KOCAELİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLİŞİM SİSTEMLERİ MÜHENDİSLİĞİ ANABİLİM DALI

YÜKSEK LİSANS TEZİ

GÖRÜNTÜ ŞİFRELEME TEKNİKLERİ VE BİR UYGULAMA TASARIMI

HASAN SAKAL

KOCAELİ 2016

KOCAELİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

BİLİŞİM SİSTEMLERİ MÜHENDİSLİĞİ

ANABİLİM DALI

YÜKSEK LİSANS TEZİ

GÖRÜNTÜ ŞİFRELEME TEKNİKLERİ VE BİR UYGULAMA TASARIMI

HASAN SAKAL

Doç.Dr. Mehmet YILDIRIM		
Danışman,	**Kocaeli Üniversitesi**	.....
Yrd.Doç.Dr. Halil YİĞİT		
Jüri Üyesi,	**Kocaeli Üniversitesi**	.....
Yrd.Doç.Dr. Ali ÇALHAN		
Jüri Üyesi,	**Düzce Üniversitesi**	.....

Tezin Savunulduğu Tarih: 06.01.2016

ÖNSÖZ VE TEŞEKKÜR

Teknolojik gelişmelere paralel olarak değişen alışkanlıklar beraberinde yeni ihtiyaçlar doğurmaktadır. Görüntü şifreleme alanında yaşanan gelişmeler de bahse konu alışkanlıklar paralelinde gelişme kaydetmektedir. Sanal ortamda görüntülerin çığ gibi büyümesi sonucunda bu görüntülerin gizliliğinin ve güvenliğinin sağlanması için kişisel ve kurumsal talepler gün geçtikçe artmaktadır. Bu taleplere cevap verebilme adına yapılan çalışmalar da görüntü şifreleme teknolojisine dayanmakta ve bu alanda yapılan çalışmalar artarak devam etmektedir.

Bu tezin hazırlanmasında bana yol gösteren ve yardımlarını esirgemeyen değerli hocam Doç.Dr.Mehmet YILDIRIM'a ve tez yazım aşamasında ilgi ve desteğini esirgemeyen biricik eşim Elmas SAKAL'a teşekkür ederim.

Ocak – 2016 Hasan SAKAL

İÇİNDEKİLER

ÖNSÖZ VE TEŞEKKÜR..... i
İÇİNDEKİLER..... ii
ŞEKİLLER DİZİNİ..... iv
TABLOLAR DİZİNİ..... v
SİMGELER VE KISALTMALAR DİZİNİ..... vi
ÖZET..... vii
ABSTRACT..... viii
GİRİŞ..... 1
1. ŞİFRELEMEYE GİRİŞ..... 5
1.1. Şifreleme Nedir ve Neden İhtiyaç Vardır?..... 5
1.2. Şifrelemenin Tarihçesi..... 8
1.3. Şifreleme Algoritmaları..... 12
1.3.1. Simetrik şifreleme algoritması..... 12
1.3.1.1. Blok şifreleme algoritması..... 13
1.3.1.2. Dizi şifreleme algoritması..... 13
1.3.1.3. DES (Data encryption standart-Veri şifreleme standardı)..... 13
1.3.1.4. AES (Advanced encryption standard-Gelişmiş şifreleme standardı)..... 13
1.3.1.5. Blowfish..... 14
1.3.2. Asimetrik şifreleme algoritması..... 14
1.3.2.1. Asimetrik şifreleme algoritmasına sayısal bir örnek..... 15
2. GÖRÜNTÜ ŞİFRELEMEYE GİRİŞ..... 18
2.1. Sayısal Görüntü Elemanları..... 19
2.1.1. Sayısal görüntü ve piksel kavramı..... 19
2.1.2. Renk kavramı ve renkli görüntü..... 22
2.1.3. Renk modelleri..... 23
2.1.3.1. RGB renk modeli..... 24
2.1.3.2. CMYK renk modeli..... 24
2.1.3.3. CIE-Lab renk modeli..... 25
2.1.3.4. HSL ve HSV renk modelleri..... 25
2.2. Sayısal Görüntü Formatları..... 26
2.2.1. BMP görüntü formatı..... 26
2.2.2. GIF görüntü formatı..... 27
2.2.3. JPEG görüntü formatı..... 27
2.2.4. PICT görüntü formatı..... 28
2.2.5. EPS görüntü formatı..... 28
2.2.6. PNG görüntü formatı..... 28
2.2.7. TIFF görüntü formatı..... 29
2.3. Şifrelenmiş Resimlere Karşı Yapılan Saldırı Türleri..... 29
2.3.1. Cipherimage-only attack (Sadece şifreli resim saldırısı)..... 29
2.3.2. Known-plainimage (Bilinen şifrelenmemiş resim saldırısı)..... 29
2.3.3. Chosen-plainimage (Seçilen şifrelenmeiş resim saldırısı)..... 29
2.3.4. Jigsaw puzzle attack (Kesik parçaları birleştirme saldırısı)..... 30
2.3.5. Neighbor attack (Komşu saldırılar)..... 30
3. GÖRÜNTÜ ŞİFRELEME YAKLAŞIMLARI..... 31

3.1. Sayısal İmza Kullanarak Görüntü Şifreleme 31
3.2. Scan (Tarama) Dilini Kullanarak Görüntü Şifreleme..... 34
3.2.1. Görüntü sıkıştırma..... 34
3.2.2. Scan (Tarama) paternine giriş..... 35
3.2.3. Scan (Tarama) paterninde sıkıştırma ve şifreleme..... 36
3.3. Ayna Benzeri Görüntü Şifreleme..... 40
3.4. Kaotik (Karmaşık) Resim Şifreleme 41
3.5. BRIE (Bit Recirculation Image Encryption) 42
3.5.1. BRIE şifreleme algoritması 43
4. GÖRÜNTÜ ŞİFRELEME İÇİN GELİŞTİRİLEN YÖNTEM..... 45
4.1. Giriş 45
4.2. 8'e 4 Kod Kullanarak Şifreleyici Görüntü Oluşturma 46
4.3. Şifreleme İçin Kullanılan Yöntem..... 49
4.4. Geliştirilen Şifreleme Yönteminin Uygulama Yazılımı..... 49
4.5. Uygulama Yazılımının Çalışması..... 50
5. SONUÇLAR VE ÖNERİLER 54
KAYNAKLAR..... 56
EKLER..... 59
KİŞİSEL YAYINLAR VE ESERLER..... 67
ÖZGEÇMİŞ..... 68

ŞEKİLLER DİZİNİ

Şekil 1.1. Açık bir metnin şifrelenmesi..... 5
Şekil 1.2. Scytale şifre üreteci..... 9
Şekil 1.3. Sekiz rotorlu bir Enigma makinesi..... 10
Şekil 1.4. Japon Purple şifreleme makinesi..... 10
Şekil 1.5. Simetrik şifreleme yapısı..... 12
Şekil 1.6. Açık anahtarlı şifreleme yapısı..... 15
Şekil 2.1. Gerçek görüntü ve sayısal görüntü..... 19
Şekil 2.2. İkili görüntü..... 20
Şekil 2.3. Bir görüntünün orijinal hali ve büyütülmüş halleri..... 21
Şekil 2.4. Farklı çözünürlüğe sahip görüntüler..... 22
Şekil 3.1. Sayısal imza tekniği ile şifreleme işleminin blok diyagramı..... 32
Şekil 3.2. Sayısal imza tekniği ile şifre çözme işleminin blok diyagramı..... 33
Şekil 3.3. Görüntü sıkıştırma ve sıkıştırma geri alma işleminin temel blok diyagramı..... 35
Şekil 3.4. Temel tarama paternleri..... 36
Şekil 3.5. Basit, genişletilmiş ve yaygın tarama paternleri..... 37
Şekil 3.6. Sıkıştırma ve şifreleme özel taraması için temel tarama paternleri..... 38
Şekil 3.7. Bölüm paternleri..... 39
Şekil 3.8. Sıkıştırılmış bir görüntünün bileşenleri..... 39
Şekil 3.9. Ayna benzeri görüntü şifreleme algoritmasının blok diyagramı..... 40
Şekil 3.10. Kaotik tabanlı görüntü şifreleme mimarisi..... 42
Şekil 3.11. BRIE algoritmasının blok diyagramı..... 44
Şekil 4.1. Farklı parolalar kullanılarak oluşturulmuş şifreleyici görüntüler..... 48
Şekil 4.2. Zigzag tarama yönteminin uygulanışı..... 49
Şekil 4.3. Uygulamanın .fig dosyası..... 50
Şekil 4.4. Uygulamanın çalışan görüntüsü..... 50
Şekil 4.5. Orijinal Lena görüntüsü..... 51
Şekil 4.6. Parola 1 ile yapılan şifreleme ve şifre çözme işlemi neticesinde elde edilen görüntü..... 51
Şekil 4.7. Parola 2 ile yapılan şifreleme ve şifre çözme işlemi neticesinde elde edilen görüntü..... 51
Şekil 4.8. Parola 3 ile yapılan şifreleme ve şifre çözme işlemi neticesinde elde edilen görüntü..... 52
Şekil 4.9. Mevcut tarama yöntemi ile yapılan şifreleme ve şifre çözme işlemi neticesinde elde edilen görüntü..... 53

TABLOLAR DİZİNİ

Tablo 2.1. Bir pikselin koordinat sisteminde gösterilmesi 21
Tablo 4.1. Alfanümerik karakterleri ile birlikte 8'e 4 kodlarının 36 muhtemel kombinasyonu 47

SİMGELER VE KISALTMALAR DİZİNİ

nm : Nanometre, (μm)
mm : Milimetre, (mm)

Kısaltmalar

AES : Advanced Encryption Standard (Gelişmiş Şifreleme Standardı)
BCH : Bose, Chaudhuri, Hocquenghem
BMP : Bitmap
BRIE : Bit Recirculation Image Encryption (Bit Ötelemeli Görüntü Şifreleme)
CIE : Caotic Image Encryption (Karmaşık Görüntü Şifreleme)
CMYK : Cyan, Magenta, Yellow, Key (Cam Göbeği, Mor, Sarı, Siyah)
CMYKOG : Cyan, Magenta, Yellow, Key, Orange, Green (Cam Göbeği, Mor, Sarı, Siyah, Turuncu, Yeşil)
DCT : Discrete Cosine Transform (Ayrık Kosinüs Dönüşümü)
DES : Data Encryption Standard (Veri Şifreleme Standardı)
EPS : Encapsulated PostScript (Kapsüllenmiş Postscript)
FEAL : Fast Data Encipherment Algorithm (Hızlı Veri Şifreleme Algoritması)
GIF : The Graphic Interchange Format (Grafik Değişim Biçimi)
HCL : Hue, Chroma, Luminance (Ton, Renk Parlaklığı, Işık)
HSB : Hue, Saturation, Brightness (Ton, Doygunluk, Parlaklık)
HSL : Hue, Saturation, Lightness (Ton, Doygunluk, Aydınlık)
HSV : Hue, Saturation, Value (Ton, Doygunluk, Değer)
IDEA : International Data Encryption Algorithm (Uluslararası Veri Şifreleme Algoritması)
JPEG : The Joint Photographic Experts Group (Birleşik Fotoğraf Uzmanları Grubu)
JTC : Joint Transform Correlator (Ortak Dönüşüm İlişkilendirici)
LZW : Lemperl, Ziv, Welch
NIST : National Institute of Standards and Tecnology (ABD Milli Standartlar ve Teknoloji Enstitüsü
PICT : Picture File Format (Resim Dosya Biçimi)
PNG : Portable Network Graphics (Taşınabilir Ağ Grafikleri)
PSNR : Peak Signal to Noise Ratio (Tepe Sinyal Gürültü Oranı)
RC2 : Rivest's Cipher or Ron's Code2 (Rivest'in Şifresi veya Ron'un Kodu 2)
RC5 : Rivest's Cipher or Ron's Code5 (Rivest'in Şifresi veya Ron'un Kodu 5)
RGB : Red, Green, Blue (Kırmızı, Yeşil, Mavi)
RSA : Rivest, Shamir, Adleman
SAFER : Secure and Fast Encryption Routine (Güvenli ve Hızlı Şifreleme Rutini)
TIFF : Tag Interchange File Format (Etiket Değişim Dosya Biçimi)

GÖRÜNTÜ ŞİFRELEME TEKNİKLERİ VE BİR UYGULAMA TASARIMI

ÖZET

Teknolojik gelişmeler ile gün geçtikçe alışkanlıklar ve ihtiyaçlar değişmektedir. Bu değişim çok hızlı olmakla beraber insanların birbirlerine ve bilgiye erişim olanakları da kolaylaşmaktadır. Bu şekilde, hayat standartlarımız olumlu yönde değiştiği gibi, beraberinde bazı problem alanları da oluşmaktadır. İnsanlar bilgiye çabuk erişmek istedikleri gibi, aynı zamanda kendilerine ait bilgilerin mahremiyetini de korumak istemektedirler. Bu istek “bilgi güvenliği” kavramını ortaya çıkarmıştır. Bilgi güvenliği; bilginin istenmeyen kişilerin erişimine kapanmasını ve yetki sahibi kişilerin güvenli şekilde bilgiye erişebilmesini sağlamak yönünde alınacak tedbirlerden oluşmaktadır. Bu tedbirler ışığında çok sayıda çalışma yapılmıştır. Bilgi güvenliği, kapsamı geniş bir alan olduğundan alt başlıklara bölünmüştür. Bu alanda yapılan çalışmalar bu alt başlıklardan oluşmaktadır. Bu alt başlıklardan birisi de görüntü güvenliğidir. Bu tez çalışmasında; şifreleme ile ilgili temel bilgiler verilmiş, görüntü güvenliğini sağlamak için kullanılan görüntü şifreleme algoritmaları anlatılmış, geliştirmiş olduğumuz hibrit bir görüntü şifreleme yöntemi önerilmiş ve bu yöntem bir uygulama ile anlatılmıştır.

Anahtar Kelimeler: Görüntü Şifreleme, Resim Şifreleme, Sayısal İmza, Şifreleme, Zigzag Tarama Paterni.

IMAGE ENCRYPTION TECHNIQUES AND AN APPLICATION DESIGN

ABSTRACT

Day after day habits and needs vary with technological developments. Alongside this change is very rapid, people's access to each other and information is also easier. In this way, although our standard of living changes in a positive direction, it is composed of some problem areas. People want to access information quickly, but also they want to protect the privacy of the information of their own. This requesition creates "information security" concept. Information security consists of some precautions. These precautions are to avoid unwanted people from gaining access to the information and to ensure that authorized people access to information in a safe way. Owing to these precautions, numerous studies were occured. Because information security has a broad area, it is divided into subsections. Studies in this area are about these subsections. One of these subsections is the image security. In this study; basic information about encryption was described, image encryption algorithms ensure the safety of image were described, a hybrid image encryption technique which designed in this study was proposed and this technique was described with an application.

Keywords: Image Encryption, Image Coding, Digital Signature, Encryption, Zigzag Scan Pattern.

GİRİŞ

Şifreleme bilgi güvenliğinin temel alanlarından biridir. İnternetin hayatımızın her alanına girmesiyle beraber şifrelemeye olan ihtiyaç ve buna paralel olarak şifreleme alanındaki gelişmeler hızla artmaktadır. Günümüz bilgi sistemleri için hayati bir yere sahip olan şifreleme ile; uzaktan erişim, sertifika tabanlı kimlik doğrulama, çevrimiçi sipariş ve ödemeler, e-posta ve mesaj güvenliğinin sağlanması vb. ihtiyaçlar karşılanabilmektedir. Bu ihtiyaçların karşılanması; bir depolama biriminde kaydedilen ya da ağ üzerinden iletilen verilere sadece izin verilen kullanıcılar tarafından erişilebilmesi anlamına gelmektedir. Bir depolama biriminde kaydedilen ya da güvensiz ağ ortamında iletilen veriler şifreleme ile okunamaz hale getirilirler. Yetkili kullanıcı veriye eriştiğinde, okunamaz haldeki bu veri uygun şifre çözme anahtarı ile tekrar orijinal haline dönüşür. Bu işlem ile gizli veri, güvensiz iletim ortamlarında yetkisiz erişimlere karşı korunaklı hale gelmektedir.

Araştırmacılar geleneksel metin şifreleme yöntemlerinin görüntü şifreleme yöntemlerinde yetersiz kaldığını ortaya çıkarmıştır. Görüntü verilerinin boyutunun metin verilerine göre çok fazla olması, görüntü verileri için farklı şifreleme yaklaşımlarının ortaya çıkmasına neden olmuştur. Bu yaklaşımlar genel olarak kayıplı görüntü şifreleme algoritmaları ve kayıpsız görüntü şifreleme algoritmaları olmak üzere iki kategoride sınıflandırılmıştır. Kayıplı şifreleme yöntemlerinde şifresi çözülen görüntü az ya da çok bozulmaktadır. Kayıplı şifreleme yöntemi, yüksek görüntü kalitesi gerektirmeyen uygulamalar için kullanılabilir. Bu uygulamalarda kayıplı algoritmalar neticesinde oluşacak bozulmalar kabul edilebilir seviyede olmalıdır.

Diğer taraftan, kayıpsız şifreleme algoritmaları yüksek görüntü kalitesi gerektiren uygulamalarda kullanılmak için daha uygundur. Kayıpsız şifreleme metodlarında orijinal görüntü ile orijinal görüntünün şifrelenmesi ve müteakiben şifresinin çözülmesi neticesinde elde edilen görüntü arasında piksel farkı olmayacağından, görüntünün çözünürlüğü yani kalitesinde eksilme meydana gelmeyecektir.

Literatürde çeşitli şifreleme şemaları üzerinde çalışmalar yapılmıştır:

Sinha ve Singh [1] güvenli görüntü iletimi için sayısal imzaların kullanıldığı bir teknik önermiştir. Onların yaklaşımına göre orijinal görüntü kullanılarak elde edilen sayısal imza, orijinal görüntünün kodlanmış haline eklenir. Görüntü kodlama işlemi BCH

(Bose, Chaudhuri, Hocquenghem) hata kodu kullanılarak gerçekleştirilir. Son kullanıcıda şifreli görüntünün şifresi çözüldüğünde, sayısal imza görüntünün gerçekliğini doğrulamak için de kullanılabilir.

Maniccam ve Bourbakis [2] kayıpsız sıkıştırma ile gri tonlamalı ve ikili görüntülerin şifrelemesini gerçekleştiren kayıpsız bir şifreleme metodu sunmuştur. Bu metod tarama (scan) metodolojisi tarafından üretilen tarama paternlerine dayanmaktadır.

Chang ve arkadaşları [3] görüntülerin şifrelenmesi için vektörleri kullanan bir çalışma sunmuştur. Bu çalışmada görüntüler ardışıl kodlama yapabilmek maksadıyla vektörlere ayrıştırılmıştır.

Yen ve Guo [4] karmaşık bir sistem tarafından üretilen ikili dizilerden oluşan ayna benzeri görüntü şifreleme algoritmasını sunmuştur. Benzer bir çalışma Gao ve arkadaşları [5] tarafından da yapılmıştır. Bu çalışmada Gao görüntü şifreleme için üç metod önermiştir.

Xu ve Jiali [6] sundukları çalışmada zigzag dönüşüm metodunu kullanmıştır.

Zhang ve Karim [7] gri ölçekli görüntüleri şifrelemek için kullanılan mevcut şifreleme sistemlerini kullanarak renkli görüntüleri şifreleyen bir yöntem önermiştir. Bu yöntemde, renkli görüntüler endekslenmiş görüntü biçimlerine dönüştürülmektedir. Kodlama aşamasında, görüntü iki maske kullanılarak beyaz gürültü olarak kodlanmaktadır. Bu iki maskeden ilki giriş düzleminde, diğeri ise Fourier düzlemindedir. Şifre çözme aşamasında ise renkli görüntü, şifresi çözülmüş endekslenmiş görüntünün RGB (Red, Green, Blue-Kırmızı, Yeşil, Mavi) formatına geri dönüştürülmesiyle elde edilmektedir.

Görüntü şifreleme alanında yapılan bazı çalışmalar da, frekans alanında görüntü şifreleme üzerine gerçekleştirilmiştir. Krikor ve arkadaşları [8] görüntü şifreleme alanında, karakteristik değerler olarak alınan bazı DCT (Discrete Cosine Transform) yüksek frekansları seçen bir yöntem önermiştir. Bu yöntemde ortaya çıkan şifreli bloklar rasgele karıştırılmaktadır.

Droogenbroeck ve Benedett [9] şifreleme için sıkıştırılmış görüntülerden AC katsayıları seçmiştir. Bu yöntemde DC katsayıları, önemli ve görünür bilgiyi taşıdıkları ve tahmin edilebilir oldukları için şifreli değildir. Sıkıştırma ve şifreleme aşamaları bu yöntemde birbirinden ayrılmaktadır. Bu durum ilave çalışma zamanı maliyeti olarak karşımıza çıkmaktadır.

Tang [10] DCT tabanlı video ve görüntülere uygulanan ve zigzag permütasyon olarak adlandırılan bir yöntem önermiştir. Yöntem belirli bir düzeyde gizlilik sağlamaktadır.

Younes ve Jantan [11] görüntü dönüşümü ve tanınmış Blowfish şifreleme ve şifre çözme algoritması birleşimine dayalı, blok tabanlı bir dönüşüm algoritmasını tanıtmıştır. Bu çalışmada orijinal görüntü, dönüştürülmüş ve Blowfish algoritması kullanılarak şifrelenmiş bloklara ayrılmıştır. Bu çalışma göstermiştir ki; küçük blok boyutu kullanmak daha az korelasyon ve daha yüksek entropi sonucunu doğurmaktadır.

Bir diğer çalışmada da İsmail ve arkadaşları [12] kaos tabanlı şifreleme algoritması üzerine araştırmalar yapmıştır.

Bu tez çalışması, şifrelemenin uygulama alanlarından birisi olan görüntü güvenliğinin günümüzde ne kadar önemli olduğunu vurgulamak ve görüntü güvenliğini sağlama yolunda alınabilecek önlemlerden birisi olan görüntü şifreleme konusunda bir uygulama sunmak amacıyla yazılmıştır. Çalışma toplam beş bölümden oluşmaktadır:

Bölüm 1'de, şifrelemenin tanımı yapılmış ve neden şifrelemeye ihtiyaç duyulduğu anlatılmış, şifrelemenin tarihi gelişimi hakkında bilgiler verilmiş, tarihi gelişim sürecinde kullanılan şifreleme teknik ve donanımlarından örnekler sunulmuş, simetrik ve asimetrik şifreleme olarak ikiye ayrılan şifreleme algoritmalarına değinilmiş ve bu algoritmaların temel mantığı anlatılmıştır.

Bölüm 2'de, görüntü şifreleme kavramı açıklanmış, sayısal görüntü, piksel ve renk kavramları açıklanmış ve renk modelleri hakkında bilgiler verilmiş, sayısal görüntü formatlarından BMP (Bitmap), GIF (Graphic Interchange Format), JPEG (Joint Photographic Experts Group), PICT (Picture File Format), EPS (Encapsulated PostScript), PNG (Portable Network Graphics) ve TIFF (Tag Interchange File Format) formatları hakkında bigiler verilmiş, şifrelenmiş resimlere karşı yapılabilecek saldırı türleri anlatılmıştır.

Bölüm 3'te, görüntü şifreleme yaklaşımları anlatılmış ve bu yaklaşımlara ait blok diyagramlar verilmiştir.

Bölüm 4'te ise geliştirmiş olduğumuz hibrit bir görüntü şifreleme uygulamasına yer verilmiştir. Uygulama kısmında şifreleyici görüntü ile şifreleme yapma mantığı çerçevesinde "Çift Tarama (Double Scan)" yöntemi kullanılmıştır. Bu yöntemle beraber kullanılan, Sinha ve Singh'in [1] çalışmasında belirttiği sayısal imza mantığına benzer "şifreleyici görüntü" ve şifreleyici görüntü elde etmek maksadıyla kullanılan 8'e

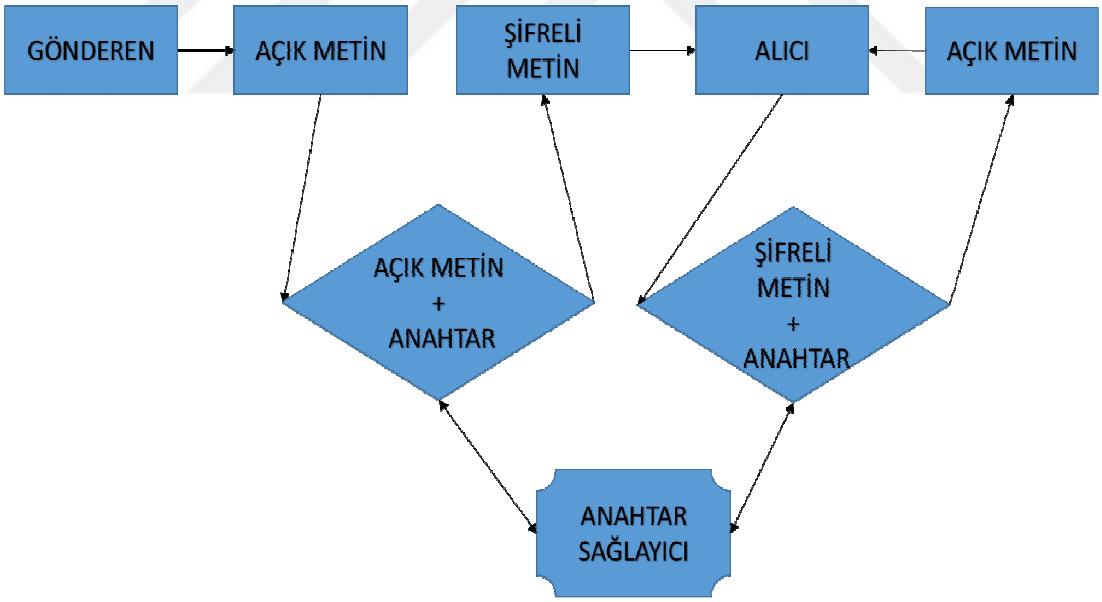
4 kodlar hibrit bir teknik ortaya çıkarmıştır. Ayrıca yapılan şifreleme ve şifre çözme işlemleri neticesinde oluşan resmin tepe gürültü oranı dB cinsinden hesaplanmıştır. Uygulamada, değişik anahtar kelimeler kullanıldığında farklı şifreleyici görüntüler oluştuğundan, girilen anahtar kelimenin karmaşıklığı ile doğru orantılı olarak şifrelemenin kalitesinin arttığı görülmüştür.

1.ŞİFRELEMEYE GİRİŞ

1.1. Şifreleme Nedir ve Neden İhtiyaç Vardır?

Şifreleme, açık halde erişilebilir bulunan herhangi bir bilginin, istenmeyen kişiler tarafından anlaşılamayacak ve çözülemeyecek hale getirilmesiyle ilgilenen bir bilim dalıdır [13]. Bu tanım ışığında, şifrelemenin amacının bilgi ve belgelerin güvenliğini sağlamak olduğu anlaşılmaktadır. Şifrelenen bir belgeye, yetki verilen; yani geçerli anahtara sahip olan kişiler haricinde kimsenin erişememesi amaçlanmaktadır.

Düz metinden oluşan iletiler açısından konu incelenecek olursa; bir iletinin içeriğini saklamak üzere yapılan gizleme işlemi de şifreleme olarak tanımlanmaktadır. Düz metin, herhangi bir metin dosyası, resim, ses veya görüntü dosyası olabilir. Şifrelenmiş bir ileti şifreli bir metindir. Şifreli metini düz metine geri çevirme işlemi ise şifre çözmedir. Şifreleme işleminin algoritması Şekil 1.1'de gösterilmektedir.



Şekil 1.1. Açık bir metnin şifrelenmesi

Sıradan şifreleme yöntemlerinde mesajı gönderen kişi ve alıcı kişi tek bir gizli anahtara sahiptir. Gönderen kişinin şifreleme yaptığı anahtar aynı zamanda alıcı kişi için de şifre çözme anahtarıdır. Bu yönteme "gizli anahtar şifreleme" ya da "simetrik şifreleme" denir [14]. Bu yöntemde tek bir anahtar olduğundan, gönderici şifreleme yaptığı anahtarı bir şekilde alıcı kişiye ulaştırmalıdır. Bu işi güvenli bir şekilde yapmak

zordur. Elektronik ortam kullanılıyor ise bu anahtarın nerede ve nasıl saklanacağı ve alıcıya nasıl ulaştırılacağı önemlidir ve birtakım riskler içerir. Eğer başka bir kişi bu anahtarı ele geçirir ise anahtar ile şifrelenmiş bütün veriye ulaşabilecektir. Bu nedenle, yüksek güvenlik içeren uygulamalar için simetrik şifreleme uygun değildir. Bunun yerine şifreleme ve şifre çözmede farklı anahtarların kullanıldığı asimetrik şifreleme yöntemleri kullanılmalıdır.

Elektronik iletişim günümüzde, kağıt ile yapılan iletişimin yerini tamamen almak üzeredir. İster devlet kurumu ister özel kurum olsun, tüm kurumlar e-posta sunucuları, evrak yönetim sistemleri ve kurumsal iş takip yazılımları kullanmakta ve işlerini çevrimiçi sistemler üzerinden yürütmektedir. Elektronik iletişim ağları üzerinden iletilen bilgilerin güvenliğinin sağlanması da son derece önem arz etmektedir. Açık ağlardan gönderilen iletiler üçüncü şahıslar tarafından dinlenme ve değiştirilme tehdidi altındadır. Kurumlar bunun önüne geçmek amacı ile güvenlik alanına önemli yatırımlar yapmaktadırlar. Bu yatırımlarda amaç bilginin gizliliğinin, gerçekliğinin, doğruluğunun ve güvenirliğinin sağlanmasıdır. Bunu sağlamanın yolu da şifreleme biliminden geçmektedir.

Haberleşen iki taraf, bilgisayar ağlarını, yani kablolu veya kablosuz iletişim kanallarını kullanarak bir bilgiyi/mesajı bir taraftan diğerine iletirler. Bu iletim esnasında haberleşen taraflar çeşitli tehditlerle karşı karşıya kalırlar. Bu tehditleri şu şekilde özetleyebiliriz;

- Gizlilik İhlali: Gönderici ile alıcı arasındaki haberleşme kanalına sızan bir saldırgan, istasyonlar arasındaki mesaj trafiğini dinleyerek elde ettiği mesajları okuyabilir. Bu durum haberleşmenin gizliliğini bozabilir. Bu tehdit dinleme tehdidi olarak bilinir.
- Bütünlük İhlali: Gönderici ile alıcı arasındaki haberleşme kanalına sızan bir saldırgan, göndericinin mesajlarını değiştirerek, alıcıya giden mesajı istediği biçime sokabilir. Bu durum, mesajın bütünlüğünü bozduğundan bütünlük ihlali olarak adlandırılır.
- İnkar Etme İhlali: Mesajı gönderen veya alan tarafın bu işi yaptığını inkar etmesi söz konusu olabilir. Bu kötü niyetli girişimi boşa çıkaracak mekanizmalara ihtiyaç vardır.
- Kimlik Doğrulama İhlali: Saldırgan, alıcıya göndericinin kimliğini taklit ederek bir mesaj gönderebilir. Bu durumda, eğer alıcı güvenilir bir kimlik doğrulaması yapmıyorsa yanlış mesajlarla kandırılabilir.

- Süreklilik İhlali: Saldırgan, haberleşen iki taraf arasındaki hattı veya haberleşme araçlarını kullanılamaz hale getirerek haberleşmenin sürekliliğini engellemeye çalışır [16].

Modern şifrelemenin sağlaması gereken hususlar aşağıda belirtilmektedir.

- Gizlilik: Yetkisi olmayan kişilerin bilgiye erişememesidir.
- Bütünlük: Bilginin kaynaktan hedefe gittiği süreçte veya saklandığı yerde değiştirilmemesidir. Bilgi güvenliğinde zaafiyetlerin olduğu sistemlerde kötü niyetli kişiler iletim esnasında iletilen veriyi değiştirebilir ve bu sayede alıcı, göndericinin gönderdiği veriden farklı bir veri alablir.
- Reddedilemezlik / İnkar Edilememezlik: Bilgiyi oluşturan veya gönderen kişinin, daha sonra oluşturulan veya gönderilen bu bilginin kendisine ait olmadığını inkar edememesidir. Elektronik sistemlerde bu hususu sağlamak üzere “elektronik imza” teknolojisi kullanılmaktadır. Elektronik imzaya “sayısal imza” da denilmektedir.
- Kimlik Doğrulama: Gönderen ve alıcı kişiler, birbirlerinin kimliklerini doğrulayabilirler. Bir iletinin alıcısı bu iletinin kaynağını araştırmak isteyebilmektedir. Davetsiz bir misafir başkasının kimliğine bürünme şansına erişmemelidir. Kimlik belirleme işlemi, bilginin doğru kaynaktan alındığını doğrulamak için kullanılmaktadır [15].
- Haberleşmenin Sürekliliği: Haberleşmenin kesintiye uğramadan yapılmasıdır.

Bilginin güvenliğini sağlamak için, başkası tarafından dinlenme, verinin değiştirilmesi, kimlik taklidi gibi tehditler ortadan kaldırılmalıdır. Bu maksatla kullanılan temel araç şifrelemedir.

Bilgi toplumlarına bakıldığında, teknolojinin de yardımıyla milyonlarca kişinin gözetiminin yerel hükümetler tarafından yapıldığını görmekteyiz. Şifreleme sayısal dünyadaki kişilerin gözetiminin yapılmasını sağlayan başlıca araçtır. Şifreleme, artık sadece resmi özelliğe sahip olan veya uzak durulması gereken askeri bir araç değildir. Şifrelemeyi öğrenmek ve onun modern toplumlarda sağladığı avantajlardan yararlanmak hem kişisel gizliliğimiz hem de elektronik dünyadaki güvenliğimiz için kaçınılmazdır.

Şifrelemenin çok kullanılan bazı tipleri özel donanımlar gerektirmektedir. Bununla beraber, geçmiş yıllarda yazılımsal şifreleme tekniklerinin kullanımında bir artış görülmektedir. Ordu ve aşırı önemli ticari uygulamalar ise şifrelemede donanım

tekniklerini tercih etmektedirler. Donanım tekniklerinin seçilmesi için üç ana sebep bulunmaktadır. Bunlar;

- Hız
- Güvenlik
- Kurulum kolaylığı

Özel yapılandırılmış donanımlar her türlü yazılım tekniğinden daha hızlıdır. Bir bilgisayarda, yazılım şifreleme tekniğinin fiziksel güvenliği yoktur. Bu yüzden, fark edilmeden algoritma ile oynamak mümkündür. Fakat, donanım teknikleri bu probleme karşı daha iyi koruma sağlamaktadır. Açılması zor olan kutular saldırganların uzak tutulmasında donanım kullanmanın bir diğer yoludur. Ayrıca yongalar, algoritma anahtarlarını okuyacak saldırganlara karşı koruma sağlayacak şekilde tasarlanabilirler [14].

Tüm bu yazılanlar ışığında, şifrelemeye neden ihtiyaç duyulduğunu özetleyecek olursak; bilgisayar dünyasında bulunan veriler 1'ler ve 0'lar halinde bulunmaktadır. Bu veriler şifreleme ile koruma altına alınmadığında, istenmeyen kişiler tarafından elde edilebilecek ve savunmasız kalacaktır. Günümüz teknolojisinde, istenmeyen kişilerin verilere sahip olabileceği çok farklı ortamlar mevcuttur. Bu ortamlar şunlardır: İnternet, e-posta, anlık mesajlaşma yazılımları, kablosuz haberleşme teknolojileri, usb bellek, harici sabit disk, kişisel bilgisayarlar vb. Bu ortamlarda verilerin güvenli bir şekilde tutulabilmesi için şifreleme bilimine ihtiyaç duyulmaktadır.

1.2. Şifrelemenin Tarihçesi

Şifreleme (Cryptography), yapı olarak Yunanca iki kelimenin birleşiminden oluşmaktadır ve "gizli yazı" anlamını taşıyan derinlemesine matematiksel bir konudur [17].

Şifrelemenin ilk bilinen kullanım yeri, M.Ö. 1990 yıllarındaki mezar kitabeleridir. Haberleşme amacıyla, ilk defa M.Ö. 475 yılında kullanılmıştır. Eski Yunan ve Romalılar döneminde, M.Ö. 400 yıllarında, Spartalıların kullandığı "scytale" şifresi ve M.Ö. 50 yıllarında Sezar'ın geliştirdiği yerine koymalı "sezar" şifresi en temel şifreleri oluşturmaktadır [15]. Scytale şifre üretecinin resmi Şekil 1.2'de gösterilmektedir. Haberleşme güvenliği ve şifreleme üzerine ilk yazı, M.Ö. 350 yılında yayımlanmıştır. Askeri manada şifreleme, ilk defa, Sezar tarafından M.Ö. 60 yılında kullanılmıştır. Şifre çözme ile ilgili bilinen en eski bilimsel eser, 1412 yılında, Mısırlı bilim adamı El-Kalkashandi tarafından yayımlanmıştır.



Şekil 1.2. Scytale şifre üreteci [18]

Rönesans, diğer sanat ve bilim dallarında olduğu gibi şifrelemede de yeni yaklaşımlara yol açmış ve bu dönemde polialfabetik şifreler ortaya çıkmıştır. Şifreleme alanında “polygraphia” adlı kitap bu dönemde yayımlanmış olup, Johannes Trithemius (1462-1516) tarafından yazılmıştır [15].

20. Yüzyılın ilk yarısında dikkati çeken temel olaylar; 1917 yılında Amerika Birleşik Devletlerinin I. Dünya savaşına girmesine yol açan Zimmermann olayı ve gerçek anlamda kırılamayacak tek simetrik şifre olan tek kullanımlık şifre algoritmasının 1926’da Vernam tarafından yayımlanmasıdır [14].

Zimmermann olayı, modern dönemi hazırlayan ilk büyük ve etkili şifre kırma olayıdır. Zimmermann Telgrafı (Zimmermann Note/Telegram) olarak bilinen olayda, Almanya Dışişleri Bakanı Arthur Zimmermann tarafından gönderilen telgraf Alman Dışişleri şifreleme standartlarına göre kodlanmıştı. Mesaj, Meksika’yı Almanya’nın yanında, Amerika’nın karşısında savaşa davet ediyordu. İki İngiliz şifre çözücünün mesaj içeriğini çözmeleri ve bunu ABD Başkanı Wilson’a okutmaları sonucunda 2 Nisan 1917’de ABD Birinci Dünya Savaşı’na girmiş oldu. İngiliz kablo gemisi TELECONIA Almanların transatlantik kablolarını keserek trafiği İsveç ve Amerikan sahipli kablolara yönlendirmesi ile şifre çözücüler gönderici ve alıcı arasında giden mesaja müdahil olmuşlardı.

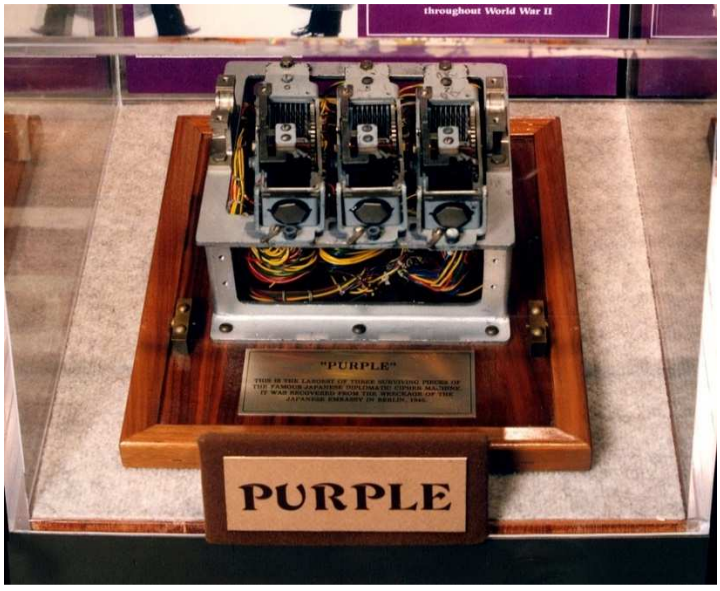
Bugünkü anlamlarıyla çağdaş şifreleme cihazları, elektrik enerjisinin bu cihazlarda kullanılmasıyla başlamıştır. Bu alandaki en özgün örnekler, Polonyalılar tarafından tasarlanıp, Almanlar tarafından geliştirilen Enigma (Şekil 1.3) ve yine Almanlar tarafından yapılan Geheimschreiber cihazlarıdır. II. Dünya savaşında Almanya

tarafından yoğun bir şekilde kullanılan Enigma, İngilizlerce yapılan ve ilk bilgisayarlardan biri olarak adlandırılabilecek Colossus tarafından kırılmıştır.



Şekil 1.3. Sekiz rotorlu bir Enigma makinesi [19]

II. Dünya Savaşı yıllarında Amerika Birleşik Devletleri'nde, çağdaş şifre analizinin doğuşuna şahit olunmuştur. Bugün tüm simetrik şifreleme sistemleri için kullanılan şifre analiz yöntemleri bu yıllarda William F. Friedman (1891-1969) ve grubu tarafından geliştirilmiştir. Savaş yılları boyunca Japonlar tarafından kullanılan Purple (Şekil 1.4) şifresi Friedman'ın şifre analiz çalışmaları sonucunda kırılmıştır. Günümüzde şifre kırma çalışmalarının tamamını içine alan şifre analizi teriminin başlangıcı da yine Friedman'dır [15].



Şekil 1.4. Japon Purple şifreleme makinesi [20]

1948 ve 1949 yılları, şifre analizinin matematiksel olarak formalize edildiği yıllar olmuştur. Bilgi kuramının oluşturucusu olan Shannon'un bu alanda yayımladığı ilk bildiri, günümüzde de çağdaş şifre analizinin temeli olarak kabul edilir.

Günümüzde şifrelemeye yönelik kaydadeğer gelişmeler 1970'li yıllardan itibaren ortaya çıkmıştır. IBM firması, 1971 yılında 128 bit uzunluğunda anahtarla çalışan Sabah Yıldızı (Venüs – Lucifer) olarak bilinen şifreleme tekniğini geliştirmiştir. Aynı algoritma 1977 yılında, 56 bit anahtar uzunluğuyla DES (Data Encryption Standard-Veri Şifreleme Standardı) algoritması adıyla Amerika Birleşik Devletleri Standartları Enstitüsünce standartlaştırılmıştır.

Açık anahtarlı şifreleme tekniği ilk defa 1976 yılında Diffie ve Hellman tarafından ortaya atılmıştır. Temel teorisi 1976 yılında atılmış olan asimetrik şifreleme sistemi, 1978 yılında tam olarak formülleştirilerek, açık anahtarlama şifreleme sistemleri başlığı altında ve oluşturanların baş isimlerinden oluşan RSA (Rivest, Shamir, Adleman) algoritması tanımıyla kullanıma girmiştir. Çok karmaşık olmayan, mod ve üs hesaplamalarına dayanan matematiksel işlemlerin sonucunda, iki büyük asal sayıdan birer tane açık ve kişisel anahtar üreten bu şifreleme sisteminin en büyük özelliği kişisel anahtarın, açık anahtarı oluşturan parçalardan üretilmesinin olanak dışı olmasıdır.

RSA algoritması 1994 yılında kırılmıştır. Dünya üzerindeki 1600 bilgisayarda sekiz ay süren çalışma sonucunda, 129 basamaklı bir sayının iki asal çarpanı bulunabilmiştir.

RSA, DES'e alternatif olarak üretilmişti. RSA ile bir verinin tamamını şifrelemek için gereken işlemlerin çok olması nedeniyle uzun bir zaman almaktaydı. Ancak, hesaplama zamanı RSA'dan çok daha hızlı olan DES ile verinin şifrelenmesi ve daha sonra DES anahtarının RSA ile şifrelenerek şifreli veriye eklenmesi şifreleme işlemini oldukça hızlandırmaktadır. Fakat güvenliğin çok önemli olduğu durumlarda sadece RSA şifreleme sistemini kullanmak daha mantıklı bir seçim olmaktadır [21].

1997 yılında NIST (National Institute of Standards and Technology-ABD Milli Standartlar ve Teknoloji Enstitüsü) tarafından, yeni bir gizli anahtarlı şifreleme standardı için gerekli kriterler belirlenmiş ve tüm dünyaya duyurulmuştur [22]. Birçok bilim adamı tarafından, aday olarak gönderilen şifreleme yordamları elemeye tabi tutulmuş ve içlerinden beş tanesi finalist olarak seçilmiştir. 2000 yılında da bunlardan Vincent Rijmen ve Joan Daemen tarafından geliştirilen Rijndael yordamı yeni şifreleme standardı olarak kabul edilmiştir [23]. Böylece DES'in yerini AES (Advanced Encryption Standard-Gelişmiş Şifreleme Standardı) almıştır. AES ile

tanımlanan şifreleme algoritması, hem şifreleme hem de şifreli metni çözmede kullanılan anahtarların birbiriyle ilişkili olduğu, simetrik anahtarlı bir algoritmadır. AES için şifreleme ve şifre çözme anahtarları aynıdır.

1.3. Şifreleme Algoritmaları

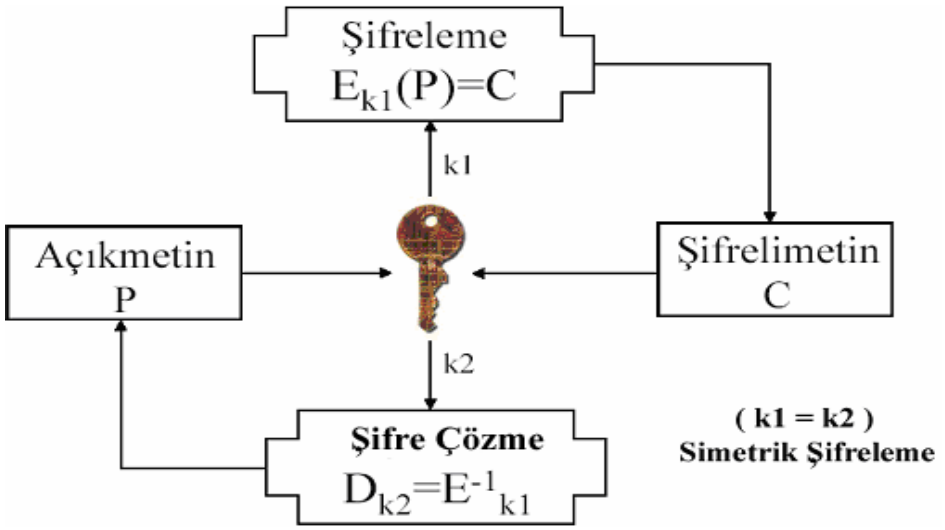
Şifreleme algoritmaları simetrik ve asimetrik şifreleme algoritması olmak üzere iki grupta incelenmektedir.

1.3.1. Simetrik şifreleme algoritması

Simetrik şifreleme; gizli anahtarlı şifreleme ya da tek anahtarlı şifreleme olarak da adlandırılır. Bu algoritmada şifreleme ve şifre çözmek için bir tane gizli anahtar kullanılmaktadır. Bu anahtar hem şifrelemede hem de şifre çözmede kullanılmaktadır. Şifreli mesaj gönderildiğinde şifreleme anahtarı da bir şekilde alıcıya ulaştırılması gerekmektedir. Alıcıya anahtar ulaşmaz ise gelen mesajı açamayacaktır.

Simetrik şifreleme algoritmasında güvenlik anahtardadır. Anahtarı bir şekilde elde eden herkes o anahtar ile şifrelenmiş verilere erişebilme kabiliyetine sahip olacaktır. İletişimin gizli kalması için anahtarın da gizli kalması gerekmektedir [24].

Simetrik şifrelemenin en önemli avantajlarından birisi oldukça hızlı olmasıdır. Asimetrik şifrelemeyle karşılaştırıldığında hız konusunda simetrik algoritmalar çok daha başarılıdır. Bununla birlikte içerdiği basit işlemlerden dolayı, simetrik algoritmayı elektronik cihazlarda uygulamak çok daha kolaydır. Ayrıca simetrik algoritmalarda kullanılan anahtarın boyu ve dolayısıyla bit sayısı da daha küçüktür. Simetrik algoritmaların şifre yapısı Şekil 1.5'de gösterilmektedir.



Şekil 1.5. Simetrik şifreleme yapısı [14]

Simetrik algoritmalar blok şifreleme ve dizi şifreleme algoritmaları olarak ikiye ayrılmaktadır.

1.3.1.1. Blok şifreleme algoritması

Blok şifreleme algoritmaları veriyi bloklar halinde işlemektedir. Bu blokları bazen bağımsız, bazen de birbirine bağlı olarak şifrelemektedir. Bu algoritmalarda iç hafıza yoktur, bu yüzden hafızasız şifreleme adını da almıştır. Bütünlük kontrolü gerektiren uygulamalarda genellikle blok şifreleme algoritmaları tercih edilir. Modern bir bilgisayar algoritması için, tipik bir blok büyüklüğü 64 bittir [25].

1.3.1.2. Dizi şifreleme algoritması

Dizi şifreleme algoritmaları veriyi bir bit dizisi olarak alır. Bir üreteç aracılığı ve bir anahtar yardımıyla istenilen uzunlukta kayan anahtar adı verilen bir dizi üretilir. Kayan anahtar üretimi zamana bağlıdır ve bu yüzden bu algoritmalara aynı zamanda hafızalı şifreleme denir. Düz metin üzerinden zaman başına belli bir anda tek bir bit veya bazen sekiz bit olarak çalışır. Telsiz haberleşmesi gibi gürültülü ortamlarda ses iletimini sağlamak için genellikle dizi şifreleme algoritmaları kullanılır [25].

1.3.1.3. DES (Data encrytion standard - Veri şifreleme standardı)

Dünyada en yaygın kullanılan şifreleme algoritmalarından birisidir. DES, IBM tarafından geliştirilmiştir. 1975 yılında “Federal Register” tarafından yayınlanmıştır. DES 64 bitlik veriyi 56 bitlik anahtar kullanarak şifreler. Ayrıca klasik Feistel Ağı kullanılarak temelde şifreleme işleminin deşifreleme işlemiyle aynı olması sağlanmıştır. Kullanılan teknikler yayılma ve karıştırmadır. DES’in en büyük dezavantajı anahtar uzunluğunun 56 bit olmasıdır. 1975 yılında yayınlanan bu algoritma günümüzde geliştirilen modern bilgisayarlar tarafından yapılan saldırılar karşısında yetersiz kalmaktadır. Daha güvenli şifreleme ihtiyacından dolayı DES, 3DES olarak geliştirilmiştir. 3DES algoritması geriye uyumluluğu da desteklemek amacıyla 2 adet 56 bitlik anahtar kullanır. 3DES algoritması, DES algoritmasının şifreleme, deşifreleme, şifreleme şeklinde uygulanmasıdır [26].

1.3.1.4. AES (Advanced encrytion standard - Gelişmiş şifreleme standardı)

DES’e göre daha güvenli bir sistemdir. Çeşitli bilim adamları tarafından DES’in kırılması üzerine 2001 yılında geliştirilmiştir. Belçikalı Vincent Rijmen ve Joan Daemen tarafından bulunmuş, DES'in eksik taraflarının düzeltilmesiyle oluşturulmuş bir blok şifreleme algoritmasıdır. 128 bit, 192 bit ve 256 bit olmak üzere üç farklı anahtar uzunluğuna sahip olabilir. AES’in güçlü yönleri donanımda ve yazılımda hızlı

olması, daha kolay uygulanabilir olması ve çok daha az hafızaya gerek duyması olarak söylenebilir. Günümüzde bilinen tüm akademik, pratik ve doğrudan (brute force) saldırılara karşı dayanıklı olduğu düşünülmektedir. En yaygın olarak kullanılan simetrik şifreleme algoritmasıdır.

1.3.1.5. Blowfish

Blowfish, 64-bit öbek büyüklüğüne ve 32 bit'ten 448 bit'e kadar anahtar uzunluğuna sahiptir. DES'in eksik kalmaya başlamasından sonra onun yerini alması amacıyla tasarlanmıştır. Blowfish algoritması en az 4 kb RAM'a ihtiyaç duyar. Bu yüzden akıllı kartlar gibi küçük sistemlerde kullanılamaz. Yüksek şifreleme ve e-posta gibi rutin kullanıcı uygulamaları konusundaki etkinliğiyle başarılı bir algoritma olarak değerlendirilmektedir. Blowfish kullanımını artıran özelliklerinden birisi, geliştirildiğinde halen kullanılmakta olan diğer şifreleme algoritmaları lisanslı ve paralı satılmasına rağmen, Blowfish'in tamamen ücretsiz olmasıydı. Blowfish piyasada kullanılan en hızlı blok şifreleyicilerdendir ve içerdiği karmaşık anahtar çizelgesi şifrenin kırılmasını zorlaştırmıştır [25].

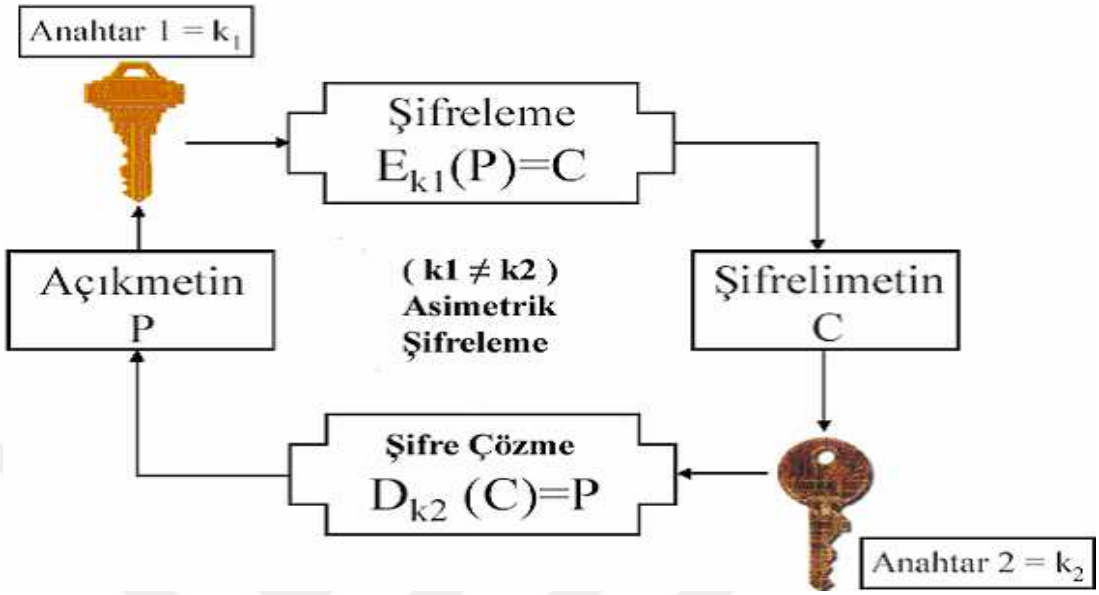
DES, AES ve Blowfish dışında kullanılan bazı simetrik algoritmalar aşağıda verilmiştir: IDEA (International Data Encryption Algorithm-Uluslararası Veri Şifreleme Algoritması), RC2 (Rivest's Cipher veya Ron's Code2), RC5 (Rivest's Cipher veya Ron's Code5), FEAL (Fast Data Encipherment Algorithm), SAFER (Secure and Fast Encryption Routine), Skipjack (Clipper Chip), GOST 28147-89, ASEKAL-21.

1.3.2. Asimetrik şifreleme algoritması

Gizli anahtarlı yapılarda genellikle güvenli anahtar yönetiminin sağlanmasında problemler yaşanmaktadır. Simetrik şifreleme tekniğinde bulunan anahtar dağıtım problemini çözmek için şifreleme ve şifre çözme işlemlerinin her birisi için ayrı ayrı anahtar kullanma prensibine dayanan bir şifreleme sistemi geliştirilmiştir. Bu sistemde şifreleme işlemi herkes tarafından bilinen açık bir anahtarla yapılır. Şifreleme ve şifre çözme işlemi birbirinin simetriği olmayan algoritmalarla gerçekleştirildiğinden dolayı da bu sistem asimetrik şifreleme sistemi olarak adlandırılmaktadır.

Asimetrik şifrelemede; bir kullanıcının açık anahtarıyla şifrelenen bir mesajı, yalnız ve ancak o kullanıcıya ait özel anahtar çözebilmektedir. Aynı şekilde, herhangi bir kullanıcının özel anahtarıyla attığı sayısal imzanın doğrulanabilmesi, yalnızca o kullanıcının açık anahtarını kullanarak mümkün olabilmektedir. Açık anahtar herkese açıktır, elektronik kimlik belgelerinin içinde diğer kişisel bilgilerle birlikte tutulur ve

herkes birbirinin açık anahtarını istediği zaman elde edebilir. Asimetrik şifreleme algoritmasının yapısı Şekil 1.6'da gösterilmektedir.



Şekil 1.6. Açık anahtarlı şifreleme yapısı [14]

1.3.2.1. Asimetrik şifreleme algoritmasına sayısal bir örnek

Asimetrik şifrelemede açık anahtar ve özel anahtar olmak üzere iki tane anahtar kullanılmaktadır. Bunlardan açık anahtar ile sadece sifreleme yapılabilirken, özel anahtar ile sifre çözme islemi yapılabilmektedir. RSA algoritmasının kullanıldığı basit bir asimetrik şifreleme işleminin matematiksel aşamaları aşağıda gösterilmektedir:

Önce 2 tane asal sayı seçilmektedir:

a=3
b=11

Daha sonra bu iki asal sayının çarpımından oluşan N sayısı oluşturulmaktadır.

N=(axb)
N=(3x11)
N=33

N sayısı açık anahtar ve özel anahtarın bir parçasıdır. Daha sonra a ve b sayısının 1 eksiklerinin çapımından bir x sayısı oluşturulmaktadır.

x=(a-1)x(b-1)
x=(3-1)x(11–1)

x=2x10
x=20

Daha sonra x sayısı ile ortak böleni olmayan bir e sayısı oluşturulmaktadır.

e=7 olsun.

Bu oluşturulan e ve N sayıları açık anahtardır.

Daha sonra bir adet d sayısı üretilmektedir. Bu d sayısı e sayısı ile çarpılıp x sayısı ile mod işlemine tabi tutulduğunda kalanı 1 olacak bir sayı olmalıdır. Bunun matematiksel ifadesi şu sekildedir.

dxe=1(mod x)
dx7=1(mod 20)
d = 3 olabilir.

Oluşturulan bu d sayısı ile N sayısı da özel anahtardır.

Açık anahtar: e = 7 ve N = 33
Özel anahtar: d = 3 ve N = 33

16 sayısının şifrelenmesi ve şifresinin çözülmesini gösteren örnek aşağıda gösterilmektedir. 16 sayısının açık anahtarda bulunan e sayısı ile üssünün alınması ve N sayısı ile çıkan sonucun modunun alınması neticesinde şifreleme işlemi yapılmaktadır. Yani;

Şifreli Metin = 16^7 (mod 33)
Şifreli Metin = 268435456 (mod 33)
Şifreli Metin = 25

Şifre çözme işlemi için 25 sayısının d ile üssü alınıp n ile mod işlemine tabi tutulmaktadır.

Çözülmüş Metin = 25^3 (mod 33)
Çözülmüş Metin = 15625 (mod 33)
Çözülmüş Metin = 16

Bu örnekte şifrenin kırılması için gerekli olan d sayısı herkese açık olan N sayısından bulunabilir. Tek yapılması gereken N sayısının asal çarpanlarına ayrılmasıdır. 33 sayısının asal çarpanları;
33 = 3x11

Verilen bu örnekte özel anahtar çok kolay bir şekilde bulunabildiğinden şifrenin kırılması işlemi basit olmaktadır. Bunun önlenmesi için 128 bit vb. şifreleme yöntemleri ile çok büyük asal sayılar kullanılmaktadır. Ortalama 45 haneli iki asal sayının çarpımı 90 haneye yakın bir sayı çıkmaktadır. Dolayısıyla bu tip bir sayıyı asal çarpanlarına ayırmak çok kolay değildir. 128 bitlik bir şifrenin çözülmesi için ihtimal sayısı 2^{128}'dir. Bu ihtimalin normal bir bilgisayar ile ortalama 2 trilyon yılda çözülebileceği belirtilmiştir. Japonya'da 64 bitlik bir şifre yaklaşık 100.000 bilgisayarın beraber çalışması neticesinde yaklaşık 3,5 yılda çözülmüştür.

2. GÖRÜNTÜ ŞİFRELEMEYE GİRİŞ

Teknolojik gelişmelerin çok hızlı olduğu günümüzde haberleşme, iletişim ve bilgiye erişim gün geçtikçe hızlanmaktadır. Bu gelişmeler paralelinde kişi ve kurumlar, gerek kişisel ihtiyaçlarında, gerekse kurumsal ihtiyaçlarında elektronik ortamı yoğun olarak kullanmaktadırlar. Artık kağıt ortamında bilgi tutma faaliyetleri sona ermek üzeredir. Önceleri insanlar hatıra defterleri ve şiir defterleri yazar, kişisel fotoğraflarını albümlerde muhafaza ederlerdi. Kurumlar da yazışmalarında, arşiv kayıtlarının saklanmasında, mali gelir-gider tablolarının hesaplanmasında vs. kağıt kullanırlardı. Fakat günümüz teknolojilerinde bütün bunları daha kolay bir şekilde yapabilecekleri elektronik ortamlar gelişti ve gelişmeye devam etmektedir.

Elektronik ortam; verilerin üzerine kaydedilip saklandığı ortamların genel adıdır. Bu ortamda saklanan bilgiler çok sayıda kişinin erişimine açık olacağından “bilmesi gereken” prensibine göre bu bilgilere kimin erişebileceğini belirlememiz gerekmektedir. Bu ihtiyaç elektronik ortamda güvenlik kavramını ortaya çıkarmıştır.

Günlük hayatımızda resimler geniş bir kullanım alanına sahiptir. Yoğun kullanılıyor olmasından dolayı da onların güvenliğinin sağlanması büyük önem kazanmaktadır. Kişisel resimlerimizin saklanması, askeri bir tatbikat görüntülerinin komuta karargahına aktarılması, insansız hava araçlarının istihbari maksatla çektiği görüntülerin ana üsse aktarılması, banka binalarının planlarının muhafazası vb. hususlarda güvenliğe çok önem verilmektedir. Bu güvenliği sağlamanın yollarından birisi ve belki de en önemlisi bu resimlerin şifrelenmesi ve şifreli halinin saklanması veya gönderilmesidir.

Birçok geleneksel ya da modern şifreleme teknikleri text verilerini korumak için tasarlanmışlardır. Fakat resimler text’ten farklıdır. Resimleri şifrelemek için geleneksel şifreleme tekniklerini (RSA ve DES gibi) kullanabilmemize rağmen bu teknikler iki nedenden dolayı uygun değildir; birincisi resimlerin boyutları text verisinden genellikle daha büyüktür. Bu nedenle resimleri bu yöntemlerle şifrelemek için daha fazla zamana ihtiyaç duyulmaktadır. Diğer neden de, şifreli resim verisinin şifresi çözüldüğünde, şifresi çözülen resmin orijinal resme birebir eş olması zorunluluğu yoktur. İnsan algısının karakteristiklerine göre resimdeki ufak bozulmalar genellikle kabul edilebilir durumdadır.

2.1. Sayısal Görüntü Elemanları

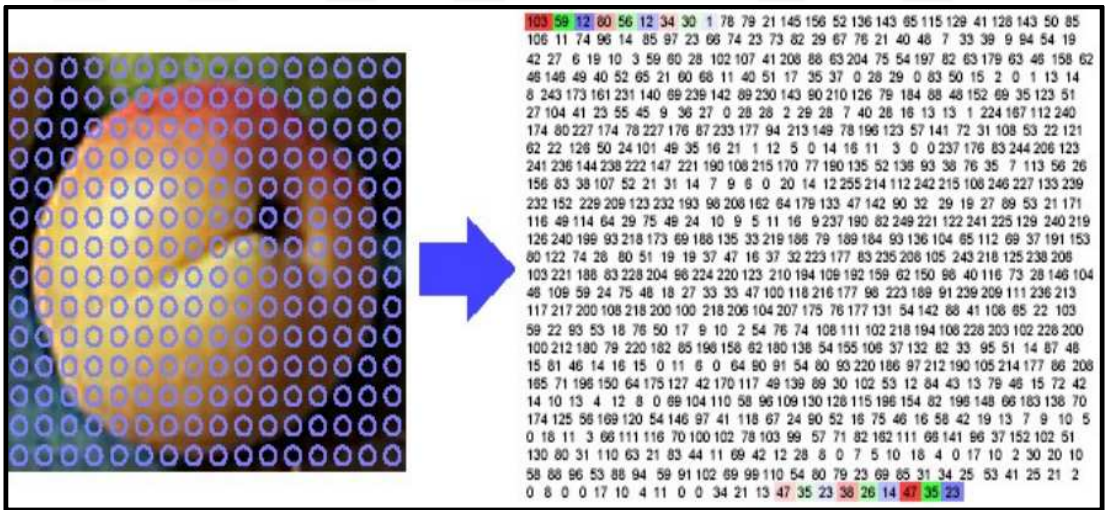
Görüntü şifreleme algoritmalarına geçmeden önce devam eden alt başlıklarda görüntü ile ilgili temel bileşenlerin ne olduğuna değinilecektir.

2.1.1. Sayısal görüntü ve piksel kavramı

Sayısal görüntü, temel anlamda piksel öğelerden oluşan görüntüdür. Başka bir ifadeyle sayısal görüntü, piksel öğelerden oluşan elektronik bir fotoğraftır. Her bir piksel öğesi siyah, beyaz ve grinin bir tonu ile ya da bir rengi içeren bir renk tonu değeri ile temsil edilmektedir. İki rakamlı sıfır ve birlerden oluşan kodlar bu sayısal görüntüleri bilgisayar ortamında karakterize etmektedir [27].

I(x,y) analog bir görüntü veya resim olsun; “I” bir şiddet birimi (örneğin parlaklık), “x” ve “y” ise görüntünün yatay ve dikey eksen koordinatlarına karşılık gelen değerlerdir. Sayısal görüntü ise, bu analog görüntünün M sütun ve N satırdan oluşacak şekilde örneklenmesi sonucu elde edilir. Satır ve sütunun kesiştiği her bir bölgeye piksel adı verilir. Sayısal görüntüye çevrilen bir resimde NxM adet piksel bulunur.

Analog bir görüntü ve bu görüntünün sayısal görüntüye çevrilmiş hali Şekil 2.1’de gösterilmektedir.



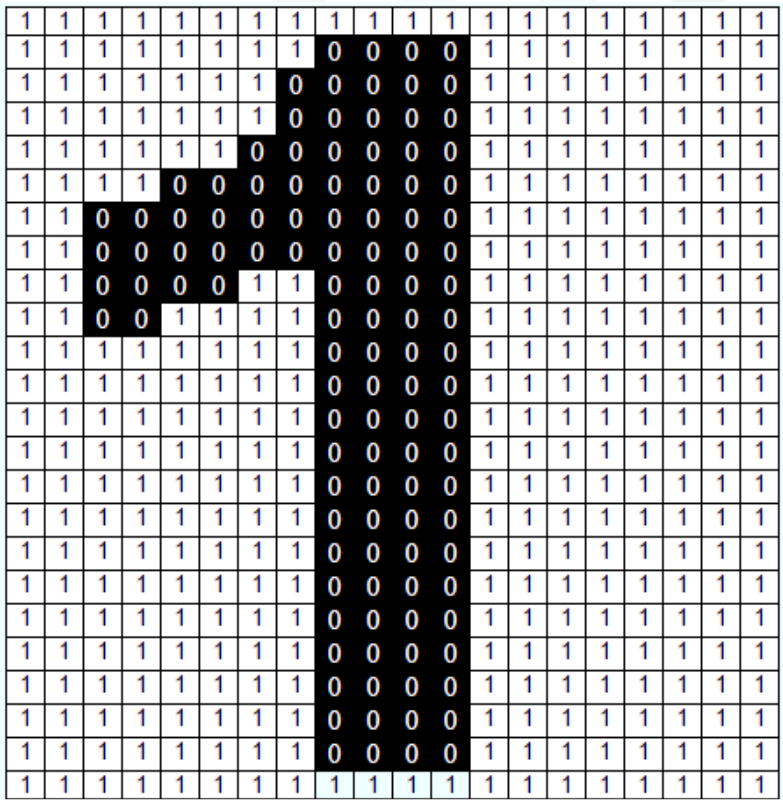
Şekil 2.1. Gerçek görüntü ve sayısal görüntü [28]

Sayısal görüntülerin temel yapı taşı olan noktalara piksel denir. Sayısal görüntüler, yatay ve dikey olarak yan yana sıralanmış piksellerden oluşmaktadırlar. Eğer bir görüntüde piksel sayısı çok ise , o görüntü o derece kalitelidir. Eğer görüntüde piksel sayısı az ise, yeterince net olmayan ve bulanık hatlı bir görüntünün oluşması söz konusudur.

Bir pikselin iki temel özelliği söz konusudur [29]:

- Radyometrik özelliği: Pikselin algılandığı elekromanyetik spekrumdaki gri değeri ifade eder.
- Geometrik özelliği: Görüntü matrisinde sahip olduğu matris koordinatlarını ifade eder.

İki gri değerden oluşan resim “siyah-beyaz resim” olarak adlandırılmaktadır. Siyah beyaz resimdeki pikseller ya siyah ya da beyazdır. Şekil 2.2’de örnek olarak verilen sayısal görüntüde beyaz pikseller 1, siyah pikseller 0 değeri ile gösterilmektedir. Bu şekilde 0 ve 1 ile kodlanmış piksellerden oluşan görüntülere ikili görüntü (binary image) adı verilir.



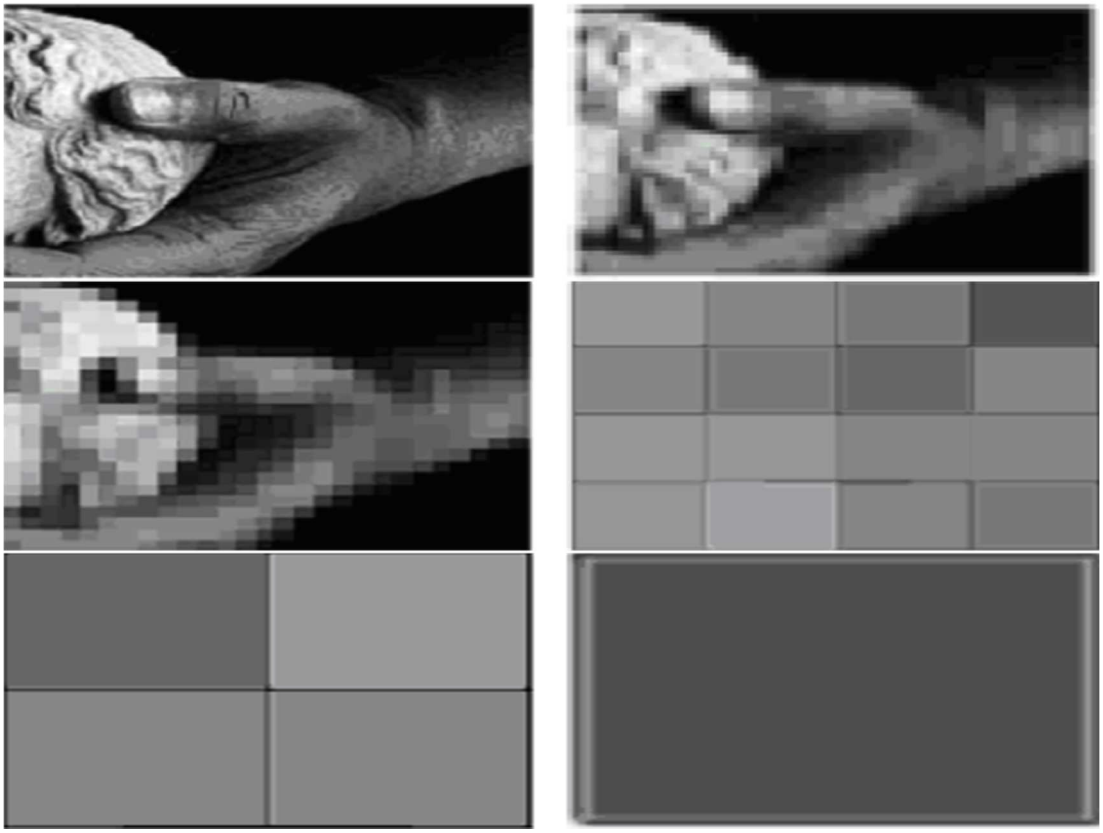
Şekil 2.2. İkili görüntü [30]

Tablo 2.1’de ise MxN boyutlarındaki bir görüntünün herhangi bir pikselinin koordinat sisteminde gösterimi verilmektedir.

Tablo 2.1. Bir pikselin koordinat sisteminde gösterilmesi [30]

	1	2	3	.....	M
1					
2		(x-1,y-1)	(x-1,y)	(x-1,y+1)	
3		(x,y-1)	(x,y)	(y,y+1)	
.....		(x+1,y-1)	(x+1,y)	(x+1,y+1)	
N					

Herhangi bir görüntü büyüdükçe görüntüdeki detay yorumlama olanağı gittikçe yok olur. Yani görüntü büyüdükçe görüntünün netliği azalır ve bulanıklaşır. Böylece görüntünün kalitesi de azalır. Şekil 2.3'te bu durum açıkça görülmektedir.



Şekil 2.3. Bir görüntünün orijinal hali ve büyütülmüş hallleri [30]

Şekil 2.3'te sol üstte orijinal görüntü olmak üzere, görüntü büyütülmeye başlandığında en son sağ alttaki görüntü elde edilir. Bu da, piksele götürür. Şekil 2.3'teki görüntü ile Şekil 2.2'deki ikili görüntü arasındaki temel farklılık, her pikselin gri değerinin farklı

olmasıdır. Oysa ikili görüntüde pikseller 0 veya 1 değeri alabiliyordu. Daha başka bir deyişle ya siyah ya da beyaz olabiliyorlardı.

Gri tonlu görüntülerde; görüntü farklı gri ton değerlerinden oluşur. Gri değer aralıkları G={0,1,2,……..255} şeklinde ifade edilir. Bunun anlamı şudur: Bir gri tonlu görüntüde 256 tane farklı gri ton değeri daha doğrusu gri değer bulunabilir. Burada 256 gri değer bir byte ile temsil edilir (1 Byte=8 Bit ve 2^8=256). 0 gri değeri kural olarak siyah renge, 255 gri değeri ise beyaz renge karşılık gelir. Bu değerler arasında ise gri tonlar oluşur.

Görüntünün kalitesini etkileyen bir diğer unsur da görüntüdeki piksel sayısıdır. Buna ilişkin örnek görüntüler Şekil 2.4'te gösterilmektedir.



Şekil 2.4. Farklı çözünürlüğe sahip görüntüler [30]

2.1.2. Renk kavramı ve renkli görüntü

Renk, ışığın gözün retinasına değişik biçimde ulaşması ile ortaya çıkan bir algılamadır. Bu algılama, ışığın maddeler üzerine çarpması ve kısmen soğurulup kısmen yansıması nedeniyle çeşitlilik gösterir ki bunlar renk tonu veya renk olarak adlandırılır. Tüm dalga boyları birden aynı anda gözümüze ulaşırsa bunu beyaz, hiç ışık ulaşmazsa siyah olarak algılarız. İnsan gözü 380nm ile 780nm arasındaki dalgaboylarını algılayabilir, bu sebepten elektromanyetik spektrumun bu bölümüne görünen ışık denir. Göz, üç temel birleştirici renk olan kırmızı, yeşil ve mavi renklere tekpi verir ve beyin, diğer renkleri bu üç rengin farklı kombinasyonları olarak algılar. Renklerin algılanışı dış koşullara bağlı olarak değişmektedir. Aynı renk güneş ışığında

ve mum ışığında farklı algılanabilmektedir. Fakat insanın görme duyusu ışığın kaynağına uyum sağlayarak, onların her iki koşulda da aynı renk olduğunu algılar [31].

Renkli görüntü R(Kırmızı), G(Yeşil), B(Mavi) olarak kodlanmış aynı objeye ait üç adet gri düzeyli görüntünün üst üste ekrana iletilmesi ile oluşur. Elektromanyetik spektrumda 0,4-0,5 nm dalga boyu mavi renge; 0,5-0,6 nm dalga boyu yeşil renge; 0,6-0,7 nm dalga boyu kırmızı renge karşılık gelir. Bu dalga boylarında elde edilmiş üç gri düzeyli görüntü bilgisayar ekranında sırası ile kırmızı-yeşil-mavi kombinasyonunda üst üste düşürülecek olursa renkli görüntü elde edilmiş olur [29].

Renklerin algılanması, ışığın bir cisme çarparak yansıması ve cismin göz yardımıyla beyne iletilmesi sayesinde gerçekleşir. Biz bir cismi sadece gözlerimiz cismin yansıttığı ışık tarafından uyarıldığı zaman görür ve bunu bir renk olarak algılarız.

Beyaz ışığın bir prizmadan geçmesi durumunda ışığın kırıldığı ve gökkuşağının yedi rengine ayrıldığı görülür. Bu ışık bir cisimle karşılaştığında, bir bölümü cismin üzerine yansır. Bizim cismin rengi olarak algıladığımız işte bu yansımadır.

İnsanların algılayabildiği iki çeşit renk vardır. Bunlardan birisi ışık yayan bir cismin rengidir ve “direkt renk” olarak adlandırılır. Diğeri ise aydınlatılmış bir cismin rengidir ve “yansıyan renk” olarak adlandırılır. Işık yayan bir cisim, güneş gibi doğal veya bilgisayar ekranı, ampul gibi yapay olabilir. Yansıyan renk, aydınlatılmış bir cismin rengidir. Bu renk cismin yüzeyinden ve yüzeyinin iç kısmından yansıyan ışığın bir birleşimidir.

RGB renk modeli, İngilizcedeki “red”, “green” ve “blue”, yani “kırmızı”, ”yeşil” ve ”mavi” kelimelerinin baş harflerinden ismini alan bir renk uzayıdır. Bu üç renk %100 oranında karıştırıldığında beyaz renk ve %0 oranında karıştırıldığında siyah renk elde edilir. Ana renkler olan kırmızı, mavi ve yeşilin karışım oranı değiştikçe yeni renkler meydana gelir.

2.1.3. Renk modelleri

Temel olarak kabul edilen üç renk modeli vardır. Bunlar RGB, CMYK (Cyan, Magenta, Yellow, Key-Cam Göbeği, Mor, Sarı, Siyah) ve LAB renk modelleridir. Bunların yanında HSL (Hue, Saturation, Lightness-Ton, Doygunluk, Aydınlık), HSV (Hue, Saturation, Value-Ton, Doygunluk, Değer) ve CIE (Caotic Image Encryption-Karmaşık Görüntü Şifreleme) renk modelleri ve baskı ortamlarında kullanılan, Pantone, Tire ve Dublex isimli modeller de vardır.

2.1.3.1. RGB renk modeli

RGB modeli bilgisayar ekranları veya katodik televizyon tüpleri gibi, doğrudan emilimle çalışan cihazlarda kullanılmaktadır.

RGB modeli ismini; Red (Kırmızı), Green (Yeşil), Blue (Mavi) kelimelerinin kısaltmasından alır. İnsanın gözünde bulunan ve bu renklere denk gelen ışık dalgaboyu sensörleri bu modelin temelini oluşturur. Bunların arasında kalan dalgaboylarında da bu üç sensörün herbiri değişik seviyelerde tepki verir ve bu tepki beyinde renk algısını yaratır. Örneğin gökkuşağının sarı olarak adlandırdığımız dalgaboyunda bir ışık gözümüze düştüğünde ağırlıklı olarak kırmızı ve yeşil sensörler uyarılır. Beynimizde bu kombinasyon sarıya dönüşür. Kırmızı ışık geldiğinde ise sadece kırmızı sensörler uyarılır. Hem kırmızı hem yeşil hem de mavi ışığın aynı anda gelmesi ile tüm dalgaboylarının aynı anda gelmesi aynı etkiyi yaratır ve beynimiz beyaz ışığı algılar. Bu nedenle, bu üç renkte ışık kaynaklarımız varsa ve şiddetlerini de sönük ve parlak olarak ayarlayabiliyorsak, tüm renkleri elde etmemiz mümkündür.

RGB modelinin kullanımı çok yaygındır, fakat donanıma da çok bağımlıdır. Donanımın değişmesi rengin de değişmesine neden olur. Bu sebeple tarayıcı, ekran ve yazıcı gibi donanımlarda kullanımı uygun değildir.

2.1.3.2. CMYK renk modeli

CMYK, RGB'den oldukça farklı bir renk modelidir. Adını Cyan, Magenta, Yellow ve Key renklerinin baş harflerinden alan CMYK, baskı işlemlerinde kullanılan renkleri belirtir. Işığı baz alan RGB uzayının bileşenlerini tanımlamakta üç renk kullanılır ve RGB renk uzayında tüm renkler "pigment" tabanlıdır. CMYK renk uzayına ismini veren renklerin Türkçedeki tam karşılığı; Cyan-Cam Göbeği, Magenta-Mor, Yellow-Sarı ve Key-Siyah şeklindedir. Matbaa teknolojinin gelişmesi ile birlikte kullanılması zorunluluk haline gelen CMYK renk uzayı, bilgisayarın her eve girmesi ile birlikte ev kullanıcılarının kullandığı yazıcılar için de temel renk uzayı olmuştur.

CMYK renk uzayının yeni nesil matbaacılık işlerinde kullanılması ile birlikte bazı sorunlar da oluşmuştur. Turuncu gibi bazı renklerin baskı sonrası tatmin edici sonuçlar vermemesi ve gereken kaliteye ulaşılamaması, matbaacılıkta kullanılan CMYK renk uzayının eksilerinden biri olarak görülür. CMYK renk uzayının matbaacılık açısından en çok eleştirilen bir diğer yönü de baskı maliyetlerini yükseltmesidir. Zira bazı temel renklerin basılması için dahi birden fazla bileşenin kullanılması baskı maliyetlerinin hatırı sayılır bir oranda artmasına neden olmaktadır. Örneğin; ana

renklerden biri olarak kabul edilen yeşil rengin baskısında dahi Sarı yani Yellow ve Cam Göbeği yani Cyan bileşenlerin karıştırılması gerekir.

Teknolojik anlamda baskı tekniklerinin çok daha kaliteli ve işlevsel hale gelmesini sağlayan CMYK renk uzayı, pratik uygulamalarda bir takım sorunlara neden olsa da dünya genelinde kabul görmüştür. Şüphesiz birçok teknolojinin geliştirilmesi esnasında öncelik insan ihtiyaçlarının karşılanması olduğundan, ortaya çıkan yeni teknolojinin üretim maliyetleri ile ilgili sorunlar ilk aşamada düşünülmemektedir. Sürekli olarak gelişen teknoloji sayesinde tüm sektörlerde olduğu gibi matbaacılık sektöründe de daha işlevsel ve ekonomik çözümler aranmış ve sonuç olarak da ortaya CMYKOG (Cyan, Magenta, Yellow, Black, Orange, Green-Cam Göbeği, Mor, Sarı, Siyah, Turuncu, Yeşil) denen renk uzayı çıkmıştır. Hexachrome olarak da adlandırılan CMYKOG renk uzayında tahmin edilebileceği gibi 4 değil 6 renk bileşeni kullanılmaktadır.

Hexachrome renk uzayı matbaacılık işlemlerinde daha işlevsel ve daha da önemlisi daha ekonomik çözümler sunmaktadır. Dijital baskı teknolojilerinin oldukça geniş imkanlar sunması ve basım tekniklerinin gerçek anlamda kimlik değiştirmesi ile birlikte çıkan matbaacılık ihtiyaçlarının daha geniş kapsamda karşılanmasını sağlayan CMYKOG renk uzayı, 6 bileşenli yapısıyla baskı maliyetlerinin de ciddi oranda azalmasını sağlamıştır [32].

2.1.3.3. CIE-Lab renk modeli

Lab modeli doğada var olan renklerin gözle görülebilen en geniş alanını ölçmeye yarayan uluslararasi bir ölçü standardıdır. Bu yolla renkleri ölçebilir ve kodlayabiliriz.

CIE Lab renk modeli, rengin insan tarafından algılanış şeklini temel alır. Lab modelindeki sayısal değerler, normal görme yeteneğine sahip bir insanın gördüğü tüm renkleri tanımlar. Lab modelinde bir aygıtın (sözgelimi monitör, masaüstü yazıcısı veya dijital kamera) renkleri oluşturması için belirli bir renk verici öğeden ne kadar gerektiğinden ziyade rengin nasıl göründüğünü tanımladığından, Lab modeli aygıttan bağımsız bir renk modeli olarak kabul edilir. Renk yönetimi sistemleri Lab modelini, bir rengi bir renk uzayından diğerine, sonuçları önceden tahmin edilebilecek şekilde dönüştürmek için kullanır [33].

2.1.3.4. HSL ve HSV renk modelleri

HSL kısaltmasındaki harfler, tonlamaları, doygunluğu (matlık ve parlaklığı) ve aydınlığı (açıklık ve koyuluğu) temsil eder. Model bazı bilgisayarlar tarafından

desteklenmemektedir. Daha az yaygın olan HSB (Hue, Saturation, Brightness-Ton, Doygunluk, Parlaklık) ve HCL (Hue, Chroma, Luminance-Ton, Renk Parlaklığı, Işık) modelleri de HSL'nin kapsadığı modellerdir. Bir resim üzerinde detay kaybetmeden renk değişiklikleri yapma olanağı verirler.

HSV renk uzayı 1978 yılında Alvy Ray Smith tarafından tanımlandı. Amacı RGB uzayına göre insan görü düzeneğine daha yakın bir yapı oluşturmaktı. HSV, RGB renk uzayından doğrusal olmayan bir dönüşüm ile elde edilir. HSV ayrıca aygıt bağımlıdır. Yani bu uzayda tanımlı bir renk, rengi üreten cihaza göre değişim gösterebilir. Cihazdan bağımsız renk gösterimi icin CIE Lab kullanılmalıdır [34].

2.2. Sayısal Görüntü Formatları

Temel olarak üç çeşit görüntü dosyası vardır: Bunlar bitmap, vektör ve meta dosyalarıdır. Bitmap, bilgisayar ekranında bir resmi görüntülemek maksadıyla her piksel için renk bilgilerinin verildiği resim formatlarına verilen genel addır. Vektörel görüntü dosyalarında ise görüntü matematiksel veri olarak kaydedilir ve çözünürlükten bağımsızdır. Matematiksel ifadelerle oluşturulduğundan detay kaybetmeden herhangi bir boyuta yeniden ölçeklendirilebilen grafik türüdür. Meta dosya formatlarında ise görüntü hem piksel (bitmap) hem de matematiksel veri olarak ya da bunların her ikisi olarak kaydedilebilir.

Büyük kapasitedeki görüntü dosyalarının açılması uzun sürer, bilgisayar sabit belleğinde çok yer kaplar ve yazıcıdan çıktısının alınması da uzun sürer. Küçük boyutlu görüntü dosyalarında ise daha iyi performans elde edilir. Tüm görüntü tipleri için kullanılabilir tek bir görüntü formatı mevcut değildir. Farklı boyutta görüntüler için farklı tipte görüntü formatları kullanılmaktadır.

En çok bilinen ve kullanılan görüntü formatları aşağıdaki bölümlerde açıklanmaktadır.

2.2.1. BMP görüntü formatı

BMP Windows işletim sisteminin kullandığı bir görüntü dosya biçimidir. BMP formatı sıkıştırma yapmadığı için PNG, JPEG gibi görüntü formatlarına göre çok daha fazla yer kaplamaktadır. Bu format 16 ya da daha çok renk kaydedilebilen oldukça hızlı bir formattır. Bu formatta görüntü içerisindeki renk sayısından çok görüntünün büyüklüğü önemlidir.

BMP formatının avantajı; bütün pikseller herhangi bir değişiklik ve modifikasyon için birbirinden bağımsızdır. Bu değişiklikler görüntünün kalitesinde azalmaya neden olmaz. En önemli dezavantajı ise bu dosyaların boyutunun büyük olmasıdır. Genel

olarak BMP dosyaları başlık ve görüntü hakkında tanımlayıcı bilgi (genişlik, yükseklik gibi) ile görüntü piksellerinin gerçek değerlerini içeren tablo ve piksel veri alanlarından oluşur.

2.2.2. GIF görüntü formatı

GIF, 1987 yılında CompuServe tarafından geliştirilmiştir. Bu format web grafikleri ve bilgisayarlar arası grafik dosyaları alışverişi için en popüler dosya formatlarından birisidir. GIF, 8 bit renge (yani 256 renk) kadar destek verir. Bilinen bütün tarayıcılar tarafından görüntülenebilir. Az renk içermesi nedeniyle genelde grafiklerin saklanması için kullanılır. GIF ayrıca yüksek çözünürlük gerektirmeyen animasyonlar için de kullanılabilir.

GIF dosyaları kaydedildiği zaman otomatik olarak LZW (Lempel, Ziv, Welch) olarak bilinen sıkıştırma metodu ile kayıpsız olarak sıkıştırılmaktadır. Bu sıkıştırma metodunda kayıp olmadığı için görüntü kalitesinde azalma da meydana gelmemektedir.

GIF'in güçsüz yanı en fazla 256 rengi destekliyor olmasıdır. Farklı formattaki bir görüntü dosyası GIF formatına dönüştürüldüğünde, program görüntüyü 24 bit renkten 8 bit renge düşürmüş olur. 24 bit milyonlarca rengi destekliyor iken, 8 bit sadece 256 rengi desteklediğinden bu dönüştürme işlemi neticesinde, görüntüdeki renk kalitesinde azalma meydana gelmektedir. Bu nedenle, genellikle dijital fotoğrafçılıkta kullanılmamaktadır.

2.2.3. JPEG görüntü formatı

JPEG görüntü formatı, en popüler web grafik formatlarından bir diğeridir. 24 bit renk desteği vardır. JPEG dosya formatı RGB renk modelinin kullandığı renklerin hepsini içermektedir.

JPEG, sıkıştırma (zip) programlarının kullandığı sıkıştırma algoritmasını kullanmaktadır. Sıkıştırma metodunda kayıplar olmaktadır. Bu nedenle sıkıştırma neticesinde görüntü kalitesinde bir miktar azalma olmaktadır.

JPEG'in avantajlı yönü yüksek sıkıştırılabilme kabiliyetidir. Bu nedenle JPEG dosyalarının boyutu düşüktür. Boyutunun düşük olması internette en çok kullanılan resim formatı olmasını sağlamıştır. Dezavantaj olarak da sıkıştırma neticesinde kalitede azalma meydana gelmesini söyleyebiliriz. Sıkıştırma arttıkça görüntüdeki detay ve kalite daha da azalmaktadır. Sıkıştırma oranın artmasıyla keskin hatların

etrafında dalgalanmalar ve detay kaybı, daha yüksek sıkıştırma oranlarında da bloklanma belirgin hale gelir.

2.2.4. PICT görüntü formatı

PICT formatı, öncelikli olarak Macintosh platformunda kullanılmaktadır. Standart meta dosya formatı olarak Macintosh görüntü dosyaları için varsayılan görüntü formatıdır. PICT formatı en çok bitmap görüntülerinde kullanılmaktadır. Fakat vektörel görüntülerde de kullanılabilir. PICT formatı Macintosh platformlarında sınırlı miktarda sıkıştırmayı desteklediğinden, bu dosyaların kapasitesi genellikle büyüktür. Bu nedenle bu formattaki dosyalar daha çok video düzenleme, animasyonlar, bilgisayar sunumları ve multimedya yazma maksatlarıyla kullanılır.

2.2.5. EPS görüntü formatı

EPS formatı, görüntü dosyalarını grafik dosya formatı olarak kullanılabilir hale getirmek niyetiyle kullanılmaktadır. EPS formatı bir meta dosya formatıdır. Yani hem bitmap görüntülerinde hem de vektörel görüntülerde kullanılabilmektedir. EPS formatı ayrıca Windows ve Macintosh dahil olmak üzere değişik platformlar üzerinde kullanılabilmektedir. Bir EPS formatlı görüntüyü bir dokümana yerleştirip, bu görüntüyü aşağıya ya da yukarıya doğru ölçeklendirdiğimizde görüntü kalitesinde azalma meydana gelmemektedir.

2.2.6. PNG görüntü formatı

PNG formatı, bir bitmap görüntü formatı olmakla beraber kayıpsız sıkıştırma yapma kabiliyetine sahiptir. GIF formatının varisi olması ve ağ üzerindeki görüntüler için ana format olması hedeflenmiştir. PNG’nin geliştirilmesini doğuran etken, Unisys firmasının GIF’de kullanılan LZW algoritması üzerindeki patent hakkının ihlallerini takip edeceğini duyurması olmuştur. GIF'deki LZW algoritması yerine PNG'de, patent problemi olmayan zip, gzip ve türevlerince de kullanılan LZ77 algoritması kullanılmaktadır. Benzer ayarlarda LZ77 algoritmasının LZW algortiamsına göre daha iyi neticeler verdiği görülmüştür. Ancak, her iki algoritma da resmin iki boyutlu doğasını gözardı ederek, resimleri tek boyutlu veri dizisi kabul ederek sıkıştırma işlemi yaptıklarından optimum kayıpsız iki boyutlu sıkıştırmadan uzaktırlar.

PNG platformdan bağımsızdır. GIF ile karşılaştırıldığında PNG daha iyi renk desteği, daha iyi saydamlık ve gelişen görüntü gösterimi için daha iyi bir metod sunmaktadır.

2.2.7. TIFF görüntü formatı

TIFF formatı, uygulama ile yazılım platformları arasında bitmaplerin değişimi ve depolanması için kullanılan, etiket tabanlı uluslararası bir standarttır. TIFF, bir çok yazılım uygulaması ile uyumludur ve Windows, Macintosh ve Unix gibi platformlar arasında kullanılabilirliği vardır. TIFF karmaşık bir formattır. Bu nedenle dosya boyutu genellikle GIF ve JPEG formatlı dosyalardan daha büyüktür. TIFF kayıpsız LZW sıkıştırmasını destekler. Bununla beraber sıkıştırılmış bir TIFF formatlı dosyayı açmak daha uzun sürer.

2.3. Şifrelenmiş Resimlere Karşı Yapılan Saldırı Türleri

Kurumlar ve şirketler şifreleme sistemleri kurduklarında ilk önce bu sistemin ne kadar güvenli olduğunu öğrenmek istemektedirler. Bu nedenle sistemin güvenliğini test etmek için bazı saldırı senaryoları gerçekleştirmektedirler. Bu saldırı senaryolarını genelde kurum dışından, bu iş için ehil kişi ve firmalara yaptırmaktadırlar.

Şifrelenmiş resimlerin güvenliğinin test edilebilmesi için bazı saldırı tipleri mevcuttur. Saldırı yapan kişinin kullanılan şifreleme algoritmasını bildiği varsayılarak yapılan bu saldırı tipleri şunlardır:

2.3.1. Cipherimage-only attack (Sadece şifreli resim saldırısı)

Bu saldırı yönteminde, saldırıda bulunan yetkisiz kişinin ağ üzerinden şifreli resimi bir şekilde elde ettiği, ancak şifreli resme ait olan gizli anahtara sahip olmadığı varsayılmaktadır. Burada amaç şifreli resmi kullanarak gizli anahtara ulaşmaktır.

2.3.2. Known-plainimage attack (Bilinen şifrelenmemiş resim saldırısı)

Bu saldırı yönteminde, saldırıda bulunan yetkisiz kişinin birkaç şifrelenmemiş resim ve şifrelenmiş resim çiftini ele geçirdiği varsayılır. Burada amaç şifrelenmemiş resimleri şifrelemek için kullanılan anahtarı belirlemek ya da şifreli resimleri çözebilecek bir algoritma geliştirmektir.

2.3.3. Chosen-plainimage attack (Seçilen şifrelenmemiş resim saldırısı)

Bu saldırı yönteminde saldırıda bulunan kişi, şifrelenmemiş resimleri ve onların şifreli halini seçebilmektedir. Bu yöntem bilinen şifrelenmemiş resim saldırısı yönteminden çok daha etkili bir yöntemdir. Çünkü saldırgan, şifrelemek için bazı özel şifrelenmemiş resimleri kendisi seçebilmektedir. Bu sayede gizli anahtar hakkında daha fazla bilgi edinebilmektedir.

2.3.4. Jigsaw puzzle attack (Kesik parçaları birleştirme saldırısı)

Bu saldırı yönteminde saldırıda bulunan kişi, şifreli resmi küçük parçalara ayırmaktadır. Daha sonra bu küçük parçalar saldırgan tarafından teker teker kırılmaktadır. Her bir parça resmin tamamından daha küçük olacağından, parçaların şifresini kırmak için gereken zaman şifreli resmin şifresini kırmak için gereken zamandan çok daha az olacaktır. Bu nedenle bu yöntem diğer saldırı yöntemlerinden daha etkili bir yöntemdir.

2.3.5. Neighbor attack (Komşu saldırılar)

Bu saldırı yönteminde saldırıda bulunan kişinin, şifreli resmin bir bölümünü bildiği varsayılmaktadır. Birçok resimde alan sınırları boyunca değişimler düzgündür. Bu nedenle şifre çözücü bu özelliği kullanarak komşu olan alanların sınırlarını daha kolay seçebilmektedir. Birçok resim düzgün bir yapıda olduğundan, şifre çözücü resmin bilinen kısmı için komşu olan pikselleri elde edebilmekte ve tüm şifreli resmi çözebilmektedir [35].

3. GÖRÜNTÜ ŞİFRELEME YAKLAŞIMLARI

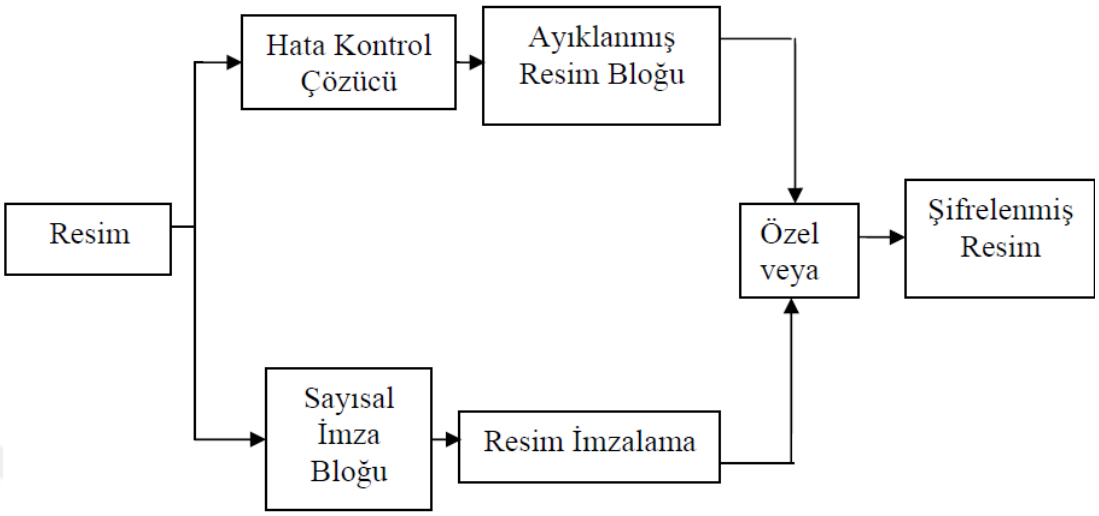
3.1. Sayısal İmza Kullanarak Görüntü Şifreleme

Elektronik ticrette veri alışverişinin ilerlemesiyle bilgi güvenliği kavramının önemi gün geçtikçe daha da artmaktadır. Görüntüler günlük hayatımızda önemli faydalar sağlamaktadır. Görüntüler birçok güvenlik doğrulama sisteminin temelini oluşturur ve insanların kimliklendirilmesi, kartların tanımlanması ve başka tanımlama işlevlerinde yaygın olarak kullanılmaktadır. Bu nedenle güvenilir görüntü şifreleme teknikleri sahtecilik, tahrifat ve yetkisiz erişime karşı verilerin korunması için büyük önem arz etmektedir. Görüntü şifreleme teknikleri yetkisiz kullanıcılar tarafından anlaşılamayan rastgeleliğe dayalı bir yöntem kullanır. Bir ana görüntü şifreleme tekniği, birincil görüntünün iki rastgele faz maskesi ile kodlanmış bir işlemini içerir. Maskelerden biri giriş düzlemine, diğeri ise uzamsal frekans düzlemine yerleştirilir. Bu durum sabit beyaz bir gürültü oluşturur. Çözme sürecinde, kodlanmış veya şifrelenmiş görüntü Fourier dönüşümüne tabi tutulur. Daha sonra rastgele sıralı bir faz maskesi kompleks eşleniği ile çarpılır. Son olarak ters Fourier dönüşüm işlemi yapılır. Yapılan tüm bu işlemler çift rastgele faz kodlama sistemi olarak bilinmektedir. Çift rastgele faz kodlama sisteminin optik uygulamalarının yapıldığı da bilinmektedir. Şifreli görüntü, rastgele faz maskesinin faz eşleniği kullanılarak yapılan bir referans ışını ve görüntü şifre çözme işlemini kullanan bir hologram olarak kaydedilir.

Sayısal imza kullanılarak görüntü şifreleme tekniğinde amaç görüntüyü şifrelemek ve iletimden önce görüntünün içine sayısal imza gömmektir. Orijinal resmin sayısal imzası, orijinal resmin kodlanmış verisine eklenmektedir. Sayısal imzaya, alıcıda geri dönüştürülebilir ilave gürültü gibi muamele edilir. Sayısal imzayı geri dönüştürebilmek için bir hata kontrol kodu orijinal görüntüyü kodlamak için kullanılır. Hata kontrol kodu orijinal görüntüye bit olarak eklenir. Hata kodlama yöntemi, gürültü nedeniyle bozulmuş bitlerin geri kazanılabilmesi için kullanılır.

Sayısal imza, hata kontrol kodundan sonra görüntüye eklenen gürültüdür. Ekleme işlemi XOR işlemine eşittir. Resmin kodlama işlemi BCH gibi uygun bir hata kodlama yöntemiyle yapılmaktadır. Şifreleme işleminin blok diyagramı Şekil 3.1'de gösterilmektedir. Burada orijinal resim sayısal imzanın oluşturulması için kullanılmıştır. Görüntü daha sonra uygun bir BCH kodu kullanılarak kodlanmıştır.

Sayısal imza kodlanmış görüntüye bloklar halinde eklenmiştir. Sonuç olarak şifreli görüntü elde edilmiştir.



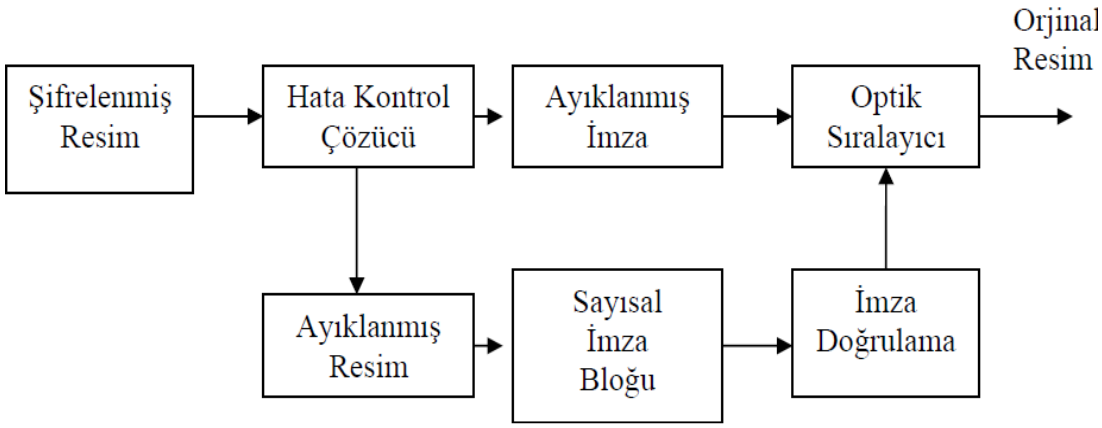
Şekil 3.1. Sayısal imza tekniği ile şifreleme işleminin blok diyagramı [14]

Görüntü şifreleme sistemi görüntülerin tüm boyutları ele alınarak tasarlanmıştır. Bununla birlikte standart bir algoritma tarafından üretilen sayısal imza, genellikle 128 bit olmak üzere, önceden belirlenmiş bir uzunlukta oluşturulur. Bu nedenle hata kontrol algoritması giriş görüntüsünün boyutuna bağlı olarak seçilmelidir. Orijinal görüntü boyutu küçükse güçlü bir hata kontrol kodu kullanılır. Orijinal görüntü boyutu büyükse aksine daha zayıf bir kod kullanılır. Hata kontrol kodu ne kadar güçlü olursa görüntünün boyutu da buna paralel olarak artacaktır. Şifreli mesaj ya iletilecektir ya da kaydedilecektir. Bu nedenle görüntüye gerektiğinden fazla ekleme yapılmaması depolama, band genişliği kullanımı gibi nedenlerden dolayı önemlidir. Buna karşın, fazla ekleme yapılması performansı düşürürken güvenliği ise artırmaktadır.

Hata kontrol kodunun seçimi ile ilgili karar, şifreleme sistemine giriş olarak kullanılacak orijinal görüntü belli olduktan sonra verilebilir. BCH kodları bu amaç doğrultusunda kullanılmaktadır. Bu kod sınıfında düzeltme ihtiyacı olan hata sayısına göre kodlama şeması belirlenebilir. Sayısal imzanın eklenmesi işlemi şu şekilde gerçekleşir: Hem kodlanmış görüntü hem de sayısal imza bloklara ayrılır. Sayısal imzalar bloklar halinde eklenir. Blokların boyutu BCH kod seçimine göre tespit edilir.

Şifreli görüntünün şifre çözme işleminin şeması Şekil 3.2'de gösterilmektedir. Alınan mesaj ilk önce hata kontrol kod çözücü bloğuna aktarılır. Bu bloğun görevi sayısal imza ile bozulmuş orijinal görüntüyü kurtarmaktır. Orijinal görüntü elde edildikten sonra, şifreli görüntü ve elde edilen orijinal görüntü kullanılarak sayısal imza elde

edilir. Geri kazanılan görüntüden daha sonra yeni bir sayısal imza üretilir. Üretilen bu sayısal imza ile kurtarılan imza bir karara varmak üzere ilişkilendirilir.



Şekil 3.2. Sayısal imza tekniği ile şifre çözme işleminin blok diyagramı [14]

İletilen görüntünün doğrulama işlemi, kurtarılan sayısal imza ile şifresi çözülen görüntüden elde edilen sayısal imzanın ilişkilendirilmesi yolu ile yapılır. Sayısal imza bir görüntüye özgü olduğundan, sadece şifresi çözülen görüntü ile giriş görüntüsü tam olarak çakıştığı zaman tepe ilişki elde edilir. Vander-Lugt veya JTC (Joint Transform Correlator-Ortak Dönüşüm İlişkilendirici) mimarisinde bir sayısal ilişki tekniği ya da bir optik ilişkilendirici, ilişkilendirme işlemini gerçekleştirmek için kullanılabilir. Sayısal teknikte Fourier dönüşümleri elektronik olarak hesaplanır. Hızlanma hızlı Fourier dönüşüm çipleri ile donatılmış özel elektronik donanımı kullanmak suretiyle mümkün olur. Bu durumda sayısal imza sadece görüntüyü şifrelemek için değil ayrıca şifresi çözülen resmin doğruluğunu kontrol etmek için de kullanılmaktadır.

Sayısal imza kullanarak görüntü şifreleme tekniği her boyuttaki veri ile iyi bir şekilde çalışır. Bu şifreleme tektiğinde güvenlik üç aşamada ele alınır. Birinci aşamada orijinal görüntünün boyutuna göre gerçek zamanlı bir hata kontrol kodu kullanılır. Her resim için özel olan hata kontrol kodu olmadan orijinal görüntüyü elde etmek çok zordur. Ayrıca sayısal imza şifrelenmiş görüntüye özel bir şekilde eklenmektedir. Son alıcıda sayısal imza, iletilen görüntünün orijinal görüntü ile doğrulanmasında kullanılabilmektedir. Bu yöntemin avantajı orijinal resmin doğrulama işleminin yapılmasıdır. Fazladan ekleme nedeniyle görüntünün boyutunun artması algoritmanın dezavantajıdır. Buna ek olarak herhangi bir sıkıştırma özelliği bulunmamaktadır.

3.2. Scan (Tarama) Dilini Kullanarak Görüntü Şifreleme

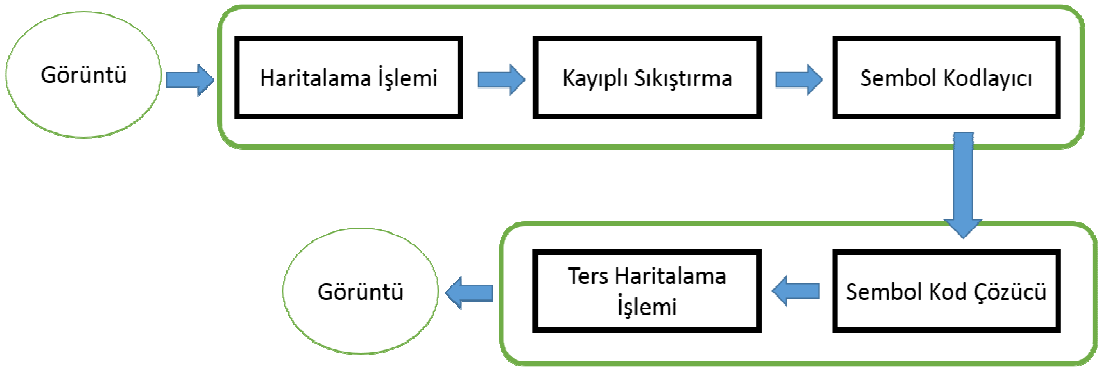
Scan dilini kullanarak yapılan görüntü şifreleme işleminde şifrelemenin yanında sıkıştırma işlemi de yapılır. Yani scan tabanlı algoritmalar hem sıkıştırma hem de şifreleme yapma kabiliyetine sahiptirler. Scan metodu ikili görüntüler üzerinde uygulanan bir yöntemdir. Metodolojinin uygulanmasında gri tonlamalı (grayscale) görüntüler bit düzlemlerine bölünürler. Algoritmanın temel amacı en az sayıda bit kullanarak sıkıştırmayı yapabilecek iyi bir tarama (scan) yolunu bulmaktır. Sıkıştırma işlemi “run-length encoding” yöntemi kullanılarak yapılır. Şifreleme işlemi gizli tutulan bir tarama yolu kullanılarak tekrar yapılır; bu şifreleme anahtarı için kullanılır.

3.2.1. Görüntü sıkıştırma

Görüntü sıkıştırma işlemi; sayısal görüntüyü oluşturmak için gereken bilgi miktarını azaltma işlemidir. Bu sayede sıkıştırılmış görüntünün boyutu azalır ve saklama ve iletim gereksinimlerini azaltarak performans artışına olumlu katkı sağlar. Sıkıştırma işlemi aşağıda verilen temel verilerden birinin ya da hepsinin azaltılması yolu ile yapılır.

- Kod Fazlalığı (Coding Redundancy)
- Piksel Fazlalığı (Interpixel Redundancy)
- Görsel Fazlalık (Psychovisual Redundancy)

Kod fazlalığı, optimum kodlamanın yapılmasını ifade eder. Piksel fazlalığı, resmin pikselleri arasındaki korelasyondan elde edilir. Görsel fazlalık, insan görme sistemi tarafından tanınmayan, görsel olmayan temel bilgileri ifade eder. Görüntü sıkıştırma teknikleri bu fazlalıklardan yararlanarak görüntüyü oluşturan bit sayısını azaltır. Sıkıştırılmış görüntünün tersi işleminde, sıkıştırılmış görüntü üzerinden orijinal görüntü elde edilir. Sıkıştırma işleminde hedef, görüntü yeniden oluşturulduğunda görsel kalitesi bozulmayacak ve orijinal görüntüye yakın olarak kalacak şekilde mümkün olduğunca bitlerin sayısını azaltmaktır. Görüntü sıkıştırma sistemleri iki farklı yapısal blokdan oluşur. Şekil 3.3’te gösterilen bu bloklar kodlayıcı ve kod çözücü bloklarıdır.



Şekil 3.3. Görüntü sıkıştırma ve sıkıştırma geri alma işleminin temel blok diyagramı

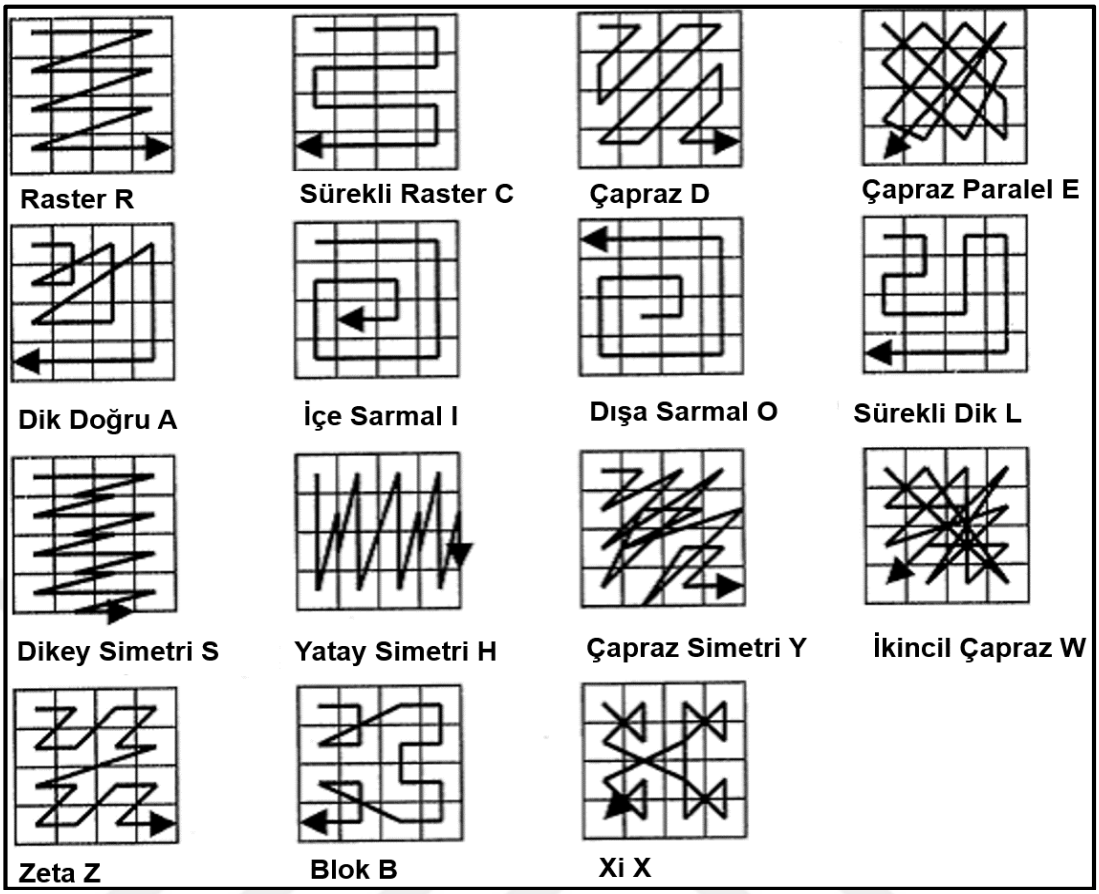
Kayıplı ve kayıpsız olmak üzere iki farklı sıkıştırma düzeni vardır. Kayıpsız sıkıştırmada sadece istatistiksel fazlalıkdan istifade edilir. Bu yöntemde sıkıştırılan görüntünün orijinal görüntü ile aynı olması muhtemeldir. LZW ya da LZ77 gibi veri sıkıştırma teknikleri GIF, PNG, ve TIFF formatlı görüntülerde kullanılabilmektedir. Doğal görüntüler için sıkıştırma oranı yaklaşık olarak 2:1 olabiliyor iken belge görüntüler için bu oran daha da fazla olabilmektedir. Kayıplı sıkıştırma işlemi ise görüntünün hem istatistiksel hem de algısal yönünden faydalanmaktadır. Bu şekilde sıkıştırılmış görüntü orijinal görüntüye göre bozulmaları içerir. Bu nedenle kayıpsız sıkıştırmaya göre sıkıştırma oranı çok daha yüksektir.

3.2.2. Scan (Tarama) paternine giriş

Tarama, çok sayıda iki boyutlu (2-D) dizinin konumsal özelliğine erişip tarama yollarını oluşturabilme yeteneğine sahip olan bir yöntemdir. Farklı uygulamalara dayalı farklı tarama yöntemleri vardır. Bu yöntemler şunlardır:

- Basit tarama (Simple scan)
- Genişletilmiş tarama (Extended scan)
- Yaygın tarama (Generalized scan)

Her farklı taramanın kendine özgü temel prensipleri ve tanımlanmış temel tarama patern dizileri vardır. Bununla birlikte tüm taramayı içeren toplamda 15 tarama paterni vardır. Her temel tarama paterni bir dönüşüm setine ve gerektiğinde basit olandan karmaşık tarama paterni elde etmek için kullanılan bir dizi kurala sahiptir. Temel tarama paternleri Şekil 3.4'te gösterilmektedir.



Şekil 3.4. Temel Tarama Paternleri [36]

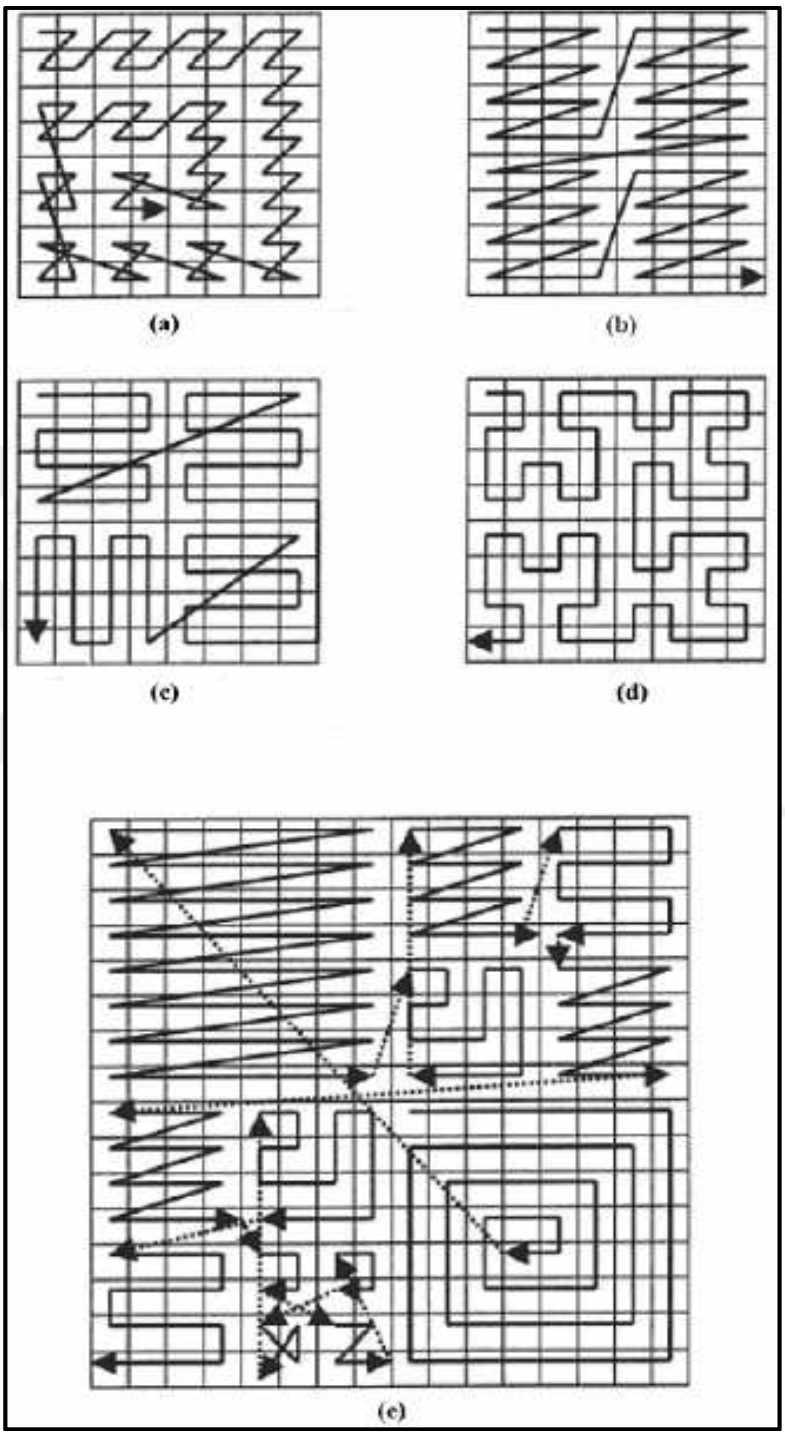
3.2.3. Scan (Tarama) paterninde sıkıştırma ve şifreleme

Tarama metodu kullanarak yapılan sıkıştırma ve şifreleme işlemi ikili görüntüler üzerinde uygulanmaktadır. Tarama yolu üzerindeki bit dizisi ile tarama yolunu temsil eden bit dizisi birlikte şifreli ve sıkıştırılmış görüntüyü temsil eder. Bu nedenle burada tarama yollarını temsil eden diziler hakkında dikkat edilmesi gereken bazı anahtar faktörler mevcuttur. Bu faktörler şunlardır:

- Tarama yolu kısa ve etkili olmalıdır ki temsil eden bit sayısı da az olsun.
- Pratikte görüntülerin çoğu homojen değildir. Bu yüzden bunlar homojen olmayan tarama yolları kullanılarak taranmalıdır.
- Bir görüntüde sıkıştırma işlemi yapmak için daha fazla bite ihtiyaç duyulan belirli bölgeler mevcuttur. Bu tür bölgeler sıkıştırılmış görüntü içinde kendi orijinal biçiminde muhafaza edilmelidir.

Bu faktörleri göz önünde bulundurarak yaygın taramanın sıkıştırma ve şifreleme için daha uygun olacağını söylemek mümkündür. Basit tarama ve genişletilmiş tarama kısa ve etkilidir. Fakat homojen olmayan görüntülerde bu tarama yöntemleri homojen

olmayan etkili bir tarama yolu sağlayamaz. Şekil 3.5'te basit, genişletilmiş ve yaygın tarama paternleri gösterilmektedir.



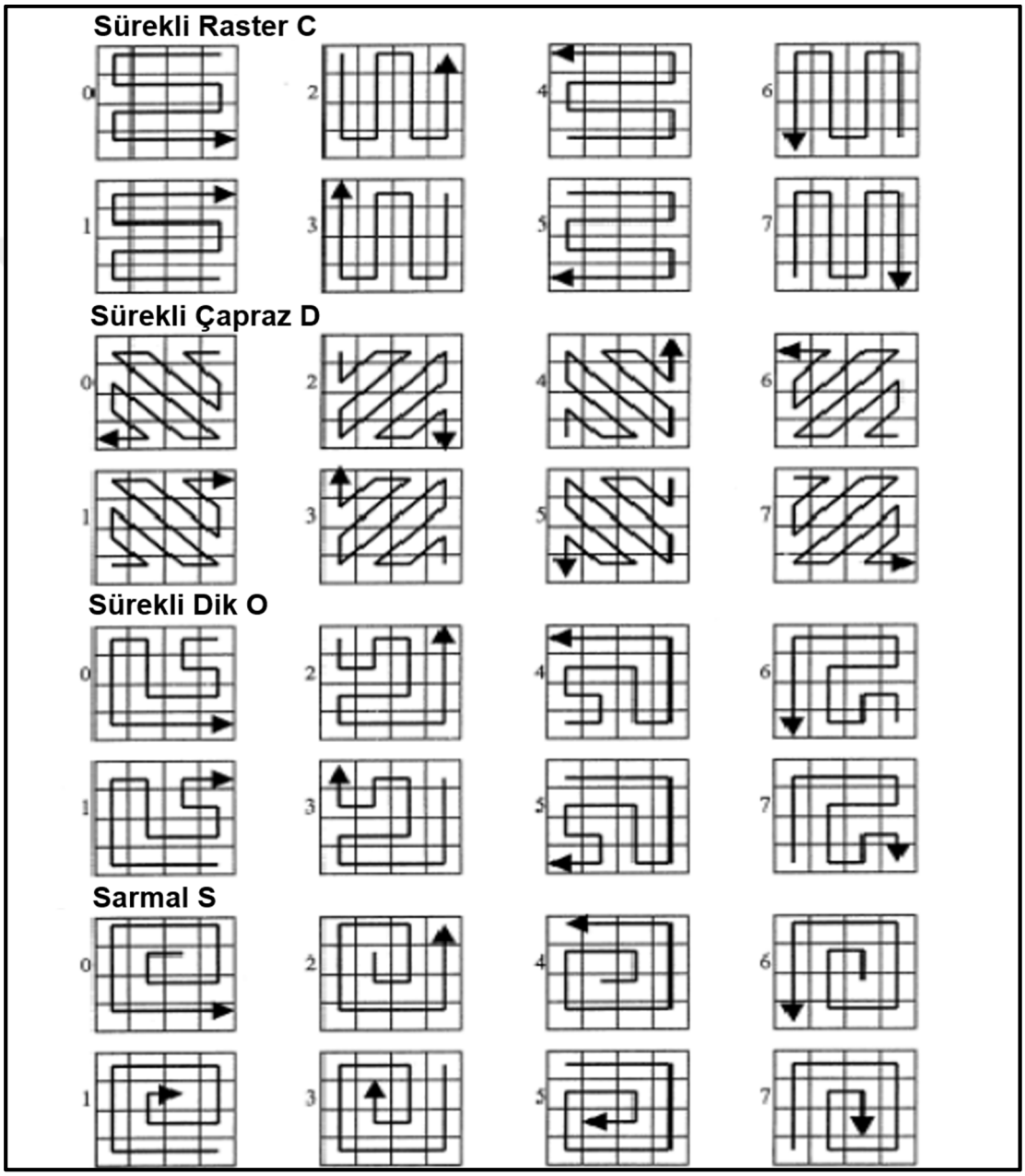
Şekil 3.5. Basit tarama (a ve b), genişletilmiş tarama(c ve d) ve yaygın tarama paternleri (e) [36]

Sıkıştırma ve şifreleme özel taramasında dört temel tarama paterni kullanılır. Bunlar;

- Raster tarama (Rasters scan C.)
- Sürekli çapraz (Continuous diagonal D.)

- Sürekli dik (Continuous orthogonal O.)
- Sarmal (Spiral S.)

Tüm bu tarama paternleri 0-7'den başlayan sekiz dönüşüme sahiptir. 1,3,5 ve 7 dönüşümleri sırasıyla 0,2,4 ve 6'nın ters dönüşümleridir. Şekil 3.6'da sıkıştırma ve şifreleme özel taraması için temel tarama paternleri gösterilmektedir.



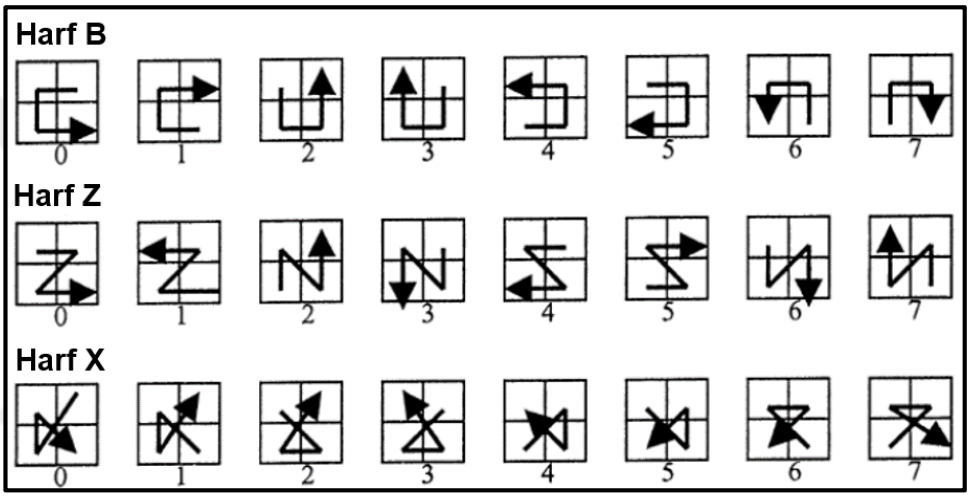
Şekil 3.6. Sıkıştırma ve şifreleme özel taraması için temel tarama paternleri [36]

Görüntülerin çoğu farklı bölümleri için farklı tarama türlerine ihtiyaç duyduklarından, sıkıştırma ve şifreleme özel taraması bir görüntünün ardışık dört alt bölgeye bölünmesine olanak tanır ve bu alt bölgelerin tümü ayrı ayrı taranır. Bir görüntü

bölümlere ayrıldığı zaman, alt bölgelerin taranma sırası bölüm paternleri tarafından tanımlanır. Üç adet bölüm paterni vardır. Bunlar:

- Harf B (Letter B)
- Harf X (Letter X)
- Harf Z (Letter Z)

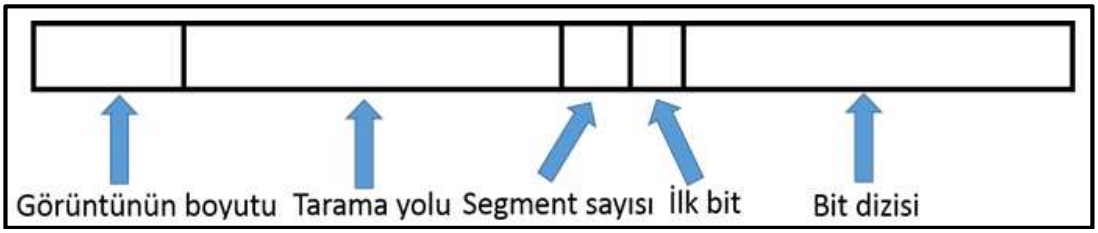
Bu paternlerin her biri aynı zamanda başlangıcı 0-7 olan sekiz dönüşüme sahiptir ve temel tarama patern dönüşümünde olduğu gibi 1,3,5 ve 7, 0,2,4 ve 6'nın ters dönüşümleri olmaktadır. Şekil 3.7'de sıkıştırma ve şifreleme özel taramasının bölüm paternleri gösterilmektedir [36].



Şekil 3.7. Bölüm paternleri [36]

Sıkıştırılmış bir resim Şekil 3.8'de gösterilen beş bileşenden oluşmaktadır. Bu bileşenler şunlardır:

- Görüntünün boyutu
- Sıkıştırma için kullanılan tarama yolu
- 0 ve 1'lerden oluşan segment sayısı
- Tarama yolundaki ilk bit
- Tarama yolundaki bit dizisi



Şekil 3.8. Sıkıştırılmış bir görüntünün bileşenleri

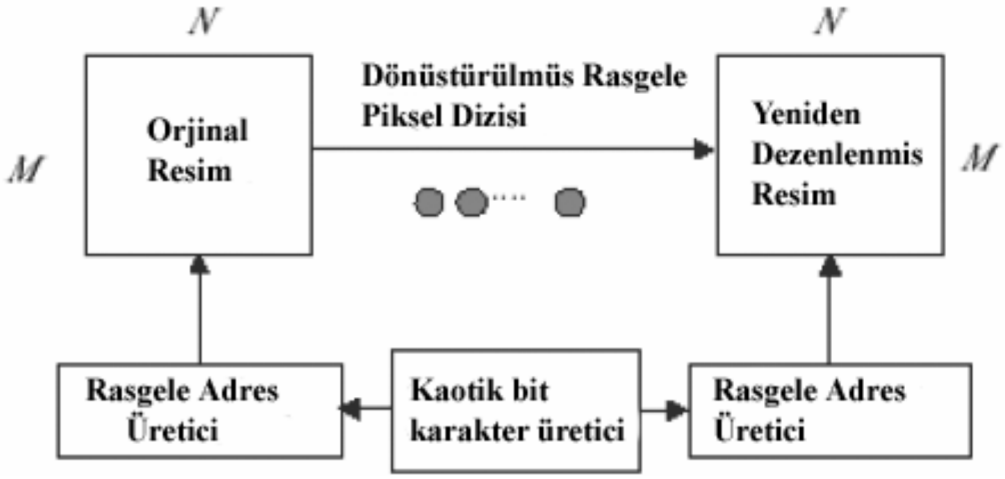
3.3. Ayna Benzeri Görüntü Şifreleme

Ayna benzeri görüntü şifreleme algoritması karmaşık bir algoritmadır ve karmaşık resim şifreleme yöntemine dayalıdır. Karmaşık bir sistemden üretilen ikili bir diziye bağlı olarak görüntünün pikselleri karıştırılmaktadır. Paralel işlem, yüksek güvenlik ve bozulmama gibi özelliklere sahiptir. Bu yöntem yer değiştirme özelliğine sahip bir resim şifreleme algoritmasıdır. Karmaşık bir sistemden oluşturulan ikili bir diziye göre resmin pikselleri ayna benzeri dört farklı operasyonla yeniden düzenlenmektedir. Permütasyon algoritmalarındaki problemler çok karmaşık yüksek hesaplamalar ve pahalı donanımlar gerektirdiğinden bu algoritma bu durumu minimuma indirmektedir.

Algoritma 7 adımdan oluşmaktadır. İlk adımda 1-D kaotik sistemi ve onun başlangıç noktası x(0) ve k=0 tanımlanır. İkinci adımda kaotik sistemden kaotik dizisi oluşturulur. Üçüncü adımda kaotik dizi kullanılarak ikili (binary) dizi oluşturulur. Son dört adımda ise görüntü pikselleri ikili diziye göre değiştirme fonksiyonu kullanılarak yeniden düzenlenir.

Şifre çözme işleminde son dört adımı ters doğrultuda izlemek gerekir. Aynı kaotik ikili dizi vasıtasıyla pikseller üzerinde aynı yer değiştirme işlemi iki kez uygulanır ise orijinal resim elde edilir.

Kaotik ikili dizi dışında şifreleme algoritmasının bilindiğini varsayarsak olası şifreleme sonuçları 2^{MxNx2} 'dir. Eğer N=M=256 ise tüm olasılıklar 2^{131072} 'dir. Kaotik ikili dizi önceden belirlenemeyeceğine göre şifrelenmiş resmi çözmek çok zordur. Bu nedenle ayna benzeri görüntü şifreleme algoritması yüksek güvenlik sağlamaktadır. Ayna benzeri görüntü şifreleme algoritmasının blok diyagramı Şekil 3.9'da gösterilmektedir.



Şekil 3.9. Ayna benzeri görüntü şifreleme algoritmasının blok diyagramı [14]

3.4. Kaotik (Karmaşık) Görüntü Şifreleme

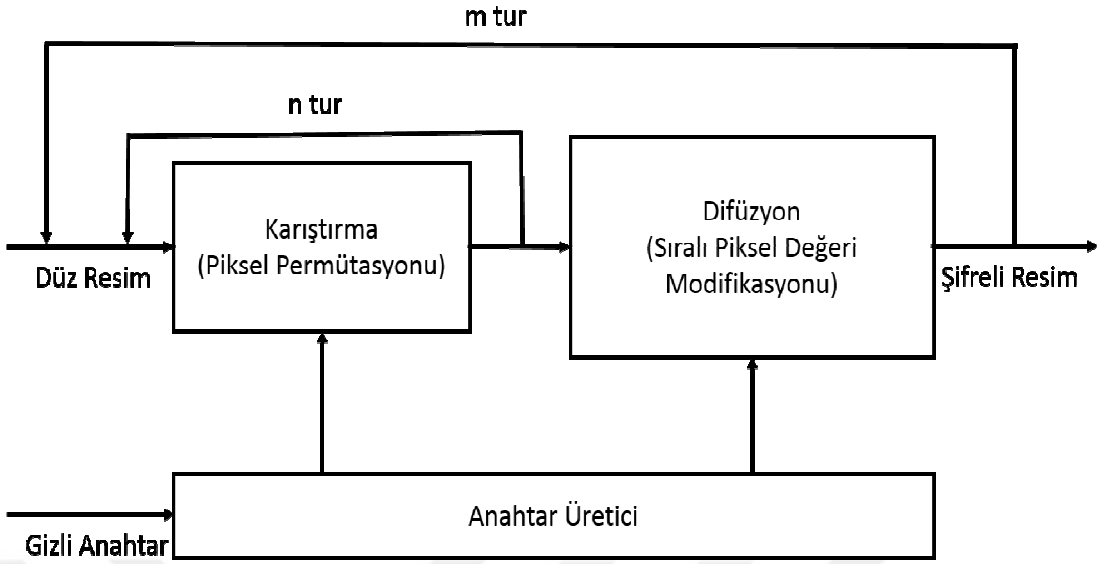
İnternet üzerinden ve kablosuz ağlar kullanılarak yapılan gerçek zamanlı görüntü aktarımındaki güvenlik ihtiyaçlarını karşılayabilmek maksadıyla görüntü şifreleme bilimi üzerinde yapılan çalışmalar gün geçtikçe önemini artırmaktadır. DES gibi geleneksel görüntü şifreleme algoritmaları büyük boyutlu görüntülerde verimli olmamaktadır.

Kaotik tabanlı şifreleme algoritması, hızlı ve yüksek güvenlikli görüntü şifrelemenin zorluklarıyla başa çıkabilecek yeni ve etkili bir yöntem önermektedir. 1989 yılında Matthews karmaşık tabanlı şifreleme algoritmasını önerdikten sonra kaotik tabanlı sistemler üzerinde yapılan çalışmalar artarak devam etmiştir. Son yıllarda da kaotik şifreleme hakkında birçok makale yayımlanmıştır.

Kaotik sistemlerin birçok önemli özelliği vardır. Bunlar; başlangıç koşullarına ve sistem parametrelerine hassas bağımlılık, yalancı rastgele özelliği, periyodik olmayan topolojik geçişliliktir. Özelliklerin çoğu şifreleme bağlamında difüzyon ve karıştırma gibi gereksinimleri karşılar. Bu nedenle kaotik şifreleme sistemlerinde daha kullanışlı ve pratik uygulamalar mevcuttur.

Kaotik tabanlı görüntü şifreleme sistemleri esas olarak iki aşamadan oluşur. Karıştırma aşaması piksel permütasyon işleminin yapıldığı aşamadır. Burada resmin tümü üzerinde, piksellerin değerlerinde değişiklik meydana gelmeyecek şekilde piksellerin konumu değiştirilerek karıştırma işlemi yapılır. Böylece görüntü tanınmayacak hale gelir. Piksel permütasyonu bir kaotik sistem tarafından gerçekleştirilir. Güvenliği artırmak için şifreleme işleminin ikinci aşaması, resimdeki bütün piksellerin değerini değiştirmeyi hedefler. Buradaki amaç saldırganlardan korunmaktır.

Difüzyon aşamasında piksel değerleri harici anahtar tarafından seçilen üç kaotik sistemden birisinden üretilen dizi tarafından sırayla değiştirilir. Tüm karıştırma ve difüzyon işlemi güvenlik seviyesi tatmin edici bir seviyeye gelene kadar tekrarlanır. Kaotik tabanlı görüntü şifreleme sistemlerinin tipik mimarisi Şekil 3.10’da gösterilmektedir.



Şekil 3.10. Kaotik tabanlı görüntü şifreleme mimarisi

Kaos ve kriptoloji bilimleri arasında doğal bir ilişki bulunmaktadır. Bu ilişki Shannon'un herhangi bir şifreleme sisteminin güvenilir olması için sahip olması gereken özellikler olan karıştırma ve difüzyon özellikleri ile kaotik sistemlerin başlangıç koşullarına duyarlı olması ve doğrusal olmaması özellikleriyle örtüşmesinden ortaya çıkmaktadır.

Karıştırma özelliğine sahip şifreleme sistemlerinde; anahtarların şifreleme algoritması, açık metin ve şifreli metin arasındaki yapılar arasında istatistiksel bağlılık olmayacak şekilde olmalıdır. Bu özelliğin olabilmesi için anahtar ve açık metinin her bitinin şifreli metini etkilemesi gerekmektedir [37].

Karıştırma ve difüzyon özellikleri dinamik sistemlerin sahip olduğu özelliklerdir. Kaotik sistemlerin başlangıç koşulları ve/veya kontrol parametrelerine bağımlılığı bir kaotik sistemden üretilen yörüngeler boyunca yayılma özelliğini sağlar. Başka bir ifade ile herhangi bir yörünge üzerinde alınan her bir değer başlangıç koşulları veya kontrol parametrelerine bağımlıdır. Başlangıç koşulları ve/veya kontrol parametrelerindeki en ufak bir değişiklik ile tamamen farklı yörüngeler oluşacağından bu bağımlılık çok güçlüdür. Sonuç olarak kaotik sistemler başlangıç koşulları ve/veya kontrol parametrelerine bağımlı yayılma özelliğine sahiptir [38].

3.5. BRIE (Bit Recirculation Image Encryption)

BRIE algoritmasının temel fikri karmaşık rastgele ikili dizi tarafından kontrol edilen piksel bitlerinin devridaimidir. Şifreleme algoritmaları arasında değer dönüşümlü bir algoritma tipidir. Öncelikle bir bit, dönüşümlü fonksiyon olarak tanımlanır. Daha sonra, ikili bir karmaşık dizi sistemden üretilir ve sonuç olarak her bir pikselin gri seviye

dönüşümü, oluşturulan dizi tarafından parametrelerin kontrolü ile haritası tanımlanır. Algoritmanın, düşük hesaplamalı karmaşıklık, yüksek güvenlik ve bozulmama özellikleri vardır.

BRIE resim şifreleme sisteminin uygulanması mimari yapısından dolayı düşük donanım karışıklığı ve yüksek hesaplama hızından dolayı kolay bir yöntemdir. Şifrelenen resim ile orijinal resmin boyutu karşılaştırıldığında algoritmanın etkin yapısı görülmektedir.

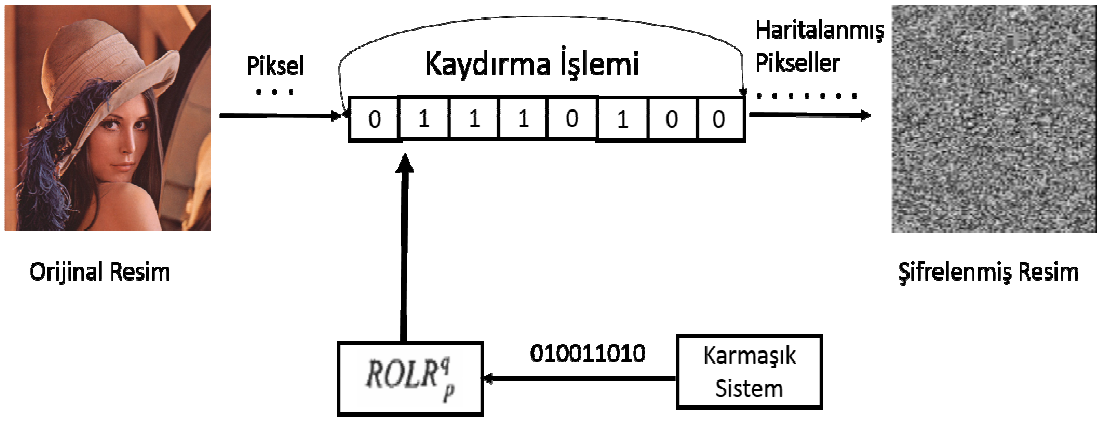
BRIE algoritmasının üç temel fikri vardır. Bunlar:

- Değer dönüşümü
- Pozisyon permütasyonu
- Onların kombinasyonları

Değer dönüşümü, orijinal sinyalin veri değerinin algoritmadaki işleme tabi tutulmasından sonra aldığı yeni değerdir. Pozisyon permütasyon algoritmaları, orijinal verinin pozisyonlarının yer değiştirmesini sağlamaktadır. Sonuç olarak, kombinasyon form permütasyonları, pozisyon permütasyonu ve değer dönüşümlerinin her ikisidir [18].

3.5.1. BRIE şifreleme algoritması

BRIE'nin gizli anahtarları α, β olmak üzere iki tamsayı ve tek boyutlu karmaşık sistemin başlangıç koşulu x(0) olarak tanımlanır. Karmaşık bir sistemden x(0),x(1),x(2),... dizisi üretilir. Daha sonra x(0),x(1),x(2),... bit dizisinden b(0),b(1),b(2),... bit dizisi üretilir. Sonraki adımda p ve q parametreleri tanımlanır. Dizi tarafından haritalanmış yapı kontrol edilerek yön yönetimi ve sayı kaydırma işlemi gerçekleştirilir. Sonuç olarak her bir piksel p ve q tarafından başarılı bir şekilde haritalanmış ve şifreli resim elde edilmiş olmaktadır. p ve q: G→G ikili gösterimin her bir dönüşümlü biti olmak üzere, x € G için eğer p=0 ise q bit küçük seviyeli bitten yüksek seviyeli bite, p=1 ise yüksek seviyeli bitten düşük seviyeli bite doğru bir dönüşüm yapılmaktadır [39]. Brie algoritmasının blok diyagramı Şekil 3.11'de gösterilmektedir.



Şekil 3.11. BRIE algoritmasının blok diyagramı

4. GÖRÜNTÜ ŞİFRELEME İÇİN GELİŞTİRİLEN YÖNTEM

4.1. Giriş

Bu bölümde, görüntü şifreleme için hibrit bir yöntem önerilmiştir. Yöntem; taşıyıcı görüntü ile şifreleme yapma mantığına dayanmaktadır.

Uygulama, Matlab R2011b programı kullanılarak hazırlanmıştır. Uygulamada şifreleme metodu olarak, tarama (scan) yöntemine göre oluşturulan şifreleyici görüntü ve tarama paternlerinin kullanıldığı hibrit bir teknik kullanılmıştır. Uygulanan yöntem tarama yöntemi gibi literatürde mevcut bir yöntemi içeriyor olsa da, şifreleme için kullanılan şifreleyici görüntü ve hibrit yöntem çalışmaya yenilik katmaktadır. Şifreleyici görüntü oluşturmak için 8 bit değere sahip alfanümerik anahtar kelime kullanılmıştır. Şifreli görüntü elde etmek için üretilen bu şifreleyici görüntü orijinal görüntüye eklenir. Aşırı derecede bozulmuş şifreli bir görüntü elde edebilmek için şifreleyici görüntü ile orijinal görüntü birleştirildikten sonra tarama yöntemi uygulanır. Elde edilen şifreli görüntünün, hibrit teknik ile daha fazla bozulmuş bir hale geldiği görülmüştür. Şifreli görüntüyü orijinal hale getirmek için ise ters işlem uygulanır.

Şifreleme işlemi görüntü bilgilerinin herhangi bir filtre ile geri dönüştürülemeyecek şekilde değiştirilmesi anlamına gelmektedir. Normalde herhangi bir görüntüye gürültü eklemesi yapma işlemi de görüntü şifreleme olarak kabul edilebilmektedir. Ancak bu şekilde yapılan şifreleme basit filtreler tarafından geri dönüştürülebilir. Bu nedenle bu uygulamada kullanılan teknikte ilk önce, hariçten girilen bir şifre vasıtasıyla oluşturulan şifreleyici görüntü ile görüntü piksellerinin ve satırların yönü değiştirildi. Daha sonra şifreleyici görüntü, orijinal görüntü için bir anahtar olarak uygulandı. Uygulamanın şifreleme bölümü için işlem maddeleri aşağıda sıralanmıştır:

- Şifrelenecek görüntünün uygulamaya eklenmesi
- Şifreleyici görüntü oluşturmak için şifrenin girilmesi
- Girilen şifre ile 4’e 8 kod ve tarama paterni kullanılarak şifreleyici görüntünün oluşturulması
- Şifreleyici görüntü ile orijinal görüntünün birleştirilmesi
- Tarama paterni kullanılarak şifrelemenin yapılması

Uygulamanın şifre çözme bölümü için işlem maddeleri aşağıda sıralanmıştır:

- Şifreyi çözmek için parolanın girilmesi
- Şifreli görüntüye ters tarama paterninin uygulanması
- Girilen şifre ile 4'e 8 kod ve tarama paterni kullanılarak şifreleyici görüntünün oluşturulması
- Şifreli görüntüden şifreleyici görüntünün çıkarılması ve orijinal görüntünün elde edilmesi

Uygulamada, şifreleme ve şifre çözme performansını karşılaştırabilmek maksadıyla PSNR (Peak Signal to Noise Ratio-Tepe Gürültü Sinyal Oranı) hesaplaması yapıldı. PSNR, görüntüler arasında en yüksek sinyal gürültü oranı hesaplaması olarak ifade edilebilir. İki görüntü arasında PSNR ölçümü desibel olarak ifade edilir. PSNR oranı; orijinal ile işlenmiş veya sıkıştırılmış görüntü arasındaki kalite ölçümü için kullanılmaktadır. PSNR değerinin yüksek olması elde edilen görüntünün kalitesinin yüksek olduğu anlamına gelmektedir. PSNR hesaplaması şifreli görüntü ile ana görüntü arasındaki tepe gürültü oranını karşılaştırmaktadır. Şifreli görüntü ile ana görüntünün PSNR'ı çok düşük ve şifresi çözülen görüntü ile ana görüntünün PSNR'ı çok yüksek olmalıdır.

4.2. 8'e 4 Kod Kullanarak Şifreleyici Görüntü Oluşturma

Bu tez çalışmasında 8'e 4 kod olarak adlandırılan bir yöntem kullanılmıştır. Bu kod dördü 1 ve dördü 0'dan oluşan ve 8 bit uzunluğunda bir koddur. Ayrıca her dörtlü grup 2 adet 0 ve 2 adet 1'den oluşacak şekilde düşünülmüştür. Tablo 4.1'de 8'e 4 kod şartını taşıyan tüm olasılıklar gösterilmiştir. Ayrıca bu tabloda gösterildiği üzere her kod bir alfanümerik karaktere atanmıştır. Alfabedeki 26 harf (Türkçe karakter barındıran harfler kullanılmamıştır) ve bir basamaklı 10 sayı ile oluşturulan 36 alfanümerik karakter sayesinde, her alfanümerik karaktere benzersiz bir kod atamak için daha uygun bir durum oluşmuştur.

Farklı anahtar kelimeler girildiğinde, her anahtar kelime orijinal görüntünün boyutuna eşit boyutta bir matris formunda alınır ve yeniden düzenlenir. Eğer anahtar kelimenin boyutu çok küçük ise aynı anahtar kelime, boyutu orijinal görüntünün boyutuna eşit oluncaya kadar tekrar edilir. Tablo 4.1'de gösterilen 8'e 4 kod ve alfanümerik karakterler kullanılarak şifreleyici görüntü oluşturulur. Anahtar kelimeye bağlı olarak oluşturulan bu şifreleyici görüntü, şifreli bir görüntü elde etmek için orijinal görüntüye eklenmek üzere kullanılır.

Tablo 4.1. Alfanümerik karakterleri ile birlikte 8'e 4 kodlarının 36 muhtemel kombinasyonu [40]

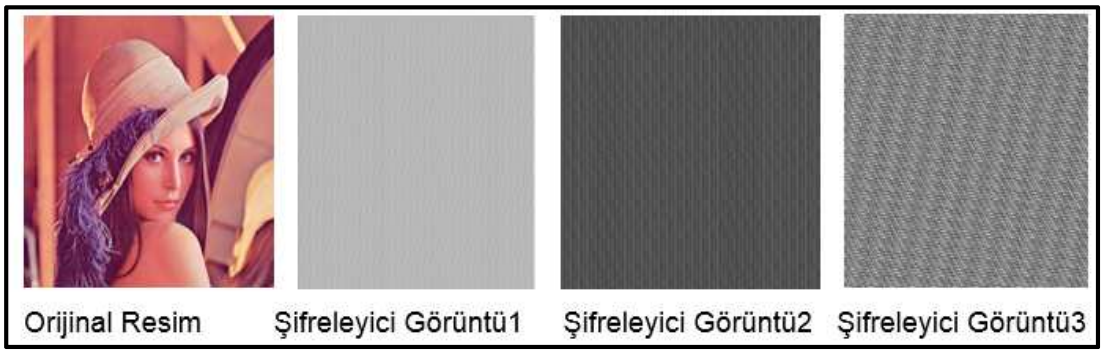
NO	BINARY	HEX	DEC	ALFANÜMERİK
1	00110011	33	51	A,a
2	00110101	35	53	B,b
3	00110110	36	54	C,c
4	00111001	39	57	D,d
5	00111010	3A	58	E,e
6	00111100	3C	60	F,f
7	01010011	53	83	G,g
8	01010101	55	85	H,h
9	01010110	56	86	I,i
10	01011001	59	89	J,j
11	01011010	5A	90	K,k
12	01011100	5C	92	L,l
13	01100011	63	99	M,m
14	01100101	65	101	N,n
15	01100110	66	102	O,o
16	01101001	69	105	P,p
17	01101010	6A	106	Q,q
18	01101100	6C	108	R,r
19	10010011	93	147	S,s
20	10010101	95	149	T,t
21	10010110	96	150	U,u
22	10011001	99	153	V,v
23	10011010	9A	154	W,w
24	10011100	9C	156	X,x

Tablo 4.1.(Devam) Alfanümerik karakterleri ile birlikte 8'e 4 kodlarının 36 muhtemel kombinasyonu [40]

25	10100011	A3	163	Y,y
26	10100101	A5	165	Z,z
27	10100110	A6	166	0
28	10101001	A9	169	1
29	10101010	AA	170	2
30	10101100	AC	172	3
31	11000011	C3	195	4
32	11000101	C5	197	5
33	11000110	C6	198	6
34	11001001	C9	201	7
35	11001010	CA	202	8
36	11001100	CC	204	9

Şekil 4.1'de aynı resim üzerinde farklı anahtar kelime kullanılarak oluşturulan 3 farklı şifreleyici görüntü verilmiştir. Bu şifreleyici görüntüler için sırasıyla şu anahtar kelimeler (parolalar) kullanılmıştır:

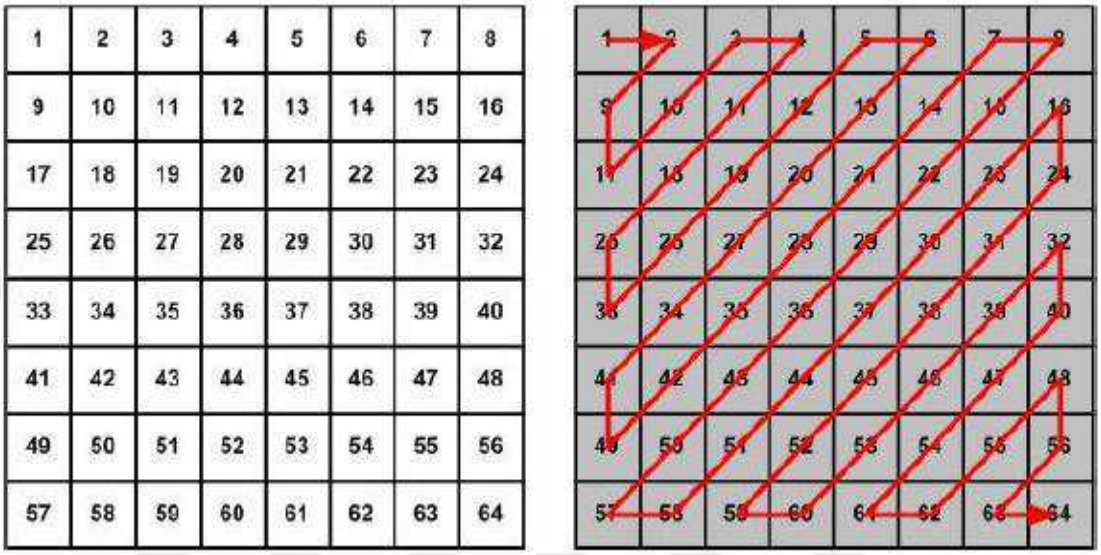
- Parola 1: 123456
- Parola 2: fenbilimleri
- Parola 3: 1yuksek2lisans3tez2015



Şekil 4.1. Farklı parolalar kullanılarak oluşturulmuş şifreleyici görüntüler

4.3. Şifreleme İçin Kullanılan Yöntem

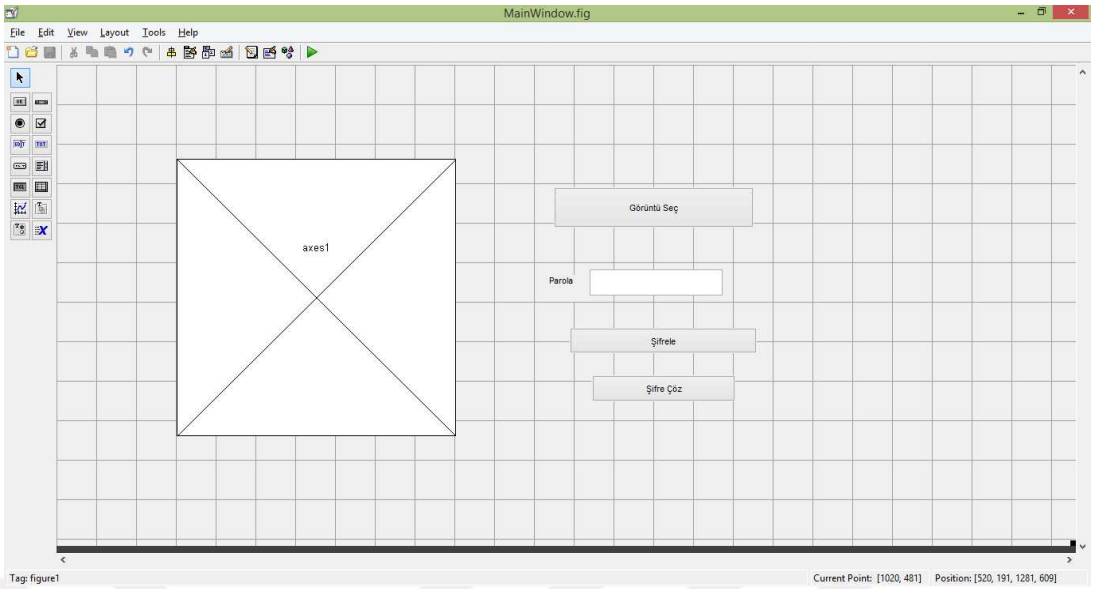
Uygulamada “Çift Tarama” yöntemi kullanılmıştır. “Çift Tarama” yönteminde şifreleyici görüntü ilk önce şifrelenmiş, daha sonra orijinal görüntüyle birleştikten sonra oluşan görüntü yeniden şifrelenmiştir. Bu şifrelemede zigzag tarama yöntemi kullanılmıştır. Zigzag tarama yönteminin uygulanışı Şekil 4.2’de gösterilmektedir.



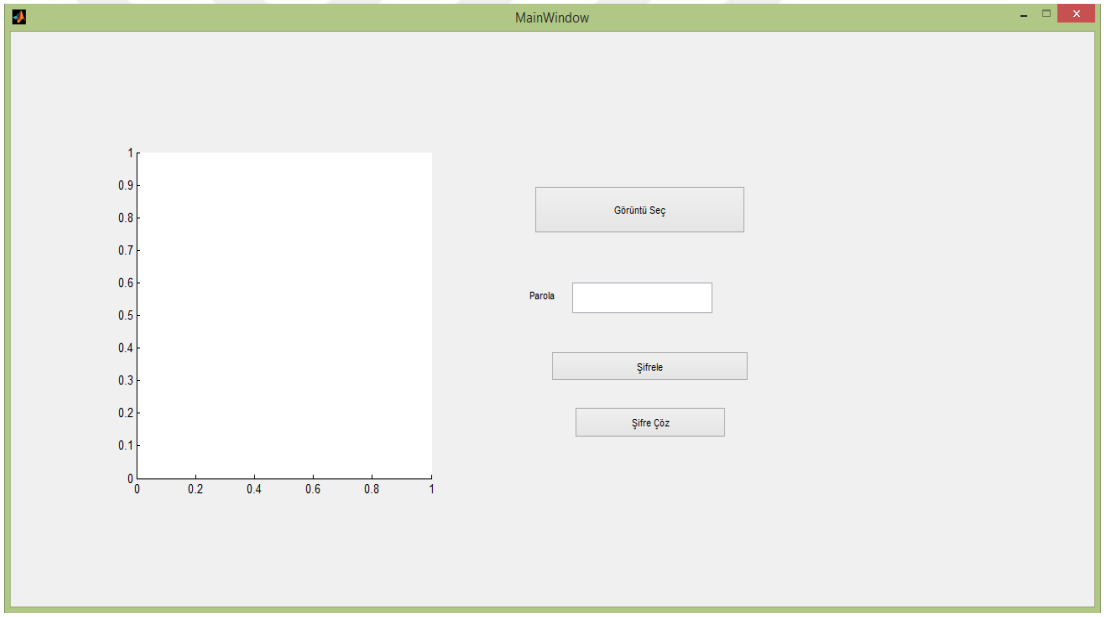
Şekil 4.2. Zigzag tarama yönteminin uygulanışı

4.4. Geliştirilen Şifreleme Yönteminin Uygulama Yazılımı

Uygulama yazılımında, şifrelemesi yapılacak görüntünün seçilmesi ve girilen parolaya göre şifreleyici görüntü ve şifrelenmiş görüntü oluşturulması maksadıyla Matlab GUI kullanılarak Şekil 4.3’deki ara yüz oluşturulmuştur. Ara yüzde görüntü seçme, şifreleme ve şifre çözme işlemlerini yaptırmak amacıyla 3 adet “push button”, seçilen, şifrelenen ve şifresi çözülen görüntünün gösterilmesi amacıyla 1 adet “axes” ve şifreleyici görüntüde kullanılacak parolanın girilmesi amacıyla 1 adet “edit text” kullanılmıştır.



Şekil 4.3. Uygulamanın .fig dosyası



Şekil 4.4. Uygulamanın çalışan görüntüsü

4.5. Uygulama Yazılımının Çalışması

Uygulama çalıştırıldığında Şekil 4.4'teki görüntü ekrana gelmektedir. Kıyaslama yapmak maksadıyla kullanılacak farklı parolalar ve bu parolalarda oluşacak şifreli görüntü ve bu görüntülere ait PSNR oranları aşağıda gösterilmiştir:

- Parola 1: 123456
- Parola 2: fenbilimleri
- Parola 3: 1yuksek2lisans3tez2015



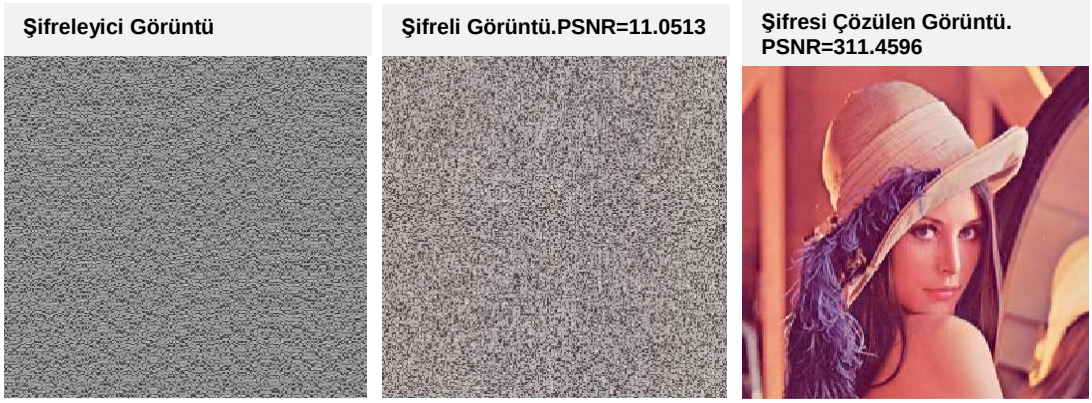
Şekil 4.5. Orijinal Lena görüntüsü



Şekil 4.6. Parola 1 ile yapılan şifreleme ve şifre çözme işlemi neticesinde elde edilen görüntü



Şekil 4.7. Parola 2 ile yapılan şifreleme ve şifre çözme işlemi neticesinde elde edilen görüntü



Şekil 4.8. Parola 3 ile yapılan şifreleme ve şifre çözme işlemi neticesinde elde edilen görüntü

Yukarıdaki şifrelemelerde kullanılan 3 farklı paroladan ilk parola sadece rakamlardan, ikinci parola sadece harflerden ve üçüncü parola da rakam ve harflerin karışımından oluşmaktadır. Yapılan şifreleme ve şifre çözme işlemleri neticesinde elde edilen görüntülerin PSNR oranları incelendiğinde parola olarak sadece rakam kullanılarak yapılan şifrelemede PSNR oranı 310, sadece harf kullanılarak yapılan şifrelemede PSNR oranı 316 ve rakam ile harfin karışımı parola kullanılarak yapılan şifrelemede PSNR oranı 311 çıkmıştır. Buradan sadece harf kullanılarak yapılan şifreleme ve şifre çözme işlemi neticesinde elde edilen görüntü kalitesinin en yüksek olduğu, sadece rakam kullanılarak yapılan şifreleme ve şifre çözme işlemi neticesinde elde edilen görüntünün kalitesinin en düşük olduğu ve rakam ile harf karışımı parola kullanılarak yapılan şifreleme ve şifre çözme işlemi neticesinde elde edilen görüntü kalitesinin ise diğer ikisinin arasında bir kalitede olduğu görülmektedir. Burada yapılan kıyaslama bu üç görüntü arasında yapılan bir kıyaslama olduğundan; kalite olarak düşük sonuç veren görüntünün kalitesinin de kabul edilebilir seviyede olduğu söylenebilir.

Bu tez çalışmasında, mevcut tarama paterni kullanılarak yapılan şifrelemedeki güvenlik seviyesi artırılmıştır. Bunu yapmak için mevcut tarama paternine ilave olarak, belirlenen bir parola neticesinde elde edilen şifreleyici görüntü kullanılmıştır. Uygulamada sadece tarama paterni kullanılarak yapılan şifreleme ve şifre çözme işlemi neticesinde elde edilen görüntüler Şekil 4.9'da verilmiştir.



Şekil 4.9. Mevcut tarama yöntemi ile yapılan şifreleme ve şifre çözme işlemi neticesinde elde edilen görüntü

Mevcut tarama yöntemi kayıpsız sıkıştırma ve şifreleme sağlayan bir yöntemdir. Fakat tarama yönteminin güvenliği kullanılan tarama paterninin gizliliğine bağlıdır. Sadece tarama paterni kullanılarak yapılan şifrelemedeki bozulma bu tez çalışmasında önerilen hibrit yönteme göre daha azdır. Hibrit yöntem ile önerilen yapıdaki şifreleyici görüntü ile çift tarama metodu, şifreli görüntüdeki bozulmayı arttırmıştır. Bu sayede önerilen hibrit yöntem ile şifreli resimdeki bozulma miktarı ile beraber güvenlik seviyesi de arttırılmıştır.

5. SONUÇLAR VE ÖNERİLER

Günümüzde internet hemen hemen hayatımızın her alanına girmiş bulunmaktadır. İnternet vasıtasıyla birçok işimizi halledebilmekteyiz; örneğin e-posta yoluyla iletişim, bankacılık işlemleri, dosya depolaması yapma, bir ürün hakkında bilgi edinme, iş başvurusu yapma gibi pek çok amaç için interneti kullanmaktayız. Bu büyük platformda, uygulamaları kullanırken kendi kişisel bilgilerimizi (kredi kartı numaramız, e-posta şifre veya kullanıcı adımız, özlük bilgilerimiz vs.) ortama sunmak veya ağ üzerinden dosya, e-posta vb. yüklemeler yapmak durumunda kalmaktayız. Bunların yanında hem kişisel işlerimizde hem de kurumsal işlemlerde görüntü trafiği de internet ortamında gün geçtikçe artmaktadır. Bu görüntülerden bazıları herkesin görmesinde sıkıntı doğurmayacak görüntüler olmakla birlikte kimi görüntüler ise başkasının görmesi veya ele geçirmesi durumunda zaafiyet yaratacak türden görüntüler olabilmektedir.

İnsanlar internet üzerinde ve sosyal paylaşım sitelerinde resimlerini paylaştığı gibi, kurumlar da uygulamalarında bilgi sistemlerine geçiş yapmakta ve bu uygulamaların bazılarında resimler kullanmaktadır. Örnek verecek olursak; askeri bir birliğin komuta merkezine istihbari değer taşıyan görüntüler gönderilmesi, bankaların planlarını sanal ortamda saklaması, özel resimlerimizin bizden başkalarının ulaşamayacağı şekilde depolanması kişiler ve kurumlar için son derece önem arz etmektedir. Bu ihtiyaçlar ışığında kişiler ve kurumlar gizlilik ve güvenliklerini sağlayacak tedbirlere ihtiyaç duymaktadır.

Veri güvenliğinin sağlanması hususunda çok sayıda çalışma yapılmıştır. Bu çalışmalardan bazıları görüntü güvenliğinin sağlanması alt başlığı üzerine olmuştur. Bu çalışmalar ışığında yapılan bu tez çalışmasında kaynakçada da gösterilen makale, tez ve internet sayfalarından faydalanılmıştır. Çalışmanın uygulama safhasında, görüntü şifreleme metodu olarak kullanılan hibrit bir yapı tez çalışmasına farklılık katmıştır. Diğer çalışmalarda belirtilen sayısal imza mantığı, bu çalışmada şifreleyici görüntü oluşturmak için kullanılmış ve bu şifreleyici görüntü ile orijinal görüntünün karıştırılarak şifrelenmesi aşamasında da çift tarama metodu kullanılmıştır.

Önerilen yöntem için bir uygulama yazılımı geliştirilmiştir. Uygulama yazılımı Matlab'da yazılmıştır. Karşılaştırma yapabilmek için üç farklı alfanümerik şifre

kullanılmış ve PSNR oranlarına bakılmıştır. Harf kullanılarak oluşturulan alfanümerik şifrede şifreleme kalitesi daha yüksek bulunmuştur.

Sonuç olarak, görüntü şifreleme alanında literatürde bulunan yöntemler, yapılan çalışmalar neticesinde artmaya devam etmektedir. Güvenlik alanındaki tehditlerin çokluğu bu tür çalışmaları hayati öneme haiz bir konuma getirmektedir. Bu tez çalışmasının da görüntü güvenliğinin sağlanması yönünde yapılan araştırmalara ışık tutması beklenmektedir.

KAYNAKLAR

[1] Sinha A., Singh K., A Technique for Image Encryption Using Digital Signature, *Elsevier Optics Communications Journal*, 2003, **218**(4-6), 229-234.

[2] Maniccam S., Bourbakis N., Lossless Image Compression and Encryption Using SCAN, *Elsevier Pattern Recognition Journal*, 2001, **34**(6), 1229-1245

[3] Chang C., Hwang M., Chen T., A New Encryption Algorithm for Image Cryptosystems, *Elsevier Journal of Systems and Software,* 2001, **58**(2), 83-91

[4] Yen J., Guo J., A New Mirror-Like Image Encryption Algorithm and Its VLSI Architecture, *Journal of Pattern Recognition and Omage Anlysis*, 2000, **10**(2), 236-247.

[5] Gao H., Zhang Y., Liang S., Li D., A New Chaotic Algorithm for Image Encryption, *Journal of Chaos, Solitons and Fractals*, 2006, **29**(2), 393-399.

[6] Xu X., Jiali F., Research and Implementation of Image Encryption Algorithm Based on Zigzag Transformation and Inner Product Polarization Vector, *IEEE International Conference on Granular Computing*, DOI: 10.1109/GrC.2010.11.

[7] Zhang S., Karim M., Color Image Encryption Using Double Random Phase Encoding, *Journal of Microwave and Optical Technology Letters*, 1999, **21**(5), 318-323.

[8] Krikor L., Baba S., Arif T., Shaaban Z., Image Encryption Using DCT and Stream Cipher, *European Journal of Scientific Research*, 2009, **32**(1), 47-57.

[9] Droogenbroeck M., Benedett R., Techniques for a Selective Encryption of Uncompressed and Compressed Images, *Advanced Concepts for Intelligent Vision Systems*, Ghent, Belgium, 9-11 September 2002.

[10] Tang L., Methods for Encrypting and Decrypting MPEG Video Data Efficiently, *4th ACM International Conference on Multimedia*, DOI: 10.1145/*244130*.244209.

[11] Ali M., Younes B. and Jantan A., Image Encryption Using Block-Based Transformation Algorithm, *IAENG International Journal of Computer Science*, 2008, **35**(1), 15-23.

[12] Ismail I., Amin M., Diab H., A Digital Image Encryption Algorithm Based A Composition of Two Chaotic Logistic Maps, *International Journal of Network Security*, 2010, **11**(1), 1-10.

[13] Özel A. Sivil Hava Radarlarında Yer-Yer Hatlarından Gönderilen Hava Resimlerinin Şifrelenmesi, Yüksek Lisans Tezi, Anadolu Ünversitesi, Fen Bilimleri Enstitüsü, Eskişehir, 2006, 181601.

[14] Güvenoğlu E., Görüntü Şifreleme Algoritmaları ve Performans Analizleri Yüksek Lisans Tezi, Trakya Ünversitesi, Fen Bilimleri Enstitüsü, Edirne, 2006, 183895.

[15] Tilborg H. C. A., *Fundamentals of Cryptology*, 1st ed., Kluwer Academic Publishers, Norwell, A.B.D., 2000.

[16] http://www.cyber-warrior.org/dokuman/Default.asp?Parametre=PrintOut&Data_id=4634 (Ziyaret Tarihi: 02 Temmuz 2015).

[17] Bishop M., *Computer Security Art and Science*, 1st ed., Pearson Education Inc., Boston, A.B.D., 2003.

[18] https://en.wikipedia.org/wiki/Scytale#/media/File:Skytale.png (Ziyaret Tarihi: 03 Temmuz 2015).

[19] https://tr.wikipedia.org/wiki/Enigma _ makinesi#/media/File: Enigma-8- rotor.jpg (Ziyaret Tarihi: 03 Temmuz 2015).

[20] https://en.wikipedia.org/wiki/Purple _ (cipher_machine)# / media/File: Type _ 97 cypher_ machine.jpg (Ziyaret Tarihi: 03 Temmuz 2015).

[21] Scheider B., *Applied Cryptography*, 2nd ed., John Wiley&Sons, New York, 1996.

[22] Stallings W., *Cryptography and Network Security: Principles and Practice*, 4th ed., Prentice Hall, New Jersey, 2006.

[23] Nechvatal J., Barker E., Bassham L., Burr W., Dworkin M., Foti J., Roback E., Report on the Development of the Advanced Encryption Standard, *National Institute of Standards And Technology*, UCID-ADA396556, 7-12, 2000.

[24] Hellman M. E., An Overview of Puplic Key Cryptography, *IEEE Communications Society Magazine*,1978, **16**(6), 42-49.

[25] http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/şifreleme-yöntemleri (Ziyaret Tarihi: 10 Temmuz 2015).

[26] Dalkılıç G., Yıldızoğlu G., Tek Anahtarlı Yeni Bir Şifreleme Algoritması Daha, *Akademik Bilişim 2008*, Çanakkale, Türkiye, 30 Ocak - 01 Şubat 2008.

[27] Parker J. R., *Algorithm for Image Processing and Computer Vision*, 2nd ed., Wiley Computer Publishing, UK, 1997.

[28] http://yzgrafik.ege.edu.tr/~tekrei/dosyalar/sunum/gi.pdf (Ziyaret Tarihi: 15Temmuz 2015).

[29] Gündüz F., Kahriman M., Sayısal Görüntü İşleme ile Geometrik Şekil ve Rotasyon Tespiti, *Elektrik-Elektronik-Bilgisayar ve Biyomedikal Mühendisliği 13.Ulusal Kongresi ve Fuarı*, Ankara, Türkiye, 23-26 Aralık 2009.

[30] http://www.yildiz.edu.tr/bayram/sgi/saygi_main.htm (Ziyaret Tarihi: 15 Temmuz 2015).

[31] https://tr.wikipedia.org/wiki/Renk (Ziyaret Tarihi: 19 Temmuz 2015).

[32] http://www.merakname.com/cmyk-nedir/ (Ziyaret Tarihi: 22 Temmuz 2015).

[33] https://helpx.adobe.com/tr/photoshop/using/color-modes.html(Ziyaret Tarihi: 22 Temmuz 2015).

[34] https://tr.wikipedia.org/wiki/HSV_renk_uzayı (Ziyaret Tarihi: 22 Temmuz 2015).

[35] Öztürk İ., Soğukpınar İ., Analysis and Comparison of Image Encryption Algorithms, *International Journal of Information Technology*, 2004, **1**(2), 64-67.

[36] Snehashıs J., Image Compression and Encryption Using Scan Pattern, Master Thesis, National Institute of Technology Rourkela, Department of Electronics and Communication, Rourkela, 2014.

[37] Paar C., Pelzl J., *Understanding Cryptography: A Textbook for Students and Practitioners*, 1st ed., Springer, Berlin, 2010.

[38] Arroyo D., Framework for the analysis and design of encryption strategies based on discrete time chaotic dynamical system, Doctoral Thesis, Universidad Politecnica De Madrid, Instituto de Fisica Aplicada, Madrid, 2009.

[39] Yen J. C., Guo J. I., A New Image Encryption Algorithm and Its VLSI Architecture, *IEEE Workshop on Signal Processing Systems (SIPS) Design and Implementation*, DOI: 10.1109/SIPS.1999.822348.

[40] Sunil K. M., Kiran K., Anand U. H., Image Encryption Using Modified 4 out of 8 Code and Chaotic Map, *International Journal of Computer Applications*, 2013, **74**(11), 1-6.

EKLER

EK-A

Şifreleme Yapmak İçin Kullanılacak Görüntünün Seçilmesini Sağlayan Kod

```
function pushbutton1_Callback(hObject, eventdata, handles)
global im;
   [fname path]=uigetfile('*.jpg','Sifrelenecek Resmi Seciniz');
   fname=strcat(path,fname);
   im=imread(fname);
   im=imresize(im,[256 256]);
   save ac im;
   imshow(im);
   title('Gercek Goruntu');
```

Şifre Girilecek Metin Bölümünün Ayarlanması

```
function edit1_Callback(hObject, eventdata, handles)
global pw;
pw=get(hObject,'String');

function edit1_CreateFcn(hObject, eventdata, handles)
if ispc && isequal(get(hObject,'BackgroundColor'),
get(0,'defaultUicontrolBackgroundColor'))
   set(hObject,'BackgroundColor','white');
end
```

Şifreleyici Görüntü Üretmede Kullanılacak 8'e 4 Kodların Oluşturulması

```
function pushbutton2_Callback(hObject, eventdata, handles)
global im
global pw
Pattern=[ '00110011';
          '00110101';
          '00110110';
          '00111001';
          '00111010';
          '00111100';
          '01010011';
          '01010101';
          '01010110';
          '01011001';
          '01011010';
          '01011100';
          '01100011';
          '01100101';
          '01100110';
          '01101001';
          '01101010';
          '01101100';
          '10010011';
          '10010101';
          '10010110';
          '10011001';
          '10011010';
          '10011100';
          '10100011';
```

```
        '10100101';
        '10100110';
        '10101001';
        '10101010';
        '10101100';
        '11000011';
        '11000101';
        '11000110';
        '11001001';
        '11001010';
        '11001100']

Chars=['a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z','0','1','2','
3','4','5','6','7','8','9']

   [x y z]=size(im);
   for(i=1:length(pw))
    a=pw(i);
    a=find(Chars==a);
    a=Pattern(a,:);
    num(i)=bin2dec(a);
   end
```

Şifreleyici Görüntünün Oluşturulması

```
   k=1;
   for(i=1:x)
      for(j=1:y)
         sg(i,j)=num(k);
         k=k+1;
         if(k>length(num))
            k=1;
         end
      end
   end
      A=sg;
      B=zigzag(A);
      B=reshape(B,size(A,1),size(A,2));
      sg=B;
   imshow(uint8(sg));
   title('Şifreleyici Görüntü');
   drawnow();
 pause(2);
```

Orijinal Görüntünün Yeniden Ölçelendirilmesi

```
  im=double(im);
   for(i=1:z)
      im(:,:,i)=im(:,:,i)/10;
   end
```

Şifreleyici Görüntü İle Orijinal Görüntünün Birleştirilmesi

```
    for(i=1:z)
        A=im(:,:,i);
        A=A+sg;
        im(:,:,i)=A;
    end
    imshow(uint8(im));
    drawnow();
    pause(2);
```

Şifreleme İşlemi İçin Tarama Paterninin Kullanılması

```
for(i=1:z)
        A=im(:,:,i);
        B=zigzag(A);
        B=reshape(B,size(A,1),size(A,2));
        im(:,:,i)=B;
 end
   imshow(uint8(im));
   drawnow();
   pause(2);
   title('Çift Tarama Şifreleme');
   enc=im;
   load ac;
   p=psnr(double(enc),double(im));
   s=num2str(p);
   s=strcat('Şifreli Görüntü. ','PSNR=',s);
   title(s);
   im=enc;
```

Şifre Çözme İşleminde Kullanılacak 8'e 4 Kodların Oluşturulması

```
function pushbutton3_Callback(hObject, eventdata, handles)
global im;
global pw;
 Pattern=[ '00110011';
          '00110101';
          '00110110';
          '00111001';
          '00111010';
          '00111100';
          '01010011';
          '01010101';
          '01010110';
          '01011001';
          '01011010';
          '01011100';
          '01100011';
          '01100101';
          '01100110';
          '01101001';
          '01101010';
          '01101100';
          '10010011';
          '10010101';
```

```
        '10010110';
        '10011001';
        '10011010';
        '10011100';
        '10100011';
        '10100101';
        '10100110';
        '10101001';
        '10101010';
        '10101100';
        '11000011';
        '11000101';
        '11000110';
        '11001001';
        '11001010';
        '11001100']
Chars=['a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z','0','1','2','
3','4','5','6','7','8','9']
   [x y z]=size(im);
   for(i=1:length(pw))
    a=pw(i);
    a=find(Chars==a);
    a=Pattern(a,:);
    num(i)=bin2dec(a);
   end
```

Şifre Çözme İşlemi İçin Ters Tarama Paterninin Kullanılması

```
 for(i=1:z)
      A=im(:,:,i);
      [x y]=size(A);
      A=reshape(A,1,size(A,1)*size(A,2));
      B=invzigzag(A,x,y);
      im(:,:,i)=B;
 end
   imshow(uint8(im));
   title('Şifre Çözülüyor');
   drawnow();
   pause(2);
```

Şifre Çözme İşleminde Kullanılacak Şifreleyici Görüntünün Oluşturulması

```
   k=1;
   for(i=1:x)
      for(j=1:y)
         sg(i,j)=num(k);
         k=k+1;
         if(k>length(num))
            k=1;
         end
      end
   end
      A=sg;
      B=zigzag(A);
      B=reshape(B,size(A,1),size(A,2));
```

```
    sg=B;
```

Şifre Çözme İşleminin Yapılması

```
  for(i=1:z)
    A=im(:,:,i);
    A=A-sg;
    im(:,:,i)=A*10;
  end
  imshow(uint8(im));
dec=im;
load ac;
p=psnr(double(dec),double(im));
s=num2str(p);
s=strcat('Şifresi Çözülen Görüntü. ','PSNR=',s);
title(s);
```

Zigzag Tarama Paterninin Oluşturulması

```
function out=zigzag(in)
% Zig-zag tarama
% Örnek,
% IN = [1   2   6   7
%       3   5   8   11
%       4   9   10  12];
% OUT = ZIGZAG(IN)
% OUT=
%   1    2    3    4    5    6    7    8    9   10   11   12
[num_rows num_cols]=size(in);
out=zeros(1,num_rows*num_cols);
cur_row=1;  cur_col=1;  cur_index=1;
% İlk Eleman
%out(1)=in(1,1);
while cur_row<=num_rows & cur_col<=num_cols
  if cur_row==1 & mod(cur_row+cur_col,2)==0 & cur_col~=num_cols
    out(cur_index)=in(cur_row,cur_col);
    cur_col=cur_col+1;                  % En Üstte Sağa  Git
    cur_index=cur_index+1;
  elseif cur_row==num_rows & mod(cur_row+cur_col,2)~=0 & cur_col~=num_cols
    out(cur_index)=in(cur_row,cur_col);
    cur_col=cur_col+1;                  % En Altta Sağa Git
    cur_index=cur_index+1;

  elseif cur_col==1 & mod(cur_row+cur_col,2)~=0 & cur_row~=num_rows
    out(cur_index)=in(cur_row,cur_col);
    cur_row=cur_row+1;                  % Aşağı En Sola Git
    cur_index=cur_index+1;

  elseif cur_col==num_cols & mod(cur_row+cur_col,2)==0 & cur_row~=num_rows
    out(cur_index)=in(cur_row,cur_col);
    cur_row=cur_row+1;                  % Aşağı En Sağa Git
    cur_index=cur_index+1;

  elseif cur_col~=1 & cur_row~=num_rows & mod(cur_row+cur_col,2)~=0
    out(cur_index)=in(cur_row,cur_col);
    cur_row=cur_row+1;      cur_col=cur_col-1;
```

```
% Aşağı Çapraz Olarak En Sola Git
      cur_index=cur_index+1;
   elseif cur_row~=1 & cur_col~=num_cols & mod(cur_row+cur_col,2)==0
      out(cur_index)=in(cur_row,cur_col);
      cur_row=cur_row-1;      cur_col=cur_col+1;
% Yukarı Çapraz Olarak En Sağa Git
      cur_index=cur_index+1;
   elseif cur_row==num_rows & cur_col==num_cols
% En Aşağı En Sağda Bulunan Elemanı Elde Et
      out(end)=in(end);
      break
% İşlemi Sonlandır
   end
end
```

Ters Zigzag Tarama Paterninin Oluşturulması

```
function out=invzigzag(in,num_rows,num_cols)
% Ters Zig-zag Tarama
% Örnek
% IN = [1    2    4    7    5    3    6    8   10   11    9   12];
% OUT = INVZIGZAG(IN,4,3)
% OUT=
%   1    2    3
%   4    5    6
%   7    8    9
%   10   11   12
tot_elem=length(in);
if nargin>3
   error('Çok Fazla Giriş Argümanı');
elseif nargin<3
   error('Çok Az Giriş Argümanı');
end
% Matris boyutları uygun olup olmadığını kontrol et
if tot_elem~=num_rows*num_cols
   error('Matris Boyutları Uyuşmuyor');
end
% Çıkış Matrisini Oluştur
out=zeros(num_rows,num_cols);
cur_row=1;  cur_col=1;  cur_index=1;
% İlk Eleman
%out(1,1)=in(1);
while cur_index<=tot_elem
   if cur_row==1 & mod(cur_row+cur_col,2)==0 & cur_col~=num_cols
      out(cur_row,cur_col)=in(cur_index);
      cur_col=cur_col+1;                    % En Üstte Sağa Git
      cur_index=cur_index+1;
   elseif cur_row==num_rows & mod(cur_row+cur_col,2)~=0 & cur_col~=num_cols
      out(cur_row,cur_col)=in(cur_index);
      cur_col=cur_col+1;                    % En Altta Sağa Git
      cur_index=cur_index+1;
   elseif cur_col==1 & mod(cur_row+cur_col,2)~=0 & cur_row~=num_rows
      out(cur_row,cur_col)=in(cur_index);
      cur_row=cur_row+1;                     % Solda Aşağı Git
      cur_index=cur_index+1;
```

```
   elseif cur_col==num_cols & mod(cur_row+cur_col,2)==0 & cur_row~=num_rows
      out(cur_row,cur_col)=in(cur_index);
      cur_row=cur_row+1;                    % Sağda Aşağı Git
      cur_index=cur_index+1;
   elseif cur_col~=1 & cur_row~=num_rows & mod(cur_row+cur_col,2)~=0
      out(cur_row,cur_col)=in(cur_index);
      cur_row=cur_row+1;     cur_col=cur_col-1;  % Çapraz Olarak Sol Aşağı Git
      cur_index=cur_index+1;
   elseif cur_row~=1 & cur_col~=num_cols & mod(cur_row+cur_col,2)==0
      out(cur_row,cur_col)=in(cur_index);
      cur_row=cur_row-1;     cur_col=cur_col+1;  % Çapraz Olarak Sağ Yukarı Git
      cur_index=cur_index+1;
   elseif cur_index==tot_elem                % Sağ Alt Eleman Girişi
      out(end)=in(end);
      break                              % İşlemi Sonlandır
   end
end
```

PSNR Hesaplama Kodunun Yazılması

```
function n = psnr(x, y)
%   PSNR İki görüntü arasındaki gürültü oranı tepe noktasını hesaplar
%   PSNR(X, Y) X ve Y görüntüleri arasındaki gürültü oranı tepe noktasını desibel
    (dB) olarak hesaplar
%   Görüntüler 256 gri seviyeye sahip olarak kabul edilir(0 .. 255).
%   X ve Y girişleri için sınıf desteği
%   float:   double, single
%   integer: uint*, int*
%   PSNR hesaplama kodlarının yazımında Stefan Roth'un çalışmalarından
faydalanılmıştır.%
diff = double(x) - double(y);
  n = 20 * log10(255 / std(diff(:)));
```

KİŞİSEL YAYIN VE ESERLER

[1] **Sakal H.**, Yıldırım M., Görüntü Şifreleme İçin Scan Paternlerini Kullanan Hibrit Bir Yöntem, *Selçuk Üniversitesi Selçuk-Teknik Dergisi,* 2016, **15**(3), 264-283.

ÖZGEÇMİŞ

1985 yılında Giresun'da doğdu. İlk, orta ve lise öğrenimini İstanbul'da tamamladı. 2007 yılında girdiği Kocaeli Üniversitesi Teknik Eğitim Fakültesi Bilgisayar Öğretmenliği (İ.Ö.) Bölümü'nden 2011 yılında Bilgisayar Öğretmeni olarak mezun oldu. 2012 yılında başladığı, Kocaeli Üniversitesi Fen Bilimleri Enstitüsü Bilişim Sistemleri Mühendisliği Anabilim Dalı'nda Yüksek Lisans eğitimine devam etmektedir. Aynı zamanda 2007-2014 yılları arasında Deniz Kuvvetleri Komutanlığı'nda Astsubay statüsünde görev yapmış, 2014 yılından itibaren yine Deniz Kuvvetleri Komutanlığı'nda Subay statüsünde görev yapmaktadır.