# İkili İmgeler için Kaos Tabanlı Yeni bir Steganografik Yöntem

# A New Steganographic Method Based on Chaos for Binary Images

Turker TUNCER
Firat University, Technology Faculty, Digital Forensics Engineering, Elazig, Turkey
turkertuncer@firat.edu.tr

## Öz

*İkili imgelere veri gizlemek gri seviyeli ve renkli imgelere ver gizlemekten daha zor bir işlemdir çünkü ikili imgelerin piksel değerleri 0 ve 1'dir. Bundan dolayı gri ve renkli imgeler için önerilen Steganografik yöntemler ikili imgeler için kullanılamamaktadır ancak ikili imgeler için önerilen Steganografik yöntemler gri ve renkli imgeler için kullanılabilmektedir. Bu makalede ikili imgeler için kaos tabanlı yeni bir Steganografik yöntem önerilmiştir. Önerilen yöntem blok tabanlıdır ve 2 x 2, 3 x 3 veya M x N boyutunda örtüşmeyen bloklar kullanılabilmektedir. Kaotik haritalardan olan lojistik harita kullanılarak gizli verinin bloğun hangi noktasına gömüleceği tespit edilmektedir ve böylece önerilen Steganografik yöntemin gizliliği sağlanmaktadır. Deneysel sonuçlarda, önerilen yöntemin veri gizleme kapasitesi, görsel kalitesi, gizliliği ve çalışma zamanı ölçülmüştür. Elde edilen sonuçlar, önerilen yöntemin başarılı olduğunu göstermektedir.*

***Anahtar Kelimeler*** *— İkili imgeler, Steganografi, Kaotik haritalar, Lojistik Harita, Bilgi Güvenliği*

## Abstract

*Data hiding for binary images is harder than data hiding for grayscale and color images because the pixel values of binary image are 0 and 1. Thus, steganographic methods which are used for grayscale and color images cannot implement to binary images but binary image steganographic methods can be implemented to grayscale and color images.*

*In this paper, we proposed a new steganographic method based chaos for binary images. The proposed method is block based and 2 x 2, 3 x 3 or M x N sized non overlapping subblocks are used to data hiding. We used logistic map to determine indices of data hiding. The logistic map supported privacy of the proposed method. The payload capacity, visual quality, privacy and execution time are measured in the experimental results. The experimental results showed that, the proposed method is successful.*

***Keywords*** *— Binary images, Steganography, Chaotic map, Logistic map, Information security.*

Gönderim ve kabul tarihi : 11.06.2016 - 01.06.2017

## 1 Giriş

Veriyi yetkisiz erişimlerden korumak bilgi güvenliğinin en temel amaçlarından birisidir [1]. İnternet kullanımının taşınabilir hale gelmesiyle birlikte kişisel veriler hızlı bir şekilde sayısal ortama aktarılmaya başlamıştır. Sayısal ortamda depolanan ve paylaşılan veriler siber uzayı oluşturmaktadır. Siber uzayda bilgi paylaşmak ve diğer bilgilere erişmenin kolaylaşmasıyla birlikte bilgi güvenliğinin önemi artmıştır. Şifreleme, steganografi ve sayısal damgalama bilgi güvenliğini sağlamak için en sık kullanılan yöntemlerdendir.

Şifreleme yöntemleri, veri gizliliğini sağlamak için mesajın içeriği değiştirilir. Şifreleme biliminde simetrik güven modeli, asimetrik güven modeli ve protokoller kullanılarak bilgi güvenliği sağlanmaktadır. Sayısal damgalama yöntemleri kullanılarak telif hakkı koruma ve kimlik doğrulama gibi işlemler gerçekleştirilmektedir. Sayısal damgalama görünür ve görünmez olarak ikiye ayrılmaktadır. Görünmez damgalar oluşturmak için genellikle veri gizleme teknikleri kullanılmaktadır. Steganografi ise güvenilir olmayan bir veri iletim

hattında güvenilir kanallar açmak için kullanılan yöntemler topluluğudur.

Steganografide temel amaç gizli mesajı örtü nesnesi içerisine fark edilmeyecek şekilde gizlenmesidir. Veri gizlenmiş sinyale stego-sinyal denilmektedir. Steganografide temel amaç, güvenilir olmayan bir veri iletim hattında güvenilir bir kanal açarak, saldırganların dikkatini çekmeden mesajı alıcı tarafa göndermek ve multimedya verilerinin telif haklarının korunmasını sağlamaktır [2-7]. Steganografinin temel bileşenleri örtü nesnesi, gizli mesaj, veri gizleme fonksiyonu, steganografi anahtarı, stego-nesne ve veri çıkarma fonksiyonudur. Veri gizleme fonksiyonu örtü nesnede gizli mesajın nasıl gizleneceğini, stego anahtarı ise gizli mesajın örtü nesnesinin hangi konumlarına gizleneceğini belirlemektedir. Veri gizleme fonksiyonu ve veri gizleme anahtarı kullanılarak gizli mesaj örtü nesnesine gömülür. İçerisine veri gizlenmiş nesne veri gizlenmiş nesne olarak adlandırılır. Veri gizlenmiş nesnede gizli mesajı çıkarabilmek için ise veri çıkarma fonksiyonu ve stego anahtar kullanılmaktadır [8].

Literatürde birçok veri gizleme algoritması önerilmiştir. Önerilen algoritmalar genellikle gri seviyeli veya renkli imgeleri kullanmaktadır. Gri seviyeli imgeler için önerilen veri gizleme algoritmaları renkli imgeler için de rahatlıkla kullanılmaktadır. Ancak ikili imgeler için bu durum söz konusu değildir. İkili imgelere veri gizlemek için daha farklı yöntemlerin kullanılması gerekmektedir. İkili imgeler için önerilen çalışmalardan bazıları aşağıdaki gibi verilmiştir.

Matsui ve Tanaka titrek fax imgelerine veri gizlemek için bit değiştirme tabanlı yeni bir metot önermiştir [9]. Low ve ark. satır aralığı ve karakter boşluklarını değiştirerek ikili imgeler için veri gizleme metodu önermiştir ve bu metot metin imgelerinde kullanılmıştır [10,11]. Bunların yanı sıra tüm ikili imgeler için genel veri gizleme metotları da önerilmiştir. Koach ve Zao ikili imgelere veri gizlemek için blok tabanlı yeni bir metot önermiştir ve bu metot genel ikili imgelere veri gizlemek için kullanmıştır [12]. Ancak bu metotla yapılan veri gizlemelerde problemler meydana gelmektedir. Bu problemlerin üstesinden gelebilmek için Wu ve ark. imgenin belirli karakteristik özellik gösteren örüntülerine veri gizlemeyi önermiştir [13]. Liu ve ark. 2 x 2 boyutunda bloklar kullanarak ikili imgelere veri gizleyen yeni bir metot önermiştir [14]. Wu ve Liu örtü imgesinin piksellerine karıştırma algoritması uygulayarak blok tabanlı veri gizleme metodu önermiştir. Bu metot yüksek görsel kaliteye sahiptir ve gizlenen veri gözle fark edilmez [15]. Venkatesan ve ark. blokların paritesini kullanarak yeni bir veri gizleme metodu önermiştir. Önerilen bu metotla blok başına bir bit veri gizlenmiştir [16]. Yung ve Yoo anahtar kimlik doğrulaması için blok maske tabanlı veri gizleme algoritması sunmuştur. Kenar uyarlamalı olan bu veri gizleme algoritmasında Canny kenar çıkarma algoritmasının maskesi kullanılmıştır ve bu metotla yüksek kapasitelerde yüksek görsel kalite değerleri elde edilmiştir [17]. Jung ve Yoo ikili imgelere veri gizlemek için yeni bir algoritma sunmuştur. Yapılan çalışmada ikili imgelere veri gizlemenin diğer imgelere veri gizlemeden daha zor olduğu ve bundan dolayı ikili imgelerde kalite kontrolünün yapılması gerekliliği ortaya konmuştur. Önerilen metot blok tabanlı bir veri gizleme metodudur ve kalite kontrolünün yapılabilmesi için parite biti kullanılmıştır [18]. Wang ve ark. ikili imgeler için yüksek kapasiteli bir veri gizleme algoritması önermiştir. Sunulan algoritma blok örüntüleri kullanmaktadır. Kullanılan bloklar 2 x 2 boyutundadır. Deneysel sonuçlar, önerilen algoritmanın literatürde daha önce önerilen algoritmalarla karşılaştırılmış ve başarılı sonuçlar elde edilmiştir [19]. Feng ve ark. [20] güvenilir bir imge steganografi algoritması önermişlerdir. Önerilen yöntemi test edebilmek için steganaliz yöntemleri kullanılmaktadır. Görsel kaliteyi arttırmak için dokusal alanlara veri gizlenmiştir. Bu yöntemin en büyük dezavantajı, veri gizleme kapasitesinin düşük olmasıdır. Ayrıca uzaysal alanda kaotik steganografiyi kullanan ve euler tabanlı kaotik steganografi yöntemleri de literatürde bulunmaktadır [21,22].

Bu çalışmada, ikili imgeler için kaos tabanlı yeni bir steganografi yöntemi geliştirilmiştir. Geliştirilen yöntemde 2 x 2, 3 x 3 veya M x N boyutunda alt bloklar kullanılarak veri gizleme işlemi gerçekleştirilir. Kaotik haritalardan olan lojistik harita kullanılarak veri gizleme anahtarı oluşturulur ve gizli veri stego anahtarının gösterdiği yere gömülmektedir. Bu çalışmada anahtarı üretmek için lojistik harita kullanılmıştır. Anahtar üretebilmek

için diğer kaotik haritalardan da faydalanılabilir. Önerilen metot bu yönüyle genişletilebilir bir yöntemdir. Önerilen yöntem kullanılarak her bir bloğa 1 bit veri gizlenmektedir. Veri çıkarma safhasında ise stego anahtar alıcı tarafa yollanır. Stego anahtar kullanılarak gizli veri elde edilir. Önerilen çalışmanın karakteristiği aşağıdaki gibi verilmiştir.

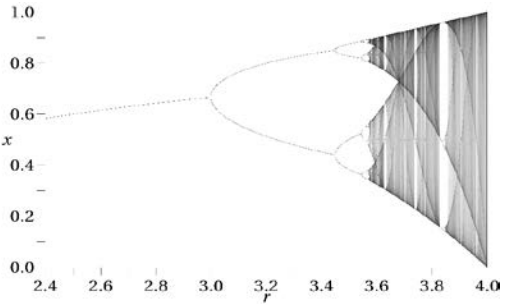
- Önerilen yöntem kaotik harita sayesinden doğrusal olmayan bir özelliğe sahiptir.
- Önerilen yöntem ile farklı birçok alt blok kullanılarak veri gizleme ve veri çıkarma işlemi yapılabilmektedir.
- Veri gizlenecek bloğu seçim kuralları kullanıcıya tarafından değiştirilebilir. Bu makalede farklı piksel yapılarına sahip bloklara veri gizleme kuralı tanımlanmıştır.
- Önerilen yöntem yüksek kapasite ve yüksek görsel kalite parametrelerini sağlamaktadır.
- Önerilen yöntemin veri gizleme ve veri çıkarma algoritmaları basittir. Bu yönüyle önerilen yöntem pratikte de uygulanabilir.
- Önerilen yöntem kullanılarak sadece ikili imgelere veri gizleme yapılmamaktadır. Gri seviyeli veya renkli imgelerin bit düzlemlerine önerilen yöntem kullanılarak veri gizlenebilmektedir.
- Bu çalışmanın 2. Bölümünde lojistik harita, 3. bölümde önerilen yöntem, 4. bölümde deneysel sonuçlar 5. bölümde ise sonuç ve önerilere yer verilmiştir.

## 2 Lojistik Harita

Kaos, doğrusal olmayan denklemleri tanımlayan matematiksel bir konudur. Bilgi güvenliğinde anahtar üretilmesi, karıştırma vb. konuda kaos dinamiklerinde ve kaotik haritalardan faydalanılmaktadır [23]. Literatürde birçok kaotik harita önerilmiştir ancak bunlardan en çok kullanılanlardan birisi ise lojistik haritadır. Lojistik harita kapalı bir çevredeki popülasyonu modellemek için önerilmiştir. Bu harita bir boyutludur [24]. Eşitlik 1' de lojistik haritanın eşitliği verilmiştir.

$$x_{n+1} = r x_n (1 - x_n) \qquad (1)$$

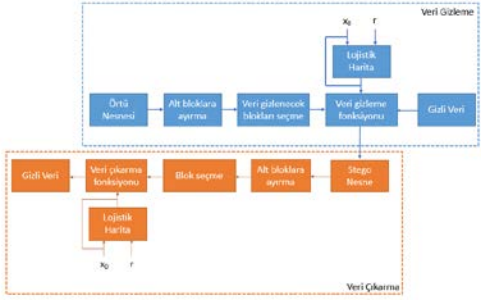
Şekil 1'de lojistik haritanın çatallanma diyagramı verilmiştir.




**Şekil 1.** Lojistik haritanın çatallanma diyagramı

## 3 Önerilen metot

Önerilen metot iki aşamadan oluşmaktadır. Bu aşamalar veri gizleme ve veri çıkarma aşamalarıdır. Önerilen steganografik yöntemin blok diyagramı Şekil 2'de verilmiştir. Veri gizlemek için örtüşmeyen alt bloklar kullanılmaktadır. Veri gizlenecek alt bloğu seçmek için ise lojistik harita kullanılarak elde edilen stego anahtar kullanılmaktadır. Eğer kullanılan alt bloğun tüm elemanları 0 veya 1'lerden oluşuyorsa o bloğa veri gizlenememektedir. Veri gizleme işleminin adımları aşağıdaki gibidir.




**Şekil 2.** Önerilen yöntemin blok diyagramı

**Adım 1:** İkili imge M x N boyutundaki örtüşmeyen bloklara ayrılır.

**Adım 2:** Tohum değerlerini ($r, x_0$) kullanarak $[0, b^2)$ arasında tamsayılar üretmek için eşitlik 1'i kullan.

**Adım 3:** Eşitlik 2 ve 3'ü kullanarak alt blokta veri gizlenecek satır ve sütun indislerini belirle

$$satir = \left\lfloor \frac{x_i}{b} \right\rfloor \qquad (1)$$

$$sutun = x_i \ (mod\ b) \qquad (2)$$

x lojistik harita kullanılarak rastgele üretilen sayı dizisi. Bu çalışmada x anahtar olarak kullanılmaktadır. b alt bloğun genişliğini veya yüksekliğini ifade etmektedir. Bu makalede alt blok olarak kare matrisler kullanılmıştır. Ancak alt blok olarak dikdörtgen matrislerde kullanılabilir.

**Adım 4:** Eğer kaotik anahtarla gösterilen pikselin değeri 0 ve gizli veri 1 ise anahtarın gösterdiği piksel 1 değerini alır. Eğer kaotik anahtarla gösterilen pikselin değerin 1 ve gizli veri 0 ise anahtarın gösterdiği piksel 0 değerini alır.

**Adım 5:** Veri gizleme işleminin ardından alt bloğun tüm değerleri 0 değerini alırsa stego anahtarın göstermediği piksellerden herhangi birine 1 değeri verilir. Eğer tüm değerler 1 değerini alırsa stego anahtarın göstermediği herhangi bir piksele 0 değeri verilir.

Bu adımın en büyük amacı; herhangi bir harita kullanmadan gizli veriyi kayıpsız bir şekilde elde edebilmektir.

**Adım 6:** Gizli veri boyutunca Adım 4-5 tekrar eder.

Veri çıkarma işleminde, lojistik haritanın tohum değerleri alıcı tarafa gönderilir. Alıcı taraf tohum değerlerini kullanarak gizli veri boyutunda ve blok genişliğinde olan stego anahtarı üretir. Stego imge alt bloklara ayrılır ve tüm değerleri 0 ve 1 olmayan bloklar veri çıkarılacak bloklar olarak seçilir. Veri çıkarma işleminin adımları aşağıdaki gibidir.

**Adım 1:** Stego imge alt bloklara ayrılır.

**Adım 2:** Tohum değerleri ve lojistik harita kullanılarak stego anahtar üretilir.

**Adım 3:** Veri çıkarılacak bloklar seçilir.

**Adım 4:** Stego anahtarın indislerini elde edebilmek için Eşitlik 2 ve 3 kullanılır.

**Adım 5:** İndisler kullanılarak gizli veri elde edilir.

*Kapasite:* Önerilen yöntemin veri gizleme kapasitesi kullanılan alt bloğun boyutu ve örtü imgenin yapısına bağlıdır. İdeal şartlarda en yüksek kapasite $\left\lfloor \frac{W}{M} \right\rfloor x \left\lfloor \frac{H}{N} \right\rfloor$ bit iken, bu değer imgenin yapısına göre değişmektedir.

**Adım 6:** Gizli veri boyutunca Adım 3-6 tekrar eder.


**Şekil 3**: Test İmgeleri [17]

## 4 Deneysel Sonuçlar

Önerilen yöntemin performansını ölçmek için 4 adet ölçüm parametresi kullanılmıştır. Kullanılan ölçüm parametreleri;

- Kapasite,
- Görsel kalite,
- Gizlilik,
- Çalışma zamanı olarak belirlenmiştir.

Bu parametrelerin performansını ölçmek için Şekil 3'te gösterilen 512 x 512 boyutundaki ikili imgeleri kullanılmıştır.

Veri gizleme kapasitesini ölçmek için 2 x 2, 3 x 3, 4 x 4 ve 8 x 8 boyutundaki örtüşmeyen alt bloklar kullanılmıştır. Elde edilen maksimum kapasite değerleri Tablo 1'de verilmiştir.

**Tablo 1. Blok boyutuna göre maksimum veri gizleme kapasiteleri.**

| | 2 x 2 | 3 x 3 | 4 x 4 | | 8 x 8 | 16 x 16 |
|---|---|---|---|---|---|---|
| Baboon | 20372 | 13999 | 9563 | | 3099 | 907 |
| Airplane | 4718 | 3623 | 2920 | | 1302 | 495 |
| Lena | 4568 | 4302 | 3515 | | 2005 | 911 |
| Gatbawi | 9085 | 7865 | 6849 | | 3472 | 1022 |
| Peppers | 3828 | 2965 | 2307 | | 1136 | 494 |
| Epitaph | 9275 | 8288 | 6806 | | 2896 | 987 |

Önerilen yöntemin kapasitelerinin literatürde daha önceden önerilmiş diğer yöntemlerle karşılaştırılması Tablo 2' de verilmiştir. Bu karşılaştırmada 3 x 3 boyutundaki bloklar kullanılmıştır.

**Tablo 2. Kapasitelerin karşılaştırılması**

| | Vankatesen ve ark.'nın yöntemi [16] | Tseng ve ark.'nın yöntemi [25] | Tuncer ve ark.'nın yöntemi [26] | Jung ve Yoo'nun yöntemi [17] | Önerilen yöntem |
|---|---|---|---|---|---|
| Baboon | 9441 | 11806 | 10800 | 11396 | 13999 |
| Airplane | 3293 | 3292 | 3414 | 3440 | 3623 |
| Lena | 3657 | 4198 | 4268 | 4415 | 4302 |
| Gatbawi | 7273 | 9551 | 10610 | 9616 | 7865 |
| Peppers | 2880 | 3015 | 3008 | 3181 | 2965 |
| Epitaph | 8953 | 9360 | 9641 | 9887 | 8288 |

*Görsel Kalite:* Önerilen yöntemin görsel kalitesini ölçmek için ortalama karesel hata (MSE) ve tepe sinyal gürültü oranı (PSNR) kullanılmıştır. MSE ve PSNR'nin eşitlikleri Eşitlik 2 ve 3'te verilmiştir.

$$MSE = \sum_{i=1}^{M}\sum_{j=1}^{N}\left(CI_{i,j} - SI_{i,j}\right)^2/(W\ x\ H) \quad (3)$$

$$PSNR = 10\ x\ log_{10}(1/MSE) \quad (4)$$

Eşitlik 3' te kullanılan *CI* örtü imgesi, *SI* stego imge, *W* imgenin satır sayısı, *H* imgenin sütun sayısıdır.

Önerilen metodun blok boyutuna göre elde edilen PSNR değerleri Tablo 3'te verilmiştir.

**Tablo 3. Blok boyutuna göre elde edilen PSNR değerleri.**

| | 2 x 2 | 3 x 3 | 4 x 4 | 8 x 8 | 16 x 16 |
|---|---|---|---|---|---|
| Baboon | 13.50 | 15.48 | 17.26 | 22.28 | 27.52 |
| Airplane | 20.08 | 21.47 | 22.58 | 26.06 | 30.25 |
| Lena | 19.91 | 20.47 | 21.59 | 23.61 | 27.65 |
| Gatbawi | 16.80 | 17.67 | 18.34 | 21.86 | 26.27 |
| Peppers | 20.75 | 22.18 | 23.31 | 26.60 | 30.76 |
| Epitaph | 17.03 | 17.85 | 18.76 | 22.76 | 27.22 |

3 x 3 blok boyutu için en yüksek kapasitede elde edilecek teorik PSNR değeri $10\ x\ log_{10}(3\ x\ 3\ x\ 2) = 12{,}56$ dB olarak hesaplanmaktadır. PSNR değeri kapasiteyle ters orantılıdır.

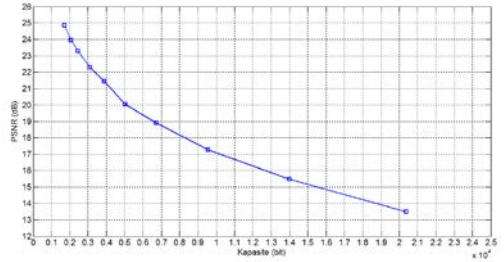
*Gizlilik:* Bu makalede gizlilik lojistik harita kullanılarak üretilen stego-anahtar tarafından sağlanmaktadır. Anahtarın büyüklüğü Eşitlik 5 kullanılarak hesaplanmaktadır.

$$ks = kapasite\ x\ \lfloor log_2 MxN \rfloor \quad (5)$$

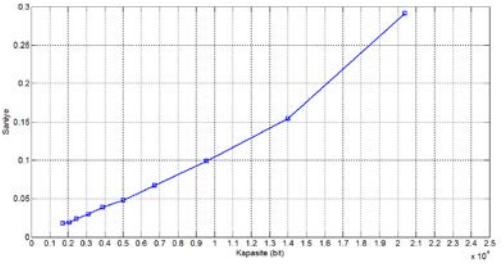
Eşitlik 5'te $ks$ anahtar boyutu, $M$ kullanılan alt bloğun genişliği, $N$ kullanılan alt bloğun yüksekliği olarak ifade edilmektedir. Örneğin 16 x 16 boyutundaki alt bloklar kullanılarak 900 bit veri gizlenirse, kullanılacak anahtar boyutu 7200 bit olarak elde edilmektedir. Anahtar boyutunun büyük olması veri gizliliğinin sağlandığını göstermektedir.

*Çalışma Zamanı:* Testler MATLAB2013a programında Windows 10 işletim sistemine sahip olan 4 GB ram ve Pentium Core i5 4300u işlemcili bir dizüstü bilgisayarda gerçekleştirilmiştir. Çalışma zamanını test edebilmek için maksimum kapasitede veri gizlenmiş ve çıkarılmıştır. Önerilen metot 21322 bit veriyi 0.2846 saniyede gizlemiş ve 0.2497 saniyede çıkarmıştır. 1000 bit veriyi ise 0.009 saniyede gizlemiş ve 0.006 saniyede çıkarmıştır.

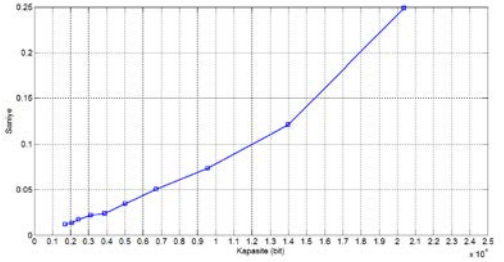
Şekil 4'te PSNR/kapasite, veri gizleme zamanı/kapasite ve veri çıkarma zamanı/kapasite değişim oranları verilmiştir.




(a)




(b)




(c)

**Şekil 4:** (a) PSNR/Kapasite, (b) Veri gizleme zamanı/kapasite, (c) Veri çıkarma/Kapasite

## 5 Sonuç

Bu çalışmada, ikili imgeler için kaos tabanlı yeni bir steganografik yöntem önerilmiştir. Önerilen yöntemde kaotik haritalardan lojistik harita kullanılarak stego anahtarı elde edilmiştir. Bu yöntem blok tabanlı bir yöntem olup, bu çalışmada 2 x 2, 3 x 3, 4 x 4, 8 x 8 ve 16 x 16 boyutunda örtüşmeyen alt bloklar kullanılmıştır. Önerilen yöntemi test etmek için kapasite, görsel kalite, gizlilik ve çalışma zamanı parametreleri kullanılmıştır. Deneysel sonuçlar önerilen algoritmanın yüksek kapasiteye ve görsel kaliteye sahip olduğunu göstermiştir. Lojistik harita kullanılarak üretilen anahtar sayesinde gizlilik sağlanmıştır. Ayrıca yapılan deneyler önerilen yöntemin hızlı çalıştığını da göstermiştir. Önerilen veri gizleme ve veri çıkarma algoritmasının karmaşıklığı Şekil 4' te de gösterildiği gibi $O(n^2)$' dir. Karmaşıklığın $O(n^2)$ çıkmasının en önemli sebebi nokta operatörü kullanılmasıdır.

Gelecekteki çalışmalarda, önerilen yöntemin gri seviyeli ve renkli imgeler için uyarlanabileceği ve kimlik doğrulama yöntemi olarak da kullanılabileceği gösterilmiştir.

## Kaynaklar


[1] Z. Ni, Y.-Q. Shi, N. Ansari, W. Su, Reversible Data Hiding, IEEE Transactions On Circuits And Systems For Video Technology, 16 (3), 2006.

[2] M. B. Begum, Y. Venkataramani, LSB Based Audio Steganography Based On Text Compression, Procedia Engineering, 30, 703-710, 2012.

[3] F. Perez-Gonzlez F. Balado, Quantized projection data hiding, inProc. IEEE Int. Conf. Image Process., 2, 889–892, 2002.

[4] Y. Q. Shi, Z. Ni, D. Zou, C. Liang, Lossless data hiding: fundamentals, algorithms and applications, IEEE Int. Symp. Circuits Syst., 33–36, 2004.

[5] Q. Mao, A fast algorithm for matrix embedding steganography, Digital Signal Processing, 25, 248-254, 2014.

[6] L. Von Ahn and N. J. Hopper, Public-key steganography, in Advances in Cryptology-Eurocrypt, Berlin, Germany: Springer-Verlag, 3027, 323–341, 2004.

[7] G.S. Lin, Y.T. Chang, W.N. Lie, A framework of enhancing image steganography with picture quality optimization and anti-steganalysis based on simulated annealing algorithm, IEEE Trans. Multimedia, 12 (5), 345–357, 2010.

[8] E. Avci, T. Tuncer, F. Ertam, Çok katmanlı görüntü steganografi, 7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 2014.

[9] K. Matsui, K. Tanaka, Video-steganography: how to secretly embed a signature in a picture, in: Proc. IMA Intellectual Property Project, 1994, pp.187–206.

[10] S.H. Low, N.F. Maxemchuk, A.M. Lapone, Document identification for copyright protection using centroid detection, IEEE Trans. Commun. (1998) 372–383.

[11] J.T. Brassil, S.H. Low, N.F. Maxemchuk, Copyright protection for the electronic distribution of text documents, in: Proc. of IEEE, 1999, pp. 1181-1196.

[12] E. Koch, J. Zhao, Embedding robust labels into images for copyright protection, in: Proc. of the

International Congress on Intellectual Property Rights for Specialized Information, Knowledge & New Technologies, 1995, pp. 242–251.

[13] M. Wu, E. Tang, B. Liu, Data hiding in digital binary images, in: IEEE Inter. Conf. on Multimedia & Expo, 2000, pp. 393–396.

[14] C. Liu, Y. Dai, Z. Wang, A novel information hiding method in binary images, J. Southeast Univ. (2003).

[15] M. Wu, B. Liu, Data hiding in binary image for authentication and annotation, IEEE Trans. Multimedia (2004) 528–538.

[16] M. Venkatesan, P. Meenakshidevi, K. Duraiswamy, K. Thiagarajah, A new data hiding scheme with quality control for binary images using block parity,in: 3rd Inter. Symposium on Information Assurance and Security, 2007, pp. 468–471.

[17] K.H. Yung, K.Y. Yoo, Data hiding method in binary images based on block masking for key authentication, Information Sciences, 277 (2014), pp. 188-196.

[18] K.H. Yung, K.Y. Yoo, Data hiding method with quality control for binary images, J. Software Engineering & Applications, 2 (2009), pp. 20-24.

[19] C.C. Wang, Y.F. Chang, C.C. Chang, J.K. Jang, C.C. Lin, A high capacity data hiding scheme for binary images basedon block patterns, The Journal of Systems and Software, 93, (2014), 152–162

[20] B. Feng, W. Lu, W. Sun, Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 2, FEBRUARY,2015, pp. 243-255.

[21] D. Bandyopadhyay, K. Dasgupta, J. K. Manda, P. Dutta, "A NOVEL SECURE IMAGE STEGANOGRAPHY METHOD BASED ON CHAOS THEORY IN SPATIAL DOMAIN", International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 3, No 1, February 2014.

[22] D.-C. Lou, C.-H. Sung, "A Steganographic Scheme for Secure Communications Based on the Chaos and Euler Theorem", IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 6, NO. 3, JUNE 2004.

[23] http://geoffboeing.com/2015/03/chaos-theory-logistic-map/ (Son Erişim Tarihi: 23.04.2016)

[24] F. Özkaynak, A. B. Özer, Lojistik Harita ile Rastgele Sayı Üretilmesi ve İstatistiki Yöntemlerle Sınanması, Journal of Istanbul Kültür University, 2006.

[25] H.W. Tseng, F.R. Wu, C.P. Hsieh, Data hiding for binary images using weight mechanism, IIHMSP, 307– 310, 2007.

[26] T. Tuncer, D. Avcı, E. Avcı, A new data hiding algorithm based on minesweeper game for binary images, Journal of the Faculty of Engineering and Architecture of Gazi University 31:4 (2016) 951-959.