiği bir ödeme uygulamasıdır. Mobil ödeme sisteminin en önemli gereksinimleri hız, güvenlik ve fonksiyonelliktir. Son model mobil cihazlar parmak izi, yüz gibi farklı biyometrik verileri okuyabilmektedir ve bu özellikler daha güvenli uygulamalar sunmaktadır. Bu tez çalışmasında, mobil ödeme sisteminde kullanılan verilerin güvenli bir şekilde aktarılması için mobil ödeme sistemlerinin ana gereksinimleri göz önünde bulundurularak biyometrik veri ile model tasarımı ve analizi yapılmıştır. Oluşturulan modelde modern blok şifreleme ve akış şifrelemenin anahtar taşı olan yerine koymalı kutu uygulama kullanıcısının parmak izi biyometrik verisinin kullanılarak oluşturulması önerilmiştir. Parmak izi yerine koymalı kutular en güvenilir simetrik şifreleme algoritması için oluşturulmuş yerine koymalı kutular ile katı çığ kriteri, doğrusal olmama, doğrusal olasılık, bit bağımsızlık kriteri, diferansiyel olasılık gibi metrikler üzerinden karşılaştırılmıştır. Parmak izi yerine koymalı kutular bütünlük, rastgelelik ve güvenilirlik aralığı metrikleri açısından da değerlendirilmiştir. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasının yürütme süresi de hesaplanıp değerlendirilmiştir. Deneysel sonuçlar gösteriyor ki, önerilen parmak izi yerine koyma kutusu etkin ve biyometrik veri kullanılan mevcut yerine koymalı kutularından daha üstündür. Yerine koymalı kutu geliştirmek için parmak izi biyometrik verisinin kullanılması ile

oluşturulan bu başarılı model, mobil ödeme sistemlerinde kullanılmakta gelecek vaat etmektedir.

Ekim 2020, 176 sayfa.

Anahtar kelimeler: Yerine Koymalı Kutu, Biyometrik Veri, Parmak İzi, Mobil Ödeme Sistemi, Gelişmiş Şifreleme Standardı

SUMMARY

Ph.D. THESIS

MODEL DESIGN AND PERFORMANCE ANALYSIS FOR SECURE STORAGE OF PERSONAL DATA IN MOBILE PAYMENT SYSTEMS

Öznur ŞENGEL

Istanbul University-Cerrahpasa

Institute of Graduate Studies

Department of Computer Engineering

Supervisor : Prof. Dr. Ahmet SERTBAŞ

Co-Supervisor : Assoc. Prof. Dr. Muhammed Ali AYDIN

Nowadays, the usage of mobile payment systems has increased and information and its security have become very important topics. A mobile payment system is a kind of payment application that is transmitted personal data over a secure and fast payment channel by using either the mobile application money account or Global System for Mobile Communication bill of the users. The most important requirements of a mobile payment system are speed, security, and functionality. The latest model of mobile devices can read different biometric data such as fingerprint, face, etc. and these options offer more secure applications. In this study, a biometric model has been proposed and analyzed by considering the major requirements of the payment systems to transmit data securely. The substitution box which is the keystone of the modern stream and block ciphers, is proposed to generate by using fingerprint biometric data of the application user. The fingerprint substitution boxes are compared with existing s-boxes for the most reliable symmetric cipher over strict avalanche criterion, nonlinearity, linear probability, bit independence criterion, differential probability. The fingerprint substitution boxes are analyzed over bijectiveness, randomness, and confidence interval, as well. The execution time of the proposed efficient biometric s-box and inverse s-box generation algorithm is also calculated and examined. The experimental results have shown that the proposed fingerprint substitution box is efficient and superior to most of the existing biometric substitution boxes.

Resulting from applying fingerprint to generate a substitution box, such a successful model is promising to be used in mobile payment systems.

October 2020, 176 pages.

Keywords: Substitution Box, Biometric Data, Fingerprint, Mobile Payment System, Advanced Encryption Standard

1. GİRİŞ

Hayatımızın her alanında kendini gösteren teknoloji hızla gelişme göstermektedir. Teknoloji alanındaki hızlı gelişim ve değişim yaşamımızı her yönüyle değiştirmeye devam ederken alışkanlıklarımızı da değiştirmektedir. Günlük yaşamımızın vazgeçilmezi olan elektronik cihazlar akıllı olmaya devam ettikçe her işlemimizi bu cihazlar aracılığıyla yapar duruma geldik.

İnternet, e-posta, akıllı telefonlar ile iletişimi benimseyen Y ve Z kuşaklarının ödeme sistemlerindeki talep ve ihtiyaçları doğrultusunda yeni uygulamalar ve ödeme kanalları oluşmaktadır. Türkiye nüfusunun büyük çoğunluğunu oluşturan Y ve Z kuşakları alışverişlerini her an, her yerden, her türlü cihazdan daha hızlı ve kolay yapmayı istemektedir. Bu istekler doğrultusunda geliştirilen sistemlerde artık ödemelerimizi cep telefonu, saat, gözlük, vücut çipi, ten gibi her an yanımızdan ayırmadığımız araçlar üzerinden gerçekleştirebilmekteyiz. Günümüzde birçok ülkede giriş kapılarını açmak başta olmak üzere deri altına yerleştirilen çipler ile işlemler gerçekleştirilmektedir. BKMLab tarafından geliştirilen "akıllı gözlükle ödeme" sistemi ile akıllı gözlüğe entegre edilen uygulama aracılığıyla ödeme gerçekleştirebiliyoruz (Bankalararası Kart Merkezi, 2014). Tüm gelişmeler mobil ödeme uygulamalarının daha da artacağına işaret etmektedir.

Mobil ödeme sistemlerinin yaygın bir şekilde kullanılmaya başlanması bu uygulamalardaki verilerin güvenli bir şekilde saklanması konusunu gündeme getirmektedir. Özellikle ödeme sistemlerinin ortak kablosuz bağlantı alanlarında (Wireless Fidelity, Wi-Fi) kullanılması, kullanılan ağın anonim şifreye sahip olması veya şifresiz olması, basit şifre ve doğrulama yöntemlerinin kullanılması verilerin üçüncü şahıslar tarafından ele geçirilmesine olanak sağlamaktadır. Ödeme sistemleri geliştirilirken kullanıcının tüm bilgilerinin gizli kalması için güvenlik sistemlerinin güvenlik denetim yapıları kullanılmaktadır. Her sistemde olduğu gibi mobil ödeme sistemlerinde de bilgilerin güvenli bir şekilde tutulması ve güvenli bir şekilde iletilmesi için şifreleme ve kimlik doğrulaması yapılmaktadır.

İyi bir veri iletişimi, bilginin karşı tarafa kesintisiz, güvenilir ve hatasız gönderilmesi ile olmaktadır. Eğer iletim kanalı güvenli değilse, sistem veriyi şifreleme algoritmaları ile korumaktadır. Modern kriptoloji simetrik ve asimetrik şifreleme olmak üzere ikiye

ayrılmaktadır. Asimetrik şifreleme açık anahtar prensibine dayanmaktadır. Açık metin herkes tarafından bilinen anahtar ile şifrelenmektedir ve o anahtara ait gizli anahtar ile şifreli metin çözülmektedir. Simetrik şifreleme de tek bir anahtar şifreleme ve şifre çözme işlemlerinde kullanmaktadır. Simetrik şifreleme, blok şifreleme ve dizi (akış) şifreleme olarak iki ana başlıkta incelenmektedir. Bu çalışmada, blok şifreleme türü olan gelişmiş şifreleme standardı (Advanced Encryption Standard, AES) kullanılmaktadır. Gelişmiş şifreleme standardı, güvenilir veri ve bilgiyi korumak için dünyadaki tüm ülkeler ve birleşmiş milletler tarafından benimsenmiştir (Dworkin ve diğ., 2001).

Yerine koymalı kutu (Substitution box, s-box), Horst Feistel (1973) tarafından tanıtılan ticari bilgisayar şifrelemesinden beri blok şifrelemenin hayati önemi olan bir parçasıdır. N-bit girişli bir yerine koymalı kutu (s-kutu), $[0, 2^{n-1}]$ aralığından 2^n tane eleman içermektedir. Bir s-kutunun tüm elemanları tek ve farklı ise bu kripto s-kutu olarak adlandırılır. İyi oluşturulmuş bir s-kutusunun ardışık elementleri arasında bir korelasyon olmamaktadır (Sakallı ve diğ., 2006). Rijndael algoritması (Daemen ve Rijmen, 2000; Daemen ve Rijmen, 2002), Nyberg (1994) tarafından sonlu alana dayalı ters haritalama ile oluşturulan s-kutuyu kullanmaktadır. Rijndael algoritması basit matematiksel denklemden dolayı aradeğerleme saldırılarına karşı zayıftır. Aradeğerleme saldırılarına karşı algoritmanın daha sağlam olması için indirgenemez polinom kullanılmaktadır ve ters haritalamadan sonra afin dönüşüm uygulanmaktadır.

Gelişmiş şifreleme standardı bugün güvenilirliği ile hala bilgi teknolojisi dünyasında güvenlik için kullanılmaktadır. Bugünün teknolojisinde ürün ne kadar küçük boyutta olursa o kadar hızlı olması beklenmektedir. Bu yüzden, gelişmiş şifreleme standardı yeterli hızda olması için belleği çok az sayıda kullanmalıdır. Algoritmanın yazılım ve donanım gerçekleştirmesi için şifreleme ile ilgili işlemci kullanılmaktadır. Yazılım gerçekleştirmesi daha az maliyetli ve esnek yapıdayken donanım gerçekleştirmesi daha hızlı ve güvenilirdir.

Gelişmiş şifreleme standardı algoritmasının gücü yerine koymalı kutu ve sütun karıştırma işlemleri ile alakalıdır. Bu iki öğe doğrusal ve diferansiyel saldırılara karşı güvenilirliği garanti etmektedir. Daha dayanıklı gelişmiş şifreleme standardı algoritması için birçok bilimsel çalışma bulunmaktadır. Bu çalışmalardan bazıları algoritmanın anahtarına (Moosavi ve diğ., 2017; Chang ve diğ., 2004), bazıları algoritmanın döngülerine (Wadi ve Zainala, 2013; Kumar ve Rana, 2016), bazıları yerine koymalı kutuya (Canright, 2005; Tiessen ve diğ., 2015) ve bazıları matematik altyapısına odaklanmaktadır. Anahtar ve s-kutu oluşumu, fonksiyon kullanılarak

veya kullanılmayarak bir dizi matematiksel işlemler ile yapılmaktadır. Eşsiz parametreler ile özel bir fonksiyon elde etmek için çok farklı yöntemler bulunmaktadır. Kişisel eşsiz parametreler biometrik verilerden elde edilebilmektedir. Biometrik veriler her kişi için özel olduğundan daha fazla oranda eşsiz ve farklı parametre elde etmeyi sağlamaktadır. Algoritmanın daha güvenilir olması için ya biometrik verileri (Soutar ve diğ., 1998; Monrose ve diğ., 2001; Chang ve diğ., 2004; Costanzo, 2004; Chen ve Chandran, 2007; Jagadeesan ve Duraiswamy, 2010; Rashid ve Zaki, 2014; Abuguba ve diğ., 2015) ya da makine öğrenmesi tekniklerini (Noughabi ve Sadeghiyan, 2010; Santhi ve diğ., 2012; Kalaiselvi ve Kumar, 2016) kullanan birçok çalışma bulunmaktadır.

Mobil ödeme alıcının ürün ve/veya hizmet bedelini bir ödeme aracı kullanmadan sadece cep telefonu numarasını kullanarak ödemesini imkan sağlayan bir servistir. Mobil ödeme sistemlerinde güvenliğin sağlanması için kullanılacak algoritmanın belirlenmesinde şifreleme-şifre çözme hızı, güç tüketimi ve güvenlik en önemli etkenlerdendir. Literatürde şifreleme algoritmalarında özellikle simetrik şifreleme üzerinde özelleştirme çalışmaları bulunmaktadır. Mobil ödeme sisteminde kullanılacak şifreleme algoritmasının özelleştirilmesinde şifreleme ve şifre çözme hızının belli bir eşik değerini aşmayacak şekilde daha güçlü hale getirilmesi problemine çözüm aranmaktadır. Mobil ödeme sistemlerinde kaynak tüketiminin minimum, güvenliğin maksimum ve işlem hızının belirli eşik değerinin altında bir şifreleme algoritmasının belirlenmesi problemine çözüm olarak bu tez çalışmasında modern blok şifreleme ve akış şifrelemenin anahtar taşı olan özelleştirilmiş yerine koymalı kutu tasarlanmıştır.

Literatürde şu ana kadar şifreleme algoritmasının daha dayanıklı olmasına yönelik yukarıda belirtilen işlemleri kullanan çok fazla çalışma bulunmaktadır. Bu tez çalışmasında daha güvenilir, kişiye özel, daha az sürede s-kutu üretmek için yeni biometrik s-kutu ileri sürülmüştür. Çalışmanın literatüre en önemli katkılarından biri; kişinin kendisine ait biyometrik veriler ile eşsiz ve kişisel bir s-kutu üretim algoritmasının geliştirilmesidir. Önerilen algoritma, en kişisel biyometrik veri olan parmak izini ve parmak izine ait her bir özelliği ayrı ayrı kullanılması nedeniyle daha iyi bir entropiye ve rastgeleliğe sahiptir. Parmak izi, s-kutunun elemanlarının rastgele elde edileceği en iyi biyometrik kaynaktır. Parmak izinden elde edilen özellikler belirli bir işlem dizisine tabi tutularak biyometrik s-kutu üretilmektedir. Bilindiği kadarıyla, s-kutunun parmak izi kullanılarak üretildiği literatürde başka bir çalışma yoktur. Bu tez çalışmasının bir diğer önemli katkısı, s-kutu oluşturma algoritması sadece birkaç

milisaniyede biyometrik s-kutuyu üretebilmektedir. Önerilen biyometrik s-kutu algoritması minimum zamanda, maksimum rastgelelik ile kişiye özel s-kutu üretmektedir. Bu tez çalışmasında önerilen biyometrik s-kutu oluşturma algoritması ile üretilen s-kutuların iyi bir s-kutuya ait güvenlik metrikleri doğrultusunda elde edilen performans sonuçları daha önceki s-kutular ile karşılaştırıldığında algoritmanın etkili olduğunu göstermektedir.

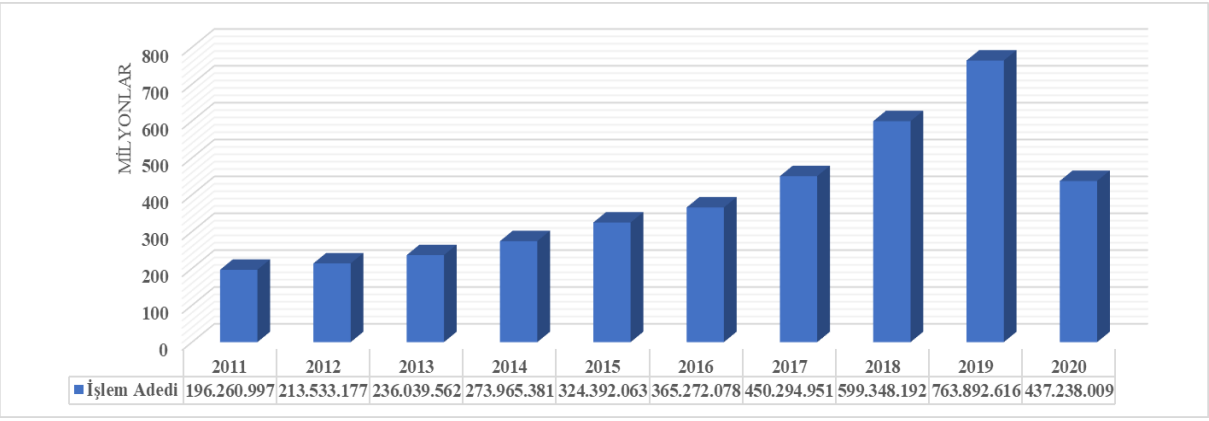
Tez çalışmasının Genel Kısımlar bölümünde mobil ödeme sistemleri, biyometrik veriler, şifreleme, şifreleme modelleri, şifreleme algoritmaları ve s-kutu hakkında genel bilgilerle birlikte tez konusu kapsamında literatürde yapılmış çalışmalara yer verilmiştir. Tez çalışması kapsamında kullanılan şifreleme modeli, şifreleme algoritması, biyometrik veri, önerilen s-kutu algoritması, önerilen ters s-kutu algoritması ve güvenlik performans metrikleri detaylı bir şekilde Malzeme ve Yöntem bölümünde açıklanmıştır. Önerilen s-kutu algoritması ile üretilen tüm s-kutular doğrusal olmama, bütünlük, katı çığ kriteri, bit bağımsızlık kriteri, doğrusal olasılık, diferansiyel olasılık gibi iyi bir yerine koymalı kutu kıstaslarına ilaveten güvenilirlik aralığı, rastgelelik, yürütme süresi metriklerinin sonuçlarına ve literatürdeki s-kutular ile karşılaştırma sonuçlarına Bulgular başlığı altında yer verilmiştir. Tartışma ve Sonuç bölümünde geliştirilen algoritmanın literatüre katkısı, performans sonuçlarına göre avantajlı ve dezavantajlı yönleri mevcut s-kutulara göre etkin olduğu yönlerinden bahsedilmiştir.

2. GENEL KISIMLAR

2.1. MOBİL ÖDEME SİSTEMLERİ

Teknoloji alanındaki hızlı gelişmelerin hayatımıza kattığı yeniliklerden biri de mobil ödeme teknolojileri ve hizmetleridir. Tüm dünyada ve ülkemizde tüketiciler, mobil cihazlarını iletişim hizmetlerinin yanı sıra bir ödeme aracı olarak kullanmaya başlamıştır. Özellikle akıllı telefon kullanıcıları, günlük hayatı kolaylaştırmaya yönelik sunulan hizmet çözümlerini yoğun olarak kullanmaktadır.

Bankalar Arası Kart Merkezi (BKM)'nin yayınladığı verilere göre Türkiye'de internet üzerinden yapılan kartlı ödemelerin sayısı Şekil 2.1'de görüldüğü gibi her yıl hızla artmakta ve 2020 yılının birinci ve ikinci döneminde (Ocak-Şubat-Mart-Nisan-Mayıs-Haziran) yaklaşık 438 milyon adet işlem gerçekleşmiştir. BKM'nin yayınlamış olduğu Kart Monitör (2017) raporuna göre yapılan anket sonucunda tüketicilerin %67'si cep telefonu, %44'ü kredi kartı, %26'sı internet üzerinden, %38'i nakit olarak, %9'u kol saati ile ödeme yöntemini tercih edeceğini belirtmiş. Bir önceki araştırma sonucuna göre cep telefonu ile ödeme yapmak isteyenlerin sayısı %25 artmıştır. Aynı araştırmaya göre tüketicilerin %44'nü market ve mağazalarda alışverişini cep telefonu ile yapmak istediğini ifade etmiştir. Yapılan araştırmalar gösteriyor ki, küçük ödemeler de dahil olmak üzere tüm ödeme işlemlerimizi kart üzerinden gerçekleştirmekteyiz. Gelişen teknoloji ve tüketicinin talebi yakın bir zamanda ödeme yapmak için kart taşımanın bile tarih olacağını göstermektedir.



Şekil 2.1: Mektupla/telefonla sipariş ve internette yapılan kartlı ödeme işlemleri adeti (Bankalararası Kart Merkezi, 2020).

Tüketiciler, yeni teknolojinin günlük ve tekrarlayan görevleri yerine getirmede kolaylık sağlamaya yönelik olmasını istemektedir. Örneğin, tüketiciler birçok ticari ve kişisel günlük ödemede hala nakit kullanılmasının zorunlu olmasını sorun olarak görmektedir. Bu sorunu en aza indirmek için yeni teknoloji tabanlı çözüm olan mobil cihazlar zengin hizmet seçenekleri ile ödeme araçları için ideal bir kanaldır. Mobil cihazın kullanımı ödeme başlangıcı için düşünülürken, temel ödemeler mevcut ödeme araçlarına dayanmaktadır.

Ülkemizde kapıda ödeme, elektronik fon transferi (EFT), havale gibi asenkron ödeme sistemleri, kredi kartı, banka kartı gibi kartlı ödeme sistemleri, BKM Express gibi çevrimiçi cüzdanlar, mobil operatörlerin ve bankaların kullandığı mobil cüzdanlar, kısa mesaj servisi tabanlı ödeme sistemleri, alt yapı sağlayıcılar ile ödeme sistemleri ve uygulama programlama arayüzü (Application Programming Interface, API) sağlayıcılar ile ödeme sistemleri kullanılmaktadır. Tüm dünyada kullanımı giderek artmakta olan mobil ödeme sistemleri ülkemizde de çevrimiçi cüzdan ve mobil cüzdan olarak yerli ve yabancı firmaların kullandığı sistemler olarak karşımıza çıkmaktadır. Genelde bankalar tarafından yenilenen ödeme araçları, mobil ödeme yöntemi söz konusu olduğunda mobil operatörlerinin sunduğu yenilikler öncülük etmeye başlamıştır.

Mobil ödeme, cep telefonumuzda kullandığınız hat üzerinden kredi kartı bilgisi ya da nakte ihtiyacımız olmadan kolay ve hızlı ödeme yapmayı sağlayan servistir. Mobil cihazımız ile satın aldığımız herhangi bir hizmet veya ürünün bedeli mobil iletişim için küresel sistem (Global System for Mobile Communication, GSM) faturası ile ya da hattımızda tanımlanmış olan bakiyeden alınarak ödenmektedir. Bu durumda mobil ödemeyi, tüm ödeme verisi ve işlemi mobil cihaz tarafından kabul edilen onaylanmış emrin iletilmesi ile gerçekleşen bir ödeme sistemi olarak tanımlayabiliriz.

Mobil ödeme sistemlerinin kurumsal ve bireysel kullanıcılar için

- Güvenli ve rahat alışveriş
- Müşteri güvenliğini ön planda tutan bir ödeme sistemi
- Hızlı alışveriş imkânı
- İnternet alışverişlerinde bilgilerin paylaşılması durumundan kurtulma
- Alışverişte zaman kavramının ortadan kalkması
- Satıcı ile yüz yüze olma zorunluluğunun ortadan kalkması

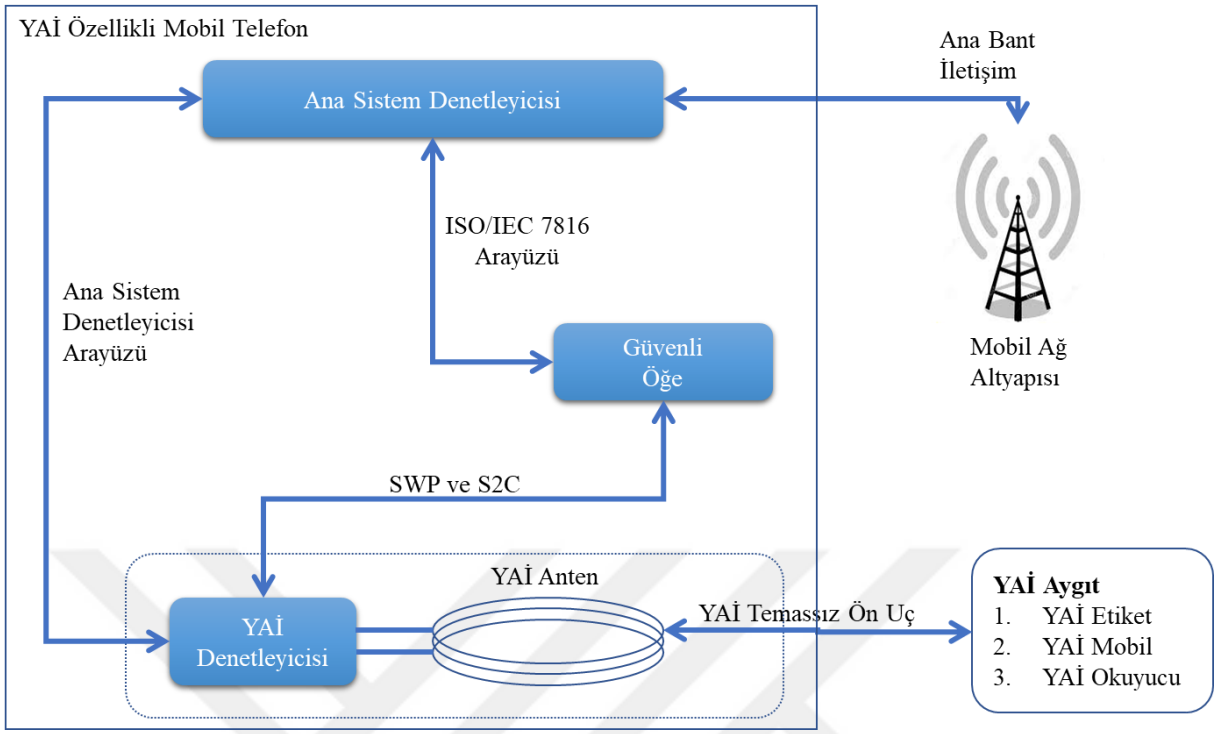
- İleri teknoloji ile uyumlu kurum farkındalığı
- Müşterilere hızlı ödeme ortamı kolaylığı sağlayarak daha fazla müşteriye hitap etme
- Rekabet üstünlüğü
- Farklı sektörlere ulaşma imkânı

gibi birçok avantajları bulunmaktadır.

Mobil ödemeler genel olarak "temassız" (proximity) veya "uzak" (remote) ödemeler olarak sınıflandırılır. Mobil temassız ödemeler için ödeme yapan ve alacaklı (ve / veya ekipmanı) aynı konumdadır ve yakın alan iletişimi (Near Field Communication, NFC), bluetooth veya veri aktarımı için kızılötesi gibi temassız radyo teknolojilerini kullanarak doğrudan birbirleriyle iletişim kurar. Mobil uzaktan ödemeler için işlem, GSM veya internet gibi telekomünikasyon ağları üzerinden gerçekleştirilir ve ödeme yapan kişinin konumundan ve / veya ekipmanından bağımsız olarak yapılabilir.

Mobil cihazın gerekli özelliklere sahip olması durumunda her iki türde ödemeyi gerçekleştirmek mümkündür. Örneğin, mobil uzaktan ödemeyi kullanan bir ödeme sistemi mobil telefonda kısa mesaj servisini kullanırken bir diğer sistem uygulamanın cihaza yüklenmesini isteyebilir. Mobil uzaktan ödeme modelinde güvenli unsur kullanılması gerekli değildir. Çünkü sistemin yapısına göre kimlik doğrulama ödeme hizmeti sağlayıcısının kullandığı yönteme uygun olarak tüketici (ödeyen taraf) ödeme sunucusundan doğrudan kimlik doğrulama yapmaktadır veya abone kimlik modülü (Subscriber Identity Module, SIM) kartlarında bulunan güvenlik özellikleri kullanılmaktadır. Mobil temassız ödemeler de (Şekil 2.2) güvenli öğenin (Secure Element) yansıra Yakın Alan İletişim Denetleyicisi (Near Field Communication Controller) ve uygulamanın güvenli çalışmasını garanti eden arayüzlerin olması gerekmektedir. Mobil temassız ödeme Yakın Alan İletişimine doğrudan erişip işlem noktası ile iletişim sağlayabilen ödeme kartı işlevini yerine getiren bir yazılımdır.

Yakın Alan İletişim (YAİ) teknolojisi 2003 yılından beri ISO RFID standardında yer alan, güvenilir temassız işlem yapabilmeyi ve kısa mesafeli elektronik cihazlara erişimi sağlayıp düşük güçlü veri alışverişi için kullanılan kablosuz bir teknolojidir. Müşteri ödemesini mobil satış noktası üzerinden gerçekleştirmek istediğinde gerekli donanıma sahip mobil telefonunu Satış Noktaları Terminali (Point of Sales Terminal, POS) cihazına yaklaştırarak şifreli veriyi iletmektedir. İletilen şifreli veri doğrulandıktan sonra ödeme gerçekleşmektedir.



Şekil 2.2: Yakın Alan İletişimine sahip mobil telefon yapısı.

Radyo Frekanslı Tanımlama (Radio Frequency Identification, RFID) teknolojisi radyo dalgalarını kullanarak YAİ teknolojisi gibi mobil POS ödemelerde RFID etiketinin okutularak veri transferinin yapıldığı YAİ teknolojisine göre daha uzun mesafeli ve daha az güvenli olan bir teknolojidir. YAİ teknolojisi RFID teknolojisine göre daha güvenli olsa da haksız kazanç sağlamaya yönelik ağın gizlice dinlenmesi ve izlenmesi gibi mobil ödeme merkezi etrafındaki alıcı ile satıcı arasındaki iletişim güvenliği konusu önem kazanmaktadır.

Mobil ödeme hizmetleri ve sistemlerinde dikkate alınması gereken önemli noktalar aşağıda verilmiştir.

- Ödeme işlemlerinin yapılması için doğrudan tüketiciden veya cihaz aracılığıyla alınan bilgilerin gizliliğinin korunması.
- Ödemeye yönelik güvenlik tedbirlerinin alınması.
- Mobil cihaz üzerinde verileri güvenli saklamak için yeterli alan sağlanması.
- Mobil cihaz üzerinde kişisel ve ödeme aracına ait bilgilerin düzenlenmesini sağlayan güvenli arayüzün tasarlanması.
- Sistemin (kullanılacak uygulamanın) tüketiciye maliyetinin ne olacağı net olarak bildirilmesi.

- Çocukların yapabileceği ödeme işlemlerine yönelik tedbirlerin alınması.
- Kullanılan uygulamalar içindeki otomatik ödeme talimatlarının kapsamlarının belirlenmesi.
- Kullanıcının ödeme seçeneğini belirleyebileceği arayüzün oluşturulması.

Mobil ödeme uygulamasında cihaza herhangi bir yazılım yüklemesi yapmadan cihazda bulunan YAİ anteni sayesinde ödeme gerçekleştirmek mümkündür. Hatta cihazın gücü tükenmiş olsa bile YAİ yongalarında var olan güç sayesinde cihaz ödeme işlemlerinde kullanılabilmektedir. İster uygulama yükleyerek isterse cihazda var olan donanım ile mobil ödeme sistemi geliştirilsin her iki durumda da en önemli konu tüketicinin mevcut durumunun korunması ve bilgilerinin gizliğinin esas alındığı güvenilir bir sistemin oluşturulmasıdır.

Mobil cihaz üzerinde bulunan uygulamalarda giriş ve ödeme işlemlerine yönelik farklı güvenlik parametreleri kullanılmıştır. Ülkemizde de yaygın olarak kullanılan ödeme işlemlerinin yoğun olarak yapıldığı mobil bankacılık sistemleri güvenliği arttırmak için sistem girişlerinde yeni yetkilendirme arayüzleri kullanmaya ve/veya veri iletimi esnasında şifreleme model ve algoritma yapıları oluşturmaya başlamış. Yapı kredinin ve birçok bankanın mobil sistemlerinde kullandığı iris okuyucu ile ödeme işlemleri herhangi bir şifre girişine ihtiyaç duymadan kimlik doğrulama sağlamaktadır.

Mobil uygulamalarda yetkilendirme için Tek Kullanımlık Şifre (One-Time Password), Ses Tabanlı Yetkilendirme (Voice Based Authentication), Görüntü Tabanlı Yetkilendirme (Image Based Authentication), Biyometrik Yetkilendirme (Biometric Authentication) gibi farklı yöntemler kullanılmaktadır.

Tek kullanımlık şifre ilk olarak Lamport (1981) tarafından ortaya çıkarılmıştır. Bu sayede sisteme her girişte farklı şifre üretilmektedir. Gong ve diğ. (2013) tarafından yapılan çalışmada Kimlik Sorma/Yanıt Verme yöntemi (Challenge-Respond Method) ile her isteğe bir şifre üretilmiştir. Bu sistemi daha iyi hale getirmek için Huang ve diğ. (2013) tarafından yapılan çalışmada şifre üretimine zaman etiketi gibi farklı parametreler eklenerek şifrenin tahmin edilebilirliğini ortadan kaldırılmaya çalışılmıştır.

Ses tabanlı yetkilendirme, yüksek sesle şifrenin söylenmesi üçüncü şahısların şifreyi öğrenmesine neden olduğundan çok fazla tercih edilmeyen bir yetkilendirme olsa da Khitrov

(2013) tarafından yapılan çalışmada ses tabanlı yetkilendirmeye ek olarak biyometrik tabanlı şifre oluşturmanın parametre olarak eklenebileceğini vurgulamaktadır.

Resim tabanlı yetkilendirmede, sisteme girişte bir veya daha fazla resmin seçilmesi (Dhamija ve Perrig, 2000; Brostoff ve Sasse, 2000) ve her girişte bu resimlerin doğru şekilde seçilmesi ile sisteme giriş kabul edilmektedir. Wiedenbeck ve diğ. (2005) tarafından yapılan çalışmada kullanılan "PassPoint" sistemi ile giriş şifresi olarak birden fazla resim sıra ile seçilmektedir ve sisteme girişlerde bu sıranın da aynı olması beklenmektedir. Bu sistem daha sonra mobil sistem üzerinde kullanılmaya başlanmıştır. Jansen (2003) ilk çalışmasında belirli sayıdaki resimler sadece bir kez seçilirken, Jansen (2004) tarafından yapılan diğer çalışmada aynı resme birden fazla kez seçilme hakkı tanınmıştır. Gong ve diğ. (2013) tarafından yapılan çalışmada dokunmatik ekrana sahip cihazlarda kişinin kendi belirlemiş olduğu bir resmi seçmesi sonucu bu resim 30 ayrı parçaya bölünmektedir. Kullanıcı bu parçalardan 3 veya 6 adet resmi şifre olarak seçmektedir. Sisteme her girişte bu resimleri seçerek kimlik doğrulaması yapmaktadır.

Yang ve Hwang (2015) tarafından yapılan çalışmada temassız ödeme yapısında kullanılan güvenli elemanı kullanarak yeni kişisel verilerin korunması konsepti geliştirmişler. POS cihazının normal çalışma prensibine sadece güvenli unsurun içinde çalıştırılabilinen ve yüklenen EMV (Europay Mastercard Visa) çekirdek yazılım modülü denenmiş. Fakat güç tüketimi ve alan yetersizliğinden dolayı EMV çekirdek normal verilerin işlendiği ve güvenli verilerin işlendiği yer olacak şekilde iki parçaya ayrılmıştır.

2.2. BİYOMETRİK VERİ

Biyometrik veri insanın fiziksel ve davranışsal karakter özellikleridir. Biyometrik veri kişilerin bir sisteme, cihaza veya veriye erişimini sağlamak ve kişinin kendisi olduğunu doğrulamak için kullanılan dijital verilerdir. Parmak izi, ses, el yazısı, retina, yüz biyometrik sembollere birer örnektir. Tüm bu tanımlayıcıların her birey için o bireye özel olduğu düşünülmektedir ve tanımlayıcıların kesinliğini arttırmak için biyometrik verilerin kombinasyonları kullanılmaktadır.

Biyometrik şifreleme, kullanan sistemlerde kimlik doğrulama için herhangi bir bilgiyi aklında tutmak veya yanlarında bir kart taşıma zorunluluğu olmadan bireyin kendine ait bir özelliğini kullanarak sistemi kullanmasına dayanmaktadır. Biyometrik sistemlerde parmak izi, el geometrisi, yüz, ses, iris, retina gibi bireyin fiziksel özelliklerini kullanarak veya imza, dudak

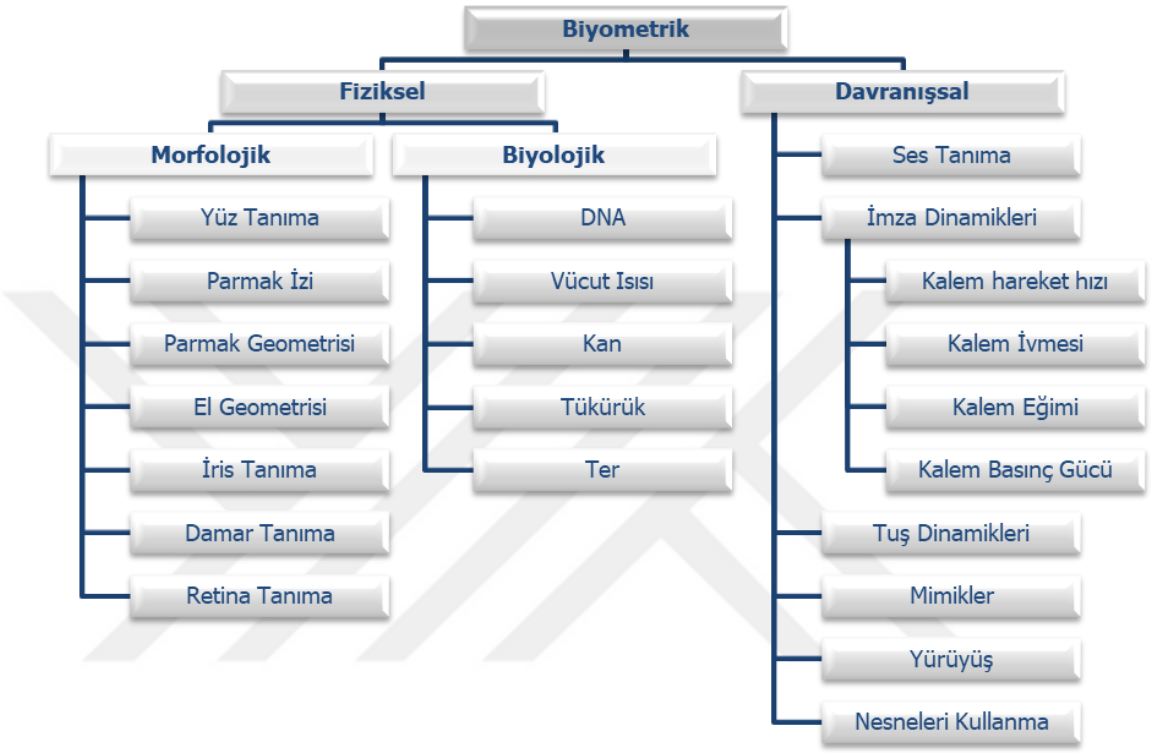
hareketleri, yazı şekli, yürüyüş şekli gibi aktif olarak o anlık davranışsal olarak elde edilen veriler kullanılmaktadır (Şekil 2.3). Kullanılan verinin bireye ait olmasından dolayı başkasına devretme, unutma, kaybetme gibi durumlarla karşılaşılması mümkün değildir. Biyometrik verilerin kaza dışında değiştirilmesi, çalınması, kaybedilmesi tehlikesi olmadığı gibi sabit verilerde değildir, zaman içerisinde değişikliğe uğrayabilmektedir. Diğer kimlik doğrulama yöntemlerine göre sağladığı güvenlik kriterleri daha fazla olduğunda güvenliğin yüksek olması gereken sistemlerde giriş parametresi olarak kullanılmaktadır.



Şekil 2.3: Biyometrik veri örnekleri.

Günümüzde birçok alanda biyometrik veri kullanılmaktadır. Bilgisayar ve elektronik aletler parmak izi ile kullanıcıyı doğrulayarak sistemin kilidini açmaktadır. Sunucu odalarının kapıları sistem yetkililerinin yüzlerini algıladığında açılmaktadır. Yardım masası sistemleri bir çalışanın destek hattındaki sesini tanıdıklarında ilgili bilgileri otomatik olarak alabilir. Bankacılık işlemlerinde, resmi işlemlerde, digital işlemlerde, bankamatik (Automated Teller Machine, ATM) kullanımında, internet alışverişlerinde, mobil alışverişlerde biyometrik teknikler kullanılmaktadır. Güvenlik söz konusu olduğunda biyometrik tekniklerin birçok avantajı olmasına rağmen bazı ek gereksinimleri de söz konusu olmaktadır. Biyometrik teknikleri kullanan sistemler genellikle ek maliyet gerektirir, yapının kullanımı konusunda uzmanlık gerektirebilmektedir, kişinin biyometrik bilgilerinin çalınmasında yenilenmesi mümkün olmamaktadır.

Biyometrik teknoloji Şekil 2.4'te gösterildiği gibi iki kategoriye ayrılmaktadır: fiziksel ölçümler ve davranışsal ölçümler. Fiziksel ölçümler davranışsal ölçümlerden daha fazla ayırt edicidir. Davranışsal ölçümler stres gibi kişiyi anlık etkileyen durumlara göre farklılık gösterebilir.



Şekil 2.4: Biyometrik teknolojisi kategorileri.

Fiziksel ölçümler, kişinin doğumu ile birlikte oluşan herkeste farklılık gösteren biyometrik ölçümlerdir. Morfolojik ve biyolojik verilerden oluşabilirler. Yüz tanıma, parmak izi, parmak geometrisi, el geometrisi, iris tanıma, damar tanıma, retina tarama morfolojik verilere DNA eşleşmesi, kan, tükürük, ter ve vücut ısısı biyolojik verilere örnek olarak verilebilir.

Davranışsal ölçümler, kişinin anlık durumuna göre karakteristik özellikleri ile ortaya çıkan biyometrik ölçümlerdir. Ses tanıma, kalemin hareket hızı, ivmesi, eğimi, basınç gücü gibi imza dinamikleri, tuş dinamikleri, nesneleri kullanma yolu, ses adımları, mimikler ve yürüyüş davranışsal ölçümlere örnek olarak verilebilir.

En sık kullanılan biyometrik verilerin tanımı ve kullanım alanlarına örnekler aşağıda verilmiştir.

- Parmak izi her kişide farklılık gösteren parmaktaki eşsiz deseni oluşturmaktadır. 1960 yılında ortaya çıkan parmak izi tanıma sistemleri en çok pasaport başvurusu ve kimlik tespitlerinde, akıllı telefon gibi teknolojik aletlerin kilidini açmak için şifre olarak kullanılmaktadır.
- İris tanıma kişinin gözünün renkli bölgesi olan kısmının oluşturduğu benzersiz desenleri tanımlamaktadır. 1990 yılının başlarında ortaya çıkan iris tanıma sistemleri havaalanı giriş çıkış kontrollerinde, güvenlik alanlarında sıklıkla kullanılmaktadır, tüketici pazarında genellikle tercih edilmez.
- Yüz tanıma kişinin yüz hatlarını oluşturan desenlerin oluşturduğu tanımadır. Güvenlik ve kanun uygulamalarında, kimlik doğrulama akıllı telefon gibi teknolojik aletlerde kilidi açmak için kullanılmaktadır.
- Retina tanıma kişinin gözünün tamamının eşsiz desenlerinin belirlenmesinin oluşturduğu tanımadır. Genelde iris tanıma ile karıştırılmaktadır. Güvenlik sistemlerinde giriş izni için kullanılmaktadır.
- Ses tanıma kişinin bir cihazla konuşurken benzersiz ses dalgalarını ölçüp tanımlamasıdır. Banka hesabınız hakkında arama yaparken kimliğimizi doğrulamak için kullanılabilir. Akıllı telefonlarda uygulamayı sesli komutlar ile yönlendirmede kullanılır.
- El geometrisi bir kişinin elinin uzunluk, kalınlık, genişlik ve yüzey alanını ölçer ve kaydeder. Genellikle havaalanları, nükleer güç istasyonları, güvenlik alanındaki uygulamalarda kullanılmaktadır.
- İmza herkesin farklı bir yazı stili olduğundan yazdıkları hız bir harften diğerine gitme hızı kaleme yaptığı basınç, yazının eğikliği gibi özelliklerin tanımlanmasıdır.
- Damar tanıma kişinin el vb. uzvundaki damarların yapısına belirlenmesidir. Çok sık kullanılmamaktadır.
- DNA tanıma kişinin DNA dizilimin yapısal motifinin oluşturulması ve bu dizilimin tanımlanmasıdır.

Güvenlik söz konusu olduğunda birçok şifreleme algoritması biyometrik veriler ile güçlendirilmeye çalışılmıştır. Anahtarın oluşturulması gibi şifreleme algoritmalarında önem arz eden bileşenlerin oluşturulmasında biyometrik verinin de eklenmesiyle kişiye ait özel bilginin olması sistem güvenilirliği arttıran unsur olmuştur.

Vigila ve diğ. (2015) tarafından yapılan çalışmada mobil telefon üzerindeki uygulamalarda parmak izi ile korumayı arttıran uygulama geliştirmişlerdir. Sistemde var olan parmak izi okuyucusundan parmak izi alınmaktadır. İlgili resimden özellik çıkarma metodu ile parmak izi üzerindeki özellikler çıkarılır. Delaunay triangulation indexing (DTI) yöntemi ile [V, R] Voronoi diagram çıkarılır ve lookup tabloları oluşturulur. Tablolar sunucu ve istemci tarafında kaydedilir ve güvenlik açısından anlamsız (dummy) değerler eklenir. Mobil sistemlerde beklenen özelliklerden güvenliği arttırmak ve anahtar boyutunu küçültmek için Eliptik Eğri Şifreleme (Elliptic Curve Cryptography, ECC) ile şifreli metin üretilir ve sunucuya gönderilir. Sunucu gelen veriyi çözerek metni elde eder. Biyometrik anahtar sunucu ve istemcilerdeki lookup tablolarında kayıtlı olan indeks değerlerinden oluşturulur. Hash fonksiyonunda zaman etiketi (timestamp) ve Voronoi değerlerini kullanarak 224 bit uzunluğunda biyometrik anahtar (KBio) üretilmektedir.

Dandawate ve Inamdar (2015) tarafından yapılan çalışmada yüz için dijital kamera, parmak izi için parmak izi okuyucu sensör ve palm vein sensör ile üç farklı veri elde etmektedir. Her bir veri için ayrı ayrı ön işlem gerçekleştirilerek özellikleri çıkarılmaktadır. Yüzdeki özellikleri çıkarmak için Temel Bileşenler Analizi (Principal component analysis, PCA), Doğrusal Ayırteden Analizi (Linear Discriminant Analysis, LDA) ve Gabor Wavelet metotları, parmak izi için Curvlet Transform, Wavelet PCA metotları kullanılmıştır. Çıkan tüm özellikleri kapsayan tek bir matris oluşturulmaktadır, oluşan matriste Discrete Cosine Transform (DCT) uygulanmaktadır. Şifreleme için RSA algoritması kullanılmıştır.

Faquih ve diğ. (2015) tarafından yapılan çalışmada kablosuz sensör ağları için gerekli olan güvenlik kriterlerini, anahtar dağıtım yaklaşımlarını ele alarak iki veya daha fazla şifreleme tekniğini birleştiren hibrit bir güvenlik yapısı önermiştir. Önerilen yapı sayesinde sistem simetrik ve asimetrik şifrelemenin yapılarını kullanıp daha etkin ve kolay bir yapıda bilgiyi şifreleyebilecektir. Açık anahtar şifreleme ile anahtarın şifrelenmesi ve simetrik anahtarlama ile verinin şifrelenmesi genellikle kullanılan bir yapıdır.

Shankar ve Eswaran (2016) tarafından yapılan çalışmada görsel şifreleme üzerinde gizli resim karartma yöntemi ile (k, n) şifreleme yöntemi oluşturulmuştur. Gönderilecek resim piksel değerlerine (h x w) ayrılmaktadır ve R, G, B değerleri çıkarılmaktadır. Paylaşım sayısı “n”in 1 eksiği kadar “h x w” değerlerinden oluşan rastgele matris oluşturulmaktadır. Üç adet rastgele sayı üretilip artan sırada değerler sıralanır ve dört ana matris oluşturulur. Şifrelemeyi

gerçekleştirebilmek için her renk bileşeni için anahtar matris üretilmektedir. Oluşan ana matrisler ile ilgili anahtar matris XOR operasyonu sonucu dört ayrı paylaşım (share) elde edilir. Elde edilen paylaşım kullanıcıya gönderilmektedir. Tüm paylaşımlar alındığında gizli resim elde edilmiş olur.

Panchal ve Samanta (2016) tarafından yapılan çalışmada anlık parmak izi okuyucusundan alınan görüntüyü geliştirdikleri 5 adımlık işlem serisinden geçirerek biyometrik anahtar oluşturmaktadırlar. Oluşturulan anahtar ile veriler şifrelenip şifreli metin oluşturulmaktadır. Farklı kalitedeki aynı parmak izinden alınan görüntülerden aynı anahtarı %97 başarı oranı ile elde etmişler.

Ang ve diğ. (2005) çalışmalarında parmak izini iki durumda kullanmışlardır: 1) Kullanıcı U (User)'nun parmak izinin şablonu T (Template) oluşturulup (U, T) ikilisi veri tabanında saklı tutulur, 2) yetkilendirmek için kullanıcı U'nun parmak izi okunur R (Reader), eğer okunan R ile T eşleşirse kullanıcı sisteme kabul edilir. Anahtar k ve şablon T kullanılarak iptal edilebilir biyometrik Tc oluşturulmaktadır. Anahtarı iki şekilde saklamaktadırlar: 1) kullanıcı ve iptal edilebilir biyometrik eşlemesi (U, Tc), 2) kullanıcı, iptal edilebilir biyometrik eşlemesi ve anahtar (U, Tc, k).

Chang ve diğ. (2004) çalışmalarında biyometrik veriden ayırt edilebilir özellik çıkarımını Doğrusal Ayırteden Analizi ile gerçekleştirip grafik elde etmektedir. Elde edilen veri üzerinden özgün ortalamanın global ortalamadan k kez büyük olduğu alan ayırt edilebilir özellik olarak kabul edilip ikili formata çevrilir.

Santhi ve diğ. (2012) çalışmalarında 24 adet resmin bulunduğu veri tabanından bir resim seçilmektedir. Seçilen resimden GLCM özellik çıkarımı yapılmaktadır, Temel Bileşenler Analizi ile boyut azaltma gerçekleştirilmiştir. Bu işlemleri gerçekleştirirken ölçümler sırsında farklı matematiksel işlemlere başvurarak farklı matrisler elde etmektedir. Elde ettiği matrisleri birleştirip şifrelemede kullanacağı anahtarı oluşturmaktadır.

Abuguba ve diğ. (2015) çalışmasında hem yüz hem de iris biyometrik verilerini kullanarak 256 bitlik anahtar üretmektedir. Özellik çıkarımı, yüz özellik çıkarımı ve anahtar üretimi olmak üzere üç modülden oluşmaktadır. Yüz ve iristen özellik çıkarımları sonucu oluşan 256 bitlik matrislerin her elemanı kontrol edilmektedir. Yüz matrisinin i. indisi 0 ise iris matrisindeki i.

indisinin ikili formattaki 0'ların sayısı, yüz matrisinin i. indisi 1 ise iris matrisindeki i. indisinin ikili formattaki 1'lerin sayısı olacak şekilde anahtar üretilmektedir.

Chen ve Chandran (2007) çalışmasında yüz resimlerini kullanarak AES için 128 bitlik anahtar üretmektedir. Yüz resimlerini Radon dönüştürücü ve Iterative dönüştürücü sonucunda ikili hale getirmektedir. Özellik çıkarımı ile biyometrik anahtar oluşturulmaktadır. Oluşturulan anahtar Rees-Solomon kodlama ile anahtar ve başvuru çizelgesi (lookup) tabloları oluşturulmaktadır.

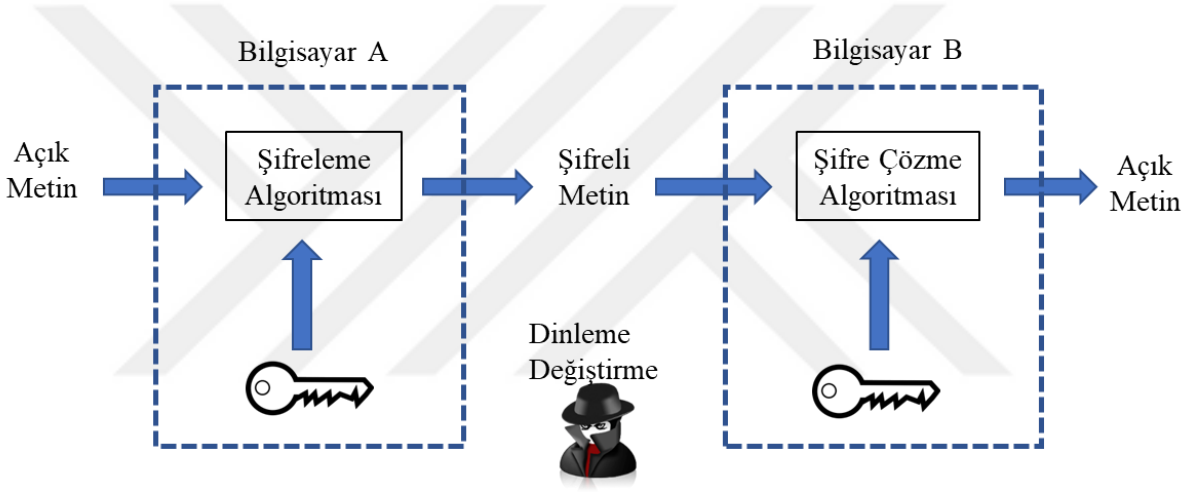
Literatürde ve uygulama alanında biyometrik yöntemler üzerinde birçok çalışma yapılmıştır. Bu çalışmaların bazıları ve çalışmalarda kullanılan tekniklerin açıklaması Tablo 2.1'de verilmiştir.

Tablo 2.1: Literatürde kullanılmış diğer teknikler.

Çalışma	Kullanılan teknikler
Uludağ ve diğ. (2004)	Biyometrik şablonla bir şifreleme anahtarını monolitik olarak birleştirmektedir, bu şekilde anahtar geçerli bir biyometrik kimlik doğrulaması olmadan çözümlenemez.
Singhvi ve diğ. (2009)	Yinelemeli tek yönlü dönüşümün çıktısından bit dizisi üretmek için Reed-Solomon hata kodlama kodları ile entropi bağımlı özellik çıkarma işlemi entegre edilmiştir.
Wu ve diğ. (2010)	Yüz biyometrisine bağlı biyometrik kriptosistem oluşturulmuştur. Şifreleme aşamasında Temel Bileşen Analizi (PCA) kullanılır.
Nguyen ve Nguyen (2008)	Özel anahtarı şifrelemek ve özel anahtarı güvenli bir şekilde korumak için Biyometrik Şifreleme Anahtarı (BEK).
Ratha ve diğ. (2007)	Parmak izi görüntülerinden çoklu iptal edilebilir tanımlayıcılar.
Rathgeb ve Uhl (2009)	İkili biyometrik şablonlardan biyometrik anahtarlar üretme. İkili iris kodları, bulanık biyometrik verilerden anahtarlar oluşturmak için kullanılır.
Hao ve diğ. (2006)	İris biyometriğini kriptografik uygulamalara dahil etmek için güvenli bir yol. Hadamard ve Reed-Solomon kodlarını birleştiren iki katmanlı hata düzeltme tekniği kullanılmaktadır.
Gong ve diğ. (2008)	İris özellik tabanlı PKI anahtar oluşturma şeması. PKI anahtar üretimi için daha uzun ve ek ayırt edilebilir bit akışı üretilebilir.
Connie ve diğ. (2005)	Palmprint şablonları, ayırt edici bir kod elde etmek için sözde rastgele anahtarların bir araya getirilmesiyle (hashlemek) elde edilir.
Jo ve diğ. (2007)	Biyometri yardımıyla dijital imza ve kriptografi iletişimi üretmek için basit bir teknik.

2.3. ŞİFRELEME

Eski çağlardan beri özellikle diplomasi ve savaşlarda bilginin gizli tutulması önemli bir konu olmuştur. Hızla gelişen teknoloji ile askeri, elektronik, mobil ve banka gibi birçok sistemin en önemli ihtiyaçlarından biri verinin güvenli bir şekilde taşınması ve gizliliğidir. Geçmişten günümüze verinin güvenli bir şekilde iletilmesi için farklı şifreleme algoritması ile şifrelenmiş ve hala çözümlenmemiş birçok eser bulunmaktadır. Eski Mısırlılar anıtlara yazdıkları resimli yazıları, İbraniler kutsal kitaplarındaki bazı kelimeleri, Julius Caesar, Sezar şifresi olarak bilinen yerine koyma şifresi ile verileri, Leon Alberti bir şifre tekerleği kullanarak verileri şifrelemiştir.



Şekil 2.5: Şifreleme sistemi.

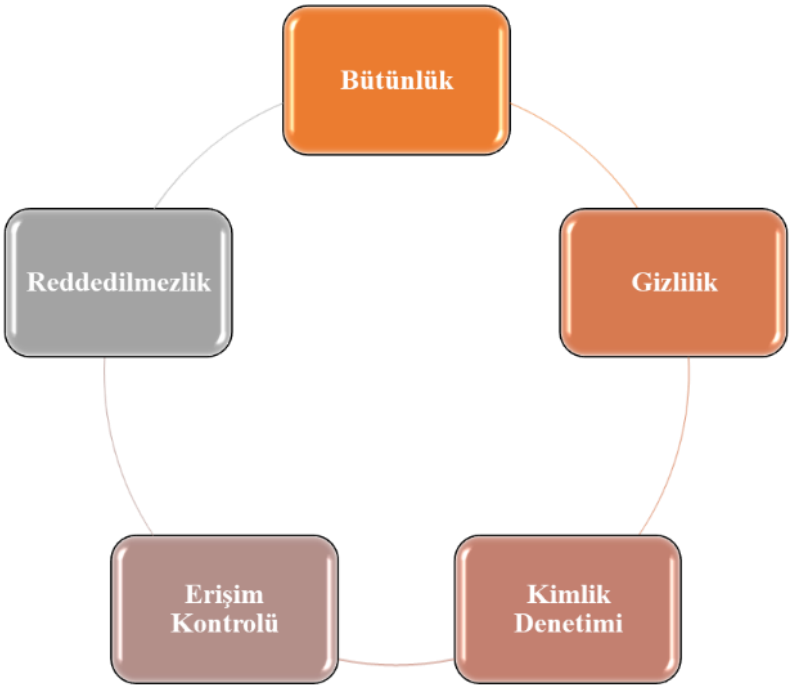
Şifreleme, şifre bilimi ve şifre analizi bilimi olmak üzere iki ana bölümden oluşmaktadır. Şifre bilimi bakışımlı (symmetric) ve bakışımsız (asymmetric) şifreleme türlerinden birini kullanarak bilginin gizlenmesini, şifre analizi bilimi şifreli bir sistemin açıklarının tespit edilmesini ele almaktadır. Şifrelemeyi verinin iletimi sırasında güvenliğini ve değiştirilmesini önlemeye yönelik yapılan işlemler bütünü olarak tanımlayabiliriz. Geleneksel şifreleme mantığına bakacak olursak, şifreleme ve şifre çözme olmak üzere iki kısımdan oluşmaktadır. Şekil 2.5' te Bilgisayar A, ağı dinleyen bir gözlemcinin gönderilecek veri hakkında bilgi edinemeden gönderebileceği güvenli bir kanal üzerinden veriyi Bilgisayar B'ye göndermek istemektedir. A ve B bilgisayarlarının bildiği gizli bir anahtar ile veri Bilgisayar A tarafından şifreleme algoritması ile şifrelenmektedir. Şifrelenen veri güvenli veya güvenli olmayan bir kanal üzerinden Bilgisayar B'ye gönderilmektedir. Bilgisayar B aldığı şifreli metni daha önceden bildiği gizli anahtar ile şifre çözme algoritmasında çözerek veriyi elde etmektedir.

Şifreleme ve şifre çözme işlemlerini yapabilmek için algoritmalar kullanılmaktadır. Şifreleme algoritması (Encryption algorithm, E) düz metnin (Plain text, P) gizli bir anahtar (K) ile şifreli metne (Ciphertext, C) dönüştürülmesi adımlarını içermektedir. Denklem (2.1)'de gösterildiği gibi ifade edilmektedir. Şifre çözme algoritması (Decryption algorithm, D) şifreli metnin (C) gizli bir anahtar (K) yardımıyla düz metne (P) dönüştürülmesi adımlarını içermektedir. Denklem (2.2)'de gösterildiği gibi ifade edilmektedir.

$$C = E(P, K) \tag{2.1}$$

$$P = D(C, K) \tag{2.2}$$

Şifreleme teknikleri bir sistemde Şekil 2.6'da verilen Bütünlük, Gizlilik, Kimlik Denetimi, Erişim Kontrolü ve Reddedilmezlik kriterlerini sağlamak amacı ile kullanılmaktadır. Bütünlük ile gönderilen mesajın üzerinde değişiklik ve/veya düzenleme yapılmadığı, Gizlilik ile bilginin başkalarının eline geçmesinin engellenmesi, Kimlik Denetimi ile alıcı ve gönderenin kimliklerinin doğrulanması, Erişim Kontrolü ile yetkisi olmayan kişilerin erişiminin engellenmesi, Reddedilmezlik ile gönderen ve alıcı yaptığını inkar edememesi amaçlanmaktadır.



Şekil 2.6: Şifreleme teknikleri.

Şifreleme sisteminde kullanılan algoritmalar, düz metinden şifreli metni elde etme işleminin türü, kullanılan anahtar sayısı ve düz metnin işlenme şekli olmak üzere birbirinden bağımsız üç kategoride incelenebilir. Tüm şifreleme algoritmaları düz metinden şifreli metni elde etmek için, düz metindeki her öğe (bit, harf, karakter vb.) diğer bir öğe ile eşleştiren yerine koymalı (substitution) ve düz metindeki her öğeyi yeniden düzenleyen karılmaya dayalı (transposition) iki genel prensibe dayanmaktadır. Kullanılan anahtar sayısına göre gönderen ve alıcının aynı anahtarı kullandığı gizli anahtarlı ve gönderen ve alıcının farklı anahtar kullandığı açık anahtarlı olarak iki ana kategoriye ayrılmaktadır. Düz metnin işlenme şekline göre öğeleri bir blok olarak işlendiği blok şifrelemesi ve öğelerin tek tek işlendiği akış şifrelemesi olarak ikiye ayrılır.

Geçmişten günümüze sezar şifreleme, yerine koymalı şifreleme, Vigenere şifreleme, Vernam şifreleme, permütasyon şifreleme, açık anahtarlı şifreleme, gizli anahtarlı şifreleme gibi birçok şifreleme yöntemi kullanılmıştır.

2.3.1. SEZAR ŞİFRELEME

Mono alfabetik şifreleme olan ve ilk kez Romalı Julius Caesar tarafından kullanılan Sezar şifreleme yöntemi harflerin ötelenmesine dayanan yerine koymalı şifreleme yöntemidir. Tablo 2.2'de gösterildiği gibi kelimenin yazıldığı alfabenin harf sırasının 3 harf kaydırılması (K=3) ile şifre tablosu oluşturulur. Oluşan şifre tablosu kullanılarak Denklem (2.3) kullanılarak düz metindeki her harfe karşılık sayısal değer yazılarak şifreli metin oluşturulmaktadır. Şifreli metinden düz metin elde etmek için Denklem (2.4) kullanılmaktadır.

$$C \equiv P + 3 \ (mod\ 29) \qquad 0 \leq C < 29, 0 \leq P < 29 \tag{2.3}$$

$$P \equiv C - 3 \ (mod\ 29) \qquad 0 \leq C < 29, 0 \leq P < 29 \tag{2.4}$$

"MERHABA" kelimesini düz metin olarak ele aldığımızda M harfi Tablo 2.2.'de 15 değerine karşılık gelmektedir. Denklem 2.3'te P değerini 15 olarak düzenlediğimizde C değeri 18 olarak hesaplanır ve Ö harfi elde edilir. Tüm harfler için işlem tekrarlanır ve "ÖĞTJÇÇ" şifreli metni elde ederiz.

Tablo 2.2: Sezar şifreleme veri tablosu.

Düz metin (P)		Şifreli metin (C)		Düz metin (P)		Şifreli metin (C)	
A	0	Ç	3	M	15	Ö	18
B	1	D	4	N	16	P	19
C	2	E	5	O	17	R	20
Ç	3	F	6	Ö	18	S	21
D	4	G	7	P	19	Ş	22
E	5	Ğ	8	R	20	T	23
F	6	H	9	S	21	U	24
G	7	I	10	Ş	22	Ü	25
Ğ	8	İ	11	T	23	V	26
H	9	J	12	U	24	Y	27
I	10	K	13	Ü	25	Z	28
İ	11	L	14	V	26	A	0
J	12	M	15	Y	27	B	1
K	13	N	16	Z	28	C	2
L	14	O	17				

2.3.2. YERİNE KOYMALI ŞİFRELEME

Yerine koymalı şifreleme yönteminde alfabedeki her harf bir kurala bağlı olmaksızın başka bir harf ile değiştirilir. Tablo 2.3'te görüldüğü gibi kelimenin yazıldığı alfabenin harf sırası rastgele bir sıraya karşılık gelerek şifre tablosu oluşturulur. Düz metindeki her harfin tablodaki karşılığı bulunarak şifreli metin elde edilir. "MERHABA" kelimesini düz metin olarak ele aldığımızda her harfi Tablo 2.3'teki karşılığını bulup yazdığımızda "DZEVKTK" şifreli metni elde ederiz.

Tablo 2.3: Tablo yöntemi şifreleme veri tablosu.

P	**C**	**P**	**C**	**P**	**C**	**P**	**C**	**P**	**C**	**P**	**C**
A	K	E	Z	I	C	M	D	R	E	Ü	Y
B	T	F	B	İ	L	N	Ş	S	Ü	V	N
C	A	G	Ö	J	S	O	Ç	Ş	M	Y	İ
Ç	J	Ğ	P	K	Ğ	Ö	U	T	R	Z	F
D	O	H	V	L	I	P	H	U	G		

Şifreli metinden düz metin elde etmek için aynı şifreleme tablosunda şifreli karakterlerin (C) yerine karşılık gelen P değerleri yazılır. "ŞKÜCIÜCŞ" kelimesini şifreli metin olarak ele aldığımızda her harfi Tablo 2.3'teki karşılığını bulup yazdığımızda "NASILSIN" düz metnini elde ederiz.

2.3.3. VIGENERE ŞİFRELEME

Çoklu alfabetik şifreleme olan Vigenere şifrelemede n harften oluşan bir anahtar kelime seçilir. Düz metin seçilen anahtar kelimenin uzunluğu kadar eşit parçaya bölünür. Denklem (2.4) kullanılarak düz metindeki (P) her harfe karşılık sayısal değer yazılarak şifreli metin (C) oluşturulmaktadır.

$$C_a \equiv P_a + K_a \ (mod\ 29) \qquad 0 \leq C < 29, 0 \leq P < 29, 1 \leq a \leq n \qquad (2.4)$$

"MERHABA" kelimesini düz metin ve "SEN" kelimesini anahtar kelime olarak ele aldığımızda düz metin "MER HAB A" şeklinde bloklara ayrılır. "M" harfinin ve "S" harfinin sayısal karşılıkları Denklem (2.4) kullanılarak "G" olarak şifrelenir. Tüm bloklar şifrelendikten sonra "GIGBEO" şifreli metin elde edilir.

2.3.4. VERNAM ŞİFRELEME

Vernam şifreleme tek kullanımlık karakter dizisi (One-Time Pad) Gilbert Sandford Vernam tarafından bulunmuştur. Rastgele üretilen bir karakter dizisi kullanılmaktadır. Düz metindeki her karakter üretilen rastgele dizide karşılık gelen karakter ile modüler toplama işlemine tabi tutularak şifreli metin oluşturulmaktadır. Modüler toplama işlemi bit seviyesinde yapılmaktadır.

"MERHABA" açık metnini Verman şifreleme ile şifrelemek için " i#yt%n+" karakter dizisini kullandığımızda "M" karakteri "i" karakteri ile modüler toplama işlemine tabi tutulduğunda Tablo 2.4'te görüldüğü gibi "$" şifreli karakteri elde edilir. Tüm karakterler için işlem tekrar edildiğinde "$f+<d,j" şifreli metin elde edilir.

Tablo 2.4: Vernam şifreleme ile modüler toplama işlemi.

“M” karakteri	**“i” karakteri**	**“$” karakteri**
1	1	0
0	1	1
0	0	0
1	1	0
1	0	1
0	0	0
1	1	0

2.3.5. PLAYFAIR ŞİFRELEMESİ

Playfair şifreleme 5x5 boyutlu matrise alfabedeki harflerin yerleştirildiği en bilindik çoklu harf şifrelemedir. Şifreleme için belirlenen anahtar kelimede tekrar eden harfler bir kez kullanılacak şekilde matrise yerleştirilir. Alfabede geri kalan harfler sıra ile I/J aynı hücrede yer alacak şekilde yerleştirilir. Düz metin iki harfli bloklara ayrılır, ikili bloklarda tekrar eden harfler varsa iki harfin arasına “X” harfi konulur. Şifreleme için aşağıdaki kurallar uygulanır.

1. Düz metindeki iki harf aynı sütunda yer alıyorsa harflerin altlarındaki satırda yer alan harf ile şifrelenir.
2. Düz metindeki iki harf aynı satırda yer alıyorsa her harf sağ tarafındaki harf ile şifrelenir.
3. Yukarıdaki koşulları sağlamıyorsa düz metindeki harfleri bir dikdörtgenin köşeleri olarak düşünüp diğer köşelerdeki harfler (harfin aynı satır komşusu) ile şifrelenir.

“CRYPTOGRAPHY” anahtar kelimesi ile Tablo 2.5’teki matris oluşturulur. “HELLO” düz metni ikili bloklara ayırdığımızda iki “L” harfi arasına “X” harfi yerleştirip “HE LX LO” elde ederiz. “HE” bloğu 3. kurala göre “GI” veya “GJ” olarak, “LX” 3. kurala göre “QU” olarak, “LO” 1. kurala göre “UD” olarak şifrelenir. “GIQUUD” şifreli metin elde edilir.

Tablo 2.5: Playfair şifreleme matrisi örneği.

C	R	Y	P	T
O	G	A	H	B
D	E	F	I/J	K
L	M	N	Q	S
U	V	W	X	Z

2.3.6. HILL ŞİFRELEME

1929 yılında matematikçi Lester Hill tarafından geliştirilen blok şifreleme yönteminin kullanıldığı doğrusal cebire dayanan şifrelemedir. Açık metin, belirlenen anahtar matris boyutuna uygun olacak şekilde bloklara ayrılır. Verilen anahtar matrisi ile açık metin matrisi çarpılır, elde edilen sonuçlar karaktere dönüştürülür.

$$C_a = \mathrm{E}(P_a, \mathrm{K}) = P_a \cdot \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} (mod\ 29) \tag{2.5}$$

"BCÇD" anahtarı ile 2x2 matris elde edilir. "MERHABA" düz metni anahtar boyutuna göre bloklara ayrılır, eksik kalan blok olduğunda belirlenen bir harf ile doldurulur. "MERHABA" düz metni "ME RH AB AZ" şeklinde ikili bloklara ayrılır. "BCDE" anahtar metni ile her bloktan Denklem (2.5) kullanılarak şifreli blok elde edilir. "ME" bloğunu "ÜG" olarak, "RH" bloğu "HH" olarak, "AB" bloğu "CD" olarak, "AZ" bloğu "YÜ" olarak bulunur ve "ÜGHHCDYÜ" şifreli metni elde edilir.

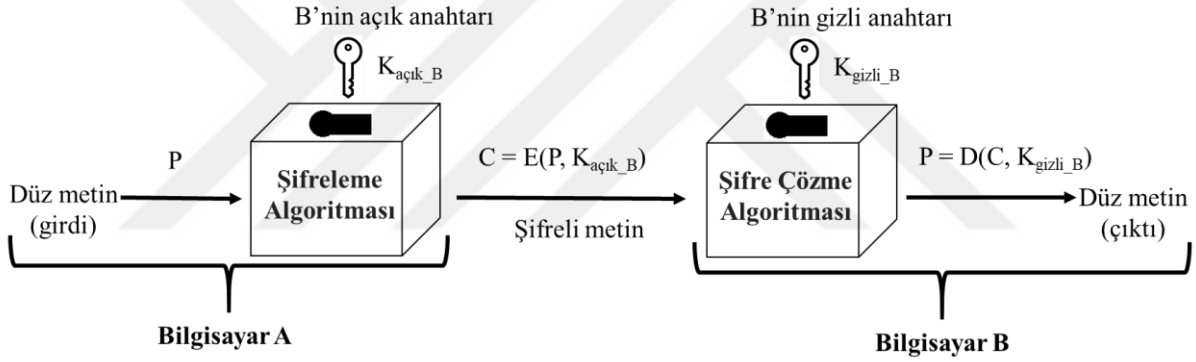
2.3.7. PERMÜTASYON ŞİFRELEME

Permütasyon şifreleme modern simetrik sistemlerin tasarımının temel parçalarından biridir. Permütasyon dönüşüm anahtarı belirlenir, anahtar uzunluğuna göre düz metin parçalara ayrılır. Dönüşüm anahtarındaki yapıya göre düz metinde yer alan karakterler yeniden yerleştirilir. Her parça sırası değiştirilmeden yana yana dizilir ve şifreli metin elde edilir. "MERHABA" düz metnini Denklem (2.5) belirtilen permütasyona göre (harfleri 24135 sırasında olacak şekilde değiştir.) 5 karakterlik parçalar ayrılıp boş kalan kısımlara karakter eklenerek "MERHA BATKS" elde edilir. Permütasyon kuralı her blok için uygulandığında "EHMRAAKBTS" şifreli metin elde edilir.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix} \quad (2.5)$$

2.3.8. AÇIK ANAHTARLI ŞİFRELEME (BAKIŞIMSIZ ŞİFRELEME)

Açık anahtarlı şifreleme yerine koyma ve permütasyon kullanılmasından ziyade matematik fonksiyonların dayanmaktadır. Açık anahtarlı şifreleme bakışımsız, iki ayrı anahtarın kullanıldığı, bilginin şifrelenmesinin yanı sıra iki tarafın kullanacağı anahtarın güvenli olarak belirlenmesi ve değiş tokuş edilmesi, sayısal imzalar ile kimlik doğrulama ve bilgi bütünlüğünün korunması alanlarında kullanılmaktadır. Açık anahtarlı şifreleme algoritmaları şifreleme ve şifre çözme için birbiri ile ilişkili gizli ve açık anahtar olmak üzere iki farklı anahtar kullanmaktadır. Deffie-Helman (DH), Rivest-Shamir-Adleman (RSA), ElGamal ve Paillier bilinen açık anahtarlı şifreleme algoritmalarıdır.



Şekil 2.7: Açık anahtarlı şifreleme algoritmalarının çalışma yapısı.

Algoritma birbiri ile haberleşecek makinelerin şifreleme ve şifre çözme algoritmalarında kullanacağı anahtar çiftleri üretmektedir. Her kullanıcının bildiği açık anahtar ve o açık anahtar ile şifrelenen metni çözmek için kullanılan gizli anahtarı bulunmaktadır. Şekil 2.7'de görüldüğü gibi Bilgisayar A gizli bir mesajı Bilgisayar B'ye göndermek istediğinde açık metni Bilgisayar B'nin açık anahtarı ile şifrelemektedir. Şifreli metnin ulaştığı Bilgisayar B kendi gizli anahtarını kullanarak şifreli metni çözmektedir. Gizli anahtar sadece Bilgisayar B'de bulunduğundan şifreyi sadece kendisi çözebilmektedir.

2.3.8.1 RIVEST-SHAMIR-ADLEMAN ALGORİTMASI

Açık anahtarlı şifreleme yapısının en iyi karşılayan ve yaygın bir şekilde kabul gören Rivest-Shamir-Adleman (RSA) algoritması (Rivest ve diğ., 1978) blok şifreleme yapısını

kullanmaktadır. Diffie and Hellman (1976a, 1976b) tarafından yayınlanan açık anahtarlı şifreleme yapısı için MIT'de Ron Rivest, Adi Shamir, and Len Adleman tarafından 1977 yılında geliştirilmiş ve 1978 yılında yayınlanmıştır.

Denklem (2.6) kullanarak düz metinden şifreli metin, Denklem (2.7) kullanılarak şifreli metinden düz metin elde edilir. Gönderen *e* değerini, alıcı *d* değerini, gönderen ve alıcı *n* değerini (açık anahtar = {e, n}, gizli anahtar = {d, n}) bilmektedir. Anahtar üretimi için öncelikle iki asal sayı (p, q) seçilir. Asal sayıların çarpımı (n = pq) ve asal sayıların bir eksiklerinin çarpımı (Φ(n)= (p-1)(q-1)) hesaplanır. Φ(n) değerinden küçük ve asal, bir hariç e değeri seçilir. Seçilen e değeri ile d değerini çarptığımızda sonucun mod Φ(n) değerinin 1'e eşit olmasını sağlayan d değeri bulunur.

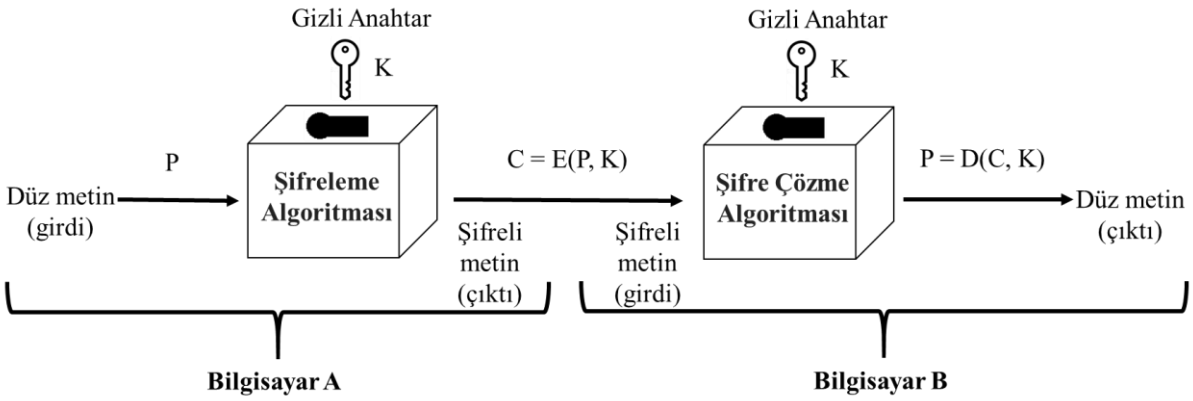
$$C = P^e \pmod{n} \tag{2.6}$$

$$P = C^d \pmod{n} \tag{2.7}$$

2.3.9. GİZLİ ANAHTARLI ŞİFRELEME (BAKIŞIMLI ŞİFRELEME)

Gizli anahtarlı şifreleme bakışımlı, şifreleme ve şifre çözme işlemlerinde tek anahtarın kullanıldığı yerine koyma ve/veya dönüştürme yapılarına dayanan şifreleme algoritmalarıdır. Gönderici şifreli metin ile belirlenmiş gizli anahtarı da göndermektedir bu yüzden anahtarın karşı tarafa güvenle iletilmesi gerekmektedir. Sezar, Vigenere, Veri Şifreleme Standardı (Data Encryption Standard-DES), Triple DES (3DES), RC5, Blowfish, IDEA, SAFER, Gelişmiş Şifreleme Standardı (Advanced Encryption Standard-AES) bilinen gizli anahtarlı şifreleme algoritmalarıdır.

Şekil 2.8'de görüldüğü gibi Bilgisayar A gizli bir mesajı Bilgisayar B'ye göndermek istediğinde açık metni Bilgisayar B'nin gizli anahtarı ile şifrelemektedir. Şifreli metnin ulaştığı Bilgisayar B aynı gizli anahtarı kullanarak şifreli metni çözmektedir.



Şekil 2.8: Gizli anahtarlı şifreleme algoritmalarının çalışma yapısı.

2.3.9.1. VERİ ŞİFRELEME STANDARDI

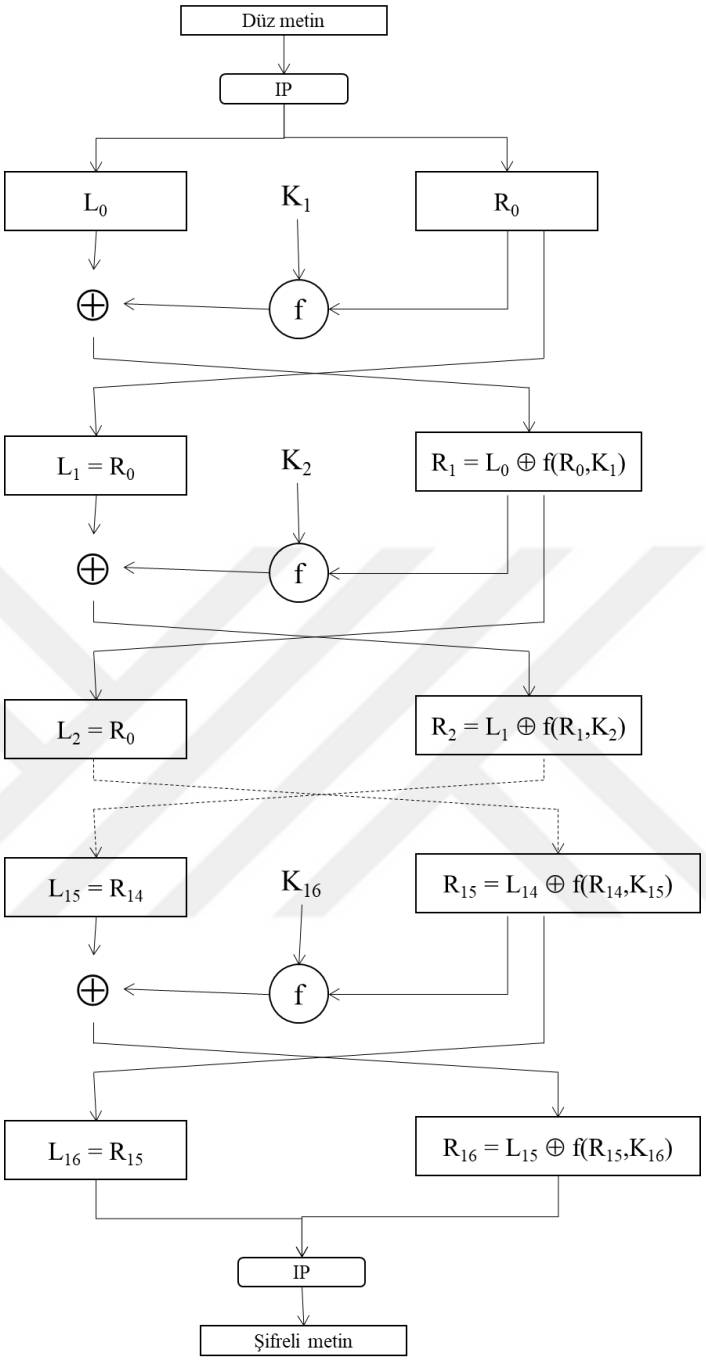
1973 yılında Ulusal Ölçütler Bürosu Federal Kütükte bulunan şifreleme sistemleri için bir talepte bulunduğunda IBM tarafından geliştirilmiş LUCIFER (Feistel, 1973) olarak bilinen şifreleme sisteminin yeniden yapılandırılmış halidir. Veri Şifreleme Standardı, 1977 yılında şimdi Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology, NIST) olarak bilinen Ulusal Standartlar Bürosu (National Bureau of Standards) tarafından Federal Bilgi İşleme Standardı 46 (Federal Information Processing Standard 46, FIPS PUB 46) olarak en çok kullanılan şifreleme şemasıdır. DES yapısında kullanılan yöntem veri şifreleme algoritmasıdır (Data Encryption Algoritm, DEA). DEA ile şifrelenmemiş 64 bitlik düz metnin 56 bitlik anahtar kullanılarak şifrelenip 64 bitlik şifrelenmiş metin elde edilmektedir. DES simetrik şifreleme prensibine dayanan blok şifreleme algoritmasıdır. Veri bloklarını şifrelemede ve şifreli metni çözmede aynı algoritma ve anahtarı kullanılır.

Şekil 2.9'da yer alan düz metnimiz x olsun, öncelikle Denklem (2.8) kullanılarak ilk yer değiştirme kuralına göre (Initial Permutation, IP) 32 bitlik sol (L_0) ve 32 bitlik sağ (R_0) olacak şekilde iki parçaya bölünerek x_0 oluşturulmaktadır. DES algoritması, ilk bölünmeden sonra 16 adımda tekrar eden bir işlem gerçekleştirmektedir. Her adımda L_i Denklem (2.9) verildiği gibi R_i Denklem (2.10) verildiği gibi her adımda anahtarda (K) eklenerek hesaplanmaktadır.

$$x_0 = IP(x) = L_0R_0 \tag{2.8}$$

$$L_i = R_{i-1} \tag{2.9}$$

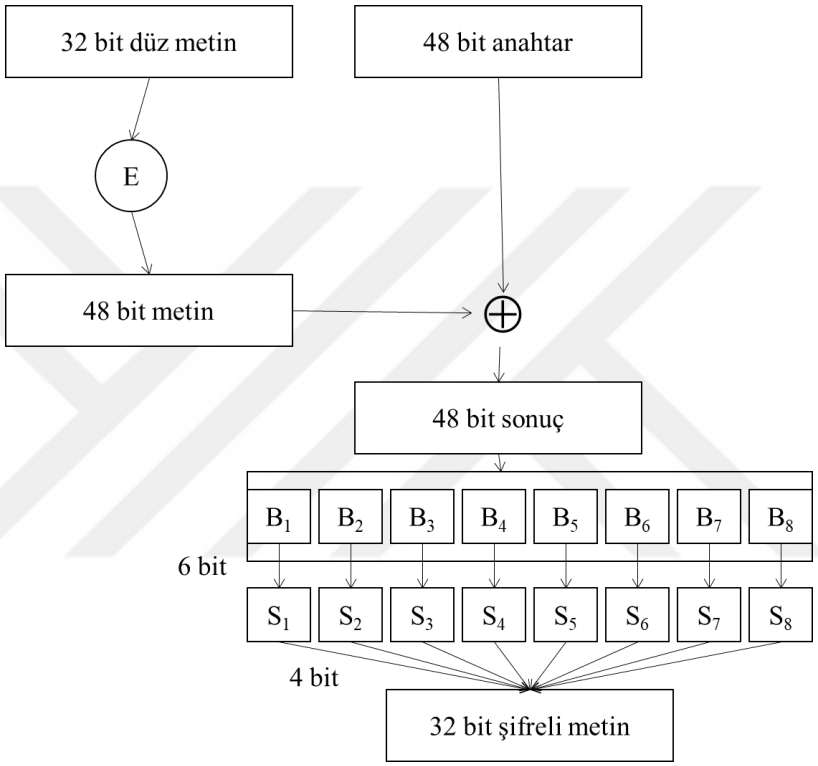
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \tag{2.10}$$



Şekil 2.9: Veri şifreleme standardının çalışma yapısı.

Denklem (2.10) kullanılan f fonksiyonunun çalışma şeması Şekil 2.10'da verilmiştir. 32 bit uzunluğundaki ilk değeri alıp E genişletme fonksiyonu (expansion permutation) ile 16 bitinin ikişer kez tabloda yer alması ile 48 bitlik veri haline getirilir. E fonksiyonu sonucu elde edilen veri ile 56 bitlik anahtar veriden seçilen 48 bitlik veri dışlayan veya (exclusive-or) işlemine tabi tutulur. Sonuç olarak, sekiz adet altışar bitlik katarların yan yana dizilmiş hali elde edilir. Daha sonra 32 bit üreten 8 yerine koymalı kutu içerisine gönderilir ve tekrar değiştirilir.

Şekil 2.10'da belirtilen yerine koymalı kutular her S_i (i = 8) içinde 0 ile 15 arası tamsayılar bulunan 4 x 16'lık değişmeyen bir dizidir. 6 bit olarak verilmiş olan B_j $S_j(B_j)$ olarak hesaplanır. $B_j = b_1b_2b_3b_4b_5b_6$ ise b_1b_6 'nın ikili gösterimi S_j'nin r satırını ($1 < r < 3$); $b_2b_3b_4b_5$ ise S_j'nin c sütununu ($0 < c < 15$) gösterdiğini varsayalım. Buna göre $S_j(B_j) = S_j(r,c)$ şeklinde ifade edilir ve dört bit uzunlukta ikili biçimde yazılır ve 32 bitlik sonuç elde edilir. Son adımda elde edilen L_{16} ve R_{16} son olarak yer değiştirmeden geçirilerek şifreli metin elde edilir.



Şekil 2.10: Veri şifreleme standardında yer alan f fonksiyonunun çalışma yapısı.

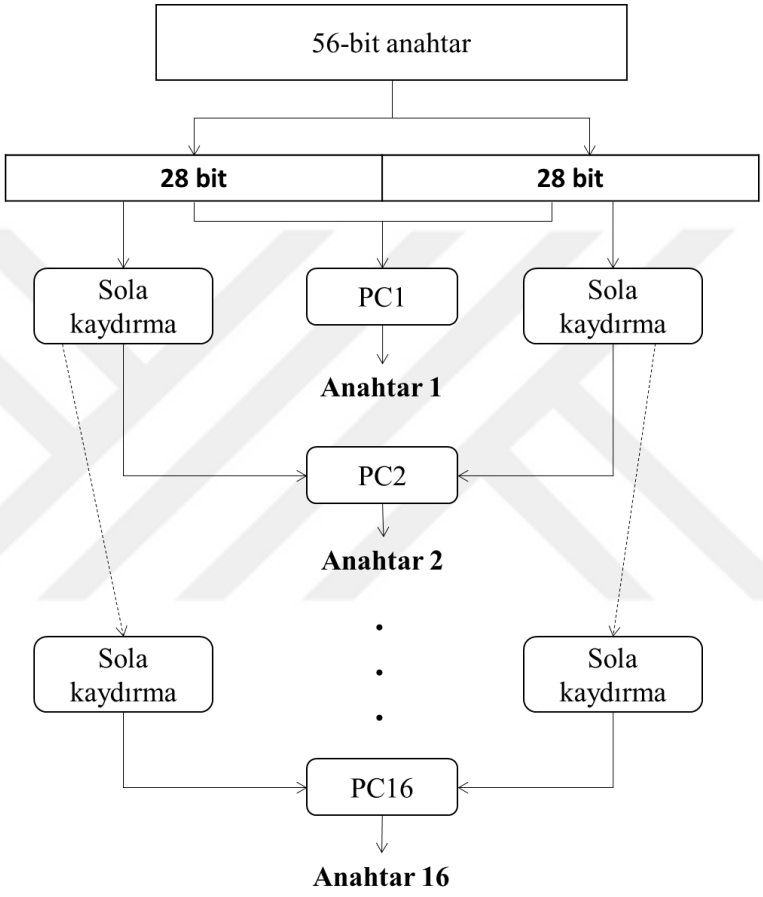
DES algoritmasında 64 bit uzunluğundaki anahtarın 56 biti anahtarı içerirken 8 biti eşlik denetim bitini olarak kullanılmaktadır. Eşlik denetim biti anahtarın elde edilmesinde kullanılmamaktadır. Şekil 2.11'de gösterildiği gibi 56 bitlik anahtar öncelikli olarak iki parçaya ayrılır. C_0 anahtar bitinin ilk 28 bitlik kısmını, D_0 anahtar bitinin son 28 bitini temsil ettiğini varsayalım.

Denklem (2.11) ve (2.12) algoritmanın her turunda anahtar bitinin değişimi göstermektedir. Denklem (2.11) ve (2.12) yer alan LS fonksiyonu i değerine bağlı olarak bir ya da iki adım sola ötelemeyi gösteren dairesel öteleme işlemidir. Öteleme işleminde i değeri 1, 2, 9, veya 16 değerlerinde bir adım sola diğer durumlarda iki adım sola öteleme yapılır. Her öteleme işlemi

sonucunda anahtar elde edilmesi için Şekil 2.11'de belirtilen PC1, PC2, …, PC16 sabit yer değiştirme fonksiyondan geçer.

$$C_i = LS_i(C_{i-1}) \qquad 1 \leq i \leq 16 \tag{2.11}$$

$$D_i = LS_i(D_{i-1}) \qquad 1 \leq i \leq 16 \tag{2.12}$$

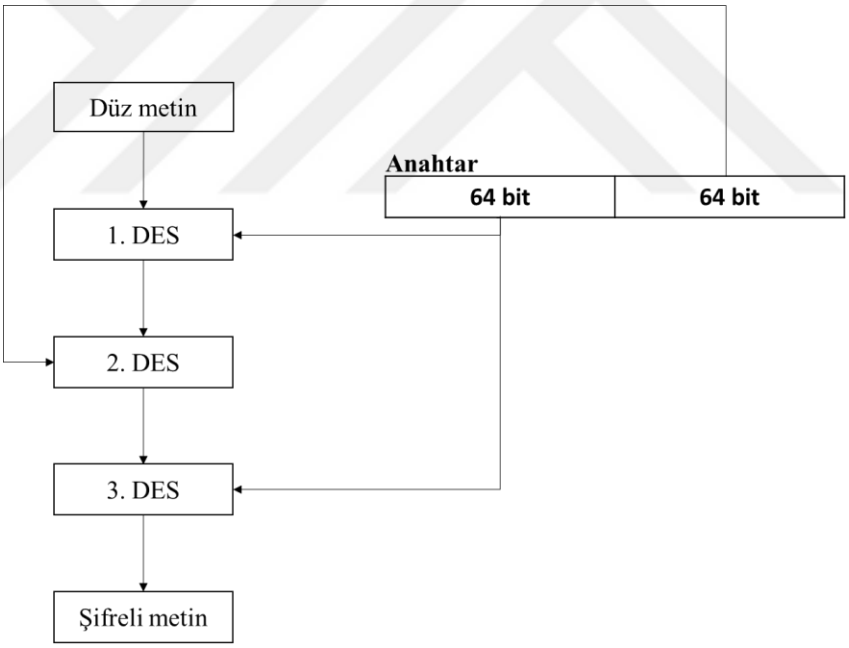


Şekil 2.11: Veri şifreleme standardında anahtarın elde edilmesi.

DES algoritması 1997 yılında RSA güvenlik firmasının düzenlenen bir konferansta İngilizce bir cümleyi DES algoritması ile şifreleyerek web sayfalarına koyduklarını ve şifreyi çözene para ödülü verileceğini ilan etti. "DESCHALL" adlı gönüllülerden oluşan bir takım 5 ay sonra şifreyi kaba-kuvvet yöntemi ile (brute-force) kırdıklarını ve düz metnin "Strong cryptography makes the world a safer place" olduğunu duyurdular. Kriptografi uzmanlarının da belirttiği yargı olan DES'in güçlü bilgisayarların ortak düzenlediği bir kaba kuvvet saldırısı ile kırılabileceğini kanıtlamış oldu. Zaman içinde bilgisayarları işlem hızının artması ile saldırılar daha kolay hale gelmiştir.

2.3.9.2. ÜÇLÜ VERİ ŞİFRELEME STANDARDI

DES algoritmasının zaman içinde kırılması ve kaba-kuvvet saldırılarına karşı koymakta zorlandığı için hem yeni bir şifreleme algoritması bulma çalışmaları hem de var olan standardı güçlü hale getirme çalışmaları hız kazanmıştı. DES algoritmasının daha güçlü versiyonları anahtar uzunluğunun arttırılmasıyla ortaya çıktı. Mevcut DES algoritmasının çift DES, üçlü DES gibi versiyonları kullanılmaya başlanmıştır. Üçlü DES, 1978 yılında IBM tarafından geliştirilmiştir. Üçlü DES çift yönlü çalıştığından şifrelenmiş veri geri çözülebilir. DES algoritmasına göre üç kat daha yavaş çalışmaktadır. Anahtar boyutu 64 bitten 128 bite çıkarılmış, çalışma yapısı aynen korunmuştur. 128 bitlik anahtar öncelikle iki 64 bitlik parçaya bölünerek DES yapısına anahtar olarak verilmiştir. Anahtar girdileri ardışık yapıda kullanılmamıştır. Şekil 2.12'de gösterildiği gibi, ilk 64 bitlik parçası birinci ve üçüncü DES yapısına, ikinci 64 bitlik parçası 2. DES yapısına anahtar girişi olarak verilmektedir.



Şekil 2.12: Üçlü veri şifreleme standardının çalışma şeması.

Bankacılık sistemi, ciddi güvenlik programları ve elektronik ödeme sistemlerinde kullanılmaktadır. Bilgisayarın donanımsal açıklarını kapattığı gibi çift yönlü çalıştığından istenildiği zaman şifre çözülebilir. Güvenlik anahtarın zorluğu ile doğru orantılıdır. Zayıf anahtar şifrenin kolay çözülmesine neden olur. Üçlü DES algoritmasından daha gelişmiş olan AES algoritmasına göre altı kat daha yavaş çalışmaktadır.

2.3.9.3. GELİŞMİŞ ŞİFRELEME STANDARDI

Joan Daeman ve Vincent Rijmen Rijndael ismiyle 1997 yılında Ulusal Standartlar ve Teknoloji Enstitüsü tarafından ilan edilen yarışmaya katılmış ve 2000 yılından itibaren veri şifreleme standardının yerini geliştirilmiş şifreleme standardı olarak belirlenmiştir. Yeni algoritma farklı anahtar boyutuna izin vermesi, çeşitli donanımlar üzerinde çalışabilir olması, hız ve kriptografik güç bakımından daha iyi olması özelliklerini barındırmaktaydı.

Gelişmiş şifreleme standardı 128 bit düz metin ve 128, 192 ve 256 bit olmak üzere üç farklı anahtar uzunlukları ile şifreleme sağlamaktadır. Algoritma anahtar uzunluğuna göre AES-128, AES-192 ve AES-256 olarak adlandırılmaktadır. Şifreleme ve şifre çözme algoritmaları için 128 bit uzunluğundaki girdi 4x4 kare matris şeklinde bloklara ayrılmaktadır. Matrisin her öğesi 8 bit uzunluğunda veri içerir ve her satır ve sütunda 32 bit uzunluğunda veri bulunmaktadır. Şifreleme ve şifre çözmenin her bölümünde blok durum dizisine (state array) aktarılır. Durum dizisinin her satırı sözcük (word) olarak adlandırılır. Algoritmanın anahtar uzunluğuna göre döngü sayısı, sözcük uzunluğu ve matris uzunluğu değişmektedir. Tablo 2.6'a gösterildiği gibi AES-128 4x4 matris uzunluğu ile 10 döngüde, AES-192 6x6 matris uzunluğu ile 12 döngüde, AES-256 8x8 matris uzunluğu ile 14 döngüde şifreleme yapmaktadır.

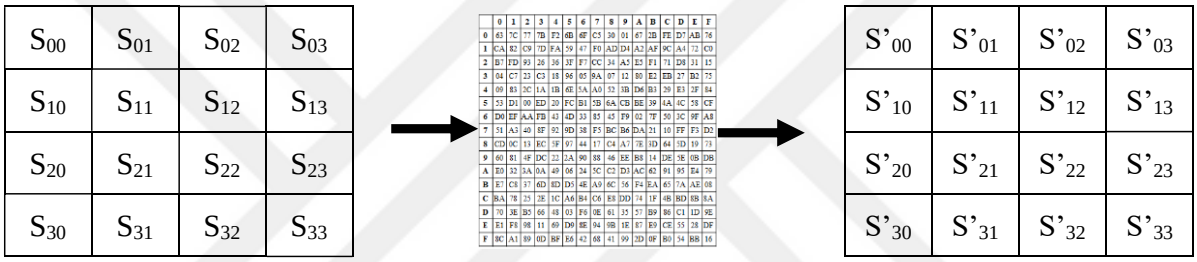
Tablo 2.6: Gelişmiş şifreleme standardının değişken değerleri.

Anahtar uzunluğu	Sözcük uzunluğu	Döngü sayısı	Matris uzunluğu
128	4	10	0 < m < 16
192	6	12	0 < m < 24
256	8	14	0 < m < 32

Algoritmanın son döngüsü hariç sırasıyla Bayt Değiştirme (Substitute Bytes), Satır Kaydırma (ShiftRows), Sütun Karıştırma (MixColumns) ve Döngü Anahtarını Ekleme (AddRoundKey) olacak şekilde 4 ayrı dönüşüm fonksiyonu şifreleme için kullanılmaktadır. Algoritmanın son döngüsü hariç sırasıyla Ters Bayt Değiştirme (InvSubBytes), Ters Satır Kaydırma (InvShiftRows), Ters Sütun Karıştırma (InvMixColumns) ve Döngü Anahtarını Ekleme (AddRoundKey) olacak şekilde 4 ayrı dönüşüm fonksiyonu şifre çözme için kullanılmaktadır. Son adımda sütun değiştirme fonksiyonu hariç diğer fonksiyonlar kullanılmaktadır.

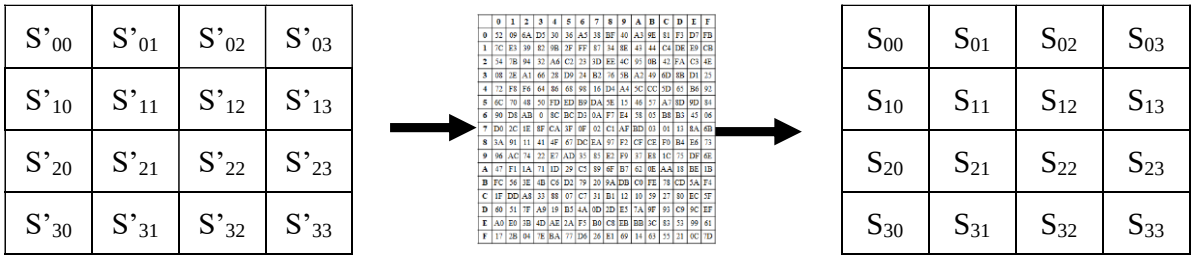
2.3.9.3.1. BAYT DEĞİŞTİRME VE TERS BAYT DEĞİŞTİRME

Bayt değiştirme, AES algoritmasının ilk ve tek lineer olmayan işlemidir. Durum dizisinin her elemanı önceden hesaplanmış yerine koymalı kutudaki bilgiler ile değiştirilmektedir. Durum dizisinin ilk öğesi bayt olarak adlandırılır ve $b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x^1 + b_0x^0$ şeklinde yazılır. Baytın ilk dört bitinin ($b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4$) onaltılı sayı sisteminde karşılığı yerine koymalı kutunun satır bilgisini, son dört bitinin ($b_3x^3 + b_2x^2 + b_1x^1 + b_0x^0$) onaltılı sayı sisteminde karşılığı yerine koymalı kutunun sütun bilgisini vermektedir. Satır ve sütun bilgilerinin yerine koymalı kutudaki kesiştiği hücrede yer alan değer durum dizisindeki okunan değer ile değiştirilir. Durum matrisindeki tüm değerler bu şekilde okunup karşılık gelen değerler ile yer değiştirilip Şekil 2.13'te gösterilen yeni durum dizisi oluşturulur.



Şekil 2.13: Bayt değiştirme işlemi.

Yerine koymalı kutu şifreleme işlemi için kullanılmaktadır. Şifre çözme işlemi için yerine koymalı kutunun tersi alınarak ters yerine koymalı kutu oluşturulmaktadır. Şifre çözme adımlarında ters bayt değiştirme adımına girdi olarak gelen durum dizisinin tüm öğeleri bayt değiştirme aşamasında olduğu gibi bu sefer ters yerine koymalı kutudaki değer ile yer değiştirilir ve Şekil 2.14'te gösterilen yeni durum dizisi oluşturulur.

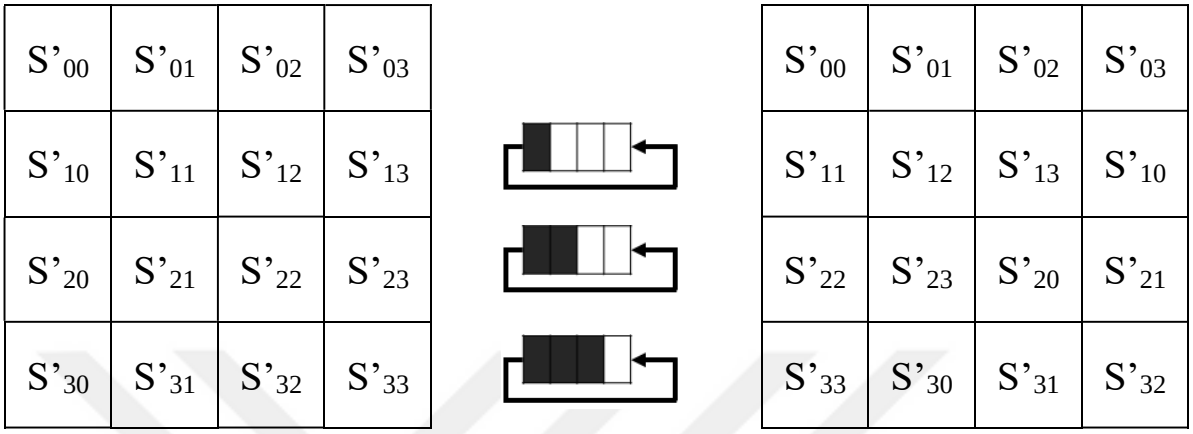


Şekil 2.14: Ters bayt değiştirme işlemi.

2.3.9.3.2. SATIR KAYDIRMA VE TERS SATIR KAYDIRMA

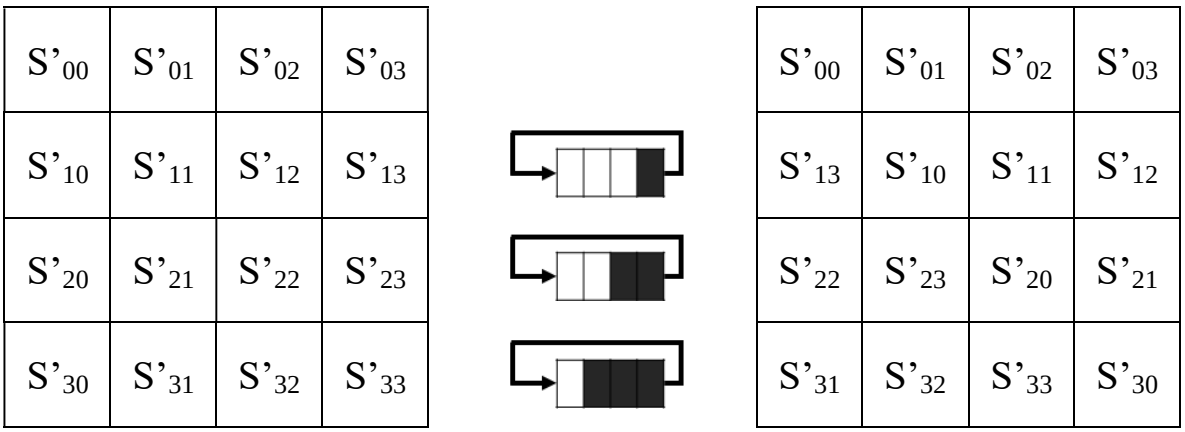
Satır kaydırma işleminde durum dizisinin ilk satırı hariç tüm satırları belirli bir düzende sola kaydırılmaktadır. İkinci satır bir öğe, üçüncü satır iki öğe, dördüncü satır üç öğe sola kaydırılıp

Şekil 2.15'teki yeni durum dizisi oluşturulur. Bir başka deyişle, durum dizisinin ikinci satırının ilk baytı ikinci satırın sonuna, üçüncü satırının ilk iki baytı üçüncü satırın sonuna, dördüncü satırının ilk üç baytı dördüncü satırın sonuna eklenir.



Şekil 2.15: Satır kaydırma işlemi.

Ters satır kaydırma işlemi şifre çözme adımlarından biri ve satır kaydırma işleminin tam tersi uygulanmaktadır. Ters satır kaydırma adımına girdi olan durum dizisinin ilk satırı aynen kalır ve ikinci satır bir öğe, üçüncü satır iki öğe, dördüncü satır üç öğe sağa kaydırılıp Şekil 2.16'daki yeni durum dizisi oluşturulur. Bir başka deyişle, durum dizisinin ikinci satırının son baytı ikinci satırın başına, üçüncü satırının son iki baytı üçüncü satırın başına, dördüncü satırının son üç baytı dördüncü satırın başına eklenir.



Şekil 2.16: Ters satır kaydırma işlemi.

2.3.9.3.3. SÜTUN KARIŞTIRMA VE TERS SÜTUN KARIŞTIRMA

Sütun karıştırma adımında durum dizisinin her sütunundan farklı bir sütun elde edilmektedir ve şifreleme ve şifre çözme işlemlerinde son döngüde kullanılmamaktadır. Durum dizisinin ilk sütunu Şekil 2.17'de verilen matris ile çarpılır ve yeni sütun elde edilir. Durum dizisinin tüm sütunları ayrı ayrı sabit matris ile çarpılır ve yeni durum dizi oluşur.

S'$_{00}$	S'$_{01}$	S'$_{02}$	S'$_{03}$
S'$_{11}$	S'$_{12}$	S'$_{13}$	S'$_{10}$
S'$_{22}$	S'$_{23}$	S'$_{20}$	S'$_{21}$
S'$_{33}$	S'$_{30}$	S'$_{31}$	S'$_{32}$

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S'_{00} \\ S'_{11} \\ S'_{22} \\ S'_{33} \end{bmatrix} = \begin{bmatrix} S''_{00} \\ S''_{10} \\ S''_{20} \\ S''_{30} \end{bmatrix}$$

S''$_{00}$	S''$_{01}$	S''$_{02}$	S''$_{03}$
S''$_{10}$	S''$_{11}$	S''$_{12}$	S''$_{13}$
S''$_{20}$	S''$_{21}$	S''$_{22}$	S''$_{23}$
S''$_{30}$	S''$_{31}$	S''$_{32}$	S''$_{33}$

Şekil 2.17: Sütun karıştırma işlemi.

Sütun karışma adımında kullanılan sabit matrisin tersi alınarak yeni sabit matris oluşturulur. Durum dizisinin ilk sütunu Şekil 2.18'de verilen matris ile çarpılır ve yeni sütun elde edilir. Durum dizisinin tüm sütunları ayrı ayrı sabit matris ile çarpılır ve yeni durum dizi oluşur.

S'$_{00}$	S'$_{01}$	S'$_{02}$	S'$_{03}$
S'$_{13}$	S'$_{10}$	S'$_{11}$	S'$_{12}$
S'$_{22}$	S'$_{23}$	S'$_{20}$	S'$_{21}$
S'$_{31}$	S'$_{32}$	S'$_{33}$	S'$_{30}$

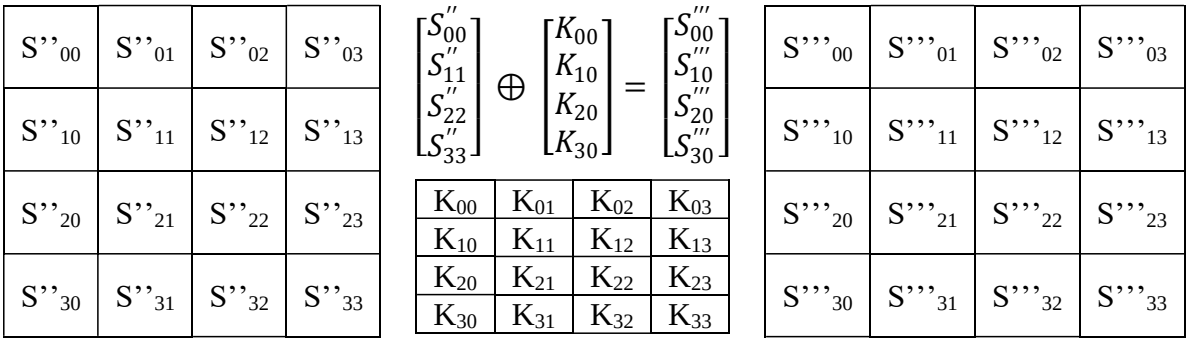
$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \begin{bmatrix} S'_{00} \\ S'_{13} \\ S'_{22} \\ S'_{31} \end{bmatrix} = \begin{bmatrix} S''_{00} \\ S''_{10} \\ S''_{20} \\ S''_{30} \end{bmatrix}$$

S''$_{00}$	S''$_{01}$	S''$_{02}$	S''$_{03}$
S''$_{10}$	S''$_{11}$	S''$_{12}$	S''$_{13}$
S''$_{20}$	S''$_{21}$	S''$_{22}$	S''$_{23}$
S''$_{30}$	S''$_{31}$	S''$_{32}$	S''$_{33}$

Şekil 2.18: Ters sütun karıştırma işlemi.

2.3.9.3.4. DÖNGÜ ANAHTARINI EKLEME

Algoritmanın her döngüsünde anahtardan üretilen döngü anahtarı durum dizisine eklenir. Şekil 2.19'da görüldüğü gibi döngü anahtarı ile durum dizisi veri dışlayan veya işlemine tabi tutulup, yeni durum dizisi oluşur. Dışlayan veya işleminin tersi aynı değeri verdiği için ters döngü anahtarı işlemi döngü anahtarı işlemi ile aynıdır.



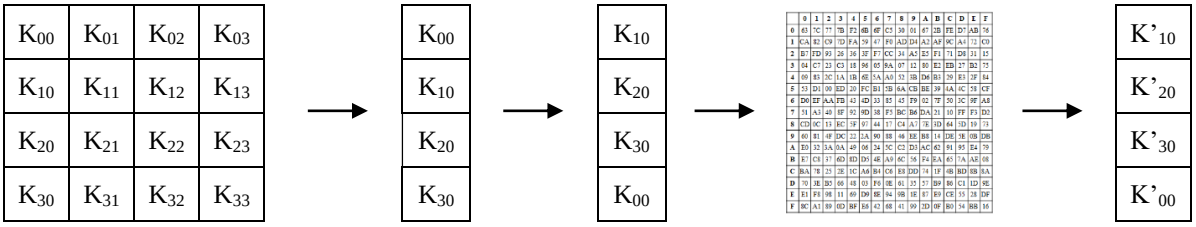
Şekil 2.19: Döngü anahtarını ekleme işlemi.

2.3.9.3.5. DÖNGÜ ANAHTARIN ÜRETME

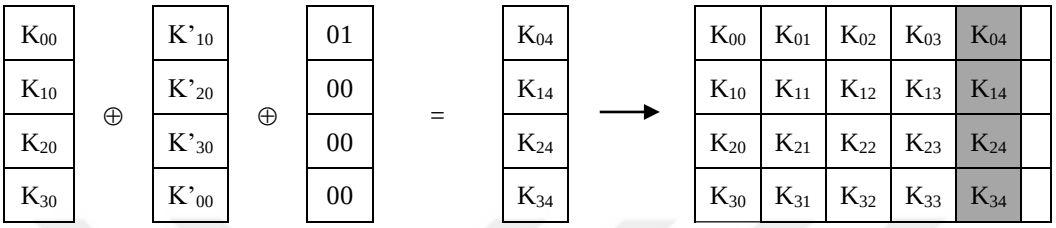
AES algoritması döngü anahtarı ekleme işlemi ile başlamaktadır ve her döngüde gizli anahtardan türemiş farklı anahtar kullanmaktadır. Anahtar üretme işlemi algoritmanın döngü sayısı kadar yapılmaktadır. Her döngüde anahtar bir önceki döngüde kullanılan anahtara ait bilgiler ile üretilmektedir. Şekil 2.20'de döngü anahtarının oluşturma adımları verilmiştir.

Algoritmada kullanılan gizli anahtar, boyutuna göre anahtar matrise dönüştürülür. AES-128 için 4x4 anahtar matrisi, AES-192 için 6x6 anahtar matrisi ve AES-256 için 8x8 anahtar matrisi oluşturulur. Oluşan anahtar matrisinin son sütunu önce aşağıya doğru bir öğe ötelenir, yani sütunun ilk öğesi en sona eklenir. Oluşan yeni sütundaki her bir öğe yerine koymalı kutudaki değeri ile değiştirilir. Anahtar dizisinin ilk sütun, oluşan yeni sütun ve ilk döngüye ait RCON değeri dışlayan veya işlemi ile yeni sütun oluşturur. Oluşan yeni sütun yeni döngü anahtarının ilk sütunudur ve anahtar matrisinin beşinci sütunudur.

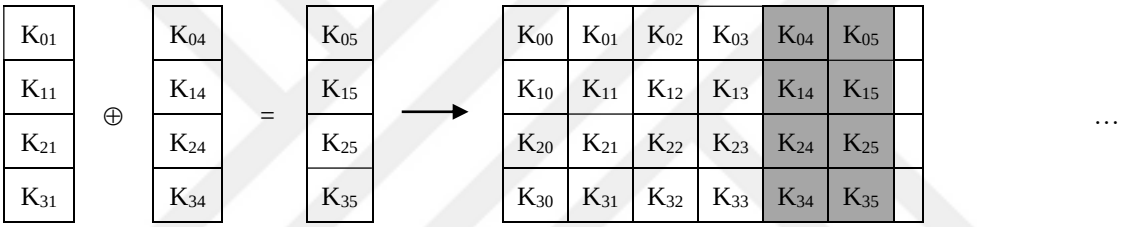
Yeni döngü anahtarının ilk sütunu ile bir önceki döngü anahtarının ikinci sütunu dışlayan veya işlemi ile yeni döngü anahtarının ikinci sütunu yani anahtar matrisinin altıncı sütunu elde edilir. Yeni döngü anahtarının ikinci sütunu ile bir önceki döngü anahtarının üçüncü sütunu dışlayan veya işlemi ile yeni döngü anahtarının üçüncü sütunu yani anahtar matrisinin yedinci sütunu elde edilir. Yeni döngü anahtarının üçüncü sütunu ile bir önceki döngü anahtarının dördüncü sütunu dışlayan veya işlemi ile yeni döngü anahtarının dördüncü sütunu yani anahtar matrisinin sekizinci sütunu elde edilir. Bu işlem sonunda yeni döngü anahtarı oluşum işlemi tamamlanmıştır.



(a) sözcük döndürme ve yer değiştirme



(b) ilk döngü anahtarı için ilk sütun hesaplama



(c) ilk döngü anahtarı için diğer sütunların hesaplanması

Şekil 2.20: Döngü anahtarını oluşturma adımları.

Şekil 2.20'de belirtilen adımlar her döngü için tekrarlanmaktadır. Yeni anahtarın ilk sütunun oluşmasında kullanılan RCON vektörü Tablo 2.7'de verilmiştir. Anahtar hangi döngü için oluşturuyorsa o döngüye ait RCON vektörü kullanılır. Anahtar genişletme tamamlandığında AES-128 için 4x44, AES-192 için 6x78, AES-256 için 8x120 boyutunda matris elde edilmiştir.

Tablo 2.7: AES algoritmasının RCON değerleri.

Döngü	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
RCON vektörü	01	02	04	81	10	20	40	80	1B	36
	00	00	00	00	00	00	00	00	00	00
	00	00	00	00	00	00	00	00	00	00
	00	00	00	00	00	00	00	00	00	00

2.4. ŞİFRELEME MODELİ

Bir sistemi güvenli hale getirmek için anahtarın güvenli bir şekilde saklanması gerekmektedir. Genellikle şifre çözmeye yönelik hamleler anahtarı bulmaya yöneliktir. Sistemi gözlemleyen üçüncü şahısların amacı farklı şifreleme modellerinde elde ettikleri bilgi ile anahtarı bulup yapıyı değiştirmeye yöneliktir. Siyah Kutu Şifreleme Modeli (Black Box Cryptography Model), Gri Kutu Şifreleme Modeli (Gray Box Cryptography Model) ve Beyaz Kutu Şifreleme Modeli (White Box Cryptography Model, WBC) olmak üzere üç farklı şifreleme modeli bulunmaktadır.

2.4.1. SİYAH KUTU ŞİFRELEME MODELİ

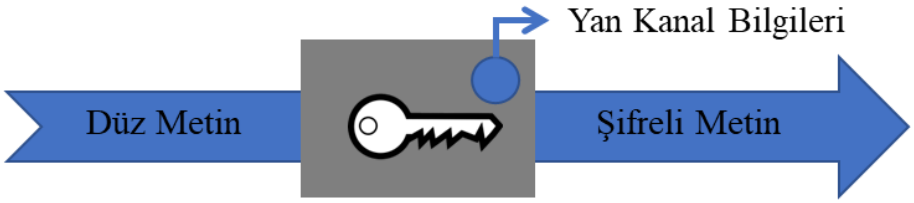
Sisteme saldıran kişinin sistemde kullanılan anahtara veya içyapısındaki herhangi bir bilgiye fiziksel olarak erişiminin bulunmadığı sadece sistemin dışa verdiği bilgi ve davranışların gözlemlenebildiği geleneksel şifreleme modelidir. Siyah kutu modeli Şekil 2.21'de görüldüğü gibi sadece düz metin (sistemin girdisi) ve şifreli metne (sistemin çıktısı) erişebilme imkanı sağlarken sistemin kullandığı şifreleme algoritması ve diğer işlenebilen kodlara erişimi yoktur.



Şekil 2.21: Siyah kutu şifreleme modeli.

2.4.2. GRİ KUTU ŞİFRELEME MODELİ

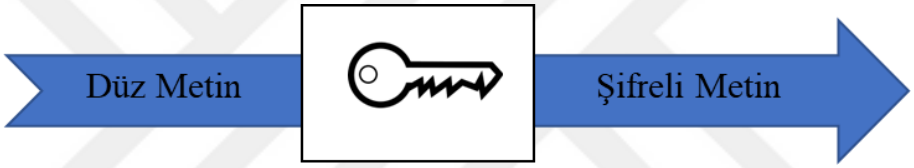
Sisteme saldıran kişinin sistemde kullanılan anahtara Şekil 2.22'de görüldüğü gibi yan kanal bilgileri sayesinde kısmı fiziksel erişimi bulunmaktadır. Şifreleme sisteminin fiziksel uygulamasından kazanılan bilgiler sayesinde sisteme saldırılması mümkündür. Sistemin güç tüketimi (power consumption), zamanlama (timing), hata analizi (fault analysis) olarak bilinen yan kanal bilgileri (side channel information) saldırgan tarafından bilinebilmektedir ve bu bilgileri kullanarak sistemi kırmaya çalışmaktadır.



Şekil 2.22: Gri kutu şifreleme modeli.

2.4.3. BEYAZ KUTU ŞİFRELEME MODELİ

Sisteme saldıran kişinin sistemde çalıştırılan yapıda tam kontrolü bulunmaktadır. Kullanılan sistemin çalıştırılabilir dinamik kodları ve önemli verileri izleyebilme, sistemdeki algoritmaya erişebilme ve düzenleyebilme gibi yetkileri bulunabilmektedir. Şekil 2.23'te görüldüğü gibi sistem tamamıyla açık olarak işlevlerini yerine getirmektedir.



Şekil 2.23: Beyaz kutu şifreleme modeli.

Beyaz Kutu Şifreleme (Beunardeau ve diğ., 2016) sistemi kırmayan çalışan kişilerin sistem üzerinde tüm yetkilere sahip olmasına rağmen güvenliği sağlayacağını garanti eden bir sistem sunmaktadır. Donanımsal olarak kullanıldığında güvenilir donanımlar (Trusted Execution Enviroment) sayesinde güvenliği sağlarken yazımsal olarak güvenli yapılar üzerinde yazılımın saklanmasını amaçlamaktadır. Eğer sistem için işlemlerin daha hızlı olması önemli ise en uygun şifreleme modeli beyaz kutu şifreleme modelidir (Şengel ve diğ., 2019).

Beyaz Kutu şifreleme tekniği üçüncü şahısların sistem üzerinde tam kontrolü olmasına rağmen yazılım uygulamasına ait şifreleme algoritmasında kullanılan anahtarın tespit edilip yenilenmesine karşı korumayı amaçlamaktadır.

Güvenli bir beyaz kutu şifreleme uygulaması güvenilir olmayan bir platformda algoritmanın tüm detaylarının bilinmesi ve şifreleme algoritmasının çalıştırılmasının açık olmasına rağmen kullanılan şifreleme anahtarının açığa çıkarılmasını önleyen bir yapıda sistemin oluşturulmasını amaçlamaktadır.

Beyaz Kutu şifreleme ile ilgili ilk çalışmalar Chow ve diğ. (2003a, 2003b) şifreleme ilkelerini Gelişmiş Şifreleme Standardı (Advanced Encryption Standard-AES) ile beyaz kutu uygulaması ve Veri Şifreleme Standardı (Data Encryption Standard-DES) ile beyaz kutu uygulamaları ile başlamıştır. Her iki yapıda tüm şifrelemenin küçük boyuttaki başvuru çizelgesi (lookup table) özeti olarak gösterilen döngü fonksiyonlarına ayrılma temel stratejisine dayanmaktadır.

Chow ve diğ. (2003a, 2003b) geliştirdiği algoritmalar 2^{14} karmaşıklığında DES (Wyseur ve diğ., 2007), 2^{22} karmaşıklığında AES (Lepoint ve diğ., 2014) kırılmış olsa da başvuru çizelgelerini kullanan beyaz kutu uygulamasının dizaynı için CEJO yapısı birçok şifreleme yapısında kullanılmıştır. Araştırmacıların çoğu CEJO yapısını geliştirmek ve üzerinde saldırı senaryoları üretmek için kullanmışlardır. Billet ve diğ. (2004) (BGE saldırıları olarak bilinen) uygulamada kullanılan gizli anahtarın 2^{30} karmaşıklığında değiştirilebileceğini bir saldırı ile göstermişlerdir. Michiels ve diğ. (2009) çalışmasında Substitution Linear Transformation (SLT) şifrelemeye yönelik genel beyaz kutu uygulamasında bir saldırı önerdi. Tolhuizen (2012) çalışmasında BGE saldırısını en iyi zaman karmaşıklığında geliştirmiştir. Lepoint ve diğ. (2014) Tolhuizen (2012) çalışmasına dayanarak BGE saldırısını zaman karmaşıklığını $O(2^{22})$ düşürmüştür.

Billet ve Gilbert (2003) Isomorphism of Polynomials (IP) problemine (Patarin, 1996) dayanan aynı şifrelere eşdeğer temsilciler teklif ettiler fakat IP probleminin (Faugère ve Perret, 2006) çözümü yayınlanmasıyla birlikte kırılmıştır.

Karroumi (2010), AES şifrelemenin ikili ifadesini kullanarak döngü fonksiyonlarındaki aritmetik işlemleri değiştirip beyaz kutu AES uygulaması önermiştir. Aynı zamanda Karroumi (2011) çalışmasında çift şifre kullanarak beyaz kutu AES uygulamasını korumayı amaçlamıştır.

Gueron (2013) çalışmasında şifre çözme kodunda direk olarak şifreleme anahtarı veya hafızada kayıtlı olan döngü anahtarlarını kullanmadan Intel'in yeni "AES Instructions" kullanarak bir metot geliştirmiştir. Böylece başvuru çizelge tabanlı alternatiflerine göre yaklaşık 2.6 kez daha hızlı bir yapı oluşmuştur. İşlemlerin paralel olarak çalışmasını sağlayarak, optimizasyon tekniklerini kullanarak ve "mapped key Schedule" metodu ile daha hızlı bir yapı elde edilmiştir.

Azhar ve diğ. (2014) anahtarların bit-string ifadesini fonksiyonel ifadeye çeviren "soft code" anahtarlar oluşturmuşlardır. Bu işlemi 4 ana adımda gerçekleştirmektedirler. Birinci adımda rastgele oluşturulan anahtarı rastgele (True Random Number Generator) üretilen bir n sayıda

parçaya ayırıyorlar. Her parça belirli bir matametiksel işlemden geçirilerek şifreleniyor. Bir önceki adımda belirlenen matematiksel ilişki C_i "instruction" olarak tutulur ve her "instruction" referans parçayı girdi olarak alan doğru çıktıyı üreten bir fonksiyona dönüştürülür. Girdi yanlış olduğunda orijinal parça değeri üretilemeyeceği için tüm anahtara da erişilemeyecektir. Her bir parça ardışıl fonksiyonlara dönüştürülerek yazılım kaynak kodu (software source code) zinciri oluşturulmaktadır. Son adımda, uygulama kodu ile "soft-coded" anahtarları derleniyor ve gerektiğinde yazılım şifreleme algoritmaları da kullanmaktadırlar.

Luo ve diğ. (2014) çalışmalarında temelde 10 özyinelemede çalışan AES algoritmasını kullanarak her özyineleme üç adımda gerçekleştirmektedir. Birinci adımda satır kaydırma işlemi, ikinci adımda XOR işlemleri, üçüncü adımda AES algoritmasında yer alan döngü anahtarını ekleme, bayt değiştirme, sütun karıştırma işlemleri gerçekleştirilmektedir.

Shi ve He (2014) yaptıkları çalışmada düşük hafıza gereksinimi ve düşük hesaplama maliyeti hedefledikleri için kablosuz ağları korumak için kullanılan Çin'in blok şifreleme standardı olan SMS4 algoritmasını kullanmışlardır. Algoritmanın S-kutusu oluşturulurken farklı bir formül kullanmaktadır. Oluşan S-kutuları üzerinden şifreleme algoritmasını kullanarak verileri şifrelemektedirler. Yapmış oldukları algoritmada başvuru çizelgeleri ve matrislerinin boyutunun 144.625KB olduğunu ve bu zamana kadar yapılan çalışmalardan daha az alan kapladıklarını diğer algoritmalar ile karşılaştırarak belirtmişler. Hız olarak karşılaştırdıklarında diğer algoritmalara göre orta hızda ve henüz herhangi bir saldırısı bilinmeyen bir algoritma olduğunu göstermektedirler.

Tüm geliştirilen algoritmalar için aynı zamanda saldırı senaryoları üreten ve bu senaryolara göre sistemin açık yanlarını geliştirmek için parametreler belirleyen çalışmalarda mevcut. Delerablée ve diğ. (2014) çalışmasında simetrik şifreleme ile beyaz kutu güvenlik notasyonları ve saldırı atakları dahilinde nasıl güvenliği sağladıklarını göstermektedir. Aynı çalışmaya göre sistemin kırılabilir olmaması (unbreakability) gizli anahtarın programın içine güvenli bir şekilde saklanması, tek yönlülük (One-wayness) programın tersinin olmaması yani şifrelenen veri geriye dönük çözülememesi (hashing ile tek yönlü şifreleme), sistemin daha küçük boyutlara sıkıştırılabilir olmaması (incompressibilty), ve son olarak şifreleme deşifreleme yapılarının kopyalanabilir olmaması (traceabilty) önemli güvenlik notasyonlarıdır. Wu ve diğ. (2016) yaptıkları çalışmada hem siyah kutu model saldırıları hem de beyaz kutu model saldırılarında var olan Model Inversion saldırılarını kullanıp formüle eden bir yöntem

uygulamışlar. Yapmış oldukları çalışmada katmanlar arası veri aktarımındaki açıklar ve iletim sırasında elde edilen bilgiler doğrultusunda beyaz kutu şifrelemenin kolayca kırılabileceğini vurgulamışlar. Jia ve diğ. (2016) çalışması beyaz kutu uygulamasında blok şifreleme yapısına karşı saldırı yapısını blok şifrelemeden elde edilen girdi çıktı eşleşmelerin olası dağılımlarından alt anahtarın değiştirilebileceğini dayanmaktadır.

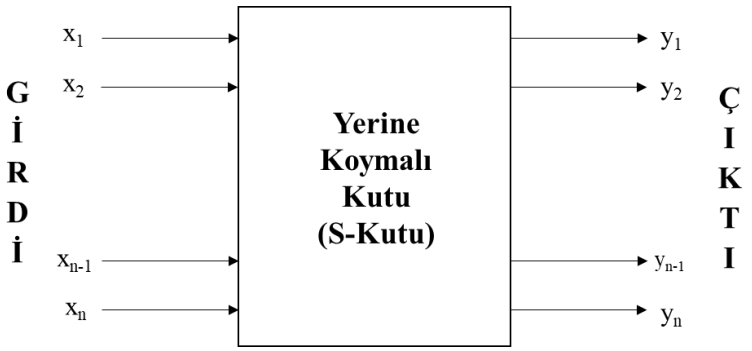
2.5. YERİNE KOYMALI KUTU (S-KUTU)

Yerine koymalı kutular blok şifreleme algoritmalarının tek doğrusal olmayan en önemli elemanıdır ve s-kutu seçimi şifrenin karmaşıklığını doğrudan etkilemektedir. S-kutu anahtar ve şifreli metin arasındaki ilişkiyi belirlemektedir. Bu yüzden, şifreleme ile ilgili özellikleri iyi olan s-kutularının seçilmesi doğrusal ve diferansiyel saldırılara karşı algoritmayı güvenli kılmak için önemlidir (Şengel ve diğ., 2020b). S-kutular tasarlanırken

- sözde rastgele üretim,
- sonlu cisimde ters alma,
- sonlu cisimde üs alma,
- buluşsal (heuristic) teknikler

gibi farklı yöntemler kullanılmaktadır.

N-bit girişli bir s-kutu, [0, 2^{n-1}] aralığından 2^n tane eleman içermektedir. S kutusu, durum dizisinin elemanları onaltılı sayı tabana göre oluşmaktadır. Durum dizisinin her bir öğesi 8-bitlik veri içermektedir. Algoritmada kullanılan S-kutu 16 satır ve 16 sütundan oluşur ve 8-bit uzunluğunda 256 (16x16) tane öğe içerir. S-kutu satır sütun göstergeleri “0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F” şekildedir. NxN s-kutu yapısı Şekil 2.24’te verilmiştir. S-kutusundan veri okumak için y = S(x) fonksiyonu kullanılır. Fonksiyonun girdisi onaltılı sayı tabanında verilmektedir. Girdinin en soldaki değeri onaltılı sayı sisteminde karşılığı yerine koymalı kutunun satır bilgisini, en sağdaki değeri onaltılı sayı sisteminde karşılığı yerine koymalı kutunun sütun bilgisini vermektedir. Satır ve sütun değerlerinin kesişim noktasında yer alan değer onaltılı sayı sisteminde çıktı değerini vermektedir.



Şekil 2.24: NxN s-kutu yapısı.

Rijndael algoritması Nyberg (1994) çalışmasında önerdiği sonlu cisimde ters alma tabanlı S-kutuları kullanmaktadır. İndirgenemez polinom, afin dönüşüm ve ekleme sabiti AES s-kutusunun üç önemli parametresidir. AES s-kutusu aşağıdaki iki dönüşümü kullanılarak elde edilmektedir.

1. 2^8 Galois alanı'nda (Galois Field, GF) ters alma işlemi, indirgenemez polinomu kullanılarak gerçekleştirilir.
2. GF(2^8) üzerinde Denklem (2.13) kullanılarak afin dönüşüm uygulanır.

$$\begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \\ s_6 \\ s_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \quad (2.13)$$

Tablo 2.8'de verilen AES s-kutusu $x^8 + x^4 + x^3 + x + 1$ indirgenemez polinomu ve 0x63 (01100011) ekleme sabitini kullanarak oluşmuştur. S-kutunun indisi girdi olarak alınır ve indirgenemez polinoma göre tersi hesaplanır. Örneğin; S(00) için 0. satır ve 0. sütun değerini bulmak için polinoma göre tersi genişletilmiş öklit algoritması ile 00 bulunur, S(01) için 0. satır ve 1. sütun değerini bulmak için polinoma göre tersi genişletilmiş öklit algoritması ile 01 bulunur, S(02) için 0. satır ve 2. sütun değerini bulmak için polinoma göre tersi genişletilmiş öklit algoritması ile 8D bulunur. Ters dönüşüm sonucu elde edilen değer afin matris ile çarpma ve sonra ekleme sabiti ile dışlayan veya işlemine tabi tutularak ilgili indis için değer elde edilir. S-kutunun tüm indisleri için işlemler tekrarlanarak s-kutu oluşturulur.

Tablo 2.8: AES s-kutusu.

satır \ sütun	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Elde edilen AES s-kutusu algoritmanın şifreleme adımlarından döngü anahtarının oluşturulması ve bayt değiştirme işlemlerinde kullanılmaktadır. S-kutu fonksiyonunun girdisi 0x5E olduğunda en soldaki 5 değeri satırı, en sağdaki E değeri sütunu göstermektedir. Tablo 2.8'de 5. satır ve E. sütunda yer alan 0x58 değeri fonksiyonun çıktısı olur.

Tablo 2.9'da verilen AES ters s-kutusu $x_8 + x_4 + x_3 + x + 1$ indirgenemez polinomu ve 0x05 (00000101) ekleme sabitini kullanarak oluşmuştur. Ters s-kutunun indisi girdi olarak alınır ve indirgenemez polinoma göre tersi hesaplanır. Ters dönüşüm sonucu elde edilen değer afin matrisinin tersi ile çarpma ve sonra ekleme sabiti ile dışlayan veya işlemine tabi tutularak ilgili indis için değer elde edilir. Afin dönüşümü için Denklem (2.14) kullanılmaktadır. Ters s-kutunun tüm indisleri için işlemler tekrarlanarak ters s-kutu oluşturulur.

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \\ s_6 \\ s_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad (2.14)$$

Tablo 2.9: AES ters s-kutu.

satır \ sütun	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3	8	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

Elde edilen AES ters s-kutusu algoritmanın şifre çözme adımlarından döngü anahtarının oluşturulması ve ters bayt değiştirme işlemlerinde kullanılmaktadır. Ters s-kutu fonksiyonunun girdisi 0x58 olduğunda en soldaki 5 değeri satırı, en sağdaki 8 değeri sütunu göstermektedir. Tablo 2.9'da 5. satır ve 8. sütunda yer alan 0x5E değeri fonksiyonu çıktısı olur. Ters s-kutunun fonksiyonunun çıktısı s-kutu fonksiyonunun girdisi olarak gelmektedir. Bu durumda s-kutu oluşturulduktan sonra ters s- kutu s-kutu değerleri ile oluşturulabilir.

Günümüze kadar AES s-kutusunun yapısına benzer ve onun kadar güçlü birçok çalışma yapılmıştır. Oluşturulan s-kutuların farklı yapıları temel alarak AES s-kutusu kadar saldırılara dayanıklı s-kutuların üretilebileceğini göstermiştir. İndirgenemez polinomlu s-kutular, kaotik tabanlı s-kutular, makine öğrenmesi teknikleri ile oluşturulan s-kutular ve biyometrik tabanlı s-kutular oluşturulmuştur.

2.5.1. İNDİRGENEMEZ POLİNOMLU S-KUTULAR

S-kutu oluştururken kullanılan tekniklerden biri olan sonlu cisimde ters alma yöntemini kullanmak için Galois alanda (Galois Field, GF) indirgenemez polinom bulunmalıdır. S-kutu oluşturmak için kullanılacak indirgenemez polinom seçilirken iki özelliğe dikkat edilmelidir:

1. Polinomların sonu 1 ile bitmelidir. Çünkü sonu 1 ile bitmez ise x ile bölünebilir durumda olur. Bu da indirgenebilir polinom olduğunu belirtir.
2. İki farklı polinomun çarpımı halinde yazılamazsa bu polinom indirgenebilir polinomdur.

Galois alanı'nda GF(2^8) 'de 30 tane indirgenemez polinom bulunmaktadır ve bu polinomların bazıları asaldır. GF(2^8)'deki indirgenemez polinomların hepsi Tablo 2.10'da verilmiştir. AES 11B indirgenemez polinomunu kullanmaktadır.

Bir indirgenemez polinom ile farklı afin matrisleri kullanılarak birden fazla s-kutu oluşturulabilir. Chandrasekharappa ve diğ. (2011) çalışmalarında 2^{63} afin matrisin her indirgenemez polinomla oluşturabileceğini belirtmişler. Aynı çalışmalarında bu yöntem ile 50 adet farklı s-kutu üretmişler ve $x^8 + x^6 + x^5 + x^4 + x^3 + x + 1$, $x^8 + x^7 + x^5 + x^4 + x^3 + x^2 + 1$, $x^8 + x^6 + x^3 + x^2 + 1$, $x^8 + x^6 + x^5 + x^2 + 1$indirgenemez polinomları ile üretilen s-kutuların en yüksek çığ etkisine sahip olduğunu göstermişlerdir.

Sinha ve Arya (2012) çalışmalarında indirgenemez polinomlar ile oluşturulan s-kutuların hepsini iyi bir s-kutu için gerekli olan güvenlik kriterlerinden birkaçı için değerlerini karşılaştırmıştır ve $x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + 1$, $x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1$, $x^8 + x^7 + x^3 + x + 1$, $x^8 + x^6 + x^3 + x^2 + 1$, $x^8 + x^6 + x^3 + x^2 + 1$, $x^8 + x^7 + x^6 + x^5 + x^2 + x + 1$indirgenemez polinomların AES s-kutusu ile aynı özellikte oldukları gözlenmiştir. Aynı çalışmada, bir indirgenemez polinom için üç farklı afin matrisi kullanarak elde ettikleri s-kutuları analiz

ettiklerinde farklı afin matrislerinin bazı s-kutuların güvenlik parametrelerinde daha iyi sonuç elde ettiklerini gözlemlemişler.

Tablo 2.10: GF(2^8)'de asal ve/veya indirgenemez polinomlar.

İkili Sayı Sistemi	Onaltılı Sayı Sistemi	Polinom	Polinom Türü
100011011	11B	$x^8 + x^4 + x^3 + x + 1$	İndirgenemez
100011101	11D	$x^8 + x^4 + x^3 + x^2 + 1$	Asal ve indirgenemez
100111001	139	$x^8 + x^5 + x^4 + x^3 + 1$	İndirgenemez
100101011	12B	$x^8 + x^5 + x^3 + x + 1$	Asal ve indirgenemez
100101101	12D	$x^8 + x^5 + x^3 + x^2 + 1$	Asal ve indirgenemez
100111111	13F	$x^8 + x^5 + x^4 + x^3 + x^2 + x + 1$	İndirgenemez
101001101	14D	$x^8 + x^6 + x^3 + x^2 + 1$	İndirgenemez
101011111	15F	$x^8 + x^6 + x^4 + x^3 + x^2 + x + 1$	Asal ve indirgenemez
101100011	163	$x^8 + x^6 + x^5 + x + 1$	Asal ve indirgenemez
101100101	165	$x^8 + x^6 + x^5 + x^2 + 1$	İndirgenemez
101101001	169	$x^8 + x^6 + x^5 + x^3 + 1$	Asal ve indirgenemez
101110001	171	$x^8 + x^6 + x^5 + x^4 + 1$	Asal ve indirgenemez
101110111	177	$x^8 + x^6 + x^5 + x^4 + x^2 + x + 1$	İndirgenemez
101111011	17B	$x^8 + x^6 + x^5 + x^4 + x^3 + x + 1$	İndirgenemez
110000111	187	$x^8 + x^7 + x^2 + x + 1$	Asal ve indirgenemez
110001011	18B	$x^8 + x^7 + x^3 + x + 1$	İndirgenemez
110001101	18D	$x^8 + x^7 + x^3 + x^2 + 1$	Asal ve indirgenemez
110011111	19F	$x^8 + x^7 + x^4 + x^3 + x^2 + x + 1$	İndirgenemez
110100011	1A3	$x^8 + x^7 + x^5 + x + 1$	İndirgenemez
110101001	1A9	$x^8 + x^7 + x^5 + x^3 + 1$	Asal ve indirgenemez
110110001	1B1	$x^8 + x^7 + x^5 + x^4 + 1$	İndirgenemez
110111101	1BD	$x^8 + x^7 + x^5 + x^4 + x^3 + x^2 + 1$	İndirgenemez
111000011	1C3	$x^8 + x^7 + x^6 + x + 1$	Asal ve indirgenemez
111001111	1CF	$x^8 + x^7 + x^6 + x^3 + x^2 + x + 1$	Asal ve indirgenemez
111010111	1D7	$x^8 + x^7 + x^6 + x^4 + x^2 + x + 1$	İndirgenemez
111011101	1DD	$x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + 1$	İndirgenemez
111100111	1E7	$x^8 + x^7 + x^6 + x^5 + x^2 + x + 1$	Asal ve indirgenemez
111110011	1F3	$x^8 + x^7 + x^6 + x^5 + x^4 + x + 1$	İndirgenemez
111110101	1F5	$x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1$	Asal ve indirgenemez
111111001	1F9	$x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1$	İndirgenemez

Das ve diğ. (2012) çalışmalarında AES algoritmasında kullanılan s-kutu herkes tarafından bilindiği için saldırıya açık olduğunu ileri sürmüşler. AES s-kutusu için algoritmayı her kullandığımızda farklı indirgenemez polinom ile s-kutu üretip AES algoritmasının kullanmış olduğu indirgenemez polinomu gizli anahtar ile alıcıya gönderebileceklerini belirtmişler. Böylece algoritmanın güvenilirliğini arttırmışlar.

Das ve diğ. (2013) çalışmalarında oluşturdukları algoritma ile 0A, 0F, 15, 2A, 2B, 31, 32, 35, 38, 40, 4A, 4E, 54, 5E, 62, 6E, 74, 7E ekleme sabitlerini üretmişler. 11D indirgenemez polinomu ile 0A, 31, 4A, 74, 9D, CA, D5 ve F0 ekleme sabitlerini kullanarak s-kutular üretmişler ve her s-kutunun analizini yapmışlar. Yapılan analizler sonucu 11D indirgenemez polinomu ile 31 ekleme sabiti kullanılarak oluşturulan s-kutu 11B indirgenemez polinomu ile 63 sabiti ile oluşturulan standart s-kutudan daha iyi olduğunu bulmuşlar.

Gangadari ve Ahamed (2015) çalışmalarında 30 indirgenemez polinomun ile üretilen s-kutuları lineer olmama, entropi, korelasyon sapması (Correlation Immunity Bias), katı çığ etkisi kriterlerine göre analiz ettiklerinde $x^8 + x^6 + x^5 + x + 1$ indirgenemez polinonum daha iyi sonuç verdiği sonucunu elde etmişler. Aynı çalışmada farklı afin matrisleri ile s-kutu oluşturduklarında her afin matrisin farklı güvenlik sonuçlar elde etmişler.

Farklı Galois alanı'nda indirgenemez polinomlar kullanılarak farklı boyutlarda s-kutular da oluşturulmuştur. Sakallı ve diğ. (2014) çalışmalarında $GF(2^4)$ için indirgenemez polinom tanımına göre +1 ile biten $x^4 + 1$, $x^4 + x + 1$, $x^4 + x^2 + 1$, $x^4 + x^2 + x + 1$, $x^4 + x^3 + 1$, $x^4 + x^3 + x + 1$, $x^4 + x^3 + x^2 + 1$, $x^4 + x^3 + x^2 + x + 1$ polinomlarını bulmuşlar. Bu polinomlardan $x^4 + x + 1$, $x^4 + x^3 + 1$ ve $x^4 + x^3 + x^2 + x + 1$ polinomlarını indirgenemez polinom olduğunu ispatlayarak bulmuşlardır. Her polinom için farklı afin matris ile 3 ayrı s-kutu oluşturmuşlar. Bu çalışma ile farklı yapılarda s-kutu oluşturulabileceğini ve 4-bit giriş 4-bit çıkışlı s-kutuların gerekli uygulamalarda kullanılabileceğini göstermişler.

2.5.2. KAOTİK S-KUTULAR

S-kutu oluştururken kullanılan tekniklerden biri olan buluşsal teknikler yöntemine en iyi örneklerden biri kaotik sistemlerdir. Kaotik sistemlerin şifreleme alanında bu kadar tercih edilmesinin nedeni bazı önemli özellikleri sayesindedir (Zhang ve diğ., 2006; Zhang ve diğ., 2009; Zhang ve diğ., 2010; Kocarev ve Lian, 2011). Şifreleme ile ilgili sistemlerin

gereksinimlerinden olan karışıklık (confision) ve difüzyon (diffusion) özelliklerini garanti eden bu özellikler aşağıda listelenmiştir (Kocarev ve Lian, 2011).

- Kaotik sistemlerin uzun dönem davranışları periyodik değildir.
- Sistem gezingeleri (trajectories) ilk koşullara ve kontrol parametrelerine bağlıdır.
- Sistemin denklemi rastgele değil, belirgindir. Düzensiz davranışların nedeni gürültüden ziyade içsel doğrusal olmamadandır.

Kaotik değerleri tam sayı değerlerine dönüştürülmesi kaos tabanlı s-kutu tasarımlarında en yaygın kullanılan yaklaşımdır. Bu yaklaşım ile sürekli değerleri kaotik yörüngeler tamsayı değerli rastgele dizi üretmek için sayısallaştırılır. Sayısallaştırılmış rastgele dizi rastgele s-kutunun kaynak entropisidir.

Literatürdeki kaos tabanlı s-kutu yapımı ile ilgili birçok çalışma bulunmaktadır. Tang ve diğ. (2005), Tang ve Liao (2005), Chen ve diğ. (2007), Jakimoski ve Kocarev (2001) çalışmalarında ayrık zaman kaotik sistemlerin çıktılarını s-kutu hücrelerine dönüştürerek kaos tabanlı s-kutular üretmişlerdir. Khan ve Shah (2014), Altaleb ve diğ. (2017), Belazi ve Latif (2017), Belazi ve diğ. (2017b), Lambić (2017), Khan ve Asghar (2018) çalışmalarında farklı tasarım yapıları ile ayrık zaman kaotik sistemlerinin basit matematiksel yapısını birleştirip yeni önerilerde bulunmuşlar. S-kutu üretiminde sürekli zaman kaotik sistemler ilk olarak Özkaynak ve Özer (2010) çalışması ile başlamış ve Khan ve diğ. (2012), Khan ve diğ. (2013), Çavuşoğlu ve diğ. (2017) sürekli zaman kaotik sistemi kullanarak birçok iyi tasarım ortaya çıkarmışlar.

S-kutuların performans özelliğini geliştirmek için kaotik sistemlerin zaman gecikmesi (Özkaynak ve Yavuz, 2013), hiper kaotik yapı (Liu ve diğ., 2015; Khan, 2015; Özkaynak, 2015), kesirli kaotik sistem (Khan ve Shah, 2015; Farwa ve diğ., 2016; Jamal ve diğ., 2016; Özkaynak ve diğ., 2017; Belazi ve diğ., 2017a) gibi zengin dinamik özelliklerinden yararlanılmıştır.

S-kutu tasarımlarında, şifreleme yönünden daha iyi performans sağlayan s-kutuları elde etmek için kaotik sistemler ile optimizasyon algoritmalarının birlikte kullanıldığı birçok çalışma bulunmaktadır.

Chen (2008) çalışmasında kare matris dizisi oluşturmada Baker haritalamayı ve başlangıç tablosunu oluşturmak için Chebyshev haritalamayı kullanarak algoritma oluşturmaktadır.

Yapılan çalışmada hem kaotik haritalamanın hem de benzetilmiş tavlama (simulated annealing) yöntemine dayanan etkili bir algoritma geliştirilmiş.

Lambić (2014) düşük karmaşıklıkta ve geniş anahtar aralığında olacak şekilde kaotik haritalamaya ve bileşik (composition) metotlara dayanan s-kutu oluşturmuş. Liu ve diğ. (2015) çalışmasında üç boyutlu dört-kanat otonom kaotik sistem kullanarak s-kutu oluşturmaktadır. Lambić (2017) çalışmasında ayrık kaotik haritalama tekniğine dayanarak geliştirdiği algoritma ile s-kutu oluşturmaktadır.

Çavuşoğlu ve diğ. (2017) rastgele sayı üretmek için yeni Zhongtang kaotik sistemini kullanarak karmaşık ve dinamik özellikleri olan etkili s-kutu üretimi için rastgele sayı üreten algoritma tasarlamışlar.

Khan ve Asghar (2018) dirençli doğrusal olmayan mekanizmaları sentezlemek için Gingerbreadman kaotik haritalama ve S_8 permütasyonu kullanarak bir s-kutu oluşturma tekniği sunmaktadır. S-kutunu ilk koşullarını kaotik sistemden elde ediyor ve elde edilen her değer için sonraki adımda S_8 permütasyonu yöntemini kullanıp s-kutuyu oluşturuyor.

Bazı çalışmalar kaotik s-kutu oluşturmak için karmaşık çok boyutlu araştırma uzayında en iyi olan genetik algoritmaya başvurmaktadır. Wang ve diğ. (2012) s-kutuların oluşturulması problemini gezgin satıcı problemine (travelling salesman problem) benzeterek kaotik ve genetik algoritmadan yararlanarak s-kutu tasarlamışlar. Aynı çalışmada genetik algoritmanın ilk bireyler iki kaotik haritalamayı (logistic haritalama ve tent haritalama) tekrarlayarak oluşturulmaktadır ve optimizasyon ve kontrol parametreleri kaotik haritalama tarafından elde edilmektedir.

Wang ve Peng (2012) genetik algoritmanın s-kutu performansını geliştirmek için kullanmışlar. Çalışmalarında kaotik haritalama yöntemleri ile üretmiş oldukları s-kutuları ilk bireyler olarak sisteme verip genetik algoritmanın optimizasyon değerleri ile en iyi performansı veren s-kutuyu üretmeye çalışmaktadırlar. En iyi değer olarak s-kutunun doğrusal olmama özelliğini kullanmışlar.

Guesmi ve diğ. (2014) s-kutu üretmek için genetik algoritma ve kaotik haritalama yöntemlerini kullanarak üç aşamalı algoritma geliştirmişler. Algoritmanın ilk adımında ilk s-kutu üretilmektedir. İkinci aşamada genetik algoritmanın kontrol parametreleri kaotik Lorenz

sistemini kullanılarak belirlenmektedir. Üçüncü aşamada en yüksek doğrusal olmama özelliğine sahip s-kutu genetik algoritma teknikleri ile elde edilmektedir.

Ahmad ve diğ. (2015) kaotik logistic haritalama ve tent haritalama yönteminin birleşimi ile ilk s-kutuyu elde etmektedirler. Başlangıç s-kutusunu kenar matrisi (edge matrix) ile gezgin satıcı problemine dönüştürmektedirler. Karınca kolonisi optimizasyon algoritması (Ant Colony Optimization) tekniğini kullanarak en iyi doğrusal olmama özelliğini sağlayan s-kutuyu bulmaktadır.

Tian ve Lu (2016) kaotik haritalama ve yapay arı kolonisi algoritması (artificial bee colony algorithm) ile s-kutu tasarımı yapmışlar. Çalışmalarında başlangıç s-kutusunu elde etmek için altı boyutlu bileşik çoklu kaotik haritalama (the six-dimensional compound hyperchaotic map) yöntemini kullanırken s-kutu performansı için yapay arı kolonisi algoritmasını kullanmaktadır. Uygunluk fonksiyonu (fitness function) için doğrusal olmama ve diferansiyel dağılım özeliklerini kullanmaktadır.

Tian ve Lu (2017) kaotik haritalama ve bakteriyel arama optimizasyon algoritması (bacterial foraging optimization) ile s-kutu tasarımı yapmışlar. Çalışmalarında başlangıç s-kutusunu elde etmek için sarmalanma logistik haritalama (intertwining logistic map) yöntemini kullanırken s-kutu performansı için bakteriyel arama optimizasyon algoritmasını kullanmaktadır. S-kutunu doğrusal olmama ve diferansiyel dağılım özeliklerini uygunluk fonksiyonları olarak kullanılmaktadır.

Ahmad ve diğ. (2016) çalışmasında parçalı doğrusal kaotik haritalama (piece-wise linear) yöntemi ilk başlangıç s-kutusunu oluşturduktan sonra gezgin satıcı problemi öncesi oluşan s-kutuyu her biri 8 düğüm ve 28 kenar içerecek şekilde 32 alt çizgeye (graph) bölmektedir. Gezgin satıcı problemi algoritmasında en iyi sonucu alacak şekilde s-kutu oluşturulmaktadır.

Farah ve diğ. (2017) kaotik haritalama ve öğretme-öğrenme tabanlı optimizasyon (Teaching–Learning-Based Optimization) yöntemleri ile s-kutu tasarlamışlar. Oluşturdukları metot her döngünün satırı sola kaydırma ve sütün döndürme olacak şekilde iki dönüşüm içeren 8 döngüden oluşmaktadır. İlk başta s-kutusu için girdi değerleri üretilir, sonra her döngüden kullanılan yöntemler kullanılarak s-kutunun çıktısını hesaplamak için lojistik haritalamanın kontrol parametresi ve başlangıç koşulu üretilir. S-kutunun performansı analizini arttırmak için öğretme-öğrenme tabanlı optimizasyon kullanılır.

Ahmed ve diğ. (2019) ayrık kaotik haritalama ve ateşböceği algoritmasını (firefly algorithm) kullanarak s-kutu oluşturmuşlar. Başlangıç s-kutusunu ayrık kaotik haritalama ile elde edip en iyi s-kutuyu elde etmek için yapay ateşböceği algoritmasını kullanmışlar. Kaotik haritalama ile ateşböceği algoritması için gerekli olan ateşböceklerini elde etmiş oluyorlar. Yeterli sayıda ateşböceği elde ettiklerinde algoritma en iyi doğrusal olmama değerini veren s-kutuyu elde edene kadar çalışmaktadır.

Zhang ve diğ. (2018) eski Çin felsefesi olan I-Ching içermiş olduğu yenilikçi operatörleri (I-Ching operators, ICOs) kullanarak s-kutu tasarlamıştır. I-Ching felsefesinden üretilmiş olan intrication, turnover ve mutual operatörleri ikili fonksiyonun (Boolean function) çıktı yerini değiştirmek için şifrelemede s-kutu tasarımında kullanılmaktadır.

Ullah ve diğ. (2017) sonlu alanda kaotik sistemlerden kaotik lojistik tent sistemi ile doğrusal kesirli dönüşüm (linear fractional transformation) kombinasyonunu kullanarak s-kutular oluşturmuşlar. Doğrusal kesirli dönüşüm için gerekli olan ilk değerleri lojistik tent sistem ile elde etmektedirler. Doğrusal kesirli dönüşüm kullanarak daha güçlü cebirsel özellikli s-kutular oluşturduklarını göstermektedirler.

Özkaynak (2019) çalışmasında ayrık zaman kaotik sistemleri ve sürekli zaman kaotik sistemlerine dayanarak oluşturdukları s-kutulardan en iyi sonucu veren iki farklı s-kutuyu vermişlerdir. Her iki sistemde elde ettikleri s-kutuların maksimum lineer olmama özelliğinin matematiksel yapılar ile geliştirilmesi gerektiğini belirtmişler.

Kaotik sistemler ile üretilen s-kutuların daha iyi sonuç verebilmesi rastgele üretilen değerlere ve bu işlemde kullanılan ilk koşullar ve kontrol parametrelerinin tasarımının iyi belirlenmesine bağlıdır. Özkaynak (2017) çalışmasında en çok bilinen iris veri setinde yer alan özeliklerden Sepal uzunluğu, sepal genişliği, petal uzunluğu ve petal genişliğini kaotik sistemin ilk koşul ve kontrol parametreleri olarak kullanmıştır.

Kaotik sistemlerin farklı boyut özelliği kullanarak geliştirilmiş s-kutuları da bulunmaktadır. Ye ve Zhimao (2018) çalışmalarında iyi dinamik bir s-kutu üretmek için altı boyutlu kesirli Lorenz-Duffing kaotik sistem ve O-shaped path scrambling algoritmasını geliştirmişler. Altı boyutlu kesirli Lorenz-Duffing kaotik sistemi ön s-kutu üretimini yapmak için, O-shaped path scrambling algoritmasını s-kutu elemanlarının sırasının rastgele olmasını sağlamak için kullanmaktadır. Al Solami ve diğ. (2018) çalışmalarında yedi sistem parametresi, on iki terimi

ve üç kübik lineer olmayan ürün terimi ile 5 boyutlu hiperkaotik sistem ile s-kutu oluşturmaktadır. Peng ve diğ. (2011) çalışmalarında 4 boyutlu hiperkaotik sistem ile s-kutu oluşturmaktadır. Alzaidi ve diğ. (2018) çalışmalarında tek boyutlu kaotik haritalamayı kullanarak ve belirlenen uygunluk fonksiyonu ile üretilen s-kutunun β-tepe tırmanma algoritması yardımıyla en iyi olan s-kutuyu oluşturmuşlardır. Lambić (2020) sayıların çarpımı ve dairesel kaydırma işlemlerini temel alan yeni tek boyutlu ayrık-uzay (discrete-space) kaotik haritalamayı sunmuş.

Juremi ve diğ. (2017) "Determinant Rotation" olarak isimlendirdikleri matematiksel işlem yapısı oluşturarak AES algoritmasının her döngüsünde farklı s-kutu kullanılmasını sağlayan yeni bir bölüm oluşturmuşlar. Ullah ve diğ. (2018) çalışmasında matematiksel dönüşümler kullanarak s-kutu tasarımı yapmışlar. 256 öğe içeren bir grubun kesirli dönüşüm kullanarak matematiksel işlemleri sonucu oluşturdukları s-kutuların cebirsel saldırılara karşı dayanıklı olduğunu belirtmektedirler.

Ahmad ve Malik (2016) çalışmasında kaotik tabanlı sinir ağı ile s-kutu üretme algoritması tasarlamışlar. Sinir ağı, sekiz nöronlu girdi katmanı, tek nöronlu çıktı katmanı ve iki gizli katmandan (Gizli katmanın birincisinde 4 nöron, ikincisinde 2 nöron bulunmaktadır.) oluşmaktadır. Arrañaga ve diğ. (2017) çalışmasında $GF(2^8)$ ters alma işlemi ardından her bir bit için üç katmanlı (girdi, çıktı, ve gizli) sinir ağı 8 alt ağ ile s-kutu üretmektedir. Bir bit için oluşturulan alt ağ, 4 nöronlu girdi katmanı, tek nöronlu çıktı katmanı ve 2 nöronlu gizli katmanı ile toplamda 7 nörondan oluşmaktadır.

Khan ve diğ. (2019a) Gaussian dağılım metodunu ve metodun rastgele ürettiği sayıları, "Box-Muller" dönüşüm, "polarization decision", ve "central limit" algoritmasını içeren doğrusal kesirli dönüşümü s-kutuyu oluşturmak için kullanmaktadırlar. Khan ve diğ. (2019b) blok şifreleme algoritmasında kullanılan matematik temellerinin zincirini oluşturan yerine koymalı devşirim ağ (Substitution permutation network, SP-network) yapısını kullanmaktadır. SP-ağ, s-kutu, devşirim kutu ve anahtar oluşturmayı içermektedir.

Tanyildizi ve Özkaynak (2019) "logistic map", "tent map", "sine map", ve "circle map" kaotik haritalama metotları için en iyi ilk durum ve kontrol parametrelerini yedi farklı optimizasyon algoritmaları ile belirlemişler. En iyi ilk durum ve kontrol parametreleri ile kaotik s-kutular

oluşturmuşlar ve testler sonucu en iyi performansı sağlayan s-kutu analiz sonuçları ile ilan etmişler.

Yi ve diğ. (2019) kablosuz sensör ağlar için blok şifreleme algoritması tasarlamışlar. Blok şifreleme algoritmasında kullanacakları s-kutuyu "compound chaotic map", "sinusoidal chaotic map", "Baker map" ve "linear congruence generator" kullanarak oluşturmuşlar.

Lu ve diğ. (2019) daha iyi kaotik performans ve aralığa sahip olan yeni bileşik kaotik sistem "tent-logistic" sistemi ile s-kutu oluşturma algoritması önermişler. Lu ve diğ. (2020) en iyi kaotik aralığa ve kaotik özellikler sahip olan yeni ayrık bileşik kaotik sistem (discrete compound chaotic system), Logistic-Sine sistem sunmuşlar ve Logistic-Sine sistemini s-kutu oluşturmak için kullanmışlar.

Zhang ve diğ. (2020) hem "fractional-order logistic" sistem ile etkin s-kutu oluşturma algoritması tasarlamışlar hem de "fractional-order Logistic system", s-kutuları, "Secure Hash" algoritmasını "MD2" kullanarak resim şifreleme şeması sunmuşlar.

Mahmood Malik ve diğ. (2020) daha güçlü s-kutu tasarımı için afin dönüşüm matrisini kaotik sistemden yararlanarak oluşturmuştur. Kaotik tabanlı afin dönüşümü üretme metodu dönüşümlü matris yapısı üzerinde oluşturarak AES s-kutusuna kullanılan afin dönüşümü önemli ölçüde değiştirdiklerini göstermişler.

2.5.3. BİYOMETRİK S-KUTULAR

Şifreleme algoritmalarının daha güvenli hale gelmesi için kişiye özel eşsiz verilerin kullanımı gün geçtikçe artmaktadır. Şifreleme algoritmalarında kullanılan anahtar gibi özel girdilerde biyometrik veri kullanımı çok yaygındır. Blok şifrelemenin en önemli öğelerinden olan s-kutu tasarımında da biyometrik veriler kullanılmaktadır.

Deoksiribo nükleik asit (DNA) şifreleme (Gehani ve diğ., 2003) s-kutu üretiminde DNA yapısının kullanılmasına ön ayak olmuştur. DNA yapısı çifte sarmal yapılıdır ve çift zincirden oluşmaktadır. İki zincir birbirinin tamamlayıcısıdır ve nükleotit zinciri olarak isimlendirilir. Nükleotit zincirinde dört adet nükleotit asit bazı bulunmaktadır. Adaenin (A), Guanin (G), Sitozin (C), ve Timim (T) DNA nükleotit zincirinde bulunan bazlardır. DNA bazları çift olarak eşleşmektedir. DNA nükleotit zincirlerinden birinin dizilimi biliniyorsa diğer zincir

oluşturulabilmektedir. Adenin, Timinin bazı ile eşleşirken, Sitozin (C), Guanin(G) ile eşleşmektedir. Örneğin, TACGTC diziliminin karşılığı ATGCAG olmaktadır.

DNA şifrelemede her bazı temsil eden harf farklı kombinasyonlarda ifade edilmektedir. İkili sistemde A için 00, C için 01, G için 10, T için 11 kullanılmaktadır (Ning, 2009). DNA diziliminin ikili sistemdeki karşılığı oluşturulmaktadır. Örneğin, TACGTC diziliminin ikili sistemdeki karşılığı 110001101101 şeklinde oluşturulur.

Al-Wattar ve diğ. (2015a) DNA tabanlı s-kutuyu 4 adımda oluşturmaktadır. İlk adımda, DNA dizilimindeki her bayt 4 adet (w, x, y, z) baz içerecek şekilde ikili sistemde karşılığı oluşturulmaktadır. İkinci adımda, "Forward" ve "Reverse" fonksiyonları ile dizilim tekrardan oluşturulmaktadır (w, x', y, z'). Üçüncü adımda, yeni dizilim XOR işlemine tabi tutulur. Son adımda, "central dogma transcription" olarak adlandırdıkları işlem serisi gerçekleştirilmektedir.

Al-Wattar ve diğ. (2015b) s-kutu oluşturmak için iki DNA dizilimi kullanmaktadır. İlk DNA dizilimini 4 baz olacak şekilde ayırılmaktadır. Her oluşan 4 baz ilk s-kutunun bir öğesini oluşturmaktadır. İkinci DNA dizilimini aynı şekilde 4 baz olacak şekilde ayrılmaktadır. Her dört bazın soldan iki bazı yeni s-kutunun satırını, sağdan iki bazı yeni s-kutunun sütunu temsil etmektedir ve ikili sistemde karşılığı bulunarak s-kutunun hücresi bulunur. Yeni s-kutuda belirlenen hücresine ilk s-kutunun öğesi yazılır. Tüm s-kutu oluşana kadar işlemler tekrar edilir.

Kadhim ve diğ. (2016) veri işleme, DNA toplama, DNA çıkarma, mantıksal ve aritmetik işlemler ve arama işlemi olmak üzere 5 adımda s-kutu oluşturulmaktadır. Veri işleme adımında, iki karakter dizisi belirlemiş oldukları 8 kurala göre DNA dizilimine dönüştürülür. DNA toplama adımında, belirlenen iki DNA dizilimi ayrı ayrı ekleme kuralına göre yeni dizilimler oluşturulur. DNA çıkarma adımında, iki dizilimden boyut azaltılarak tek bir dizilim oluşturulur. Mantıksal ve aritmetik işlemler adımında, DNA dizilimi XOR ve modüler aritmetik işlem serisinden geçerek s-kutu oluşmaya başlamaktadır. Arama adımında, oluşan s-kutuda tekrar eden değerler varsa işlemler tekrar etmeyen sonuçlarla elde edilen s-kutu oluşana kadar devam etmektedir.

Farhan ve diğ. (2020) DNA tabanlı s-kutulardan (Al-Wattar ve diğ., 2015b; Kadhim ve diğ., 2016) esinlenerek RNA dizilimi ile s-kutu oluşturmuşlar. Algoritmanın ilk adımında belirlenen gizli karakter dizisi Kadhim ve diğ., (2016) çalışmalarında kullanmış olduğu veri işleme adımını uygulayarak bir DNA dizilimi oluşturmaktadırlar. Oluşan DNA dizilimi RNA

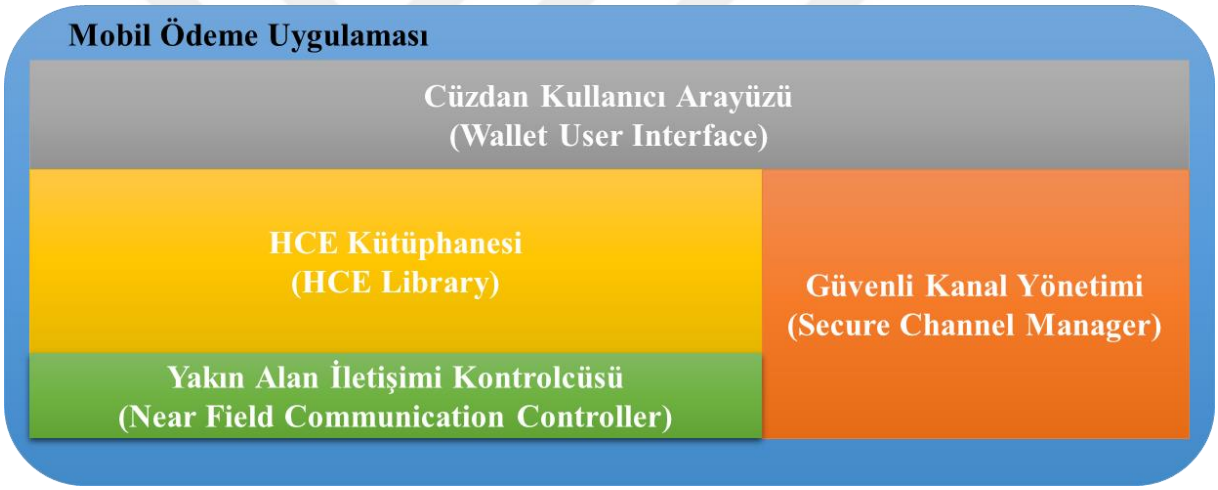
dizilimine dönüştürülür. Bu işlemi yaparken DNA dizilimin baz eşlemesinden yararlanılmıştır. DNA diziliminde yer alan Timim bazı Urasil (U) bazına dönüştürülerek RNA elde edilir. Bio-işleme adımında, elde edilen RNA dizilimi iki parçaya bölünür. İlk kısmı belirlemiş oldukları ekleme kuralına tabi tutulur, ikinci kısmı belirlemiş oldukları çıkarma kuralına tabi tutulur ve elde edilen iki RNA parçası belirlemiş oldukları XOR işlemi kuralları ile tek bir dizilim elde edilir. Elde edilen RNA ile s-kutu hücresi ve onun öğesi elde edilir. Son olarak tekrar eden ve eksik değerler kontrol edilerek s-kutu tamamlanır.

3. MALZEME VE YÖNTEM

Bu bölüm; tez çalışması kapsamında kullanılan şifreleme modeli ve algoritmasının yapısını, biometrik veriyi, önerilen etkin biyometrik s-kutu ve ters s-kutu algoritmasını, güvenlik performans metriklerini içermektedir.

3.1. MODELİNİN TANIMLANMASI

Mobil Ödeme Uygulaması Android tabanlı cep telefonları üzerinde çalışan mobil cüzdan uygulamasıdır. Mobil ödeme uygulaması Şekil 3.1'de görüldüğü gibi cüzdan kullanıcı ara yüzü, uygulama kütüphanesi, güvenli kanal yönetimi ve NFC kontrolcüsü modüllerinden oluşmaktadır.



Şekil 3.1: Mobil ödeme uygulaması.

Cüzdan kullanıcı arayüz modülü, geliştirilmiş olan mobil cüzdan uygulamasının kullanıcı ile aktif iletişim kurmaya yarayan kullanıcı arayüz kütüphanesidir. Bu kütüphanede, sistemde kullanılacak arayüzlerin tasarımı, kodlaması için gerekli olan tüm alt yapının saklandığı kısımdır.

Güvenli Kanal Yönetimi, mobil ödeme uygulaması ve HCE bulut sistemleri arasındaki iletişimin güvenliğini sağlayan alt kütüphanedir.

NFC Kontrolcüsü pos cihazı ile uygulama arasındaki iletişimi sağlayan modüldür.

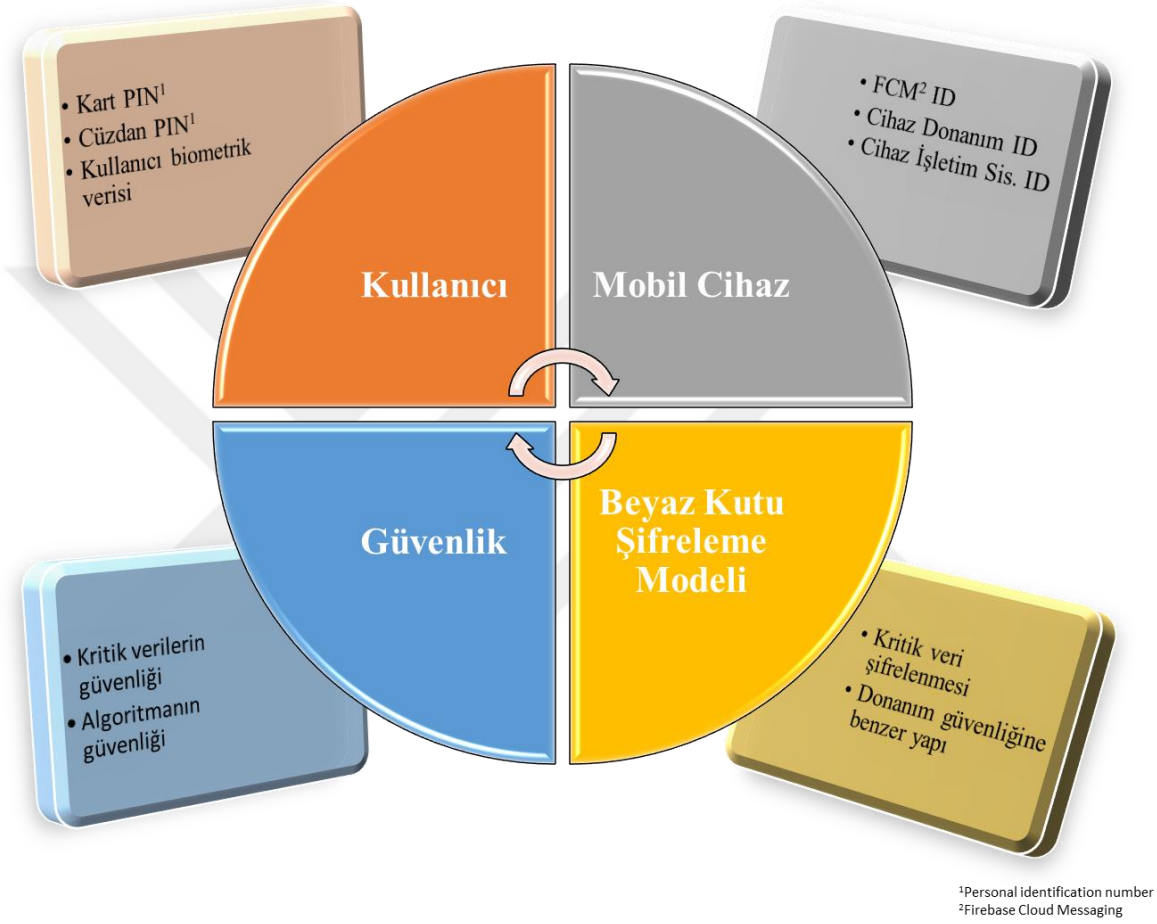
HCE kütüphanesi uygulamanın Android cihazlar üzerinden çalışmasını sağlamak amacıyla gerekli olan tüm bileşenleri içeren Java ve NDK tabanlı bir kütüphanedir. HCE kütüphanesi kütüphane arayüzü, kütüphane yönetimi, uygulaması, bulut iletişimcisi, beyaz kutu kütüphanesi, şifrelenmiş yerel veri tabanı, servisleri gibi farklı bileşenleri içermektedir.

- HCE kütüphane arayüzü, HCE kütüphanesi ve uygulama arayüzü arasındaki tüm iletişimi yöneten alt kütüphanedir.
- HCE kütüphane yönetimi, fonksiyonlarının tamamını yöneten, gerektiğinde veritabanı ile iletişim kuran, gerektiğinde bulut ile iletişim kuran ana alt modüldür.
- HCE uygulaması, temassız bir kart gibi çalışmayı sağlayan emülasyon kütüphanesidir.
- Bulut iletişimcisi, bulut ile tüm iletişimleri yöneten bir arayüz katmanıdır.
- Beyaz kutu kütüphanesi, ihtiyaç duyulan verilerin güvenliğini sağlamak amacıyla geliştirilmiş olan yazılım tabanlı karmaşık kripto algoritmalarını içeren alt kütüphanedir.
- Şifrelenmiş yerel veritabanı, ihtiyaç duyulan verilerin şifreli olarak saklandığı veritabanıdır. Veritabanındaki verilerin güvenliği beyaz kutu kütüphanesi bileşeni ile sağlanmaktadır.

Belirtilen modüllerden en önemlisi kişisel verilerin saklamak amacıyla geliştirilecek olan yazılım tabanlı kripto algoritmalarını içeren kütüphanedir. Şifreleme modelinden güvenliğin yanı sıra fonksiyonel olması beklenmektedir. Fonksiyonellikten kasıt sistemin her türlü ortama uyum sağlayacak şekilde sistemin işlevini devam etmesidir. Oluşturulacak kütüphanede verilerin saklanması için kullanılacak algoritma belirlenmesi karşılaştırmalı olarak 3.2 bölümünde verilmiştir.

Mevcut mobil ödeme sisteminde kullanıcı, mobil cihaz, şifreleme modeli ve güvenlik olmak üzere 4 ana bileşen bulunmaktadır. Mobil ödeme sisteminin bileşenleri ve bu bileşenlerin sağlamış olduğu veri ve olanaklar Şekil 3.2’de verilmiştir. Sistem kullanıcısı işlemlerini gerçekleştirirken kart numarası, cüzdan numarası ve biyometrik verisini kullanabilmektedir. Sistem, yüklü olduğu cihazdan işlem gerçekleşirken cihaza ait donanım numarası, işletim sistemi numarası ve mesaj numarası verileri kullanabilmektedir. Sistemin kullanacağı veri şifreleme modeli beyaz kutu şifreleme modelidir. Beyaz kutu şifreleme modeli ile geliştirilen sistemler, sistemi gözlemleyen üçüncü şahısların sistem ile ilgili tüm bilgilere erişebilmesine

olanak sağlamaktadır. Bu yüzden sistemde bulunan verilerin gizli olması çok önemlidir. Sistemin donanım güvenliğine sahip gibi güvenli olması ile sistemde bulunan kritik verilerin şifrelenmesi de gerekmektedir. Şifreleme algoritmasının bilinen şifreleme algoritmasının yapısı dışında olması gerektiğinden gerekli güvenlik eklentilerine ihtiyaç duyulmaktadır.



Şekil 3.2: Kullanılacak platformun sağladığı olanaklar.

3.2. ŞİFRELEME ALGORİTMASININ YAPISI

Mobil ödeme sistemleri banka kartlarında kullanılan şifreleme algoritmalarının temeline dayanmaktadır. Bankalar Arası Kart Merkezi'nin belirlemiş olduğu standart olarak kullanılan şifreleme algoritmaları bulunmaktadır. Kredi kartındaki şifreli verinin aktarılması ve banka tarafından onaylanması işlemlerinde Veri Şifreleme Standardı (DES) kullanılmaktadır. Mobil ödeme sistemlerinde bankalar ile olan iletişim sırasında yapılan işlemlere güvenlik anlamında herhangi bir müdahale yapılamamaktadır. Uygulamanın güvenlik açısından geliştirilmesi için diğer katmanlardaki verilerin güvenliği esas alınmaktadır.

Bankacılık uygulamalarında kredi kartlarında yer alan donanım güvenlik modülü (Hardware Security Module, HSM) kullanılmaktadır. Donanım güvenlik modülü, güçlü kimlik doğrulama için gerekli hassas kriptografik anahtarları koruyup, yöneten ve güvenli bir şekilde fiziksel ortama saklamak ve kriptografik işlemleri en hızlı şekilde gerçekleştirmek için tasarlanan donanım cihazlarıdır. HSM cihazları dakikada çok fazla şifreleme işlemi yapmalarının yanı sıra bu işlemleri özel tasarımları sayesinde işlemci yüklemeleri en aza indirgendiğinden çok hızlı bir şekilde gerçekleştirebilmektedir. Günümüzde artan sahtekarlık, dolandırıcılık ve bilgilerin ele geçirilmesi gibi olayların oluşmasını minimuma indirgemek için HSM kullanılmaktadır. Birçok uygulama yazılım tabanını güçlendirilip HSM ile entegre olduğu sürece sistemlerin üçüncü şahıslar tarafından kırılması zor olacağından güvenli bir şekilde çalışacaktır.

Günümüzde birçok uygulamada (örneğin e-fatura) HSM kullanma gerekliliği banka kanunları ile gelmektedir. Donanım güvenlik modülleri ile simetrik ve asimetrik anahtarları oluşturma ve saklama, şifreleme ve şifre çözme (encrypt / decrypt), imzalama ve onaylama (sign / verify), özetleme (hashing) gibi yazılımsal kripto uygulamaları daha ucuz ve düşük güvenlik ile gerçekleştirdiğimiz birçok uygulamayı güvenliğin son derece önemli olduğu alanlarda daha güçlü hale getirebiliriz.

Online bankacılık, veri tabanı şifreleme, kod imzalama, e-pasaport, e-faturalama, bilgi ve sunuculara kimlik erişim onayı, güvenli IP telefon uygulamaları, yoğun kriptografik operasyonların hızlandırılması, anahtar yönetim çözümleri, belge imzalama gibi uygulamalarda donanım güvenlik modülü kullanılmaktadır.

HSM kullanımı güvenlik ve performans yönünden çok fazla avantaj sağlamaktadır. Anahtar korunum işlemleri modül içinde yapılmaktadır, dış dünyaya kapalı olduğundan korunumlar özel kök anahtarlar ile yapılmaktadır, rastgele anahtar oluşturma hızı yazılımsal yapılara göre oldukça performanslıdır ve saldırılara karşı kendini sıfırlama özelliğine sahiptirler. Hem asimetrik hem de simetrik şifreleme algoritmalarında anahtar oluşturma, veri şifreleme ve şifre çözme işlemlerini kendi üzerlerindeki işlemcileri sayesinde daha hızlı bir şekilde yapabilmektedir. Bir HSM güvenlik sertifikasyonu kullanılacağı uygulama yapısının kanunlarına göre şekillenip sertifikasyon süreçlerinden geçmeden kullanılmamaktadır. Bankalar Arası Kart Merkezi'nin kredi kartlarında kullandığı HSM güvenlik sertifikasyonunda veri şifreleme algoritmasının temeline dayanan Veri Şifreleme Standardını kullanmaktadır.

Oluşturulan şifreleme modeli, Bankalar Arası Kart Merkezi'nin kullandığı standartların dışına çıkılmadan uygulamada kullanabileceğimiz şifreleme algoritmalarının çalışma yapısı ve modele entegrasyonu şeklinde planlandı.

En çok kullanılan simetrik ve asimetrik şifreleme algoritmalarından DES, Üçlü-DES, AES ve RSA Tablo 3.1'e yıl, şifreleme türü, temel, prensip, blok boyutu, anahtar boyutu, şifreleme-şifre çözmede anahtar kullanımı, şifreleme-şifre çözme algoritması, döngü sayısı, güvenlik, şifreleme-şifre çözme hızı, güç tüketimi, yazılım/donanım uygulamaları gibi etkenler yönünden karşılaştırılmıştır (Mathur ve Kesarwani, 2013; Mahajan ve Sachdeva, 2013; Padmavathi ve Kumari, 2013; Singhal ve Singhal, 2016; Şengel ve diğ., 2018, Şengel ve diğ., 2020a).

AES ve DES en çok tercih edilen blok şifreleme algoritmalarıdır. DES algoritması şifrelemeyi 64-bit blok boyutunda 56-bit anahtar boyutu ile 16 döngü ile, AES algoritması şifrelemeyi farklı anahtar boyutları ile farklı döngü sayıları ile 128-bit blok boyutu ile gerçekleştirmektedir. Anahtarın boyutu şifreleme algoritmasının güvenilirliğini arttıran en önemli unsurlardan biridir. DES 56-bit anahtar boyutu ile yaklaşık 72 katrilyon olasılığı bulunmaktadır, bu değer çok büyük görünse de günümüz bilgisayarlarının işlemci güçleri göz önünde bulundurulduğunda kaba kuvvet atakları için güvenlik zafiyeti içermektedir (Mathur ve Kesarwani, 2013). DES algoritmasındaki güvenlik zafiyetini geliştirmek için üçlü DES algoritması ile anahtar boyutu 168-bit olmuştur. Üçlü DES algoritması, DES algoritmasına göre üç kat daha fazla CPU gücü aldığından performans açısından yeterli olmadığı gözlemlenmiştir (Mathur ve Kesarwani, 2013). AES algoritması tasarımı gereği donanımda daha verimli, yazılımda daha hızlı olduğundan hem donanım hem de yazılım tabanlı uygulamalarda Üçlü DES'e göre daha iyi performans gösterdiği gibi blok boyutu ve anahtar boyutunun çeşitliliğinden dolayı da daha güvenilirdir (Mathur ve Kesarwani, 2013).

Mobil ödeme sistemleri hem donanım tabanlı hem de yazılım tabanlı olarak geliştirilen uygulamalardır. Mobil ödeme sistemleri için kullanılacak algoritmanın belirlenmesinde şifreleme-şifre çözme hızı, güç tüketimi, yazılım/donanım uygulamalarında kullanımı ve güvenlik en önemli etkenlerdendir (Şengel ve diğ., 2020a). Tablo 3.1'de belirtildiği gibi AES algoritması uygulama alanı açısından hem donanım hem de yazılım uygulamalarında özellikle de akıllı telefon, akıllı kart gibi küçük cihazlarda daha verimli ve hızlıdır. Tablo 3.1'de belirtildiği gibi AES algoritması şifreleme-şifre çözme hızı bakımından diğer algoritmalara göre daha hızlıdır. Tablo 3.1'de görüldüğü gibi AES ve DES algoritmaları güç tüketimi

açısından diğer algoritmalara göre daha düşüktürler. Tablo 3.1'de görüldüğü gibi güvenlik açısından AES algoritması anahtar uzunluğuna bakımından diğer algoritmalara göre daha güvenilirdir.

Tablo 3.1: Şifreleme algoritmalarının özellikleri.

Etken	**DES**	**Üçlü DES**	**AES**	**RSA**
Yıl	1977	1978	2000	1978
Şifreleme Türü	Simetrik blok şifreleme	Simetrik blok şifreleme	Simetrik blok şifreleme	Asimetrik şifreleme
Temel	Veri bloğu iki parçaya ayrılır.	Veri bloğu iki parçaya ayrılır.	Veri bloğu tek bir parçada işlenir.	İki farklı anahtar kullanılmaktadır.
Prensip	Feistel şifreleme yapısı üzerinde çalışmaktadır.	Feistel şifreleme yapısı üzerinde çalışmaktadır.	Yerine Koyma ve Permütasyon yapısında çalışmaktadır	Çok büyük tam sayılarla işlem yapmanın zorluğuna dayanır
Blok boyutu	64-bit	64-bit	128-bit	En az 512 bit
Anahtar boyutu	56-bit	168-bit	128, 192, 256 bit	1024 bitten büyük
Şifreleme-şifre çözmede anahtar kullanımı	Aynı anahtar	Aynı anahtar	Aynı anahtar	Farklı anahtar
Şifreleme-şifre çözme algoritması	farklı	farklı	farklı	aynı
Döngü sayısı	16	48	10, 12, 14	1
Güvenlik	Anahtar boyutunun küçük olmasından daha az güvenli	DES'e göre daha güvenli	Gizli anahtar boyutunun büyüklüğü ile daha güvenli	Şifrelemede kullanılan asal sayıların büyüklüğü ile
Şifreleme-Şifre çözme hızı	yavaş	daha yavaş	daha hızlı	daha yavaş
Güç tüketimi	düşük	daha fazla	düşük	yüksek
Yazılım/donanım uygulamaları	Donanımda daha iyi	Donanımda daha iyi	Hem donanım hem de yazılımda daha iyi	Verimli değil

Diferansiyel, doğrusal, kaba kuvvet, oracle gibi olası saldırı türleri bakımından şifreleme algoritmalarını karşılaştırdığımıza Tablo 3.2'de verildiği gibi AES algoritması diferansiyel, interpolasyon, kare saldırı gibi saldırılara karşı daha dirençlidir. Yerine koymalı tablo tasarımlarının güçlüğü bakımından bakıldığında DES algoritmasın s-kutusunun güçlü yapıda olmadığı görülmektedir. Üçlü DES algoritması diferansiyel kripto ataklar ile düz metni analiz edebilmektedirler.

Tablo 3.2: Şifreleme algoritmaların güvenlik saldırıları açısından karşılaştırması.

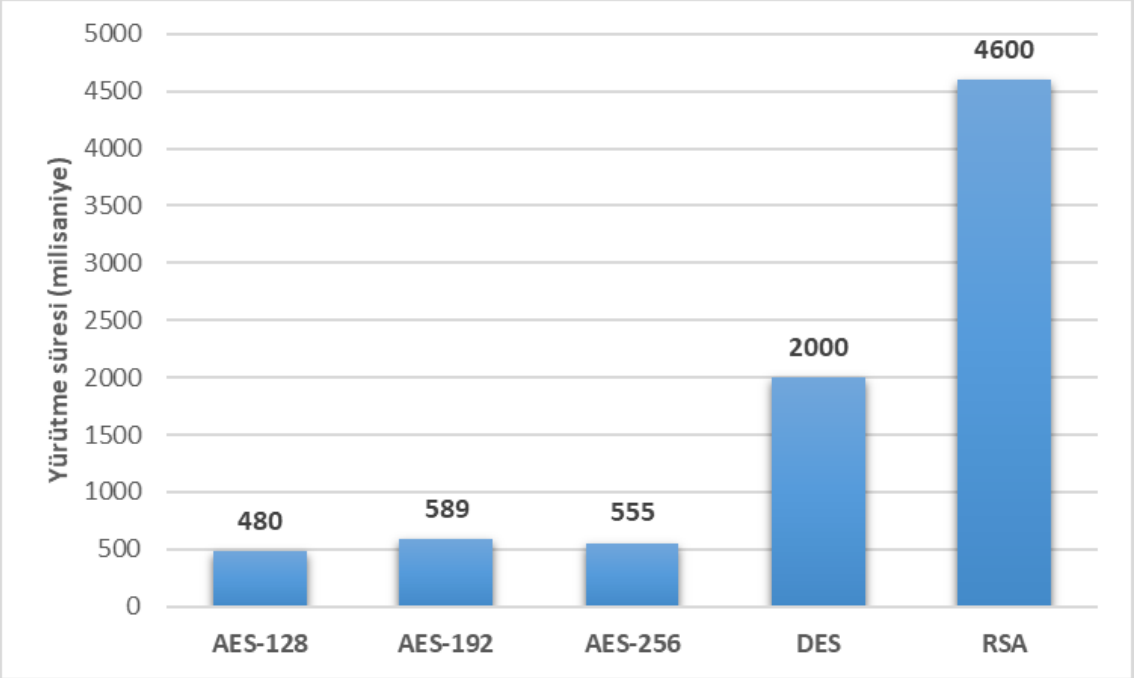
Saldırı Türü	DES	Üçlü DES	AES	RSA
Diferansiyel saldırı	Zayıf	Zayıf	Güçlü	-
Doğrusal saldırı	Zayıf	-	Güçlü	-
Kaba kuvvet saldırı	Zayıf	Zayıf	Güçlü	Zayıf
Oracle saldırı	-	-	-	Zayıf
Yerine koyma tabloları	Zayıf	-	-	-

Mobil ödeme sistemleri için en önemli etkenlerden biri şifreleme ve şifre çözme işlemlerinin hızıdır. DES, Üçlü DES, AES ve RSA algoritmalarının şifreleme işlemlerine ait hız değerleri Tablo 3.3'te verilmiştir. Tüm algoritmalar NetBeans IDE 8 yazılımı yardımıyla c programlama dilinde yazıldı. Tüm algoritmalar 64-bit Windows 10 işletim sistemi, 16 GB RAM ve Intel Core i7-7500-U (2.70 GHz - 2.90 GHz) işlemcisine sahip bir makinede aynı düz metnin 10 kez şifrelenmesiyle test edilmiştir.

Tablo 3.3: Şifreleme yürütme süreleri.

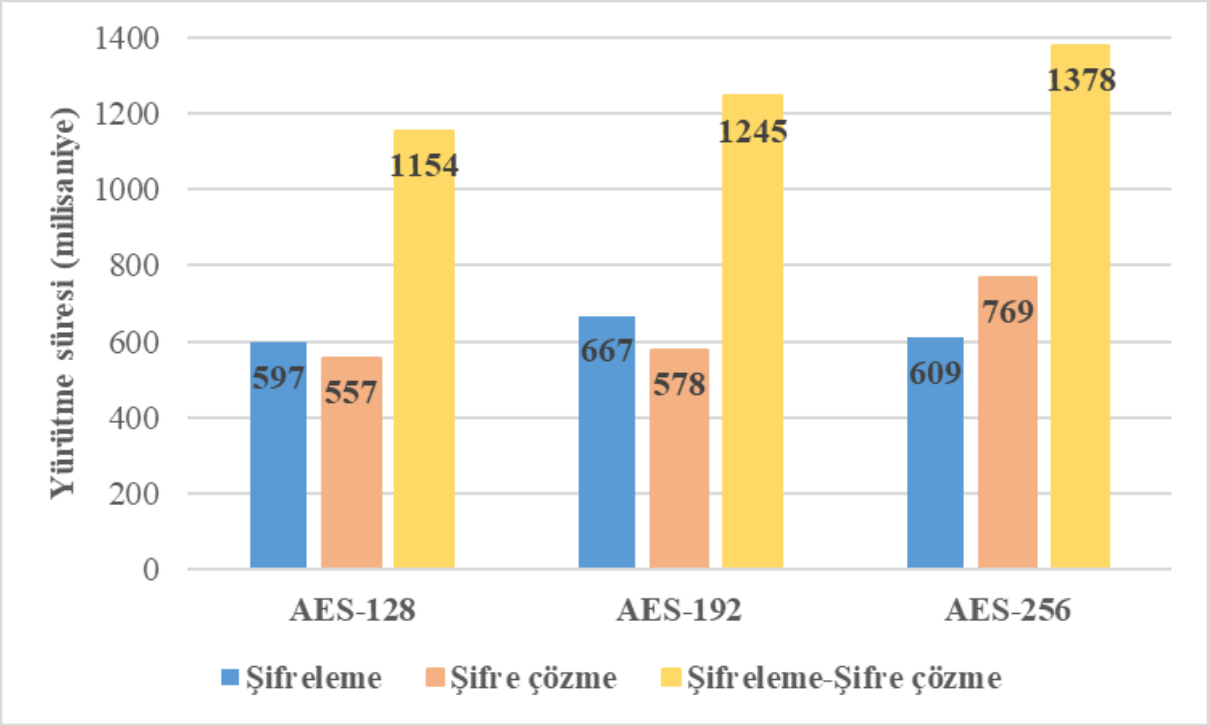
Algoritma	Test 1	Test 2	Test 3	Test 4	Test 5	Test 6	Test 7	Test 8	Test 9	Test 10
RSA	8000	6000	5000	5000	5000	3000	3000	3000	4000	4000
DES	5000	3000	2000	1000	2000	2000	1000	1000	1000	2000
AES-128	828	375	374	374	437	377	376	828	453	375
AES-192	2000	375	438	828	375	375	375	375	375	374
AES-256	2000	375	437	375	438	375	429	375	375	374

Şifreleme sırasında en fazla yürütme süresine RSA algoritması sahiptir. RSA algoritması şifrelemede kullanacağı anahtarı ne kadar büyük seçerse saldırılara karşı o kadar direnç gösterebilmektedir. Bu durum göz önünde bulundurulduğunda RSA algoritması anahtar boyutunu arttırdıkça şifreleme süresi uzamaktadır ve bu mobil ödeme sistemleri için uygun olmadığını göstermektedir. İkinci sırada ortalama 2 saniye şifreleme süresi ile DES algoritması bulunmaktadır. Üçlü DES algoritması, DES algoritmasının üç kez tekrarlanması ile verileri şifrelediğinden şifreleme süresi DES algoritmasının yaklaşık üç katı elde edilmiştir. AES algoritmasına baktığımızda ortalama olarak tüm anahtar boyutlarında diğer algoritmalara göre daha hızlı şifreleme gerçekleştirmişlerdir. Şekil 3.3'te test sonuçlarının ortalama hızları milisaniye türünden verilmiştir. AES algoritmalarını karşılaştırdığımızda anahtar boyutu ve döngü sayısının artması ile algoritmanın yürütme süresinin arttığı gözlemlenmiştir.



Şekil 3.3: Şifreleme algoritmalarının ortalama yürütme süreleri.

Yürütme süresine göre en iyi sonucu veren AES şifreleme algoritmasının anahtar boyutuna göre elde edilen şifreleme ve şifre çözme süreleri Şekil 3.4'te verilmiştir. Anahtar boyutunun artması sistemi daha güvenilir hale getirdiği gibi sistemin yürütme süresi de artmaktadır.



Şekil 3.4: AES algoritmasının anahtar boyutuna göre şifreleme ve şifre çözme süreleri.

Mobil ödeme sisteminde kişisel verilerin saklamak amacıyla geliştirilecek olan yazılım tabanlı kripto algoritmalarını içeren kütüphanede kullanılmak üzere beyaz kutu şifreleme modeli için şifreleme-şifre çözme hızı, güç tüketimi, yazılım/donanım uygulamalarında kullanımı ve güvenlik etkenleri açısında AES-128 algoritması kullanılmasına karar verilmiştir. Beyaz kutu şifreleme modeli tüm sistemin açık olması anlamına gelmektedir. Bu model ile geliştirilen sistemde AES algoritmasının bilinen yapısının kullanılması güvenlik olarak eksik kalmaktadır. Bilinen AES yapısının daha güvenilir hale getirmek için algoritmada kullanılan parametrelerin geliştirilmesine yönelik çalışmalar yapılmıştır.

3.3. BİYOMETRİK VERİ (NEDEN PARMAK İZİ?)

Yüz, parmak izi, iris, ses, imza, el geometrisi gibi biyometrik veriler birçok uygulamada kullanılmaktadır. Her biyometrik veri sahip olduğu güçlü ve zayıf yanları ile hangi uygulamalarda kullanmak için uygun olduğu belirlenmektedir. Tüm uygulamaların gereksinimlerini tümüyle sağlayan tek bir biyometrik veri bulunmamaktadır. Bir uygulama geliştirildiğinde kullanılacak verinin özellikleri ile ne kadar uyumlu olduğuna bakılmaktadır.

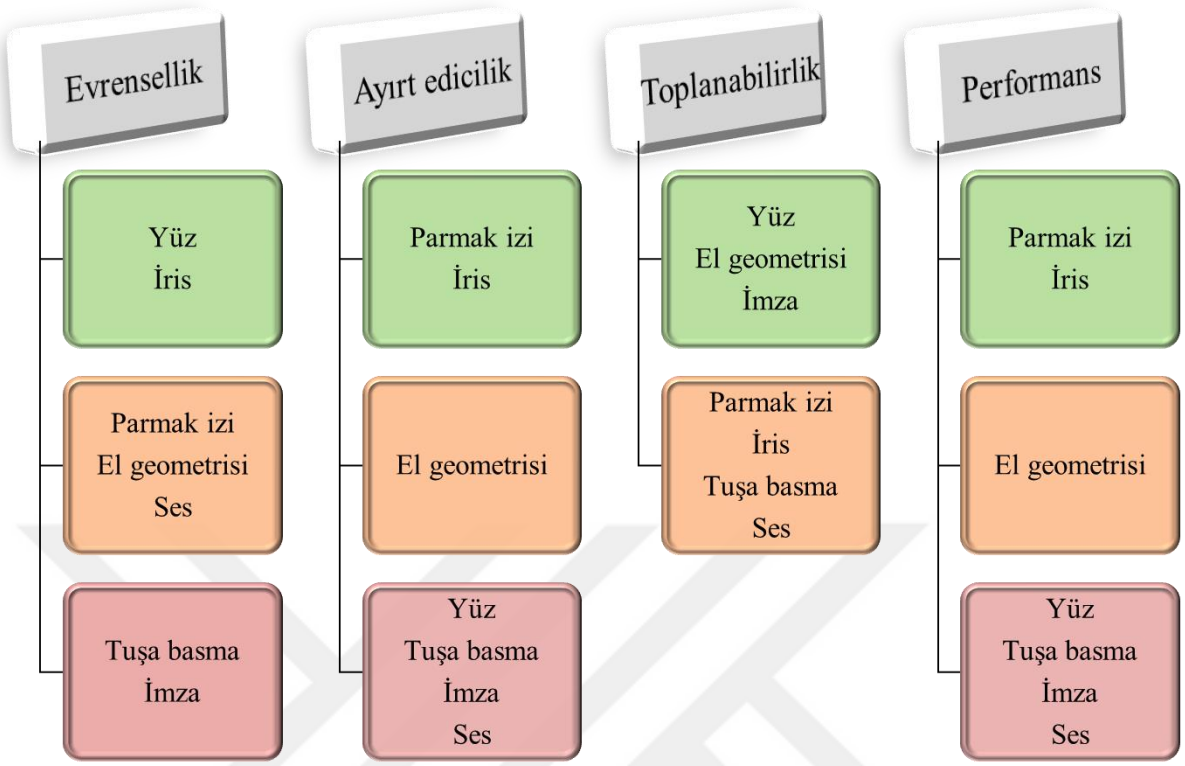
Biyometrik verilerin evrensellik, ayırt edicilik, kalıcılık, toplanabilirlik, performans, kabul edilebilirlik, kusursuzluk olmak üzere 7 faktöre dayalı biyometrik tanımlayıcılar bulunmaktadır (Uludag ve diğ., 2004). Evrensellik, ayırt edicilik, kalıcılık, toplanabilirlik biyometrik verinin özellikleri, performans, kabul edilebilirlik, kusursuzluk biyometrik verini kullanıldığı sistemin özelliklerini temsil etmktedir. Evrensellik, tüm insanlar bu biyometrik özelliğe sahip olup olmama oranına bakılmaktadır. Ayırt edicilik, ilgili biyometrik veri ile insanların birbirinden ayırt edilip edilmeme oranına bakılmaktadır. Kalıcılık, biyometrik verinin kişide ne kadar süre etkin olup olmadığına bakılmaktadır. Toparlanabilirlik, biyometrik verinin kişilerden ne kadar iyi elde edilebilir ve ölçülebilir olduğunu belirlemektedir. Performans, biyometrik verinin doğruluğu ve elde edilme hızının oranıdır. Kabul edilebilirlik, kullanıcıların sistemde ilgili biyometrik veriyi kullanma isteğinin oranıdır. Kusursuzluk, biyometrik verinin sistem üzerinden ne kadar iyi bir oranda elde edilebildiğidir.

Biyometrik tanımlayıcılarından yüz, parmak izi, el geometrisi, iris, tuşa basma, imza ve sesin biyometrik tanımlayıcı özelliklerini hangi oranda (yüksek, orta, düşük) sağladığı Tablo 3.4'te verilmiştir. Evrensellik özelliği, yüz ve iris tanımlayıcılarında yüksek; parmak izi, el geometrisi ve ses tanımlayıcılarında orta; tuşa basma ve imza tanımlayıcılarında düşük oranda sağlanmaktadır. Ayırt edicilik ve performans özellikleri, parmak izi ve iris tanımlayıcılarında yüksek; el geometrisi tanımlayıcısında orta; yüz, tuşa basma, imza ve ses tanımlayıcılarında düşük oranda sağlanmaktadır. Kalıcılık özelliği, parmak izi ve iris tanımlayıcılarında yüksek; yüz ve el geometrisi tanımlayıcılarında orta; tuşa basma, imza v ses tanımlayıcılarında düşük oranda sağlanmaktadır. Toplanabilirlik özelliği yüz, el geometrisi ve imza tanımlayıcılarında yüksek, diğer tanımlayıcılarında orta oranda sağlanmaktadır. Kabul edilebilirlik ve kusursuzluk özellikleri, yüz, imza ve ses tanımlayıcılarında yüksek; parmak izi, el geometrisi ve tuşa basma tanımlayıcılarında orta; sadece iris tanımlayıcısında düşük oranda sağlanmaktadır. Parmak izi ve el geometrisi tüm özellikleri ya yüksek ya da orta oranda sağlamaktadır. Diğer tanımlayıcılar en az iki özelliği düşük oranda sağlamaktadır.

Tablo 3.4: Biyometrik verilerin tanımlayıcı özellikleri.

Biyometrik Tanımlayıcı Özellikleri / Biyometrik Tanımlayıcı	Evrensellik	Ayırt edicilik	Kalıcılık	Toplanabilirlik	Performans	Kabul edilebilirlik	Ksursuzluk
Yüz	Yüksek	Düşük	Orta	Yüksek	Düşük	Yüksek	Yüksek
Parmak izi	Orta	Yüksek	Yüksek	Orta	Yüksek	Orta	Orta
El geometrisi	Orta	Orta	Orta	Yüksek	Orta	Orta	Orta
İris	Yüksek	Yüksek	Yüksek	Orta	Yüksek	Düşük	Düşük
Tuşa basma	Düşük	Düşük	Düşük	Orta	Düşük	Orta	Orta
İmza	Düşük	Düşük	Düşük	Yüksek	Düşük	Yüksek	Yüksek
Ses	Orta	Düşük	Düşük	Orta	Düşük	Yüksek	Yüksek

Mobil ödeme sistemlerinde kullanılması planlanan biyometrik tanımlayıcın evrensellik, ayırt edicilik, toplanabilirlik ve performans özelliklerini barındırması beklenmektedir. Mobil ödeme sistemleri için evrensellik, ayırt edicilik, toplanabilirlik ve performans özelliklerini yüksek oranda sağlayan biyometrik tanımlayıcılar yeşil renkli alanda, orta oranda sağlayan biyometrik tanımlayıcılar turuncu renkli alanda, düşük oranda sağlayan biyometrik tanımlayıcılar kırmızı renkli alanda Şekil 3.5'te listelenmişlerdir. Toplanabilirlik açısından değerlendirdiğimizde günümüzde mobil cihazların çoğu yüz, parmak izi, ses biyometrik tanımlayıcılarını okuyabilmektedir. Genel olarak sistemlerde en iyi performansı sağlayan parmak iz ve iris biyometrik tanımlayıcılarıdır. İnsanlar arasında ayırt edicilik özelliğini ele aldığımızda yine parmak izi ve iris biyometrik tanımlayıcıları bu özelliği yüksek oranda sağlamaktadır.



Şekil 3.5: Mobil ödeme sistemindeki biyometrik tanımlayıcı özellikleri.

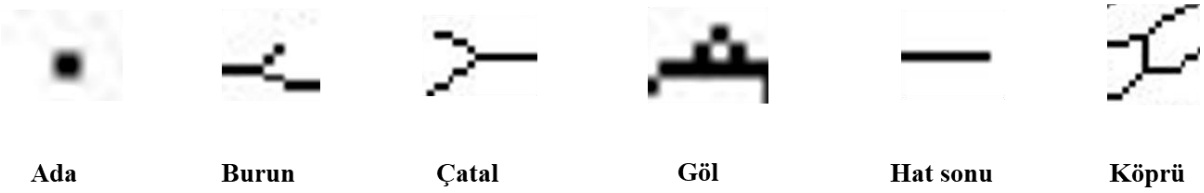
Mobil ödeme sistemlerinin biyometrik tanımlayıcı özelliklerini parmak izi ve iris tanımlayıcıları yüksek oranda sağlamaktadır. Biyometrik tanımlayıcı özelliklerinin tümünü ele aldığımızda parmak izi tanımlayıcısının hiç düşük oranda sağladığı bir özellik bulunmamaktadır. Sonuç olarak, her iki durumun kesişimi parmak izi biyometrik tanımlayıcısının mobil ödeme sistemleri için uygun olduğunu göstermektedir.

3.3.1. PARMAK İZİ VE ÖZELLİKLERİ

Parmak izi kişinin parmak ucunu bir yüzeye değdirdiğinde o kişiye özel çizgilerin oluşturduğu desendir. Parmak izi genelde birbirine paralel olan hat (ridge) ve çukurlardan oluşmaktadır. Parmak izini kişiye özel yapan orta noktalarda oluşturduğu desenlerdir. Bu desenler bir yöne doğru eğimli yapıdaysa ilmek (loop), yuvarlak halkalar şeklinde görünüyorsa halka (whorl), parmak izindeki yapının üçgen şeklini oluşturuyorsa üçgen (delta), deniz dalgasının yapmış olduğu görünüme benziyorsa kaş kemeri (arches) olarak adlandırılmaktadırlar.

Parmak izindeki hatların oluşturduğu karakteristik noktalara özellikli noktalar veya nitem (minutiae) denir. Parmak izine genel olarak baktığımızda birbirine benzer bir çizgi kümesi

olarak görünse de detayda çok farklı yapılardan oluşmaktadır. Bir parmak izinde sıklıkla görülen özellikli noktalar Şekil 3.6'da verilmiştir. Parmak izindeki özellikler ada veya nokta (island), burun (supur), çatal (bifurcation), göl (lake), hat sonu (ridge), köprü (crossover) yapılarıdır. Bu yapılardan çatal ve hat sonu özellikleri parmak izinde çok sayıda görülürken diğer özellikler bu iki özelliğin kombinasyonları olarak görülmektedir.

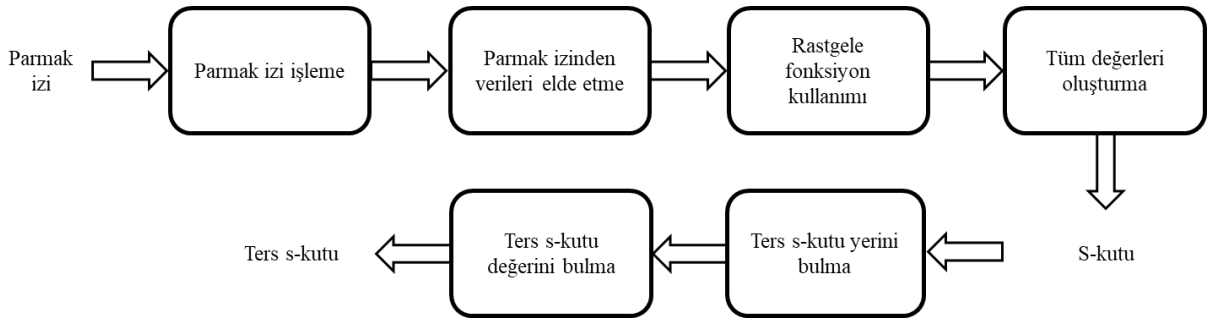


Şekil 3.6: Parmak izi ayrıntıları.

Ada parmak izinde görülen en küçük özelliktir. Burun parmak izindeki hattan bir çıkıntının oluşmasıdır. Çatal bir hattın en az iki veya daha fazla hatta dallanması durumudur. Göl bir hattan ayrılırken tekrar aynı hatta geri dönen ve küçük boşluk oluşturan yapılardır. Hat sonu parmak izinde aniden sonlanan noktaları göstermektedir. Köprü iki hat arasında yeni bir hat oluşmuş ise bu hattın oluşturduğu yapıdır.

3.4. ÖNERİLEN ETKİN BİYOMETRİK S-KUTU ALGORİTMASI

Bu tez çalışmasında, şifreleme algoritmasını güvenilirliği kişinin parmak izi ile oluşturulan biyometrik 8x8 s-kutu ve ters s-kutu oluşturma algoritması kullanılarak arttırılmıştır. Önerilen algoritmanın blok diyagramı Şekil 3.7'de gösterilen s-kutu ve ters s-kutu oluşturma olmak üzere iki ana fonksiyondan oluşmaktadır. S-kutu oluşturma dört ana aşamadan oluşmaktadır. Ters s-kutu oluşturma s-kutu oluşturma adımlarına ek olarak 2 ana aşamadan oluşmaktadır.



Şekil 3.7: Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasının blok diyagramı.

Tez kapsamında önerilen etkin biyometrik 8x8 s-kutu ve ters s-kutu oluşturma algoritması Algoritma 1'de sunulmuştur. Algoritma aşağıda yer alan 6 aşamadan oluşmaktadır.

Parmak izi işleme aşaması: Mobil cihazın parmak izi okuyucusundan veri (*F*) elde edilir. Parmak izi ikili formata (*B*) çevirilir. Parmak izinin etrafındaki gereksiz boşluklardan kurtulmak için *B* ölçeklendirilir. Ölçeklenmiş parmak izinin hatları bwmorph fonksiyonu yardımıyla elde edilir. Parmak izinin hatları inceltilerek parmak izi işleme aşaması sonlandırılır.

Parmak izinden verileri elde etme aşaması: Parmak izinde yer alan hat sonu ve/veya çatallanma özellikleri bulunur. Parmak izinde her pikselin etrafında bir birim kare oluşturulacak şekilde tüm pikseller taranır. Ana piksel ile bağlantılı olan her piksel için sayaç değeri bir arttırılır. Bu şekilde tüm pikseller taranır ve elde edilen sayaç değerleri ilgili matrise yazılır. Matriste çatallanma olan yerleri tespit etmek için değerin 3'ten büyük olduğu hücrelerin bulunduğu yerin koordinatları *B* matrisine yazılır. Matriste hat sonu olan yerleri tespit etmek için değerin 2'ye eşit olduğu hücrelerin bulunduğu yerin koordinatları *R* matrisine yazılır. Parmak izi özelliklerinden hangisi kullanılıyor ise o özelliğin matrisinde yer alan koordinat bilgileri xor işlemine tabi tutulur. Bu işlem sonucu elde edilen sonuç *result* olarak kaydedilir. *Result* matrisinde tüm elemanlar taranır. Eğer aynı değer ikinci kez tekrar ediyor ise ikinci eleman matristen silinir.

Rastgele fonksiyon kullanımı aşaması: Parmak izinden elde edilen verilerin 0-255 arasında hangileri elde edilmediyse bu değerler bir matriste saklanır. S-kutunun boşta kalan indisleri bir matriste saklanır. Rastgele fonksiyonu ile değer indis eşleşmesi yapılır.

Değerleri oluşturma aşaması: Parmak izinden elde edilen değerler sırası ile *S* değişkenine kaydedilir. Geri kalan değerler rastgele fonksiyonun sonucuna göre *S* değişkenine kaydedilir. Tüm değerlerin yazılması ile s-kutu elde edilir.

Ters s-kutu yerini bulma aşaması: S-kutusunda tüm elemanlar onaltı tabanlı sayı sistemi olarak saklanmaktadır. Elde edilen s-kutunun ilk elemanı okunur. İlk elemanın en düşük değerli biti ters s-kutunun sütun bilgisini, en yüksek değerli biti ters s-kutunun satır bilgisi bulunur. Ters s-kutuda her yeni değerin yazılacağı satır ve sütun ikilisi bu şekilde bulunmaktadır.

Ters s-kutu değerini bulma aşaması: S-kutudan değer okunurken hangi satır ve sütundan değer okunduysa bu bilgiler değişkenlerde saklanmaktadır. Okunan değerin bulunduğu satır bilgisi en yüksek değerli biti, sütun bilgisi en düşük değerli biti olarak elde edilir. Elde edilen değer ters s-kutuda ilgili hücreye yazılır.

Algoritma 1: Önerilen Etkin Biyometrik S-Kutu ve Ters S-Kutu Oluşturma Algoritması

Girdi: Parmak izi *F* ve parmak izi özelliği *ozellik*

Çıktı: S-kutu *S* ve ters s-kutu *IS*

```
Parmak izi F'yi oku ve ikili formata B'ye çevir
B'yi ölçekle
B1 = bwmorph(B) fonksiyonu çağır
T = bwmorph(B, "Thinned")
for satir = 1 to boyut_T do
    for sutun = 1 to boyut_T do
        if komşu pikselde değer var then
            piksel_sayac = piksel_sayac + 1
        end if
        matrix(satir, sutun) = piksel_sayac
    end for
end for
if ozellik == 1 then
    B[satir, sutun] = find (matrix() > 3)
    for i = 1 to satir_size do
        result = xor (satir, sutun)
    end for
    for k = 1 to result_size do
```

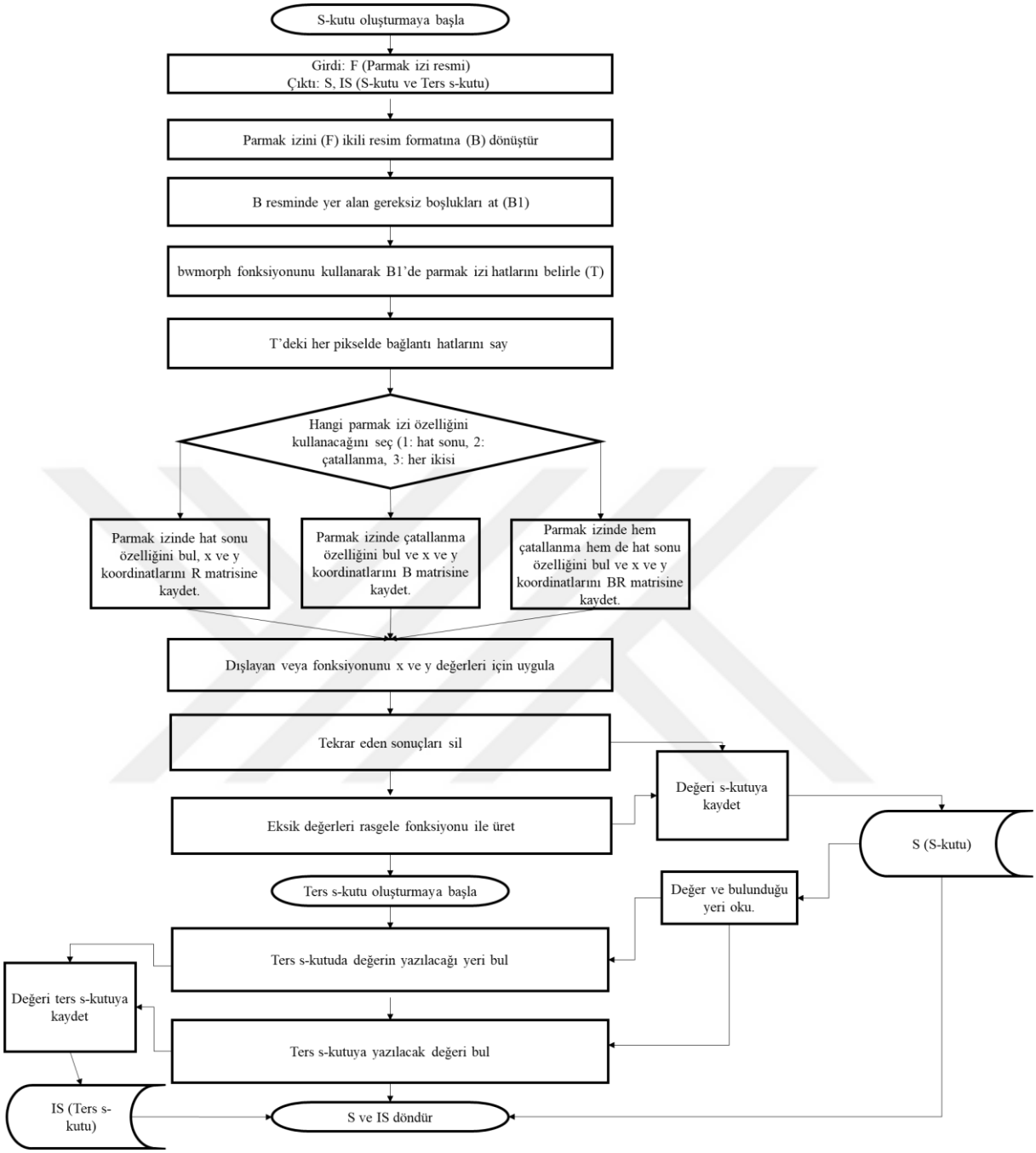
Algoritma 1 (devam)

```
19:         if result(k) == result(k + 1) then
20:             delete(result(k + 1))
21:         end if
22:     end for
23:     eksik_deger = find_eksik_deger(result)
24:     S = ekle(result, random(eksik_deger)
25: end if
26: if ozellik == 2 then
27:     R[satir, sutun] = find (matrix() = 2)
28:     for i = 1 to satir_size do
29:         result = xor (satir, sutun)
30:     end for
31:     for k = 1 to result_size do
32:         if result(k) == result(k + 1) then
33:             delete(result(k + 1))
34:         end if
35:     end for
36:     eksik_deger = find_eksik_deger(result)
37:     S = ekle(result, random(eksik_deger)
38: end if
39: if ozellik == 3 then
40:     B[satir, sutun] = find (matrix() > 3)
41:     R[satir, sutun] = find (matrix() = 2)
42:     combine B and R to BR
43:     for i = 1 to satir_size do
44:         result = xor (satir, sutun)
45:     end for
46:     for k = 1 to result_size do
47:         if result(k) == result(k + 1) then
48:             delete(result(k + 1))
49:         end if
50:     end for
51:     eksik_deger = find_eksik_deger(result)
52:     S = ekle(result, random(eksik_deger)
```

Algoritma 1 (devam)

```
53: end if
54: for satir 0 to 15 do
55:     for sutun 0 to 15 do
56:         assign satir and sutun to value
57:         assign first digit of S(satir, sutun) to yeni_satir
58:         assign second digit of S(satir, sutun) to yeni_column
59:         set value to IS(yeni_satir, yeni_column)
60      end for
61: end for
62: return S, IS
```

Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasını daha iyi anlatmak için işlevsel akış diyagramı Şekil 3.8.'de verilmiştir.



Şekil 3.8: Önerilen parmak izi s-kutu algoritmasının işlevsel akış diyagramı.

3.4.1. PARMAK İZİ İLE S-KUTU OLUŞTURMA

Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasının s-kutu oluşturma kısmı aşağıda yer alan 10 adımdan oluşmaktadır.

Adım 1: Mobil cihazın parmak izi okuyucusu ile Şekil 3.9'daki parmak izi görüntüsü elde edilir.



Şekil 3.9: Parmak izi görüntüsü.

Adım 2: Parmak izi görüntüsünün ikili görüntüsü elde edilip etrafındaki gereksiz boşluklardan kurtulmak için yeniden ölçeklendirilir. Parmak izinin ölçeklendirme sonrası elde edilen görüntüsü Şekil 3.10'da verilmiştir.



Şekil 3.10: Ölçeklendirilmiş ikili formattaki parmak izi görüntüsü.

Adım 3: Parmak izinde iki kısım bulunmaktadır: çizgileri temsil eden hat ve çukurları temsil eden vadi. Algoritmada parmak izinin hatları üzerinden işlem yapıldığından parmak izinin hatlarını elde etmek için "bwmorph" fonksiyonu kullanılır. Elde edilen hatların daha ince görüntülenmesi için fonksiyonun "Thinned" özelliği kullanılır. Hatları inceltilmiş parmak izi görüntüsü Şekil 3.11'de verilmiştir.



Şekil 3.11: Hatları inceltilmiş parmak izi görüntüsü.

Adım 4: İnceltilmiş parmak izi görüntüsündeki her piksel etrafında belirli boyutta kare oluşturacak şekilde taranır. Seçilen pikselin etrafındaki pikseller ile bağlantısı kontrol edilir. Etrafındaki her bağlantı için sayı bir arttırılır. Tüm parmak izi görüntüsü bu şekilde kontrol edilerek bağlantı sayıların yer aldığı bir matris oluşturulur.

Adım 5: Parmak izinin hat sonu özelliği kullanılacak ise "*ozellik*" değişkeni 1, çatallanma özelliği kullanılacak ise "*ozellik*" değişkeni 2, hem hat sonu hem de çatallanma özelliği kullanılacak ise "*ozellik*" değişkeni 3 olarak belirlenir.

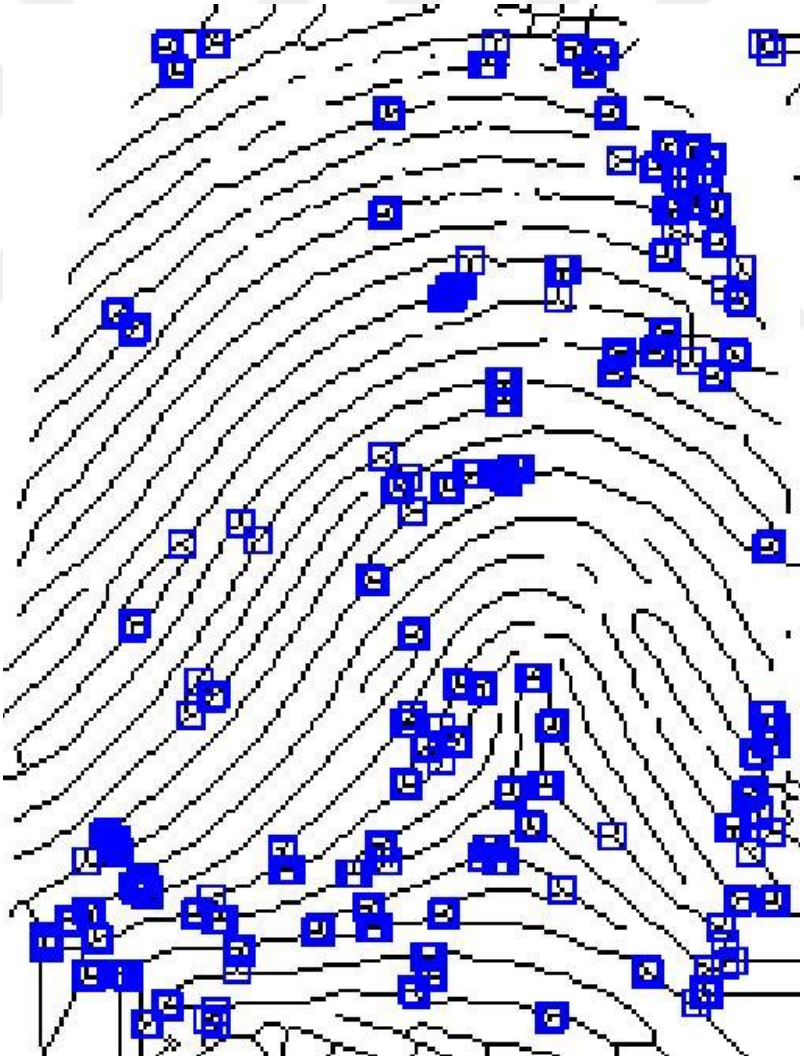
Adım 6: Eğer "*ozellik*" değişkeni 1 ise bağlantı matrisinde 2'ye eşit olan hücreler belirlenir. Belirlenen hücrelerin x-y koordinatları "*R*" matrisine yazılır. Koordinat bilgileri parmak izi görüntüsünün ilk pikseli (0,0) noktası olarak düşünülerek belirlenmiştir. Eğer "*ozellik*" değişkeni 2 ise bağlantı matrisinde 3'ten büyük olan hücreler belirlenir. Belirlenen hücrelerin x-y koordinatları "*B*" matrisine yazılır. Parmak izi görüntüsünün çatallanma özelliğine ait koordinat bilgileri Tablo 3.5'te verilmiştir. Eğer "*ozellik*" değişkeni 3 ise hem bağlantı matrisinde 2'ye eşit olan hücreler belirlenip hücrelerin x-y koordinatları "*R*" matrisine hem de bağlantı matrisinde 3'ten büyük olan hücreler belirlenip hücrelerin x-y koordinatları "*B*" matrisine yazılır. Hat sonu ve çatallanma özelliklerinin x-y koordinatları "*RB*" matrisine yazılır. Parmak izinden bulunan çatallanma özellikleri Şekil 3.12'de, hat sonu özellikleri Şekil 3.13'te verilmiştir.

Tablo 3.5: Parmak izinde bulunan çatallanma özelliğinin koordinat bilgileri.

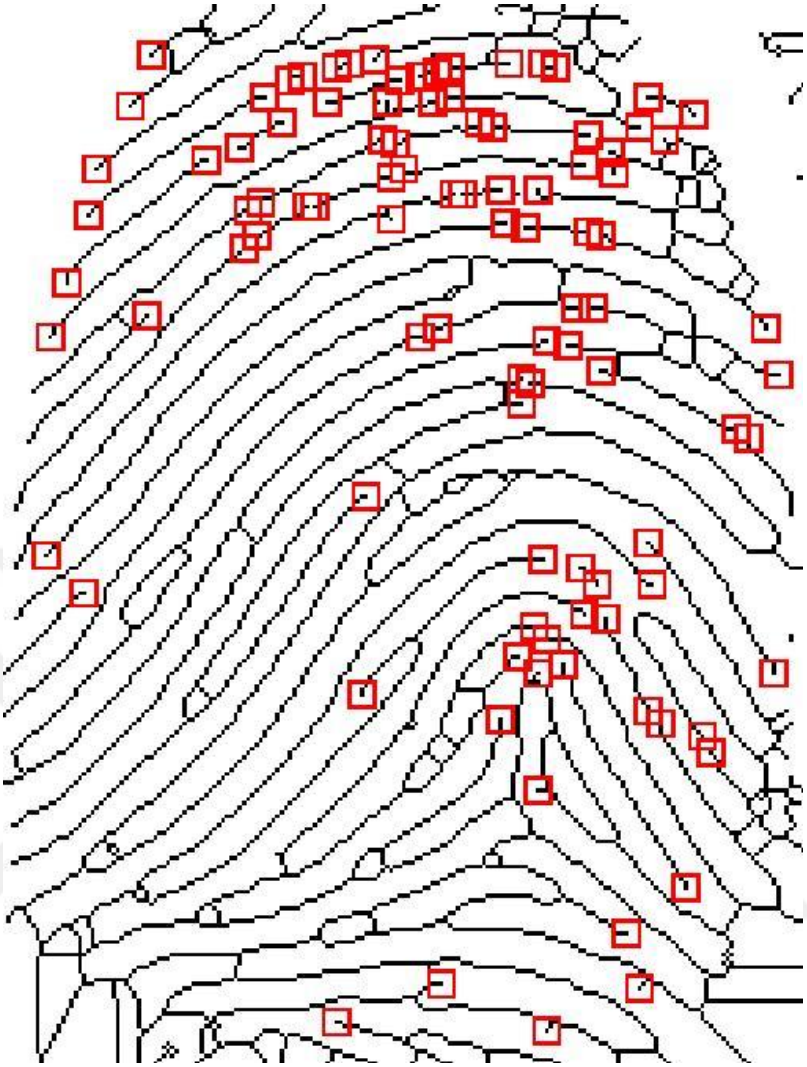
y	x	y	x	y	x
57	14	57	60	172	86
44	15	58	60	14	89
45	15	49	61	15	90
45	16	46	63	16	90
30	22	47	63	15	91
31	22	46	64	26	91
31	23	53	64	117	91
140	23	62	64	16	92
18	28	206	64	17	92
218	33	20	65	25	92
219	33	207	65	117	92
219	34	20	66	118	92
47	37	21	66	25	93
75	39	25	69	33	93
51	41	26	69	40	93
52	41	26	70	25	94
51	42	27	75	33	94
171	42	49	75	40	94
172	42	17	76	33	95
172	43	49	76	40	95
136	47	50	76	41	96
136	48	53	76	45	97
137	48	54	76	46	97
36	53	17	77	18	98
36	54	29	77	46	98
37	54	54	77	18	99
41	55	17	78	19	99
42	55	22	79	22	100
42	56	23	79	23	100
49	56	30	79	23	101

Tablo 3.5 (devam): Parmak izinde bulunan çatallanma özelliğinin koordinat bilgileri.

y	x	y	x	y	x
50	56	23	80	175	101
50	57	36	80	78	102
42	59	37	80	16	103
58	59	245	80	78	103
67	59	37	81	79	103
41	60	171	85	16	104
42	60	172	85		



Şekil 3.12: Parmak izinde çatallanma özelliğinin bulunduğu yerler.



Şekil 3.13: Parmak izinde hat sonu özelliğinin bulunduğu yerler.

Adım 7: Elde edilen koordinat bilgileri bit tabanlı Denklem (3.1)'de verildiği gibi xor işlemine tabi tutulur. Parmak izi görüntüsünün çatallanma özelliğine ait koordinat bilgilerinin xor işlemi sonucu elde edilen veriler Tablo 3.6'da verilmiştir.

$$00111001_2 \oplus 00001110_2 = 00110111_2 \quad (3.1)$$

Tablo 3.6: XOR işleminin sonucu.

y	x	$x \oplus y$	y	x	$x \oplus y$	y	x	$x \oplus y$
57	14	55	57	60	5	172	86	250
44	15	35	58	60	6	14	89	87
45	15	34	49	61	12	15	90	85
45	16	61	46	63	17	16	90	74
30	22	08	47	63	16	15	91	84
31	22	09	46	64	110	26	91	65
31	23	08	53	64	117	117	91	46
140	23	155	62	64	126	16	92	76
18	28	14	206	64	142	17	92	77
218	33	251	20	65	85	25	92	69
219	33	250	207	65	142	117	92	41
219	34	249	20	66	86	118	92	42
47	37	10	21	66	87	25	93	68
75	39	108	25	69	92	33	93	124
51	41	26	26	69	95	40	93	117
52	41	29	26	70	92	25	94	71
51	42	25	27	75	80	33	94	127
171	42	129	49	75	122	40	94	118
172	42	134	17	76	93	33	95	126
172	43	135	49	76	125	40	95	119
136	47	167	50	76	126	41	96	73
136	48	184	53	76	121	45	97	76
137	48	185	54	76	122	46	97	79
36	53	17	17	77	92	18	98	112
36	54	18	29	77	80	46	98	76
37	54	19	54	77	123	18	99	113
41	55	30	17	78	95	19	99	112
42	55	29	22	79	89	22	100	114
42	56	18	23	79	88	23	100	115
49	56	9	30	79	81	23	101	114

Tablo 3.6 (devam): XOR işleminin sonucu.

y	x	$x \oplus y$	y	x	$x \oplus y$	y	x	$x \oplus y$
50	56	10	23	80	71	175	101	202
50	57	11	36	80	116	78	102	40
42	59	17	37	80	117	16	103	119
58	59	1	245	80	165	78	103	41
67	59	120	37	81	116	79	103	40
41	60	21	171	85	254	16	104	120
42	60	22	172	85	249			

Adım 8: Elde edilen sonuçlarda tekrar eden veri olup olmadığı kontrol edilir. Tekrar eden veri varsa ilk değer bırakılır sonraki tekrarları silinir. Parmak izi görüntüsünün çatallanma özelliğine ait koordinat bilgilerinin XOR işlemi sonucu elde edilen verilerden tekrar eden değerlerin silinmiş hali Tablo 3.7'de verilmiştir.

Tablo 3.7: Tekrar eden değerlerin silinmesi.

y	x	$x \oplus y$		Sonuç
57	14	55		55
44	15	35		35
45	15	34		34
45	16	61		61
30	22	08		08
31	22	09		09
31	23	**08**	→	155
140	23	155		14
18	28	14		251
218	33	251		250
219	33	250		249
219	34	249		10
47	37	10		108
75	39	108		26

Tablo 3.7 (devam): Tekrar eden değerlerin silinmesi.

y	x	$x \oplus y$		Sonuç
51	41	26		29
52	41	29		25
51	42	25		129
171	42	129		134
172	42	134		135
172	43	135		167
136	47	167		184
136	48	184		185
137	48	185		17
36	53	17		18
36	54	18		19
37	54	19	→	30
41	55	30		11
42	55	**29**		1
42	56	**18**		120
49	56	**9**		21
50	56	**10**		22
50	57	11		
42	59	**17**		
58	59	1		
67	59	120		
41	60	21		
42	60	22		

Adım 9: Parmak izinden elde edilen değerler ile 0-255 arasında hangi değerlerin eksik olduğu belirlenir. Eksik olan değerler Tablo 3.8'de verilmiştir.

Tablo 3.8: 0-255 arası eksik olan değerler.

0	1	2	3	4	7	13	15	20	23	24	27	31	32	33	36
37	38	39	43	44	45	47	48	49	50	51	52	53	54	56	57
58	59	60	62	63	64	66	67	70	72	75	78	82	83	90	91
94	96	97	98	99	100	101	102	103	104	105	106	107	109	111	128
130	131	132	133	136	137	138	139	140	141	143	144	145	146	147	148
149	150	151	152	153	154	156	157	158	159	160	161	162	163	164	166
168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183
186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201
203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218
219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234
235	236	237	238	240	241	242	243	244	245	246	247	248	252	253	255

Adım 10: Tekrar eden değerlerin silinmesi sonucu elde edilen değerler onaltılı tabanda s-kutuya ilk hücreden başlayacak şekilde eklenir. S-kutuda geri kalan boş hücrelere bir önceki adımda belirlenen eksik değerler rastgele eklenir. S-kutuya elde edilen son değerlerin nasıl yerleştirildiği Tablo 3.9'da verilmiştir.

Tablo 3.9: S-kutuya değerlerin yerleştirilmesi.

sütun / satır	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	37	23	22	3D	08	09	9B	0E	FB	FA	F9	0A	6C	1A	1D	19
1	81	86	87	A7	B8	B9	11	12	13	1E	0B	01	78	15	16	05
2	06	0C	10	6E	75	7E	8E	8F	55	56	57	5C	5F	50	7A	5D
3	7D	79	7B	59	58	51	47	74	A5	FE	4A	54	41	2E	4C	4D
4	45	29	2A	44	7C	7F	76	77	49	4F	70	71	72	73	CA	28
5	3B	3C	40	43	42	83	68	6B	6A	4B	D2	48	BF	BE	53	27
							⋮									

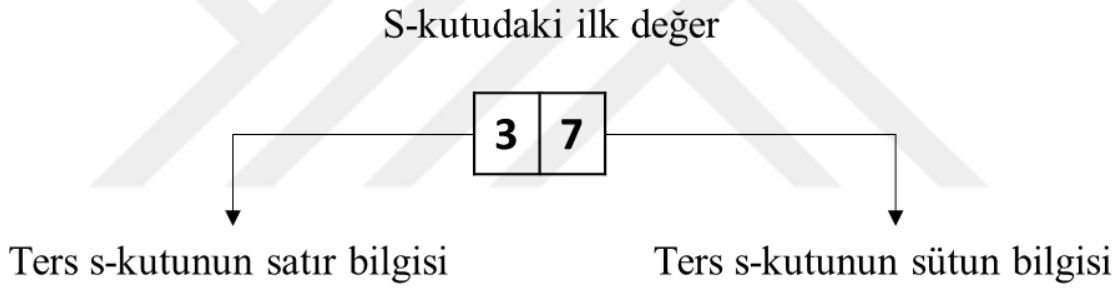
3.4.2. PARMAK İZİ İLE TERS S-KUTU OLUŞTURMA

Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasının ters s-kutu oluşturma kısmı aşağıda yer alan 6 adımdan oluşmaktadır.

Adım 1: S-kutusundan ilk hücreden başlayarak değer okunur. Tablo 3.9'da verilen s-kutunun ilk değeri 37.

Adım 2: Onaltılı sayı sisteminde okunan sayının en düşük değerli biti ters s-kutunun satır bilgisi olarak okunur. S-kutuda okunan değerden satır bilgisinin belirlenmesi Şekil 3.14'te verilmiştir.

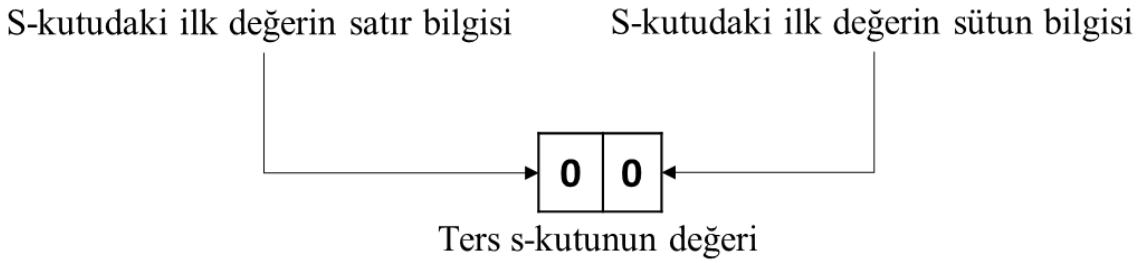
Adım 3: Onaltılı sayı sisteminde okunan sayının en yüksek değerli biti ters s-kutunun sütun bilgisi olarak okunur. S-kutuda okunan değerden sütun bilgisinin belirlenmesi Şekil 3.14'te verilmiştir.



Şekil 3.14: S-kutu değerinden ters s-kutunun satır ve sütun bilgisini bulma.

Adım 4: S-kutusundan değerin okunduğu hücrenin bulunduğu satır bilgisi okunur. Okunan satır bilgisi ters s-kutunun en düşük değerli bitini olarak yazılır. S-kutunun okunan değerinin satır bilgisinden ters s-kutunun değerinin oluşturması Şekil 3.15'te verilmiştir.

Adım 5: S-kutusundan değerin okunduğu hücrenin bulunduğu sütun bilgisi okunur. Okunan sütun bilgisi ters s-kutunun en yüksek değerli bitini olarak yazılır. S-kutunun okunan değerinin sütun bilgisinden ters s-kutunun değerinin oluşturması Şekil 3.15'te verilmiştir.



Şekil 3.15: S-kutunun satır-sütun bilgisinden ters s-kutunun değer bilgisini oluşturma.

Adım 6: Tüm s-kutudaki değerler okunana kadar Adım 1'den Adım 5'e kadar olan işlemler tekrar edilir. S-kutudan ters s-kutunun oluşturulması Şekil 3.16'da verilmiştir.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	37	23	22	3D	08	09	9B	0E	FB	FA	F9	0A	6C	1A	1D	19
1	81	86	87	A7	B8	B9	11	12	13	1E	0B	01	78	15	16	05
⋮																

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0									04	05						
1																
2			02	01												
3								00						03		
4																
⋮																

Şekil 3.16: S-kutudan ters s-kutunun oluşturulması.

3.5. GÜVENLİK PERFORMANS METRİKLERİ

Bu bölümde, önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasının değerlendirilmesi için kullanılan performans metrikleri sunulmaktadır. S-kutunun güvenilirliğini belirleyen metrikler doğrusal olmama, katı çığ etkisi, doğrusal olasılık, diferansiyel olasılık, bit bağımsızlık kriteri, bütünlüktür (Webster ve Tavares, 1986; Adams ve Tavares, 1990). S-kutunun güvenlik metriklerinin yanısıra rastgelelik ve güvenilirlik aralığı metrikleri kullanılmıştır. Algoritmanın performans metriği olarak yürütme süresi kullanılmıştır.

3.5.1 DOĞRUSAL OLMAMA

Blok şifrelemede kullanılan bir s-kutunun temel amacı düz metinden şifreli metin elde edilmesindeki değişimin doğrusal olmamasıdır. Doğrusal olmama (Nonlinearity, NL), doğrusal kriptoanalizi hafifletmek için blok şifrelerin güçlü bir bağışıklığına ve karışıklığına bağlıdır. S-kutuyu oluşturan değerlerin oluşumunun doğrusal olmamasını ölçmek için kullanılır. S-kutusunda elde edilen değerlerinin arasında tanımlı bir ilişki belirlenmemesi gerekmektedir. Eğer formüle edilebilen bir ilişki mevcut ise algoritmanın oluşturduğu s-kutu doğrusaldır ki s-kutunun en önemli özelliği şifreleme algoritmasını doğrusal olmasını önlemektedir.

Bir fonksiyonun doğrusal olmaması bu fonksiyon ile her doğrusal fonksiyon arasındaki Hamming mesafesinin minimum olması olarak tanımlanır. 8-bitlik bir ikili fonksiyonun doğrusal olmaması Denklem (3.2)'de verilen Walsh spektrum kullanılarak hesaplanır.

$$NL_f = 2^{n-1}\left(1 - 2^{-n} max_{\omega \in GF(2^n)} \left| s_{<f>}(\omega) \right| \right) \tag{3.2}$$

Fonksiyonun çevrimsel spektrumu (cyclic spectrum) Denklem (3.3) kullanılarak hesaplanır.

$$s_{<f>}(\omega) = \sum_{x \in GF(2^n)} (-1)^{f(x) \oplus x \cdot \omega} \tag{3.3}$$

Bir s-kutunun doğrusal olmaması doğrusal olasılık ile hesaplanabilir. Doğrusal olasılıkta elde edilen en yüksek değer alınır. 8-bit kullanılarak ile oluşturulan s-kutunun doğrusal olmaması s-kutunun doğrusal olasılığının en yüksek değerinden yararlanılarak Denklem (3.4) kullanılarak hesaplanır.

$$NL = 2^{n-1} - \max(LP) \tag{3.4}$$

Bir s-kutunun doğrusal olmama yüzdesi Denklem (3.5) kullanılarak hesaplanmaktadır.

$$NL\ Yüzdesi = \frac{NL}{2^{n-1} - 2^{\frac{n}{2}-1}} \tag{3.5}$$

3.5.2. KATI ÇIĞ KRİTERİ

Güvenli bir s-kutu tasarımı için ikinci önemli kriter katı çığ kriteridir (Strict Avalanche Criterion, SAC). Genelde bir şifreleme algoritmasının, girişinde yapılan bir değişimin, çıkışa

etkisidir. Örneğin şifreleme algoritmasının aldığı değerlerde bir bitin değiştirilmesi, sonuçtaki çıktıyı büyük ölçüde etkiliyorsa, bu sistemde çığ etkisinden söz edilebilir. Benzer şekilde şifreleme sistemine verilen bir girdi, sonuçta çok ciddi değişikliklere sebep oluyorsa, örneğin bir biti farklı bilginin sonucunun yarısının fazla veya az farklı olması gibi durumda şifreleme algoritması saldırıya açık kabul edilebilir.

Çığ etkisi girdi bitlerinin bir bitindeki değişikliğin çıktı bitinin yarısın etkilemesidir ve Denklem (3.6) kullanılarak hesaplanır. Bütünlük girdi bitindeki her bit her çıktı bitin bir katkısının olmasıdır. Düz metindeki birkaç bitin değişikliği şifreli metindeki bazı bitlerdeki değişikliğe sebep oluyorsa girdi-çıktı arasındaki bu değişiklik üçüncü şahıslar tarafından düz metin ile anahtarın tespit edilmesinde kullanılır.

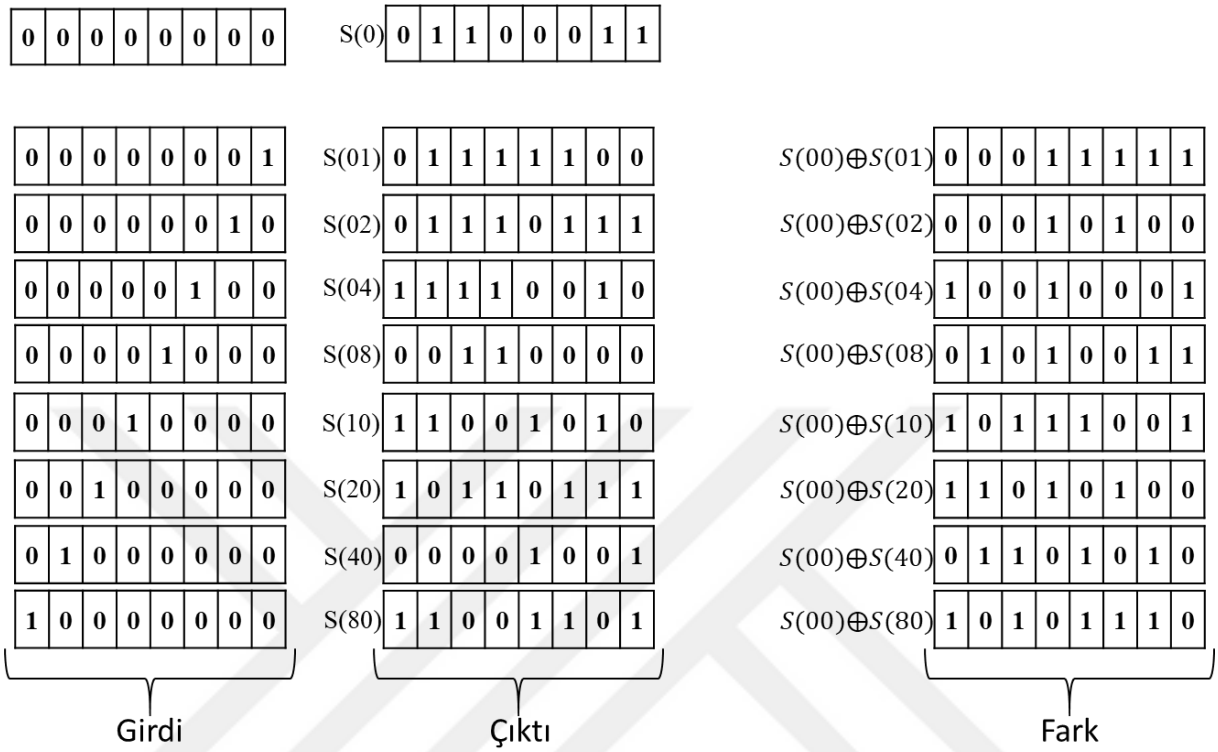
$$\text{Çığ } etkisi = \frac{değişen\ çıktı\ biti\ sayısı}{toplam\ çıktı\ biti\ sayısı} = 0.5 \tag{3.6}$$

S-kutunun karmaşıklık yeteneği katı çığ kriteri sonuçlarına göre analiz edilir. S-kutu çığ etkisi ve bütünlük kriterlerini sağlıyorsa katı çığ kriteri özelliğini de sağlamaktadır. Bu durumda katı çığ etkisi s-kutu oluşturma fonksiyonunun girdisinin m. bitinin değişmesinin fonksiyonun çıktısının n. bitinin değişme olasılığı yaklaşık olarak %50 olmasıdır ve Denklem (3.7) kullanılarak hesaplanır.

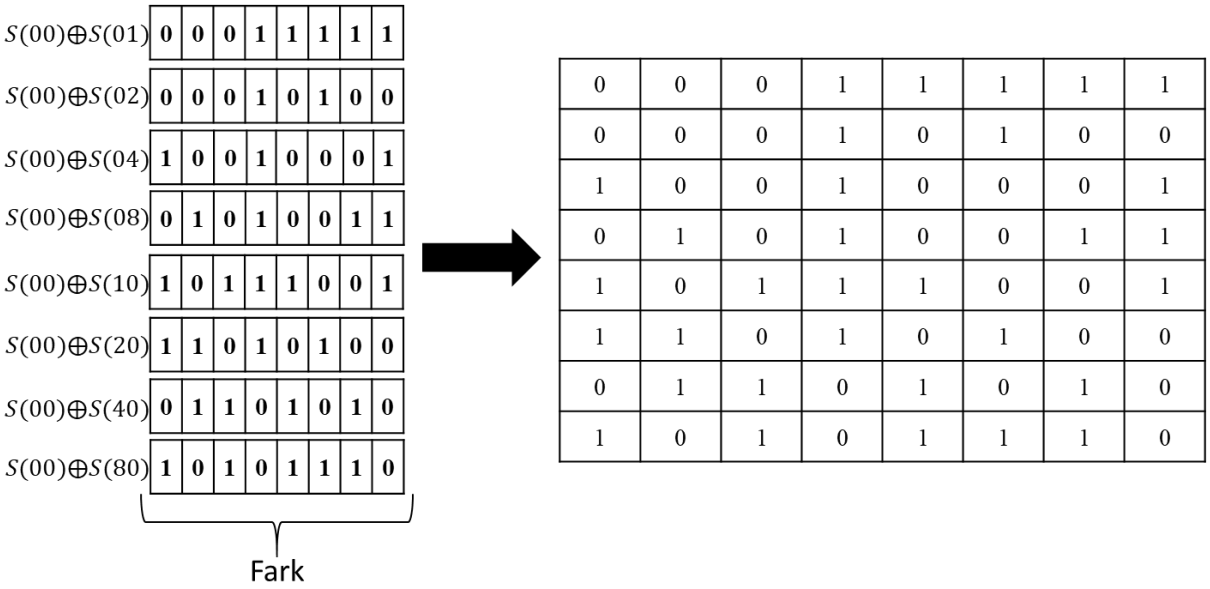
$$\frac{\omega t(a_j^{\Delta x_i})}{2^n} = \frac{1}{2} \qquad i, j \in \{0, 1, 2, \cdots, n\} \tag{3.7}$$

S-kutunun girdi bitindeki bir bit değişikliği çıktı bitlerinin yarısını değiştirmesi katı çığ kriterini göstermektedir. S-kutunun ikili sayı sisteminde girdisi verilir ve s-kutu çıktısı hesaplanır. İkili sayı sisteminde verilen girdinin her biti tek tek değiştirilir. Her bit değişikliği sonucu girdi olarak kullanılarak s-kutu çıktısı hesaplanır. Bit değişikliği sonrası elde edilen çıktı ile ilk durumdaki çıktı arasındaki fark hesaplanır. Katı çığ kriterinin hesaplanmasında farkın AES s-kutusuna göre ilk döngüde nasıl elde edildiği Şekil 3.17'de gösterilmiştir. Fark hangi çıktı bitinde ise o bitin sayacı bir arttırılır. Bu şekilde her girdinin değişikliğinin etkilediği çıktı bitini gösteren 8x8 boyutunda fark matrisi oluşturulur. Şekil 3.17'de verilen bilgiler doğrultusunda oluşan matris Şekil 3.18'de verilmiştir. Tüm s-kutu girdileri için fark hesaplamaları yapılıp matris güncellenir. Fark matrisi tamamlandığında Denklem (3.7) verildiği gibi 2^n sayısına

bölünür. En son oluşan 8x8 boyutundaki matrisin ortalaması s-kutunun katı çığ kriteri değerini göstermektedir.



Şekil 3.17: Katı çığ kriteri metriğinin işleyişine örnek.



0	0	0	1	1	1	1	1
0	0	0	1	0	1	0	0
1	0	0	1	0	0	0	1
0	1	0	1	0	0	1	1
1	0	1	1	1	0	0	1
1	1	0	1	0	1	0	0
0	1	1	0	1	0	1	0
1	0	1	0	1	1	1	0

Şekil 3.18: Fark işleminin sonucunun fark matrisine işlenmesine örnek.

3.5.3. DOĞRUSAL OLASILIK

Bir s-kutunun doğrusal saldırılara karşı dayanıklılığı test etmek için s-kutunun doğrusal olasılığı (Lineer Probability, LP) ve doğrusal yaklaşım tablo (Lineer Approximation Table, LAT) değeri hesaplanmalıdır. Doğrusal yaklaşım tablosunun en yüksek değerinin en düşük olması ile s-kutunun doğrusal saldırılara karşı dayanıklı olduğunu göstermektedir. N bit girişli ve n bit çıkışlı bir s-kutusunun 2^n x 2^n boyutlarında LAT oluşmaktadır. LAT değerleri Denklem (3.8) kullanılarak her a, b, Γ_a, $\Gamma_b \in GF(2^n)$ için hesaplanmaktadır.

$$LAT(\Gamma_a, \Gamma_b) = \#\{x \in GF(2^n): \Gamma_a \cdot x = \Gamma_b \cdot S(x)\} - 2^{n-1} \tag{3.8}$$

Doğrusal olasılık Denklem (3.9) kullanılarak hesaplanmaktadır. Denklem (3.9) yer alan Γ_a girdi maskesi, Γ_b çıktı maskesi, "." nokta çarpımını, "#" koşulu sağlayan x değerlerinin sayısını vermektedir.

$$LP = max_{\Gamma_a, \Gamma_b \neq 0} \left| \frac{\#\{x \in GF(2^n): \Gamma_a \cdot x = \Gamma_b \cdot S(x)\}}{2^n} - \frac{1}{2} \right| \tag{3.9}$$

Bir s-kutunun doğrusal olasılığının hesaplanması için öncelikler doğrusal yaklaşım tablosu oluşturulur. Hesaplamanın yapıldığı 4x4 boyutundaki s-kutu Tablo 3.10'da verilmiştir.

Tablo 3.10: 4x4 s-kutu.

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(x)	B	5	2	0	A	7	4	D	1	F	8	E	6	9	C	3

Doğrusal yaklaşım tablosunun oluşturmak için Γ_a girdi maskesi, Γ_b çıktı maskesi belirlenir. Girdi maskesi B_{16}, çıktı maskesi 2_{16} belirlendiğinde ikili sayı sisteminde bir olan bitler belirlenerek denklemin elde edilmesi Şekil 3.19'da verilmiştir.

Girdi maskesi	1	0	1	1
Çıktı maskesi	0	0	1	0

$$X_1 \oplus X_3 \oplus X_4 \oplus Y_2 = 0$$

Şekil 3.19: Denklemin elde edilmesi.

Elde edilen denklem tüm s-kutunun girdi-çıktı eşlemesine uygulanır. Denklemin sonucu Tablo 3.11'de verilmiştir. Belirlenen girdi maskesi ve çıktı maskesine göre s-kutunun girdi-çıktı eşlemesinin kaçında 0 değeri elde edilmiş sayılır. Tablo 3.11'deki sonuca göre 9 tane 0 değeri, 7 tane 1 değeri elde edilmiştir. 0 değerlerinin, olasılığı hesaplanıp olasılıklar matrisine ve 1/2 değerine göre sapması hesaplanıp sapmalar matrisine yazılır. 0 değerlerinin olasılığı 9/16, olasılığın 1/2'ye göre sapması 9/16 - 1/2 = 1/2 olarak hesaplanır.

Tablo 3.11: Denklemin tüm s-kutunun girdi-çıktı eşlemesine uygulanması.

X1	**X2**	**X3**	**X4**	**Y1**	**Y2**	**Y3**	**Y4**	$X_1 \oplus X_3 \oplus X_4 \oplus Y_2$
0	0	0	0	1	0	1	1	0
0	0	0	1	0	1	0	1	0
0	0	1	0	0	0	1	0	1
0	0	1	1	0	0	0	0	0
0	1	0	0	1	0	1	0	0
0	1	0	1	0	1	1	1	0
0	1	1	0	0	1	0	0	0
0	1	1	1	1	1	0	1	1
1	0	0	0	0	0	0	1	1
1	0	0	1	1	1	1	1	1
1	0	1	0	1	0	0	0	0
1	0	1	1	1	1	1	0	0
1	1	0	0	0	1	1	0	1
1	1	0	1	1	0	0	1	0
1	1	1	0	1	1	0	0	1
1	1	1	1	0	0	1	1	1

Olasılık hesabında tüm değerlerin mutlak değeri matrise yazılır. Tüm girdi maskesi ve çıktı maskesi için yapılan işlemler tekrarlanır. En son elde edilen matristen en yüksek değer LP değeridir. LP değerinin iyi olması için en yüksek değerin en küçük olması gerekmektedir.

3.5.4. DİFERANSİYEL OLASILIK

Bir s-kutunun diferansiyel saldırılara karşı dayanıklılığı test etmek için s-kutunun diferansiyel olasılığı (Differential Probability, DP) ve diferansiyel dağılımı (Differential Uniformity, DU) hesaplanmalıdır. Doğrusal olmayan dönüşüm s-kutusunun ideal olarak farklı bir bütünlüğe sahip olması gerekir. Bir giriş farklılığı Δx, bir çıkış diferansiyeli Δy ile eşlenmelidir, böylece her x için tekdüze bir haritalama olasılığı sağlanır. N bit girişli ve n bit çıkışlı bir s-kutusunun 2^n x 2^n boyutlarında XOR tablosu oluşmaktadır. XOR değerleri Denklem (3.10) kullanılarak her Δx, Δy ∈ GF(2^n) için hesaplanmaktadır.

$$DU = max_{\Delta x \neq 0, \Delta y}(\#\{x \in GF(2^n) : S(x) \oplus S(x \oplus \Delta x) = \Delta y\}) \tag{3.10}$$

Diferansiyel olasılık, girdi ve ona karşılık gelen çıktının aynı diferansiyel sahip çiftlerin bulunmasıdır. Diferansiyel çiftleri olan Δx, Δy için Denklem (3.11) kullanılarak hesaplanır.

$$DP = max_{\Delta x \neq 0, \Delta y}\left(\frac{\#\{x \in GF(2^n) : S(x) \oplus S(x \oplus \Delta x) = \Delta y\}}{2^n}\right) \tag{3.11}$$

Bir s-kutunun diferansiyel olasılığının hesaplanması için giriş farklılığı Δx belirlenir. Hesaplamanın yapıldığı 4x4 boyutundaki s-kutu Tablo 3.10'da verilmiştir. Her giriş farklılığı Δx için çıkış diferansiyeli Δy Denklem (3.10) kullanılarak hesaplanır.

Tablo 3.12: Verilen giriş farklılıkları için çıkış farklılığının hesaplanması.

x		**y**		$\Delta y = S(x) \oplus S(x \oplus \Delta x)$		
İkili sayı sistemi	**onaltılı sayı sistemi**	**İkili sayı sistemi**	**onaltılı sayı sistemi**	**Δx = 0100**	**Δx = 0111**	**Δx = 1100**
0000	0	1011	B	0001	0110	1101
0001	1	0101	5	0010	1111	0010
0010	2	0010	2	0110	1100	1111
0011	3	0000	0	1101	1010	0011
0100	4	1010	A	0001	1010	1011
0101	5	0111	7	0010	0101	1000
0110	6	0100	4	0110	0001	1100
0111	7	1101	D	1101	0110	0011
1000	8	0001	1	0111	0010	1011
1001	9	1111	F	0110	0010	1000
1010	A	1000	8	0101	0001	1100
1011	B	1110	E	1101	1000	0011
1100	C	0110	6	0111	1000	1101
1101	D	1001	9	0110	0001	1100
1110	E	1101	C	0101	0010	1111
1111	F	0011	3	1101	0010	0011

Giriş farklılığı Δx=0100, Δx=0111, Δx=1100 için çıkış diferansiyeli Δy hesaplamaları Tablo 3.12'de verilmiştir. Giriş farklılığı Δx=0100 için 16 olası değer arasından 2 adet Δy=0001, 2 adet Δy=0010, 2 adet Δy=0101, 4 adet Δy=0110, 2 adet Δy=0111, 4 adet Δy=1101 değeri elde edilmiştir. Giriş farklılığı Δx=0111 için 16 olası değer arasından 3 adet Δy=0001, 4 adet Δy=0010, 1 adet Δy=0101, 2 adet Δy=0110, 2 adet Δy=1000, 2 adet Δy=1010, 1 adet Δy=1100, 1 adet Δy=1111 değeri elde edilmiştir. Giriş farklılığı Δx=1100 için 16 olası değer arasından 1 adet Δy=0010, 4 adet Δy=0011, 2 adet Δy=1000, 2 adet Δy=1011, 3 adet Δy=1100, 2 adet Δy=1101, 2 adet Δy=1111 değeri elde edilmiştir.

n girdi bitli bir s-kutunun XOR dağılım tablosu $2^n x 2^n$ boyutunda olacaktır. 4x4 boyutlu s-kutumuzun her girdi-çıktı fark çiftleri 16x16 boyutunda XOR dağılım tablosuna işlenir. Hesaplanan girdi-çıktı fark çiftlerinin XOR dağılım tablosuna işlenmiş hali Tablo 3.13'te verilmiştir.

Tablo 3.13: Elde edilen giriş-çıkış farklarının XOR dağılım tablosuna işlenmesi.

Δx \ Δy	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0																
1																
2																
3																
4	0	2	2	0	0	2	4	2	0	0	0	0	0	4	0	0
5																
6																
7	0	3	4	0	0	1	2	0	2	0	2	0	1	0	0	1
8																
9																
A																
B																
C	0	0	1	4	0	0	0	0	2	0	0	2	3	2	0	2
D																
E																
F																

Giriş farklılığı Δx=0100 için çıktının 0001 olma olasılığı 2/16, 0010 olma olasılığı 2/16, 0101 olma olasılığı 2/16, 0110 olma olasılığı 4/16, 0111 olma olasılığı 2/16, 1101 olma olasılığı 4/16. Giriş farklılığı Δx=0111 için çıktının 0001 olma olasılığı 3/16, 0010 olma olasılığı 4/16, 0101 olma olasılığı 1/16, 0110 olma olasılığı 2/16, 1000 olma olasılığı 2/16, 1010 olma olasılığı 2/16, 1100 olma olasılığı 1/16, 1111 olma olasılığı 1/16. Giriş farklılığı Δx=1100 için çıktının 0010 olma olasılığı 1/16, 0011 olma olasılığı 4/16, 1000 olma olasılığı 2/16, 1011 olma olasılığı 2/16, 1100 olma olasılığı 3/16, 1101 olma olasılığı 2/16, 1111 olma olasılığı 2/16. En iyi s-kutu her giriş farkının elde ettiği çıkış farkı 1 defa görülmesi ile elde edilir. Yani, giriş farkı Δx, çıkış

farkı Δy çiftinin görülme olasılığının 1/16 olmasıdır. Bu durumda XOR dağılım tablosu sadece 1 değeri ile oluşmaktadır.

Tüm çıktı farkları hesaplandıktan sonra elde edilen XOR dağılım tablosunun en yüksek değeri diferansiyel dağılımı, en yüksek değerin 2^n sayısına bölümü diferansiyel olasılığı gösterir.

3.5.5. BİT BAĞIMSIZLIK KRİTERİ

Bit bağımsızlık kriteri (Bit Independence Criterion, BIC) s-kutudaki girdi bitlerinden birindeki değişiklik girdiye karşılık gelen çıktı bitindekindeki değişikliklerin birbirinden bağımsız olmasıdır. Girdi bitindeki a. bitin değişmesi çıktı bitindeki b. ve c. bitlerinin değişiminin birbirinden bağımsız olmasıdır. 8 x 8 s-kutunun f_1, f_2, …, f_8 ikili fonksiyonları (boolean function) olsun. Eğer $F_i = f_j \oplus f_k$ herhangi bir j ve k değeri (j, k ϵ {1, 2, …, 8} ve j ≠ k) için doğrusal değilse ve sert çığ etkisi değerine yakın ise herhangi bir tek giriş biti ters çevrildiğinde, her çıkış çifti çiftinin olabildiğince sıfıra yakın bir korelasyona sahip olacağını garanti edebilir. Bu, s-kutusunun çıkış biti bağımsızlık ölçütü gereksinimini karşıladığı anlamına gelir.

Bit bağımsızlığı kriterinden doğrusal olmama (BIC-NL) ve sert çığ kriteri (BIC-SAC) şeklinde iki hesaplama yapılmaktadır. Sert çığ etkisi için bit bağımsızlık kriteri Denklem (3.12) kullanılarak elde edilen matrisin ortalamasıdır. Denklem (3.12) yer alan x ve w n bit uzunluğundaki girdilerdir ve sadece bir bit fark göstermektedir.

$$BIC - SAC = \sum_{x=0}^{2^n-1} \left(S_i(x) \oplus S_j(w) - S_i(x) \oplus S_j(x)\right) \quad i, j \in \{1, 2, \cdots, n\}, i \neq j \qquad (3.12)$$

S-kutunun BIC-SAC değerinin hesaplamak için öncelikle n bit uzunluğunda iki girdi belirleniyor. Belirlenen girdiler arasındaki fark bir bit olacak şekilde belirleniyor. Örneğin; 4 bit uzunluğunda x ve w girdilerinin en düşük değerli bitindeki değişiklik ile x=0000 ve w=0001 girdi olarak belirlenir. Girdi değerinde meydana gelen bu değişikliğin çıktı değerindeki iki bit arasındaki değişikliğinin birbiri ile olan ilişkisi incelemektedir.

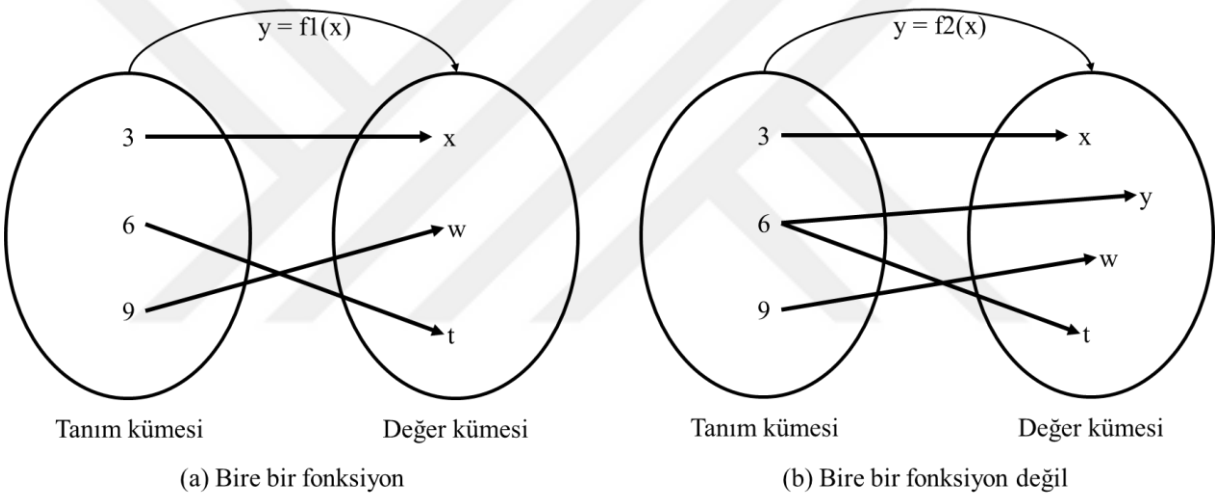
Doğrusal olmama için bit bağımsızlığı kriterinden n bit uzunluklu çıktının b. ve c. bitindeki değişikliğin Denklem (3.13) yardımıyla elde edilen matrisin ortalamasıdır.

$$BIC - NL = y_b \oplus y_c \quad b, c \in \{1, 2, \cdots, n\} \qquad (3.13)$$

S-kutunun BIC-NL değerini hesaplamak için öncelikle n bit uzunluğunda girdiye göre elde edilen çıktı değerinin bitleri arasındaki farklılıkların hesaplanıp matrise kaydedilir. Matrisin ortalaması o s-kutunun BIC-NL değerini vermektedir.

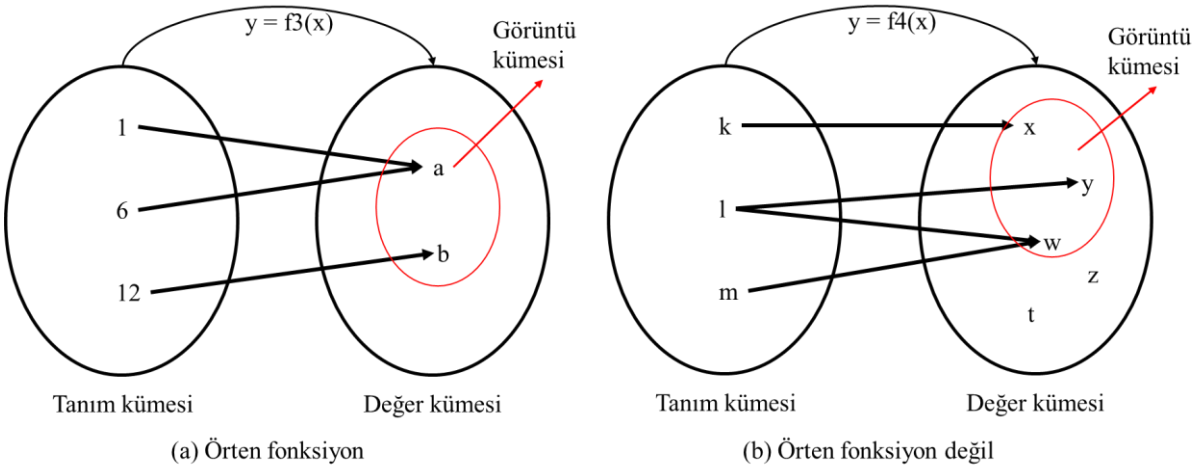
3.5.6. BÜTÜNLÜK

Bir s-kutunun bütün olması o s-kutunun tanımlı olduğu fonksiyonun birebir ve örten olmasını sağlamaktır. Tanım kümesindeki her farklı elemanın, görüntüsü de farklı ise bu tip fonksiyona bire bir (1:1) fonksiyon denir. Başka bir deyişle görüntüsünün yalnız ve yalnız tek bir karşılığı bulunmaktadır. Şekil 3.20'de bire bir fonksiyona ve bire bir olmayan fonksiyona örnek verilmiştir.



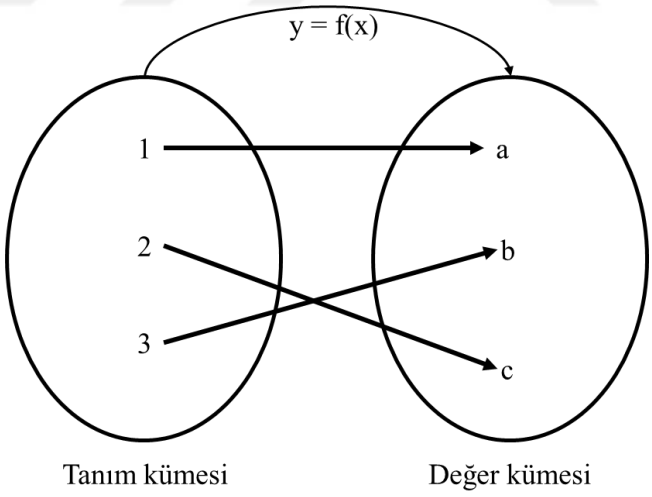
Şekil 3.20: Bire bir fonksiyon.

Tanım kümesindeki her elamanın değer kümesinde bir veya birden fazla karşılığı var ve değer kümesinde eşlenmeyen eleman yok ise bu fonksiyona örten fonksiyon denir. Değer kümesinde boşta eleman kalmıyorsa yani görüntü kümesi değer kümesine eşit olan fonksiyona örten fonksiyon denir. Şekil 3.21'de örten fonksiyona ve örten olmayan fonksiyona örnek verilmiştir.



Şekil 3.21: Örten fonksiyon.

f : A → B fonksiyonu hem bire bir hem de örten fonksiyon ise bire bir örten fonksiyon denir. Birebir örten fonksiyon; tanım kümesindeki her elemanın görüntü kümesinde tek ve tek bir karşılığı varsa fonksiyon bire bir örtendir. f : A→ B fonksiyonunun bire bir örten olabilmesi için tanım ve değer kümesinin eleman sayısı eşit (s(A) = s(B)) olmalıdır. Şekil 3.22'de bire bir örten fonksiyona örnek verilmiştir.



Şekil 3.22: Bire bir ve örten fonksiyon.

Tüm bu özelliklerin sonucunda, f : A → B fonksiyonunda farklı elemanların görüntüleri de farklı ve f(A) = B olduğunda f fonksiyon bire bir örten fonksiyondur.

3.5.7. RASTGELELİK

Rastgelelik s-kutu oluşturan algoritmanın birbirinden bağımsız rastgele sayılar üretmesini ölçmektedir. S-kutuda yer alan her değerin oluşması arasında bir korelasyon olmaması gerekmektedir. Eğer s-kutuda yer alan değerler arasında net bir korelasyon var ise bu sistemin açığı olarak kabul edilir. Bu ilişkinin üçüncü şahıslar tarafından elde edilmesi şifreleme algoritmasının bir açığı olduğundan veri gizliliğinin sağlanmaması anlamına gelmektedir.

Bir s-kutu 0 ile 255 arasında değerler almaktadır. S-kutunun sütunlarının arasında bir fonksiyon tanımlanmaması gerekmektedir. Tablo 3.14'te verilen 4x4 boyutundaki s-kutunun birinci sütunu (S1) ile ikinci sütunu (S2) arasında "S2 = S1 – 1" şeklinde bir ilişki, s-kutunun birinci sütunu (S1) ile dördüncü sütunu (S4) arasında "S4 = S1 – 2" şeklinde bir ilişki, s-kutunun ikinci sütunu (S2) ile dördüncü sütunu (S4) arasında "S4 = S2 – 1" şeklinde bir ilişki bulunmaktadır. Bu şekilde s-kutunun sütunları arasında ilişki tahmin edilebiliyorsa birinci sütunun oluşturduktan sonra diğer sütunlar aradaki ilişkiye göre kolayca oluşturabilir.

Tablo 3.14: 4x4 s-kutu örneği.

sütun / satır	**0**	**1**	**2**	**3**
0	8	7	0	6
1	B	A	1	9
2	5	4	2	3
3	E	D	F	C

3.5.8. GÜVENİLİRLİK ARALIĞI

Gözlemlenen veriler üzerine yapılan bir istatiksel hesaplamadır. Bu hesaplamaya göre algoritmanın üretmiş olduğu s-kutularını güvenli değer aralığını %95'lik güvenilirlik seviyesi ile hesaplamaktadır. Güven aralığı Denklem (3.14) kullanılarak hesaplanmaktadır. Denklem (3.14)'te yer alan X gözlemlenen verilerin ortalaması, Z güvenilirlik seviyesine göre seçilen değer, s standart sapma ve n_g gözlem sayısını temsil etmektedir.

$$X \pm Z\left(\frac{s}{\sqrt{n_g}}\right) \tag{3.14}$$

3.5.9. YÜRÜTME SÜRESİ

Yürütme süresi algoritmanın çalışmaya başlamasında çıktı üretiminin bitimine kadar geçen sürenin hesaplanmasıdır. S-kutunun şifreleme algoritmasının en önemli parçalarından biridir ve şifreleme algoritmasında kullanılabilmesi için üretiminin algoritmanın süresini etkilememelidir. Bir s-kutu ne kadar güvenli ise bir o kadar kısa sürede üretilmesi gerekmektedir. Özellikle mobil cihazlarda kullanılacak bir s-kutunun verimli olabilmesi için şifreleme işleminin yapıldığı sürenin belirli bir eşik değerinin altında olmalıdır. Eğer s-kutu üretimi şifreleme işlemini eşik değerinin üzerine çıkarıyorsa s-kutu algoritması şifreleme algoritması için uygun değildir.

4. BULGULAR

Tez kapsamında önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ve algoritmanın etkinliğinin ölçümlerinin hesaplanması için kullanılan güvenlik performans metrikleri 64-bit Windows 10 işletim sistemi, 16 GB RAM ve Intel Core i7-7500-U (2.70 GHz - 2.90 GHz) işlemcili bir bilgisayarda çalışan MATLAB R2019b yazılımında gerçeklenmiştir. Bu bölümde, önerilen etkin biyometrik s-kutu algoritması ile elde edilen parmak izi s-kutuların güvenlik performans metriklerinin sonuçları, literatürde yer alan polinomlu, kaotik ve biyometrik s-kutuların ile güvenlik performans metrik sonuçları ve önerilen parmak izi s-kutuları ile karşılaştırması yer almaktadır.

4.1. ÖNERİLEN PARMAK İZİ S-KUTULARINA AİT BULGULAR

Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması için 11 parmak izi kullanılmıştır. Her bir parmak izinden çatallanma, hat sonu ve hem çatallanma hem de hat sonu özellikleri kullanılarak üç ayrı parmak izi s-kutusu elde edilmiştir. Bu bölümde elde edilen parmak izi s-kutuların doğrusal olmama, katı çığ kriteri, doğrusal olasılık, diferansiyel olasılık, bit bağımsızlık kriteri gibi güvenlik metriklerinin yanı sıra bütünlük, rastgelelik, güvenilirlik aralığı performansları ve algoritmanın yürütme süresi sonuçları yer almaktadır.

11 parmak izinde çatallanma, hat sonu ve hem çatallanma hem de hat sonu parmak izi özelliklerini kullanılarak oluşturulan s-kutuların katı çığ kriteri, maksimum ve minimum doğrusal olmama, doğrusal olmama yüzdesi, diferansiyel dağılım, diferansiyel olasılık, doğrusal yaklaşım tablo değeri, doğrusal olasılık, bit bağımsızlık kriteri için katı çığ kriteri, bit bağımsızlık kriteri için doğrusal olmama sonuçları Tablo 4.1'de verilmiştir.

Tablo 4.1: Önerilen parmak izi s-kutuların güvenlik metriklerinin sonuçları.

S-kutu		SAC	NL			DU	DP	LAT	LP	BIC-SAC	BIC-NL
Parmak İzi	Parmak İzi Özelliği		maks.	min.	yüzdesi (%)						
1	Çatallanma	0,4761	164	92	77	32	0,1250	36	0,1406	0,4949	101
	Hat sonu	0,5098	162	94	78	14	00547	34	0,1328	0,5019	103
	Çatallanma-Hat sonu	0,4753	166	88	73	32	0,1250	40	0,1563	0,4948	101

Tablo 4.1 (devam): Önerilen parmak izi s-kutuların güvenlik metriklerinin sonuçları.

S-kutu		SAC	NL			DU	DP	LAT	LP	BIC-SAC	BIC-NL
Parmak İzi	Parmak İzi Özelliği		maks.	min.	yüzdesi (%)						
2	Çatallanma	0,5002	162	94	78	10	0,0391	34	0,1328	0,5047	103
	Hat sonu	0,5034	168	88	73	12	0,0469	40	0,1563	0,5013	103
	Çatallanma-Hat sonu	0,4941	166	88	73	10	0,0391	40	0,1563	0,4989	102
3	Çatallanma	0,4993	162	94	78	10	0,0391	34	0,1328	0,4983	102
	Hat sonu	0,4941	172	84	70	10	0,0391	44	0,1719	0,5004	103
	Çatallanma-Hat sonu	0,4888	172	84	70	10	0,0391	44	0,1719	0,4997	102
4	Çatallanma	0,5100	164	92	77	12	0,0469	36	0,1406	0,4976	102
	Hat sonu	0,5002	170	86	72	10	0,0391	42	0,1641	0,4996	102
	Çatallanma-Hat sonu	0,4924	180	76	63	18	0,0703	52	0,2031	0,4986	102
5	Çatallanma	0,4785	170	86	72	14	0,0547	42	0,1641	0,4974	102
	Hat sonu	0,5059	162	92	77	12	0,0469	36	0,1406	0,4987	102
	Çatallanma-Hat sonu	0,4839	164	90	75	12	0,0469	38	0,1484	0,4941	101
6	Çatallanma	0,4934	160	92	77	10	0,0391	36	0,1406	0,4960	102
	Hat sonu	0,5020	162	90	75	12	0,0469	38	0,1484	0,5043	103
	Çatallanma-Hat sonu	0,4980	164	74	62	14	0,0547	54	0,2109	0,4939	101
7	Çatallanma	0,4912	164	92	77	12	0,0469	36	0,1406	0,5021	103
	Hat sonu	0,5032	162	94	78	12	0,0469	34	0,1328	0,4970	102
	Çatallanma-Hat sonu	0,4971	160	96	80	14	0,0547	32	0,1250	0,4942	101

Tablo 4.1 (devam): Önerilen parmak izi s-kutuların güvenlik metriklerinin sonuçları.

S-kutu		SAC	NL			DU	DP	LAT	LP	BIC-SAC	BIC-NL
Parmak İzi	Parmak İzi Özelliği		maks.	min.	yüzdesi (%)						
8	Çatallanma	0,4963	162	62	52	20	0,0781	66	0,2578	0,4911	101
	Hat sonu	0,4983	166	90	75	12	0,0469	38	0,1484	0,5033	103
	Çatallanma-Hat sonu	0,4875	164	66	55	24	0,0938	62	0,2422	0,4885	100
9	Çatallanma	0,5012	162	76	63	12	0,0469	52	0,2031	0,4987	102
	Hat sonu	0,5051	160	94	78	10	0,0391	34	0,1328	0,4973	102
	Çatallanma-Hat sonu	0,4951	164	84	70	14	0,0547	44	0,1719	0,4980	102
10	Çatallanma	0,4968	160	96	80	20	0,0781	32	0,1250	0,5003	103
	Hat sonu	0,5002	162	92	77	14	0,0547	36	0,1406	0,5015	103
	Çatallanma-Hat sonu	0,4954	164	84	70	26	0,1016	44	0,1719	0,5016	103
11	Çatallanma	0,5017	162	94	78	12	0,0469	34	0,1328	0,5075	104
	Hat sonu	0,4900	166	86	72	14	0,0547	42	0,1641	0,5005	103
	Çatallanma-Hat sonu	0,4846	162	94	78	10	0,0391	34	0,1328	0,5006	103

4.1.1. DOĞRUSAL OLMAMA SONUÇLARI

Bir s-kutunun doğrusal olmama özelliği iki sınır noktasına bakılarak elde edilmiştir. Bir s-kutunun doğrusal olmama yüzdesi o s-kutunun en düşük doğrusal olmama değeri üzerinden hesaplanmaktadır. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasını kullanarak elde edilen 33 tane parmak izi s-kutusundan en yüksek doğrusal olmama yüzdesi %80, en düşük doğrusal olmama yüzdesi %52 ve ortalama doğrusal olmama yüzdesi %73'tür. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasını kullanarak elde edilen 33 tane parmak izi s-kutusundan en yüksek doğrusal olmama aralığı [96, 180], en düşük doğrusal olmama aralığı [62, 160] olarak bulunmuştur. En yüksek doğrusal olmama değeri 180, en düşük doğrusal olmama değeri 62 olarak bulunmuştur.

Önerilen s-kutular parmak izinin farklı özellikleri kullanılarak elde edilmiştir. Çatallanma, hat sonu ve hem çatallanma hem de hat sonu özellikleri kullanılarak elde edilen 33 adet parmak izi s-kutusunun her parmak izi özelliğine göre elde edilen maksimum, minimum ve ortalama doğrusal olmama ve doğrusal olmama yüzdeleri Tablo 4.2'de verilmiştir.

Tablo 4.2: Parmak izi özelliklerine göre önerilen parmak izi s-kutularının doğrusal olmama sonuçları.

S-kutu		Doğrusal Olmama		Doğrusal Olmama Yüzdesi (%)
		En yüksek	En düşük	
Çatallanma	Maksimum	170	96	80
	Ortalama	163	88	73
	Minimum	160	62	52
Hat sonu	Maksimum	172	94	78
	Ortalama	165	90	75
	Minimum	160	84	70
Çatallanma-Hat sonu	Maksimum	180	96	80
	Ortalama	166	84	70
	Minimum	160	66	55

Çatallanma özelliği ile elde edilen parmak izi s-kutularının en yüksek doğrusal olmama yüzdesi %80, en düşük doğrusal olmama yüzdesi %52, ortalama doğrusal olmama yüzdesi %73 olarak hesaplanmıştır. Hat sonu özelliği ile elde edilen parmak izi s-kutularının en yüksek doğrusal olmama yüzdesi %78, en düşük doğrusal olmama yüzdesi %70, ortalama doğrusal olmama yüzdesi %75 olarak hesaplanmıştır. Hem çatallanma hem de hat sonu özelliği ile elde edilen parmak izi s-kutularının en yüksek doğrusal olmama yüzdesi %80, en düşük doğrusal olmama yüzdesi %55, ortalama doğrusal olmama yüzdesi %70 olarak hesaplanmıştır.

Bir s-kutunun en iyi doğrusal olmama özelliğine sahip olması o s-kutunun doğrusal olmama yüzdesinin yüksek olmasına bağlıdır. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasının sonuçlarına göre en yüksek %80 doğrusal olmama değeri çatallanma özelliği ile oluşan parmak izi s-kutularında ve hem çatallanma hem de hat sonu özellikleri ile oluşan parmak izi s-kutularında elde edilmiştir. Fakat bu iki parmak izi özelliği ile aynı zamanda en

kötü yüzde değerleri veren s-kutular da üretilmiştir. Çatallanma özelliği kullanılarak üretilen parmak izi s-kutularının doğrusal olmama yüzdesine bakıldığında elde edilen en yüksek ve en düşük değer arasındaki fark 0.28 iken hem çatallanma hem de hat sonu özelliği kullanılarak üretilen parmak izi s-kutularının doğrusal olmama yüzdesine bakıldığında elde edilen en yüksek ve en düşük değer arasındaki fark 0.25'tir. Hat sonu özelliği kullanılarak üretilen parmak izi s-kutularının doğrusal olmama yüzdesine bakıldığında elde edilen en yüksek ve en düşük değer arasındaki fark 0.08'dir. En düşük far değeri hat sonu özelliği ile elde edilmiştir. Sonuç olarak, elde edilen doğrusal olmama performans metriğine göre en iyi sonucu veren parmak izi özelliği hat sonudur.

4.1.2. KATI ÇIĞ KRİTERİ SONUÇLARI

Bir s-kutunun katı çığ kriteri metriği açısından en iyi sonucu 0,5000 civarında ise sağlamaktadır. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasını kullanarak elde edilen 33 tane parmak izi s-kutusundan en yüksek katı çığ kriteri 0,5100, en düşük katı çığ kriteri 0,4753 ve ortalama katı çığ kriteri 0,4954 değerleri ile elde edilmiştir.

Önerilen s-kutular parmak izinin farklı özellikleri kullanılarak elde edilmiştir. Çatallanma, hat sonu ve hem çatallanma hem de hat sonu özellikleri kullanılarak elde edilen 33 adet parmak izi s-kutusunun her parmak izi özelliğine göre elde edilen maksimum, minimum ve ortalama katı çığ kriteri değerleri Tablo 4.3'te verilmiştir.

Tablo 4.3: Parmak izi özelliklerine göre önerilen parmak izi s-kutularının katı çığ kriteri sonuçları.

S-kutu		**SAC**
Çatallanma	**Maksimum**	0,5100
	Ortalama	0,4950
	Minimum	0,4761
Hat sonu	**Maksimum**	0,5098
	Ortalama	0,5011
	Minimum	0,4900
Çatallanma- Hat sonu	**Maksimum**	0,4980
	Ortalama	0,4902
	Minimum	0,4753

Çatallanma özelliği ile elde edilen parmak izi s-kutuların en yüksek SAC değeri 0,5100, en düşük SAC değeri 0,4761, ortalama SAC değeri 0,4950 olarak hesaplanmıştır. Hat sonu özelliği ile elde edilen parmak izi s-kutuların en yüksek SAC değeri 0,5098, en düşük SAC değeri 0,4900, ortalama SAC değeri 0,5011 olarak hesaplanmıştır. Hem çatallanma hem de hat sonu özelliği ile elde edilen parmak izi s-kutuların en yüksek SAC değeri 0,4980, en düşük SAC değeri 0,4753, ortalama SAC değeri 0,4902 olarak hesaplanmıştır.

Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile elde edilen s-kutuların parmak izi özelliğine göre en iyi SAC değerine hat sonu parmak izi özelliği ile elde edilmiştir. Hat sonu özelliği kullanılarak oluşturulan parmak izi s-kutularında [0,4900, 0,5098] SAC aralığında en iyi ortalama SAC değeri olan 0,5011 elde edilmiştir. Hem çatallanma hem de hat sonu özelliği kullanılarak oluşturulan parmak izi s-kutularında [0,4753, 0,4980] SAC aralığında en kötü ortalama SAC değeri olan 0,4980 elde edilmiştir. Sonuç olarak, elde edilen katı çığ kriteri performans metriğine göre en iyi sonucu veren parmak izi özelliği sırasıyla hat sonu, çatallanma ve hem çatallanma hem de hat sonu s-kutularıdır.

4.1.3. DOĞRUSAL OLASILIK SONUÇLARI

Bir s-kutunun doğrusallığı o s-kutunun doğrusal yaklaşım tablo ve doğrusal olasılık değerlerine göre analiz edilmiştir. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasını kullanarak elde edilen 33 tane parmak izi s-kutusundan en yüksek LAT değeri 66, en düşük LAT değeri 32, ortalama LAT değeri 41 olarak hesaplanmıştır. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasını kullanarak elde edilen 33 tane parmak izi s-kutusundan en yüksek LP değeri 0,2578, en düşük LP değeri 0,1250, ortalama LP değeri 0,1586 olarak hesaplanmıştır.

Önerilen s-kutular parmak izinin farklı özellikleri kullanılarak elde edilmiştir. Çatallanma, hat sonu ve hem çatallanma hem de hat sonu özellikleri kullanılarak elde edilen 33 adet parmak izi s-kutunun her parmak izi özelliğine göre elde edilen maksimum, minimum ve ortalama doğrusal dağılım tablosu değeri ve doğrusal olasılığı Tablo 4.4’te verilmiştir.

Tablo 4.4: Parmak izi özelliklerine göre önerilen parmak izi s-kutularının doğrusal olasılık sonuçları.

S-kutu		LAT	LP
Çatallanma	**Maksimum**	66	0,2578
	Ortalama	40	0,1555
	Minimum	32	0,1250
Hat sonu	**Maksimum**	44	0,1719
	Ortalama	38	0,1484
	Minimum	34	0,1328
Çatallanma-Hat sonu	**Maksimum**	62	0,2422
	Ortalama	44	0,1719
	Minimum	32	0,1250

Bir s-kutunun en iyi doğrusal olmama özelliğine sahip olması o s-kutunun doğrusal olma değerlerinin minimum olmasına bağlıdır. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasına göre üretilen parmak izi s-kutuların doğrusal saldırılara karşı dayanıklılığı elde edilen LAT ve LP değerlerinin en düşük olduğu s-kutular ile sağlanabilmektedir. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasında kullanılan 11 parmak izinin özelliklerine göre LAT ve LP değerlerini incelediğimizde maksimum olarak elde edilen LAT ve LP değerleri ne kadar düşük ise o parmak izi özelliği ile oluşturulan s-kutu daha doğrusal değildir.

Hat sonu özelliği kullanılarak oluşturulan parmak izi s-kutuları [34, 44] LAT aralığında en iyi ortalama değer olan 38 LAT değeri ve [0,1328, 0,1719] LP aralığında en iyi ortalama değer olan 0,1484 LP değeri elde edilmiştir. Çatallanma özelliği kullanılarak oluşturulan parmak izi s-kutuları [32, 66] LAT aralığında en kötü ortalama değer olan 40 LAT değeri ve [0,1250, 0,2578] LP aralığında en iyi ortalama değer olan 0,1555 LP değeri elde edilmiştir. Hem çatallanma hem de hat sonu özelliği kullanılarak oluşturulan parmak izi s-kutuları [32, 62] LAT aralığında en kötü ortalama değer olan 44 LAT değeri ve [0,1250, 0,2422] LP aralığında en iyi ortalama değer olan 0,1719 LP değeri elde edilmiştir. Sonuç olarak, elde edilen doğrusal olasılık performans metriğine göre en iyi sonucu veren parmak izi özelliği hat sonudur. Önerilen etkin

biyometrik s-kutu ve ters s-kutu oluşturma algoritmasından parmak izinin hat sonu özelliği kullanılarak oluşturulan s-kutular doğrusal saldırılara karşı daha dayanıklıdır.

4.1.4. DİFERANSİYEL OLASILIK SONUÇLARI

Bir s-kutunun diferansiyelliği o s-kutunun diferansiyel dağılım ve diferansiyel olasılık değerlerine göre analiz edilmiştir. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasını kullanarak elde edilen 33 tane parmak izi s-kutusundan en yüksek DU değeri 32, en düşük DU değeri 10, ortalama DU değeri 15 olarak hesaplanmıştır. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma s-kutu algoritmasını kullanarak elde edilen 33 tane parmak izi s-kutusundan en yüksek DP değeri 0,1250, en düşük DP değeri 0,0391, ortalama DP değeri 0,0568 olarak hesaplanmıştır.

Önerilen s-kutular parmak izinin farklı özellikleri kullanılarak elde edilmiştir. Çatallanma, hat sonu ve hem çatallanma hem de hat sonu özellikleri kullanılarak elde edilen 33 adet parmak izi s-kutunun her parmak izi özelliğine göre elde edilen maksimum, minimum ve ortalama diferansiyel dağılım değeri ve diferansiyel olasılığı Tablo 4.5'te verilmiştir.

Tablo 4.5: Parmak izi özelliklerine göre parmak izi s-kutularının diferansiyel olasılık sonuçları.

S-kutu		**DU**	**DP**
Çatallanma	**Maksimum**	32	0,1250
	Ortalama	15	0,0582
	Minimum	10	0,0391
Hat sonu	**Maksimum**	14	0,0547
	Ortalama	12	0,0469
	Minimum	10	0,0391
Çatallanma-Hat sonu	**Maksimum**	32	0,1250
	Ortalama	17	0,0653
	Minimum	10	0,0391

Çatallanma özelliği ile elde edilen parmak izi s-kutularında en yüksek diferansiyel dağılım 32, en düşük diferansiyel dağılım 10, ortalama diferansiyel dağılım 15 olarak hesaplanmıştır. Hat

sonu özelliği ile elde edilen parmak izi s-kutularında en yüksek diferansiyel dağılım 14, en düşük diferansiyel dağılım 10, ortalama diferansiyel dağılım 12 olarak hesaplanmıştır. Hem çatallanma hem de hat sonu özelliği ile elde edilen parmak izi s-kutularında en yüksek diferansiyel dağılım 32, en düşük diferansiyel dağılım 10, ortalama diferansiyel dağılım 17 olarak hesaplanmıştır.

Çatallanma özelliği ile elde edilen parmak izi s-kutularından en yüksek diferansiyel olasılığı 0,1250, en düşük diferansiyel olasılığı 0,0391, ortalama diferansiyel olasılığı 0,0582 olarak hesaplanmıştır. Hat sonu özelliği ile elde edilen parmak izi s-kutularından en yüksek diferansiyel olasılığı 0,0547 en düşük diferansiyel olasılığı 0,0391, ortalama diferansiyel olasılığı 0,0469 olarak hesaplanmıştır. Hem çatallanma hem de hat sonu özelliği ile elde edilen parmak izi s-kutularından en yüksek diferansiyel olasılığı 0,1250, en düşük diferansiyel olasılığı 0,0391, ortalama diferansiyel olasılığı 0,0653 olarak hesaplanmıştır.

Bir s-kutunun en iyi diferansiyel özelliğine sahip olması o s-kutunun diferansiyel olasılığının minimum olmasına bağlıdır. Önerilen s-kutu algoritmasına göre üretilen s-kutuların diferansiyel saldırılara karşı dayanıklılığı elde edilen DU ve DP değerlerinin en düşük olduğu s-kutular ile sağlanabilmektedir. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasında kullanılan 11 parmak izinin özelliklerine göre DU ve DP değerlerini incelediğimizde maksimum olarak elde edilen DU ve DP değerlerin ne kadar düşük ise o parmak izi özelliği diferansiyel saldırılara karşı daha dayanıklıdır.

Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasının sonuçlarına göre en düşük diferansiyel olasılığı değeri 0,0391 tüm parmak izi özellikleri ile oluşan s-kutularda elde edilmiştir. Fakat önemli olan en yüksek diferansiyel olasılık değerini veren s-kutunun diferansiyel olasılık değerinin 0,0391 değerine yakın olmasıdır. Çatallanma özelliğinin 0,0391 değerine yakınlığı 0,0859, hat sonu özelliğinin 0,0391 değerine yakınlığı 0,0156, hem çatallanma hem de hat sonu özelliğinin 0,0391 değerine yakınlığı 0,0859'dur. Sonuç olarak, hat sonu özelliği kullanılarak oluşturulan parmak izi s-kutularının DU ve DP değerleri diğer parmak izi özelliklerine göre daha iyi sonuç verdiğinden önerilen etkin biyometrik s-kutu oluşturma algoritmasından parmak izinin hat sonu özelliği kullanılarak oluşturulan s-kutular diferansiyel saldırılara karşı daha dayanıklıdır.

4.1.5. BİT BAĞIMSIZLIK KRİTERİ SONUÇLARI

Bir s-kutunun bit bağımsızlık kriteri için katı çığ kriteri metriği açısından en iyi sonucu 0,5000 civarında ise sağlamaktadır. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasını kullanarak elde edilen 33 tane parmak izi s-kutudan en yüksek bit bağımsızlık kriteri için katı çığ kriteri değeri 0,5075, en düşük bit bağımsızlık kriteri için katı çığ kriteri değeri 0,4885 ve ortalama bit bağımsızlık kriteri için katı çığ kriteri değeri 0,4987 olarak hesaplanmıştır.

Bir s-kutunun bit bağımsızlık kriteri için doğrusal olmama metriği açısından en iyi sonucu 103 ise sağlamaktadır. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasını kullanarak elde edilen 33 tane parmak izi s-kutusundan en yüksek bit bağımsızlık kriteri için doğrusal olmama değeri 104, en düşük bit bağımsızlık kriteri için doğrusal olmama değeri 100 ve ortalama bit bağımsızlık kriteri için doğrusal olmama değeri 102 olarak hesaplanmıştır.

Önerilen s-kutular parmak izinin farklı özellikleri kullanılarak elde edilmiştir. Çatallanma, hat sonu ve hem çatallanma hem de hat sonu özellikleri kullanılarak elde edilen 33 adet parmak izi s-kutunun her parmak izi özelliğine göre elde edilen maksimum, minimum ve ortalama bit bağımsızlık kriteri için katı çığ kriteri ve bit bağımsızlık kriteri için doğrusal olmama değerleri Tablo 4.6'da verilmiştir.

Tablo 4.6: Parmak izi özelliklerine göre parmak izi s-kutularının bit bağımsızlık kriteri sonuçları.

S-kutu		**BIC-SAC**	**BIC-NL**
Çatallanma	**Maksimum**	0,5075	104
	Ortalama	0,4990	102
	Minimum	0,4911	101
Hat sonu	**Maksimum**	0,5043	103
	Ortalama	0,5005	103
	Minimum	0,4970	102
Çatallanma-Hat sonu	**Maksimum**	0,5016	103
	Ortalama	0,4966	102
	Minimum	0,4885	100

Çatallanma özelliği ile elde edilen parmak izi s-kutularından en yüksek BIC-SAC değeri 0,5075, en düşük BIC-SAC değeri 0,4911, ortalama BIC-SAC değeri 0,4990 olarak hesaplanmıştır. Hat sonu özelliği ile elde edilen parmak izi s-kutuların en yüksek BIC-SAC değeri 0,5043, en düşük BIC-SAC değeri 0,4970, ortalama BIC-SAC değeri 0,5005 olarak hesaplanmıştır. Hem çatallanma hem de hat sonu özelliği ile elde edilen parmak izi s-kutuların en yüksek BIC-SAC değeri 0,5016, en düşük BIC-SAC değeri 0,4885, ortalama BIC-SAC değeri 0,4966 olarak hesaplanmıştır.

Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile elde edilen parmak izi s-kutuların parmak izi özelliğine göre en iyi BIC-SAC değerine hat sonu parmak izi özelliği ile elde edilmiştir. Sonuç olarak, elde edilen bit bağımsızlık kriteri için katı çığ etkisi performans metriğine göre en iyi sonucu veren parmak izi özelliği sırasıyla hat sonu, çatallanma ve hem çatallanma hem de hat sonu s-kutularıdır.

Çatallanma özelliği ile elde edilen parmak izi s-kutularında en yüksek BIC-NL değeri 104, en düşük BIC-NL değeri 101, ortalama BIC-NL değeri 102 olarak hesaplanmıştır. Hat sonu özelliği ile elde edilen parmak izi s-kutularında en yüksek BIC-NL değeri 103, en düşük BIC-NL değeri 102, ortalama BIC-NL değeri 103 olarak hesaplanmıştır. Hem çatallanma hem de hat sonu özelliği ile elde edilen parmak izi s-kutularında en yüksek BIC-NL değeri 103, en düşük BIC-NL değeri 100, ortalama BIC-NL değeri 102 olarak hesaplanmıştır.

Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile elde edilen parmak izi s-kutularının parmak izi özelliğine göre en iyi BIC-NL değerine hat sonu parmak izi özelliği ile elde edilmiştir.

4.1.6. BÜTÜNLÜK SONUÇLARI

Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile oluşan parmak izi s-kutuların tümü y = S(x) fonksiyonu ile S: x ∈ N → y ∈ N koşulunda oluşturulmuştur. N değeri ikili sayı sisteminde [0, 255] aralığında tekrar etmeyecek şekilde değer almaktadır. “x” değerinin onaltılı sayı sistemindeki karşılığı s-kutusunun satır ve sütununu göstermektedir. Denklem (4.1) kullanılarak her x değeri için farklı bir y değeri elde edilmektedir.

$$S(r,c) = S(hex(x)) \quad r = 1,2,\cdots,F; c = 1,2,\cdots,F \tag{4.1}$$

Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile oluşan parmak izi ters s-kutuların tümü $y = S^{-1}(x)$ fonksiyonu ile S: $x \in N \rightarrow y \in N$ koşulunda oluşturulmuştur. N değeri ikili sayı sisteminde [0, 255] aralığında tekrar etmeyecek şekilde değer almaktadır. "x" değerinin onaltılı sayı sistemindeki karşılığı ters s-kutusunun satır ve sütununu göstermektedir. Denklem (4.2) kullanılarak her x değeri için farklı bir y değeri elde edilmektedir.

$$S^{-1}(r,c) = S^{-1}\big(hex(x)\big) \quad r = 1,2,\cdots,F; c = 1,2,\cdots,F \tag{4.2}$$

11 parmak izinden bir tanesinin çatallanma özelliği kullanılarak elde edilen parmak izi s-kutusu Tablo 4.7'de verilmiştir.

Tablo 4.7: Parmak izlerinden biri ile oluşturulmuş s-kutu.

satır \ sütun	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	53	80	50	74	A8	46	45	BC	41	8B	9D	BF	54	26	5D	49
1	48	BD	D8	62	9C	B9	2D	73	6C	D6	29	4B	68	8F	B3	2F
2	47	83	A4	70	61	91	40	A7	FC	6A	89	FD	28	79	7E	33
3	90	3D	59	60	25	4D	85	5C	9B	DC	DD	CE	00	34	2B	51
4	43	78	7A	A1	EF	3C	44	C7	0D	65	38	76	42	AA	E9	C6
5	1C	67	77	5E	F1	6E	ED	F3	07	6F	13	19	E7	5A	98	14
6	A2	EA	E6	FA	06	12	9E	FB	C0	4A	AE	EB	D9	0C	11	B1
7	05	04	DE	03	B8	2E	B7	81	84	C5	2C	71	93	E2	BB	1D
8	C4	20	87	DF	C8	BA	24	A3	B4	D0	82	E0	10	F4	D4	23
9	0A	64	A6	18	D2	92	E1	AD	A9	D1	F7	72	99	B6	0F	8D
A	8E	66	09	E8	97	AF	3A	D3	86	3E	96	17	CD	EE	CA	B5
B	95	9F	8C	B0	4C	F2	7C	88	6D	F0	BE	7B	7D	D5	B2	75
C	56	39	A0	94	DB	6B	52	5F	57	69	4E	C3	AC	7F	D7	1B
D	16	DA	8A	A5	08	0E	63	E3	FE	27	F6	1F	0B	21	EC	E5
E	F8	CB	C2	C9	3B	01	2A	15	F9	55	22	37	CC	31	C1	9A
F	32	1A	AB	E4	1E	35	58	36	02	3F	5B	4F	F5	30	CF	FF

y = S(x) fonksiyonu için x değerini "167" olarak belirlediğimizde, hex(167) fonksiyonunun sonucu "A7" olarak bulunur. "A" s-kutunun satır bilgisini, "7" s-kutunun sütun bilgisini temsil

etmektedir. Tablo 4.7'de verilen parmak izi s-kutusunda elde edilen satır sütun kesişimi onaltılı sayı sisteminde "D3" yani ikili sayı sisteminde "211" değerini vermektedir. y = S(x) fonksiyonu için x değerini "48" olarak belirlediğimizde, hex(48) fonksiyonunun sonucu "30" olarak bulunur. "3" s kutunun satır bilgisini, "0" s-kutunun sütun bilgisini temsil etmektedir. Tablo 4.7'de verilen parmak izi s-kutusunda elde edilen satır sütun kesişimi onaltılı sayı sisteminde "90" yani ikili sayı sisteminde "144" değerini vermektedir. Sonuç olarak, [0, 255] aralığında verilen x değeri için s-kutu fonksiyonu [0, 255] aralığında bir değer ürettiğinden oluşturulan parmak izi s-kutularında bütünlük değeri sağlanmıştır.

11 parmak izinden bir tanesinin çatallanma özelliği kullanılarak elde edilen parmak izi s-kutunun ters s-kutusu Tablo 4.8'de verilmiştir.

Tablo 4.8: Parmak izlerinden biri ile oluşturulmuş ters s-kutu.

satır \ sütun	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	3C	E5	F8	73	71	70	64	58	D4	A2	90	DC	6D	48	D5	9E
1	8C	6E	65	5A	5F	E7	D0	AB	93	5B	F1	CF	50	7F	F4	DB
2	81	DD	EA	8F	86	34	0D	D9	2C	1A	E6	3E	7A	16	75	1F
3	FD	ED	F0	2F	3D	F5	F7	EB	4A	C1	A6	E4	45	31	A9	F9
4	26	08	4C	40	46	06	05	20	10	0F	69	1B	B4	35	CA	FB
5	02	3F	C6	00	0C	E9	C0	C8	F6	32	5D	FA	37	0E	53	C7
6	33	24	13	D6	91	49	A1	51	1C	C9	29	C5	18	B8	55	59
7	23	7B	9B	17	03	BF	4B	52	41	2D	42	BB	B6	BC	2E	CD
8	01	77	8A	21	78	36	A8	82	B7	2A	D2	09	B2	9F	A0	1D
9	30	25	95	7C	C3	B0	AA	A4	5E	9C	EF	38	14	0A	66	B1
A	C2	43	60	87	22	D3	92	27	04	98	4D	F2	CC	97	6A	A5
B	B3	6F	BE	1E	88	AF	9D	76	74	15	85	7E	07	11	BA	0B
C	68	EE	E2	CB	80	79	4F	47	84	E3	AE	E1	EC	AC	3B	FE
D	89	99	94	A7	8E	BD	19	CE	12	6C	D1	C4	39	3A	72	83
E	8B	96	7D	D7	F3	DF	62	5C	A3	4E	61	6B	DE	56	AD	44
F	B9	54	B5	57	8D	FC	DA	9A	E0	E8	63	67	28	2B	D8	FF

$y = S^{-1}(x)$ fonksiyonu için x değerini "180" olarak belirlediğimizde, hex(180) fonksiyonunun sonucu "B4" olarak bulunur. "B" ters s-kutunun satır bilgisini, "4" ters s-kutunun sütun bilgisini temsil etmektedir. Tablo 4.8'de verilen parmak izi ters s-kutusunda elde edilen satır sütun kesişimi onaltılı sayı sisteminde "88" yani ikili sayı sisteminde "136" değerini vermektedir. $y = S^{-1}(x)$ fonksiyonu için x değerini "15" olarak belirlediğimizde, hex(15) fonksiyonunun sonucu "0F" olarak bulunur. "0" ters s-kutunun satır bilgisini, "F" ters s-kutunun sütun bilgisini temsil etmektedir. Tablo 4.8'de verilen parmak izi ters s-kutusunda elde edilen satır sütun kesişimi onaltılı sayı sisteminde "9E" yani ikili sayı sisteminde "158" değerini vermektedir. Sonuç olarak, [0, 255] aralığında verilen x değeri için ters s-kutu fonksiyonu [0, 255] aralığında bir değer ürettiğinden oluşturulan parmak izi ters s-kutularında bütünlük değeri sağlanmıştır.

4.1.7. RASTGELELİK SONUÇLARI

S-kutu üretirken elemanların birbirinden bağımsız rastgele sayılardan oluşması gerekmektedir. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile oluşan her parmak izi s-kutusu birbirinden bağımsızdır. Bir parmak izinden 3 adet s-kutu üretilmektedir ve üretilen parmak izi s-kutuları arasında korelasyon bulunmamakla birlikte parmak izi s-kutusunun bir hücresindeki değerin komşu değerleri arasında da korelasyon bulunmamaktadır. Bu durumda önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasının üretmiş olduğu parmak izi s-kutuları saldırılara karşı daha dayanıklı, tahmin edilemez ve takip edilemezdir.

11 parmak izinden bir tanesinin çatallanma özelliği kullanılarak elde edilen parmak izi s-kutusu Tablo 4.9'da verilmiştir. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile üretilen parmak izi s-kutunun sütunları arasında matematiksel bir ilişki görülmemektedir. Birbiri ile bitişik olan hücreler, ardışık hücreler arasında ve satırlar arasında da korelasyon bulunmamaktadır. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasının ürettiği değerler rastgele olarak belirlenmiş bir yapıdadır.

Tablo 4.9: Parmak izinden çatallanma özelliği kullanılarak elde edilen s-kutu.

satır \ sütun	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	31	30	66	65	09	07	EE	EF	73	7C	56	24	76	4E	8B	74
1	C1	C3	ED	CA	D3	0E	BC	2F	18	43	5F	E6	1F	37	D7	E3
2	71	0D	3C	3B	11	1E	8F	B7	D8	F9	80	85	17	FC	51	8E
3	83	90	9C	78	20	CE	F8	2B	6B	35	C0	DD	DF	F0	B6	91
4	8A	C8	2C	A1	D9	47	3E	4F	C5	69	4D	EC	22	3A	23	72
5	96	AC	C6	0B	AE	59	5D	A8	CD	A3	A7	16	64	1B	81	93
6	CB	7D	A9	99	57	B8	A0	54	40	42	EB	49	08	E5	1D	F1
7	FB	AB	BA	32	F5	9B	2A	39	98	DB	E9	1C	B1	6C	F3	55
8	8D	D6	58	36	33	6F	B0	0A	02	9F	0C	62	9E	67	50	A4
9	13	E1	77	A5	27	45	AA	26	B2	03	5C	C2	79	EA	94	B9
A	CF	12	70	44	B3	10	BF	FE	19	7A	FD	60	0F	F4	15	D0
B	E8	9A	FA	87	BE	2E	AD	21	5A	1A	6E	C4	4C	2D	25	97
C	DE	28	7B	00	D4	F7	86	88	34	DA	7F	38	48	84	06	C9
D	B4	29	6A	DC	8C	4B	F6	E0	75	04	95	52	14	D5	A2	D1
E	6D	01	F2	B5	D2	46	82	53	5B	68	FF	7E	BB	3D	5E	89
F	E4	61	3F	63	C7	41	E2	AF	A6	E7	CC	4A	92	9D	05	BD

11 parmak izinden bir tanesinin hat sonu özelliği kullanılarak elde edilen parmak izi s-kutusu Tablo 4.10'da verilmiştir. Birbiri ile bitişik olan hücreler, ardışık hücreler arasında, sütunlar ve satırlar arasında da korelasyon bulunmamaktadır. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasının ürettiği değerler tamamen rastgele olarak belirlenmiş bir yapıdadır.

Tablo 4.10: Parmak izinden hat sonu özelliği kullanılarak elde edilen s-kutu.

satır \ sütun	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	CC	98	99	D1	4E	49	6B	6A	A9	6C	AD	23	76	61	6E	9F
1	27	46	6D	9D	36	B2	22	65	7A	74	67	8B	9A	FB	A4	30
2	45	43	6F	8E	A7	4C	A0	BD	89	9E	73	84	C6	47	44	54
3	AB	0D	F3	7D	7E	F2	8F	8C	9C	AA	88	CF	4F	E8	EF	E7
4	C0	1F	78	5E	51	BA	BC	97	FF	19	A8	B4	81	CE	10	B7
5	F8	21	53	52	B5	EE	C7	16	79	48	8D	8A	E4	F4	CD	4A
6	BE	83	82	F5	60	50	85	86	80	01	11	05	62	A5	EC	28
7	13	F6	E2	D5	2A	18	FD	E9	D0	1A	69	AF	91	F1	0A	77
8	9B	FE	95	D9	5A	59	BF	A1	40	58	4B	AE	E6	DF	DE	5B
9	C3	DC	DD	FC	0C	C1	15	2B	39	63	D4	75	0E	CA	E5	EB
A	37	66	29	C4	C2	DA	EA	AC	08	3B	92	7C	2C	2E	CB	70
B	06	C5	55	7F	12	26	0F	1D	ED	72	B1	1B	02	94	A6	3A
C	3E	7B	F0	0B	C9	F9	87	B0	07	E3	3D	42	3C	B9	90	68
D	20	B6	D6	D2	E0	B8	1C	A2	5F	14	96	1E	2D	71	57	F7
E	E1	BB	35	09	3F	C8	34	32	31	B3	24	41	FA	25	00	64
F	56	5D	D7	33	2F	A3	17	DB	D8	03	38	93	D3	5C	4D	04

11 parmak izinden bir tanesinin hat sonu özelliği kullanılarak elde edilen parmak izi s-kutusu Tablo 4.11'de verilmiştir. Birbiri ile bitişik olan hücreler, ardışık hücreler arasında, sütunlar ve satırlar arasında da korelasyon bulunmamaktadır. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasının ürettiği değerler tamamen rastgele olarak belirlenmiş bir yapıdadır.

Tablo 4.11: Parmak izinden hem çatallanma hem de hat sonu özelliği kullanılarak elde edilen s-kutu.

satır \ sütun	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	31	30	66	65	09	07	EE	EF	73	7C	CC	98	99	D1	4E	49
1	6B	6A	A9	6C	AD	23	76	61	6E	9F	27	46	6D	9D	36	B2
2	22	7A	74	67	8B	9A	FB	A4	45	43	6F	8E	A7	4C	A0	BD
3	89	9E	84	C6	47	44	54	AB	0D	F3	7D	7E	F2	8F	8C	9C
4	AA	88	CF	4F	E8	E7	C0	1F	78	5E	51	BA	BC	97	FF	19
5	A8	B4	81	CE	10	B7	F8	21	53	52	B5	C7	16	79	48	8D
6	8A	E4	F4	CD	4A	BE	83	82	F5	60	50	85	86	80	01	11
7	05	62	A5	EC	28	13	F6	E2	D5	2A	18	FD	E9	D0	1A	69
8	AF	91	F1	0A	77	9B	FE	95	D9	5A	59	BF	A1	40	58	4B
9	AE	E6	DF	DE	5B	C3	DC	DD	FC	0C	C1	15	2B	39	63	D4
A	75	0E	CA	E5	EB	37	29	C4	C2	DA	EA	AC	08	3B	92	2C
B	2E	CB	70	06	C5	55	7F	12	26	0F	1D	ED	72	B1	1B	02
C	94	A6	3A	3E	7B	F0	0B	C9	F9	87	B0	E3	3D	42	3C	B9
D	90	68	20	B6	D6	D2	E0	B8	1C	A2	5F	14	96	1E	2D	71
E	57	F7	E1	BB	35	3F	C8	34	32	B3	24	41	FA	25	00	64
F	56	5D	D7	33	2F	A3	17	DB	D8	03	38	93	D3	5C	4D	04

Verilen parmak izi s-kutuları aynı parmak izinden üretilmiştir. Aynı parmak izinde yer alan çatallanma ve hat sonu özellikleri ile oluşturulmuş 3 parmak izi s-kutusunun aralarında hiç korelasyon bulunmamaktadır. Bu durumda önerilen algoritmanın kullandığı parmak izi aynı olsa da birbirinden bağımsız parmak izi s-kutuları üretilerek rastgelelik özelliği sağlanmıştır.

4.1.8. GÜVENİLİRLİK ARALIĞI SONUÇLARI

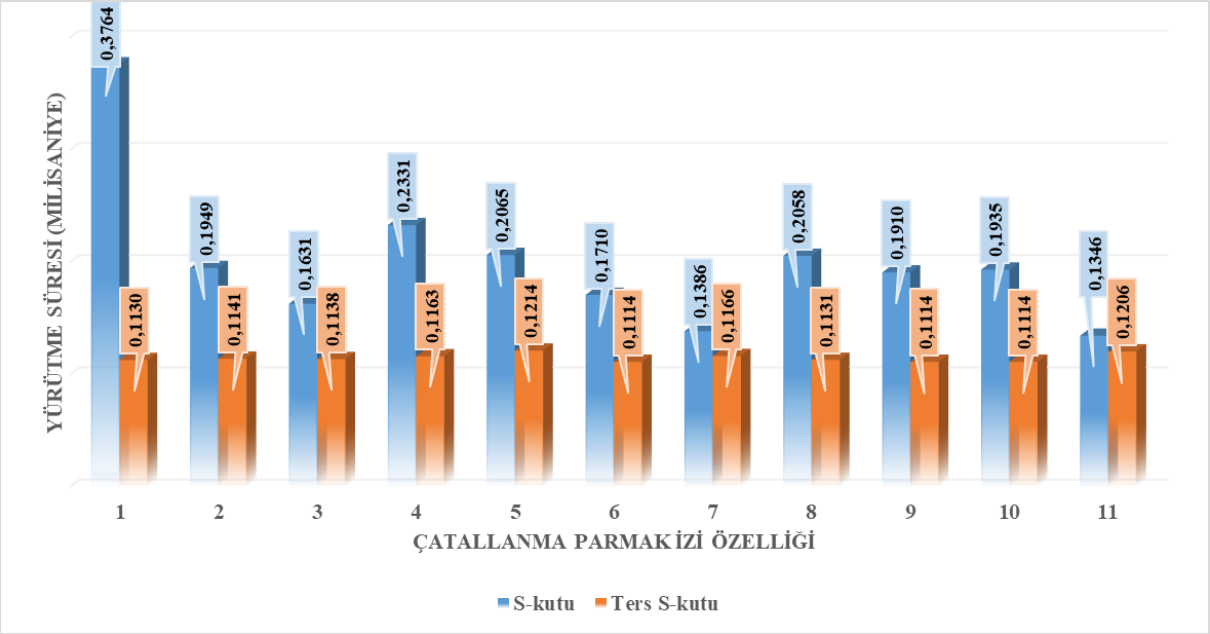
Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile oluşturulan parmak izi s-kutularında gözlemlenen değerlerin ortalaması 12,5, %95'lik güven seviyesine göre Z değeri 9,11, standart sapma 74 olarak hesaplanmıştır. Bu değerler doğrultusunda Denklem (3.) kullanılarak en düşük değer 85 ve en yüksek değer 170 olarak bulunur. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile oluşturulan parmak izi s-kutularının

hepsinin güvenilirlik aralığı [85, 170] olarak bulunmuştur ve bu değer AES s-kutusunun güvenilirlik aralığı ile aynıdır.

4.1.9. YÜRÜTME SÜRESİ SONUÇLARI

Oluşturulan s-kutular ve ters s-kutuların oluşturulma süreleri kullanılacak sisteme uygunluğunun tespiti açısından önem taşımaktadır. Mobil ödeme uygulamalarında kullanılacak ise bu sistemler için hız ve güvenilirlik ön plandadır. Eğer sistem hız açısından katkı sağlamıyor ise güvenilirliği ne kadar çok yüksek olursa olsun kullanılamamaktadır. Bu yüzden önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasının her parmak izi türü için s-kutu ve ters s-kutu üretim sürelerin hesaplanmıştır.

Önerilen etkin biyometrik s-kutu algoritması kullanılarak parmak izinin çatallanma özelliği ile üretilen parmak izi s-kutu ve ters s-kutuların yürütme süreleri Şekil 4.1'de verilmiştir.

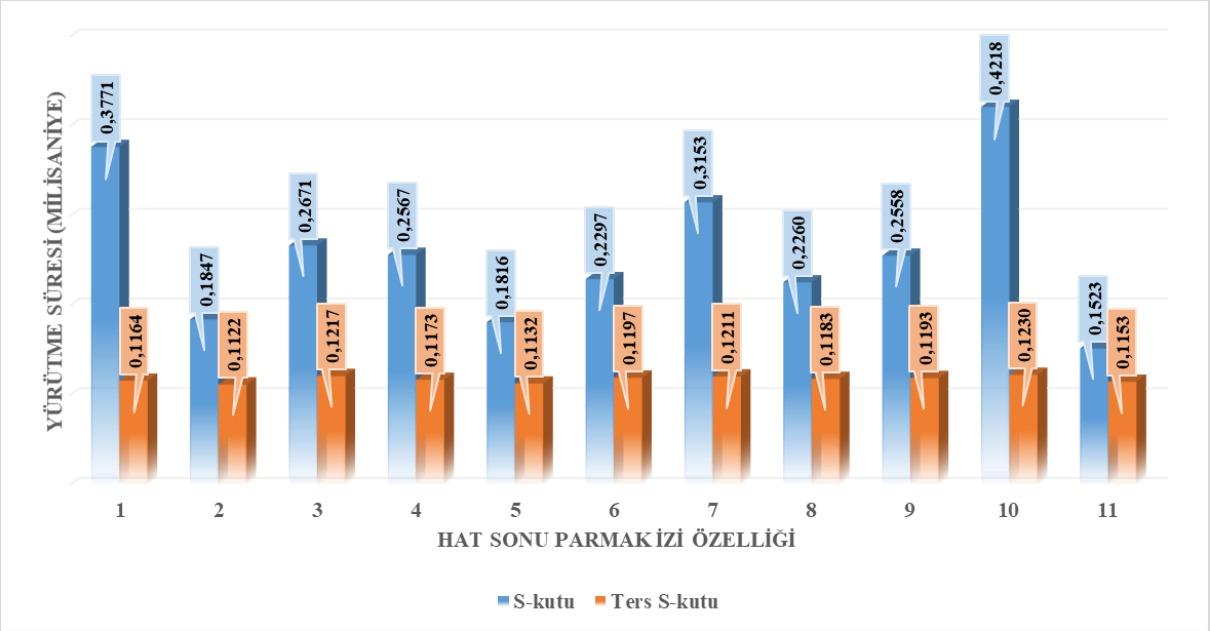


Şekil 4.1: Çatallanma parmak izi özelliğinin yürütme süreleri.

Parmak izindeki çatallanma sayısına göre algoritma yürütme süreleri değişmektedir. Eğer parmak izinde çok sayıda çatallanma özelliği var ise yürütme süresi artar, eğer parmak izinde az sayıda çatallanma özelliği ver ise yürütme süresi aynı oranda azalır. Çatallanma parmak izi özelliği ile oluşturulan parmak izi s-kutularının oluşma süresi en düşük 0,1346 milisaniye, en yüksek 0,3764 milisaniye olarak hesaplanmıştır. Çatallanma parmak izi özelliği ile oluşturulan

parmak izi ters s-kutularının oluşma süresi en düşük 0,1114 milisaniye, en yüksek 0,1214 milisaniye olarak hesaplanmıştır.

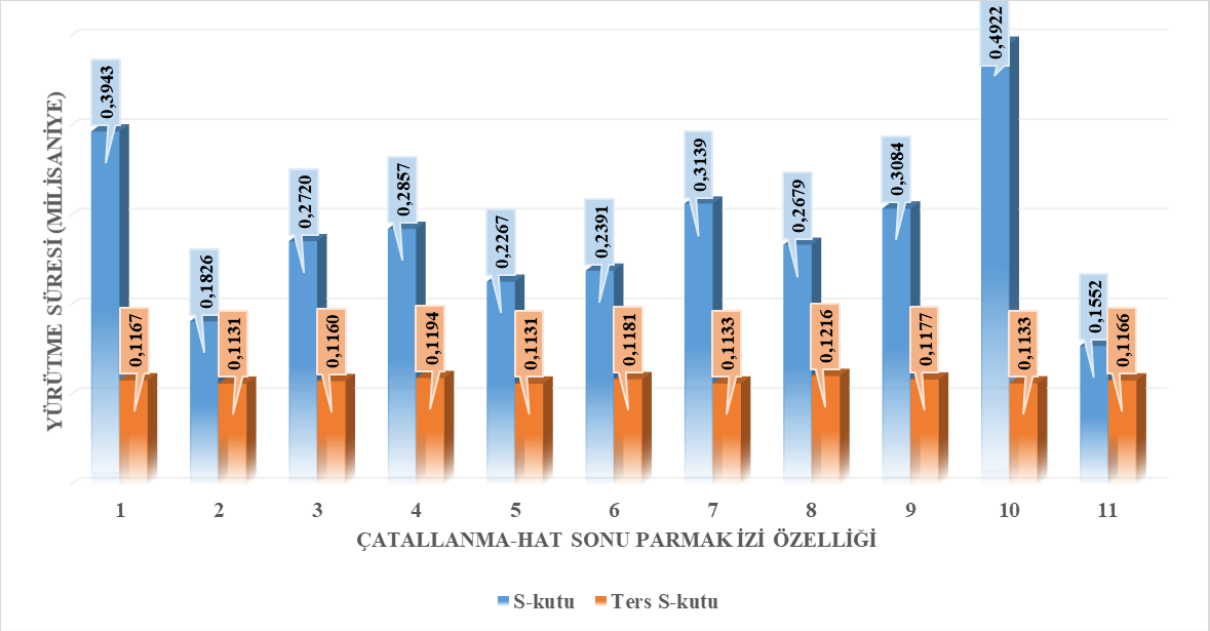
Önerilen etkin biyometrik s-kutu algoritması kullanılarak parmak izinin hat sonu özelliği ile üretilen parmak izi s-kutu ve ters s-kutuların yürütme süreleri Şekil 4.2'de verilmiştir.



Şekil 4.2: Hat sonu parmak izi özelliğinin yürütme süreleri.

Parmak izindeki hat sonu sayısına göre algoritma yürütme süreleri değişmektedir. Eğer parmak izinde çok sayıda hat sonu özelliği var ise yürütme süresi artar, eğer parmak izinde az sayıda hat sonu özelliği ver ise yürütme süresi aynı oranda azalır. Hat sonu parmak izi özelliği ile oluşturulan parmak izi s-kutularının oluşma süresi en düşük 0,1523 milisaniye, en yüksek 0,4218 milisaniye olarak hesaplanmıştır. Hat sonu parmak izi özelliği ile oluşturulan parmak izi ters s-kutularının oluşma süresi en düşük 0,1122 milisaniye, en yüksek 0,1230 milisaniye olarak hesaplanmıştır.

Önerilen etkin biyometrik s-kutu algoritması kullanılarak parmak izinin hem çatallanma hem de hat sonu özelliği ile üretilen parmak izi s-kutu ve ters s-kutuların yürütme süreleri Şekil 4.3'te verilmiştir.



Şekil 4.3: Çatallanma-hat sonu parmak izi özelliğinin yürütme süreleri.

Parmak izindeki hem çatallanma hem de hat sonu sayısına göre yürütme süreleri değişmektedir. Eğer parmak izinde çok sayıda hem çatallanma hem de hat sonu özelliği var ise yürütme süresi artar, eğer parmak izinde az sayıda hem çatallanma hem de hat sonu özelliği ver ise yürütme süresi aynı oranda azalır. Hem çatallanma hem de hat sonu parmak izi özelliği ile oluşturulan parmak izi s-kutularının oluşma süresi en düşük 0,1552 milisaniye, en yüksek 0,4922 milisaniye olarak hesaplanmıştır. Hem çatallanma hem de hat sonu parmak izi özelliği ile oluşturulan parmak izi ters s-kutularının oluşma süresi en düşük 0,1131 milisaniye, en yüksek 0,1216 milisaniye olarak hesaplanmıştır.

Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasının her parmak izinden elde edilen 3 ayrı parmak izi s-kutusu ve ters s-kutusunun oluşturulma süreleri Tablo 4.12'de verilmiştir.

Tablo 4.12: Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasının yürütme süreleri.

Parmak izi	Parmak izi özelliği	S-kutu	Ters s-kutu
1	**Çatallanma**	0,376394	0,112985
	Hat sonu	0,377098	0,116367
	Çatallanma-Hat sonu	0,394340	0,116731

Tablo 4.12 (devam): Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasının yürütme süreleri.

Parmak izi	Parmak izi özelliği	S-kutu	Ters s-kutu
2	**Çatallanma**	0,194901	0,114146
	Hat sonu	0,184684	0,112163
	Çatallanma-Hat sonu	0,182588	0,113132
3	**Çatallanma**	0,163073	0,113797
	Hat sonu	0,267054	0,121675
	Çatallanma-Hat sonu	0,271994	0,115953
4	**Çatallanma**	0,233148	0,116266
	Hat sonu	0,256725	0,117328
	Çatallanma-Hat sonu	0,285695	0,119391
5	**Çatallanma**	0,206530	0,121377
	Hat sonu	0,181596	0,113158
	Çatallanma-Hat sonu	0,226730	0,113085
6	**Çatallanma**	0,170987	0,111405
	Hat sonu	0,229663	0,119719
	Çatallanma-Hat sonu	0,239077	0,118133
7	**Çatallanma**	0,138607	0,116557
	Hat sonu	0,315267	0,121071
	Çatallanma-Hat sonu	0,313891	0,113272
8	**Çatallanma**	0,205761	0,113137
	Hat sonu	0,226040	0,118325
	Çatallanma-Hat sonu	0,267894	0,121615
9	**Çatallanma**	0,190995	0,111441
	Hat sonu	0,255837	0,119295
	Çatallanma-Hat sonu	0,308365	0,117693
10	**Çatallanma**	0,193491	0,111385
	Hat sonu	0,421776	0,122959
	Çatallanma-Hat sonu	0,492159	0,113332
11	**Çatallanma**	0,134575	0,120603
	Hat sonu	0,152314	0,115253
	Çatallanma-Hat sonu	0,155195	0,116643

Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasının her parmak izinden elde edilen 33 adet parmak izi s-kutularının ve ters s-kutularının oluşturma sürelerinin ortalama değeri, her parmak izinden 3 ayrı özelliğe göre parmak izi s-kutularının ve ters s-kutularının oluşturma sürelerinin ortalama değerleri Tablo 4.13'te verilmiştir.

Tablo 4.13: Parmak izi özelliklerine göre önerilen algoritmanın ortalama yürütme süreleri.

Parmak izi özellikleri	S-kutu	Ters s-kutu
Çatallanma	0,200769	0,114827
Hat sonu	0,260732	0,117938
Çatallanma-Hat sonu	0,285266	0,116271
Tüm parmak izi s-kutuları	0,248923	0,116345

Her parmak izinde farklı sayıda çatallanma ve hat sonu özelliği bulunmaktadır. Bu farklılığı değerlendirmek için 11 farklı parmak izinin önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasının yürütme süreleri karşılaştırıldı. 11 parmak izinden elde edilen 33 parmak izi s-kutusu ortalama 0,249 milisaniye, 33 parmak izi ters s-kutusu ortalama 0,116 milisaniyede oluşturulmuştur. Parmak izi özellikleri açısından değerlendirdiğimizde, bir parmak izinde en çok hat sonu özelliği sayısı bulunmaktayken en az çatallanma özelliği sayısı bulunmaktadır. Özelliğin parmak izinde bulunma sayısı ile doğru orantılı olarak önerilen algoritmanın yürütme süresi de artmaktadır. Sonuç olarak, parmak izi özelliklerini en kısa yürütme süresinden en uzun yürütme süresine doğru sıraladığımızda çatallanma, hat sonu ve hem çatallanma hem de hat sonu olduğu gözlemlenmiştir. Önerilen etkin biyometrik s-kutu oluşturma algoritmasının yürütme süresi 0,29 milisaniyeden az, ters s-kutu oluşturma algoritmasının yürütme süresi 0,12 milisaniyeden az olduğu gözlemlenmiştir. Oluşan tüm parmak izi s-kutu ve ters s-kutular geçerli yürütme süresine sahiptir.

4.2. ÖNERİLEN PARMAK İZİ S-KUTULARIN MEVCUT S-KUTULAR İLE KARŞILAŞTIRILMASI

Literatürde en iyi güvenlik performans metrikleri polinomlu s-kutular ile elde edilmiştir. Farklı yapılar ile oluşturulan s-kutuların güvenlik ölçütleri AES gibi indirgenemez polinom ile üretilen s-kutular ile kıyaslanmaktadır. Kaotik s-kutuların bazıları polinomlu s-kutulara yakın güvenlik performans metrikleri sunan s-kutulardır. Mevcut biyometrik s-kutular ne polinom ile üretilen

s-kutuların performans metriklerine ne de kaotik s-kutuların performans metriklerine ulaşabilmiştir. Bu bölümde, önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile oluşturulan parmak izi s-kutuları mevcut polinomlu, kaotik ve biyometrik s-kutular ile karşılaştırılmıştır.

Güvenlik performans metriklerine göre önerilen parmak izi s-kutuları mevcut DNA ve RNA biyometrik verileri kullanılarak oluşturulan biyometrik s-kutulardan çok daha iyi sonuç vermiştir. Güvenlik performans metriklerine göre önerilen parmak izi s-kutuları mevcut kaotik s-kutularının bazılarından çok daha iyi sonuç verdiği gibi polinomlu s-kutu sonuçlarına da yakınsadığı gözlenmiştir.

Parmak izinin özellikleri kullanılarak elde edilen 33 adet s-kutuların her özelliğe göre ortalama NL, SAC, DU, DP, LAT, LP, BIC-NL ve BIC-SAC değerleri Tablo 4.14'te verilmiştir. Parmak izi özellikleri ile oluşturulan s-kutuların performans sonuçlarını karşılaştırdığımızda hat sonu özelliği ile elde edilen s-kutuların daha iyi sonuçlar verdiği gözlenmiştir.

Tablo 4.14: Parmak izi özelliklerine göre elde edilen ortalama sonuçlar.

Parmak izi özelliği	SAC	NL			DU	DP	LAT	LP	BIC-SAC	BIC-NL
		maks.	min.	yüzdesi (%)						
Çatallanma özelliğinin ortalaması	0,4950	163	88	73	15	0,0582	40	0,1555	0,4990	102
Hat sonu özelliğinin ortalaması	0,5011	165	90	75	12	0,0469	38	0,1484	0,5005	103
Çatallanma-hat sonu özelliğinin ortalaması	0,4902	166	84	70	17	0,0653	44	0,1719	0,4966	102
Tüm parmak izi ortalaması	0,4954	165	87	73	15	0,0568	41	0,1586	0,4987	102

Literatürde kabul görmüş polinomlu, kaotik ve biyometrik s-kutuların NL, SAC, DU, DP, LAT, LP, BIC-NL ve BIC-SAC değerleri ile önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile oluşturulan parmak izi s-kutularının Tablo 4.1'de verilen güvenlik metrikleri ile karşılaştırdığımızda parmak izi ile oluşturulan s-kutulardan güvenlik parametrelerine göre en

iyi sonucu veren parmak izi s-kutularından biri sonuçları ile Tablo 4.15'te verilmiştir. Ekler bölümünde elde edilen parmak izi s-kutu örnekleri verilmiştir.

Tablo 4.15: Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile elde edilen bir s-kutu ve sonuçları.

SAC	NL			DU	DP	LAT	LP	BIC-SAC	BIC-NL
	maks.	min.	yüzdesi (%)						
0,5002	162	94	78	10	0,0391	34	0,1328	0,5047	103

satır \ sütun	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	40	4F	1C	1F	1E	59	22	23	0A	32	2D	31	65	68	4D	85
1	26	F0	7D	44	8C	53	5B	C2	C0	AA	EA	D5	3F	D1	FE	58
2	96	1B	41	DE	A4	9C	E5	A8	52	73	6F	47	8F	FB	F4	1A
3	04	C5	C7	2B	B7	4A	89	83	EF	5D	D3	50	06	09	14	C1
4	86	E8	7B	BE	5A	CD	81	33	21	48	75	AE	6C	D4	15	CA
5	30	79	70	0E	AD	BB	97	A9	F3	77	AF	DF	CC	A0	DD	1D
6	56	D8	D2	F5	80	4E	B3	0D	B9	0C	DC	35	19	C6	95	5F
7	3B	EE	3E	11	B0	E1	E6	5C	74	9F	A1	36	FD	87	8D	84
8	3A	29	93	ED	AB	05	B2	E3	34	BD	51	63	E0	45	98	7F
9	94	C8	EB	62	E7	A6	92	9E	38	E9	B8	DB	D0	B6	99	91
A	16	6E	7E	57	E2	FC	25	43	9D	F8	CE	A2	BF	8B	64	BC
B	12	46	61	8A	B1	10	90	3D	03	DA	F1	7C	2C	71	6A	AC
C	3C	66	27	24	82	D7	F2	A5	42	72	17	49	E4	69	F6	20
D	07	D9	2F	2A	88	C4	F7	EC	01	18	78	0F	7A	02	4B	0B
E	C3	FF	D6	B4	00	A7	6D	28	76	4C	2E	67	08	9A	54	FA
F	13	39	C9	60	A3	F9	B5	8E	55	CF	9B	CB	BA	5E	37	6B

4.2.1. POLİNOMLU S-KUTULAR İLE KARŞILAŞTIRILMASI

Literatürde kullanılan en önemli indirgenemez polinomlar ile oluşturulan s-kutular AES (Daemen ve Rijmen, 2002), Gray (Cui ve Yuanda,2007) ve APA (Tran ve diğ., 2008) s-kutularıdır. Bu s-kutuların güvenlik performans metriklerinin sonuçları ideal değerler olarak ele alınmaktadır. Chandrasekharappa ve diğ. (2011) çalışmasında 11B AES indirgenemez

polinomunu kullanarak farklı parametreler ile birleştirmiş ve yeni bir s-kutu elde etmiştir. Aynı polinomun kullanılmasına rağmen s-kutu oluşturma değişkenlerinin değişmesi ile performans sonuçlarında AES s-kutusuna göre düşüş gözlenmiştir. Chandrasekharappa ve diğ. (2011) çalışmasında kullandığı diğer indirgenemez polinom 14D ile daha düşük sonuçlar elde etmiştir. Das ve diğ. (2013) çalışmasında 11D indirgenemez polinomu ile 0A, 31, 4A, 74, 9D, CA, D5, F0 toplam sabitleri ile sekiz adet s-kutu oluşturmuştur. Aynı polinomun kullanılarak toplam sabitinin değiştirilmesi ile farklı s-kutular oluşmuştur fakat elde edilen s-kutuların güvenlik metriklerinin sonuçları değişmemiştir. 11D indirgenemez polinomunun performans sonuçlarının AES s-kutusuna göre düşük olduğu gözlenmiştir.

İndirgenemez polinom kullanılarak oluşturulan bu s-kutuların NL, SAC, DU, DP, LAT, LP, BIC-NL ve BIC-SAC performans sonuçları Tablo 4.16'da verilmiştir.

Tablo 4.16: İndirgenemez polinom ile oluşturulan s-kutuların sonuçları.

S-kutu	SAC	NL			DU	DP	LAT	LP	BIC-SAC	BIC-NL
		maks.	min.	yüzdesi (%)						
Daemen ve Rijmen (2002) AES	0,5049	144	112	93	4	0,0156	16	0,0625	0,5046	103
Cui ve Yuanda (2007) GRAY	0,4998	144	112	93	4	0,0156	16	0,0625	0,5026	103
Tran ve diğ. (2008) APA	0,5007	144	112	93	4	0,0156	16	0,0625	0,4997	102
Chandrasekharappa ve diğ. (2011) 11B	0,5195	148	108	90	6	0,0234	20	0,0781	0,5006	103
Chandrasekharappa ve diğ. (2011) 14D	0,5210	149	107	89	8	0,0313	21	0,0820	0,5007	103
Das ve diğ. (2013) 11D-0A	0,5068	156	100	83	8	0,0313	28	0,1094	0,5047	103
Das ve diğ. (2013) 11D-31	0,5068	154	100	83	8	0,0313	28	0,1094	0,5047	103
Das ve diğ. (2013) 11D-4A	0,5068	156	100	83	8	0,0313	28	0,1094	0,5047	103

Tablo 4.16 (devam): İndirgenemez polinom ile oluşturulan s-kutuların sonuçları.

S-kutu	SAC	NL			DU	DP	LAT	LP	BIC-SAC	BIC-NL
		maks.	min.	yüzdesi (%)						
Das ve diğ. (2013) 11D-74	0,5068	156	100	83	8	0,0313	28	0,1094	0,5047	103
Das ve diğ. (2013) 11D-9D	0,5068	156	100	83	8	0,0313	28	0,1094	0,5047	103
Das ve diğ. (2013) 11D-CA	0,5068	156	100	83	8	0,0313	28	0,1094	0,5047	103
Das ve diğ. (2013) 11D-D5	0,5068	156	100	83	8	0,0313	28	0,1094	0,5047	103
Das ve diğ. (2013) 11D-F0	0,5068	156	100	83	8	0,0313	28	0,1094	0,5047	103

İndirgenemez polinomlar ile oluşturulan s-kutuların performans metrikleri ile ilgili aşağıdaki sonuçlar elde edilmiştir.

- En düşük SAC değeri 0,4998 ve en yüksek SAC değeri 0,5210'dur.
- En düşük NL yüzdesi %83 ve en yüksek NL yüzdesi %93'tür.
- En düşük DU değeri 4 ve en yüksek DU değeri 8'dir.
- En düşük DP değeri 0,0156 ve en yüksek DP değeri 0,0313'tür.
- En düşük LAT değeri 16 ve en yüksek LAT değeri 28'dir.
- En düşük LP değeri 0,0625 ve en yüksek LP değeri 0,1094'tür.
- En düşük BIC-SAC değeri 0,4997 ve en yüksek BIC-SAC değeri 0,5047'dir.
- En düşük BIC-NL değeri 102 ve en yüksek BIC-NL değeri 103'tür.

4.2.2. KAOTİK S-KUTULAR İLE KARŞILAŞTIRILMASI

Literatürde yer alan kaotik s-kutular güvenlik parametreleri ile AES s-kutusu ile elde edilen değerler ile karşılaştırılmaktadır. AES s-kutusuna göre ideal SAC değeri 0,5049 ve BIC-SAC değeri 0,5046, ideal NL yüzdesi %93, ideal BIC-NL 103, ideal DP 0,0156 değeri, ideal LP değeri 0,0625'tir. Literatürde kullanılan kaotik s-kutuların NL, SAC, DU, DP, LAT, LP, BIC-NL ve BIC-SAC sonuçları Tablo 4.17'de verilmiştir. Kaotik s-kutuların ortalama SAC değeri

0,5014, NL yüzdesi %79, DU 10, DP 0,0391, LAT 33, LP 0,1303, BIC-SAC 0,5021, BIC-NL 103'tür.

Kaotik s-kutularını AES s-kutusu ile karşılaştırdığımızda hemen hemen tüm kaotik s-kutular AES s-kutu güvenlik parametrelerine yakınsayarak elde edilmiştir.

- Özkaynak ve Özer (2010), Altaleb ve diğ. (2017), Ullah ve diğ. (2017) s-kutuları AES s-kutusu ile aynı SAC değerine sahipken diğer kaotik s-kutuların bu SAC değerine yakınsadığı gözlenmiştir.
- Farwa ve diğ. (2016), Altaleb ve diğ. (2017), Ullah ve diğ. (2017), Mahmood Malik ve diğ. (2020) s-kutuları dışında diğer kaotik s-kutuların ideal NL değerine ulaşamadığı gözlenmiştir.
- Farwa ve diğ. (2016), Altaleb ve diğ. (2017), Ullah ve diğ. (2017), Mahmood Malik ve diğ. (2020) s-kutuları AES s-kutusu ile aynı DP değerine sahipken diğer kaotik s-kutuların bu DP değerine yakınsadığı gözlenmiştir.
- Farwa ve diğ. (2016), Altaleb ve diğ. (2017), Ullah ve diğ. (2017), Mahmood Malik ve diğ. (2020) s-kutuları AES s-kutusu ile aynı LP değerine sahipken diğer kaotik s-kutuların bu LP değerine yakınsadığı gözlenmiştir.
- Altaleb ve diğ. (2017) ve Ullah ve diğ. (2017) s-kutuları AES s-kutusu ile aynı BIC-SAC değerine sahipken diğer kaotik s-kutuların bu BIC-SAC değerine yakınsadığı gözlenmiştir.
- Özkaynak ve Yavuz (2013), Lambić (2014), Khan (2015), Farwa ve diğ. (2016), Jamal ve diğ. (2016), Belazi ve diğ. (2017a), Belazi ve Latif (2017), Çavuşoğlu ve diğ. (2017), Özkaynak (2017)-1, Özkaynak ve diğ. (2017), Alzaidi ve diğ. (2018), Ullah ve diğ. (2018), Zhang ve diğ. (2018), Ahmed ve diğ. (2019), Özkaynak (2019)-3, Yi ve diğ. (2019), Lu ve diğ. (2020), Zhang ve diğ. (2020)-2 s-kutuları dışındaki kaotik s-kutular AES s-kutusu ile aynı BIC-NL değerini elde ettiği gözlenmiştir.

Tablo 4.17: Kaotik s-kutuların sonuçları.

S-kutu	SAC	NL			DU	DP	LAT	LP	BIC-SAC	BIC-NL
		maks.	min.	yüzdesi (%)						
Özkaynak ve Özer (2010)	0,5049	162	94	78	10	0,0391	34	0,1328	0,5010	103
Peng ve diğ. (2011)	0,4995	160	94	78	12	0,0469	34	0,1328	0,5044	103
Wang ve diğ. (2012)	0,5068	160	92	77	10	0,0391	36	0,1406	0,5017	103
Wang ve Peng (2012)	0,4988	164	92	77	10	0,0391	36	0,1406	0,5027	103
Khan ve diğ. (2013)	0,4954	160	92	77	12	0,0469	36	0,1406	0,5048	103
Özkaynak ve Yavuz (2013)	0,5061	164	88	73	10	0,0391	40	0,1563	0,4983	102
Guesmi ve diğ. (2014)	0,4971	160	96	80	10	0,0391	32	0,1250	0,5035	103
Lambić (2014)	0,5012	152	104	87	8	0,0313	24	0,0938	0,5056	104
Ahmad ve diğ. (2015)	0,5015	160	90	75	10	0,0391	38	0,1484	0,5016	103
Khan (2015)	0,4812	174	82	68	16	0,0625	46	0,1797	0,4967	102
Khan ve Shah (2015)	0,4978	164	92	77	12	0,0469	36	0,1406	0,5010	103
Liu ve diğ. (2015)	0,4976	160	96	80	10	0,0391	32	0,1250	0,5013	103
Ahmad ve diğ. (2016)	0,5037	160	90	75	10	0,0391	38	0,1484	0,5040	103
Ahmad ve Malik (2016)	0,4988	164	92	77	10	0,0391	36	0,1406	0,5031	103
Farwa ve diğ. (2016)	0,5103	144	112	93	4	0,0156	16	0,0625	0,5064	104
Jamal ve diğ. (2016)	0,4836	163	85	71	14	0,0547	43	0,1680	0,4948	101
Tian ve Lu (2016)	0,5073	162	90	75	10	0,0391	38	0,1484	0,5020	103

Tablo 4.17 (devam): Kaotik s-kutuların sonuçları.

S-kutu	SAC	NL			DU	DP	LAT	LP	BIC-SAC	BIC-NL
		maks.	min.	yüzdesi (%)						
Altaleb ve diğ. (2017)	0,5049	144	112	93	4	0,0156	16	0,0625	0,5046	103
Belazi ve diğ. (2017b)	0,5056	160	88	73	10	0,0391	40	0,1563	0,5019	103
Belazi ve diğ. (2017a)	0,5115	156	100	83	8	0,0313	28	0,1094	0,4982	102
Belazi ve Latif (2017)	0,5010	162	94	78	12	0,0469	34	0,1328	0,5063	104
Çavuşoğlu ve diğ. (2017)	0,5039	162	92	77	10	0,0391	36	0,1406	0,5059	104
Farah ve diğ. (2017)	0,5120	162	94	78	10	0,0391	34	0,1328	0,5042	103
Lambić (2017)	0,5034	162	94	78	10	0,0391	34	0,1328	0,5015	103
Özkaynak (2017)-1	0,5012	160	96	80	10	0,0391	32	0,1250	0,5001	102
Özkaynak (2017)-2	0,5103	162	94	78	10	0,0391	34	0,1328	0,5005	103
Özkaynak ve diğ. (2017)	0,4963	162	92	77	10	0,0391	36	0,1406	0,4938	101
Tian ve Lu (2017)	0,5093	164	92	77	10	0,0391	36	0,1406	0,5025	103
Ullah ve diğ. (2017)	0,5049	144	112	93	4	0,0156	16	0,0625	0,5046	103
Alzaidi ve diğ. (2018)	0,5000	160	96	80	10	0,0391	32	0,1250	0,5052	104
Al Solami ve diğ. (2018)	0,5017	160	94	78	10	0,0391	34	0,1328	0,5006	103
Ullah ve diğ. (2018)	0,5034	162	94	78	12	0,0469	34	0,1328	0,4980	102
Ye ve Zhimao (2018)	0,4976	162	94	78	10	0,0391	34	0,1328	0,5022	103
Zhang ve diğ. (2018)	0,4946	168	88	73	10	0,0391	40	0,1563	0,5054	104

Tablo 4.17 (devam): Kaotik s-kutuların sonuçları.

S-kutu	SAC	NL			DU	DP	LAT	LP	BIC-SAC	BIC-NL
		maks.	min.	yüzdesi (%)						
Ahmed ve diğ. (2019)	0,4944	160	94	78	10	0,0391	34	0,1328	0,4978	102
Khan ve diğ. (2019a)	0,5039	149	107	89	6	0,0234	21	0,0820	05040	103
Khan ve diğ. (2019b)-1	0,5066	156	100	83	8	0,0313	28	0,1094	0,5031	103
Khan ve diğ. (2019b)-2	0,5044	160	96	80	10	0,0391	31	0,1250	0,5005	103
Lu ve diğ. (2019)	0,5151	158	92	77	12	0,0469	36	0,1406	0,5049	103
Özkaynak (2019)-1	0,4941	160	96	80	10	0,0391	32	0,1250	0,5013	103
Özkaynak (2019)-2	0,4971	162	92	77	10	0,0391	36	0,1406	0,5008	103
Özkaynak (2019)-3	0,5002	162	86	72	12	0,0469	42	0,1641	0,5070	104
Özkaynak (2019)-4	0,4988	164	92	77	12	0,0469	36	0,1406	0,5047	103
Tanyildizi ve Özkaynak (2019)	0,4995	162	94	78	12	0,0469	34	0,1328	0,5037	103
Yi ve diğ. (2019)	0,4976	164	92	77	12	0,0469	36	0,1406	0,4963	102
Lambić (2020)	0,5010	160	94	78	10	0,0391	34	0,1328	0,5005	103
Lu ve diğ. (2020)	0,5029	162	94	78	10	0,0391	34	0,1328	0,5070	104
Mahmood Malik ve diğ. (2020)	0,5010	144	112	93	4	0,0156	16	0,0625	0,5027	103
Zhang ve diğ. (2020)-1	0,5029	160	90	75	12	0,0469	38	0,1484	0,5006	103
Zhang ve diğ. (2020)-2	0,5002	162	94	78	12	0,0469	34	0,1328	0,5054	104

Literatürdeki kaotik s-kutuların güvenlik parametrelerinin sonuçları parmak izi s-kutuları ile karşılaştırıldığında;

- Kaotik s-kutuların en düşük SAC değeri 0,4812 ve en yüksek SAC değeri 0,5151'dir. Önerilen 33 parmak izi s-kutusundan 30 tanesi bu aralıkta SAC değerine sahiptir. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile oluşturulan parmak izi s-kutularının %91'i katı çığ kriterini sağlamaktadır.
- Kaotik s-kutuların en düşük NL yüzdesi %68 ile [82, 144] NL aralığındadır ve en yüksek NL yüzdesi %93 ile [112, 174] NL aralığındadır. Önerilen 33 parmak izi s-kutusundan 28 tanesi bu aralıkta NL değerine sahiptir. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile oluşturulan parmak izi s-kutularının %85'i doğrusal olmama özelliğini sağlamaktadır.
- Kaotik s-kutuların en düşük DU değeri 4 ve en yüksek DU değeri 16'dır. Önerilen 33 parmak izi s-kutusundan 26 tanesi bu aralıkta DU değerine sahiptir. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile oluşturulan parmak izi s-kutularının %79'u diferansiyel dağılım özelliğini sağlamaktadır.
- Kaotik s-kutuların en düşük DP değeri 0,0156 ve en yüksek DP değeri 0,0625'tir. Önerilen 33 parmak izi s-kutusundan 26 tanesi bu aralıkta DP değerine sahiptir. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile oluşturulan parmak izi s-kutularının %79'u diferansiyel olasılık özelliğini sağlamaktadır.
- Kaotik s-kutuların en düşük LAT değeri 16 ve en yüksek LAT değeri 46'dır. Önerilen 33 parmak izi s-kutusundan 28 tanesi bu aralıkta LAT değerine sahiptir. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile oluşturulan parmak izi s-kutularının %85'i LAT özelliğini sağlamaktadır.
- Kaotik s-kutuların en düşük LP değeri 0,0625 ve en yüksek LP değeri 0,1797'dir. Önerilen 33 parmak izi s-kutusundan 28 tanesi bu aralıkta LP değerine sahiptir. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile oluşturulan parmak izi s-kutularının %85'i doğrusal olasılık özelliğini sağlamaktadır.
- Kaotik s-kutuların en düşük BIC-SAC değeri 0,4938 ve en yüksek BIC-SAC değeri 0,5070'tir. Önerilen 33 parmak izi s-kutusundan 30 tanesi bu aralıkta BIC-SAC değerine sahiptir. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile oluşturulan parmak izi s-kutularının %91'i bit bağımsızlık kriteri için katı çığ kriteri özelliğini sağlamaktadır.

- Kaotik s-kutuların en düşük BIC-NL değeri 101 ve en yüksek BIC-NL değeri 104'tür. Önerilen 33 parmak izi s-kutusundan 32 tanesi bu aralıkta BIC-NL değerine sahiptir. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile oluşturulan parmak izi s-kutularının %97'si bit bağımsızlık kriteri için doğrusal olmama özelliğini sağlamaktadır.

Önerilen parmak izi s-kutularının ortalama değerleri ile kaotik s-kutulara ait sonuçlar karşılaştırıldığında;

- Tüm parmak izi s-kutularının ortalama NL yüzdesi [87, 165] doğrusal olmama aralığında %73 oranı ile Özkaynak ve Yavuz (2013), Belazi ve diğ. (2017b), Zhang ve diğ. (2018) s-kutuları ile aynı, Khan (2015), Jamal ve diğ. (2016), Özkaynak (2019)-3 s-kutularından daha iyi sonuç vermiştir. Hat sonu parmak izi özelliği ile elde edilen parmak izi s-kutularının ortalama NL yüzdesi [90, 165] doğrusal olmama aralığında %75 oranı ile Ahmad ve diğ. (2015), Ahmad ve diğ. (2016), Tian ve Lu (2016), Zhang ve diğ. (2020)-1 s-kutuları ile aynı, Özkaynak ve Yavuz (2013), Khan (2015), Jamal ve diğ. (2016), Belazi ve diğ. (2017b), Zhang ve diğ. (2018), Özkaynak (2019)-3 s-kutularından daha iyi sonuç vermiştir.
- Tüm parmak izi s-kutuların ortalama 0,4954 SAC değeri ile Khan (2015), Farwa ve diğ. (2016), Jamal ve diğ. (2016), Belazi ve diğ. (2017a), Farah ve diğ. (2017), Özkaynak (2017)-2, Tian ve Lu (2017), Zhang ve diğ. (2018), Ahmed ve diğ. (2019), Lu ve diğ. (2019), Özkaynak (2019)-1 s-kutularından daha iyi sonuç vermiştir. Hat sonu parmak izi özelliği ile elde edilen parmak izi s-kutuları ortalama 0,5011 SAC değeri ile Lambić (2014), Ahmad ve diğ. (2015), Belazi ve Latif (2017), Özkaynak (2017)-1, Alzaidi ve diğ. (2018), Özkaynak (2019)-3, Lambić (2020), Mahmood Malik ve diğ. (2020), Zhang ve diğ. (2020)-2 s-kutuları ile aynı, diğer kaotik s-kutularından daha iyi sonuç vermiştir.
- Tüm parmak izi s-kutuları ortalama 15 DU ve 0,1586 DP değerleri ile Khan (2015) s-kutusundan daha iyi sonuç vermiştir. Hat sonu parmak izi özelliği ile elde edilen parmak izi s-kutuları ortalama 12 DU ve 0,0469 DP değerleri ile Peng ve diğ. (2011), Khan ve diğ. (2013), Khan ve Shah (2015), Belazi ve Latif (2017), Ullah ve diğ. (2018), Lu ve diğ. (2019), Özkaynak (2019)-3, Özkaynak (2019)-4, Tanyildizi ve Özkaynak (2019), Yi ve diğ. (2019), Zhang ve diğ. (2020)-1, Zhang ve diğ. (2020)-2 s-kutuları ile aynı, Khan (2015) ve Jamal ve diğ. (2016) s-kutularından daha iyi sonuç vermiştir.

- Tüm parmak izi s-kutuları ortalama 41 LAT ve 0,1586 LP değerleri ile Khan (2015), Jamal ve diğ. (2016), Özkaynak (2019)-3 s-kutusundan daha iyi sonuç vermiştir. Hat sonu parmak izi özelliği ile elde edilen parmak izi s-kutuları ortalama 38 LAT ve 0,1484 LP değerleri ile Ahmad ve diğ. (2015), Ahmad ve diğ. (2016), Tian ve Lu (2016), Zhang ve diğ. (2020)-1 s-kutuları ile aynı, Özkaynak ve Yavuz (2013), Khan (2015), Jamal ve diğ. (2016), Belazi ve diğ. (2017b), Zhang ve diğ. (2018), Özkaynak (2019)-3, s-kutularından daha iyi sonuç vermiştir.
- Tüm parmak izi s-kutuları ortalama 0,4987 BIC-SAC değeri ile Özkaynak ve Yavuz (2013), Khan (2015), Belazi ve diğ. (2017a), Özkaynak ve diğ. (2017), Ullah ve diğ. (2018), Ahmed ve diğ. (2019), Yi ve diğ. (2019) s-kutularından daha iyi sonuç vermiştir. Hat sonu parmak izi özelliği ile elde edilen parmak izi s-kutuları ortalama 0,5005 SAC değeri ile Özkaynak (2017)-1, Özkaynak (2017)-1, Khan ve diğ. (2019b)-2, Lambić (2020) hariç diğer kaotik s-kutularından daha iyi sonuç vermiştir.
- Tüm parmak izi s-kutuları ortalama 102 BIC-NL değeri ile Özkaynak ve Yavuz (2013), Khan (2015), Belazi ve diğ. (2017a), Özkaynak (2017)-1, Ullah ve diğ. (2018), Ahmed ve diğ. (2019), Yi ve diğ. (2019) s-kutuları ile aynı, Lambić (2014), Farwa ve diğ. (2016), Jamal ve diğ. (2016), Belazi ve Latif (2017), Çavuşoğlu ve diğ. (2017), Özkaynak ve diğ. (2017), Alzaidi ve diğ. (2018), Zhang ve diğ. (2018), Özkaynak (2019)-3, Lu ve diğ. (2020), Zhang ve diğ. (2020)-2 s-kutularından daha iyi sonuç vermiştir. Hat sonu parmak izi özelliği ile elde edilen parmak izi s-kutuları ortalama 103 BIC-NL değeri ile Özkaynak ve Yavuz (2013), Lambić (2014), Khan (2015), Farwa ve diğ. (2016), Jamal ve diğ. (2016), Belazi ve diğ. (2017a), Belazi ve Latif (2017), Çavuşoğlu ve diğ. (2017), Özkaynak (2017)-1, Özkaynak ve diğ. (2017), Alzaidi ve diğ. (2018), Ullah ve diğ. (2018), Zhang ve diğ. (2018), Ahmed ve diğ. (2019), Özkaynak (2019)-3, Yi ve diğ. (2019), Lu ve diğ. (2020), Zhang ve diğ. (2020)-2 s-kutularından daha iyi ve diğer kaotik s-kutuları ile aynı BIC-NL değerini vermiştir.

4.2.3. BİYOMETRİK S-KUTULAR İLE KARŞILAŞTIRILMASI

Literatürde yer alan biyometrik s-kutularından Kadhim ve diğ. (2016) çalışmasında DNA dizilimi ile oluşturulan iki s-kutunun (DNA-1: (SHARED KEY = COMPUTER AND SERVER NAME = SCIENCE ve DNA-2: SHARED KEY = BOMPUTER AND SERVER NAME = SCIENCE) ve Farhan ve diğ. (2020) çalışmasında RNA dizilimi ile oluşturulan beş s-kutunun

(RNA-1: Secret key = ABC, RNA-2: Secret key = !kh, RNA-3: Secret key = U@m, RNA-4: Secret key = %:%, RNA-5: Secret key = %:%) NL, SAC, DU, DP, LAT, LP, BIC-NL ve BIC-SAC güvenlik metriklerinin sonuçları Tablo 4.18'de verilmiştir.

Tablo 4.18: Mevcut biyometrik s-kutuların sonuçları.

S-kutu	SAC	NL			DU	DP	LAT	LP	BIC-SAC	BIC-NL
		maks.	min.	yüzdesi (%)						
Kadhim ve diğ. (2016) DNA-1	0,4785	170	80	67	26	0,1016	48	0,1875	0,5020	103
Kadhim ve diğ. (2016) DNA-2	0,4524	182	54	45	58	0,2266	74	0,2891	0,4761	100
Farhan ve diğ. (2020) RNA-1	0,4890	168	74	62	16	0,0625	54	0,2109	0,4934	101
Farhan ve diğ. (2020) RNA-2	0,4824	172	84	70	12	0,0469	44	0,1719	0,4973	102
Farhan ve diğ. (2020) RNA-3	0,4971	164	92	77	12	0,0469	36	0,1406	0,5016	103
Farhan ve diğ. (2020) RNA-4	0,4741	184	72	60	14	0,0547	56	0,2188	0,4971	102
Farhan ve diğ. (2020) RNA-5	0,4932	166	84	70	12	0,0469	44	0,1719	0,5020	103

Literatürdeki biyometrik s-kutuların güvenlik parametrelerinin sonuçları parmak izi s-kutuları ile karşılaştırıldığında;

- Biyometrik s-kutuların en düşük SAC değeri 0,4524 ve en yüksek SAC değeri 0,4971'dir. En iyi s-kutunun 0,50 SAC değerine sahip olması gerekmektedir fakat hem Kadhim ve diğ. (2016) çalışmasındaki DNA s-kutuları hem de Farhan ve diğ. (2020) çalışmasındaki RNA s-kutuları ile bu değere ulaşılmamıştır. Önerilen 33 parmak izi s-kutularının hepsi biyometrik s-kutularına göre çok daha iyi SAC değerine sahiptir.
- Biyometrik s-kutuların en düşük NL yüzdesi %45 ile [54, 164] NL aralığındadır ve en yüksek NL yüzdesi %77 ile [92, 184] NL aralığındadır. Kadhim ve diğ. (2016)

çalışmasındaki DNA s-kutularının ortalama NL yüzdeleri ve Farhan ve diğ. (2020) çalışmasındaki RNA s-kutularının ortalama NL yüzdeleri %70 değerinin altında kalmıştır. Önerilen parmak izi s-kutularının ortalama yüzdeleri %70 değerinin üzerindedir. Önerilen 33 parmak izi s-kutularının hepsi hem DNA hem de RNA ile oluşturulan s-kutularına göre çok daha iyi NL değerine sahiptir.

- Biyometrik s-kutuların en düşük DU değeri 12 ve en yüksek DU değeri 58'dir. Önerilen 33 parmak izi s-kutudan tümü bu aralıkta DU değerine sahiptir. Önerilen parmak izi s-kutularının hepsi Kadhim ve diğ. (2016) çalışmasındaki DNA s-kutularına göre daha iyi diferansiyel dağılım özelliğine sahiptir. Önerilen parmak izi s-kutularının %79'u Farhan ve diğ. (2020) çalışmasındaki RNA ile oluşturulan s-kutulara göre daha iyi diferansiyel dağılım özelliğine sahiptir.
- Biyometrik s-kutuların en düşük DP değeri 0,0469 ve en yüksek DP değeri 0,2266'tir. Önerilen 33 parmak izi s-kutudan tümü bu aralıkta DP değerine sahiptir. Önerilen parmak izi s-kutularının hepsi Kadhim ve diğ. (2016) çalışmasındaki DNA ile oluşturulan s-kutulara göre daha iyi diferansiyel olasılık özelliğine sahiptir. Önerilen parmak izi s-kutularının %79'u Farhan ve diğ. (2020) çalışmasındaki RNA ile oluşturulan s-kutulara göre daha iyi diferansiyel olasılık özelliğine sahiptir.
- Biyometrik s-kutuların en düşük LAT değeri 36 ve en yüksek LAT değeri 74'tür. Önerilen 33 parmak izi s-kutudan tümü bu aralıkta LAT değerine sahiptir. Önerilen parmak izi s-kutularının hepsi Kadhim ve diğ. (2016) çalışmasındaki DNA ile oluşturulan s-kutulara göre LAT özelliğini daha iyi sağlamaktadır. Önerilen parmak izi s-kutularının %94'ü Farhan ve diğ. (2020) çalışmasındaki RNA ile oluşturulan s-kutulara göre LAT özelliğini daha iyi sağlamaktadır.
- Biyometrik s-kutuların en düşük LP değeri 0,1406 ve en yüksek LP değeri 0,2891'dir. Önerilen 33 parmak izi s-kutudan tümü bu aralıkta LP değerine sahiptir. Önerilen parmak izi s-kutularının hepsi Kadhim ve diğ. (2016) çalışmasındaki DNA ile oluşturulan s-kutulara göre doğrusal olasılık özelliğini daha iyi sağlamaktadır. Önerilen parmak izi s-kutularının %94'ü Farhan ve diğ. (2020) çalışmasındaki RNA ile oluşturulan s-kutulara göre doğrusal olasılık özelliğini daha iyi sağlamaktadır.
- Biyometrik s-kutuların en düşük BIC-SAC değeri 0,4761 ve en yüksek BIC-SAC değeri 0,5020'dir. Önerilen 33 parmak izi s-kutularının hepsi biyometrik s-kutularına göre çok daha iyi BIC-SAC değerine sahiptir.

- Biyometrik s-kutuların en düşük BIC-NL değeri 100 ve en yüksek BIC-NL değeri 103'tür. Önerilen 33 parmak izi s-kutularının hepsi hem Kadhim ve diğ. (2016) çalışmasındaki DNA hem de Farhan ve diğ. (2020) çalışmasındaki RNA ile oluşturulan s-kutularına göre çok daha iyi BIC-NL değerine sahiptir.

Kadhim ve diğ. (2016) çalışmasındaki DNA s-kutuların ortalama SAC, NL yüzdesi, DU, DP, LAT, LP, BIC-SAC, BIC-NL değerleri sırasıyla 0,4655, %56, 42, 0,1641, 61, 0,2383, 0,4890, 102'dir. Farhan ve diğ. (2020) çalışmasındaki RNA s-kutuların ortalama SAC, NL yüzdesi, DU, DP, LAT, LP, BIC-SAC, BIC-NL değerleri sırasıyla 0,4872, %68, 13, 0,0516, 47, 0,1828, 0.4983, 102'dir. Biyometrik s-kutuların ortalama SAC, NL yüzdesi, DU, DP, LAT, LP, BIC-SAC, BIC-NL değerleri sırasıyla 0,4810, %64, 21, 0,0837, 51, 0,1987, 0,4957, 102'dir. Önerilen parmak izi s-kutularının güvenlik parametrelerinin ortalama değerleri ile biyometrik s-kutuların güvenlik parametrelerinin ortalama sonuçları karşılaştırıldığında parmak izi s-kutularının ortalama NL, SAC, DU, DP, LAT ve LP sonuçları biyometrik s-kutuların ortalama NL, SAC, DU, DP, LAT ve LP değerlerinden daha iyidir.

Biyometrik s-kutu oluşturma algoritmasının bir diğer önemli ölçütü algoritmanın s-kutu ve ters s-kutu üretimindeki yürütme süresidir. Kadhim ve diğ. (2016) çalışmasındaki DNA ve Farhan ve diğ. (2020) çalışmasındaki RNA ile oluşturulan s-kutuların ve ters s-kutuların oluşturulma süreleri milisaniye cinsinden Tablo 4.19'da verilmiştir.

Tablo 4.19: Biyometrik s-kutu ve ters s-kutu algoritmalarının yürütme süreleri.

Biyometrik S-kutu	S-kutu oluşturma süresi	Ters s-kutu oluşturma süresi
Kadhim ve diğ. (2016) DNA-1	0,216	0,240
Kadhim ve diğ. (2016) DNA-2	0,388	0,400
Farhan ve diğ. (2020) RNA-1	130	130
Farhan ve diğ. (2020) RNA-2	130	130
Farhan ve diğ. (2020) RNA-3	130	130
Farhan ve diğ. (2020) RNA-4	143	143
Farhan ve diğ. (2020) RNA-5	143	143

DNA s-kutusu oluşturma algoritmasının ortalama yürütme süresi 0,320 milisaniye, DNA ters s-kutusu oluşturma algoritmasının ortalama yürütme süresi 0,320 milisaniyedir. RNA s-kutusu

oluşturma algoritmasının ortalama yürütme süresi 135 milisaniye, RNA ters s-kutusu oluşturma algoritmasının ortalama yürütme süresi 135 milisaniyedir. Önerilen etkin biyometrik s-kutu oluşturma algoritmasının ortalama yürütme süresi 0,248 milisaniye, önerilen etkin biyometrik ters s-kutu oluşturma algoritmasının ortalama yürütme süresi 0,115 milisaniyedir. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasının yürütme süresi hem Kadhim ve diğ. (2016) çalışmasındaki DNA hem de Farhan ve diğ. (2020) çalışmasındaki RNA ile s-kutu ve ters s-kutu oluşturma algoritmalarına göre daha kısadır.

5. TARTIŞMA VE SONUÇ

Mobil cihaz kullanım oranın artışı ile her türlü işlemin bu cihazlar üzerinden kolay ve hızlı bir şekilde yapmaya teşvik eden mobil uygulamalarda artmıştır. Temassız işlemlerin büyük bir önem kazandığı son dönemlerde özellikle alışveriş yaparken temassız özelliği olmayan nakit, kredi kartı, banka kartı ile işlem yapmak yerine mobil cihaz üzerinde tanımlı uygulama ile alışverişler yapılmaya başlandı. Mobil uygulamalar, ödeme işlemlerinde birçok avantaj sağladığından mobil uygulama geliştiricileri için bu uygulamaların kullandığı verilerin güvenliği konusunu büyük önem taşımıştır. Mobil cihaz üzerinden yapılan işlemler arttıkça mobil uygulamalardaki veriler üçüncü şahısların güvenlik saldırıları için odak noktası haline gelmiştir.

Bir mobil ödeme sisteminin genel yapısına baktığımızda mobil uygulama için kullanıcı arayüzü, uygulamada veri saklama, işleme ve iletme işlemlerinin tanımlı olduğu kütüphanesi, işlem sırasında iletilmesi gereken verinin güvenliğinin sağlandığı güvenli kanal yönetimi ve temassız iletişimi sağlamak için NFC kontrolcüsü modüllerine sahiptir. Mobil ödeme sistemlerinde kullanılacak verilerin güvenliği için en çok kullanılan ve daha güvenli olan AES algoritması tercih edilmiştir. Sistem beyaz kutu şifreleme modeli üzerine kurulduğundan sistem ile ilgili tüm kaynakların açık olması bilinen AES algoritmasının kullanılması yeterince güvenli olmayacaktı. Bu yüzden, AES algoritmasının en önemli elementlerinde olan s-kutusunda değişiklik yapıldı. Literatürde indirgenemez polinomla üretilen, kaotik sistemlerle üretilen ve DNA şifreleme yöntemini kullanarak üretilen çok sayıda s-kutu bulunmaktaydı. Fakat hiçbir çalışma kişinin kendine ait biyometrik verisi ile bir s-kutu oluşturmamaktaydı. Mevcut çalışmalarda kullanılan biyometrik veriler var olan biyometrik veritabanlarını kullanmaktaydı. Mevcut biyometrik veritabanlarını kullanmak o veritabanının üçüncü şahısların eline geçmesi ile sistemin saldırıya açık olması anlamına geliyordu. Seçilecek biyometrik veri mevcut veritabanlarından kullanılmayacağından tüm mobil cihazlarda okunabilir olması gerekiyordu. Hemen hemen tüm mobil cihazlarda okuyucusu bulunan her kişiye göre en yüksek düzeyde farklılık gösteren eşsiz parmak izi biyometrik verisi kullanılmıştır.

Bu tez çalışmasında, yeni, basit ve etkili parmak izi s-kutusu oluşturmak için etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması önerilmiştir. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile oluşturulan parmak izi s-kutularının güvenlik açısından

uygunluğu doğrusal olmama, katı çığ kriteri, doğrusal dağılım, doğrusal olasılık, diferansiyel yaklaşım tablo değeri, diferansiyel olasılık, bit bağımsızlık kriteri, bütünlük, rastgelelik, güvenilirlik aralığı metrikleri ile test edilmiştir. Aynı zamanda önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasının yürütme süreleri de hesaplanmıştır.

Parmak izi s-kutuları önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasında tercih edilen parmak izi özelliğine göre farklı performans sonuçları üretmiştir. Tüm güvenlik metriklerinin sonuçlarına bakıldığında parmak izinin hat sonu özelliği ile önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritmasından elde edilen parmak izi s-kutuları en iyi sonuçları vermiştir. Parmak izi özelliği ile elde edilen çatallanma, hat sonu, çatallanma-hat sonu s-kutularının güvenlik performans metrikleri sonuçlarına göre;

- Çatallanma özelliği ile oluşturulan parmak izi s-kutularının SAC değerlerinin ortalaması 0,4950, hat sonu özelliği ile oluşturulan parmak izi s-kutularının SAC değerlerinin ortalaması 0,5011, hem çatallanma hem de hat sonu özelliği ile oluşturulan parmak izi s-kutularının SAC değerlerinin ortalaması 0,4902 olarak hesaplanmıştır. Katı çığ kriteri açısından en iyi parmak izi s-kutuları parmak izinin hat sonu özelliğini kullanılarak oluşturulan s-kutularında elde edilmiştir.
- Çatallanma özelliği ile oluşturulan parmak izi s-kutularının doğrusal olmama yüzde değerlerinin ortalaması %73, hat sonu özelliği ile oluşturulan parmak izi s-kutularının doğrusal olmama yüzde değerlerinin ortalaması %75, hem çatallanma hem de hat sonu özelliği ile oluşturulan parmak izi s-kutularının doğrusal olmama yüzde değerlerinin ortalaması %70 olarak hesaplanmıştır. Önerilen parmak izi s-kutularının tümü %70 oranında doğrusal olmadığı görülmüştür.
- Çatallanma özelliği ile oluşturulan parmak izi s-kutularının diferansiyel yaklaşım tablo ve diferansiyel olasılık değerlerinin ortalaması sırasıyla 15 ve 0,0582, hat sonu özelliği ile oluşturulan parmak izi s-kutularının diferansiyel yaklaşım tablo ve diferansiyel olasılık değerlerinin ortalaması sırasıyla 12 ve 0,0469, hem çatallanma hem de hat sonu özelliği ile oluşturulan parmak izi s-kutularının diferansiyel yaklaşım tablo ve diferansiyel olasılık değerlerinin ortalaması sırasıyla 17 ve 0,0653 olarak hesaplanmıştır. DP değeri ne kadar düşük ise oluşan s-kutu diferansiyel saldırılara karşı daha dayanıklıdır. Parmak izi özelliklerine göre hat sonu özelliği ile oluşturulan parmak izi s-kutuları diferansiyel saldırılara karşı daha dayanıklıdır. Önerilen parmak izi s-

kutularının tümü en kötü 0,0653 diferansiyel olasılık ile diferansiyel saldırılara karşı dayanıklıdır.

- Çatallanma özelliği ile oluşturulan parmak izi s-kutularının doğrusal dağılım ve doğrusal olasılık değerlerinin ortalaması sırasıyla 40 ve 0,1555, hat sonu özelliği ile oluşturulan parmak izi s-kutularının doğrusal dağılım ve doğrusal olasılık değerlerinin ortalaması sırasıyla 38 ve 0,1484, hem çatallanma hem de hat sonu özelliği ile oluşturulan parmak izi s-kutularının doğrusal dağılım ve doğrusal olasılık değerlerinin ortalaması sırasıyla 44 ve 0,1719 olarak hesaplanmıştır. LP değeri ne kadar düşük ise oluşan s-kutu doğrusal saldırılara karşı o kadar dayanıklıdır. Parmak izi özelliklerine göre hat sonu özelliği ile oluşturulan parmak izi s-kutuları doğrusal saldırılara karşı daha dayanıklıdır. Önerilen parmak izi s-kutularının tümü en kötü 0,1719 doğrusal olasılık ile doğrusal saldırılara karşı dayanıklıdır.
- Çatallanma özelliği ile oluşturulan parmak izi s-kutularının BIC-SAC değerlerinin ortalaması 0,4990, hat sonu özelliği ile oluşturulan parmak izi s-kutularının BIC-SAC değerlerinin ortalaması 0,5005, hem çatallanma hem de hat sonu özelliği ile oluşturulan parmak izi s-kutularının BIC-SAC değerlerinin ortalaması 0,4966 olarak hesaplanmıştır. Önerilen parmak izi s-kutularının tümü ideal BIC-SAC değerini sağlamaktadır. Bit bağımsızlık kriteri için katı çığ kriteri açısından en iyi değer parmak izinin hat sonu özelliğini kullanılarak oluşturulan parmak izi s-kutularında elde edilmiştir.
- Çatallanma özelliği ile oluşturulan parmak izi s-kutularının BIC-NL değerlerinin ortalaması 102, hat sonu özelliği ile oluşturulan parmak izi s-kutularının BIC-NL değerlerinin ortalaması 103, hem çatallanma hem de hat sonu özelliği ile oluşturulan parmak izi s-kutularının BIC-SAC değerlerinin ortalaması 102 olarak hesaplanmıştır. Bit bağımsızlık kriteri için doğrusal olmama metriği açısından en iyi değer parmak izinin hat sonu özelliğini kullanılarak oluşturulan parmak izi s-kutularında elde edilmiştir.

S-kutuların doğrusal saldırılara karşı dayanıklılığı s-kutunun LP değeri ile ters orantılıdır. LP değeri ne kadar düşük ise s-kutu doğrusal saldırılara karşı o kadar dayanıklıdır. Önerilen parmak izi s-kutularının doğrusal olasılık değerlerinin ortalaması 0,1586 iken mevcut DNA s-kutularının doğrusal olasılık değerlerinin ortalaması 0,2383 ve mevcut RNA s-kutularının doğrusal olasılık değerlerinin ortalaması 0,1828 olarak hesaplanmıştır. Elde edilen sonuçlar

gösteriyor ki önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile oluşturulan parmak izi s-kutuları hem DNA hem de RNA s-kutularına göre doğrusal saldırılara karşı daha dayanıklıdır.

S-kutuların diferansiyel saldırılara karşı dayanıklılığı s-kutunun DP değeri ile ters orantılıdır. DP değeri ne kadar düşük ise s-kutu doğrusal saldırılara karşı o kadar dayanıklıdır. Önerilen parmak izi s-kutularının diferansiyel olasılık değerlerinin ortalaması 0,0568 iken mevcut DNA s-kutularının diferansiyel olasılık değerlerinin ortalaması 0,1641 ve mevcut RNA s-kutularının diferansiyel olasılık değerlerinin ortalaması 0,0516 olarak hesaplanmıştır. Elde edilen sonuçlar gösteriyor ki önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile oluşturulan parmak izi s-kutuları RNA s-kutuları ile hemen hemen aynı dayanıklılıktayken DNA s-kutularına göre diferansiyel saldırılara karşı daha dayanıklıdır.

Mevcut kaotik s-kutularına göre önerilen parmak izi s-kutularının tümünün %91'i katı çığ kriterini, %85'i doğrusal olmama özelliğini, %79'u diferansiyel dağılım ve diferansiyel olasılık özelliğini, %85'i doğrusal dağılım ve olasılık özelliğini, %91'i bit bağımsızlık kriteri için katı çığ kriteri özelliğini, %97'si bit bağımsızlık kriteri için doğrusal olmama özelliğini sağlamıştır.

Önerilen parmak izi s-kutularının tümü mevcut biyometrik s-kutularına göre çok daha iyi güvenlik performans sonuçları sağlamıştır. Önerilen parmak izi s-kutularının SAC değerlerinin ortalaması 0,4954 iken mevcut biyometrik s-kutularının ortalama SAC değeri 0,4810, önerilen parmak izi s-kutularının NL yüzdesinin ortalaması %73 iken mevcut biyometrik s-kutularının NL yüzdesinin ortalaması %51, önerilen parmak izi s-kutularının diferansiyel olasılık değerlerinin ortalaması 0,0568 iken mevcut biyometrik s-kutularının diferansiyel olasılık değerlerinin ortalaması 0,0837, önerilen parmak izi s-kutularının doğrusal olasılık değerlerinin ortalaması 0,1586 iken mevcut biyometrik s-kutularının doğrusal olasılık değerlerinin ortalaması 0,1987, önerilen parmak izi s-kutularının BIC-SAC değerlerinin ortalaması 0,4987 iken mevcut biyometrik s-kutularının ortalama BIC-SAC değeri 0,4957, hem önerilen parmak izi s-kutularının hem de mevcut biyometrik s-kutularının BIC-NL değerlerinin ortalaması 102 olarak hesaplanmıştır.

Mobil ödeme sistemlerinde işlemin hızlı olması güvenliği kadar önemlidir. Şifreleme algoritmasında yapılan değişikliğin şifreleme işleminin süresine eklentisi en az olacak şekilde tasarlanmaktadır. Önerilen etkin biyometrik s-kutu oluşturma algoritmasının ortalama yürütme

süresi 0,248 milisaniye ile mevcut biyometrik s-kutulardan daha kısa sürede s-kutu oluşturmaktadır. Önerilen etkin biyometrik ters s-kutu oluşturma algoritmasının ortalama yürütme süresi 0,115 milisaniye ile mevcut biyometrik s-kutulardan daha kısa sürede s-kutu oluşturmaktadır.

Mobil uygulama içerisinde kişisel verilerin saklanması için kullanılan algoritmanın kişiye özel parametreler içererek daha eşsiz ve güvenilir bir algoritmanın geliştirilmesi çalışmanın literatüre katkısıdır. Bilindiği kadarıyla, literatürde blok şifreleme algoritmalarının en önemli parçası olan s-kutu oluşturulmasında kişinin parmak izinin kullanıldığı başka bir çalışma yoktur. Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile elde edilen parmak izi s-kutularının güvenlik metriklerinin sonuçlarına göre elde ettiği başarısı göz önünde bulundurularak, algoritma; benzersiz ve rastgele parmak izi s-kutusunun şifreleme algoritmaları için mobil cihazlarda kullanılabilirliğini garanti etmektedir. Çalışmanın ileriki aşamalarında parmak izi s-kutularının şifreleme algoritmalarında kullanılması planlanmaktadır.

Tez çalışmasının geliştirilmesi kapsamında, mobil ödeme sistemlerinde verinin iletimi sırasında POS ve cihaz arasındaki iletişim, GSM protokolünden kaynaklanan açıklar, akıllı cihaza yönelik saldırılar, mobil ödeme sisteminde kullanılan iletişim teknolojilerine yönelik dinleme, veri bozulması, veri değiştirilmesi, araya girme ve tekrarlamaya yönelik güvenlik risklerine karşı güvenlik çözümlerinin belirlenmesi ile sistemin güvenilirliğini arttırmaya yönelik yeni çalışmalar geliştirilebilir.

KAYNAKLAR

Abuguba, S., Milosavljevic, M.M., Macek, N., 2015, An efficient approach to generating cryptographic keys from face and iris biometrics fused at the feature level, *International Journal of Computer Science and Network Security (IJCSNS)*, 15(6), 6-11.

Adams, C., and Tavares, S., 1990, Good S-Boxes Are Easy To Find, *Conference on the Theory and Application of Cryptology, Advances in Cryptology — CRYPTO' 89*, 20-24 Ağustos 1989, Santa Barbara, CA, USA, Lecture Notes in Computer Science, Springer, New York, NY, 978-0-387-97317-3, 612-615.

Ahmad, M., Bhatia, D., Hassan, Y., 2015, A novel ant colony optimization based scheme for substitution box design, *Procedia Computer Science*, 57(2015), 572-580.

Ahmad, M., ve Malik, M., 2016, Design of chaotic neural network based method for cryptographic substitution box, *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, 3-5 Mart 2016, Chennai, India, IEEE, 978-1-4673-9939-5, 864-868.

Ahmad, M., Mittal, N., Garg, P., Khan, M.M., 2016, Efficient cryptographic substitution box design using travelling salesman problem and chaos, *Perspectives in Science*, 8, 465-468.

Ahmed, H.A., Zolkipli, M.F., Ahmad, M., 2019, A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map, *Neural Computing and Applications*, 31(11), 7201-7210.

Al Solami, E., Ahmad, M., Volos, C., Doja, M.N., Beg, M.M.S., 2018, A new hyperchaotic system-based design for efficient bijective substitution-boxes, *Entropy*, 20(7), 525.

Altaleb, A., Saeed, M.S., Hussain, I., Aslam, M., 2017, An algorithm for the construction of substitution box for block ciphers based on projective general linear group, *AIP Advances*, 7(3), 035116.

Al-Wattar, A.H.S., Mahmod, R., Zukarnain, Z.A., Udzir, N. I., 2015a, Generating a new s-box inspired by biological DNA, *International Journal of Computer Science and Application*, 4(1), 32-42.

Al-Wattar, A.H.S., Mahmod, R., Zukarnain, Z.A., Udzir, N.I., 2015b, A new DNA-based s-box, *International Journal of Engineering & Technology IJET-IJENS*, 15(4), 1-9.

Alzaidi, A.A., Ahmad, M., Doja, M.N., Solami, E.A., Beg, M.M.S., 2018, A New 1D Chaotic Map and β -Hill Climbing for Generating Substitution-Boxes, *IEEE Access*, 6, 55405-55418.

Ang, R., Safavi-Naini, R., McAven, L., 2005, Cancelable Key-Based Fingerprint Templates, *Australasian Conference on Information Security and Privacy - ACISP 2005*, 4-6 Temmuz 2005, Brisbane, QLD, Australia, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 3574, 978-3-540-26547-4, 242-252.

Arrañaga, J.D.R., Chavarin, J.A.S., Panduro, J.J.R., Alvarez, E.C.B., 2017, New s-box calculation for Rijndael-AES based on an artificial neural network, *Electrónica*, 6(2), 49-69.

Azhar, I., Ahmed, N., Abbasi, A.G., Kiani, A., Shibli, A., 2014, Keeping secret keys secret in open systems, *2014 International Conference on Open Source Systems & Technologies*, 18-20 Aralık 2014, Lahore, Pakistan, IEEE, 978-1-4799-2054-9, 100-104.

Bankalararası Kart Merkezi, 2014, Giyilebilir cihazlarla ilk ödeme deneyimi, *BKM Kart Monitör Araştırması 2014*, 10.

Bankalararası Kart Merkezi, 2017, Geleceğimiz daha fazla mobil ödeme, *BKM Kart Monitör Araştırması 2017*, 11.

Bankalararası Kart Merkezi, 2020, Mektupla/ Telefonla Sipariş ve İnternette Yapılan Kartlı Ödeme İşlemleri, [16.09.2020].

Belazi, A., and Abd El-Latif, A.A., 2017, A simple yet efficient S-box method based on chaotic sine map, *Optik*, 130, 1438-1444.

Belazi, A., Abd El-Latif, A.A., Diaconu, A.-V., Rhouma, R., Belghith, S., 2017a, Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms, *Optics and Lasers in Engineering*, 88, 37-50.

Belazi, A., Khan, M., Abd El-Latif, A.A., Belghith, S., 2017b, Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption, *Nonlinear Dynamics*, 87(1), 337-361.

Beunardeau, M., Connolly, A., Géraud, R., Naccache, D., 2016, White-Box Cryptography: Security in an Insecure Environment, *IEEE Security & Privacy*, 14(5), 88-92.

Billet, O., ve Gilbert, H., 2003, A Traceable Block Cipher, *International Conference on the Theory and Application of Cryptology and Information Security - ASIACRYPT 2003*, 30 Kasım-4 Aralık 2003, Taipei, Taiwan, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 978-3-540-20592-0, 331-346.

Billet, O., Gilbert, H., Ech-Chatbi, C., 2004, Cryptanalysis of a White Box AES Implementation, *International Workshop on Selected Areas in Cryptography-SAC 2004*, 9-10 Ağustos 2004, Waterloo, ON, Canada, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 978-3-540-24327-4, 227-240.

Brostoff, S., and Sasse, M.A., 2000, Are Passfaces more usable than passwords? A field trial investigation, People and computers XIV—usability or else!, *Springer*, 978-1-85233-318-8, 405-424.

Canright, D., 2005, A Very Compact S-Box for AES, *International Workshop on Cryptographic Hardware and Embedded Systems - CHES 2005*, 29 Ağustos- 1 Eylül 2005, Edinburgh, United Kingdom, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 3659, 978-3-540-28474-1, 441-455.

Chandrasekharappa, T.G.S., Prema, K.V., Shama, K., 2011, S-boxes generated using affine transformation giving maximum avalanche effect, *International Journal on Computer Science and Engineering*, 3(9), 3185.

Chang, Y-J., Zhang, W., Chen, T., 2004, Biometrics-based cryptographic key generation, *2004 IEEE International Conference on Multimedia and Expo (ICME) (IEEE Cat. No.04TH8763)*, 27-30 Haziran, Taipei, Taiwan, IEEE, 0-7803-8603-5, 2203-2206.

Chen, G., 2008, A novel heuristic method for obtaining S-boxes, *Chaos, Solitons & Fractals*, 36(4), 1028-1036.

Chen, B. and Chandran, V., Biometric Based Cryptographic Key Generation from Faces, 2007, *9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications (DICTA 2007)*, 3-5 Aralık 2007, Glenelg, Australia, IEEE, 0-7695-3067-2, 394-401.

Chen, G., Chen, Y., Liao, X. 2007, An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps, *Chaos, Solitons & Fractals*, 31(3), 571-579.

Chow, S., Eisen, P., Johnson, H., Van Oorschot, P.C., 2003a, White-Box Cryptography and an AES Implementation, *International Workshop on Selected Areas in Cryptography-SAC 2002*, 15-16 Ağustos 2002, St. John's, NF, Canada, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 978-3-540-00622-0, 250-270.

Chow, S., Eisen, P., Johnson, H., Van Oorschot, P.C., 2003b, A White-Box DES Implementation for DRM Applications, *ACM Workshop on Digital Rights Management-DRM 2002*, 18 Kasım 2002, Washington, DC, USA, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 978-3-540-40410-1, 1-15.

Connie, T., Teoh, A., Goh, K.O.M., Ngo, D., 2005, PalmHashing: A novel approach for cancelable biometrics, *Information Processing Letters*, 93(1), 1-5.

Costanzo, C., 2004, Biometric Cryptography: Key Generation Using Feature and Parametric Aggregation.

Cui, L., and Yuanda, C., 2007, A new S-box structure named Affine-Power-Affine, *International Journal of Innovative Computing, Information and Control*, 3(3), 751-759.

Çavuşoğlu, Ü., Zengin, A., Pehlivan, I., Kaçar, S., 2017, A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system, *Nonlinear Dynamics*, 87(2), 1081-1094.

Daemen J., and Rijmen V., 2000, The Block Cipher Rijndael, *International Conference on Smart Card Research and Advanced Applications - CARDIS 1998*, 14-16 Eylül 1998, Louvain-la-Neuve, Belgium, Lecture Notes in Computer Science, Berlin, Heidelberg, 978-3-540-67923-3, 227-284.

Daemen, J., and Rijmen,V., 2002, The Design of Rijndael: AES - The Advanced Encryption Standard, *Springer*, Berlin Heidelberg, 978-3-662-04722-4.

Dandawate, Y.H., and Inamdar, S.R., 2015, Fusion based Multimodal Biometric cryptosystem, *2015 International Conference on Industrial Instrumentation and Control (ICIC)*, 28-30 Mayıs 2015, Pune, India, IEEE, 978-1-4799-7165-7, 1484-1489.

Das, I., Nath, S., Roy, S., Mondal, S., 2012, Random S-Box generation in AES by changing irreducible polynomial, *2012 International Conference on Communications, Devices and Intelligent Systems (CODIS)*, 28-29 Aralık 2012, Kolkata, India, IEEE, 978-1-4673-4699-3, 556-559.

Das, S., Zaman, J. U., Ghosh, R., 2013, Generation of AES S-Boxes with various modulus and additive constant polynomials and testing their randomization, *Procedia Technology*, 10, 957-962.

Delerablée, C., Lepoint, T., Paillier, P., Rivaini M., 2014, White-Box Security Notions for Symmetric Encryption Schemes, *International Conference on Selected Areas in Cryptography - SAC 2013*, 14-16 Ağustos 2014, Burnaby, BC, Canada, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 978-3-662-43413-0, 247-264.

Diffie, W., and Hellman, M., 1976a, New directions in cryptography, *IEEE transactions on Information Theory*, 22(6), 644-654.

Diffie, W., and Hellman, M., 1976b, Multiuser cryptographic techniques, *National computer conference and exposition (AFIPS '76)*, 7-10 Haziran 1976, Association for Computing Machinery, New York, NY, USA, 109-112.

Dhamija, R., and Perrig, A., 2000, Deja Vu-A User Study: Using Images for Authentication, *Proceedings of the 9th Conference on USENIX Security Symposium*, 14-17 Ağustos 2000, Denver, Colorado, USA, Berkeley, CA, United States, USENIX Association, 9, 4-4.

Dworkin, M.J., Barker, E.B., Nechvatal, J.R., Foti, J., Bassham, L.E., Roback, E., Dray Jr. J.F., 2001, Advanced Encryption Standard (AES) (FIPS PUB 197), *National Institute of Standards and Technology (NIST)*, United State.

Faquih, A., Kadam P., Saquib, Z., 2015, Cryptographic techniques for wireless sensor networks: A survey, *2015 IEEE Bombay Section Symposium (IBSS)*, 10-11 Eylül 2015, Mumbai, India, IEEE, 978-1-4673-9542-7, 1-6.

Farah, T., Rhouma, R., Belghith, S., 2017, A novel method for designing S-box based on chaotic map and Teaching–Learning-Based Optimization, *Nonlinear Dynamics*, 88(2), 1059-1071.

Farhan, A.K., Ali, R.S., Yassein, H.R., Al-Saidi, N.M.G., Abdul-Majeed, G.H., 2020, A new approach to generate multi s-boxes based on RNA computing, *International Journal of Innovative Computing, Information and Control*, 16(1), 331-348.

Farwa, S., Shah, T., Idrees, L., 2016, A highly nonlinear S-box based on a fractional linear transformation, *Springer Plus*, 5(1).

Faugère, J.-C., and Perret L., 2006, Polynomial Equivalence Problems: Algorithmic and Theoretical Aspects, *Annual International Conference on the Theory and Applications of*

Cryptographic Techniques - EUROCRYPT 2006, 28 Mayıs-1 Haziran 2006, St. Petersburg, Russia, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 978-3-540-34546-6, 30-47.

Feistel, H., 1973, Cryptography and Computer Privacy, *Scientific American*, 228(5), 15-23.

Gangadari, B. R., and Ahamed, S. R., 2015, Analysis and algebraic construction of S-Box for AES algorithm using irreducible polynomials, *2015 Eighth International Conference on Contemporary Computing (IC3)*, 20-22 Ağustos 2015, Noida, India, IEEE, 978-1-4673-7947-2, 526-530.

Gehani, A., LaBean, T., Reif, J., 2003, DNA-based Cryptography, *Aspects of Molecular Computing*, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 167-188.

Gong, L., Pan, J., Liu, B., Zhao, S., 2013, A novel one-time password mutual authentication scheme on sharing renewed finite random sub-passwords, *Journal of Computer and System Sciences*, 79(1), 122-130.

Gong, Y., Deng, K., Shi, P., 2008, PKI Key Generation Based on Iris Features, *2008 International Conference on Computer Science and Software Engineering*, 12-14 Aralık 2008, Hubei, China, IEEE, 978-0-7695-3336-0, 166-169.

Gueron, S., 2013, White Box AES Using Intel's New AES Instructions, *2013 10th International Conference on Information Technology: New Generations*, 15-17 Nisan 2013, Las Vegas, NV, USA, IEEE, 978-0-7695-4967-5, 417-421.

Guesmi, R., Farah, M.A.B., Kachouri, A., Samet, M., 2014, A novel design of Chaos based S-Boxes using genetic algorithm techniques, *2014 IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA)*, 10-13 Kasım 2014, Doha, Qatar, IEEE, 978-1-4799-7100-8, 678-684.

Hao, F., Anderson, R., Daugman, J., 2006, Combining Crypto with Biometrics Effectively, *IEEE Transactions on Computers*, 55(9), 1081-1088.

Huang, Y., Huang, Z., Zhao, H., Lai, X., 2013, A new one-time password method, *IERI Procedia*, 4(2013), 32-37.

Jagadeesan, A., and Duraiswamy, K., 2010, Secured cryptographic key generation from multimodal biometrics: feature level fusion of fingerprint and iris, *International Journal of Computer Science and Information Security*, 7(2), 028-037.

Jakimoski, G., and Kocarev, L., 2001, Chaos and cryptography: block encryption ciphers based on chaotic maps, *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 48(2), 163-169.

Jamal, S.S., Khan, M.U., Shah, T. A, 2016, Watermarking Technique with Chaotic Fractional S-Box Transformation, *Wireless Personal Communications*, 90(4), 2033-2049.

Jansen, W., 2003, Authenticating users on handheld devices, *In Proceedings of the Canadian Information Technology Security Symposium*, Mayıs 2003, 1-12.

Jansen, W., 2004, Authenticating mobile device users through image selection, *WIT transactions on information and communication technologies*, 30.

Jia, Y., Lin, T., Lai, X., 2016, A generic attack against white box implementation of block ciphers, *2016 International Conference on Computer, Information and Telecommunication Systems (CITS)*, 6-8 Temmuz 2016, Kunming, China, IEEE, 978-1-5090-0690-8, 1-5.

Jo J.-G., Seo J.-W., Lee H.-W., 2007, Biometric Digital Signature Key Generation and Cryptography Communication Based on Fingerprint, *International Workshop on Frontiers in Algorithmics, FAW 2007*, 1-3 Ağustos 2007, Lanzhou, China, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 978-3-540-73813-8, 38-49.

Juremi, J., Mahmod, R., Zukarnain, Z.A., Yasin, S., Md., 2017, Modified AES s-box based on determinant matrix algorithm, *International Journal of Advanced Research in Computer Science and Software Engineering*, 7(1), 110-116.

Kadhim, F.A., Majeed, G.H.A., Ali, R.S., 2016, Proposal new s-box depending on DNA computing and mathematical operations, *2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA)*, 9-10 Mayıs 2016, Baghdad, Iraq, IEEE, 978-1-5090-3247-1, 1-6.

Kalaiselvi, K., and Kumar, A., 2016, Enhanced AES cryptosystem by using genetic algorithm and neural network in S-box, *2016 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC)*, 10-11 Mart 2016, Bangalore, India, IEEE, 978-1-5090-1936-6, 1-6.

Karroumi, M., 2011, Protecting White-Box AES with Dual Ciphers, *International Conference on Information Security and Cryptology - ICISC 2010*, 1-3 Aralık 2010, Seoul, Korea (Republic of), Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 978-3-642-24208-3, 278-291.

Khan, M., 2015, A novel image encryption scheme based on multiple chaotic S-boxes, *Nonlinear Dynamics*, 82(1-2), 527-533.

Khan, M.F., Ahmed, A., Saleem, K., 2019a, A Novel Cryptographic Substitution Box Design Using Gaussian Distribution, *IEEE Access*, 7, 15999-16007.

Khan, M.F., Ahmed, A., Saleem, K., Shah, T., 2019b, A Novel Design of Cryptographic SP-Network Based on Gold Sequences and Chaotic Logistic Tent System, *IEEE Access*, 7, 84980-84991.

Khan, M., and Asghar, Z., 2018, A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S8 permutation, *Neural Computing & Applications*, 29(4), 993-999.

Khan, M., and Shah, T., 2014, A novel image encryption technique based on Hénon chaotic map and S8 symmetric group, *Neural Computing & Applications*, 25(7-8), 1717-1722.

Khan, M., and Shah, T., 2015, An efficient construction of substitution box with fractional chaotic system, *Signal, Image and Video Processing*, 9(6), 1335-1338.

Khan, M., Shah, T., Gondal, M.A., 2013, An efficient technique for the construction of substitution box with chaotic partial differential equation, *Nonlinear Dynamics*, 73(3), 1795-1801.

Khan, M., Shah, T., Mahmood, H., Gondal, M.A., Hussain, I., 2012, A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems, *Nonlinear Dynamics*, 70(3), 2303-2311.

Khitrov, M., 2013, Talking passwords: voice biometrics for data access and security, *Biometric Technology Today*, 2013(2), 9-11.

Kocarev, L., and Lian, S., 2011, Chaos based cryptography theory algorithms and applications, *Springer Science & Business Media*, Berlin, I 978-3-642-20541-5.

Kumar, P., and Rana, S.B., 2016, Development of modified AES algorithm for data security, *Optik*, 127(4), ISSN 0030-4026, 2341-2345.

Lambić, D., 2014, A novel method of s-box design based on chaotic map and composition method, *Chaos, Solitons & Fractals*, 58, 16-21.

Lambić, D., 2017, A novel method of S-box design based on discrete chaotic map, *Nonlinear Dynamics*, 87(4), 2407-2413.

Lambić, D., 2020, A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design, *Nonlinear Dynamics*, 100, 699-711.

Lamport, L., 1981, Password authentication with insecure communication, *Communications of the ACM*, 24(11), 770-772.

Lepoint, T., Rivain, M., De Mulder, Y., Roelse, P., Preneel, B., 2014, Two Attacks on a White-Box AES Implementation, *International Conference on Selected Areas in Cryptography-SAC 2013*, 14-16 Ağustos 2013, Burnaby, BC, Canada, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 978-3-662-43413-0, 265-285.

Liu, G., Yang, W., Liu, W., Dai, Y., 2015, Designing S-boxes based on 3-D four-wing autonomous chaotic system, *Nonlinear Dynamics*, 82(4), 1867-1877.

Lu, Q.; Zhu, C.; Wang, G.A., 2019, Novel S-Box Design Algorithm Based on a New Compound Chaotic System, *Entropy*, 21(10), 1004.

Lu, Q., Zhu, C., Deng, X., 2020, An efficient image encryption scheme based on the LSS chaotic map and single s-box, *IEEE Access*, 8, 25664-25678.

Luo, R., Lai, X., You, R., 2014, A new attempt of white-box AES implementation, *Proceedings 2014 IEEE International Conference on Security, Pattern Analysis, and Cybernetics (SPAC)*, 18-19 Ekim 2014, Wuhan, China, IEEE, 978-1-4799-5353-0, 423-429.

Mahajan, Dr. P., and Sachdeva, A., 2013, A Study of Encryption Algorithms AES, DES and RSA for Security, *Global Journal of Computer Science and Technology Network, Web & Security*, 13(15), 15-22.

Mahmood Malik, M.S., Ali, M.A., Khan, M.A., Ehatisham-Ul-Haq, M., Shah, S. N. M., Rehman, M., Ahmad, W., 2020, Generation of Highly Nonlinear and Dynamic AES Substitution-Boxes (S-Boxes) Using Chaos-Based Rotational Matrices, *IEEE Access*, 8, 35682-35695.

Mathur, M., and Kesarwani, A., 2013, Comparison Between DES, 3DES, RC2, RC6, Blowfish and AES, *Proceedings of National Conference on New Horizons in IT - NCNHIT 2013*, 978-93-82338-79-6.

Michiels, W., Gorissen, P., Hollmann, H.D.L., 2009, Cryptanalysis of a Generic Class of White-Box Implementations, *International Workshop on Selected Areas in Cryptography-SAC 2008*, 14-15 Ağustos 2008, Sackville, NB, Canada, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 978-3-642-04158-7, 414-428.

Monrose, F., Reiter, M.K., Li, Q., Wetzel S., 2001, Using Voice to Generate Cryptographic Keys, *2001: A Speaker Odyssey - The Speaker Recognition Workshop*, 18-22 Haziran 2001, Crete, Greece, 237-242.

Moosavi, S.R., Nigussie, E., Virtanen, S., ve Isoaho, J., 2017, Cryptographic key generation using ECG signal, *14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 8-11 Ocak, Las Vegas, NV, USA, IEEE, 978-1-5090-6196-9, 1024-1031.

Nguyen, T.H.L., and Nguyen, T.T.H., 2008, An approach to protect Private Key using fingerprint Biometric Encryption Key in BioPKI based security system, *2008 10th International Conference on Control, Automation, Robotics and Vision*, 17-20 Aralık 2008, Hanoi, Vietnam, IEEE, 978-1-4244-2286-9, 1595-1599.

Ning, K., 2009, A Pseudo DNA Cryptography Method, *arXiv*.

Noughabi, M.N.A., and Sadeghiyan, B., 2010, Design of S-boxes based on neural networks*, *2010 International Conference on Electronics and Information Engineering*, 1-3 Ağustos 2010, Kyoto, Japan, IEEE, 978-1-4244-7679-4, 172-178.

Nyberg, K. 1994, Differentially uniform mappings for cryptography, *Workshop on the Theory and Application of of Cryptographic Techniques - EUROCRYPT '93*, 23-27 Mayıs 1993, Lofthus, Norway, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 765, 978-3-540-57600-6, 55-64.

Özkaynak, F., 2015, A novel method to improve the performance of chaos based evolutionary algorithms, *Optik*, 126(24), 5434-5438.

Özkaynak, F., 2017, From Biometric Data to Cryptographic Primitives: A New Method for Generation of Substitution Boxes, *Proceedings of the 2017 International Conference on Biomedical Engineering and Bioinformatics*, Eylül 2017, Bangkok, Thailand, New York, NY, USA, Association for Computing Machinery, 9781450352970, 27-33.

Özkaynak, F., 2019, Construction of robust substitution boxes based on chaotic systems, *Neural Computing and Applications*, 31(8), 3317-3326.

Özkaynak, F., Çelik, V., Özer, A.B., 2017, A new S-box construction method based on the fractional-order chaotic Chen system, Signal, *Image and Video Processing*, 11(4), 659-664.

Özkaynak, F., and Özer, A.B., 2010, A method for designing strong S-Boxes based on chaotic Lorenz system, *Physics Letters A*, 374(36), 3733-3738.

Özkaynak, F., and Yavuz, S., 2013, Designing chaotic S-boxes based on time-delay chaotic system, *Nonlinear Dynamics*, 74(3), 551-557.

Padmavathi, B., and Kumari, S. R., 2013, A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique, *International Journal of Science and Research (IJSR)*, 2(4), 170-174.

Panchal, G., and Samanta, D., 2016, Comparable features and same cryptography key generation using biometric fingerprint image, *2016 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)*, 27-28 Şubat 2016, Chennai, India, IEEE, 978-1-4673-9745-2, 691-695.

Patarin, J., 1996, Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms, *International Conference on the Theory and Applications of Cryptographic Techniques—EUROCRYPT '96*, 12-16 Mays 1996., Saragossa, Spain, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 978-3-540-61186-8, 33-48.

Peng, J., Zhang, D., Liao, X., 2011, A method for designing dynamical S-boxes based on hyperchaotic Lorenz system, *IEEE 10th International Conference on Cognitive Informatics and Cognitive Computing (ICCI-CC'11)*, 18-20 Ağustos 2011, Banff, AB, Canada, IEEE, 978-1-4577-1695-9, 304-309.

Rashid, M.T., and Zaki, H.A., 2014, RSA cryptographic key generation using fingerprint minutiae, *Iraqi Journal for Computers and Informatics (IJCI)*, 1(1), 66-69.

Ratha, N.K., Chikkerur, S., Connell, J.H., Bolle, R.M., 2007, Generating Cancelable Fingerprint Templates, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4), 561-572.

Rathgeb, C., and Uhl, A., 2009, Context-based texture analysis for secure revocable iris-biometric key generation, *3rd International Conference on Imaging for Crime Detection and Prevention (ICDP 2009)*, 3 Aralık 2009, London, UK, IEEE, 978-1-84919-207-1, 1-6.

Rivest, R.L., Shamir, A., Adleman, L., 1978, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, 21(2), 120-126.

Sakallı, M.T., Buluş, E., Büyüksaraçoğlu, F., Şahin, A., 2006, S Kutularında Doğrusal Eşitlik, *Sinyal İşleme ve İletişim Uygulamaları Kurultayı-SİU*, 17-19 Nisan Antalya-TÜRKİYE.

Santhi, B., Ravichandran, K.S., Arun, A.P., Chakkarapani, L., 2012, A novel cryptographic key generation method using image features, *Research Journal of Information Technology*, 4(2), 88-92.

Shankar, K., and Eswaran, P., 2016, A new k out of n secret image sharing scheme in visual cryptography, *2016 10th International Conference on Intelligent Systems and Control (ISCO)*, 7-8 Ocak 2016, Coimbatore, India, 978-1-4673-7807-9, 1-6.

Shi, Y., and He, Z., 2014, A lightweight white-box symmetric encryption algorithm against node capture for WSNs, *2014 IEEE Wireless Communications and Networking Conference (WCNC)*, 6-9 Nisan 2014, Istanbul, Turkey, IEEE, 1525-3511, 3058-3063.

Singhal, S., and Singhal, Dr. N., 2016, A Comparative Analysis of AES and RSA Algorithms, *International Journal of Scientific & Engineering Research*, 7(5), 149-151.

Singhvi, R.S., Venkatachalam, S.P., Kannan, P.M., Palanisamy, V., 2009, Cryptography key generation using biometrics, *2009 International Conference on Control, Automation, Communication and Energy Conservation*, 4-6 Haziran 2009, Perundurai, Tamilnadu, India, IEEE, 1-6.

Sinha, S.D., and Arya, C.P., 2012, Algebraic construction and cryptographic properties of Rijndael substitution box, *Defence Science Journal*, 62(1), 32.

Soutar, C., Roberge, D., Stoianov, A., Gilroy, R., Kumar, B. V., 1998, Biometric Encryption using image processing, *Proc. SPIE 3314, Optical Security and Counterfeit Deterrence Techniques II*, 1 Nisan 1998, San Jose, CA, United States.

Şengel, Ö., Aydın, M.A., Sertbaş, A., 2018, Comparison of Cryptography Algorithms for Mobile Payment Systems, *International Conference on Cyber Security and Computer Science (ICONCS 2018)*, 18-20 October 2018, Safranbolu, Karabük, Turkey, 150-155.

Şengel Ö., Aydın M.A., Sertbaş A., 2019, A Survey on White Box Cryptography Model for Mobile Payment Systems, *International Telecommunications Conference*, 28-29 Aralık 2017, Istanbul, Turkey, Lecture Notes in Electrical Engineering, Springer, Singapore, 978-981-13-0407-1, 215-225.

Şengel, Ö., Aydın, M.A., Sertbaş, A., 2020a, Determining the Cryptography Algorithm and Model for Mobile Payment Systems, *Acta-Infologica*, 4(1), 21-33.

Şengel, Ö., Aydın, M.A., Sertbaş, A., 2020b, An Efficient Generation and Security Analysis of Substitution Box Using Fingerprint Patterns, *IEEE Access*, 8, 160158-160176.

Tang, G., and Liao, X., 2005, A method for designing dynamical S-boxes based on discretized chaotic map, *Chaos, Solitons & Fractals*, 23(5), 1901-1909.

Tang, G., Liao, X., Chen, Y., 2005, A novel method for designing S-boxes based on chaotic maps, *Chaos, Solitons & Fractals*, 23(2), 413-419.

Tanyildizi E., and Özkaynak, F., 2019, A New Chaotic S-Box Generation Method Using Parameter Optimization of One Dimensional Chaotic Maps, *IEEE Access*, 7, 117829-117838.

Tian, Y., and Lu, Z., 2016, S-box: six-dimensional compound hyperchaotic map and artificial bee colony algorithm, *Journal of Systems Engineering and Electronics*, 27(1), 232-241.

Tian, Y., and Lu, Z., 2017, Chaotic S-Box Intertwining Logistic Map and Bacterial Foraging Optimization, *Hindawi Mathematical Problems in Engineering*, 2017.

Tiessen, T., Knudsen, L.R., Kölbl, S., Lauridsen, M.M., 2015, Security of the AES with a Secret S-Box, *International Workshop on Fast Software Encryption - FSE 2015*, 8-11 Mart 2015, Istanbul, Turkey, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 978-3-662-48115-8, 175-189.

Tolhuizen, L., 2012, Improved cryptanalysis of an AES implementation, *In: Proceedings of the 33rd WIC Symposium on Information Theory in the Benelux*, 68-71.

Tran, M.T., Doan, K.B., Anh, D.D., 2008, Gray S-box for advanced encryption standard, *International Conference on Computational Intelligence and Security*, 13-17 Aralık 2008, Suzhou, China, IEEE, 978-0-7695-3508-1, 253-258.

Ullah, A., Jamal, S.S., Shah, T., 2017, A novel construction of substitution box using a combination of chaotic maps with improved chaotic range, *Nonlinear Dynamics*, 88(4), 2757-2769.

Ullah, A., Jamal, S.S., Shah, T., 2018, A novel algebraic technique for the construction of strong substitution box, *Wireless Personal Communications*, 99(1), 213-226.

Uludag, U., Pankanti, S., Prabhakar, S., Jain, A.K., 2004, Biometric cryptosystems: issues and challenges, *in Proceedings of the IEEE*, 92(6), 948-960.

Wadi, S.M., and Zainal, N., 2013, Rapid Encryption Method based on AES Algorithm for Grey Scale HD Image Encryption, *Procedia Technology*, 11(2013), ISSN 2212-0173, 51-56.

Wang, Y., and Peng, L., 2012, An improved method to obtaining s-box based on chaos and genetic algorithm, *Transactions Hong Kong Institution of Engineers*, 19(4), 53-58.

Wang, Y., Wong, K.-W., Li, C., Li, Y., 2012, A novel method to design s-box based on chaotic map and genetic algorithm, *Physics Letters A*, 376(6-7), 827-833.

Webster, A.F., and Tavares, S.E., 1986, On the Design of S-Boxes, *Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology — CRYPTO '85*, 18-22 Ağustos 1985, Santa Barbara, CA, USA, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 978-3-540-16463-0, 523-534.

Wiedenbeck, S., Waters, J, Birget, J.-C., Brodskiy, A., Memon, N., 2005, Authentication using graphical passwords: Basic results, *Human-Computer Interaction International (HCII 2005)*, 25-27 Temmuz 2005, Las Vegas.

Wu, L., Liu, X., Yuan, S., Xiao, P., 2010, A novel key generation cryptosystem based on face features, *IEEE 10th International Conference On Signal Processing Proceedings*, 24-28 Ekim 2010, Beijing, China, IEEE, 978-1-4244-5897-4, 1675-1678.

Wu, X., Fredrikson, M., Jha, S., Naughton, J.F., 2016, A Methodology for Formalizing Model-Inversion Attacks, *2016 IEEE 29th Computer Security Foundations Symposium (CSF)*, 27 Haziran-1 Temmuz 2016, Lisbon, Portugal, IEEE, 2374-8303, 355-370.

Wyseur, B., Michiels, W., Gorissen, P., Preneel, B., 2007, Cryptanalysis of White-Box DES Implementations with Arbitrary External Encodings, *International Workshop on Selected Areas in Cryptography-SAC 2007*, 16-17 Ağustos 2007, Ottawa, ON, Canada, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 978-3-540-77359-7, 264-277.

Yang D., and Hwang, I., 2015, Security Enhancement Methods for Mobile POS System, *2nd ACM International Conference on Mobile Software Engineering and Systems*, 16-17 Mayıs 2015, Florence, Italy, IEEE, 978-0-7695-5566-9, 152-153.

Ye, T., and Zhimao, L., 2018, Chaotic S-box: six-dimensional fractional Lorenz–Duffing chaotic system and O-shaped path scrambling, *Nonlinear Dynamics*, 94, 2115-2126.

Yi, L., Tong, X., Wang, Z., Zhang, M., Zhu, H., Liu, J., 2019, A novel block encryption algorithm based on chaotic s-box for wireless sensor network, *IEEE Access*, 7, 53079-53090.

Vigila, S.A.M.C., Muneeswaran, K., Antony, W.T.B.A., 2015, Biometric security system over finite field for mobile applications, *IET Information Security*, 9(2), 119-126.

Zhang, H., Huang, W., Wang, Z., Chai, T., 2006, Adaptive synchronization between two different chaotic systems with unknown parameters, *Physics Letters A*, 350(5–6), 363-366.

Zhang, H., Liu, D., Wang, Z., 2009, Controlling chaos: suppression, synchronization and chaotification, *Springer Science & Business Media*, London, 978-1-84882-522-2.

Zhang, H., Ma, T., Huang, G., Wang, Z., 2010, Robust Global Exponential Synchronization of Uncertain Chaotic Delayed Neural Networks via Dual-Stage Impulsive Control, *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 40(3), 831-844.

Zhang, T., Chen, C.L.P., Chen, L., Xu X., Hu, B., 2018, Design of highly nonlinear substitution boxes based on I-Ching operators, *IEEE Transactions on Cybernetics*, 48(12), 3349-3358.

Zhang, Y.-Q., Hao, J.-L., Wang, X.-Y., 2020, An Efficient Image Encryption Scheme Based on S-Boxes and Fractional-Order Differential Logistic Map, *IEEE Access*, 8, 54175-54188.

EKLER

A. ÖNERİLEN ETKİN BİYOMETRİK S-KUTU VE TERS S-KUTU OLUŞTURMA ALGORİTMASINI KULLANARAK ELDE EDİLEN PARMAK İZİ S-KUTU ÖRNEKLERİ

EK-A.1: Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile elde edilen bir s-kutu ve sonuçları örneği-1.

SAC	NL			DU	DP	LAT	LP	BIC-SAC	BIC-NL
	maks.	min.	yüzdesi (%)						
0,5098	162	94	78	14	0,0547	34	0,1328	0,5019	103

satır \ sütun	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	8B	5C	57	99	22	33	3A	68	29	1B	1E	01	09	05	72	58
1	5A	52	5E	78	7E	4A	40	A7	44	FF	21	4B	73	69	74	48
2	34	79	87	7F	6B	56	D4	4D	6A	E3	1C	47	DD	16	AD	20
3	3C	92	04	D7	94	28	C0	A4	19	AC	B7	C4	1D	AB	CB	07
4	B5	BF	77	BA	85	1F	37	10	31	83	70	18	D9	DE	E8	E0
5	9F	3B	38	60	BE	F0	C7	55	82	8F	CC	D8	F6	51	35	26
6	EE	B4	11	D6	2D	B1	EC	42	24	3E	B6	E9	96	54	41	9C
7	88	E1	8A	9E	3D	E2	B8	65	39	49	F9	67	F3	0C	93	95
8	30	BD	2A	25	50	3F	E7	91	FE	C2	DB	A6	2B	13	A0	71
9	8C	7C	89	E4	B3	9D	23	0B	6C	D3	EB	4E	1A	E6	C6	36
A	EA	14	6F	17	8D	0F	2C	27	5B	BB	ED	53	A5	80	12	F4
B	CD	02	4C	2E	F7	A8	B2	FD	4F	C1	84	06	A3	8E	64	90
C	08	F5	F1	AE	0D	D5	CE	7B	DC	43	75	EF	A2	F8	63	B0
D	D1	00	C8	B9	61	0A	CF	BC	A1	62	2F	86	D0	D2	9B	AF
E	A9	AA	5F	66	32	F2	9A	15	FA	C9	03	FC	7D	6E	0E	6D
F	45	81	C5	7A	76	E5	98	46	C3	59	97	5D	DF	FB	CA	DA

EK-A.2: Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile elde edilen bir s-kutu ve sonuçları örneği-2.

SAC	NL			DU	DP	LAT	LP	BIC-SAC	BIC-NL
	maks.	min.	yüzdesi (%)						
0,5020	162	90	75	12	0,0469	38	0,1484	0,5043	103

satır \ sütun	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	71	86	78	87	49	95	77	64	82	F6	FC	45	8E	58	F1	DD
1	C5	62	D1	43	9C	9F	52	4D	7F	92	A6	5C	BB	A4	21	D2
2	C6	F2	BC	F4	B5	F8	66	81	4A	B0	74	9D	83	C7	76	57
3	48	14	1B	61	4B	AF	85	67	AC	89	C2	13	5F	A9	C1	FD
4	E8	ED	B2	0C	8A	2B	5D	02	E1	D3	9B	8F	80	EC	84	6C
5	5B	D9	D6	98	99	E3	9A	32	90	A2	7B	03	0F	0E	20	AB
6	70	08	75	FB	6B	01	56	1D	2D	8D	9E	6E	69	7D	E6	88
7	17	97	A0	EB	40	72	1C	B1	A3	2F	E2	7E	B7	BD	96	25
8	27	47	8B	F3	51	63	16	4F	3C	D7	CE	DC	6A	EA	94	79
9	5A	A5	B3	F0	8C	5E	28	2E	3E	AE	A8	2C	F5	59	36	68
A	35	33	30	CD	6F	3B	0D	91	3F	C3	B9	DF	34	C0	D8	C8
B	38	D5	FA	50	AA	F9	EE	E7	6D	DE	2A	42	CA	00	65	E0
C	BF	1E	55	10	39	B8	46	7A	E9	4E	D4	29	E5	09	15	41
D	60	18	CB	22	DA	11	FF	CC	31	73	7C	23	19	BA	DB	12
E	3A	B4	07	AD	37	53	24	05	0B	44	C4	D0	F7	3D	06	A7
F	FE	93	54	A1	1A	EF	04	B6	26	E4	BE	C9	0A	1F	CF	4C

EK-A.3: Önerilen etkin biyometrik s-kutu ve ters s-kutu oluşturma algoritması ile elde edilen bir s-kutu ve sonuçları örneği-3.

SAC	NL			DU	DP	LAT	LP	BIC-SAC	BIC-NL
	maks.	min.	yüzdesi (%)						
0,5002	162	92	77	14	0,0547	36	0,1406	0,5015	103

satır \ sütun	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	92	6F	93	79	65	87	84	41	62	6E	50	9B	52	72	78	88
1	89	59	4F	75	60	9C	A6	A4	74	66	B5	B6	64	91	5B	8C
2	8F	22	54	A5	A7	9F	B0	94	56	BA	1A	E7	E9	B7	86	E2
3	13	12	58	81	57	96	99	8A	1F	BB	5F	AD	A9	BE	E3	EA
4	F7	E8	04	69	90	8B	B4	9A	01	F9	6A	AF	03	A1	ED	4E
5	77	45	80	98	9E	FB	F8	FE	E0	07	B3	19	05	47	8E	8D
6	95	82	BD	F6	D8	FF	63	55	DF	DC	D0	D1	09	11	51	F5
7	F4	CB	CA	06	4A	E5	DA	1E	CF	E1	5D	16	33	C0	5E	3A
8	C5	70	2A	FA	AC	18	3B	9D	B2	2D	2E	38	C3	CC	E4	EB
9	6D	1D	C2	44	5C	7A	32	F1	B8	73	2F	97	EE	7E	7D	02
A	37	31	F2	F0	A3	5A	53	2C	4C	6C	15	F3	FD	76	23	25
B	24	D7	EF	BF	71	43	C6	D4	0B	00	FC	1B	DB	D5	B1	0C
C	27	0F	C1	B9	3F	C9	A2	AB	83	3C	DD	C8	D2	36	3E	0E
D	C4	DE	BC	67	26	A8	85	7C	48	7F	0A	AE	CD	2B	17	10
E	1C	6B	08	28	CE	EC	C7	D6	0D	4D	D3	35	21	14	3D	20
F	7B	AA	34	29	4B	E6	49	30	61	42	39	A0	46	40	68	D9

ÖZGEÇMİŞ