T.C.
TRAKYA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

KODLAMA TEORİSİ TABANLI GÖRÜNTÜ SIR PAYLAŞIM ŞEMASI YÜRÜTÜLMESİ

GÜLŞEN GÜVEN

YÜKSEK LİSANS TEZİ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

Tez Danışmanı: Dr. Öğr. Üyesi Derya ARDA

EDİRNE-2020

Gülşen GÜVEN'in hazırladığı "Kodlama Teorisi Tabanlı Görüntü Sır Paylaşım Şeması Yürütülmesi" başlıklı bu tez, tarafımızca okunmuş, kapsam ve niteliği açısından Bilgisayar Mühendisliği Anabilim Dalında bir Yüksek lisans tezi olarak kabul edilmiştir.

Jüri Üyeleri — İmza

Dr.Öğr Üyesi. Derya Arda

Dr. Öğr. Üyesi Halil Nusret Buluş

Dr. Öğr. Üyesi Cem Taşkın

Tez Savunma Tarihi: 24/01/2020

Bu tezin Yüksek Lisans tezi olarak gerekli şartları sağladığını onaylarım.

İmza

Dr. Öğr. Üyesi Derya ARDA
Tez Danışmanı

.....

Trakya Üniversitesi Fen Bilimleri Enstitüsü onayı

Prof. Dr. Murat YURTCAN
Fen Bilimleri Enstitüsü Müdürü

T.Ü.FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI YÜKSEK LİSANS PROGRAMI

DOĞRULUK BEYANI

Trakya Üniversitesi Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında, tüm verilerin bilimsel ve akademik kurallar çerçevesinde elde edildiğini, kullanılan verilerde tahrifat yapılmadığını, tezin akademik ve etik kurallara uygun olarak yazıldığını, kullanılan tüm literatür bilgilerinin bilimsel normlara uygun bir şekilde kaynak gösterilerek ilgili tezde yer aldığını ve bu tezin tamamı ya da herhangi bir bölümünün daha önceden Trakya Üniversitesi ya da farklı bir üniversitede tez çalışması olarak sunulmadığını beyan ederim.

24/01/2020

Gülşen Güven



Yüksek Lisans Tezi

Kodlama Teorisi Tabanlı Görüntü Sır Paylaşım Şeması Yürütülmesi

T.Ü. Fen Bilimleri Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

ÖZET

Günümüzde teknolojinin gelişmesiyle sayısal ortamda verilerin güvenli bir şekilde iletilmesi ve korunması gibi bilgi güvenliği gereksinimleri önem kazanmıştır. Güvenlik yöntemlerinin başında kriptoloji gelmektedir. Sır Paylaşım Şemaları, sadece bir kişiye güven olmadığı durumlarda kullanılmaktadır. Bu şemalarda amaç gizli bilginin birçok kişi arasında dağıtılarak güvenliğini arttırmaktır. Bu gizli bilgi bir şifreleme anahtar ya da bir gizli resim olabilir. Literatürde bir çok sır paylaşım şemaları mevcuttur.

Bu tezde gizli görüntülerin güvenliğini sağlamak için diğer görüntü sır paylaşım metotlarında kullanılan permütasyon işlemine gerek olmaması ve seçilen sonlu cisimde herhangi bir görüntü kaybına sebep vermemesinden dolayı kodlama teorisi tabanlı bir şema kullandık. İlk olarak $GF(2^8)$ sonlu cisminde [n,k] parametreli [12, 4] Reed Solomon kodu(RS) ile bir (k, n-k) gizli görüntü paylaşım şeması uygulanmıştır.

İkinci olarak görüntü sır paylaşım şeması için $GF(2^8)$ sonlu cisminde Hadamard matris formunda elde edilmiş olan [16, 8, 9] parametreli MDS kod kullanılmıştır. Bu MDS kodun standart formdaki üreteç matrisi $\mathrm{G} = (\mathrm{I_{kxk}}|A_{kxk})$ şeklindedir. Burada özellikle A matrisi involutif (tersi kendisi) MDS matris olacak şekilde seçilmiştir. Ayrıca involutif bir MDS matris ile görüntü paylaşımı ve görüntünün yeniden elde edilmesinde aynı matris ile işlem yapılması sağlanarak maliyeti düşürülmüştür. Sonuç olarak hafif-sıklet (lightweight) bir görüntü sır paylaşım şeması önerilerek yeni bir yapı ortaya konmuştur.

Yıl : 2020

Sayfa Sayısı :56

Anahtar Kelimeler :Görüntü Sır Paylaşımı, Kodlama Teorisi, Reed Solomon Kodlar, Hadamard Matris, MDS Kod, MDS Matris

Master's Thesis

An Implementation of Secret Image Sharing Scheme Based on Coding Theory

Trakya University Institute of Natural Sciences

Computer Engineering Department

ABSTRACT

Nowadays with the development technolojy, information technolojy requirements such as safe transmission and preservation of data in digital environment have gained importance. The most important security methods are cryptology. Many methods have been proposed in the literature to safely hide key or image. One of these methods is secret sharing schemes. In a (k, n) secret sharing scheme, the secret (key or image) is distributed among n people, and any k person or more can merge to obtain secret information. Many hidden image sharing schemes have been proposed in the literature.

In this thesis, we have benefited from coding theory to ensure the safety of hidden images. The purpose of coding theory is not to require the permutation process used in other image secret sharing methods and not to cause any image loss according to the selected finite field operations. Firstly, a (k, n-k) hidden image sharing scheme was applied with Reed Solomon code (RS) with [n, k] parameters [12, 4] in $GF(2^8)$ finite field, it was shown that the hidden image was recovered.

Then $GF(2^8)$ have the parameters [16,8,9] produced in the finite field and is MDS codes produced on the Hadamard form, it was shown that the hidden image was recovered. In addition, the cost sharing was reduced by providing an involutive MDS matrix with the same matrix for image sharing and image recovery. As a result, a new structure has been introduced by proposing a lightweight image secret sharing scheme..

Year : 2020

Number of Pages : 56

Keywords : Secret Image Scheme, Coding Theory, Reed Solomon Codes, MDS Code, Hadamard Matrix, MDS Matrix

TEŞEKKÜR

Tez danışmanlığımı üstlenen akıl danışanım, yol gösterenim çok sevdiğim değerli hocam Dr. Öğrt. Üyesi Derya ARDA' ya en içten teşekkürlerimi sunuyorum.

Tez çalışmam esnasında yardımlarını esirgemeyen Arş. Görv. Kemal AKKANAT'a teşekkürlerimi sunuyorum.

Tez yazım aşamasında bana gerekli hoşgörüyü gösteren ve imtiyaz sağlayan işverenim Ümit EREN ve Levent İZGİ'ye ve desteklerinden dolayı mesai arkadaşlarıma teşekkürlerimi sunuyorum.

Son olarak bugünlere gelmemde en büyük paya sahip sevgili aileme ve tüm arkadaşlarıma teşekkür ederim.

İÇİNDEKİLER

ÖZET iii

ABSTRACT v

TEŞEKKÜR vii

ŞEKİLLER DİZİNİ x

ÇİZELGELER DİZİNİ xi

KISALTMALAR DİZİNİ xii

BÖLÜM 1 1

GİRİŞ 1

BÖLÜM 2 4

MATEMATİKSEL TANIMLAR 4

2.1. Sonlu Cisimler 4

2.2. Sonlu Cisimlerde Matematiksel İşlemler 5

BÖLÜM 3 9

KODLAMA TEORİSİ 9

3.1. Kodlama Teorisindeki Temel Kavramlar 9

3.2. Lineer Kodlar 10

3.3. Reed Solomon Kodlar 11

3.3.1. Kodlama 13

3.3.2. Kod Çözme 13

BÖLÜM 4 14

HADAMARD MATRİSLER, MDS KODLAR VE MDS MATRİSLER 14

BÖLÜM 5 16

SIR PAYLAŞIM ŞEMALARI 16

5.1. Genel Sır Paylaşımı Tanımı 17

5.2. Shamir' in Polinomsal Tabanlı Sır Paylaşım Şeması 17

5.3. Gizli Görüntü Sır Paylaşımı 19

5.3.1. Thien ve Lin Sır Paylaşım Şeması 20

BÖLÜM 6 22

REED SOLOMON KODLARLA GÖRÜNTÜ SIR PAYLAŞIMI UYGULAMASI 22

6.1. [12,4] Reed Solomon Kod ile Görüntü Sır Paylaşımı 24

6.2. Sonuçlar ve Tartışma 27

BÖLÜM 7 28

İNVOLUTİF MDS MATRİSLER İLE GÖRÜNTÜ SIR PAYLAŞIMI UYGULAMASI 28

7.1. Hadamard- İnvolutif MDS Matris ile Görüntü Sır Paylaşım Şeması Uygulaması 28

BÖLÜM 8 37

SONUÇLAR VE ÖNERİLER 37

KAYNAKÇA 39

ÖZGEÇMİŞ 43

ŞEKİLLER DİZİNİ

Şekil 2. 1 Z_7'te Toplama ve Çarpma İşlemleri **5**
Şekil 6. 1 6x2 boyutlu sırasıyla S1,S2,S3,S4 pay görüntülerin ilk piksel değerleri 23
Şekil 6. 2 RS kod ile (k,n)=(4,8) Gizli Görüntü Paylaşım Kısmı 25
Şekil 6. 3 k=4 eşik sayıda seçilen (S_4,S_6,S_7S_8) Pay Görüntülerden Gizli Görüntüyü Yeniden Elde Etme **26**
Şekil 7. 1 8x8 MDS matrisin Magma kodu 29
Şekil 7. 2. $\boldsymbol{x^8 + x^4 + x^3 + x^2 + 1}$ indirgenemez polinomuyla $GF(2^8)$'de 30
Şekil 7. 3 256x256 boyutlu Lena.bmp 31
Şekil 7. 4 Sırayla S1,S2,S3,S4,S5,S6,S7,S8 pay görüntüler 32

ÇİZELGELER DİZİNİ

Çizelge 2. 1. $GF(2^4)$'de indirgenemez polinomu $x^4 + x^3 + x^2 + x + 1$ ve ilkel elemanı β=α+1göre cisim elemanları ve tersleri 7

Çizelge 2. 2 GF(2^3) Sonlu Cisim elemanları **8**

Çizelge 3. 1 $GF = (2^3)$ sonlu cisim uzayında $x^3 + x^2 + 1$ indirgenemez polinomuna göre cisim elemanları..... 12

KISALTMALAR DİZİNİ

GSP	Görsel Sır Paylaşım
MDS	(Maksimum Distance Seperable) Maksimum Uzaklıkla Ayrılabilen Kod
GF	Galois Field(Sonlu Cisim)
BCH	Bose-Chaudhuri – Hocquenghem
RS	Reed Solomon
SPŞ	Sır Paylaşım Şemaları
RGB	Red Green Bue

BÖLÜM 1

GİRİŞ

Günümüzde internet kullanımının artmasıyla birlikte, güvenli elektronik veri iletimi, güvenli elektronik ticaret, askeri görüntü ve bilgilerin güvenli iletimi gibi bilgi güvenliği gereksinimleri gittikçe artmaktadır. Bilgi güvenliğini sağlayabilmek için çeşitli yöntemler ve protokoller kullanılmaktadır. Yaygın olarak kullanılan güvenlik yöntemlerinin başında kriptografi gelmektedir.

Sır Paylaşım Şemaları, sadece bir kişiye güven olmadığı durumlarda kullanılmaktadır. Bu şemalarda amaç gizli bilginin birçok kişi arasında dağıtılarak güvenliğini arttırmaktır. Bu gizli bilgi bir şifreleme anahtar ya da bir gizli resim olabilir.

İlk olarak Sır Paylaşım Şeması Shamir (Shamir, 1979) ve Blakley (Blakley, 1979) tarafından önerilmiştir. Bu şemalar aynı zamanda (k,n) eşik sır paylaşım şemaları olarak bilinmektedir. Bir (k,n) şemasında gizli bilgi n paya ayrılır ve ancak k adet payın bir araya gelmesi ile yeniden elde edilir. Bu sayede gizli bilginin güvenliği sağlanmış olur. Shamir'in şeması polinomial interpolasyon tabanlıdır. Blakley'in şeması ise geometrik tabanlıdır.

Daha sonraki yıllarda Çin Kalan Teoremi tabanlı sır paylaşım şemaları Mignotte (Mignotte, 1983) ve Asmuth-Bloom (Asmuth & Bloom, 1983) tarafından önerilmiştir. Bu şemalarda çin kalan teoremi boyunca özel bir sırada pozitif tam sayı dizileri kullanılır.

Ayrıca gizli görüntünün güvenliğini sağlamak için ilk olarak 1994' de Naor ve Shamir tarafından Görsel Sır Paylaşım Şeması(GSP) önerilmiştir (Naor & Shamir, 1995). Bu şemada paylaşılan sır gizli bir görüntüdür. Shamir' in *(k,n)* GSP şemasında olduğu gibi, gizli görüntüye görsel şifreleme teknikleri uygulanarak *n* adet anlamsız pay oluşturulur ve sırrı paylaşacak katılımcılara dağıtılır. Gizli görüntünün yeniden elde

edilebilmesi için en az k adet katılımcının elindeki payları üst üste koyması gerekmektedir. Bu teknikte payların boyutunun gizli görüntünün iki katı olması sebebiyle, yeniden elde edilme aşamasında gizli görüntüyle orijinal görüntü kıyaslandığında kontrast kaybı oluşmaktadır.

2002' de Thien ve Lin, Shamir'in 1979' da önermiş olduğu (k,n) eşik şemalarını kullanan Gizli Görüntü Paylaşım yöntemini önermişlerdir (Thien & Lin, 2002). Bu yöntemde *lxl* boyutunda görüntü Shamir' in polinomsal yöntemiyle *n* adet pay görüntülere bölünmekte ve bunlardan *k* tanesi bir araya gelerek gizli görüntüyü elde edebilmektedir. Üretilen pay görüntüleri gizli görüntünün *l/k'* sı kadardır.

Bu sır paylaşım tekniklerine farklı bir bakış olarak hata doğrulama kod tabanlı sır paylaşım yöntemleri önerilmiştir (Bhondo, De Santis, Gargano, & Vaccaro, 1993). Örneğin McEliece ve Sarwate Reed Solomon Kod tabanlı sır paylaşım şemasını önermişlerdir (McEliece & Sarwate, 1981).

Biz bu çalışmada gizli görüntülerin güvenliğini sağlamak için gizli görüntü paylaştırma kısmında kodlama teorisinden yararlandık.

Bu tezde Bölüm 2' de tezde geçen matematiksel kavramlara yer verilmiştir.

Bölüm 3' de Kodlama teorisinin temel kavramları ve Reed-Solomon Kodlar anlatılmıştır.

Bölüm 4'de Hadamard

Matrisler MDS kodlar ve MDS matrisler anlatılmıştır.

Bölüm 5' de Sır Paylaşım Şemaları anlatılmıştır. Özellikle Shamir' in polinom tabanlı Sır Paylaşımı ve görüntü sır paylaşımı için Thien-Lin' in Shamir' in polinomsal tabanlı şeması açıklanmıştır.

Bölüm 6'da $GF(2^8)$ sonlu cisminde seçilen indirgenemez polinoma ve uygun ilkel elemana göre [n,k] parametreli [12,4] Reed Solomon kodu(RS) ile bir (k,n-k) gizli görüntü paylaşım şeması için bir yazılım gerçekleştirilmiştir. Gizlenmek istenen görüntü RS koduna ait üreteç matris yardımıyla (n-k) adet pay görüntüye bölünmüş ve k adet pay görüntü ile yeniden elde edildiği gösterilmiştir. Gizli görüntüyü rastgele seçilen k adet pay görüntülerden elde etme kısmında kxk boyutunda bir kare A alt matrisi üreteç matrisinden elde edilmiştir. Bu A matrisi $G' = (\mathrm{I}_{\mathrm{kxk}}|A_{kxk})$ standart formunda üreteç matrisiyle (n,k,d)=(8,4,5) parametreli

bir MDS kod ve A matrisi MDS matris olacak şekilde seçilmiştir. Ve uygulamanın değerlendirmesi yapılmıştır.

Bölüm 7'de görüntü sır paylaşım şeması için $GF(2^8)$ sonlu cisminde seçilen indirgenemez polinoma göre Hadamard matris formunda elde edilmiş olan [16,8,9] parametreli MDS kod kullanılmıştır. Bu MDS kodun standart formdaki üreteç matrisi $\mathrm{G} = (\mathrm{I}_{\mathrm{kxk}}|A_{kxk})$şeklindedir. Burada özellikle A matrisi involutif (tersi kendisi) MDS matris olacak şekilde seçilmiştir. Daha sonra resmin piksel değerleri cisim elemanları ile eşleştirilmiş ve 1xk boyutunda blok blok alınan resim değerleri seçilen involutif MDS matrisi ile çarpılıp k adet gürültülü pay görüntüler elde edilecek şekilde bir yazılım yürütülmüştür. Ve yine bu k adet pay görüntüden sıralı olarak alınan 1xk'lık değerler A matrisinin tersi ile çarpılarak orijinal görüntü yeniden elde edilmiştir. Gerçekleştirilen uygulama değerlendirilmiştir.

Bölüm 8'da sonuçlar genel olarak değerlendirilmiştir.

BÖLÜM 2

MATEMATİKSEL TANIMLAR

2.1. Sonlu Cisimler

$n: Z_n\{0,1,\ldots,n-1\}$ kümesi olmak üzere Z_n'de toplama ve çarpma işlemi tanımlanabilir. Sonuçlar n'ye göre indirgenerek hesaplanır. Z_n'de toplama ve çarpma işlemindeki aksiyomlar aşağıdaki gibidir.

Her x,y,z $\in Z_n$, '+' ve '.' ile gösterilen elemanlar sırasıyla toplama ve çarpma adındaki işlemler olmak üzere;

i.Kapalılık özelliği: $x+y,\ x.y\ \in Z_n$

ii.Değişme özelliği: $x+y=y+x\ ve\ \ x.y=y.x$

iii.Birleşme (Geçişme) özelliği:

iv.$(x+y)+z=x+(y+z)\ ve\ \ x.(y.z)=(x.y).z$

v.Dağılma özelliği: $x.(y+z)=x.y+x.z$

vi.Etkisiz eleman: $x+0=0+x=x$ ve $x.1=1.x=x$

vii.Ters eleman: Z_n'de x'in toplamaya göre tersi $n-x$'dir.

Tanım 2.1. Yukarıda verilen aksiyomlardan kapalılık, geçişme, etkisiz eleman, ters eleman aksiyomlarını sağlayan Z_n cebirsel yapısına grup denir. Bu aksiyomlarla beraber değişme özelliğini de sağlıyorsa abelian grup denir (Lidl, Niederreiter, & James, 1986).

Tanım 2.2. Verilen aksiyomlardan hepsini sağlayan Z_n cebirsel yapısı halkadır. Tam sayılar, reel sayılar ve karmaşık sayılar halka sayılara örnek gösterilebilir (Lidl, Niederreiter, & James, 1986).

Tanım 2.3. Verilen aksiyomlara ek olarak toplama ve çarpmaya göre ters alma işlemini sağlayan cebirsel yapı cisimdir.

Örneğin Z_7'de toplama ve çarpma işlemini inceleyelim;

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

*	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Şekil 2. 1 Z_7'te Toplama ve Çarpma İşlemleri

Z_7cebirsel yapısı yukarda bahsettiğimiz tüm aksiyomları yerine getirmektedir. Şekil 2.1'de gösterildiği gibi 0'ın tersi yoktur fakat diğer elemanların hepsinin tersi mevcuttur. Bu yüzden Z_7 cebirsel yapısı cisim oluşturmaktadır.

Teorem 2.1. Eğer n asal sayı ise Z_n bir cisim oluşturur (Lidl, Niederreiter, & James, 1986).

Teorem 2.2. p asal sayı ve $\alpha \in Z_n$ iken $\frac{p-1}{q}$ olacak şekilde tüm asal q'lar için $\alpha^{\frac{p-1}{q}} \neq 1 \bmod p$ şeklinde ise α mod p'ye göre ilkel elemandır (Forouzan , 2008).

Teorem 2.3. Sonlu sayıda elemanların oluşturduğu cisimlere sonlu cisim denir. q bir asal sayı ve $Z_q = \{0,1,2,\ldots,q-1\}$ q tane elemandan oluşan bir kümede modulo q toplama ve çarpma işlemleri tanımlanarak sonlu bir cisim elde edilir. Bu sonlu cisme $GF(q)$ sonlu Galois cismi denir (Murphy, 2001). Bir Galois cismi q taban olmak üzere $GF(q^n)$ şeklinde q^n eleman olacak şekilde genişletilebilir ve buna $GF(q)$'nun genişletilmiş cismi denir.

2.2. Sonlu Cisimlerde Matematiksel İşlemler

Hata düzelten kodların tasarımında ve kriptografide genişletilmiş cisimler kullanılır. Bu yüzden matematiksel işlemler büyük önem taşımaktadır. Bu bölümde $GF(q)$'nun oluşturulması gösterilecektir.

2.2.1. Toplama İşlemi

Sonlu cisim aritmetiğinde elemanlar {0,1} katsayılarına sahip polinomlar olarak temsil edilebildiğinden toplama işlemi katsayılarına sahip polinomlar olarak temsil edilebildiğinden toplama işlemi katsayılarının basitçe modulo 2 aritmetiğine göre XOR toplamıdır denilebilir (Aslan, 2008).

Örnek 2.1. $a = (01110101)\ ve\ b = (10111111)$ olsun. O zaman $a + b = 11000010$ olacaktır. Polinomsal olarak göstermek gerekirse $a = x^6 + x^5 + x^4 + x^2 + 1$ ve b= $x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$ olarak ifade edilir. Buradan $a + b = x^7 + x^6 + x^3 + x$ olarak elde edilir.

2.2.2 Çarpma İşlemi

Sonlu cisim aritmetiğinde çarpma polinomların birbiri ile aritmetik çarpılmasıdır. Fakat çarpma sonucunda doğal olarak sonlu cismin derecesinden daha yüksek dereceli eleman oluşursa sonlu cismin derecesinden küçük olacak şekilde cismi oluşturan indirgenemez polinom aracılığıyla indirgemek gerkelidir. Ancak bu işlem sonlu cisim indirgenemez polinoma göre indirgeme ya da mod alma işlemidir (Aslan, 2008).

Örnek 2.2. $a = 1001$ ve $b = 0111$ ve indirgenemez polinom $x^4 + x + 1$ seçilsin. Bu değerlere göre;

$$a.b = (x^3 + 1).(x^2 + x + 1)$$
$$= (x^5 + x^4 + x^2 + x^3 + x^2 + 1) = x^5 + x^4 + x^3 + 1 = x^2 + x + x + 1 + x^3 + 1$$
$$= x^3 + x^2$$

$x^1 = x$
.
.
$x^4 = x + 1$
$x^5 = x^2 + x$
.
.
$x^{15} = 1$
Şeklinde olacaktır.

2.2.3. Ters Alma İşlemi

n bit iki polinomun çarpımı hesaplanır. Kalanı seçilen indirgenemez polinoma göre 1 ise o zaman iki polinom birbirinin o indirgenemez polinoma göre tersidir denir.

Örnek 2.3. $GF(2^4)$ için indirgenemez polinom olarak $x^4 + x^3 + x^2 + x + 1$'i seçilsin. Bu cismin karakteristiği 2, eleman sayısı 16 ve bu cisimdeki bir üreteç eleman $\beta = (0011) = \alpha + 1$'dir. Bu β üreteç elemanının üslerini düşünelim (Aslan, 2008).

Çizelge 2. 1. $\boldsymbol{GF(2^4)}$'de indirgenemez polinomu $\boldsymbol{x^4 + x^3 + x^2 + x + 1}$ ve ilkel elemanı β=α+1göre cisim elemanları ve tersleri

β^0	(0001)	1	Tersi	β^{15}	(0001)	1
β^1	(0011)	$x+1$	Tersi	β^{14}	(1010)	x^3+x
β^2	(0101)	x^2+1	Tersi	β^{13}	(0110)	x^2+x
β^3	(1111)	x^3+x^2+x+1	Tersi	β^{12}	(0010)	x
β^4	(1110)	x^3+x^2+x	Tersi	β^{11}	(1011)	x^3+x+1
β^5	(1101)	x^3+x^2+1	Tersi	β^{10}	(1100)	x^3+x^2
β^6	(1000)	x^3	Tersi	β^9	(0100)	x^2
β^7	(0111)	x^3+x+1	Tersi	β^8	(1001)	x^3+1
β^8	(1001)	x^3+1	Tersi	β^7	(0111)	x^3+x+1
β^9	(0100)	x^2	Tersi	β^6	(1000)	x^3
β^{10}	(1100)	x^3+x^2	Tersi	β^5	(1101)	x^3+x^2+1
β^{11}	(1011)	x^3+x+1	Tersi	β^4	(1110)	x^3+x^2+x
β^{12}	(0010)	x	Tersi	β^3	(1111)	x^3+x^2+x+1
β^{13}	(0110)	x^2+x	Tersi	β^2	(0101)	x^2+1
β^{14}	(1010)	x^3+x	Tersi	β^1	(0011)	$x+1$
β^{15}	(0001)	1	Tersi	β^0	(0001)	1

Tanım 2.4.GF(2) üzerinde oluşturulan m. Dereceden p(X) polinomu m'den daha küçük dereceli polinomlara bölünemiyorsa p(X) GF(2) üzerinde indirgenemez denir (Moreira & Farrel, 2006).

Tanım 2.5. GF(2) üzerinde indirgenemez p(X) polinomunun böldüğü $X^n + 1$ polinomu için $n=2^m - 1$ ise p(X) ilkel bir polinomdur (Moreira & Farrel, 2006).

Örnek 2.4. $GF = (2^3)$ sonlu cisim uzayında $x^3 + x^2 + 1$ indirgenemez polinomuna göre cismin oluşturulmsı aşağıdaki çizelge 2.2'de verilmiştir.

Çizelge 2. 2 GF(2^3) Sonlu Cisim elemanları

Cisim Elemanları	Binary Karşılığı	Decimal Karşılığı
$a^0 = 1$	001	1
$a = a$	010	2
$a^2 = a^2$	100	4
$a^3 = a^2 + 1$	101	5
$a^4 = a^2 + a + 1$	111	7
$a^5 = a + 1$	011	3
$a^6 = a^2 + a$	110	6
$a^7 = 1$	001	1

BÖLÜM 3

KODLAMA TEORİSİ

3.1. Kodlama Teorisindeki Temel Kavramlar

Bu bölümde kodlama teorisinde kullanılan bazı kavramlar verilecektir.

Tanım 3.1. q elemanlı $A = \{a_1, a_2, a_3, \dots, a_q\}$ kümesine kod alfabesi ve elemanlarına kod sembolü denir.

i. A kümesi üzerindeki n uzunluklu q- dizili sözcüklerin oluşturduğu C kümesine bir q dizili kod denir. Her $w \in A$ için n uzunluklu bir q dizili sözcük $w = (w_1, w_2, w_3, \dots, w_n)$ olarak tanımlanır.

ii. C kodunun bir elemanına kod sözcüğü denir.

iii. C deki kod sözcük sayısı $|C| = M$ ile gösterilir ve C'nin boyutu olarak tanımlanır.

iv. n uzunluğunda M elemanlı bir kod (n, M) ile gösterilir (Chapman & Vermani, 1996).

Tanım 3.2. $\mathrm{i} = 1,2, \dots, \mathrm{n}$ için $x_i, y_i \in A$ olmak üzere $\mathrm{x} = (\mathrm{x}_1, \mathrm{x}_2, \mathrm{x}_3, \dots, \mathrm{x}_\mathrm{n})$ ve $\mathrm{y} = (\mathrm{y}_1, \mathrm{y}_2, \mathrm{y}_3, \dots, \mathrm{y}_\mathrm{n})$ iki kod söz arasındaki Hamming uzaklık $\mathrm{d}(\mathrm{x}, \mathrm{y}) = |\{\mathrm{i}: 1 \leq \mathrm{i} \leq \mathrm{n}, \mathrm{x}_\mathrm{i} \neq \mathrm{y}_\mathrm{i}\}|$şeklinde tanımlanır. $d(x_i, y_i) = \begin{cases} 0\,; x_i = y_i \\ 1; x_i \neq y_i \end{cases}$ 'dir.

$x, y, z \in A$, n uzunluklu sözcükler olsun.

i. $0 \leq d(x, y) \leq n$

ii. $d(x, y) = 0 \Leftrightarrow x = y$

iii. $d(x, y) = d(y, x)$

iv. $d(x, z) \leq d(x, y) + d(y, z)$

koşulları sağlanır (Chapman & Vermani, 1996).

Tanım 3.3. Bir C kodunun minimum uzaklığı

$\mathrm{d} = \mathrm{d(C)min} = \mathrm{d(x,y)} \mid \mathrm{x} \neq \mathrm{y}, \mathrm{x}, \mathrm{y} \in \mathrm{C}$ olarak tanımlanır.

Tanım 3.4. C koduna uzunluğu n, eleman sayısı M ve minimum uzaklığı d olan bir (n, M, d) parametreli kodu adı verilir.

Tanım 3.5. Bir tanımdaki p bir asal sayı, $t \in Z_+$ olmak üzere $q = p^t$ olsun. $f, Z_+[x]$'de t. dereceden asla bir polinom olmak üzere $F_q \cong {Z_+[x]}/{(f)}$ biçiminde yazılan q elemanlı F_q cismine bir Galois Cismi denir. Galois cismi $GF(q)$ ya da F_q olarak gösterilir.

3.2. Lineer Kodlar

Tanım 3.6. F_n^q, F_q üzerinde bir vektör uzayı olsun. F_n^q'in her alt uzayı F_q cismi üzerinde n uzunluklu bir lineer kod olarak tanımlanır.

Tanım 3.7. C, IF_q^n vektör uzayının k boyutlu bir alt uzayı ise C doğrusal kodu $[n, k]$ ile d minimum uzaklığı da $[n, k, d]$ ile gösterilir ve C bir lineer $[n, k, d]$ koddur denir. C, $[n, k, d]$ parametreli bir doğrusal kod ise kodun eleman sayısı $M = q^k$ 'dir (Chapman & Vermani, 1996).

Tanım 3.8. x, IF_q^n vektör uzayının herhangi bir elemanı olmak üzere x'in sıfırdan farklı bileşenlerinin sayısına x elemanının Hamming ağırlığı denir ve $w(x)$ ile gösterilir.

Bir C kodunun sıfırdan farklı tüm kod kelimelerinin ağırlıklarının en küçüğüne C kodunun minimum ağırlığı denir ve $w(C)$ ile gösterilir. Bir C kod sözünün hamming ağırlığı sıfırdan farklı bileşenlerinin sayısıdır. C, $\mathrm{IF_q}$ üzerinde bir lineer kodun minimum ağırlığı $\mathrm{w(C)min} = \mathrm{w(x)|x} \neq 0, \mathrm{x} \in \mathrm{C}$ şeklinde tanımlanmaktadır. Bir lineer C kodunun minimum uzaklığı minimum ağırlığa eşittir. Bu tanımlara göre q dizili lineer kodun [n,k,d;q] parametreleri n uzunluğu, k boyutu ve d minimum uzaklığını göstermektedir (Chapman & Vermani, 1996).

Tanım 3.9. $C[n, k, d: q]$ parametrelerine sahip bir lineer kod olsun. Satırları C kodunun tabanındaki k adet vektörleri kullanılarak elde edilen kxn boyutlu matrise, C kodunun üreteç matrisi denir ve G ile gösterilir (Yuan, 2005).

Teorem 3.1. C kodunun üreteç matrisi $\mathrm{G} = (\mathrm{I_k}|\mathrm{A})$ formunda ise buna standart formda üreteç matris denir.

Tanım 3.10. C kodunun üreteç matrisi $\mathrm{G} = (\mathrm{I_k}|\mathrm{A})$ olmak üzere $\mathrm{GH^T} = 0$ şartını sağlayan $\mathrm{H} = (-\mathrm{A^T}|\mathrm{A_{n-k}})$ matrisine de C kodunun kontrol matrisi denir (Roman, 1992).

3.3. Reed Solomon Kodlar

Reed- Solomon (RS) kodları ikili olmayan BCH kodlarının bir alt kümesidir. RS kodları dairesel kodlardır. Reed ve Solomon tarafından 1960 yılında tanımlanmıştır. RS kodları sabit k ve n değerleri için en yüksek minimum Hamming uzaklığa sahiptir. t sayıda hata düzeltebilen bir RS kodunun parametreleri şu şekildedir (Fossorier, Mihaljevic, & Imai, 1999).

Blok uzunluğu: $\mathrm{n} = (\mathrm{q} - 1)$

Parite kontrol bit sayısı: $\mathrm{k} = \mathrm{n} - 2\mathrm{t}$

Minimum uzaklığı: $\mathrm{d_{min}} = 2\mathrm{t} + 1$

p sonlu alanda bir asal sayı olduğunda, sonlu alandaki elemanların sayısı bu asal sayının kuvveti olmalıdır. $GF(q = p^m)$.

$GF(q = p^m)$ sonlu cisminin ilkel elemanı α olmak üzere, t sayıda hata düzeltebilen doğrusal, dairesel ve blok kod olan RS kodunun üreteç polinomunun tüm kökleri $\alpha, \alpha^2, \alpha^3, \ldots \alpha^{2t}$ olarak tanımlarsak RS kodunun üreteç polinomu aşağıdaki gibidir (Lin & Costello, 2004).

$$g(x) = (x + a)(x + \alpha^2) \ldots (x + \alpha^{2t})$$
$$= g_0 + g_1 x + g_2 x^2 + \ldots + g_{2t-1} x^{2t-1} + g_{2t} x^{2t}$$

Üreteç matrisi G , dairesel kod olduğu için her satır bir kaydırılarak aşağıdaki gibi elde edilir.

$$G = \begin{bmatrix} g_0\, g_1\, g_2 \ldots g_{2t}\ 0\ 0\ 0 \ldots 0 \\ 0\, g_0\, g_1\, g_2\ \ldots g_{2t}\ 0\ 0 \ldots 0 \\ 0\ 0\ g_0\, g_1\, g_2 \ldots g_{2t}\ 0 \ldots 0 \\ . \qquad\qquad\qquad\qquad . \\ . \qquad\qquad\qquad\qquad . \\ . \qquad\qquad\qquad\qquad . \\ 0\ 0 \ldots\ \ldots\ g_1\, g_2 \ldots\ \ \ldots g_{2t} \end{bmatrix}$$

Örnek 3.1 $GF = (2^3)$ sonlu cisim uzayında $x^3 + x^2 + 1$ indirgenemez polinomuna göre (7,3,5) RS kodun üreteç polinomu ve üreteç matrisi G'nin bulunmasını inceleyelim:

Çizelge 3. 1 $\boldsymbol{GF = (2^3)}$ sonlu cisim uzayında $\boldsymbol{x^3 + x^2 + 1}$ indirgenemez polinomuna göre cisim elemanları

Cisim Elemanları	İkilik Karşılığı	Desimal Karşılığı
$a^0 = 1$	001	1
$a = a$	010	2
$a^2 = a^2$	100	4
$a^3 = a^2 + 1$	101	5
$a^4 = a^2 + a + 1$	111	7
$a^5 = a + 1$	011	3
$a^6 = a^2 + a$	110	6
$a^7 = 1$	001	1

Üreteç polinomu şu şekildedir.

$$g(x) = (x + a)(x + a^2)(x + a^3)(x + a^4)$$
$$= (x^2 + a^2x + ax + a^3)(x^2 + a^4x + a^3x + 1)$$
$$= (x^2 + (a^3 + a)x + a^3)x^2 + (a^4 + a^3)x + 1)(x^2 + a^6x + a^3)(x^2$$
$$+ ax + 1 = x^4 + ax^3 + x^2 + a^6x^3 + x^2 + a^6x + a^3x^2 + a^4x + a^3$$

$$g(x) = x^4 + a^2x^3 + a^3x^2 + x + a^3$$

Üreteç matrisi

$$G = \begin{bmatrix} a^3 & 1 & a^3 & a^2 & 1 & 0 & 0 \\ 0 & a^3 & 1 & a^3 & a^2 & 1 & 0 \\ 0 & 0 & a^3 & 1 & a^3 & a^2 & 1 \end{bmatrix}$$

Standart formdaki Üreteç Matrisi:

$$G = \begin{bmatrix} 1 & 0 & 0 & a^3 & 1 & a^3 & a^2 \\ 0 & 1 & 0 & a^5 & 1 & a & a \\ 0 & 0 & 1 & a^4 & 1 & a^6 & a^4 \end{bmatrix} = [IA]$$

Desimal formu: $G = \begin{bmatrix} 1 & 0 & 0 & 5 & 1 & 5 & 4 \\ 0 & 1 & 0 & 3 & 1 & 2 & 2 \\ 0 & 0 & 1 & 7 & 1 & 6 & 7 \end{bmatrix}$

3.3.1. Kodlama

$\mathrm{k} = \mathrm{n} - 2\mathrm{t}$ olmak üzere, kodlanacak mesaj polinomu $\mathrm{m(x)} = \mathrm{m_0} + \mathrm{m_1 x} + \cdots + \mathrm{m_{k-1} x^{k-1}}$ m(x)'in g(x) üreteç polinomu ile çarpılması sonucu RS kod sözcükleri k sembollük mesaj polinomu sistematik olmayacak şekilde elde edilir. Sadece $GF(q)$ içinde $g(x)$'e tam olarak bölünen sözcükler RS kod sözcükleri olabileceği dikkate alınırsa kodlama, bir bölme işlemi ile gerçekleştirilebilir. $m(x)$ polinomu, x^{n-k} ile çarpılıp $g(x)$'e bölünsün. Bölümden kalan $p(x)$, $x^{n-k}m(x)$ ifadesine eklenirse elde edilecek polinom $g(x)$'e tam olarak bölünebilir ve bu polinomla ifade edilen kod sözcük $v(x)$ sistematik haldedir.

3.3.2. Kod Çözme

RS kodlarının çözümü için kullanılan yöntemlerden biri Öklid algoritmasıdır.(Detaylı anlatımı için (Arda D. , 2011) kaynağına bakılabilir). RS kodlarının çözümünde izlenecek adımlar aşağıdaki gibidir (Zorlu, 2006).

1. Hata belirteçlerinin hesabı
2. Hata yeri polinomu s(X) 'in bulunması
3. s(X) 'in kökleri olan hata yerlerinin bulunması (Chine araştırması)
4. Hata değerlerinin hesaplanması (Forney algoritması)
5. Hatalı sözcüklerin düzeltilmesi

BÖLÜM 4

HADAMARD MATRİSLER, MDS KODLAR VE MDS MATRİSLER

Bu tezde $GF(2^m)$ sonlu cismi üzerinde m. dereceden bir indirgenemez p(x) polinomu olmak üzere Hadamard matristen involutif (tersi kendisi) MDS matris ile görüntü sır paylaşım şeması gerçekleştirilmiştir. Bunun için öncelikle MDS matrisler ve MDS kodlar ve Hadamard matrisler hakkında bilgiler verilmiştir.

Tanım 4.1. GF(q) uzayında [n,k,d;q] parametreli C kodu $d_{min} \leq n - k + 1$ singleton sınırı ile MDS (Maximum Distance Separable-Maximum uzaklıkla ayrılabilen) kod olarak tanımlanır. Ayrıca üreteç matrisi $G = [I_{kxk}|A_{kx(n-k)}]$ standart formunda olan bir MDS kodun A matrisinin her kare alt matrisi nonsingular $(det \neq 0)$'dır.

Bu üreteç matrisinin her k sütunu lineer bağımsızdır. MDS kodların en iyi bilinen sınıfı Reed-Solomon kodlardır (Pieprzyk & Zhang, 2004).

MDS matrisler MDS kodlardan türetilmiştir. MDS matrisler ile ilgili bazı önemli özellikler aşağıdaki tanımlarda ve önermelerde verilmiştir.

Önerme 4.1. d uzaklığına sahip bir C lineer kodunun H kontrol matrisinin her d-1 sütunları lineer bağımsızdır.

Tanımlandığı gibi bir MDS kod n-k+1 uzaklığa sahiptir. Böylece, kontrol matrisinin her n-k sütunlarının kümesi lineer bağımsızdır (Pieprzyk & Zhang, 2004).

Tanım 4.2. kxk boyutunda bir A matrisinin her kare alt matrisinin determinantı sıfırdan farklı ise bu bir MDS matristir. kxk boyutlu MDS matrisler k+1 maksimum diferansiyel ve lineer dal sayısına sahiptir.

- Aynı zamanda bir MDS matrisin bütün elemanları sıfırdan farklı olmalıdır.
- kxk boyutunda bir A matrisi MDS ise A'nın dal sayısı (branch number) k+1'dir.
- A bir MDS matris ise A^T'de bir MDS matristir.

Tanım 4.3. Bir A kare matrisi $A^2 = I$ şartını sağlıyorsa yani A'nın tersi kendisine eşitse ($A = A^{-1}$) involutif matris olarak adlandırılır.

Tanım 4.4. Bir A kare matrisi $A.A^T = I$ şartını sağlıyorsa A ortogonel matristir.

Tanım 4.5. H, $2^t x 2^t$ olmak üzere kxk boyutunda Hadamard matrisi aşağıdaki gibi gösterilir.

$$H = had(U,V) = \begin{bmatrix} U & V \\ V & U \end{bmatrix}$$

U ve V $2^{t-1}\ x\ 2^{t-1}$ formunda Hadamard matrislerdir (Nakahara & Abrahao, 2009).

Önerme 4.1. $GF(2^m)$ üzerinde kxk'lık bir H Hadamard matrisi involutif ise ilk satır elemanlarının XOR toplamları 1'e eşittir.

Örnek 4.1 $\{a, b, c, d\}$ elemanlarından $4x4$ boyutunda bir Hadamard matris aşağıdaki gibi oluşturulur.

$$U = \begin{bmatrix} a & b \\ b & a \end{bmatrix} \qquad V = \begin{bmatrix} c & d \\ d & c \end{bmatrix}$$

$$H = had(U,V) = \begin{bmatrix} U & V \\ V & U \end{bmatrix} = \begin{bmatrix} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{bmatrix}$$

Örnek 4.2. $p(x) = x^4 + x + 1$ ile tanımlı $GF(2^4)$ cisminden 4x4 Hadamard involutif bir MDS matris aşağıdaki gibidir (Akkanat, 2017).

$$A = \begin{bmatrix} 1 & x & x^2 & x^5 \\ x & 1 & x^5 & x^2 \\ x^2 & x^5 & 1 & x \\ x^5 & x^2 & x & 1 \end{bmatrix}$$

BÖLÜM 5

SIR PAYLAŞIM ŞEMALARI

Sır Paylaşım Şemaları, sadece bir kişiye güven olmadığı durumlarda kullanılmaktadır. Bu şemalarda amaç gizli bilginin birçok kişi arasında dağıtılarak güvenliğini arttırmaktır. Bu gizli bilgi bir şifreleme anahtar ya da bir gizli resim olabilir.

İlk olarak Sır Paylaşım Şeması Shamir (Shamir, 1979) ve Blakley (Blakley, 1979) tarafından önerilmiştir. Bu şemalar aynı zamanda (k,n) eşik sır paylaşım şemaları olarak bilinmektedir. Bir (k,n) şemasında gizli bilgi n paya ayrılır ve ancak k adet payın bir araya gelmesi ile yeniden elde edilir. Bu sayede gizli bilginin güvenliği sağlanmış olur. Shamir'in şeması polinomial interpolasyon tabanlıdır. Blakley'in şeması ise geometrik tabanlıdır.

Ayrıca gizli görüntünün güvenliğini sağlamak için ilk olarak 1994' de Naor ve Shamir tarafından Görsel Sır Paylaşım Şeması(GSP) önerilmiştir (Naor & Shamir, 1995). Bu şemada paylaşılan sır gizli bir görüntüdür. Bu teknikte payların boyutunun gizli görüntünün iki katı olması sebebiyle, yeniden elde edilme aşamasında gizli görüntüyle orijinal görüntü kıyaslandığında kontrast kaybı oluşmaktadır.

2002' de Thien ve Lin, Shamir'in 1979' da önermiş olduğu (k,n) eşik şemalarını kullanan Gizli Görüntü Paylaşım yöntemini önermişlerdir (Thien & Lin, 2002). Bu yöntemde *lxl* boyutunda görüntü Shamir' in polinomsal yöntemiyle *n* adet pay görüntülere bölünmekte ve bunlardan *k* tanesi bir araya gelerek gizli görüntüyü elde edebilmektedir. Üretilen pay görüntüleri gizli görüntünün *l/k'* sı kadardır.

Bu sır paylaşım tekniklerine farklı bir bakış olarak hata doğrulama kod tabanlı sır paylaşım yöntemleri önerilmiştir (Bhondo, De Santis, Gargano, & Vaccaro, 1993).

Örneğin McEliece ve Sarwate Reed Solomon Kod tabanlı sır paylaşım şemasını önermişlerdir (McEliece & Sarwate, 1981).

5.1. Genel Sır Paylaşımı Tanımı

Bir sır paylaşım şemasında D dağıtıcı ve $P_1,...,P_n$ yetkili kişiler olmak üzere aşağıdaki temel yapı ile gerçekleştirilir.

- **Dağıtım Şeması:** D dağıtıcı S sır bilgiyi $1 \le i \le n$ olmak üzere her P_i yetkililerine s_i pay bilgisi dağıtılır.
- **Yeniden elde etme:** S sır bilgisi, s_i yetkililerinin paylarını birleştirilmesi ile yeniden elde edilir. Burada $i \in A$ ve $A \subseteq \{P_1,...,P_n\}$ olmak üzere her yetkilendirilmiş katılımcıların kümesi ile sır bilgi elde edilir.

Sır paylaşım şemalarının güvenlik gereksinimleri şu şekildedir:

- Her yetkili katılımcılar paylarını birleştirerek S sır bilgisini elde edebilirler.
- Her yetkilendirilmemiş katılımcılar paylarını birleştirdiğinde *S* sırrı hakkında hiçbir bilgiyi elde edemezler.

Bu güvenlik gereksinimlerini doğrulayan Sır Paylaşım Şeması mükemmel olarak adlandırılır (Schoenmaker, 2011).

5.2. Shamir' in Polinomsal Tabanlı Sır Paylaşım Şeması

Shamir tarafından 1979' da önerilen ilk sır paylaşım şeması Shamir' in eşik şeması polinom tabanlıdır. Bir (k, n) sır paylaşımında p bir asal sayı ve Z_p sonlu bir cisim, k eşik değer ve $a_0 \in Z_p$ sır bilgisi (0, p-1) aralığında olmak üzere $a_1,...,a_{k-1} \in Z_p$ rastgele elemanları seçilip $k-1$dereceli polinomu kurulur. Ve aşağıdaki polinom ile n kişi arasında dağıtılır.

$$f(x) = \left(a_{(k-1)}x^{(k-1)} + \cdots + a_1x + a_0\right) \in Z_p[x] \qquad (5.1)$$

- **Dağıtım Kısmı:**

Gizli bilgi farklı x değerleri ile aşağıdaki denklem kullanılarak dağıtma işlemi yapılır.

$$h(x) \equiv \left(a_{(k-1)}x^{(k-1)} + \cdots + a_1 x + a_0\right) mod p \tag{5.2}$$

$y_i = h(x_i) \bmod p$ eşitsizliğine göre gizli bilgi içeren paylar (x_i, y_i) şeklinde n adet yetkili kullanıcılara dağıtılır.

- **Sır Bilginin Yeniden Elde Edilmesi:**

a_0 sırrını ve $k-1$ dereceli $h(x)$ polinomunu bulmak için k adet yetkilinin payları yeterlidir. $h(x)$ ve a_0 lagrange polinomundan yeniden elde edilir. İlk olarak $l_k(x)$ polinomu şu şekilde tanımlanır (Denning, 1982) (Trappe & Washington, 2006) (Zhu, Bao, Deng, & Kankanhalli, 2005).

$$I_t(x) = \prod_{\substack{i=1 \\ i \neq t}}^{k} \frac{x - x_i}{x_t - x_i} mod(p) \tag{5.3}$$

Lagrange interpolasyon polinomu:

$$p(x) = \sum_{t=1}^{k} y_t l_t(x) \tag{5.4}$$

Örnek 5.1. (k,n)=(3,4) eşik şemasında 4 katılımcı var ve bunlardan herhangi 3 tanesi gizliliği belirleyebilir. Ancak (k-1) yani 2 kişi gizlilik hakkında hiçbir şey belirleyemez. S=5 sayısı gizliliğimiz olsun. p=13 asal bir sayı ve $a_1, a_2 \epsilon Z_{13}$ rastgele aşağıdaki polinom seçilsin.

$$h(x) = (5 + 7x + 3x^2)(mod 13)$$

Bu polinomu kullanarak 4 paylaşımcıya (x,h(x)) anahtar parçası dağıtılsın.

$x = 1$ için; h(1)=(5+7*1+3*1)mod13=15mod13=2

$x = 2$ için; h(2)=(5+7*2+3*4)mod13=31mod13=5

$x = 3$ için; h(3)=(5+7*3+3*9)mod13=52mod13=1

$x = 4$ için; h(4)=(5+7*4+3*16)mod13=81mod13=3

(1,2); (2,5); (3,1); (4,3)

Bu ayrık noktalardan herhangi 3 tanesi ile ilgili polinom ve sır bilgisini bulalım:

$(x_1,y_1)= (1,2); (x_2,y_2)= (2,5); (x_3, y_3)= (3,1)$

k=3 eşik değerdeki pay değerleri lagrange interpolasyonu ile şu şekilde hesaplanır.

$$h(x) = \left[y_1 \frac{(x-x_2)(x-x_3)}{(x_1-x_2)(x_1-x_3)} + y_2 \frac{(x-x_1)(x-x_3)}{(x_2-x_1)(x_2-x_3)} + y_3 \frac{(x-x_1)(x-x_2)}{(x_3-x_1)(x_3-x_2)} \right] mod\ p$$

$$h(x) = \left[2\frac{(x-2)(x-3)}{(1-2)(1-3)} + y_2 \frac{(x-1)(x-3)}{(2-1)(2-3)} + y_3 \frac{(x-1)(x-2)}{(3-1)(3-2)} \right] mod\ 13$$

$$h(x)=[(x^2-5x+6)-5(x^2-4x+3)+7(x^2-3x+2)] mod\ 13$$

$$= (3x^2-6x+5) mod\ 13$$

$= 3x^2 + 7x + 5$

Bu polinom görüldüğü gibi orijinal h(x) polinomudur. Ayrıca sabit terim olan 5 sır bilgisidir (Arda, Buluş, Akgün, & Yerlikaya, 2008).

5.3. Gizli Görüntü Sır Paylaşımı

İnternetin ve teknolojinin gelişmesiyle birlikte dijital ortamda elektronik bilgiler, videolar, resimler, metinler ve sesler gibi çeşitli bilgiler paylaşılmaktadır. Paylaşılan bu veriler gizlilik gerektiren askeri veya tıbbi bir görüntü olabilmektedir. Bundan dolayı gizli görüntünün güvenliğini sağlamak için literatürde gizli görüntü sır paylaşım şeması gibi yöntemler önerilmiştir.

İlk olarak Görsel Sır Paylaşım Şeması (GSP) 1994' de Naor ve Shamir tarafından önerilmiştir (Naor & Shamir, 1995). Bu şemada paylaşılan sır gizli bir görüntüdür. Shamir' in *(k,n)* GSP şemasında olduğu gibi, gizli görüntüye görsel şifreleme teknikleri uygulanarak *n* adet anlamsız pay oluşturulur ve sırrı paylaşacak katılımcılara dağıtılır. Gizli görüntünün yeniden elde edilebilmesi için en az *k* adet katılımcının elindeki payları

üst üste koyması gerekmektedir. Eğer katılımcı sayısı *k'* dan az ise gizli görüntü hakkında hiçbir bilgiye ulaşılamaz. Bu teknikte payların boyutunun gizli görüntünün iki katı olması sebebiyle, yeniden elde edilme aşamasında gizli görüntüyle orijinal görüntü kıyaslandığında kontrast kaybı oluşmaktadır (Cimato, Cimato, & De Santis, 2007).

(k,n) GSP şemalarının başarımı için dört parametre kullanılmaktadır.

1. Güvenlik: k' dan az pay bir araya gelerek sır hakkında hiçbir bilgi elde edememelidir.
2. Doğruluk: En az k adet payın bir araya gelerek elde edilen sır bilgisinin orjinaliyle benzerliğidir.
3. Hesaplama Karmaşıklığı: Payları elde etmede kullanılan işlem sayısıdır.
4. Büyüme oranı: Gizli görüntüdeki bir pikselin paylarda kaç piksel ile ifade edildiğine bağlı olarak değişen orandır (Ulutaş, Ulutaş, & Nabiyev, 2011).

2002' de Thien ve Lin, Shamir'in 1979' da önermiş olduğu (k,n) eşik şemalarını kullanan Gizli Görüntü Paylaşım yöntemini önermişlerdir (Thien & Lin, 2002). Bu yöntemde *lxl* boyutunda görüntü Shamir' in polinomsal yöntemiyle *n* adet pay görüntülere bölünmekte ve bunlardan *k* tanesi bir araya gelerek gizli görüntüyü elde edebilmektedir. Üretilen pay görüntüleri gizli görüntünün *l/k'* sı kadardır.

Gizli Görüntü paylaşım şemalarında gri seviyeli görüntüler için piksel değerleri [0-255] aralığındadır . Paylaşma şemasında kullanılan polinomun modül değeri bu aralıkta seçilen en büyük asal olan 251' dir. Asal sayı seçilmesindeki önem orijinal görüntüyü elde etmede tek bir çözüme ulaşılmasıdır. Ancak burada elde edilen piksel değerleri [0-250] arasındadır. Dolayısıyla [251-255] aralığındaki değerler yoktur ve 250' ye ötelenmişlerdir. Bu da görüntüde parlaklık kaybına sebep olmaktadır.

Renkli görüntüler için de renk aralığı RGB paletinde bulunun Red-Green-Blue renkleri için ayrı ayrı [0-255]' dir (Şahin Mesut & Arda, 2009).

5.3.1. Thien ve Lin Sır Paylaşım Şeması

Thien ve Lin, Shamir tarafından 1979' da geliştirilen sır paylaşım şemasını kullanarak (k, n) eşik-tabanlı bir görüntü paylaşımı önermiştir. lxl boyutlu gizli resimden n tane pay görüntü elde etmek için $(k-1)$ dereceli bir polinom kullanılmaktır.

$0 \le i \le \left(\frac{l}{k}\right)$ ve $1 \le j \le l$ olmak üzere polinom şu şekilde tanımlanmaktadır. Polinomun modül değeri [0,255] aralığında seçilen en büyük asal olan p=251' dir.

$$S_x(i,j) = I(ik+1,j) + I(ik+2,j)x + \cdots + I(ik+k,j)x^{(k-1)}(modp) \qquad (5.5)$$

Oluşturulan pay görüntülerin boyutu, gizli resmin l/k' sı büyüklüğündedir. Elde edilen n adet pay görüntüden en az k adet bir araya gelerek Lagrange İnterpolasyon yöntemi ile orijinal görüntü yeniden elde edilir.

Thien ve Lin ayrıca görüntünün paylara bölme işleminden önce permüte edilmesi yolu ile güvenliğinin daha da artırmasını önermektedir. Permütasyon işlemi herhangi bir anahtar değeri ile ya da çeşitli algoritmalarla yapılabilmektedir. Bu şekilde güvenlik ve saldırılara karşı dayanıklılık arttırılmış olmaktadır (Thien & Lin, 2002).

BÖLÜM 6

REED SOLOMON KODLARLA GÖRÜNTÜ SIR PAYLAŞIMI UYGULAMASI

Örnek 6.1: Daha önce örnek 2.1'de oluşturulan GF(2^3) uzayında elde edilen G üreteç matris ve (7,3) RS kodu kullanarak (3,4) görüntü sır paylaşım şeması uygulamasını gerçekleştirelim. Burada gizlenecek görüntünün sözde pixel değerleri çizelge 6. 1'deki gibi olsun.

Çizelge 6.1. Sözde resim piksel değerlerinin cisim elemanları ile gösterimi

a^2	a^5	a^6	1	a	a^2
a	a^4	a^3	a^3	a^4	1
1	a^3	a^2	a^4	a	a^2
a^6	a^5	a^4	a^2	a^3	a^5
a	a^3	a^2	a^4	a^5	a
a^2	a	a^3	a^5	a^2	a^4

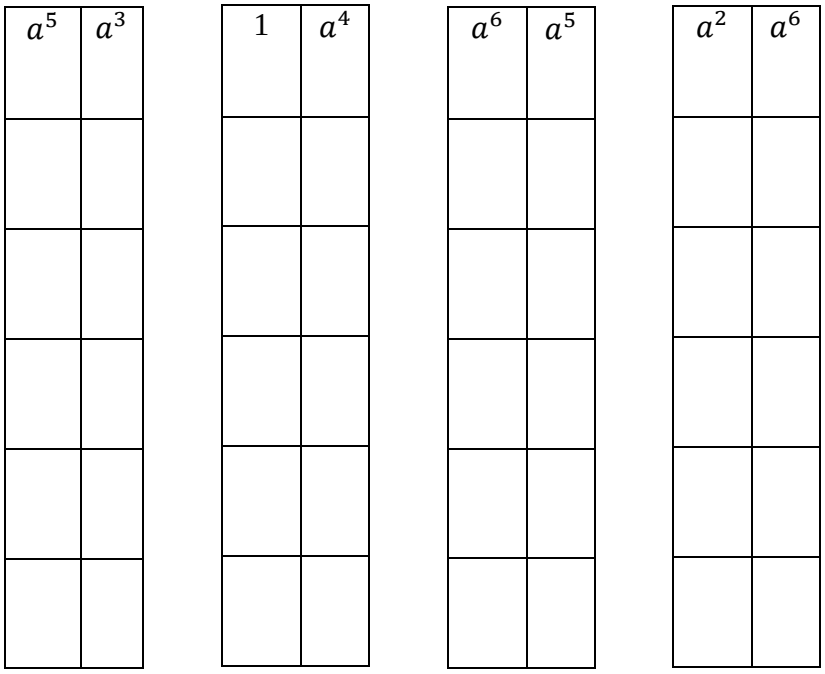
Gizli Görüntünün Paylaşım Kısmı:

$$\mathrm{v} = \mathrm{u} * \mathrm{G} = [\langle a^2 a^5\ a^6 | 1\ a\ a^2 | a\ a^4\ a^3 \dots \dots a^5 a^2 a^4 \rangle] * \begin{bmatrix} 1\ 0\ 0\ a^3\ 1\ a^3 a^2 \\ 0\ 1\ 0\ a^5\ 1\ a\ \ a \\ 0\ 0\ 1\ a^4\ 1\ a^6 a^4 \end{bmatrix}$$

şeklinde "k" uzunluğunda yani k adet piksel değeri örneğimizde 3 uzunluğunda piksel değeri G matrisi ile çarpılır. Sıralı olarak diğer 3 uzunluklu piksel değerleri alınarak G üreteç matrisi ile çarpılarak 4 adet pay görüntünün piksel değerleri elde edilir.

$$v_1 = u_1 * \mathrm{G} = [a^2 a^5\ a^6] * \begin{bmatrix} 1\ 0\ 0\ a^3\ 1\ a^3 a^2 \\ 0\ 1\ 0\ a^5\ 1\ a\ \ a \\ 0\ 0\ 1\ a^4\ 1\ a^6 a^4 \end{bmatrix} = [a^2 a^5\ a^6, a^5\ 1\ a^6 a^2]$$

İlk üç bileşen dışındaki elde edilen bu değerler 4 pay görüntünün ilk piksel değerleridir.



Şekil 6. 1 6x2 boyutlu sırasıyla S1,S2,S3,S4 pay görüntülerin ilk piksel değerleri

Gizlenen Görüntünün Yeniden Elde Edilmesi Kısmı

Gizlenen görüntü eşik değer k=3 adet rastgele pay görüntüden yeniden elde edilebilir. Bunun için (S1,S3,S4) pay görüntülerini kullanalım. Paylaşım kısmında kullanılan üreteç matrisinin (1. 3. ve 4.) sütunlarından bir kare A matrisi oluşturuldu.

$$A = \begin{bmatrix} a^3 & a^3 & a^2 \\ a^5 & a & a \\ a^4 & a^6 & a^4 \end{bmatrix} \quad Bu\ matrisin\ Gf(2^3)'ego\ddot{r}e\ tersi \quad A^{-1} = \begin{bmatrix} \alpha & a^5 & \alpha \\ a^4 & \alpha^4 & \alpha^6 \\ a^2 & a^3 & a^3 \end{bmatrix}$$

S1- S3-S4 pay görüntülerin piksel değerlerini alalım, bunu ters matris ile çarparsak orijinal görüntünün piksel değerlerini yeniden elde edebiliriz.

$$(\alpha^5\alpha^6\alpha^2) \quad x \begin{bmatrix} \alpha & a^5 & \alpha \\ a^4 & \alpha^4 & \alpha^6 \\ a^2 & a^3 & a^3 \end{bmatrix} = (\alpha^2\alpha^5\alpha^6)$$

$$(\alpha^3\alpha^5\alpha^6) \quad x \begin{bmatrix} \alpha & a^5 & \alpha \\ a^4 & \alpha^4 & \alpha^6 \\ a^2 & a^3 & a^3 \end{bmatrix} = \begin{pmatrix} 1 & \alpha & \alpha^2 \end{pmatrix}$$

Şeklinde tüm değerler işlenerek orijinal görüntünün değerleri yeniden elde edilir.

6.1. [12,4] Reed Solomon Kod ile Görüntü Sır Paylaşımı

$GF(2^8)$ sonlu cisminde $p(x) = x^8 + x^4 + x^3 + x^2 + 1$ indirgenemez polinomuna göre α ilkel eleman olmak üzere dört hata düzelten [255,247] RS kodu, kısaltılmış [n,k,d]=[12,4] parametrelerine sahip RS kodu ile (k,n-k) görüntü sır paylaşım şeması uygulanmıştır. Gerçekleştirilen uygulama Visual Studio 10 ile C# programlama dilinde yapılmıştır. Uygulama gizli görüntüyü pay görüntülere ayırma ve eşik değerdeki pay görüntüden gizli görüntüyü yeniden elde etme şeklinde iki aşamadan oluşmaktadır. Uygulamada $p(x) = x^8 + x^4 + x^3 + x^2 + 1$ indirgenemez polinomuna göre [12,4] RS kodun üreteç polinomu ve standart formdaki üreteç matrisi aşağıdaki gibi elde edilmiştir.

$$g(x) = (x + \alpha)(x + \alpha^2)(x + \alpha^3)(x + \alpha^4)(x + \alpha^5)(x + \alpha^6)(x + \alpha^7)(x + \alpha^8)$$

$$g(x) = a^{36} + a^{203}x + a^3x^2 + a^{220}x^3 + a^{253}x^4 + a^{211}x^5 + a^{240}x^6 + a^{176}x^7 + x^8$$

$$G = \begin{bmatrix} 1\ 0\ 0\ 0\ a^{156}\ a^{198}\ a^{25}\ a^{14}\ a^{177}\ a^{84}\ a^{40}\ a^{238} \\ 0\ 1\ 0\ 0\ a^{19}\ a^{222}\ a^{64}\ a^{176}\ a^{251}\ a^{245}\ a^{182}\ a^{93} \\ 0\ 0\ 1\ 0\ a^{229}\ a^{136}\ a^{139}\ a^{11}\ a^{209}\ a^{115}\ a^{139}\ a^{131} \\ 0\ 0\ 0\ 1\ a^{167}\ a^{222}\ a^{184}\ a^{217}\ a^{175}\ a^{204}\ a^{140}\ a^{219} \end{bmatrix}$$

Uygulama için 256x256 büyüklüğünde RGB renk kanalında bitmap türünde Babun resmi seçilmiştir. Daha sonra bu resim gri seviyeli görüntüye dönüştürülmüştür. Daha sonra görüntü aşağıda verilen algoritma1'e ve (4,8) eşik şemasına göre 8 adet pay görüntülere bölünmüştür. Elde edilen pay görüntülerinin her birinin boyutu 256x32' dir.

Bu 8 adet pay görüntüden en az 4 pay görüntü ile gizli görüntü algoritma2'de açıklandığı gibi yeniden elde edilmiştir (Yang, Hsieh, & Cai, 2014).

Algoritma1: (4,8) gizli görüntüyü paylaştırma

Girdi: I gizli görüntü ve GF(2^8) sonlu cisminde [12,4]-RS kodu ve RS kodunun standart formda üreteç matrisi G'dir.

1.Adım: I gizli görüntünün boyutu μ olmak üzere, k-piksel bloklarına bölünür (Her piksel değerleri GF(2^8)'in elemanıdır.).

2.Adım: Her $0 \leq i \leq \mu - 1$ olmak üzere $u = (p_{ik}, p_{ik+1}, p_{ik+2}, \dots, p_{ik+k-1})$,

$v = u * G = u * [I|P]$, $v = v_0, v_1 \dots v_{n-1}$ I, kxk boyutunda birim matris ve P, kxn boyutunda parity matris

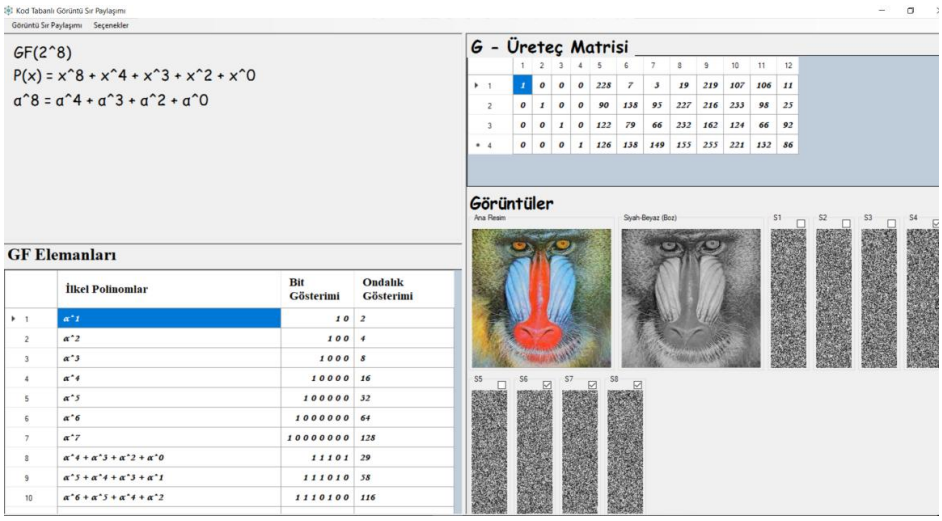
$v = (p_{ik}, p_{ik+1}, p_{ik+2}, \dots, p_{ik+k-1} || s_{in}, s_{in+1}, s_{in+2}, \dots, s_{in+n-1})$ şeklinde her iterasyonda k piksel bloğuna uygula.

3.Adım: j=1'den j=n'e kadar

$\{S_j = s_{j-1} || s_{n+j-1} || s_{2n+j-1} || \dots || s_{(\mu-1)xn+j-1}\}$

|| opertarörü n adet payın oluşumu için bir payın pixellerini birleştirmek için kullanılır.

Çıktı: S_1-S_n n adet pay görüntü (Şekil 6.2)



Şekil 6. 2 RS kod ile (k,n)=(4,8) Gizli Görüntü Paylaşım Kısmı

Algoritma2: (4,8) gizli görüntüyü yeniden elde etme

Girdi: 8 pay görüntüden herhangi 4 pay görüntü (Şekil 6.3).

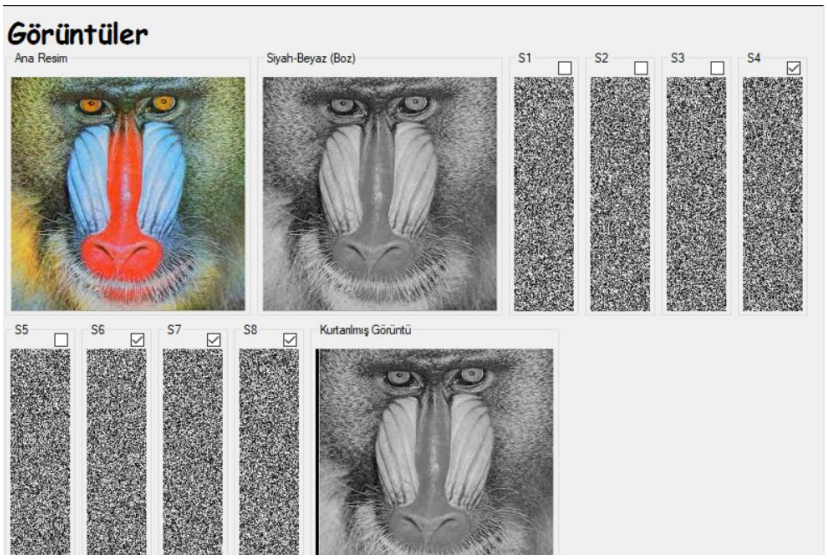
1.Adım: S_1, ..., S_8 herhangi 4 pay görüntüyü al

2.Adım: G üreteç matrisinden kxk'lık A alt matrislerini bul

3.Adım: A matrisinin tersini bul

4.Adım:$0 \leq i \leq \mu - 1 \{(p_{ik}, p_{ik+1}, p_{ik+2}, \dots, p_{ik+k-1}) = (s_{in}, s_{in+1}, s_{in+2}, \dots, s_{in+n-1}) * [A]^{-1}\}$

Çıktı: I gizli görüntü



Şekil 6. 3 k=4 eşik sayıda seçilen (S_4,S_6,S_7S_8) Pay Görüntülerden Gizli Görüntüyü Yeniden Elde Etme

Uygulamada gizli görüntüyü yeniden elde etme aşamasında 4-6-7-8 pay görüntüleri kullanılmıştır. Bu görüntüler kullanılarak kxk yani 4x4 boyutunda bir kare A alt matrisi, G üreteç matrisinin 4.,6.,7. ve 8. sütunlarından elde edilmiştir. Bu A matrisi $G' = (I_{kxk}|A_{kxk})$ standart formunda üreteç matrisiyle (n,k,d) parametreleri (8,4,5) olan bir MDS kodtur. Dolayısıyla A matrisi MDS matristir. Bu A MDS matrisi ve tersi aşağıda verilmiştir.

$$A = \begin{bmatrix} a^{14} & a^{84} & a^{40} & a^{238} \\ a^{176} & a^{245} & a^{182} & a^{93} \\ a^{11} & a^{115} & a^{139} & a^{131} \\ a^{217} & a^{204} & a^{140} & a^{219} \end{bmatrix} \quad A^{-1} = \begin{bmatrix} \alpha^{221} & \alpha^{194} & \alpha^{179} & \alpha^{239} \\ \alpha^{29} & \alpha^{178} & \alpha^{5} & \alpha^{147} \\ \alpha^{115} & \alpha^{82} & \alpha^{109} & \alpha^{8} \\ \alpha^{30} & \alpha^{245} & \alpha^{148} & \alpha^{247} \end{bmatrix}$$

6.2. Sonuçlar ve Tartışma

Bu tezde gizli görüntülerin güvenliğini sağlamak için kodlama teorisinden faydalanılmıştır. Özellikle $GF(2^8)$ sonlu cisminde üretilen [n,k]=[12,4] parametrelerine sahip RS kodu ile gizli görüntü (n-k) adet pay görüntülere bölünüp k adet pay görüntüyle yeniden elde edildiği gösterilmiştir.

Kodlama teorisi tercih etmedeki amaç, polinom tabanlı görüntü sır paylaşım metotlarında kullanılan permütasyon işlemine gerek olmadan gizlenmek istenen görüntünün piksel değerleri öncelikle cisim elemanları ile eşleştirilip seçilen (n,k) parametreli RS kodunun üreteç matrisi ile çarparak (n-k) adet pay görüntüler elde edebilmektir. Ve en az k adet pay görüntüyle herhangi bir görüntü kaybı olmaksızın orijinal görüntü yeniden elde edilebilmektedir. Çünkü $GF(2^8)$ uzayında [0-255] aralığındaki tüm renk değerleri tanımlanabilmektedir. Ayrıca kodlama teorisi kullanımı, yalancı kullanıcı olması durumunda ya da dışardan sisteme sızmaya çalışan birilerini önlemede avantaj sağlamaktadır. Hata düzeltme algoritmalarıyla kayıp ya da yalancı katılımcıların pay değerleri tespit edilip düzeltilerek orijinal veri yeniden elde edilebilir. Bu da kodlama teorisi kullanımdaki verinin güvenliğini sağlamada ve aynı zamanda kimlik doğrulamada etkili olduğunu ortaya koymaktadır.

BÖLÜM 7

İNVOLUTİF MDS MATRİSLER İLE GÖRÜNTÜ SIR PAYLAŞIMI UYGULAMASI

MDS matris tasarımında dairesel matrislerden ve Hadamard matrislerden faydalanılır. İnvolutif MDS matrisler ise şifreleme ve şifre çözme maliyeti aynı olduğundan verimli ve güvenli uygulamalar için önemli bir yere sahiptir (Akleylek & Sakallı, 2016). 6. Bölümde anlatıldığı gibi dairesel Reed Solomon kodlar ile alt matrisleri MDS matris olan üreteç matrisle görüntü sır paylaşım uygulamasını göstermiştik. Bu tip dairesel matrisler kullanımı donanım uygulamalarında maliyet açısından büyük avantaj sağlamaktadır.

Bu bölümde gri seviyedeki görüntüler için Hadamard matrislerden elde edilmiş olan involutif(tersi kendisi) MDS matris ile görüntü sır paylaşım şeması önerilmiş ve uygulaması gösterilmiştir. Hadamard matrisleri kullanmak involutif matris ($A = A^{-1}$) oluşturmak için büyük bir avantaj sağlar. Ayrıca involutif bir MDS matris ile görüntü paylaşımı ve görüntünün yeniden elde edilmesinde aynı matris ile işlem yapılması sağlanarak maliyeti düşürülmüştür. Dolayısıyla hafif- siklet(lightweight) bir görüntü sır paylaşım şeması önerilerek ve uygulanarak yeni bir yapı ortaya konmuştur.

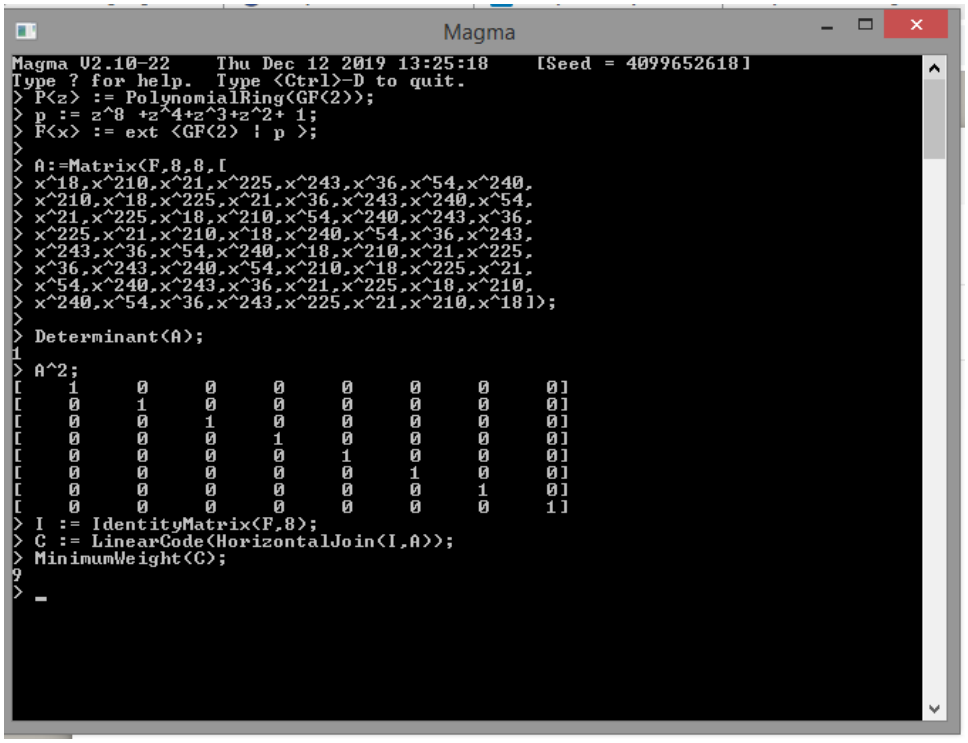
7.1. Hadamard- İnvolutif MDS Matris ile Görüntü Sır Paylaşım Şeması Uygulaması

Tezin bu bölümünde $GF(2^m)$ üzerinde görüntü sır paylaşım için kullanılacak olan involutif MDS matrisin elde edilmesinde, sonlu cisim işlemlerinde ve uygulama kısmında Magma yazılım paketi (Bosma, Cannon & Playoust, 1997) kullanılmıştır.

Matlab 2013a' da resim işleme kısmı yapılmıştır. Yani uygulamada kullanılan 256x256 gri seviyeli Lena.bmp resminin piksel değerleri Matlab ile elde edilmiştir. Uygulamada kullanılan 8×8 boyutunda $GF(2^8)$ üzerinde tanımlı indirgenemez polinomu $p(x) = x^8 + x^4 + x^3 + x^2 + 1$ ve minimum uzaklığı d=9 olan [16,8,9] MDS kodun Hadamard matris formunda involitif MDS matrisi ve Magma kodu aşağıdaki verilmiştir.

$$A^{-1} = A = \begin{bmatrix} x^{18} & x^{210} & x^{21} & x^{225} & x^{243} & x^{36} & x^{54} & x^{240} \\ x^{210} & x^{18} & x^{225} & x^{21} & x^{36} & x^{243} & x^{240} & x^{54} \\ x^{21} & x^{225} & x^{18} & x^{210} & x^{54} & x^{240} & x^{243} & x^{36} \\ x^{225} & x^{21} & x^{210} & x^{18} & x^{240} & x^{54} & x^{36} & x^{243} \\ x^{243} & x^{36} & x^{54} & x^{240} & x^{18} & x^{210} & x^{21} & x^{225} \\ x^{36} & x^{243} & x^{240} & x^{54} & x^{210} & x^{18} & x^{225} & x^{21} \\ x^{54} & x^{240} & x^{243} & x^{36} & x^{21} & x^{225} & x^{18} & x^{210} \\ x^{240} & x^{54} & x^{36} & x^{243} & x^{225} & x^{21} & x^{210} & x^{18} \end{bmatrix}$$

Aşağıda verilen Magma kodu yardımıyla A matrisinin MDS matris olma durumu doğrulanabilir.



Şekil 7. 1 8x8 MDS matrisin Magma kodu

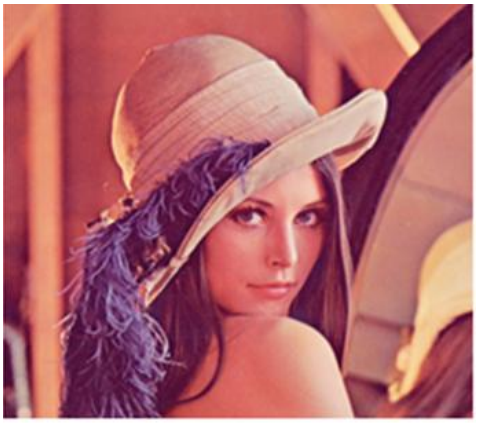
Cisim Eleman ($x^{\text{piksel değeri}}$)	**Elemana Karşılık Gelen Piksel**	**Elemanın Polinom İfadesi**	**Polinomun Katsayıları**
1	0	1	00000001
x^{25}	25	$x^1 + 1$	00000011
x^{50}	50	$x^2 + 1$	00000101
x^{26}	26	$x^2 + x^1$	00000110
x^3	3	x^3	00001000
x^{51}	51	$x^3 + x^1$	00001010
x^{238}	238	$x^3 + x^1 + 1$	00001011
x^{27}	27	$x^3 + x^2$	00001101
x^{199}	199	$x^3 + x^2 + x^1$	00001110
x^{75}	75	$x^3 + x^2 + x^1 + 1$	00001111
x^{100}	100	$x^4 + 1$	00010001
x^{14}	14	$x^4 + x^1 + 1$	00010011
x^{52}	52	$x^4 + x^2$	00010100
x^{141}	141	$x^4 + x^2 + 1$	00010101
x^{239}	239	$x^4 + x^2 + x^1$	00010110

Şekil 7. 2. $\boldsymbol{x^8 + x^4 + x^3 + x^2 + 1}$ indirgenemez polinomuyla $\boldsymbol{GF(2^8)}$'de üretilen elemanlar ve resmin piksel değerleri ile eşleşmesi

256x256 boyutundaki gri seviyedeki Lena görüntüsünün her bir pikselinin onluk sistemdeki sayı değeri $GF(2^8)$ üzerinde tanımlı cisim elemanlarına karşılık gelecek şekilde ilkel elemanın üssü olarak alınır. Bu çalışmada elemanları $GF(2^8)$'de tanımlı bir sonlu cismin seçilmesinin nedeni görüntü paylaşım şemasında kullanılacak gri seviye görüntülerin her bir pikselinin 0-255 arasında tam sayı değer alabilen 8 bit ile ifade

edilmesidir. $GF(2^8)$'de tanımlı cismin elemanları $x^0, x^1, \ldots, x^{255}$ arasında tanımlanır. Bu nedenle her bir piksel değeri $GF(2^8)$'de tanımlı cismin elemanı olarak ifade edilebilir. Dolayısıyla kayıpsız bir görüntü sır paylaşım şeması uygulanabilmektedir. Yukarıda şekil 7.2'de $x^8 + x^4 + x^3 + x^2 + 1$ indirgenemez polinomu kullanılarak üretilen 255 tane elemanın 15 tanesi ve her bir elemanın hangi piksel değerine karşılık geleceği gösterilmiştir (Pehlivanoğlu, Duru, & Sakallı, 2016).

Uygulamada gizli görüntü paylaşım şeması için resmin piksel değerleri önce sonlu cisim elemanları ile eşleştirilir. Daha sonra kullanılan matrisin boyutu kadar eleman yani 1x8'lik piksel blokları halinde [16,8,9] MDS kodun 8x8'lik involutif MDS matris ile çarpılarak 8 pay görüntü elde edilir. Elde edilen pay görüntülerin her birinin boyutu 256x32' dir. Bu 8 adet pay görüntünün herbirinden öncelikle ilk piksel değerleri alınarak oluşturulan 1x8'lik bir veri bloğu ve aynı şekilde diğer piksel değerleri tersi kendisi olan MDS matris ile çarpılarak orijinal görüntü yeniden elde edilir.

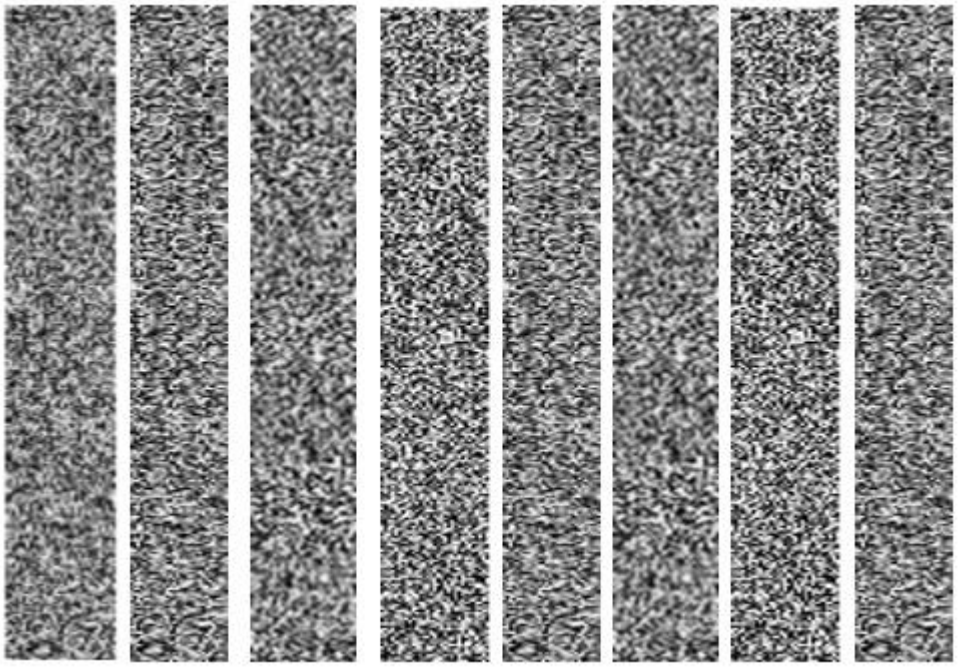


Şekil 7. 3 256x256 boyutlu Lena.bmp

Aşağıda gri renk paletinde Lena.bmp görseline ait ilk 110 piksel değerleri verilmiştir. Daha sonra bu piksel değerleri cisim elemanları ile eşleşip 8'er bloklar halinde MDS matrisle çarpılarak sıralı olarak 8 pay görüntünün pikselleri oluşturulur.

A:=Matrix(256,256,[165,161,157,157,161,163,162,159,159,159,157,156,155,155,154,154,158,162,165,166,168,172,172,170,170,175,171,159,149,140,123,105,96,94,94,98,102,105,108,111,107,108,109,109,108,109,110,111,112,109,107,109,110,112,116,120,12

3,121,123,126,127,126,128,132,130,128,128,130,133,134,132,130,125,128,131,131,13
0,130,133,136,132,135,136,134,134,135,133,131,136,133,131,132,134,135,133,130,13
8,137,136,136,136,136,134,133,133,134,132,129,129,132]



Şekil 7. 4 Sırayla S1,S2,S3,S4,S5,S6,S7,S8 pay görüntüler

Bu pay görüntülerin örneğin 1. Pay görüntünün bir kısmının piksel değerleri ve sonlu cisimdeki karşılığı aşağıda verilmiştir.

146 235 31 146 251 176 166 100 215 41 44 50 170 52 244 196 19 202 21 172 156 46 139 58 250 26 204 95 251 42 38 9; 39 33 156 139 133 21 11 2 166 110 218 230 7 0 177 186 39 244 188 113 70 118 240 237 179 241 195 0 136 63 181 86; 43 100 155 243 248 134 42 88 131 1 217 122 62 146 199 24 245 165 188 33 8 134 27 233 144 180 220 70 254 82 122 89; 223 120 100 30 80 143 178 136 53 92 86 19 0 111 91 13 87 58 67 163 242 232 173 22 9 182 56 243 80 64 179 57; 143 249 233 170 33 191 95 94 196 222 248 35 17 234 66 150 34 193 75 10 87 48 208 68 34 14 240 242 77 75 111 31;

[x^146 x^235 x^31 x^146 x^251 x^176 x^166 x^100 x^215 x^41 x^44 x^50 x^170 x^52 x^244 x^196 x^19 x^202 x^21 x^172 x^156 x^46 x^139 x^58 x^250 x^26 x^204 x^95 x^251 x^42 x^38 x^9]

[x^39 x^33 x^156 x^139 x^133 x^21 x^11 x^2 x^166 x^110 x^218 x^230 x^7 1 x^177 x^186 x^39 x^244 x^188 x^113 x^70 x^118 x^240 x^237 x^179 x^241 x^195 1 x^136 x^63 x^181 x^86]

2. Pay görüntünün bir kısmının piksel değerleri ve cisimdeki karşılığı :

130 230 224 206 14 118 247 80 85 32 53 196 46 166 238 38 195 131 47 108 127 94 95 209 209 47 246 221 64 215 67 250; 188 196 67 250 196 209 29 75 213 100 57 191 21 167 24 148 179 183 241 120 49 51 150 152 192 216 232 20 59 42 128 230; 112 85 20 27 175 186 32 144 46 24 146 9 64 29 85 31 115 1 231 176 169 72 156 106 181 246 13 174 184 78 205 144; 91 91 3 3 3 3 91 91 99 238 100 20 222 116 148 204 58 52 8 171 136 0 8 163 108 102 128 81 190 156 118 73;

[x^130 x^230 x^224 x^206 x^14 x^118 x^247 x^80 x^85 x^32 x^53 x^196 x^46 x^166 x^238 x^38 x^195 x^131 x^47 x^108 x^127 x^94 x^95 x^209 x^209 x^47 x^246 x^221 x^64 x^215 x^67 x^250]

[x^188 x^196 x^67 x^250 x^196 x^209 x^29 x^75 x^213 x^100 x^57 x^191 x^21 x^167 x^24 x^148 x^179 x^183 x^241 x^120 x^49 x^51 x^150 x^152 x^192 x^216 x^232 x^20 x^59 x^42 x^128 x^230]

1.pay görüntünün elde edilmesindeki magma kodunun bir kısmı aşağıda verilmiştir.

```
crp:=Matrix(F,8,8,[1..2^6]);
        for j:= 1 to 256 do
        for k:= 1 to 256 do
        B[j,k]:=x^A[j,k];
        end for;
        end for;

for j:= 0 to 31 do
for k:= 1 to 8 do
        if (h1 eq 0) then PrintFile ("Us8.txt",j*8+k);
        im0[1,ind0]:=j*8+k;
        ind0:=ind0+1;
        ind0;
        end if;
        end for;
        end for;

crp:=Matrix(F,8,8,[1..2^6]);
crp:=Matrix(F,8,8,[
x^18,x^210,x^21,x^225,x^243,x^36,x^54,x^240,
x^210,x^18,x^225,x^21,x^36,x^243,x^240,x^54,
x^21,x^225,x^18,x^210,x^54,x^240,x^243,x^36,
x^225,x^21,x^210,x^18,x^240,x^54,x^36,x^243,
```

```
x^243,x^36,x^54,x^240,x^18,x^210,x^21,x^225,

x^36,x^243,x^240,x^54,x^210,x^18,x^225,x^21,

x^54,x^240,x^243,x^36,x^21,x^225,x^18,x^210,

x^240,x^54,x^36,x^243,x^225,x^21,x^210,x^18]);


//0. parça


for j:= 1 to 256 do

for k:= 1 to 4 do

  rt1:=Matrix(F,1,8,[B[j,im0[1,(k-1)*8+1]],B[j,im0[1,(k-1)*8+2]],B[j,im0[1,(k-
        1)*8+3]],B[j,im0[1,(k-1)*8+4]],B[j,im0[1,(k-1)*8+5]],B[j,im0[1,(k-
          1)*8+6]],B[j,im0[1,(k-1)*8+7]],B[j,im0[1,(k-1)*8+8]]]);

bn:=rt1*crp;

for m:= 1 to 8 do

p0[j,(k-1)*8+m]:=bn[1,m];

6end for;

end for;

end for;

PrintFile ("p0.txt",p0);
```

Diğer pay görüntüler için de aynı işlem gerçekleştirilir. Pay görüntülerden orijinal görüntünün yeniden elde edilmesinde benzer şekilde bu defa MDS matrisinin tersi ile çarpılır. Tersi kendisi olduğu için yine aynı matrisle çarparak görüntü elde edilir.

Hadamard matris formunda elde edilmiş olan [16, 8, 9] parametreli MDS kod standart formdaki üreteç matrisi $G = (I_{kxk}|A_{kxk})$ şeklindedir. Burada özellikle A matrisi involutif (tersi kendisi) MDS matris olacak şekilde seçilmiştir. Ayrıca involutif bir MDS matris ile görüntü paylaşımı ve görüntünün yeniden elde edilmesinde aynı matris ile işlem

yapılması sağlanarak maliyeti düşürülmüştür. Sonuç olarak hafif- sıklet (lightweight) bir görüntü sır paylaşım şeması önerilerek yeni bir yapı ortaya konmuştur.

BÖLÜM 8

SONUÇLAR VE ÖNERİLER

Teknolojinin gelişmesiyle birlikte gizli bilgi iletimindeki güvenlik açıkları ve siber saldırıların artması bu bilginin dış ortamlara karşı korunmasını gerektirmektedir. Özellikle askeri, istihbarat ve bankacılık gibi gizli ve güvenli bilgi akışının zorunlu olduğu açıktır. Bu nedenle bilginin gizliliğini ve güvenliğini sağlamak için pek çok yöntemler kullanılmaktadır. Bunlardan bazıları steganografi ve kriptolojidir. Bunların yanında Sır Paylaşım Şemalarından faydalanılır. Amaç gizlenmesi gerekli olan gizli bilgi tek bir yetkilide ya da ortamda saklanmaktansa birçok yetkiliye dağıtarak güvenliği arttırmaktır.

Bu tezde gizli görüntülerin güvenliğini sağlamak için kodlama teorisinden faydalanılmıştır. Özellikle $GF(2^8)$ sonlu cisminde üretilen [n,k]=[12,4] parametrelerine sahip RS kodu ile gizli görüntü (n-k) adet pay görüntülere bölünüp k adet pay görüntüyle yeniden elde edildiği gösterilmiştir.

Kodlama teorisi tercih etmedeki amaç, polinom tabanlı görüntü sır paylaşım metotlarında kullanılan permütasyon işlemine gerek olmadan gizlenmek istenen görüntünün seçilen (n,k) parametreli RS kodunun üreteç matrisi ile çarparak (n-k) adet pay görüntüler elde edebilmektir. Ve en az k adet pay görüntüyle herhangi bir görüntü kaybı olmaksızın orijinal görüntü yeniden elde edilebilmektedir. Çünkü $GF(2^8)$ uzayında [0-255] aralığındaki tüm renk değerleri tanımlanabilmektedir. Ayrıca kodlama teorisi kullanımı, yalancı kullanıcı olması durumunda ya da dışardan sisteme sızmaya çalışan birilerini önlemede avantaj sağlamaktadır. Hata düzeltme algoritmalarıyla kayıp ya da yalancı katılımcıların pay değerleri tespit edilip düzeltilerek orijinal veri yeniden elde

edilebilir. Bu da kodlama teorisi kullanımdaki verinin güvenliğini sağlamada ve aynı zamanda kimlik doğrulamada etkili olduğunu ortaya koymaktadır.

İkinci olarak görüntü sır paylaşım şeması için $GF(2^8)$ sonlu cisminde Hadamard matris formunda elde edilmiş olan [16, 8, 9] parametreli MDS kod kullanılmıştır. Bu MDS kodun standart formdaki üreteç matrisi $\mathrm{G} = (\mathrm{I_{kxk}}|A_{kxk})$ şeklindedir. Burada özellikle A matrisi involutif (tersi kendisi) MDS matris olacak şekilde seçilmiştir. Ayrıca involutif bir MDS matris ile görüntü paylaşımı ve görüntünün yeniden elde edilmesinde aynı matris ile işlem yapılması sağlanarak maliyeti düşürülmüştür. Sonuç olarak hafif-sıklet (lightweight) bir görüntü sır paylaşım şeması önerilerek yeni bir yapı ortaya konmuştur.

Bunun gibi birçok farklı yapılarda kodlarla ve matrislerle görüntü sır paylaşım şemaları uygulanabilir. Ayrıca daha özel involutif MDS matrisler ile daha az maliyetli ve güvenli bir görüntü sır paylaşım şemalarının olması öngörülmekte ve gelecek çalışmalarımızda teorik ve uygulamalarla ortaya konması planlanmaktadır.

KAYNAKÇA

Akkanat, K. (2017). MDS yayılım matrislerinde izomorfizmalar üzerine yeni bir çalışma. Trakya Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi.

Akleylek, S., & Sakallı, M. T. (2016). MDS Matrisleri Üzerine Bazı Sonuçlar. *Dokuzuncu Uluslarası Bilgi Güvenliği ve Kriptoloji Konferansı.*

Arda, D. (2011). Kodlama teorisinin kriptografik açıdan incelenmesi. Trakya Üniversitesi Fen Bilimleri Enstitüsü Doktora Tezi.

Arda, D., Buluş, E., Akgün, F., & Yerlikaya, T. (2008). Secret Sharing Scheme in Cryptographic Key Management Problem. *International Scientific Conference UNITECH.* Gabroyo.

Aslan, B. (2008). Boole Fonksiyonları ve S-Kutularının Kriptografik Özelliklerinin İncelenmesi ve Ters Haritalama Tabanlı Cebirsel Açıdan Güçlendirilmiş Bir Skutusu Önerisi. Trakya Üniversitesi Fen Bilimleri Enstisüsü Yüksek Lisans Tezi.

Asmuth, C., & Bloom, J. (1983). Modular Approach to Key Safeguarding. *IEEE Transactions on Information Theory*, 208-210.

Bhondo, C., De Santis, A., Gargano, L., & Vaccaro, U. (1993). Secret sharing schemes with veto capabilities. *In Workshop on Algebraic Coding*, 82-89.

Blakley, G. R. (1979). Safeguarding cryptographic keys . *National Computer Conference*, 48,313-317.

Chapman, & Vermani, L. R. (1996). *Elements of Algebraic Coding Theory.* Chapman & Hall.

Cimato, Cimato, S., & De Santis, A. (2007). Colored visualcryptography without color darkening. *Theoretical Computer Science*, 261-276.

Denning, R. D. (1982). Cryptography and Data Security. Boston: Addison-Wesley Longman. *Longman Publishling Co.,Inc*.

Forouzan , B. A. (2008). *Cryptography and Network Security.* New York, USA: McGraw-Hill Inc.

Fossorier, M. P., Mihaljevic, M., & Imai, H. (1999). Reduced complexity iterative decoding of low-density parity-check codes based on belief propagation. *IEEE Trans. Commun*, 673-680.

Lidl, R., Niederreiter, H., & James, N. S. (1986). Breaking the Cade cipher. *In Conference on the Theory and Application of Cryptographic Techniques* , 60-63.

Lin, S., & Costello, D. (2004). Error Control Coding. *Fundamentals and Applications Prentice-Hall*, 704-712.

McEliece, R. J., & Sarwate, D. V. (1981). On sharing secrets and Reed-Solomon codes. *Communications of the ACM*, 583-584.

Mignotte, M. (1983). *How to Share a Secret* (s. 371-375). içinde Burg Feuertein.

Moreira, J. C., & Farrel, P. G. (2006). *Essentials of error control coding.* John Wiley & Sons.

Murphy, T. (2001). Finite fields. *University of Dublin School of Mathematics Ireland*, 27-29, 55-56.

Nakahara, J., & Abrahao, E. (2009). A new involutory MDS Matrix for the AES. *International Journal of Network Security*, 109-116.

Naor, M., & Shamir, A. (1995). Visual Cryptography. *Advances in Cryptology-Eurocrypt'94, LNCS, vol. 950*, 1-12.

Pehlivanoğlu, M., Duru, N., & Sakallı, M. T. (2016). Sonlu Cisim Teorisine Dayalı Gri Seviye Görüntü Şifreleme. *Bilecik Şeyh Edebali Ünv. Fen Bilimleri Dergisi Cilt:3 Sayı:2 ISSN2458-7575*.

Pieprzyk, J., & Zhang, X. M. (2004). On cheating immune secret sharing. *Discrete Mathematics and Theoretical Computer Science*, 253-264.

Roman, S. (1992). *Coding and Information Theory.* Springer.

Schoenmaker, B. (2011). Cryptography 2/Crytographic Protocols. *Lecture Notes Part 1 Crytographic Protocols*.

Shamir, A. (1979). How to Share a Secret. *Communications of the ACM*, 22, 612-613. .

Şahin Mesut, A., & Arda, D. (2009). Renkli Görüntü Dosyaları Üzerinde Gizlilik Paylaşımı Uygulaması. *IV İletişim Teknolojileri Sempozyumu.* Adana.

Thien, C., & Lin, J.-C. (2002). Secret image sharing. *Computers & Graphics, Volume 26, Issue 5*, 765-770.

Trappe, W., & Washington, L. (2006). Introduction to Cryptography with Coding Theory,Second Edition. *USA: Pearson Education, Inc. Pearson Prentice Hall*.

Ulutaş, G., Ulutaş, M., & Nabiyev, V. (2011). Medical image security and EPR hiding using Shamir's secret sharing scheme. *Journal of Systems and Software*, 341-353.

Yang, C.-N., Hsieh, C.-L., & Cai, S.-R. (2014). Secret Image Sharing Schemes by Using Maximum Distance Separable Code. *International Journal of Machine Learning and Computing*, 522-526.

Yuan, J. (2005). Secret sharing schemes from linear codes. *Hong Kong University of Science and Technology (Hong Kong)*, 206-212.

Zhu, B., Bao, F., Deng, R., & Kankanhalli, M. (2005). Efficient and robust key management for large mobile ad hoc networks. *Computer Networks*, 657-682.

Zorlu, Y. (2006). Reed-Solomon Kodların AWGN ve Rayleigh Kanallarda Başarım Analizi.

ÖZGEÇMİŞ

Gülşen GÜVEN, 1993 yılında Samsun'da doğdu. Liseyi Samsun'da 2011 yılında tamamladı. 2012 yılında Trakya Üniversitesi Bilgisayar Mühendisliği Bölümünü kazandı. 2016 yılında fakülteyi bitirip Trakya Üniversitesi Fen Bilimleri Enstitüsünde Hesaplamalı Bilimler alanında yüksek lisansa başladı. 2017 bahar döneminde Bilgisayar Mühendisliğine yatay geçiş yaptı. 2020 Ocak ayında İstanbul Maltepe'de İce Teknoloji E-Dönüşüm firmasında çalışmaya başladı.