Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Dergisi, Cilt: 3, Sayı: 2, 2016
ISSN: 2458-7575 (http://edergi.bilecik.edu.tr/index.php/fbd)

Sonlu Cisimler Teorisine Dayalı Gri Seviye Görüntü Şifreleme

Grayscale Image Encryption Based on Theory of Finite Fields

Meltem KURT PEHLİVANOĞLU[1*], Nevcihan DURU[2], M. Tolga SAKALLI[3]

Özet- **Teknolojinin gelişmesiyle birlikte, gizliliğin ve güvenliğin sağlanması için yapılan çalışmalar önem kazanmıştır. Bilginin üçüncü kişilerin eline geçmeden gönderici ve alıcı tarafları arasında iletilmesi için birçok yöntem geliştirilmiştir. Bu çalışmada 128x128 boyutundaki gri seviye görüntülerin piksel değerleri; taraflar (gönderici ve alıcı) arasında belirlenen indirgenemez polinoma göre, Galois Field (2^8) (GF(2^8)) de tanımlı sonlu cisim elemanlarıyla ifade edilmiştir. Her bir sonlu cisim elemanının ifade ettiği polinom katsayıları, 8 bit ikilik sayı gibi düşünülmüş, bu sayı; onluk sayı sistemine dönüştürülmüştür. Elde edilen onluk sayı sistemindeki değerler orijinal gri seviye görüntüdeki piksel değerleriyle değiştirilerek, elde edilen şifreli görüntü alıcıya gönderilmiştir. Çalışmada sonlu cisim elemanlarının üretilmesi, şifreleme ve deşifreleme işlemleri için Matlab programlama dili kullanılmıştır. Geliştirilen yöntem sayesinde şifrelenen gri seviye görüntüler kayıpsız olarak deşifrelenmiştir.**

Anahtar Kelimeler- **Görüntü Şifreleme, Sonlu Cisimler, Gri Seviye Görüntü Şifreleme, Deşifreleme.**

Abstract- **With the development of technology, studies to ensure privacy and security have gained importance. For transmitting information between sender and recipient sides without getting third parts many methods have been developed. In this study, according to irreducible polynomial that is determined between the parties (sender and recipient), the pixel values of grayscale images which are of size 128x128 that are expressed by finite field elements over Galois Field (2^8) (GF(2^8)). Polynomial coefficients of each finite field element considered as 8-bit binary number, than this number is converted to decimal number. These decimal numbers are replaced with the original grayscale pixel values than encrypted image is sent to the recipient. In this study Matlab is used to getting finite field elements, encryption and decryption process. Thanks to improved method encrypted grayscale images are decrypted as lossless.**

Keywords- **Image Encryption, Finite Fields, Grayscale Image Encryption, Decryption**

I. GİRİŞ

Alıcı ve gönderici tarafların yer aldığı haberleşme sistemlerinde; yetkisiz kişiler tarafından sistemi oluşturan kanala girilmesi, taraflar arasında paylaşılan önemli ve gizli bilgilerin dinlenmesi, bilgilerin elde edilmesi veya değiştirilmesi gizlilik ve mahremiyet açısından önemli bir problemdir. Bu problemin çözülmesi için, iletilecek verilerin şifrelenmesi yaygın olarak kullanılan yöntemlerden biridir.

Görüntülerin şifrelenmesi için kullanılan görüntü şifreleme algoritmaları temelde; değer dönüşümü, yerel permütasyon, değer dönüşümü ve yerel permütasyon kombinasyonları fikirlerine dayanır [1]. Değer dönüşümü algoritmalarında, orijinal veri kullanılan algoritma sonucunda elde edilen yeni değerle ifade edilir. Yerel permütasyon algoritmalarında orijinal verinin pozisyonları değiştirilirken, değer dönüşümü ve yerel permütasyon kombinasyonları algoritmalarında ise değer dönüşümü ve yer değiştirme işlemleri bir arada uygulanır.

Literatürde görüntülerin şifrelenmesi için geliştirilen birçok yöntem mevcuttur. Yen ve Guo 1998 yılındaki çalışmalarında [2] başlangıçta üretilen kaotik dizinin, bağıl dizilerin üretilmesinde kullanıldığı karmaşık yapılı sisteme dayanan görüntü şifreleme algoritması geliştirmişlerdir. Guo ve Yen [2] 1999 yılında yaptıkları çalışmalarında ise resmin piksellerinin ikili diziye göre yer değiştirildiği ayna benzeri resim şifreleme algoritmasını önermişlerdir. Chang ve arkadaşları 2000 yılında vektör kuantalama tabanlı görüntü şifreleme algoritması önermişlerdir [4]. Maniccam ve Bourbakis 2001 yılındaki çalışmalarında [5] SCAN dili ile yapılan görüntü şifreleme algoritmasını iyileştirerek kayıpsız sıkıştırma ve görüntü şifreleme yapan bir algoritma geliştirmişlerdir.

*Sorumlu yazar iletişim: meltem.kurt@kocaeli.edu.tr
[2,3]İletişim: nduru@kocaeli.edu.tr, tolga@trakya.edu.tr,
[1,2]*Bilgisayar Mühendisliği Bölümü, Mühendislik Fakültesi, Kocaeli Üniversitesi*
[3]*Bilgisayar Mühendisliği Bölümü, Mühendislik Mimarlık Fakültesi, Trakya Üniversitesi*

Cebirsel yapılar kullanılarak görüntü şifreleme ve görüntü gizleme yapan çalışmalar incelendiğinde 2005 yılında Scripcariu ve Frunza [6] GF üzerinde tanımlı tersi alınabilen fonksiyon tabanlı görüntü şifreleme algoritması önermişlerdir. 2010 yılında Andaç ve arkadaşları [7] gri seviye resimler üzerinde rasgele LSB (En Önemli Bit) yöntemini ve sayi teorisini kullanarak, bu resimler içine bilgi gizleyen yöntem önermişlerdir. 2011 yılında Lin ve Wang [8] Lin ve Chan'ın önerdiği tersi alınabilen görüntü steganografide gizlilik paylaşım şeması yöntemini geliştirmişler, geliştirdikleri yöntemde tüm işlemleri GF(2^a) üzerinde tanımlamışlardır. Srividya ve Akhila 2014 yılındaki çalışmalarında [9] GF(p^m) üzerinde Bezier Eğrisi tabanlı görüntü şifreleme yapan bir yöntem önermişlerdir. Chhotaray ve arkadaşları [10] 2015 yılındaki çalışmalarında AES (128) şifreleme algoritması kullanarak görüntü şifreleme yapmışlardır.

Literatürde görüntü şifreleme ile ilgili yapılmış çalışmalar incelendiğinde, sonlu cisimlerle görüntü piksellerinin ifade edildiği herhangi bir çalışmaya rastlanmamıştır. Bu çalışmada gri seviye görüntü şifreleme için sonlu cisim teorisi kullanan yeni bir yöntem önerilmiştir. Bu yöntemde görüntüye ait her bir piksel değeri GF(2^8) de tanımlı eleman cinsinden değer dönüşümü yapılarak şifrelenmiştir. Alıcı şifrelenmiş görüntüleri önerilen yöntemle deşifrelediğinde, kayıpsız olarak orijinal görüntü elde edilir. Geliştirilen algoritma Matlab programlama dilinde yazılmış, deneysel sonuçlar elde edilmiştir.

Çalışmada kullanılan matematiksel yapı ikinci bölümde verilmiştir. Üçüncü bölümde önerilen yöntem ayrıntılı olarak açıklanmıştır. Dördüncü bölümde ise önerilen yönteme ait deneysel sonuçlar verilmiş, son bölümde sonuç ve ileriki çalışmalardan bahsedilmiştir.

II. MATEMATİKSEL YAPI

Bu bölümde çalışma içinde kullanılan matematiksel yapı ile ilgili bilgi verilmiştir.

Tanım 2.1. Zm toplama (+) ve çarpma (●) tabanlı aritmetik modulo kümesi olmak üzere bazı aksiyomlar verilsin [11],

+ işlemi üzerinde kapalılık özelliği: $a, b \in Z_m \rightarrow a + b \in Z_m$
● işlemi üzerinde kapalılık özelliği: $a, b \in Z_m \rightarrow a \bullet b \in Z_m$
+ işlemi üzerinde değişme özelliği: $a, b \in Z_m \rightarrow a + b = b + a$
● işlemi üzerinde değişme özelliği: $a, b \in Z_m \rightarrow a \bullet b = b \bullet a$
+ işlemi üzerinde geçişme özelliği: $a, b, c \in Z_m \rightarrow (a + b) + c = a + (b + c)$
● işlemi üzerinde geçişme özelliği: $a, b, c \in Z_m \rightarrow (a \bullet b) \bullet c = a \bullet (b \bullet c)$
● işlemi üzerinde dağılma özelliği: $a, b, c \in Z_m \rightarrow (a \bullet b) \bullet c = a \bullet (b \bullet c)$
$a, b, c \in Z_m \rightarrow a \bullet (b + c) = a \bullet b + a \bullet c$
0 + işlemi üzerinde birim eleman olmak üzere: $a + \mathbf{0} = a, \forall a \in Z_m$
1 ● işlemi üzerinde birim eleman olmak üzere: $a \bullet \mathbf{1} = a, a \bullet \mathbf{0} = \mathbf{0}, \forall a \in Z_m$
+ işlemi üzerinde *a* elemanının tersi: $a \in Z_m \rightarrow$ m-*a*'dır.
● işlemi üzerinde *a* elemanının tersi: $a \in Z_m \rightarrow a^{-1}$'dir ve $a^{-1} \bullet a = \mathbf{1}$

Tanım 2.2. Z_m kümesi 1, 2, 5, 6 ve 7 numaralı aksiyomları sağlıyorsa + ve/veya ● işlemlerine göre gruptur denir.
Tanım 2.3. Z_m kümesi grup olmak üzere 3, 4 numaralı aksiyomları da sağlıyorsa Z_m kümesine Abelyen /Değişmeli (Abelian Group) grup denir.
Tanım 2.4. Z_m kümesi Abelyen grup olmak üzere, 8, 9 numaralı aksiyomları da sağlıyorsa Z_m kümesine halka denir.
Tanım 2.5. Z_m kümesi halka olmak üzere 10, 11 numaralı aksiyomları da sağlıyorsa Z_m kümesine cisim denir. Bir cisim sonlu elemanlardan oluşuyorsa bu cisme sonlu cisim denir.
Tanım 2.6. p^n elemanlı bir sonlu cisim Galois cismi olarak tanımlanır GF(p^n) ile gösterilir.
Tanım 2.7. GF(*p*)[x], a_i katsayıları GF(*p*) cisminde olan, rastgele dereceli $a_0 + a_1x + a_2x^2 + ... + a_{n-1}x^{n-1}$, $a_i \in \{0,1\}$, polinomlarının birleşimidir [12].
Tanım 2.8. GF(*p*)[x]'de düşük dereceden polinomların çarpımı şeklinde yazılamayan *f(x)* fonksiyonuna, GF(*p*)'de indirgenemez denir [12].
Tanım 2.9. Taban cisminden, genişletilmiş cismin tüm elemanlarını üretebilen polinoma ilkel (asal) polinom denir.

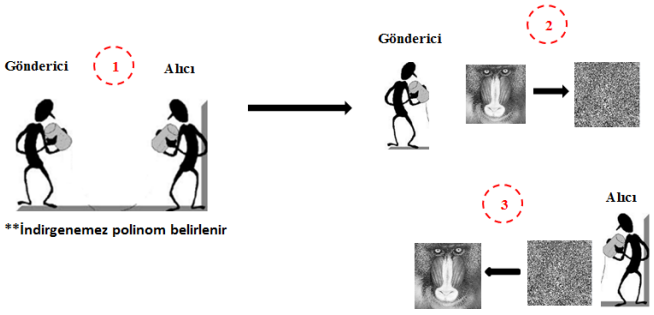
Örneğin Z_2 [x] / $1+x+x^4$ bir sonlu cisim olmak üzere, bu sonlu cismin eleman sayısı 16'dır. GF(2^4) şeklinde gösterilebilir. Bu sonlu cisme ait 0 haricindeki elemanlar ve bu elemanların nasıl elde edildiği Tablo 1'de ayrıntılı olarak verilmiştir.

Tablo 1. Z_2 [x] / $1+x+x^4$ sonlu cismin elemanları

Eleman	$1+x+x^4$ İndirgenemez Polinomu ile İlgili Elemanın Elde Edilmesi	Elemanın Polinom İfadesi
x^1	x	x
x^2	x^2	x^2
x^3	x^3	x^3
x^4	$1+x+x^4 \rightarrow x^4 = x+1$	x+1
x^5	$x^5=x^4*x \rightarrow (x+1)*x = x^2+x$	x^2+x
x^6	$x^6=x^4*x^2 \rightarrow (x+1)*x^2 = x^3+x^2$	x^3+x^2
x^7	$x^7=x^6*x \rightarrow (x^3+x^2)*x = x^4+x^3 = x^3+x+1$	x^3+x+1
x^8	$x^8=x^6*x^2 \rightarrow (x^3+x^2)*x^2 = x^5+x^4 = (x^2+x)+(x+1) = x^2+1$	x^2+1
x^9	$x^9=x^6*x^3 \rightarrow (x^3+x^2)*x^3 = x^6+x^5 = (x^3+x^2)+(x^2+x) = x^3+x$	x^3+x
x^{10}	$x^{10}=x^9*x \rightarrow (x^3+x)*x = x^4+x^2 = x^2+x+1$	x^2+x+1
x^{11}	$x^{11}=x^{10}*x \rightarrow (x^2+x+1)*x = x^3+x^2+x$	x^3+x^2+x
x^{12}	$x^{12}=x^{11}*x \rightarrow (x^3+x^2+x)*x = x^4+x^3+x^2 = x^3+x^2+x+1$	x^3+x^2+x+1
x^{13}	$x^{13}=x^{12}*x \rightarrow (x^3+x^2+x+1)*x = x^4+x^3+x^2+x = (x+1)+x^3+x^2+x = x^3+x^2+1$	x^3+x^2+1
x^{14}	$x^{14}=x^{13}*x \rightarrow (x^3+x^2+1)*x = x^4+x^3+x = (x+1)+x^3+x = x^3+1$	x^3+1
x^{15}	$x^{15}=x^{14}*x \rightarrow (x^3+1)*x = x^4+x = (x+1)+x = 1$	1

III. ÖNERİLEN YÖNTEM

Bu çalışmada gri seviyedeki görüntüleri şifrelemek için anahtara dayalı olmayan bir yapı önerilmiştir. Önerilen yöntemin yapısı Şekil 1' de verilmiştir.



Şekil 1. Önerilen gri seviye görüntü şifreleme yöntemi

Şekil 1'den de görüleceği gibi önerilen yöntem üç ana adımdan oluşmaktadır. İlk adımda alıcı ve gönderici tarafları indirgenemez polinom üzerinde anlaşır, 2. adımda ise gönderici belirlenen indirgenemez polinoma göre GF(2^8)'de cismin elemanlarını üretir, daha sonra bu elemanların polinom ifadelerinin katsayıları ikilik tabanda bir sayı gibi düşünülüp bu sayılar onluk sayı sistemine dönüştürülür. 128x128 boyutundaki gri seviye görüntüdeki her bir piksel, elemanları GF(2^8) üzerinde tanımlı cismin elemanlarıyla eşleştirilir daha sonra bu piksel değerleri eşleştirilen cisim elemanın onluk sayı sistemindeki değeriyle değiştirilir ve görüntü şifrelenir. Üçüncü adım deşifreleme adımıdır. Bu adımda alıcı şifrelenmiş görüntüyü göndericiden alır, indirgenemez polinomu ve cisim elemanlarını bildiği için şifrelenmiş piksel değerlerini, cismin elemanı olarak ifade edilen değerlerle eşleştirilerek gri seviyeli orijinal görüntüyü elde eder.

Bu çalışmada elemanları GF(2^8) de tanımlı bir sonlu cismin seçilmesinin nedeni, şifrelemek için kullanılacak gri seviye görüntülerin her bir pikselinin 0-255 arasında tam sayı değer alabilen [7] 8 bit ile ifade edilmesidir. GF(2^8) de tanımlı cismin elemanları x^1, x^2, …, x^{255} arasında tanımlanır. Bu nedenle her bir piksel değeri GF(2^8) 'de tanımlı cismin elemanı olarak ifade edilebilir.

A. İndirgenemez Polinomun Belirlenmesi

Çalışma kapsamında deneysel sonuçların elde edilmesi için tarafların indirgenemez polinomu $x^8+x^4+x^3+x^2+1$ seçtiği varsayılmıştır. Ancak Matlab üzerinde geliştirilen uygulamada indirgenemez polinom değiştirilerek cismin elemanları yeniden üretilebilir. Şekil 2'de $x^8+x^4+x^3+x^2+1$ indirgenemez polinomu kullanılarak üretilen 255 tane elemanın 23 tanesi verilmiştir. Matlab programlama dili kullanılarak elde edilen cisim elemanlarının polinom ifadeleri, polinom katsayıları ve her bir elemanın hangi piksel değerine karşılık geleceği hesaplanmıştır.

Eleman	Elemana Karşılık Gelen Piksel Değeri	Elemanın Polinom İfadesi	Polinomun Katsayıları
1	0	1	00000001
x	1	x^1	00000010
x^25	25	x^1+1	00000011
x^2	2	x^2	00000100
x^50	50	x^2+1	00000101
x^26	26	x^2+x^1	00000110
x^198	198	x^2+x^1+1	00000111
x^3	3	x^3	00001000
x^223	223	x^3+1	00001001
x^51	51	x^3+x^1	00001010
x^238	238	x^3+x^1+1	00001011
x^27	27	x^3+x^2	00001100
x^104	104	x^3+x^2+1	00001101
x^199	199	x^3+x^2+x^1	00001110
x^75	75	x^3+x^2+x^1+1	00001111
x^4	4	x^4	00010000
x^100	100	x^4+1	00010001
x^224	224	x^4+x^1	00010010
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 2. $x^8+x^4+x^3+x^2+1$ indirgenemez polinomuyla GF(2^8) 'de üretilen elemanlar

Sonlu cisim elemanlarıyla piksel değeri eşleştirilmesi için Şekil 3'de verilen yöntem kullanılmıştır. Her bir cisim elemanın üs değeri gri seviyedeki görüntünün piksel değerini ifade eder. Örneğin "27" piksel değeri, sonlu cisim elemanlarından "x^{27}" ile ifade edilir.

Sonlu Cisim Elemanı	İfade Ettiği Piksel Değeri
x piksel değeri	piksel değeri

Şekil 3. Sonlu cisim elemanıyla piksel değeri eşleştirilmesi

B. Şifreleme Adımı

Şifreleme adımında gönderici sırasıyla aşağıdaki adımları gerçekleştirir,

- Sonlu cismin her bir elemanı için; Şekil 2'de "Polinom Katsayıları" sütununda hesaplanan 8 bitlik ikilik tabandaki değerler, onluk tabana dönüştürülür.
- Gri seviye görüntünün her bir pikseli, bir önceki adımda hesaplanan onluk tabandaki değeriyle değiştirilir.
- Değiştirilen bu piksel değerleri birleştirilerek şifreli resim elde edilir.

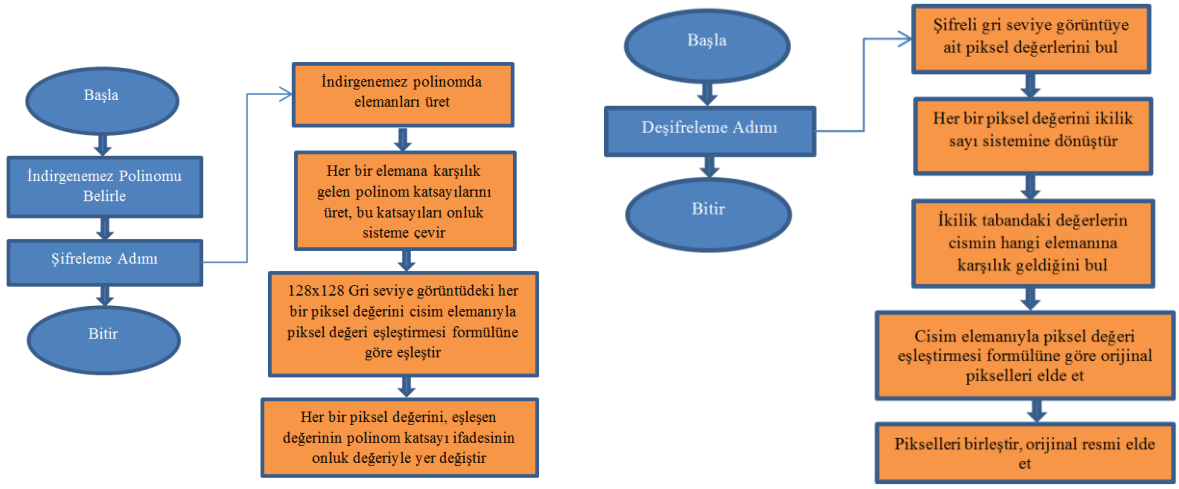
İndirgenemez Polinomun Belirlenmesi adımında verildiği gibi orijinal görüntüdeki "27" piksel değeri sonlu cismin "x^{27}" elemanıyla eşleştirilir, bu elemanın polinom katsayıları ifadesi "00001100" 'dır. Bu ifadenin onluk sayı sistemindeki gösterimi "12" 'dir. Böylece şifreleme işlemi için görüntüdeki "27" olan piksel değeri "12" olarak değiştirilir. 128x128 boyutundaki gri seviye görüntülerin şifrelenmesi için yukarıda verilen adımlar tüm pikseller için uygulanır.

C. Deşifreleme Adımı

Deşifreleme adımında ise alıcı şifrelenmiş görüntüyü alır sırasıyla,

- Şifreli gri seviye görüntüye ait piksel değerlerini elde eder,
- Her bir piksel değeri ikilik sayı sistemine dönüştürülür,
- Gönderici ile alıcı arasında belirlenen indirgenemez polinoma göre üretilen cisim elemanlarının polinom katsayıları ile her bir pikselin bir önceki adımda hesaplanan ikilik tabandaki değerleri karşılaştırılarak bu değerlerin cismin hangi elemanına karşılık geldiği bulunur. Şekil 3'de verilen eşleştirme kullanılarak görüntünün orijinal piksel değerleri hesaplanır. Hesaplanan bu piksel değerleri birleştirilerek orijinal görüntü elde edilir.

Şekil 4'de geliştirilen yöntemin şifreleme (Şekil 4.(a)) ve deşifreleme (Şekil 4.(b)) adımlarına ait akış diyagramları verilmiştir.



(a) **(b)**

Şekil 4. **(a)** Önerilen Yöntemin Şifreleme Adımları **(b)** Önerilen Yöntemin Deşifreleme Adımları

IV. DENEYSEL SONUÇLAR

Bu çalışma kapsamında geliştirilen yöntem sekiz farklı .bmp uzantılı [13] gri seviye görüntü üzerinde uygulanarak deneysel sonuçlar elde edilmiştir.

Elde edilen sonuçların başarısını analiz etmek için Wang ve arkadaşları tarafından önerilen [14] yapısal benzerlik indeksi ölçütü (Structural Similarity Index Measurement, SSIM) kullanılmıştır. SSIM; iki görüntü arasındaki kontrast, yapı ve parlaklık özelliklerini karşılaştırarak, bu iki görüntü arasındaki benzerliğin belirlenmesi için benzerlik indeksi oluşturur [14,15]. x ve y benzerlikleri karşılaştırılacak görüntüler olmak üzere, *l* parlaklık karşılaştırma (Eş. 1), *c* kontrast karşılaştırma (Eş. 2) ve *s* yapı karşılaştırma (Eş. 3) fonksiyonları olmak üzere, SSIM bu üç farklı fonksiyondan dönen değerleri parametre olarak alan bir fonksiyondur (Eş. 4) [14,15].

$$l(x,y) = \frac{2\mu_x\mu_y + c_1}{\mu_x^2 + \mu_y^2 + c_1} \tag{1}$$

μ_x ve μ_y görüntülere ait piksel yoğunluk ortalaması, c_1= $(K_1L)^2$, $K_1 \ll 1$ ve L piksel dağılım ölçütüdür.

$$c(x,y) = \frac{2\sigma_x\sigma_y + c_2}{\sigma_x^2 + \sigma_y^2 + c_2} \tag{2}$$

σ_x ve σ_y standart sapma, c_2= $(K_2L)^2$, $K_2 \ll 1$.

$$s(x,y) = \frac{\sigma_{xy} + c_3}{\sigma_x\sigma_y + c_3} \tag{3}$$

σ_{xy} ortak varyansı ifade eder.

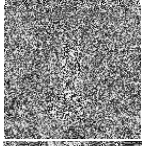
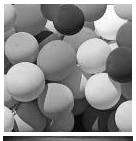
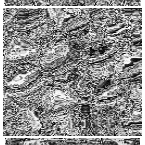
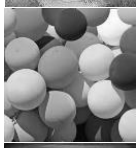
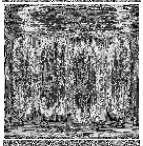
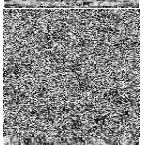
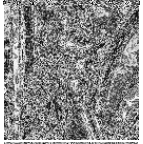
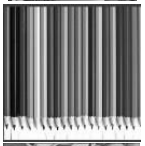
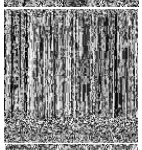
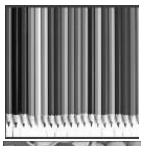
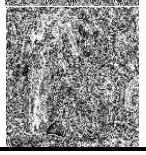
$$SSIM(x,y) = [l(x,y)^{\alpha}.c(x,y)^{\beta}.s(x,y)^{\gamma}] \tag{4}$$

$\alpha > 0, \beta > 0$ *ve* $\gamma > 0$ dır. Eğer $\alpha = \beta = \gamma = 1$ ve $c_3 = {c_2}/{2}$ ise SSIM değeri Eş. 5'de verildiği gibi olur.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_x\sigma_y + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{5}$$

Tablo 2'de önerilen yöntemle şifrelenen 128x128 boyutundaki sekiz farklı gri seviye görüntüye ait orijinal görüntü, şifreli görüntü ve deşifrelenmiş görüntü üçlüleri verilmiştir. Ayrıca önerilen yöntemle şifrelenmiş görüntüler ile orijinal görüntüler arasındaki ortalama SSIM değerleri ve deşifrelenmiş görüntüler ile orijinal görüntüler arasındaki ortalama SSIM değerleri aynı tabloda verilmiştir.

Tablo 2. Önerilen yöntemin farklı gri seviye görüntüler üzerinde test edilmesi

Gri Seviye Görüntü İsmi	Orijinal Görüntü	Önerilen Yöntemle Elde Edilen		Şifreli Görüntü İle Orijinal Görüntü Arasındaki Ortalama SSIM Değeri	Deşifrelenmiş Görüntü İle Orijinal Görüntü Arasındaki Ortalama SSIM Değeri
		Şifrelenmiş Görüntü	Deşifrelenmiş Görüntü		
cameraman128.bmp				0.0488	0.9987
baboon128.bmp				0.0546	1
baloon128.bmp				0.0214	1
door128.bmp				0.0069	1
flower128.bmp				0.0801	1
lena128.bmp				0.0455	1
pencil128.bmp				0.0343	0.9995
pepper128.bmp				0.0339	1

Eğer iki görüntü birbiriyle aynıysa SSIM değeri 1'dir. Tablo 2'de yer alan "Şifreli Görüntü ile Orijinal Görüntü Arasındaki Ortalama SSIM Değeri" sütunundaki değerler analiz edilirse bu değerlerin ortalama "0.040688" yani sıfıra yakın bir değer olduğu görülür. Ayrıca deşifrelenmiş görüntü ile orijinal görüntü arasındaki ortalama SSIM değerlerinin neredeyse tüm görüntülerde birbiriyle aynı olduğu ve deşifreleme adımından sonra veri kaybı olmadığı, Tablo 2'deki "Deşifrelenmiş Görüntü ile Orijinal Görüntü Arasındaki Ortalama SSIM Değeri" sütunundaki değerlerin 1'e eşit veya 1'e çok yakın olduğu görülmüştür. Ayrıca "Orijinal Görüntü" ile "Deşifrelenmiş Görüntü" sütunlarındaki görüntülerin aynı olduğu gözle de gözlemlenebilir.

V. SONUÇ VE İLERİKİ ÇALIŞMALAR

Bu çalışmada 128x128 boyutunda gri seviyeli görüntülerin şifrelenmesi için sonlu cisimler teorisinden faydalanan bir yöntem önerilmiştir. Yöntem sekiz farklı görüntü üzerinde test edilmiş, şifrelenmiş görüntülerden orijinal görüntüler kayıpsız olarak elde edilmiştir.

İleriki çalışmalarda bu yöntem daha büyük boyuttaki görüntüler üzerinde test edilebilir. Ayrıca güvenliğin arttırılması için bu yönteme ek olarak simetrik şifreleme algoritmalarından biri kullanılarak yöntemin başarısı arttırılabilir.

KAYNAKLAR

[1] Güvenoğlu, E. ve Suçsuz, N., "Yer Değiştirme ve Değer Dönüştürme Özelliğine Sahip Görüntü Şifreleme Algoritmalarının Analizi," *Akademik Bilişim Konferansları 2007-AB2007,* Kütahya, Türkiye, Ocak 2007.

[2] Yen, J. C. and Guo, J. I., "A new chaotic image encryption algorithm," *National Lien-Ho College of Technology and Commerce*, Taiwan, China, 1998.

[3] Guo, J. I. and Yen, J. C., "A new mirrorlike image encryption algorithm and its VLSI architecture," *10 th. VLSI Design/CAD Symposium, Taiwa*n, China, 1999.

[4] Chang, C. , Hwang, M. and Chen, T., "A new encryption algorithm for image cryptosystems," *The Journal of Systems and Software*, vol. 58, pp. 83-91, 2000.

[5] Maniccam, S. S. and Bourbakis, N. G., Lossless image compression and encryption using SCAN,"*International Journal of Pattern Recognition*, vol. 34, 2001.

[6] Scripcariu, L. and Frunza, M. D., "New Image Encryption Algorithm Based on Inversable Functions Defined on Galois Fields",*In Proc. of the Intern. Symposium on Signals, Circuits and Systems ISSCS 2005*, vol 1., pp. 243-246, 2005.

[7] Şahin, A., Buluş, E. ve Sakallı, M. T., "Gri Seviye Resimler Üzerinde Rasgele Lsb Yöntemini ve Sayi Teorisini Kullanarak Bilgi Gizleme Ve Steganaliz," Akademik Bilişim Konferansları 2006-AB2006, Denizli, Türkiye, Şubat 2006.

[8] Lin, Y. and Wang, P., "Improved Invertible Secret Image Sharing with Steganography," 2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Dalian, China, 2011.

[9] Srividya, B. V. and Akhila, S., "A Heuristic Approach for Secured Transfer of Image Based on Bezier Curve over Galois Field GF(pm)," Proceedings of International Conference on Circuits, Communication, Control and Computing (I4C 2014), MSRIT, BANGALORE, India, November 2014.

[10] Chhotaray, S. K., Chhotaray, A. and Rath, G. S., "A New Method of Generating Public Key Matrix and Using It for Image Encryption," *2015 2nd International Conference on Signal Processing and Integrated Networks (SPIN*), Noida, Delhi-NCR, India, 2015.

[11] Danacıoğlu, N. ve Muluk, F. Z., Galois cisimleri ve en yüksek çözümlü 2k-1 tasarımlarının oluşturulması, İ*statistikçiler Dergisi*,vol. 3,2010.

[12] Yavuzer Aslan, F. "Blok şifrelerde kullanılan doğrusal dönüşüm yapılarının incelenmesi," Yüksek Lisans Tezi, *Trakya Üniversitesi Fen Bilimleri Enstitüsü*, Edirne, 21, 2012.

[13] Vikipedi BMP. [Online]. Available: https://tr.wikipedia.org/wiki/BMP, 2016.

[14] Wang, Z., Bovik, A.C., Sheikh, H.R. and Simoncelli, E.P. Image Quality Assessment: From Error Visibility to Structural Similarity, *IEEE Transactions On Image Processing*,vol. 13, April 2004,.

[15] Kaya, Y. ve Kayci, L., "Kelebek Görüntülerinin Sınıflandırılması İçin Bir İçerik Bazlı Görüntü Erişim Sistemi," *Akademik Bilişim*, Mersin, Türkiye, Şubat 2014.