Haliç Üniversitesi Fen Bilimleri Dergisi 2021, 4/1: 25-40
DOI: 10.46373/hafebid.858834

# Yeni Kaotik Video Steganografi Metodu

Damla AKYÜZ[1*], Mustafa Cem KASAPBAŞI[1]

[1] İstanbul Ticaret Üniversitesi, Bilgisayar Mühendisliği, İstanbul, Türkiye
**Orcid:**0000-0002-3583-6858, 0000-0001-6444-6659

**Geliş Tarihi:** 12.01.2021
***Sorumlu Yazar e mail:** damlas.senkul@gmail.com **Kabul Tarihi:** 17.02.2021

**Atıf/Citation:** Akyüz, D., Kasapbaşı, M.D. "Yeni Kaotik Video Şifreleme Metodu", Haliç Üniversitesi Fen Bilimleri Dergisi 2021, 4/1: 25-40.

**Araştırma Makalesi/** ***Research Article***

## Özet

Günümüzde, teknoloji ve internetin gelişerek yaygınlaşmasıyla, güvenli veri transferi için farklı yöntemler ve teknikler uygulanmaya başlanmıştır. Gelişen bu yöntemlerden biri de Steganografi'dir. Steganografi, iletilecek bilginin, istenmeyen kişiler tarafından fark edilmesini önlemek için farklı araçlara gizlenmesi sanatıdır. Taşıyıcı araçlarda gözle görülür değişiklik yapılmadan mesajın gizlenmesi hedeflenir. Bu çalışmada, önerilen kaotik yöntem ile video üzerinde veri gizlenmesi amaçlanmıştır. Videoda, veri gizlenecek çerçeveler ve pikseller belirli bir düzen olmadan kaotik bir yöntemle seçilerek, RGB değerlerinin en az anlamlı bitinin değiştirilmesi ile veri bir piksele 1 byte gizli bilgi olacak şekilde gizlemesi gerçekleştirilmiştir. Oluşturulan taşıyıcı videonun ve videonun ilk halinin görsel değerleri karşılaştırılarak gizlemenin başarısı PSNR, SNR, Entropi, SSIM, MSE yöntemleri ile ölçülmüştür.

**Anahtar Kelimeler:** Steganografi, Kaos, Video Steganografi, Veri Gizleme

# New Chaotic Video Steganography Method

## Abstract

Nowadays, with the development and widespread use of technology and Internet, different methods and techniques have been applied for secure data transfer. One of these developing methods is Steganography. Steganography is an art through which the information to be transmitted is hidden in different tools in order to prevent its recognition by unwanted people. It is aimed to hide the message with no explicit change made in transmissive vehicles. In this study, it is aimed to hide data on the

video by means of the technical chaotic method proposed. In the video, frames and pixels to hide data are selected in through a chaotic method without a specific order, and data concealment is realized by changing the least significant bit of RGB values, data concealment is realized in an equilibrium of one byte of hidden data to one pixel. By comparing the transmissive video formed and the visual values of its original form, the success of hiding was measured by the methods such as PSNR, SNR, Entropy, SSIM and MSE.

**Keywords:** Steganography, Chaos, Video Steganography, Data Hiding

## 1. Giriş

Steganografi, iletilecek bilginin, istenmeyen kişiler tarafından fark edilmesini önlemek için farklı araçlara gizlenmesi sanatıdır [1]. Steganografinin amacı fark edilmeden gizli bir şekilde iletişim kurmaktır. Steganografi ile Metin, Ses, Resim ve Video gibi çoklu ortam dosya formatları kullanılarak gizleme işlemi gerçekleştirilebilir [2].

Steganografi sisteminin kapasite ve güvenlik olmak üzere iki önemli yönü vardır. Kapasite, fark edilir hale gelmeden maksimum kaç byte veri gizlenebileceğini ifade eder. Güvenlik, üçüncü kişilerin verilere erişimini engellemeye yöneliktir [3].

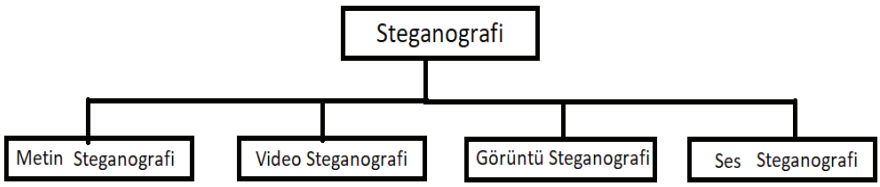
## 2. Literatür Araştırması

Bilgileri gizlemek için birçok teknik vardır. Uzamsal (Spatial) ve frekans alanına göre metotlar farklılıklar göstermektedir.

Ancak bu çalışmada uzamsal metotlardan biri olan en az anlamlı bit (LSB- Least Significant Bit) Steganografi yöntemi kullanılmıştır. Uzamsal metotlardan olan LSB steganografisi ile çoklu ortamın saklandığı verilerin en anlamsız olan biti veya bitleri, saklanmak istenen verinin bitleri ile yer değiştirilir [4]. Güvenliği artırmak için taşıyıcı ortama veriler saklanmadan önce şifreleme yapılmak istenebilir. Şifrelenmiş veriler, LSB tekniği kullanılarak görüntüye gömülür. Steganografi görüntüsü, metin biçiminde 16 tabanına dönüştürülür ve

çerçeve dönüştürme tekniği kullanılarak, videoya gömülür. Bu işleme, verilerin stenografi tekniği, yani görüntü stenografisi ve video stenografisi ile işlendiği çok düzeyli stenografi denir. Bu, verilerin güvenliğini artırır ve veriler bir makineden diğerine kolayca iletilerek çok düzeyli güvenlik sağlar[5].

Şekil 1 de Steganografinin uygulandığı çeşitli kullanım ortamları gözükmektedir.




**Şekil 1.** Steganografi kullanılan ortamlar

***Metin Steganografisi,*** gizli metin mesajını, başka bir metin içinde saklı mesaj olarak gizleme veya orijinal gizli mesajla ilgili bir mesajı oluşturma mekanizmasıdır [6].

Metin Steganografi yöntemleri:

a. Formata dayalı (Format based): Bu yöntemde, söz ve cümlelerdeki mesajlar değiştirilmemektedir; yalnızca özel karakterler, yani beyaz boşluk steganografisi kullanılarak sözcükler, satırlar ve paragraflar arasındaki boşluklarda değişiklikler yapılmaktadır [7] .
b. Rastgele ve istatiksel üretim yöntemleri (Random and statistical generation methods): Bu yöntemde, tam bir paragraf oluşturmak için fazladan bir karmaşıklık (zaman ve boşluk) eklenir; bu gizli mesaj asıl mesajının içine gizlenir [8].
c. Dilbilimsel yöntem (Linguistic method): Bu yöntem, gizlenecek mesajın dil yapısına (noktalama işaretleri) veya iki ana türü olan mesajı gizlemek için anlamsal kelimelere bağlı olarak başka bir mesajdaki veriyi gizlemek için kullanılır [9].

***Video Steganografisi- (Mesajın videoda saklanması-Hiding in video)***, Bir mesajı videoya gizlemek için, çok fazla işlem süresi ve alanı gerekir. Her bir bit akışının değerlerinin değiştirilmesi, bit akışı matrisini oluşturmak için gizli mesajın ikili değerine bağlıdır [10] .

***Görüntü Steganografi (Mesajın görüntüye saklanması-Hiding in image),*** Bir görüntünün içinde gizli bir mesaj göndermek amaçlı kullanılmak anlamına gelir[11].

***Ses Steganografisi (Mesajın ses içine saklanması-Hiding in audio,*** Bu teknik, örneğin bir yazar hakkındaki bilgileri gizlemek gibi ses filigranı için kullanılır. Ses dosyasına ve gizleme mekanizmalarına bağlı olarak, ses steganografisinin LSB Kodlaması, Eşlik Kodlaması, Faz Kodlaması, Yayılı Spektrum ve Yankı Gizleme gibi birçok türü vardır [12].

Bahsedilen steganografi kullanım ortamları içinde verileri gizlemek için en yaygın kullanılan teknik uzamsal teknikler içinde olan LSB yöntemidir [13]. Her pikselin en önemsiz bitini gizlenecek mesajın bitleriyle değiştirerek bir görüntünün içinde mesajların gizlendiği LSB steganografi tekniğidir [14]. 24 bit renkli bir görüntü kullanırken, kırmızı, yeşil ve mavi renklerin her birinden bir bit bileşen kullanılabilir, böylece her pikselde toplam 3 bit depolanabilir [15].

Bu çalışmada da mesajların gizleneme ortamı olarak video seçilmiştir. Gizli bir mesajı bir video çerçevelerinin içine gizlemek için uygun bir taşıyıcı video gereklidir. Bu çalışmada ayrıca kırmızı, mavi ve yeşil renklerin en düşük değerlikli sırası ile 3 biti, 3 biti ve 2 biti kullanılarak bir piksele 1 baytlık bilgi saklanabilmiştir.

## 3. Materyal ve Metot

### 3.1 Kaos Teorisi ve Lojistik Harita

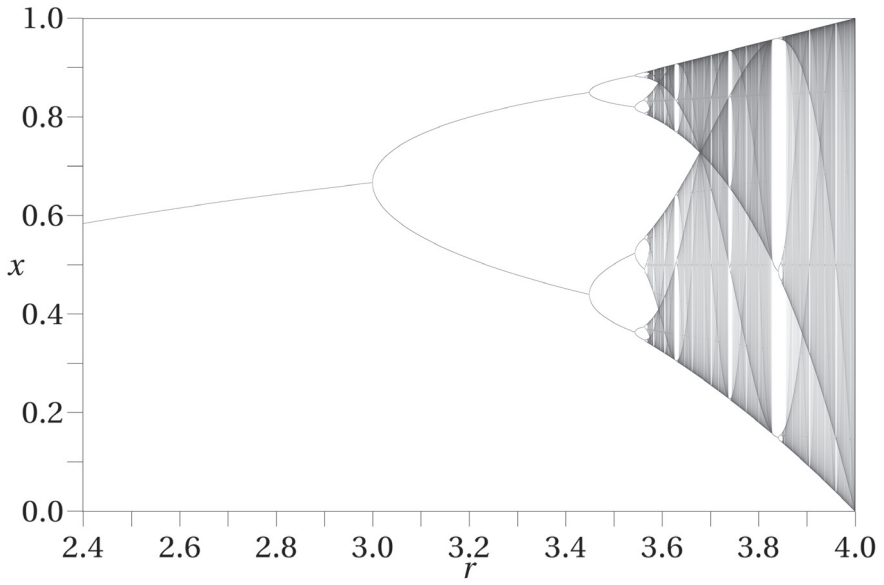
Kaotik sistemler, doğrusal olmayan dinamik sistemlerin basit bir alt türüdür. Çok az etkileşimli parçalar içerebilirler ve bunlar çok basit kuralları takip edebilir, ancak bu sistemlerin tümü, başlangıç koşullarına

çok hassas bir bağımlılığa sahiptirler. Belirleyici basitliklerine rağmen, zamanla bu sistemler tamamen tahmin edilemez ve farklı (kaotik) davranışlar üretebilir [16].

Lojistik harita modeli, bir popülasyonun taşıma kapasitesine ulaştıkça azalmadan önce nasıl yavaş, sonra hızlı büyüdüğünü gösteren ortak s-eğrisi lojistik fonksiyonuna dayanmaktadır. Lojistik fonksiyon, zamanı sürekli olarak değerlendiren diferansiyel bir denklem kullanır. Lojistik harita, bunun yerine ayrık zaman adımlarına bakmak için doğrusal olmayan bir fark denklemi kullanır.

Lojistik Harita, biyolog Robert May[17] tarafından 1976 tarihli bir makalede popüler hale getirilmiştir. Lojistik harita denklemi Denklem (1) de verilmiştir. Bu şekilde adlandırılır çünkü herhangi bir zaman adımındaki nüfus değerini bir sonraki adımdaki değerine eşler:

$$x_{i+1} = \lambda * x_i * (1 - x_i) \quad (1)$$




**Şekil 2.** Lojistik harita çatallanma gösterimi: Yatay eksen λ, düşey eksen x değerleridir **[18]**

$x_{i+1}$ kaotik sistemin bir sonraki değeri, bu çalışmada λ için, [3.9- 4] arası sistem daha çok kaotik davrandığı (Şekil 2) kısım kullanılmıştır.

Bu çalışmada uygulanan yöntem ile kaotik fonksiyonumuzu kullanarak oluşan değerleri, gizli verinin saklanacağı piksel yerini belirlemekte kullanılmıştır. Sunulan çalışma Veri saklama ve Veri çıkartma olmak **üzere** 2 aşamalıdır. Verinin önerilen kaotik yöntem ile gizlenmesi ve geri çıkarılması. İlgili kısımlar için algoritmalar aşağıdaki gibi verilmiştir. Algoritma 1 gizli verinin video ortamına saklanması adımları göstermekte iken Algoritma 2, stego videodan gizli mesajın geri alınması aşamalarını göstermektedir[19].

**Algoritma 1** Veri Saklama Algoritması

```
INPUT: input_video, input_text
1.  INITIAL ASSIGNMENTS: x = 0.418; λ = 3.995; alfa = 10^14;
2.  for j=1 to text_size do
3.     S = frame_count * video_height * video_width;
4.     x = λ * x * (1 - x);
5.     value = j + floor ( mod(( alfa * x), S));
6.     n_frame = floor(value / (video_width * video_height));
7.     n_height = floor(mod(value,(video_width * video_height)) / video_width);
8.     n_width = floor(mod(value,(video_width * video_height)) / video_height);
9.     pixel_values(j,:) = [n_frame n_height n_width f(j)];
10. end for
11. array_size = size(pixel_values,1);
12. frame_pointer = 0;
13.
14. while hasFrame(vidObj)
15.    frame_pointer=frame_pointer+1;
16.    Extracted = pixel_values((pixel_values(:,1)==frame_pointer),:);
17.    vidFrame = readFrame(vidObj);
18.    fname=fullfile('path\orj_frames',strcat('frame-',num2str(frame_pointer),'.png'));
19.    imwrite(vidFrame,fname);
20.    if (size(Extracted,1) > 0)
21.       vidFrame = hide_function(vidFrame,Extracted);
22.       fname=fullfile(path\changed_frames',strcat('frame-',num2str(frame_pointer),'.png'));
23.       imwrite(vidFrame,fname);
24.    end if
25.       writeVideo(videoOut,vidFrame);
26. end while
27.    close(videoOut);
28.    status=1;
29. OUTPUT: 1; (Stego Video)
```

**Algoritma 2** Veri Çıkartma Algoritması

```
INPUT: Stego_video, text_size
30. INITIAL ASSIGNMENTS: x = 0.418; λ = 3.995; α = 10^14;
    text_size = 20000;
31. for j=1 to text_size do
32.       S = frame_count * video_height * video_width;
33.       x =λ1* x *(1 − x);
34.       value = j + floor ( mod(( alfa * x), S));
35.       n_frame =(value / (video_width * video_height));
36.       n_height = floor(mod(value,(video_width * video_hei-
          ght)) / video_width);
37.       n_width = floor(mod(value,(video_width * video_hei-
          ght)) / video_height);
38.       pixel_values(j,:) = [n_frame n_height n_width f(j)];
39. end for
40. while hasFrame(vidObj)
41.    frame_pointer=frame_pointer+1;
42.    hided_in_frame = pixel_values((pixel_values(:,1)==f-
       rame_pointer),:);
43.    hided_size = size(hided_in_frament_frame = readFrame(-
       vidObj);
44.       if (hided_size > 0)
45.             for c=1:hided_size
46.             i = hided_in_frame(c,2);
47.             j = hided_in_frame(c,3);
48.             index = hided_in_frame(c,4);
49.             r1=current_frame(i,j,1);
50.             r2=current_frame(i,j,2);
51.             r3=current_frame(i,j,3);
52.             R(index)=extract_text(r1,r2,r3);
53.         end for
54.     end if
55. end while
56. fid = fopen('out_text.txt','wb');
57. fwrite(fid,char(R),'char');
58. fclose(fid);
59. status=1;
60. OUTPUT: 1; (Video)
```

## 3.2 Kalite ölçüm yöntemleri

### 3.2.1 MSE (Mean Squared Error)

Sıkıştırılmış ve orijinal görüntü arasındaki kümülatif kare hatasını temsil eder. Basitçe, ortalama kare hatası, bir regresyon eğrisinin bir dizi noktaya ne kadar yakın olduğunu söyler. MSE, bir makine öğrenmesi modelinin performansını ölçer ve her zaman pozitif değerlidir. Sıfıra yakın olan değerlerin daha iyi bir performans gösterdiği söylenebilir. Denklem (2) de gösterilmiştir. [20]

$$MSE=\frac{1}{MN}\sum_{j=1}^{M}\sum_{k=1}^{N}(Xj,k-X'j,k)^2 \quad (2)$$

### 3.2.2PSNR(Peak Signal Noise Ratio)

PSNR, kayıplı ve kayıpsız sıkıştırmanın yeniden yapılandırma kalitesini ölçmek için kullanılır. Bu durumda sinyal, orijinal verilerdir ve gürültü, sıkıştırma ile ortaya çıkan hatadır. PSNR, en kolay şekilde ortalama hata karesi ile tanımlanır. Görüntü ve sinyal işleme ile ilgili çoğu araştırma, kalite ölçüm aracı olarak PSNR kullanmaktadır. Ortalama kare hatasının (MSE) logaritmasının hesaplanmasından elde edilir. PSNR ne kadar yüksekse, sıkıştırılmış veya yeniden yapılandırılmış görüntünün kalitesi o kadar iyidir. Denklem (3) de gösterilmiştir. [20]

$$PSNR=10log\frac{(2^n-1)^2}{MSE}=10log\frac{255^2}{MSE} \quad (3)$$

### 3.2.3 SNR (Signal Noise Ratio)

Bilim ve mühendislikte kullanılan, bir sinyalin seviyesini arka plandaki gürültü seviyesiyle karşılaştıran bir ölçüdür. SNR, sinyal gücünün gürültü gücüne oranı olarak tanımlanır, genellikle desibel cinsinden ifade edilir. 1: 1'den yüksek bir oran (0 Db' den büyük bir oran) gürültüden daha fazla sinyal olduğunu gösterir.

SNR, elektrik sinyalleri için yaygın olarak alıntılanırken, herhangi bir sinyal formuna, örneğin bir buz çekirdeğindeki izotop seviyelerine, hücreler arasındaki biyokimyasal sinyale veya finansal ticaret sinyallerine uygulanabilir. Sinyal-gürültü oranı bazen yararlı bilgilerin bir konuşma veya takastaki yanlış veya alakasız verilere oranını ifade etmek için mecazi olarak kullanılır. Denklem (4) de gösterilmiştir. [21]

$$\text{SNR}=\frac{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f'(x,y)^2}{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}[f(x,y)-f'(x,y)]^2} \quad (4)$$

### 3.2.4 Entropi

Entropi, bir sistemdeki rastgele oluşum ve bozukluk olarak tanımlanır. P ($m_i$) bir görüntüdeki her bir pikselin olasılık durumlarını temsil eder ve M × N toplam piksel sayısıdır. Gri seviyeli bir görüntüde ($m_0$ = 0, $m_1$ = 1, ... $m_{255}$ = 255), her birinin olasılıkları gri değeri görüntünün histogramından elde edilir. Ideal entropi değeri 8'dir. Görüntü ve entropi değeri, daha düşük görüntüler için 8'den çok daha düşüktür. Eğer entropi değeri 8'den çok daha düşük ise örneğin 0'a yakın ise güvenlik tehlikesi var demektir. Denklem (5) de gösterilmiştir. [22]

$$H(m)=\sum_{i=0}^{M*N-1} p_{(m_i)}\, log_2 \frac{1}{p_{(m_i)}} \quad (5)$$

### 3.2.5 SSIM (Structural Similarities)

Steganografik olarak algılanamazlığın kalitesini, orijinal ve işlenmiş görüntü arasındaki benzerliği ölçmek için kullanılan bir yöntemdir. Parlaklık, kontrast ve yapı olmak üzere üç ana faktöre dayalı olarak oluşturulmuştur. Veri sıkıştırma gibi işlemlerden veya veri iletimindeki kayıplardan kaynaklanan görüntü kalitesi düşüşünü ölçen algısal bir ölçüdür. X orijinal görüntü, y işlenmiş görüntüdür. SSIM değerinin

1'e yakın veya eşit olması, orijinal ve işlenmiş görüntünün yapısal olarak çok benzer olduğu anlamına gelmektedir. Denklem (5) de gösterilmiştir [23].

$$SSIM(x,y)=\frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \quad (6)$$

## 4. Bulgular ve Tartışma

Bu çalışmada üretilen gizli verilerin saklanması için sıkıştırılmamış biçimde olan 9sn uzunluğunda bir avi video seçilmiştir. Çeşitli uzunluklarda metinler hazırlanarak Algoritma 1'deki yönteme göre video içine saklanmıştır. Metin uzunluğu 1KByte, 5KByte, 10KByte ve 20KByte olacak şekilde testler yapılmıştır. Gizli mesajın fark edilmemesi için daha büyük metin uzunlukları kullanılamamıştır.

**Tablo 1.** Video içinde saklanan verilerin Kalite Ölçümleri

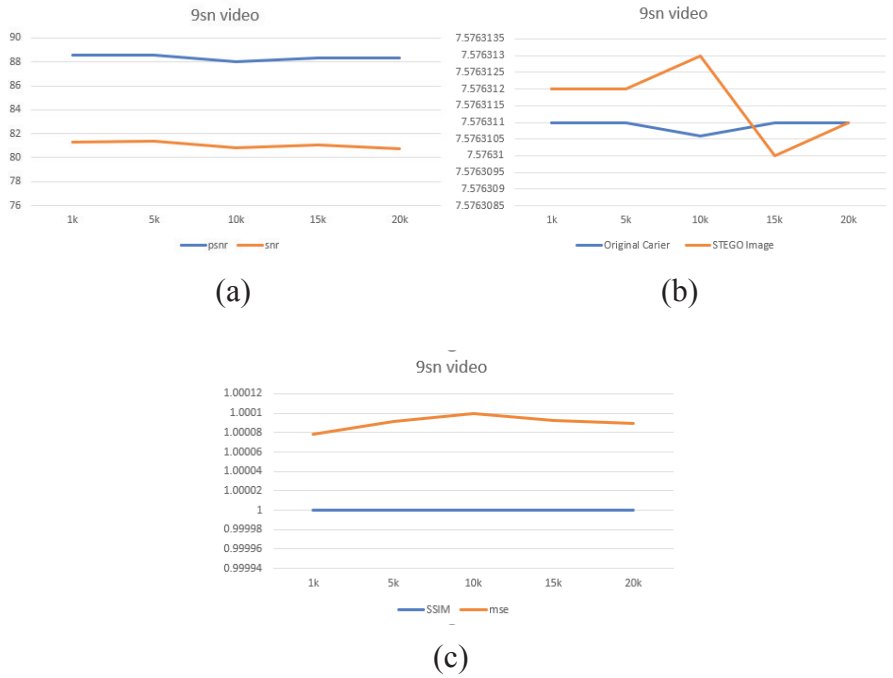
| Metin Büyüklüğü | PSNR | SNR | Orijinal Entropi | STEGO Entropi | SSIM | MSE |
|---|---|---|---|---|---|---|
| 1k | 88.53803 | 81.32454 | 7.576311 | 7.576312 | 1 | 7.83E-05 |
| 5k | 88.59374 | 81.37585 | 7.576311 | 7.576312 | 1 | 9.15E-05 |
| 10k | 88.03115 | 80.84179 | 7.576311 | 7.576313 | 1 | 0.0001 |
| 15k | 88.30103 | 81.04518 | 7.576311 | 7.576312 | 1 | 9.21E-05 |
| 20k | 88.30201 | 80.78122 | 7.576311 | 7.576311 | 1 | 8.99E-05 |

Tablo1 de çeşitli büyüklükteki verilerin gizlenmesi durumunda oluşacak kalite farkını göstermek için PSNR (Peak Signal Noise Ration), SNR( Signal Noise Ratio ), Entropi, SSMI (Structural Similarity) ve MSE (Mean Squared Error) dan yararlanılmıştır.

Gözüktüğü gibi çok yüksek PSNR, SNR değerleri elde edilmiştir. Entropide ki değişiklik fark edilecek düzeyde değildir. SSMI metriği ise en yüksek değeri olan 1 değerinde olup iki video arasındaki yapısal benzerliğin çok yüksek olduğunu göstermektedir. MSE değerleri

karşılaştırıldığında çok ufak farklar olduğu gözükmektedir. Bu ölçüm değerlerinden çıkarılabilecek sonuç, video kalitesinde bir değişiklik olmadığı bu sebeple gizli mesajın anlaşılamayacağı söylenebilir.

Şekil 3 de farklı büyüklükteki gizili mesaj büyüklüklerine göre ölçüm değerleri grafik olarak gösterilmiştir.




**Şekil 3.** 1K, 5K, 10K, 15K ve 20K gizli mesaj a göre (a) PSNR SNR değişimleri (b) Orijinal ve Stego görüntü Entropi değişimleri (c) SSMI ve MSE değişimleri

### 4.1. Tartışma

Benzer sonuçları kıyaslanmak istenmiş, diğer kaotik LSB yöntemleri kullanan çalışma sonuçları [24-29], ile karşılaştırma yapılmak istendiğinde Tablo 2 oluşturulmuştur. Karşılaştırılan çalışmalardaki kullanılan taşıyıcı videolar aynı olmadığı için sonuçları kendi içinde

değerlendirilmesi daha doğru olacaktır. Bu tabloda benzer metriklerin sonuçları kıyaslanmaktadır. Çalışmamızda kalite düşüşü olmamıştır ve çok yüksek PSNR değerleri elde edilmiştir. Bu sonuçlara dayanarak gizli mesajın anlaşılamayacağı sonucuna varılmaktadır.

**Tablo 2.** Benzer çalışmaların sonuçları

| Referans | MSE | PSNR | Açıklama |
|---|---|---|---|
| [24] | 0.1999 | 55.1217 | Videoya 623 karakter LSB yöntemi ile saklanmıştır. |
| [25] | [0-0.3] | [35-74] | Thinkerbell Kaotik harita ile piksel seçimi, LSB yöntemi ile Video içine metin gizleme |
| [26] | 0.01550 | 59.2377 | Kaotik seçimli OpenMP uygulamalı Görüntü steganografi uygulaması |
| [27] | - | [43-64] | Arnold Haritası kullanılarak, Frekans Domaininden DCT, Video içine görüntü saklama |
| [28] | - | 78.84 | Video Stegonografisi (Resim ) |
| [29] | | 36.8 | HD görüntüye,<br>QP 10, |
| Bu çalışma | 8.99E-05 | 88.30201 | Kaotik Lojistik harita ile piksel seçimi, 20 KB payload, bir pixele 1 byte gizlenebilir son 3 bit ve 2 bit |

## 5. Sonuçlar

İnternet kullanarak hızlı bilgi alışverişinin yapıldığı çağda bilgi güvenliği ve mahrem şekilde World Wide Web kullanımı için, steganografinin diğer araçların yanında gerekli bir araç olacağı düşünülmektedir. Bu makalede kaotik harita kullanarak gerçekleştirilen bir video steganografi yöntemi sunulmuştur. Video içerisine çeşitli büyüklüklerde metin yerleştirilmiş ve video kalitesindeki değişikliği çeşitli ölçütler ile değerlendirilmiştir. Testler sırasında Tablo1'de izlendiği gibi, PSNR (Peak Signal Noise Ration), SNR( Signal Noise Ratio ), Entropi, SSMI (Structural Similarity Measurment Index) ve MSE (Mean Squared Error) dan yararlanılmıştır. Yapılan çalışma benzer

başka çalışmalar ile de karşılaştırılıp tartışılmıştır. Elde edilen sonuçların ışığında Video içine önerilen kaotik yöntem gizlenen metinlerin başarılı şekilde çıkarıldığı ve kalite ölçümlerinden de çıkarılan sonuca göre anlaşılamayacak şekilde olduğu anlaşılmıştır. Mahremiyet ve gizli iletişim hakkının günümüzde daha da önem kazandığı çağımızda önerilen yöntem ile bu problemin çözümüne bir katkı sağlandığı düşünülmektedir.

## Kaynaklar

[1] Abdulla AA., (2015), Exploiting similarities between secret and cover images for improved embedding efficiency and security in digital steganography. PhD dissertation, Dept. of Applied Computing, Buckingham Univ., Buckingham, UK (pp. 15-26).

[2] Lin G-S., Chan Y-T., Lie W-N., (2010), A framework of enhancing image steganography with picture quality optimization and anti-steganalysis based on simulated annealing algorithm. IEEE Transactions on Multimedia (pp. 347–359).

[3] Ker AD., Bohme R .,(2008), Revisiting weighted stego-image steganalysis. Proc. SPIE Electronic Imaging Security Forensics Steganography and Watermarking of Multimedia Content (pp. 300–313).

[4] Ker AD., (2005), Improved detection of LSB steganography in grayscale image. International Workshop on information hiding. Springer (pp. 87–118).

[5] Luo W, Huang F., Huang J., (2010), Edge adaptive image steganography based on LSB matching revisited. IEEE Transactions on Information Forensic and Security (pp.202–218).

[6] Lin Y-T., Wang C-M., Chen W-S., Lin F-P., Lin W., (2017), A novel data hiding algorithm for high dynamic range image.IEEE Transaction on Multimedia (pp.196–212).

[7] Alwahbani S. M. H., Elshoush H.T., (2018), Chaos-Based Audio Steganography and Cryptography Using LSB Method and One-Time Pad (pp. 15–30).

[8] Bhattacharyya D., Dutta J., Das P., Bandyopadhyay R., Bandyopadhyay SK., Kim T-H., (2009), Discrete fourier transformation based image authentication technique. 8th IEEE International Conference on Cognitive Informatic (pp. 195–220).

[9] Dey S., Abraham A., Sanyal S., (2007), An LSB Data Hiding Technique Using Prime Number. Third International Symposium on Information Assurance and Security, IAS 2007, IEEE (pp. 101–108).

[10] Ker AD., (2005), A general framework for structural steganaly of LSB replacement. International Workshop on information hiding (pp. 285–301).

[11] Chen P-Y., Lin H-J., (2006), A DWT base approach for image steganography. International Journal of Applied Science and Engineering (pp. 280–290).

[12] Dey S., Abraham A., Sanyal S., (2007), An LSB Data Hiding Technique Using Natural Number Decomposition. Third International Conference on Intelligent Information Hiding and Multimedia Signal Process, IIHMSP 2007, IEEE (pp. 177–214).

[13] Chaudhary P.,(2020), Novel Image Encryption Method Base on LSB Technique and AES Algorithm (pp. 15-28).

[14] Chan C-S.,(2009), On using LSB matching function for data hiding in pixels. Fundamenta Informaticae (pp. 55–59).

[15] Fridrich J., Goljan M., (2004), On estimation of secret message length in LSB steganography in spatial domain. Proc. SPIE Electronic Imaging Security Forensics Steganography and Watermarking of Multimedia Content (pp. 15–36).

[16] Selvaraj P., Varatharajan R., (2018), Whirlpool Algorithm with Hash Function Based Watermarking Algorithm for the Secured Transmission of Digital Medical Images (pp. 13-17).

[17] May, R.,(1976), Simple mathematical models with very complicated dynamics. Nature 26 (pp. 459–467).

[18] WikiPedia, Logistic Map, https://en.wikipedia.org/wiki/Logistic_map son erişim (24.11.2020)

[19] Yayla, G. A., MATLAB, Kodlab Yayın Dağıtım (2019).

[20] Kasapbaşı, MC., Elmasry, W., (2018), New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check (pp. 8-9).

[21] https://tr.wikipedia.org/wiki/Sinyal_Gürültü_Oranı(08/01/2021)

[22] Güvenoğlu, E., Razbonyalı C., (2019), The Creation of Maze in Order to Hide Data, and the Proposal of Method Based on AES Data Encryption Algorithm (pp.20-23).

[23] Dalal, M., Juneja M.(2019) A robust and imperceptible steganography technique for SD and HD videos (p.15-19)

[24] Deshmukh P. R., Rahangdale B., (2014), Data Hiding using Video Steganography, International Journal Of Engineering Research & Technology (pp.31-37).

[25] Kar N., Aman M. A. A. A., Mandal K. and Bhattacharya B., (2017), "Chaos-based video steganography," 2017 8th International Conference on Information Technology (pp. 482-487).

[26] Gambhir, G., Mandal, J.K., (2020), Multicore implementation and performance analysis of a chaos based LSB steganography technique. Microsyst Technol https://doi.org/10.1007/s00542-020-04762-4 (pp. 6-9).

[27] Tanveer J. Siddiqui., Ashish Khare., (2020), Chaos-Based Video Steganography Method in Discrete Cosine Transform Domain, International Journal of Image and Graphics, doi: 10.1142/S0219467821500157.

[28] WikiPedia, Logistic Map, http://www.halic.edu.tr, (11/12/2020)

[29] Manisha1 S., Sharmila2 T. S., (2019), A two-level secure data hiding algorithm for video Steganography (pp. 539-541)