www.tubiad.org
ISSN:2148-3736
El-Cezerî Fen ve Mühendislik Dergisi
Cilt: 3, No: 2, 2016 (179-191)

El-Cezerî Journal of Science and Engineering
Vol: 3, No: 2, 2016 (179-191)

ECJSE

Makale / Research Paper

Resim Şifreleme Amacıyla Dinamik S Kutusu Tasarımı İçin Bir Yöntem

Erdal GÜVENOĞLU*

Maltepe Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Bilgisayar Mühendisliği Bölümü, 34857 İstanbul/TÜRKİYE
erdalguvenoglu@maltepe.edu.tr

Geliş/Received: 24.11.2015 **Düzeltme/Revised:** 16.02.2016 **Kabul/Accepted:** 29.02.2016

Özet: Yer değiştirme kutuları (Substitution Box, S-box) blok şifreleme algoritmalarında yaygın olarak kullanılmaktadır. S kutularının kullanılması şifreleme algoritmasını daha güçlü hale getiren bir özelliktir. Günümüzde yaygın olarak kullanılan AES (Advanced Encryption Standard) gibi pek çok şifreleme algoritmasının temelinde S kutuları yer almaktadır. AES şifreleme algoritması bir blok şifreleme algoritmasıdır. Blok şifreleme algoritmalarının temelinde S kutuları yardımıyla yer değiştirme işlemi yatmaktadır. Bu özelliğinden dolayı multimedya uygulamalarında da kullanılmaktadır. Günümüzde multimedya uygulamalarının yaygın olarak kullanılması ile birlikte görüntü verilerinin güvenliğinin sağlanması da önemli bir hale gelmiştir. Özellikle mobil teknolojilerin kullanımının hızla artması beraberinde güvenlik sorunlarını da getirmiştir. Güvenlik sorunlarının ortadan kaldırılmasının en iyi yolu görüntü verilerinin şifrelenmesidir. Bu çalışmada, AES blok şifreleme algoritmasında kullanılan S kutularına benzer S kutuları dinamik olarak üretilmiştir. Üretilen S kutusu yardımıyla görüntülerin şifrelenmesini ve deşifrelenmesini sağlayan bir yöntem önerilmiştir. Önerilen yöntem, S kutusunun üretilmesi ve görüntülerin şifrelenmesi/deşifrelenmesi olarak iki aşamadan oluşmaktadır. Yöntemden elde edilen sonuç görüntüleri üzerinde farklı analizler yapılarak saldırılara karşı dayanıklılığı test edilmiştir.

Anahtar kelimeler: Şifreleme; görüntü şifreleme; veri güvenliği; s-kutusu tasarımı; güvenlik analizi.

A Dynamic S-BOX Design Method for Image Encryption

Abstract: Substitution Boxes (S-Box) are frequently used by block encryption algorithms. It is because of they become more robust by employing S-Boxes. Recently, S-boxes are fundamental part of the most encryption algorithms such as Advanced Encryption Standard (AES). AES is a block encryption algorithm. Block encryption algorihms are based on substitution operations with the help of S-boxes. Therefore, it is used by multimedia applications. Nowadays, security of the image data became important because of the frequently used multimedia aplications. Especially, widespread mobile technology usage brought along the security issues. Encryption seems the most effective way of eliminating these problems. In this study, AES-like S-boxes are generated dynamically and an algorithm employing them for image encryption/decryption is proposed. Suggested method's first stage is generating an S-box and the second stage is using generated S-box for image encryption/decryption processes. Finally, various analyses are applied on the obtained result images against attacks for the evaluation of reliability.

Keywords: Encryption; image encryption; data security; s-box design; security analysis.

Bu makaleye atıf yapmak için
Güvenoğlu, E., "Resim Şifreleme Amacıyla Dinamik S Kutusu Tasarımı İçin Bir Yöntem", El-Cezerî Fen ve Mühendislik Dergisi 2016, 3(2); 179-191.

How to cite this article
Güvenoğlu, E., "A Dynamic S-BOX Design Method for Image Encryption",El-Cezerî Journal of Science and Engineering, 2016, 3(2); 179-191.

1. Giriş

Şifreleme, verilerin gizlenmesinde ve güvenli bir şekilde iletilmesinde yaygın olarak kullanılmaktadır. Şifrelemede kullanılan algoritmalar bir kripto sistemin temel öğesini oluşturmaktadır. Bir kripto sistem, şifreleme algoritması, anahtar, açık metin ve şifreli metinden meydana gelmektedir [1]. Geçtiğimiz yüzyıl da verilerin şifrelenmesi için DES (Data Encryption Standard) [2] ve AES (Advanced Encryption Standard) [2,3] gibi pek çok yöntem geliştirilmiştir. AES ve DES blok şifreleme algoritmalarıdır. AES ve DES gibi blok şifreleme algoritmaları metin türündeki verilerin şifrelenmesinde oldukça etkin rol oynamaktadır. Fakat resim ve video dosyalarının boyutlarının çok büyük olmasından dolayı resim şifreleme için kullanımları uygun görülmemektedir [4].

Blok şifreleme algoritmaları günümüzde kriptografide çok önemli bir yere sahiptir. Bu tür algoritmalar verinin şifrelenmesinde ve deşifrelenmesinde aynı anahtarı kullanmaktadırlar. Blok şifreleme algoritmalarının gücü kullanılan S kutuları ile arttırılmaktadır. S kutuları blok şifreleme algoritmalarına karıştırma özelliği katmaktadır ve tek doğrusal olmayan özelliğidir. Bu nedenle iyi seçilen bir S kutusu şifrelemenin sonucunu doğrudan etkilemektedir. S kutuları tasarlanırken pseudo-random, sonlu cisimde ters alma, sonlu cisimde üs alma ve heuristic teknikler kullanılmaktadır [5].

Günümüzde mobil teknolojilerin yaygın bir şekilde kullanılmasıyla birlikte görüntü verilerinin güvenliğinin sağlanması da kritik bir öneme sahip olmuştur. Bu güvenliğin sağlanabilmesi görüntülerin şifrelenmesi ile sağlanabilmektedir. Görüntü şifreleme teknikleri kaotik tabanlı ve kaotik tabanlı olmayan teknikler olarak iki grup altında toplanmaktadır [4]. Kaotik şifreleme algoritmaları şifreleme ve deşifreleme işlemleri için kullanıcıdan parametre almaktadırlar. Ayrıca şifreleme işlemi için kullanılan anahtar değeri şifreleme işleminin her bir adımında değişmektedir. Deşifreleme işleminde, şifreleme için kullanılmış olan kullanıcı parametresinin aynısı kullanılmadığında orjinal görüntü elde edilememektedir [6]. Görüntü şifreleme teknikleri üç temel fikre sahiptir. Bunlar yer değiştirme, değer dönüşümü ve bunların birlikte kullanıldığı permütasyon tekniklerdir [7]. Değer dönüşümü algoritmaları ile mevcut pikselin sahip olduğu renk değeri değiştirilmektedir. Yer değiştirme algoritmalarında ise mevcut piksellerin konumları bir algoritma yardımı ile başka konumlara taşınarak karıştırılmaktadır.

Kaotik şifreleme algoritmalarının dayanıklılığını arttırmanın en iyi yollarından biri blok şifreleme algoritmalarının altyapısında yer alan S kutularını kullanmaktır. Görüntü şifrelemek amacıyla AES şifreleme algoritmasının alt yapısında yer alan S kutuları kullanılabilmektedir [8, 9, 10, 11]. Bu çalışmalarda S kutuları dinamik olarak üretilmemiş ve mevcut olan S kutuları kullanılmıştır. Bu çalışmaların ortak özelliği şifreleme ve deşifreleme için önerilen kaotik yöntemler ve AES S kutuları yardımıyla piksellerin karıştırılmasıdır. Kaotik yapı ile birlikte AES şifreleme algoritması [9]' da doğrudan uygulanmıştır. AES blok şifreleme algoritması metin verilerin şifrelenmesi için etkin olarak kullanılmasına rağmen görüntü dosyalarının büyüklüğü nedeniyle doğrudan kullanımı uygun değildir.

AES S kutularının dışında Blowfish blok şifreleme algoritmasına ait S kutularını [12] ve MD5 anahtarlama algoritmasını [13] kullanan görüntü şifreleme teknikleri de bulunmaktadır. MD5 algoritması yardımı ile kullanıcı anahtarına bağlı 16 byte' lık bir anahtar dizisi elde edilmektedir. Bu anahtar dizisi bu yöntemde S kutusu görevini görmektedir. 16 byte' lık anahtar dizisi ikili gruplara ayrılmaktadır. Her bir ikili grup değeriyle görüntü pikselleri XOR işlemine tabi tutularak tekrarlı bir şekilde tüm piksellere uygulanır.

S kutularının üretimi için kaotik şifrelemede kullanılan Baker's Map ve Arnold Cat Map algoritmalarını kullanan yöntemlerde bulunmaktadır [14, 15]. Baker's Map, iki boyutlu bir

görüntünün satır veya sütunlardan bölünerek numaralandırılması ile bir haritanın elde edilmesini sağlamaktadır. Elde edilen harita yardımı ile görüntü pikselleri karıştırılmaktadır. Baker's Map ile tasarlanmış kaotik bir sistem içerinde, sistem hakkında yeterli bilginin bulunmadığı durumlarda sistemin çıkış değerlerini tahmin etmek güçtür. Fakat sistem hakkında küçük bir bilginin bilinmesi durumunda çıkış değerleri tahmin edilebilmektedir. Sistemin tekrarlı bir şekilde çalıştırıldığında belli bir süreden sonra sistem rastgele bir davranış göstermektedir. Bu nedenle şifreleme uygulamalarında kullanılmaktadır [14]. Arnold Cat Map ise, iki boyutlu ters kaotik bir haritalama kullanmaktadır. Orjinal bir görüntüdeki piksel pozisyonlarının değiştirilmesi için kullanılmaktadır. Ancak yeteri miktarda yöntem arka arkaya tekrar edilirse orjinal görüntüye ulaşılmaktadır [15].

S kutuları farklı biçimlerde üretilebilmektedir. Bunlardan bir tanesi Anchal vd. [16] tarafından önerilen DNA (Deoksiribo Nükleik Asit) tabanlı bir görüntü şifreleme yöntemidir. Bir piksel 8 bit ile temsil edilebilmektedir. Yöntemde her bit çiftine karşılık DNA yapısında yer alan baz isimleri verilmiştir. Cytosine (C - Sitozin) 00, thymine (T - Timin) 01, adenine (A - Adenin) 10 ve guanine (G - Guanin) 11 ile temsil edilmiştir. Her bir baz çiftine karşılık 1 ve 256 arasında ondalık bir sayı gelecek şekilde 16 × 16' lık bir S kutusu oluşturulmuştur. Bu yöntem sadece gri seviye görüntüler üzerinde uygulanabilmektedir. Rastgele sayı üreteçleri yardımıyla S kutularının üretilmesini ve görüntü şifrelemede kullanımını gerçekleştiren bir yöntem Khan vd. tarafından önerilmiştir [17]. Yöntemde 1 ve 256 arasında birbirinden farklı rastgele sayılar üretilerek 16 × 16' lık S kutusu elde edilmektedir. Elde edilen S kutusundan faydalanılarak ve Baker's Map algoritması kullanılarak görüntü şifreleme/deşifreleme yapılmıştır.

Bu çalışmada, kullanıcıya ait gizli bir anahtar yardımı ile AES S kutularına benzer S kutuları üreten ve S kutuları kullanılarak görüntülerin şifrelenmesini yada deşifrelenmesini sağlayan kaotik bir yöntem önerilmiştir. Önerilen yöntem iki aşamadan oluşmaktadır. Bunlardan birincisi S kutularının dinamik olarak üretilmesi yöntemi ikincisi ise şifreleme/deşifreleme yöntemidir. S kutuları doğrusal olmayan bir yapıya sahip olmalıdır. Bu nedenle S kutularının dinamik olarak üretilmesinde sözde rastgele (pseudo-random) tekniklerinden biri olan K/DSA (Knutt Durstenfeld Shuffle Algorithm) algoritması kullanılmaktadır. Önerilen yöntemin en büyük avantajı S kutusu ile birlikte Ters S kutusunun üretilmesidir. Literatürdeki yöntemlerle karşılaştırıldığında S kutusunun saklanması ihtiyacı ortadan kalkmaktadır. Ayrıca S kutusunun üretimi kullanıcı anahtarına bağlı olduğun çok geniş bir anahtar uzayına sahiptir. Önerilen şifreleme/deşifreleme yöntemi dinamik olarak üretilen S kutusu yardımıyla piksellerin konumlarının değiştirilmesine olanak sağladığından resim, video v.b. yüksek veriye sahip görüntüler üzerinde kolaylıkla uygulanabilmektedir.

2. Materyal ve Önerilen Yöntem

Bu bölümde görüntülerin şifrelenebilmesi amacıyla S kutularının dinamik olarak nasıl üretildiğine ve üretilen S kutularının görüntü şifrelemede/deşifreleme' de nasıl kullanıldığına yer verilmiştir.

2.1. K/DSA algoritması

Kart karıştırma, sayılar bilimi, şifreleme ve simülasyon gibi alanlarda günlük yaşantımızda olduğu gibi bilgisayar hesaplamalarında da rastgele sayıların permütasyonu, ya da literatürde bilinen adıyla "shuffle" sıklıkla kullanılmaktadır. Shuffle algoritmalarının bu versiyonu, 1963 yılında L.E.Moses ve R.V.Oakford [18] ve 1964' de Richard Durstenfeld [19] tarafından yayınlanmıştır. Fakat yaygın olarak Knuth Shuffle olarak bilinmiş ve 1969' daki "The Art of Computer Programming" kitabının ikinci cildinde yayınlanmıştır [20].

K/DSA, bir dizi elemanın kendi içerisinde yer değiştirmesi suretiyle karıştırılması için tasarlanmıştır. Eleman sayısı "n" olan bir "X" dizisinin elemanlarının K/DSA ile nasıl elde edildiği aşağıdaki sözde kod ile gösterilmiştir.

```
0..n arasındaki n adet eleman X dizisine yazılır.
Rastgele sayı üretimi için başlangıç değeri (seed) belirlenir.
for i from n-1 downto 0 do
begin
  0 ≤ j ≤ n-1 arasında rastgele bir tamsayı üretilir.
  X[i] ile X[j] elemanları yer değiştirilir.
end
```

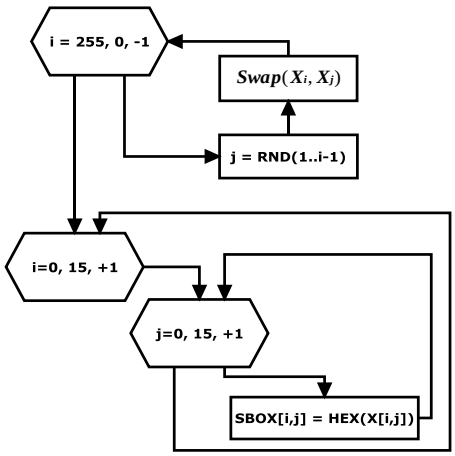
Başlangıç değeri şifrelemede kullanılacak olan gizli anahtarı temsil etmektedir. Başlangıç değerinin farklı bir değer seçilmesi durumunda farklı bir rastgele sayı dizisi elde edilecektir. K/DSA' nın çalışma prensibi şöyledir. X dizisinde 0 dan (n-1)' e kadar sıralı tamsayılar yazılmaktadır. Ardından $0 \leq j \leq (n-1)$ olacak şekilde rastgele bir j sayısı seçilmektedir. Ardından X[i] ile X[j] elemanlarının yerleri değiştirilir. Sonraki adımda bu defa $1 \leq j \leq (n-2)$ olacak şekilde yeni bir rastgele j belirlenir ve X[j] ile X[i-1] elemanları yer değiştirir. İşlem son iki sayının yerlerinin değiştirilmesine kadar devam eder. Doğal olarak sonraki adımlarda sağ tarafa aktarılmış elemanlar bir daha yer değiştiremezken sol tarafa aktarılmış elemanların yerleri tekrar tekrar değiştirilmiş olacaktır [21]. K/DSA' nın yapısı gereği rastgele sayı üretimi için başlangıç değeri (seed) aynı olduğu durumda her zaman aynı X dizisi elde edilecektir.

2.2. K/DSA ile S kutularının üretimi

Ayrıntıları yukarıda verilen K/DSA yöntemi ile görüntü şifrelemede kullanılacak olan S kutusu dinamik olarak elde edilmektedir. S kutusunun dinamik olarak elde edilmesi ve saklanmaması görüntü şifrelemede ve deşifreleme de önemli bir avantajdır. Zira şifreleme ve deşifreleme işlemi için uygun S kutularının üretilebilmesi ancak doğru anahtarın bilinmesi ile mümkündür. S kutusu 256 farklı tamsayıdan meydana gelmektedir. Dolayısı ile maksimum uzunluğu $n_{max} = 256$ olacağından, doğru S kutusunun bir denemede bulunma olasılığının;

$$P = 1/\sum_{i=1}^{n_{max}} (n_{max} - i)! \qquad (1)$$

olacağı açıktır. Önerilen yöntemde S kutusu elde edilirken beraberinde deşifreleme için kullanılacak ters S kutusu da elde edilmektedir. Dolayısı ile ters S kutusunun bir deneme de elde edilme olasılığı denklem 1 ile aynıdır. Ters S kutusunun, S kutusu ile birlikte yaratılması deşifreleme süresini önemli derecede azaltmaktadır. S kutusunun elde edilmesini sağlayan akış diyagramı Şekil 1' de gösterilmektedir.



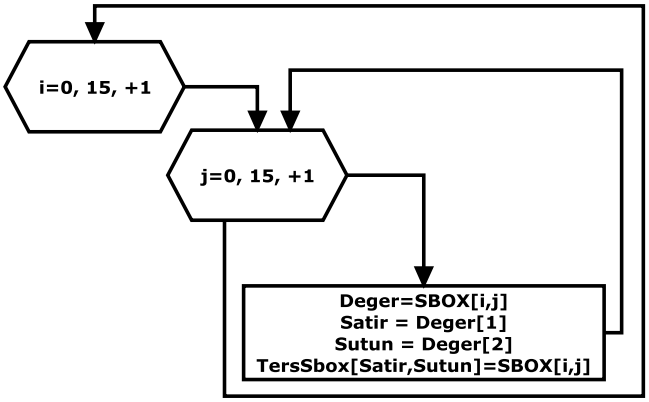
Şekil 1. S Kutusunun elde edilmesi

S kutuları 16 × 16 boyutlarında ve 256 adet değerden oluşmaktadır. K/DSA yardımı ile 256 adet tamsayı kullanıcı tarafından belirlenen başlangıç değerine göre karıştırılmaktadır. Elde edilen karıştırılmış dizinin ilk elemanından başlamak üzere her bir değerin hexadecimal (16' lık sayı sistemi) karşılıkları alınmaktadır. Hexadecimal karşılıkları 16 × 16' lık matrisin ilk hücresinden başlamak üzere satır satır yerleştirilmektedir. K/DSA ile elde edilen S kutularından olası bir tanesi Şekil 2' de gösterilmektedir.

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

Şekil 2. K/DSA yardımıyla üretilen olası S kutusu

S kutusuna bağlı olarak ters S kutusunun elde edilmesini sağlayan akış diyagramı Şekil 3' de gösterilmektedir.



Şekil 3. Ters S kutusunun elde edilmesi

Üretilen S kutusu ters S kutusunun üretilmesinde kullanılmaktadır. Ters S kutusu şöyle elde edilmektedir. Örneğin Şekil 2' de verilen S kutusunda 6. satır ve D. sütunun kesiştiği noktada AB değeri yer almaktadır. AB değeri, ters S kutusunda A. satır B. sütun olarak kabul edilecek ve S kutusundaki değer olan 6D bu kesişim noktasına yazılacaktır. Bu işlem S kutusunda yer alan bütün değerlere uygulanmaktadır. Ters S kutusunun dinamik olarak elde edilmesi, deşifreleme süresini kısaltan önemli etkendir. Üretilen olası bir ters S kutusu Şekil 4' de gösterilmektedir.

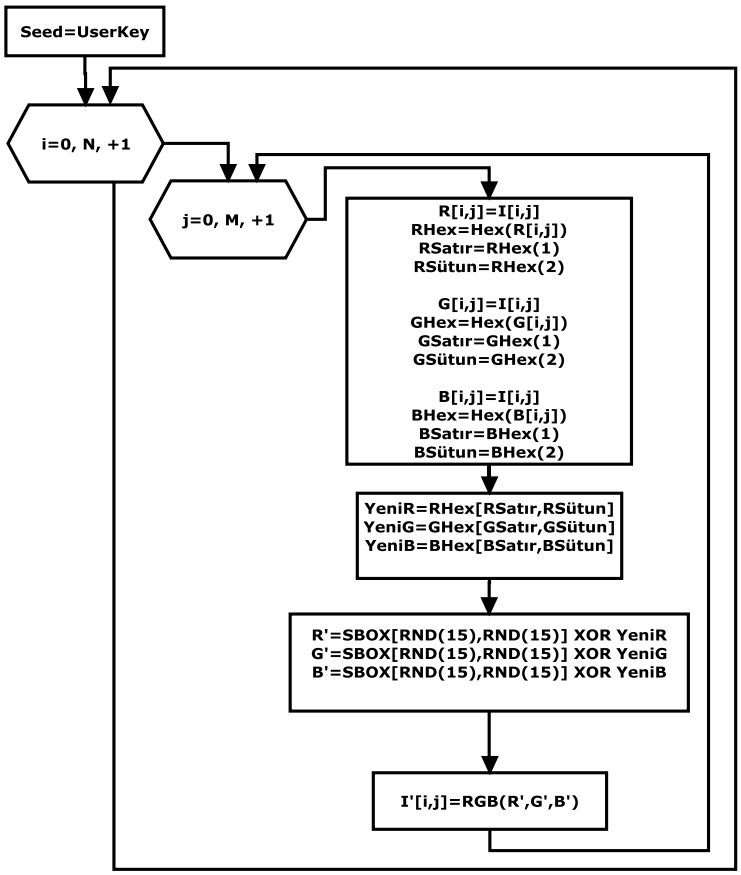
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	10	DC	01	B6	32	64	66	89	BC	88	5B	46	5F	FC	AF	44
1	4D	2F	A0	2E	BB	4E	9C	6E	7C	0E	2D	7E	9D	8C	8E	C0
2	47	D9	F0	C1	51	E8	0C	97	3A	52	2A	E1	1E	0D	54	A3
3	05	09	81	45	6C	90	8B	C2	D4	BA	82	9F	F7	20	78	D3
4	EA	71	CE	84	FE	EF	B8	A8	35	65	B5	A9	E7	BE	EC	19
5	C6	80	D7	D0	24	94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

Şekil 4. Üretilen olası ters S kutusu

Her S kutusundan sadece bir adet ters S kutusu elde edilebilmektedir. Ters S kutusunun elde edilebilmesi S kutusunun oluşturulabilmesine bağlıdır.

2.3. S kutularının görüntü şifreleme ve deşifreleme için kullanılması

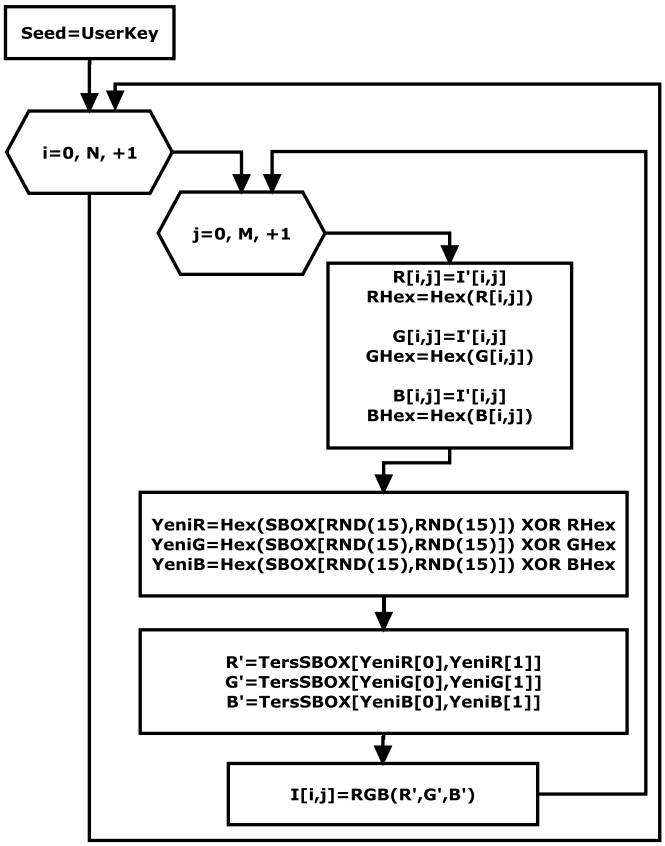
Günümüz teknolojisi göz önünde alındığında görüntü şifrelemenin renkli görüntüler üzerinde uygulanması kaçınılmazdır. Renkli görüntüler RGB (Red, Green, Blue) olmak üzere üç temel renkten oluşmaktadır. RGB uzayı kullanarak doğadaki tüm renkler bu üç temel rengin belirli oranlarda karıştırılması ile elde edilebilmektedir. Önerilen yöntemde, 24 bit derinliğe sahip bmp ve jpg formatındaki renkli görüntüler kullanılmıştır. Şifreleme işleminin ilk adımında orijinal görüntünün her pikselinin RGB değerleri elde edilmektedir. Her bir renk değerinin hexadecimal karşılığı alınmaktadır. Elde edilen hexadecimal karşılığın ilk değeri satır ve ikinci değeri ise sütun olarak kabul edilmiştir. K/DSA ile elde edilmiş olan S kutusunda satır ve sütun değerinin kesiştiği noktadaki değer yeni renk değerleri olarak işleme alınmaktadır. Bu işlem her pikselin RGB değerleri için ayrı ayrı uygulanmaktadır. Örneğin, bir pikselin RGB değerlerinin R=59, G=167 ve B=218 olduğunu varsayalım. Hexadecimal karşılıkları R=3B, G=A7 ve B=DA olmaktadır. Şekil 2' de K/DSA ile üretilen olası bir S kutusuna bakıldığında 3.satır B.sütun için yeni R=CB, A.satır 7.sütun için yeni G=76 ve D.satır A.sütun için yeni B=E6 olarak elde edilmektedir. Önerilen yöntemin daha güçlü kılınması için elde edilen yeni RGB değerleri, S kutusu içerisindeki rastgele bir koordinattaki hexadecimal değerle XOR işlemine tabi tutulmaktadır. Rastgele sayı üretimi için Sözde Rastsal Sayı Üreteci (Pseudo Random Number Generator-PRNG) kullanılmaktadır. PRNG, öğeleri arasında kolay kolay ilişki kurulamayacak bir sayı dizisi üreten algoritma türleridir [22]. Bu sayı üretim yöntemlerinin temel amacı aslında belirli bir matematiksel fonksiyona dayanarak bir sayı dizisi üretmektir. Sayı üretimi sırasında kullanılan matematiksel fonksiyon gizlenerek üretilen sayıların tahmin edilmesi engellenmeye çalışılmaktadır. PRNG ile sayı üretiminde bir başlangıç değeri yardımı ile daima aynı sayı dizisi elde edilmektedir. Dolayısı ile yöntemde kullanılan PRNG' ın başlangıç değeri olarak kullanıcı tarafından belirlenen anahtar değeri kullanılmaktadır. PRNG tarafından her RGB değeri için satır ve sütunu temsil etmek üzere iki adet hexadecimal sayı üretilmektedir. Başlangıç değeri kullanıcının gizli anahtarı olduğundan PRNG ile üretilen S kutusu koordinatları daima aynı olacaktır. Farklı bir kullanıcı anahtarı seçildiğinde farklı koordinatlar elde edilecektir. XOR işleminden sonraki yeni RGB değerleri şifrelenmiş görüntünün yeni piksel değerini temsil etmektedir. I şifrelemeden önceki orijinal görüntüyü temsil etmek üzere şifreleme işlemini gerçekleştiren akış diyagramı Şekil 5' de gösterilmektedir.



Şekil 5. Şifreleme işlemi akış diyagramı

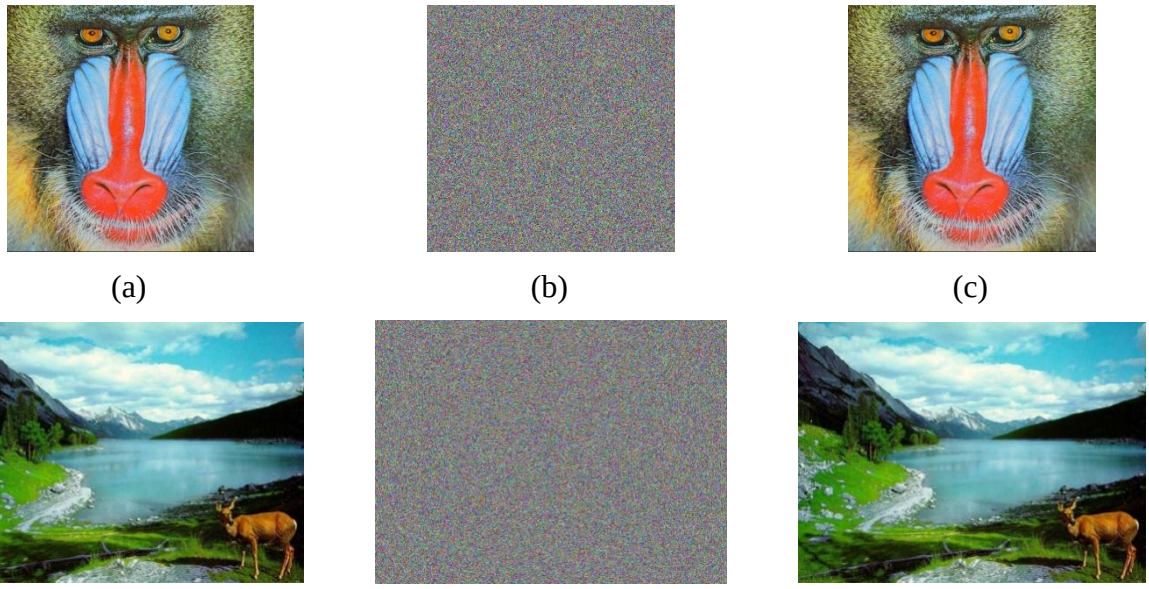
Deşifrelenmiş görüntünün elde edilmesi için kullanıcı tarafından üretilen S kutusundan ve ters S kutusundan faydalanılmaktadır. İlk olarak, şifrelenmiş olan görüntüye ait R, G, B değerleri elde edilmekte ve hexadecimal karşılıkları alınmaktadır.

Kullanıcı anahtarı yardımı kullanılarak ters S kutusunun satır ve sütunu için PRNG yardımıyla rastgele değerler üretilmektedir. Kullanıcı anahtarı değişmediği sürece her zaman aynı rastgele sayılar üretilecektir. Bu işlem her bir R, G, B değeri için ayrı ayrı gerçekleştirilmektedir. S kutusundaki hexadecimal değer ile şifreli görüntüden elde edilen R, G, B değerleri XOR işlemine tabi tutulmaktadır. XOR işleminden sonra elde edilen yeni R,G,B değerlerinin her biri için ters S kutusunda karşılık gelen satır ve sütun değerlerinin kesiştiği noktalar, orijinal görüntünün piksel değerinin elde edilmesini sağlamaktadır. Örneğin, XOR işleminden sonra elde edilen yeni R değerinin AB olduğunu varsayalım. Şekil 4' de verilen ters S kutusunda A.satır ve B.sütuna bakıldığında buna karşılık gelen değerin 6D olduğu görülecektir. Bu işlemler her pikselin XOR işleminden sonraki R,G,B değerlerine uygulanarak devam edildiğinde orijinal görüntünün piksel değerlerine ulaşılmaktadır. I' şifrelenmiş görüntüyü temsil etmek üzere deşifreleme işlemini gösteren akış diyagramı Şekil 6' da gösterilmektedir.



Şekil 6. Deşifreleme akış diyagramı

Önerilen yöntemin "12e4a" kullanıcı şifresi ile 512 × 512 boyutlarında "baboon.bmp" ve 800 × 600 boyutlarıda "manzara.jpg" görüntülerinin şifrelenmesi ve deşifrelenmesinden elde edilen sonuçlar Şekil 7' de gösterilmektedir.



(a) (b) (c)

(d) (e) (f)

Şekil 7. Uygulama sonuçları; a)Orjinal baboon.bmp; b)Şifreli baboon.bmp; c)Deşifreli baboon.bmp; d)Orjinal manzara.jpg; e)Şifreli manzara.jpg; f)Deşifreli manzara.jpg

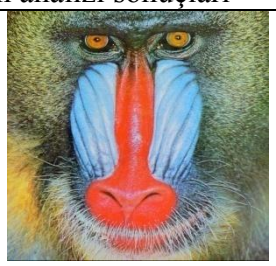
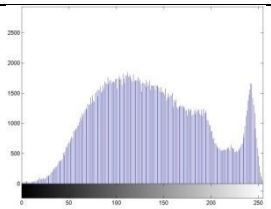
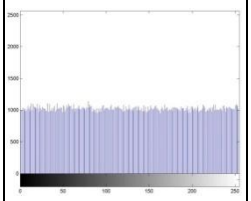
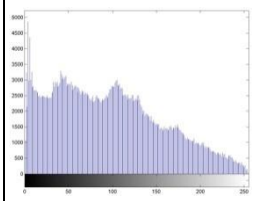
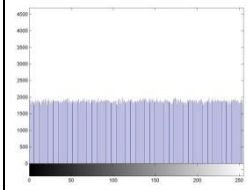
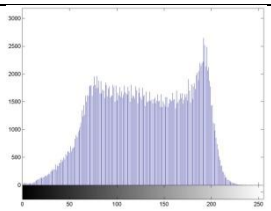
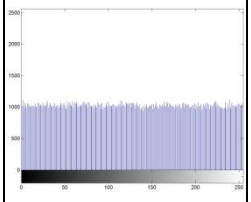
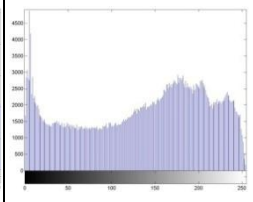
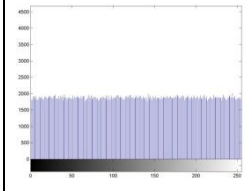
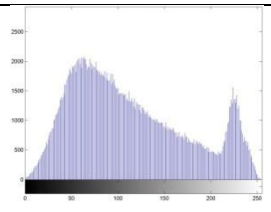
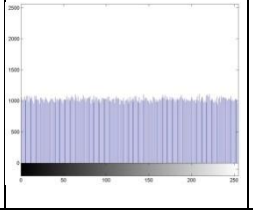
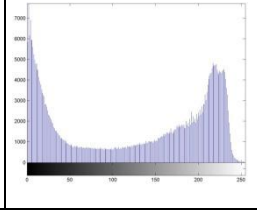
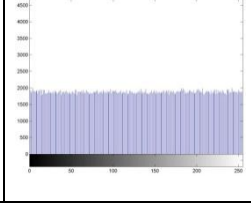
3. Bulgular ve Tartışma

Bu bölümde yukarıda ayrıntıları verilen yöntemin güvenlik analizleri tartışılmaktadır. Bu amaçla histogram, korelasyon ve anahtar uzayı analizleri gerçekleştirilerek elde edilen sonuçlar aşağıda verilmiştir.

3.1. Histogram analizleri

Histogramlar, bir resmin sahip olduğu piksel yoğunluklarının dağılımını gösteren bir grafiktir. Şifreli bir görüntünün çözülebilmesi için saldırgan histogram kullanarak frekans analizi yapmaktadır. Bu türden saldırılar istatistiksel saldırı olarak adlandırılmaktadır. Bu tür saldırıların engellenebilmesi için orjinal görüntünün histogramı ile şifreli görüntü histogramının birbirinden farklı olması gerekir. Özellikle şifreli görüntü histogramının nispeten düz veya istatistiksel olarak tekdüze bir dağılım göstermesi gerekmektedir. Şifreli görüntünün histogramının homojen dağılımı görüntü şifreleme algoritmasının kaliteli olduğunun bir göstergesidir [23]. Tablo 1' de "baboon.bmp" ve "manzara.jpg" görüntülerine ait şifrelemeden önceki ve sonraki histogramlar gösterilmiştir.

Tablo 1. Histogram analizi sonuçları

				
	Şifrelemeden önce	Şifrelemeden sonra	Şifrelemeden önce	Şifrelemeden sonra
Red Histogram				
Green Histogram				
Blue Histogram				

Tablo 1' deki şifreli görüntü histogramlarına dikkat edildiğinde orjinal görüntü histogramından önemli ölçüde farklı ve homojen dağıldığı görülmektedir. Bundan dolayı istatiksel saldırılara karşı dayanıklı ve güvenli bir sonuç elde edildiği söylenebilmektedir.

3.2. Korelasyon analizi

İstatistiksel korelasyon iki rastsal değişken arasındaki doğrusal ilişkinin gücünü belirten bir ölçüdür. n elemanlı bir dizide x ve y rastgele iki değişken olmak üzere korelasyon katsayısı aşağıdaki denklem ile hesaplanabilir [24].

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \tag{2}$$

Buradan;

$$cov(x,y) = \frac{1}{n}\sum_{i=1}^{n}[x_i - E(x)][y_i - E(y)] \tag{3}$$

$$D(x) = \frac{1}{n}\sum_{i=1}^{n}[x_i - E(x)]^2 \tag{4}$$

$$E(x) = \frac{1}{n}\sum_{i=1}^{n}x_i \tag{5}$$

olarak elde edilmektedir. Bu çalışmada, şifrelenmiş görüntüdeki piksellerin korelasyonunun hesaplanması için yatay, dikey ve çapraz komşu pikseller dikkate alınmıştır. Orjinal ve şifreli görüntülerin her biri için her yönde (yatay, dikey ve köşegen) ve birbirlerine komşu olan 2000 adet rastgele piksel seçilmiştir. Korelasyon analizi performansını değerlendirmek için bu işlemler "baboon.bmp" ve "manzara.jpg" görüntüleri üzerinde uygulanmıştır. Her bir R, G, B renk katmanı için elde edilen korelasyon hesaplama sonuçları Tablo 2 ve Tablo 3' de gösterilmektedir.

Tablo 2. "baboon.bmp" korelasyon katsayıları

		Red	**Green**	**Blue**
Orijinal Görüntü	Yatay	0.9231	0.8655	0.9073
	Dikey	0.8660	0.7650	0.8809
	Diagonal	0.8543	0.7348	0.8399
Şifreli Görüntü	Yatay	$-4.9268\text{x}10^{-5}$	-0.0035	$2.2763\text{x}10^{-4}$
	Dikey	-0.0027	-0.0010	0.0012
	Diagonal	-0.0014	-0.0011	-0.0034

Tablo 3. "manzara.jpg" korelasyon katsayıları

		Red	**Green**	**Blue**
Orijinal Görüntü	Yatay	0.9696	0.9791	0.9866
	Dikey	0.9595	0.9720	0.9809
	Diagonal	0.9491	0.9651	0.9764
Şifreli Görüntü	Yatay	$-5.1060\text{x}10^{-5}$	-0.0015	$7.4524\text{x}10^{-4}$
	Dikey	$-6.3353\text{x}10^{-4}$	-0.0012	$6.4401\text{x}10^{-4}$
	Diagonal	$-4.5858\text{x}10^{-4}$	-0.0015	$-8.1701\text{x}10^{-4}$

Yüksek bir korelasyon katsayısı +1 ve -1' e yakın olarak karakterize edilmektedir. Yani korelasyon katsayısının -1 ve +1'e çok yakın olması pikseller arasındaki ilişkinin güçlü olduğu 0' a yakın olması ise pikseller arasındaki ilişkinin zayıf olduğu anlamına gelmektedir. Tablo 2 ve 3' e dikkat edildiğinde orijinal görüntü korelasyon katsayılarının 1' e yakın, buna karşılık şifrelenmiş görüntü korelasyon katsayısının da 0' a çok yakın olduğu görülmektedir. Bu sonuçlar göz önüne alındığında S kutuları kullanarak gerçekleştirilen görüntü şifreleme yönteminin komşu pikseller arasındaki ilişkiyi 0' a yakın hale getirdiği ve başarılı sonuç verdiği söylenebilmektedir.

3.3. Yapısal Benzerlik Testi

Yapısal benzerlik indeksi (Structural Similarity - SSIM) iki görüntü arasındaki benzerliğin ölçülmesi için kullanılan bir yöntemdir. Aynı zamanda orjinal ve işlenmiş iki görüntü arasındaki kalite farkının ölçülebilmesi için de kullanılmaktadır. x orjinal görüntüyü ve y işlenmiş görüntüyü, μ_x ve μ_y, x ve y' nin ortalamalarını, σ_x^2 ve σ_y^2, x ve y' nin varyanslarını, σ_{xy}, x ve y' nin kovaryanslarını, C_1 ve C_2, görüntüleri dengelemek için kullanılan sabit değişkenleri temsil etmek üzere SSIM, Denklem 6 ile elde edilmektedir [25].

$$S(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \tag{6}$$

Burada SSIM değerinin 1' e yakın veya eşit olması orjinal ve işlenmiş görüntünün yapısal olarak birbirine çok benzediği, 0' a eşit veya çok yakın olması ise görüntüler arasındaki yapısal benzerliğin olmadığı veya çok az olduğu anlamına gelmektedir. Tablo 4' de şifrelenmiş ve deşifrelenmiş görüntüler arasındaki yapısal benzerlik testi sonuçları gösterilmiştir.

Tablo 4. Yapısal benzerlik testi sonuçları

Görüntü	**Orjinal ile şifreli görüntü arasındaki benzerlik oranı**	**Orjinal ile deşifreli görüntü arasındaki benzerlik oranı**
baboon.bmp	0.0147	1.0
manzara.jpg	0.0121	1.0

Tablo 4 dikkate alındığında deşifrelenmiş görüntü ile orjinal görüntüler arasında benzerlik oranının %100 olduğu görülmektedir. Buna karşılık orjinal ve şifrelenmiş görüntüler arasındaki benzerlik oranının gözle algılanamayacak kadar düşük olduğu sonucuna varılabilmektedir. Önerilen yöntem, değer dönüşümü ve yer değiştirme özelliklerine sahip olduğundan deşifreleme işleminde herhangi bir piksel kaybının olmadığı görülmektedir.

3.4. Entropi Testi

Entropi, bir sistemdeki rastgelelik ve düzensizlik olarak tanımlanmaktadır. *m* mesajının entropisi denklem (7) ile hesaplanmaktadır.

$$H(m) = \sum_{i=0}^{MxN-1} P(m_i) log_2 \frac{1}{P(m_i)} \tag{7}$$

Burada $P(m_i)$ bir mesajdaki m_i sembollerinin olasılık durumlarını ve $M \times N$ ise toplam sembol sayısını ifade etmektedir. Rastgele bir mesajda ideal entropi değeri 8, rastgelelik oranı daha az olan mesajlarda ise entropi değeri 8’ den daha düşük olmaktadır. Eğer entropi değeri 8’ den çok düşükse güvenliğe karşı bir tehdit olabileceği öngörülebilmektedir [26].

Şifreli resimlerin rastgele piksel değerlerinden oluştuğu düşünüldüğünde ideal entropi değerinin 8 olması beklenmektedir. Entropi testi gri seviye resimler üzerinde uygulanabilmektedir. Renkli resimlerde ise entropi testi RGB kanallarının her biri için ayrı ayrı uygulanmaktadır. Tablo 5' de orijinal, şifrelenmiş ve deşifrelenmiş renkli RGB resimlerin entropi testi sonuçları gösterilmektedir.

Tablo 5. Entropi testi sonuçları

	Orjinal Resmin Entropisi			**Şifreli Resmin Entropisi**			**Deşifreli Resmin Entropisi**		
	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue
baboon.bmp	7.7067	7.4744	7.7522	7.9992	7.9993	7.9992	7.7067	7.4744	7.7522
manzara.jpg	7.8010	7.9290	7.3831	7.9996	7.9996	7.9996	7.8010	7.9290	7.3831

Tablo 5' e dikkat edildiğinde şifrelenmiş resimlere ait entropi değerlerinin 8' e çok yakın olduğu açıkça görülmektedir. Dolayısı ile önerilen yöntemin saldırılara karşı oldukça dayanıklı olduğu söylenebilmektedir. Ayrıca orijinal ve deşifreli resimlerin entropi değerlerinin aynı olması şifreleme ve deşifreleme işlemlerinde herhangi bir veri kaybı olmadığının göstergesidir.

4. Sonuç ve Öneriler

Bu çalışmada, dinamik olarak üretilen S kutuları yardımıyla farklı dosya tipindeki görüntülerin şifrelenmesi ve deşifrelenmesi için kaotik bir yöntem önerilmiştir. S kutularının dinamik olarak üretilmesi kullanıcı anahtarına bağlıdır. Farklı kullanıcı anahtarı kullanıldığında birbirinden farklı S kutuları dinamik olarak elde edilmektedir. Dolayısı ile çok geniş bir anahtar uzayına sahiptir. Şifreleme ve deşifreleme işlemi S kutularına bağlı olduğundan orjinal görüntünün elde edilmesi ancak doğru kullanıcı anahtarının bilinmesi ile mümkün olacaktır. Ayrıca yöntemde kullanılacak olacak PRNG denklemi gizli tutulduğunda orjinal görüntünün elde edilme ihtimali de ciddi oranda azalmaktadır. Şifrelenmiş bir görüntüden orijinal görüntünün tekrar elde edilebilmesi son derece önemlidir. Deneysel sonuçlar göz önüne alındığında önerilen yöntemin herhangi bir veri kaybı olmadan doğru anahtar değeri ile orijinal görüntünün tekrar elde edilmesine olanak sağladığı gözlemlenmiştir. Yapılan tüm deneysel sonuçlardan elde edilen bulgular doğrultusunda önerilen yöntemin görüntülerin şifrelenmesi amacı ile kullanılabileceği mümkün görülmektedir.

Kaynaklar

[1] Sakallı, M. T., Buluş, E., Şahin, A., Büyüksaraçoğlu, F., Buluş, N., "AES S Kutusuna Benzer S Kutuları Üreten Simülatör", 8. Akademik Bilişim Konferansı, 9-11 Şubat 2006, Denizli,Türkiye.

[2] Daemen, J., Rijmen, V., "The design of Rijndael: AES–The advanced encryption standard", Springer, 2002 Ed., Berlin, Germany.

[3] FIPS 197, "Advanced Encryption Standard", Federal Information Processing Standard Publication 197, Washington D.C., USA.

[4] Sankpal, P.R., Vijaya, P.A., "Image Encryption Using Chaotic Maps: A Survey", Fifth International Conference on Signal and Image Processing, 8-10 January 2014, Jeju Island, pp.102-107, DOI: 10.1109/ICSIP.2014.80

[5] Sakallı, M. T., Buluş, E., Şahin, A., Büyüksaraçoğlu, F., "A. Şahin, S-kutularında Doğrusal Eşitlik - Affine Equivalence in S-boxes", IEEE Sinyal işleme ve İletişim Uygulamaları Kurultayı, 17-19 Nisan 2006, Antalya,Türkiye. DOI: 10.1109/SIU.2006.1659838

[6] Güvenoğlu, E., Tüysüz, M.A.A., "Knutt/Durstenfeld Shuffle Algoritması Tabanlı Görüntü Şifreleme Algoritması İçin Bir İyileştirme", IEEE Sinyal işleme ve İletişim Uygulamaları Kurultayı, 16-19 May 2015, Bildiriler Kitabı, Malatya, ss. 1761-1764, DOI:10.1109/SIU.2015.7130194

[7] Abraham, L., Daniel, N., "Secure Image Encryption Algorithms: A Review", International Journal of Scientific & Technology Research, 2(4) (2013) 186-189.

[8] Hussain, I., Shah, T., Gondal, M. A., " An efficient image encryption algorithm based on S_8 S-box transformation and NCA map", Optics Communications, 285(24) (2012) 4887-4890, DOI: 10.1016/j.optcom.2012.06.011

[9] Sreedharan, A., "Wavelet Based Advanced Encryption Standard Algorithm for Image Encryption", International Journal of Engineering Research and General Science, 3(1)(2015) 943-950,

[10] Jolfaei, A., Mirghadri, A. " Image Encryption Using Chaos and Block Cipher", Computer and Information Science, 4(1)(2011) 172-185, DOI: http://dx.doi.org/10.5539/cis.v4n1p172

[11] Tamimi, A.A., Abdalla A.M., "An Image Encryption Algorithm with XOR and S-box", International Conference on Image Processing, Computer Vision, and Pattern Recognition IPCV'15, 27-30 July 2015, Las Vegas, Nevada, USA, pp. 166-169.

[12] Chandrasekaran, J., Subramanyan, B., Raman, G. S., " Ensemble of blowfish With Chaos Based S Box Design for Text and Image Encryption", International Journal of Network Security & Its Applications, 3(4)(2011) 165-173.

[13] Naskar, P.K., Chaudhuri, A., " A Secure Symmetric Image Encryption Based on Bit-wise Operation", International Journal of Image, Graphics and Signal Processing (IJIGSP), 6(2)(2014) 30-38, DOI: 10.5815/ijigsp.2014.02.04

[14] Hussain, I., Shah, T., Gondal, M.A., Mahmood, H., " Efficient method for designing chaotic S-boxes based on generalized Baker's map and TDERC chaotic sequence", Nonlinear Dynamics, 74(1)(2013) 271-275, DOI: 10.1007/s11071-013-0963-z

[15] Gupta, P., Singh, S., Mangal, I., "Image Encryption Based On Arnold Cat Map and S-Box", International Journal of Advanced Research in Computer Science and Software Engineering, 4(8)(2014) 807-812.

[16] Jain, A., Agarwal, P. Jain, R., Singh, V., " Chaotic Image Encryption Technique using S-box based on DNA Approach",International Journal of Computer Applications,92(13)(2014)30-34

[17] Khan, M., Shah, T., Batool, S. I., " Construction of S-box based on chaotic Boolean functions and its application in image encryption", Neural Computing and Applications, (2015) 1-9, DOI: 10.1007/s00521-015-1887-y

[18] Moses, L.E., Oakford R.V., "Tables of Random Permutations", Stanford University Press, ISBN-13: 978-0804701488, 1963.

[19] Durstenfeld, R., "Algorithm 235: Random permutation", Communications of the ACM, 7(7) (1964) 420.

[20] Knuth, D.E., "The Art of Computer Programming", 2th Edition, Addison-Wesley, 1969, 139-140.

[21] Güvenoğlu, E., Esin, E.M., "Knutt/Durstenfeld Shuffle Algoritmasının Resim Şifreleme Amacıyla Kullanılması", Politeknik Dergisi, 12(3) (2009) 151-155.

[22] Büyüksaraçoğlu, F., Buluş, E., "Sözde Rastsal Sayı Üretiminin Kriptografik Açıdan İncelenmesi", IV.İletişim Teknolojileri Ulusal Sempozyumu, 15-16 Ekim 2009, Adana, Bildiriler Kitabı, ss. 125-130.

[23] Naveenkumar, S.K., Panduranga, H.T., "Triple image encryption based on integer transform and chaotic map", International Conference on Optical Imaging Sensor and Security (ICOSS), 2-3 July 2013, Tamil Nadu, India, pp. 1-6. DOI: 10.1109/ICOISS.2013.6678416

[24] Shannon, C.E., "A Mathematical Theory of Communication", The Bell System Technical Journal, (1948) 27, pp. 379–423, 623–656.

[25] Wang, Z., Bovik, A. C., Sheikh, H. R., Simoncelli, E. P., "Image quality assessment: from error visibility to structural similarity", IEEE Transactions on Image Processing, 13(4) (2004) 600-612, DOI: 10.1109/TIP.2003.819861

[26] Munir, R., "Security analysis of selective image encryption algorithm based on chaos and CBC-like mode", 7th International Conference on Telecommunication Systems, Services, and Applications (TSSA), 30-31 October 2012, Bali, Indonesia, pp. 142-146. DOI:10.1109/TSSA.2012.6366039