

# Yer Değiştirme ve Değer Dönüştürme Özelliğine Sahip

## Görüntü Şifreleme Algoritmalarının Analizi

Erdal Güvenoğlu<sup>1</sup>, Nursen Suçsuz<sup>2</sup>

<sup>1</sup> Maltepe Üniversitesi, Bilgisayar Mühendisliği Bölümü, 34857, İstanbul

<sup>2</sup> Trakya Üniversitesi, Bilgisayar Mühendisliği Bölümü, 22050, Edirne

erdalg@maltepe.edu.tr, nursen@trakya.edu.tr

**Özet:** Gelişen teknoloji karşısında bilgisayar ağlarının en önemli konularından biri de son derece önemli olan bilgilerin, yetkisiz kişilerin eline geçmesini engellemek olmaktadır. Bu nedenlerden dolayı geçmişten günümüze çok çeşitli şifreleme yöntemleri geliştirilmiştir. Bu çalışmada dijital dünyada çok kullanılan yer değiştirme ve değer dönüştürerek şifreleme özelliği olan görüntü şifreleme algoritmalarının analizine yer verilmektedir.

**Anahtar Kelimeler:** şifreleme, görüntü şifreleme, görüntü işleme, güvenlik.

### Analysing Image Encryption Algorithms That Have The Properties Of Replacement And Value Transformation

**Abstract:** In view of developing technology, one of the most important subjects of the computer networks is to avert unauthorized accesses to the extremely important information. Therefore various encryption techniques have been developed. In this study analysis of image encryption algorithms which has replacing and value transforming properties have been mentioned. These algorithms are widely used in digital world applications.

**Keywords:** Cryptography, Image encryption, Image processing, Security.

#### 1. Giriş

Görüntü dosyaları metin dosyalarından farklıdır. Geleneksel metin şifreleme sistemleri resimler için kullanılabilirse de, iki nedenden dolayı bu kötü bir fikir olmaktadır. Birincisi, resim yazı verilerinden çok daha büyüktür. Bu nedenle geleneksel algoritmalar resimleri şifrelemek için yavaş kalmaktadırlar. Diğer problem ise, yazı verisinin şifresi çözüldüğünde aynen geri gelmesi gerekli iken, resim dosyalarında böyle bir zorunluluk yoktur. İnsan doğası nedeniyle, şifresi çözülmüş bir resim verisinin tarz olarak gerçek resim ile aynı olması gerekmemektedir ve fark edilemeyecek kadar değişiklikler olabilmektedir.

- Değer dönüşümü
- Yerel permütasyon
- Değer dönüşümü ve yerel permütasyon kombinasyonları.

Değer dönüşümü, orjinal sinyalin veri değerinin, algoritmadaki işleme tabi tutulmasından sonra aldığı yeni değer olarak ifade edilmektedir. Yerel permütasyon algoritmaları, orjinal verinin pozisyonlarının yer değiştirmesini sağlamaktadır. Diğer özellik ise, hem yer değiştirme hemde değer dönüşümlerinin ikisinin kullanılması ile gerçekleştirilmektedir.

#### 2. Karmaşık Resim Şifreleme Algoritması

Görüntü şifreleme algoritmaları üç temel fikre dayanmaktadır.

Chang ve Chen tarafından sunulan karmaşık bir sisteme dayalı yeni bir resim şifreleme yöntemi

midir [1]. Karmaşık şifreleme algoritması, yaygın olarak kullanılan ve yer değiştirme özelliğine sahip bir görüntü şifreleme algoritmasıdır. Algoritmanın uygulanmasında herhangi bir veri kaybı olmamaktadır. Bunun nedeni pikselin değerinin değilde sadece bulunduğu pikselin yerinin değişmesinden kaynaklanmaktadır.

fj MxN büyüklüğündeki bir resmi gösterebilir.  $f(x, y)$ ,  $0 < x < M-1$ ,  $0 < y < N-1$ , f resminin (x, y) pozisyonundaki koordinatlarını ve gri resim seviyesini göstermektedir, f ise dönüştürülen resmi ifade etmektedir. Algoritmanın tanımı aşağıdaki gibidir.

**Tanım 1:**  $ROLR_{J, i}^p : f \rightarrow f$  eğer  $i \neq 0$  ise f resmindeki i.satırı ( $0 < i < M-1$ ), p piksel sola,  $i=1$  ise p piksel sağa döndürmek için tanımlanmıştır.

**Tanım 2:**  $ROUD_{J, j}^p : f \rightarrow f$  eğer  $j \neq 0$  ise f resmindeki j. sütun ( $0 < j < N-1$ ), p piksel yukarıya,  $j=1$  ise p piksel aşağıya döndürmek için tanımlanmıştır.

**Tanım 3:**  $ROUR_{f, k}^p : f \rightarrow f$  f resmindeki (x, y) pozisyonundaki pikselleri döndürmek için tanımlanmıştır, öyle ki;  $x + y = k$ ,  $0 < k < M + N - 2$ , eğer  $k=0$  ise aşağı-sol yönünde p piksel,  $k=1$  ise yukarı-sağ yönünde p piksel döndürmek için tanımlanmıştır.

**Tanım 4:**  $ROUL_{f, k}^p : f \rightarrow f$  f resmindeki (x, y) pozisyonundaki pikselleri döndürmek için tanımlanmıştır, öyle ki;  $x - y = k$ ,  $-(N - 1) < k < M - 1$ , eğer  $k=0$  ise yukarı-sol yönünde p piksel,  $k=1$  ise aşağı-sağ yönünde p piksel döndürmek için tanımlanmıştır[1].

Örneğin 5x7 boyutundaki aşağıda verilen resmi ele alalım.

$$ROLR^{22}(f), ROUR^{12}(f) \text{ ve } ROUL^2_0(f)$$

işlemlerinin sonuçları sırasıyla şekil 2'de gösterilmektedir [3].

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35

a) Orjinal Resim

1	2	3	4	5	6	7
8	9	10	11	12	13	14
20	21	15	16	17	18	19
22	23	24	25	26	27	28
29	30	31	32	33	34	35

b) Sağa – Sola Öteleme

1	2	3	4	5	18	7
8	9	10	11	24	13	14
15	16	17	30	19	20	21
22	23	6	25	26	27	28
29	12	31	32	33	34	35

c) Sola Aşağı – Yukarı Öteleme

1	2	19	4	5	6	7
8	9	10	27	12	13	14
15	16	17	18	35	20	21
22	23	24	25	26	3	28
29	30	31	32	33	34	11

d) Sağa Aşağı – Yukarı Öteleme

**Şekil 2.** Karmaşık resim şifreleme algoritmasının matrislerde gösterilmesi

### 3. Ayna Benzeri Resim Şifreleme Algoritması

Jiun- Guo ve Jui-Cheng Yen tarafından sunulan etkili bir ayna benzeri görüntü şifreleme algoritmasıdır [2]. Karmaşık bir sistemden üretilen ikili bir diziye bağlı olarak resmin pikselleri karıştırılmaktadır. Bu yöntem yer değiştirme özelliğine sahip bir resim şifreleme algoritmasıdır.

f, MxN büyüklüğünde bir resmi gösterebilir, ve  $f(x,y)$ ,  $0 < x < M-1$ ,  $0 < y < N-1$ , f resminin (x,y) koordinatındaki gri seviyesini göstermektedir.

Bu algoritma yedi adımdan oluşmakta ve belli pozisyonlardaki pikseller karşılıklı yer değiştirmektedirler.

**Adım 1:** Bir 1-D kaotik sistem ve başlangıç noktası  $x(0)$  ve  $k=0$  belirlenir.

**Adım 2:** Kaotik bir sistem için karmaşık bir dizi üretilir.

**Adım 3:** Kaotik sistemden binary bir dizi üretilir. Adım 4,5,6,7: ikili diziye göre yer değiştirme fonksiyonları ile görüntü pikselleri yeniden düzenlenir.

**Adım 4:**

```
For i= 0: M/2 - 1
For j = 0: N/2 - 1
  If b(k) = 1
    yer değiştir f(i,j) ve f(i+M/2, j+N/2);
  End
  k = k+1;
end
end
For i=M/2 : M-1
For j = 0 : N/2- 1
  If b(k) = 1
    yer değiştir f(i,j) ve f(i-M/2, j+N/2);
  End
  k = k+1;
end
end
```

**Adım 5:**

```
For i=0 : M/2-1
For j = 0 : N- 1
  If b(k) = 1
    yer değiştir f(i,j) ve f(i+M/2, j);
  End
  k = k+1;
end
end
```

**Adım 6:**

```
For i=0 : M-1
For j = 0 : N/2- 1
  If b(k) = 1
    yer değiştir f(i,j) ve f(i, j+N/2);
  End
  k = k+1;
end end
```

**Adım 7:**

```
For i=0 : M-1
For j = 0 : N/4- 1
  If b(k) = 1
    yer değiştir f(i,j) ve f(i, j+N/4);
  End
  k = k+1;
end
end
For i=0 : M-1
For j = N/2 : (3/4)xN- 1
  If b(k) = 1
    yer değiştir f(i,j) ve f(i, j+N/4);
  End
  k = k+1;
end
end
```

**Adım 8:** Algoritmayı durdur.

Şifre çözme işlemi için sadece 4 ve 7. adımları tersten izlemek gerekmektedir. Aynı karmaşık dizi vasıtasıyla pikseller üzerinde aynı yer değiştirme işlemi iki defa uygulanırsa orjinal resim elde edilmektedir [2].

#### 4. Brie Algoritması

Bu yeni bir resim şifreleme algoritması olması ile birlikte, karmaşık resim şifreleme sistemini kullanan bir resim şifreleme algoritmasıdır. Karmaşık bir sistemden bit kaydırmalı bir fonksiyon ve ikili bir dizi tanımlanmaktadır ve resimde her bir piksel gri resim pikseline dönüştürülmektedir.

Bu sistem yapısının uygulanması, mimari yapısı nedeni ile düşük donanım karmaşıklığı ve yüksek hesaplama hızından dolayı da kolay bir yöntemdir. Bu algoritma, bit ötelemesinden dolayı değer dönüşümü ve kendi içerisinde yerel permütasyon özelliğini kullanmaktadır.

$f$ ,  $M \times N$  boyutlarında bir resmi göstermek üzere,  $f(x,y)$ ,  $0 < x < M-1$ ,  $0 < y < N-1$  ve  $(x,y)$  koordinatları  $f$  resminin gri seviyesini göstermektedir ve  $G = \{0, 1, 2, 3, \dots, 255\}$  gri resim dizisi olarak tanımlanmaktadır.

**Tanım 1:**  $ROLR_p^q : G \rightarrow G$  ikili gösterimin

her bir dönüşümlü biti olmak üzere,  $x \in G$  için eğer  $p=0$  ise  $q$  bit küçük seviyeli bitten yüksek seviyeli bite,  $p=1$  ise yüksek seviyeli bitten düşük seviyeli bite doğru bir bit öteleme işlemi yapılmaktadır. Diğer bir deyişle;

$$ROLR_p^q(x = b_7b_6b_5b_4b_3b_2b_1b_0) = \begin{cases} \sum_{i=0}^7 b_i x 2^{(i-q+8) \bmod 8} & p = 0 \\ \sum_{i=0}^7 b_i x 2^{(i+q) \bmod 8} & p = 1 \end{cases}$$

şeklinde ifade edilmektedir [4]. Algoritmanın tanımı şu şekildedir.

**Adım 1:**  $M, N, a$  ve  $P$  parametreleri belirlenir.

**Adım 2:** Karmaşık bir sistem ve onun başlangıç değeri  $x(0)$  tanımlanır.

**Adım 3:** Kaotik bir sistemden  $x(0), x(1), x(2), \dots$  dizisi üretilir.

**Adım 4:**  $x(0), x(1), x(2), b(0), b(1), b(2), \dots$  bit dizisi üretilir.

**Adım 5:**

For  $x: 0$  To  $(M-1)$  DO For  $y: 0$  TO  $(N-1)$  DO

$p = b(N \times (x+y))$ ;

$q = a + P * b(N \times (x+y+1))$ ;  $f'(x, y) = ROLR_p^q(f(x, y))$ ;

**Adım 6:** Algoritmayı durdur [4].

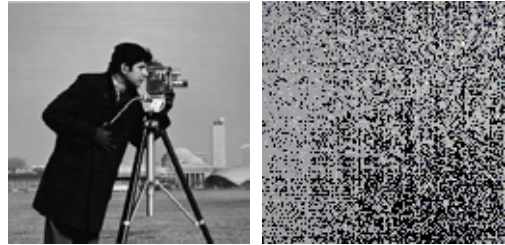
## 5. Tartışma

Yaygın olarak kullanılan karmaşık resim şifreleme algoritmasının temel avantajı, her bir pikselin, önceden tanımlanmış adım sayısına göre resmin karmaşıklığının artmasıdır. Diğer yandan insan doğası gereği, adım sayısı ne kadar az olursa şifrelenmek istenen resmin göz tarafından algılanması da kolay olacaktır.

Ayna benzeri resim şifreleme algoritmasında, her ne kadar yapı olarak karmaşık şifreleme algoritmasına benzese de farklı olarak kendi içerisinde yer değiştirme işlemi önceden tanımlanmış olan çeşitli piksel blokları arasında yapmaktadır. Algoritma yapısı bilindiğinden yer değiştirme işleminin hangi bloklarda yapıldığı da bilinebilmektedir.

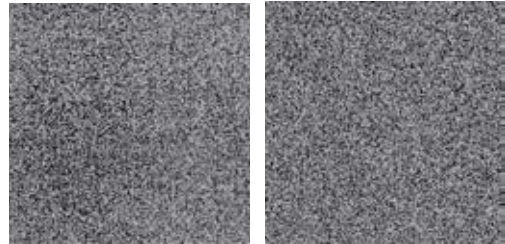
Bit ötelemeli şifreleme algoritmasında, karmaşık ve ayna benzeri şifreleme algoritmalarına karşılık piksellerin yerleri değiştirilmeyip, bulunduğu piksel koordinatında en düşük öncelikli bitten en yüksek öncelikli bite veya en yüksek öncelikli bitten en düşük öncelikli bite doğru bir yer değiştirme dolayısıyla da değer dönüştürme işlemlerini gerçekleştirmektedir. Mevcut piksellerin en düşük öncelikli bitlerine bakılıp en yüksek öncelikli bite veya en düşük öncelikli bite doğru bir öteleme yapılmaktadır.

Bu çalışmada anlatılan algoritmaların, olumlu tarafları birleştirilerek resimlerin mümkün olduğunca anlaşılmasının ve çözümlerinin zorlaştırılması sağlanmaktadır.



a. Orjinal resim

b. 4 Ötelemeli



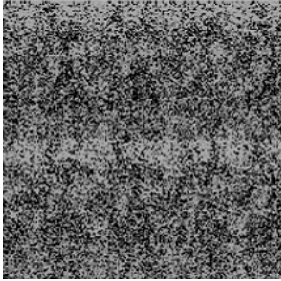
c. 8 Ötelemeli

d. 16 Ötelemeli

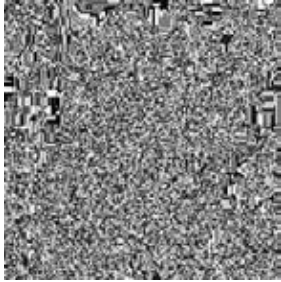
**Şekil 3.** Karmaşık resim şifreleme algoritmasının sonuçları

Sonuçları göstermek üzere Şekil 3 de verilen 247 x 247 piksel boyutunda “cameraman.tif” resmi karmaşık resim şifreleme algoritması için kullanılmıştır.

Ayna benzeri ve bit ötelemeli resim şifreleme algoritmaları içinde Şekil 3-a da gösterilen “cameraman.tif” resmi kullanılmıştır. Şekil 4’te ayna benzeri resim şifreleme algoritması ve Şekil 5’te de bit ötelemeli resim şifreleme algoritması ile elde edilen görüntüler sırasıyla verilmektedir.



Şekil 4. Ayna benzeri resim şifreleme algoritması ile şifrelenmiş resim



Şekil 5. Bit ötelemeli resim şifreleme algoritması ile şifrelenmiş resim

Görüldüğü gibi, Şekil 3-a da ki orijinal resme şifreleme algoritmaları uygulandığında Şekil 3-b de bir nesnenin olduğu algılanabilmektedir. Fakat öteleme sayısı arttıkça bu daha karmaşık gözle algılanamaz bir hale gelmektedir. Ayna benzeri ve bit ötelemeli resim şifreleme algoritmalarında ise resimlerin algılanması daha da güç hale gelmiştir.

## 6. Sonuç

Bu çalışmada, dijital dünyada kullanım oranı hızla artan resimlerin güvenliğinin sağlanması için yöntemler anlatıldı. Bu algoritmalarla çeşitli resimler üzerinde deneyler yapıldı. Deneyler sonucunda, algoritmaların avantaj ve dezavantajları belirlendi, öteleme sayısı arttıkça karmaşık şifreleme algoritmasının ve değer dönüşümü ile mevcut piksel içinde yer değiştirme özelliğine sahip bit ötelemeli resim algoritması ile şifrelenmiş resim şifreleme algoritmalarının daha güvenli olduğu görüldü.

## 7. Kaynaklar

- [1] CHANG C.C., Hwang M.S., Chen T.S., 2001, A new encryption algorithm for image cryptosystems, The Journal of Systems and Software
- [2] GUO J.I., Yen J.C., 1999, A new mirror-like image encryption algorithm and its VLSI architecture, Department of Electronics Engineering National Lien-Ho College of Technology and Commerce
- [3] ÖZTÜRK İ, Soğukpınar İ, 2004. Analysis and Comparison of Image Encryption Algorithms, IIIT Volume 1 Number 2 ISSN:1305 - 239X.
- [4] YEN J.C, Guo J.I,1999, A new image encryption algorithm and its VLSI architecture, IEEE