



**T.C. İSTANBUL T CARET
 NİVERSİTESİ**

FEN B LİMLERİ ENSTİT S 

YENİ KAOTİK VIDEO STEGANOĞRAFİ METODU

Damla AKY Z

DANIŐMAN

Dr.  ğr.  yesi Mustafa Cem KASAPBAŐI

Y KSEK LİSANS TEZİ

BİLGİSAYAR M HENDİSLİĐİ ANABİLİM DALI

İstanbul 2021

KABUL VE ONAY SAYFASI

Damla AKYÜZ tarafından hazırlanan "Yeni Kaotik Video Steganografi Metodu" adlı tez çalışması 01/03/2021 tarihinde aşağıdaki jüri üyeleri önünde başarı ile savunularak, İstanbul Ticaret Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman	Dr. Öğr. Üyesi Mustafa Cem KASAPBAŞI İstanbul Ticaret Üniversitesi
Jüri Üyesi	Prof. Dr. Serhat ÖZEKES Üsküdar Üniversitesi
Jüri Üyesi	Dr. Öğr. Üyesi Ali BOYACI İstanbul Ticaret Üniversitesi

Onay Tarihi: 15.03.2021

İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsünün 15.03.2021 tarih ve 2021/308 numaralı Yönetim Kurulu Kararının 1. maddesi gereğince, ders yüklerini ve tez yükümlülüğünü yerine getirdiği belirlenen "Damla AKYÜZ" (TC:29435394874) adlı öğrencinin mezun olmasına oy birliği ile karar verilmiştir.

Prof. Dr. Necip ŞİMŞEK
Enstitü Müdürü

AKADEMİK VE ETİK KURALLARA UYGUNLUK BEYANI

İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmada,

- Tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- Görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- Başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- Atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- Kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- Ve bu tezin herhangi bir bölümünü bu üniversitede veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı beyan ederim.

Tarih:15/03/2021

Damla AKYÜZ

İÇİNDEKİLER

İÇİNDEKİLER	i
ÖZET	ii
ABSTRACT	iii
TEŞEKKÜR.....	iv
ŞEKİLLER.....	v
ÇİZELGELER DİZİNİ	vi
SİMGELER VE KISALTMALAR DİZİNİ	vii
1.GİRİŞ	1
2.LİTERATÜR ÖZETİ.....	3
3.MATERYAL VE METOT	11
3.1 Kaos Teorisi ve Lojistik Harita.....	11
3.2 Kalite ölçüm yöntemleri	17
3.2.1 MSE (Mean Squared Error)	17
3.2.2 PSNR (Peak Signal Noise Ratio)	17
3.2.3 SNR (Signal Noise Ratio)	18
3.2.4 Entropi.....	18
3.2.5 SSIM (Structural Similarities).....	19
4.BULGULAR VE TARTIŞMA	20
5. SONUÇLAR VE ÖNERİLER.....	30
KAYNAKLAR	31
EKLER.....	34
EK A. Uygulama Algoritmaları.....	35
ÖZGEÇMİŞ	37

ÖZET

Yüksek Lisans Tezi

Yeni Kaotik Video Steganografi Metodu

Damla AKYÜZ

İstanbul Ticaret Üniversitesi

Fen Bilimleri Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Dr. Öğr. Üyesi Mustafa Cem KASAPBAŞI

2021, 37 sayfa

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: Kaos, Steganografi, Veri Gizleme, Video Steganografi

ABSTRACT

M.Sc. Thesis

New Chaotic Video Steganography Method

Damla AKYÜZ

**Istanbul Commerce University,
Graduate School of Natural and Applied Sciences
Department of Computer Engineering**

**Supervisor: Asst. Prof. Dr. Mustafa Cem KASAPBAŞI
2021, 37 pages**

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, hiding the information to be transmitted in different tools for riddles with experience with unwanted people. In written articles, it is aimed to be given visually and to hide the message. In this technique, it is aimed to hide data on the video with the technical method. In the video, frames and pixels to hide data are selected in a chaotic method without a specific order, and data concealment is realized by equalizing the least significant bit of RGB values. The success of hiding was measured by comparing the visual information of the created carrier video and the original

Keywords: Chaos, Steganography, Data Hiding, Video Steganography

TEŞEKKÜR

Bu araştırma için beni yönlendiren, karşılaştığım zorlukları bilgi ve tecrübesi ile aşmamda yardımcı olan değerli danışman hocam Dr. Öğr. Üyesi Mustafa Cem KASAPBAŞI'na teşekkürlerimi sunarım.

Tezimin her aşamasında beni yalnız bırakmayan babam Kemal ŞENKUL, annem Arife ŞENKUL ve eşim Burak AKYÜZ'e sonsuz sevgi ve saygılarımı sunarım.

Damla AKYÜZ

İSTANBUL, 2021

ŞEKİLLER

Şekil 2.1 Steganografi yöntemleri.....	4
Şekil 2.2 Steganografik sistem.....	5
Şekil 2.3 LSB yöntemi ile veri gizlemesi.....	10
Şekil 3.1 Lojistik harita çatallanma gösterimi.....	13
Şekil 4.1 (a) Psnr snr (b) orijinal ve stego görüntü entropi (c) ssım mse.....	23
Şekil 4.2 (F) Input avi video görüntüsü (E) output avi video görüntüsü.	24
Şekil 4.3 (F) orjinal frame1 görüntüsü (G) changed frame1görüntüsü.....	25
Şekil 4.4 (D) 1.29sn input avi video görüntüsü (E) 1.29sn output avi video.....	27
Şekil 4.5 1.29sn orjinal frame1 görüntüsü (G) 1.29sn changed frame1	28

ÇİZELGELER DİZİNİ

Çizelge 4. 1 0.09sn Video içinde saklanan verilerin Kalite Ölçümleri	21
Çizelge 4. 2 1.29sn Video içinde saklanan verilerin Kalite Ölçümleri	26
Çizelge 4. 3 Benzer çalışmaların sonuçları.....	29

SİMGELER VE KISALTMALAR DİZİNİ

KB	KiloBayt
LSB	En Az Anlamlı Bit (Least Significant Bit)
MSE	Ortalama Kare Hata (Mean Squared Error)
PSNR	Tepe Sinyal Gürültü Oranı (Peak Signal Noise Ratio)
SNR	Sinyal Gürültü Oranı(Signal Noise Ratio)
SSIM	Yapısal Benzerlikler(Structural Similarities)
Σ	Sigma
Λ	Lamda. Dalga boyu (Wavelength) simgesi

1.GİRİŞ

Abdulla (2015) çalışmasına göre steganografi, iletilecek bilginin, istenmeyen kişiler tarafından fark edilmesini önlemek için farklı araçlara gizlenmesi sanatıdır. Chan vd. (2010) çalışmasına göre 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.

Steganografi ile metin, video, görüntü ve ses içerisine veriler gizlenebilmektedir. Görüntü dosyalarına gizlenecek veriler metin dosyası olabilir aynı zamanda görüntü içerisine görüntü dosyası da gizlenebilmektedir. Bu yaklaşımda içerisine bilgi gizlenmek istenen ortama örtü verisi (cover-data) denmektedir. Oluşan ortama ise stego-metin (stego-text) veya stego-nesnesi (stego-object) denmektedir. Steganografi kelimesi Yunanca “steganos: gizli, saklı” ve “grafi: çizim yada yazım” kelimelerinden gelmektedir. Steganografi, Heredot ve Antik yunan zamanına dayanan çok eski bir veri gizleme yöntemidir. İran Savaşları zamanında, gizli bir mesajın kafasına dövmesinin yapılmasına izin vermiş bir ulaktan bahsetmektedir. Sonrasında saçının uzamasını beklemektedir. Bu şekilde mesajı saklamıştır. Mesajın ulaşmasını istediği yere gittiğinde ise saçını kazıtıp, mesajı gizleyerek istediği yere ulaştırmayı başarmıştır. Bu yöntem ilk steganografi yöntemi olarak bilinmektedir. Daha sonrasında steganografi, harflerin içerisine müzik notalarının tanıtılması, I. ve II. Dünya Savaşlarında kullanılmış mors kodları, II. Dünya savaşı sırasında uygulanmış olan ve başarılı olunun görünmez mürekkeplerin kullanılmaya başlanması gibi steganografi yöntemleri ile devam etmiştir (Katzenbeisser ve Petitcolas, 2000). Günümüzde geldiğimizde ise sayısal (dijital) nesneler üzerinde steganografi uygulamaları geliştirilmektedir ve gelişen teknoloji nedeniyle, verilerimizi gizlemek amacıyla son yıllarda çok sık kullanılmaya başlanmıştır. Steganografi, Dilbilim ve Teknik Steganografi olmak üzere ikiye ayrılmaktadır. Dilbilim steganografi, gizleme yapılan verinin metin (text) olduğu steganografi yöntemidir. Teknik Steganografi ise birçok dalı vardır. Bunlar; görünmez mürekkep ve bilgisayar tabanlı yöntemler gibi başlıklar altında anlatılabilmektedir. Bilgisayar tabanlı yöntemlere gelirsek, resim metin, görüntü, ses, dosyalarını kullanarak veri gizleme yöntemleridir.

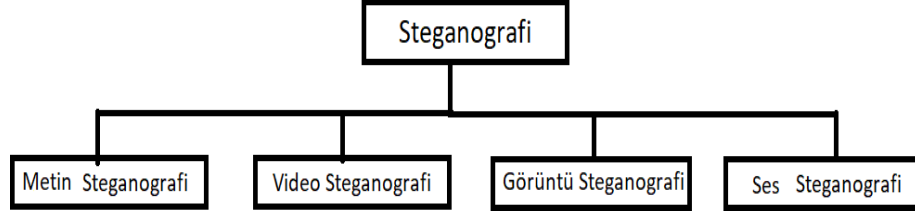
Ker ve Bohme (2008) alışmasına göre Steganografi sisteminin kapasite ve güvenlik olmak üzere iki önemli yönü vardır. Kapasite, fark edilir hale gelmeden maksimum kaç byte veri gizlenebileceğini ifade eder. Güvenlik, üçüncü kişilerin verilere erişimini engellemeye yöneliktir.

2.LİTERATÜR ÖZETİ

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

Ancak bu çalışma da 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. Ker (2005) çalışmasına göre Güvenliği artırmak için taşıyıcı ortama veriler saklanmadan önce şifreleme yapılmak istenebilir. Şifrelenmiş veriler, LSB tekniği kullanılarak görüntüye gömülür. Luo ve Huang (2010) çalışmasına göre 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.

Steganografi birçok alanda ihtiyaç duyulmaktadır. Eski dönemlerden günümüze her dönemde gerek duyulmuştur. Bu ihtiyaçlar doğrultusunda yöntemler geliştirilmiştir. Steganografi bilgi gizlemek için birçok yönetime sahiptir. Görünmez mürekkep, Dijital imza veya spektrum yöntemleri kullanılmaktadır. Günümüze geldiğinizde ise verileri dijital ortama taşınması sonucu görüntü, metin ve sinyaller içerisinde veriler gizlenmeye başlanmıştır. Bir üreticinin ürettiği video, görüntü veya ses gibi nesnelerde gizlenmek istenen verinin saklanmasına damgalama (Watermarking), karakteristik bir özelliğinin veya seri numarasının herhangi bir nesneye gizlenmesine parmak izi (finger print) adı verilmektedir. Damgalama ve parmak izi yöntemleri ile yasa dışı işlerin olmasını engellemek için ve yasal süreçlere telif hakları kurallarının çiğnenmesini engellemek için kullanılmaktadır. Bu yöntemler sayesinde bir bilgiyi herhangi bir şekilde gizleme işlemi yaparak, bir yere iletmek yerine verilerin sahiplik haklarının veya çoğaltılma izinlerinin korunması sağlanmış hale getirilmiştir. Bu şekilde gizlenen verinin telif haklarının korunması sağlanmış olmaktadır.



Şekil 2. 1 Steganografi yöntemleri

Şekil 2.1 de, Steganografinin uygulandığı çeşitli kullanım ortamları gözükmemektedir. Metin Steganografisi, Lin vd. (2017) çalışmasına göre gizli metin mesajını, başka bir metin içinde saklı mesaj olarak gizleme veya orijinal gizli mesajla ilgili bir mesajı oluşturma mekanizmasıdır.

Metin Steganografi yöntemleri:

a) Formata dayalı (Format based): Alwabhani ve Elshoush (2018) çalışmasına göre bu yöntemde, söz ve cümlelerdeki mesajlar değiştirilmemektedir; Yalnızca özel karakterler, yani beyaz boşluk steganografisi kullanılarak sözcükler, satırlar ve paragraflar arasındaki boşluklarda değişiklikler yapılmaktadır.

b) Rastgele ve istatistiksel üretim yöntemleri (Random and statistical generation methods): Bhattacharyya vd. (2009) çalışmasına göre bu yöntemde, tam bir paragraf oluşturmak için fazladan bir karmaşıklık (zaman ve boşluk) eklenir; bu gizli mesaj asıl mesajının içine gizlenir.

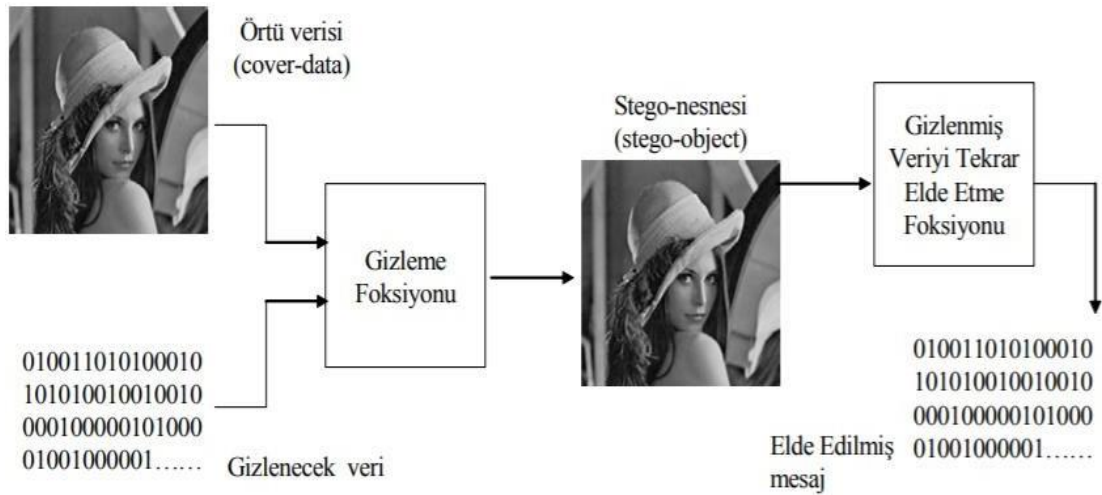
c) Dilbilimsel yöntem (Linguistic method): Dey vd. (2007) çalışmasına göre bu yöntem, gizlenecek mesajın dil yapısına (noktalama işaretleri) veya iki ana türü olan mesajı gizlemek için anlamsal kelimelere bağlı olarak başka bir mesajdaki veriyi gizlemek için kullanılır.

Video Steganografisi- (Mesajın videoda saklanması-Hiding in video), Ker (2005) çalışmasına göre 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.

Görüntü Steganografisi (Mesajın görüntüye saklanması-Hiding in image), Chen ve Lin (2006) çalışmasına göre Bir görüntünün içinde gizli bir mesaj göndermek amaçlı kullanılmak anlamına gelir.

Şahin, Buluş ve Sakallı (2006) çalışmasına göre Görüntü steganografik sistem Şekil 2.2’de gösterilmektedir. Veri gizlemek isteyen kullanıcı gizleme fonksiyonu yöntemini kullanarak steganogram oluşturmuştur.

Örtü verisi ve gizlenecek veri birleştirilerek gizleme fonksiyonu yöntemi ile stego nesnesi içerisine gizlenmiştir. Daha ayrıntılı anlatmak gerekirse, Gizleme fonksiyonu, verinin gizleneceği iletilici bir alan ve gizlenmek istenen bir veri olmak üzere iki parametreden oluşmaktadır.



Şekil 2. 2 Steganografik sistem

Görüntü steganografide, verilerin görüntü sistemleri içerisine gizlenmesi için çeşitli steganografi yöntemleri bulunmaktadır. Şekil 2.2’de kullanılan yöntemler:

a) En önemsiz bite ekleme yöntemi (Least Significant Bit Insertion Methods), uygulaması basit ve en yaygın yöntemdir. Bu yöntemin dikkatlice kullanılması gerekir. Dikkatli kullanılmaması durumunda veri kayıpları oluşmaktadır. Bu yöntemde; resmin her pikseline ait her byte’nın en önemsiz bitindeki son biti değiştirilerek bu değiştirilen bitin yerine gizlenmek istenen verinin bitleri sırasıyla yerleştirilmektedir. Değişimler insanlar tarafından farkedilememektedir. Bunun nedeni, görüntüde bulunan her bir sekiz bitin maksimum bir biti değiştirildiğinden ve herhangi bir değiştirme olmuş ise de değişiklik yapılan bitin en az anlamlı biti olmasından kaynaklanmaktadır. Son bite ekleme işlemi resmin başından veya sonundan sıralı bir şekilde olabileceği gibi, bir rasgele fonksiyon üretici (random function generator) kullanılarak da piksel üzerinde değişiklik yapılarak gerçekleştirilebilmektedir.

0-255 arasında 1 byte gri-seviye (gray-scale) görüntüler mevcuttur. Renkli dijital görüntüler 8 bit veya 24 bit olabilmektedir.

24 bit görüntüler

24 bitlik bir görüntü her bir pixel başına 3 byte kullanmaktadır. Her bir pixel için renk üç ana renkten elde edilmektedir. Kırmızı (red), Yeşil (green), Mavi (blue). Son biti değiştirmek şartıyla her bir pixel' de 3 bitlik bilgi saklayabiliriz. Eğer daha fazla sayıda bilgi gizlemek istiyorsak, gizlenmek istenen mesajı resmin içine gizlemeden önce sıkıştırırsak başarılı oluruz.

Günümüze geldiğimizde cep telefonlarından çektiğimiz 1600 * 1200 çözünürlükteki herhangi bir resmin içerisine 2 Megabayta kadar veri saklanabilmektedir.

Örnek vermek gerekirse, herhangi bir resmi veri editörüne verip resmin her bir byte 'ına 3 rakamı ile "Lojik AND" işlemi yaptırırsak. Baktığımızda siyah görüntü ile karşılaşırız. Daha sonra bu görüntüyü bir resim editörüne götürdüğümüzde resmin parlaklık değerini 85 katına çıkarttığımızda gizlenen asıl resmi görmüş oluruz.

8 bit görüntüler

8 bitlik bir görüntü de ise her bir pixel başına 1 byte kullanmaktadır. Renk sınırlamasından ötürü 8 bitlik görüntüler iyi bir sonuç vermemektedirler. Saklanması gereken bilgi, saklama yapılacak ortamı değiştirmeyecek şekilde dikkatlice bir şekilde seçilmelidir. Son bite ekleme işlemi yapıldığında, orijinal görüntüdeki renk girişleri göstergeleri değişmektedir. Bu görüntülerde beyaz, kırmızı, mavi ve yeşil olmak üzere 4 renk kullanılmaktadır.

Gri seviyeli görüntüler ve 0 ile 255 arasında tam sayılar elde edilebilmektedirler. 0 ile 255 sayıları arasındaki değerler gri renktedirler. Bu nedenden dolayı bir resme ait olan tam sayı "gri ton seviye" (gray level) olarak adlandırılmaktadır.

İkili sayı sistemine göre 10110111 sayısını ele alındığında, bu sayı onluk düzende 183 sayısının karşılığıdır. Sondaki bit' in 1 veya 0 olması bu değeri çok fazla değiştirmeyecektir. Sondaki bit değerimiz eğer 0 olsaydı bu değer 182 olacak ve renk üzerinde gözle görülecek büyük bir değişikliğe neden olmayacaktır.

b) Maskeleye ve filtreleme yöntemi (Masking and Filtering), teknikleri çoğunlukla

24 bit ve gri-seviye görüntüler de işaretleme ve filigran işlemi uygulanmaktadır. İşaretleme ya da filigran teknikleri sıkça uygulanmaktadır. Bu nedenle, görüntünün değişmesi mümkün değildir. Ayrıca Teknik açıdan filigranlar steganografik biçim değillerdir.

c) Algoritmalar ve dönüşümler yöntemi (Masking and Filtering), Bilgi gizlemek için kolay ve hızlı yöntem olarak Son bite ekleme yöntemi kullanılmaktadır. Ancak kayıplı sıkıştırmalar nedeniyle bilgiler zarar görmektedir.

Yüksek kalitede olan resimler sıkıştırılarak mesela jpeg formatlı bir resim ile internet aracılığıyla iletilmesi daha uygundur. Bu ihtiyaç sebebi ile gizlenen bilginin yok olmaması için ve görüntünün sıkıştırılmasını sağlayan bazı yöntemler ve steganografik araçlar bulunmuştur.

Sıkıştırma ve bilgi gizleme işlemlerini yapan formatlar aşağıdadır;

- Stego-Dos
- Jpeg- jsteg
- SureSign
- Picture-Mark
- S-Tools

Ses Steganografisi (Mesajın ses içine saklanması-Hiding in audio), Bu teknik, örneğin bir yazar hakkındaki bilgileri gizlemek gibi ses filigranı için kullanılır. Dey ve Abraham ve Sanyal (2007) çalışmasına göre Ses dosyasına ve gizleme mekanizmalarına bağlı olarak, ses steganografisinin LSB Kodlaması, Eşlik Kodlaması, Faz Kodlaması, Yayılı Spektrum ve Yankı Gizleme gibi birçok türü vardır.

Bahsedilen steganografi kullanım ortamları içinde verileri gizlemek için en yaygın kullanılan teknik uzamsal teknikler içinde olan LSB yöntemidir. Chaudhary (2020) çalışmasına göre Her pikselin en önemsiz bitini gizlenecek mesajın bitleriyle değiştirerek bir görüntünün içinde mesajların gizlendiği LSB steganografi tekniğidir. Chan (2009) çalışmasına göre 24 bit renkli bir görüntü kullanırken, kırmızı, yeşil ve mavi renklerin her birinden bir bit bileşen kullanılabilir, böylece her pikselde toplam

3 bit depolanabilir. Örnek verirse, Bu yöntem ile ses düzeyindeki deęişiklikler kulađımızla algılayamayacađımız seviyededir. Fridrich ve Goljan (2004) alıřmasına göre İnsan kulađının duymayacađı 20.000 Hz. üzerindeki frekanslar ayarlanarak mesajlar gizlenir.

Bu alıřmada da mesajların gizlenme ortamı olarak video seilmiřtir. Gizli bir mesajı bir video erevelerinin iine gizlemek iin uygun bir tařıyıcı video gereklidir. Bu alıřmada ayrıca kırmızı, mavi ve yeřil renklerin en dūřük deđerlikli sırası ile 3 biti, 3 biti ve 2 biti kullanılarak bir piksele 1 baytlık bilgi saklanabilmiřtir.

LSB(Least Significant Bit)

En Önemsiz Bite ekleme yöntemi (LSB) en çok tercih edilen ve uygulaması da basit steganografi yöntemidir. Gizli mesajın bitlerinin örtü imgenin piksellerin en önemsiz bitiyle yer değiştirilmesidir. Resmin satır veya sütunlarına mesajın bitleri gizlenebilir bu durumda mesajın geri elde edilmesi daha kolay olacaktır. LSB yönteminin temelinde olan piksellere birçok teknik uygulanabilir.

	Pikselin	Renk Değerinin
	Renk Değeri	İkilik Sistemdeki
		Karşılığı
Orijinal Piksel	158	1001110
Veri	159	1001111
gömülmüş		
Piksel		

Şekil 2. 3 LSB yöntemi ile veri gizlemesi

LSB yöntemi ile görsel kalite ve veri gizleme kapasiteleri elde edilmektedir. Bu yöntemin saldırılara karşı dayanıksız olması en büyük dezavantajıdır. Ek olarak saldırılara karşı dayanıksız hem de imge kimliklendirme için yeterli derecede kırılgan olmaması da ek dezavantajlarıdır. Bu yöntemin gizli veri olup olmadığını anlamaya yarayan saldırı yöntemleri için bazı yöntemler geliştirilmiştir. (Fridrich ve Goljan 2004; Selvaraj ve Varatharajan 2018) veri gizlemek için LSB yöntemi kullanılarak her pikselin en anlamsız bitleri değiştirilir. Veri gizleme işlemi tamamlandıktan sonra, gizli mesaj en anlamsız bit veya bitlerde gizlenmektedir. (May 1976; WikiPedia 2021). LSB yöntemi ile veri gizleme örneği Şekil 2. 4’de verilmiştir.

3.MATERYAL VE METOT

3.1 Kaos Teorisi ve Lojistik Harita

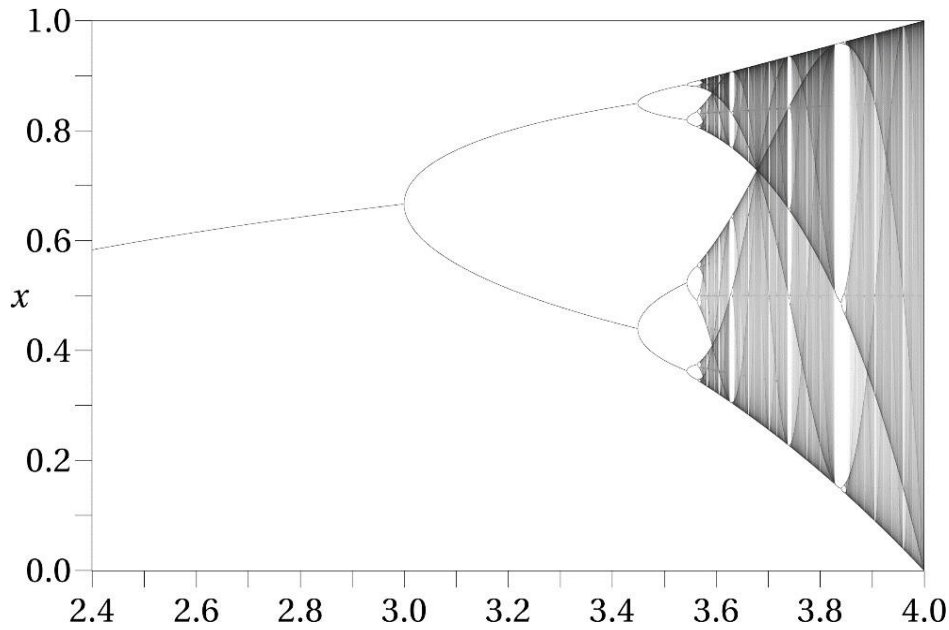
Tunçer (2016) çalışmasına göre Kaotik sistemler, doğrusal olmayan dinamik sistemlerin basit bir alt türüdür. Çok az etkileşimli parçalar içerebilirler ve bunlar çok basit kuralları takip edebilir, ancak bu sistemlerin tümü, başlangıç koşullarına çok hassas bir bağımlılığa sahiptirler. Belirleyici basitliklerine rağmen, zamanla bu sistemler tamamen tahmin edilemez ve farklı (kaotik) davranışlar üretebilir. Kaos teorisi sonuçları tahmin edilemeyen sistemleri açıklayan bilimsel bir ilkedir. Genel anlamda 1980'li yıllarda araştırılmıştır. Bir sigara dumanının havada yaptığı şekiller düzensiz ve bağımsız değildir. Sigaranın bu dinamikleri ortamdaki birçok etkene ve parametreye bağlıdır. Ancak bu parametre ve bilgiler çok fazladır ve bunları inceleyip net olarak bir kanıya varmak imkânsızdır. Sigara dumanının şeklini bulunan ortamdaki rüzgâr, sıcaklık, basınç gibi fiziksel büyüklükler etkileyebilir ve bu faktörlerin birbirine bağlı olabileceği de hesaba katıldığında durum tahmin edilemeyen bir hale gelir. Kaosun aslında hayatın her safhasında yer aldığı ve zincirleme olarak hayatta var olan tüm olguların birbirini zincirleme etkilediği düşünülmektedir. İlk olarak 1963 yılında hava durumu deterministik periyodik olmayan akışlarla ifade edilmeye çalışılmıştır. Bu hesaplarda ilk olarak 0,506127 ondalık sayısı kullanılmıştır ve daha sonra 0,506 sayısı sisteme giriş olarak verilmiştir. Seçilen bu iki sayı arasında binde bir oranında bir fark olmasına rağmen elde edilen sonuçlar arasında çok büyük farklılık meydana gelmiştir. 1972 yılında kaotik sistemlerin ortaya çıkmasında etkili olan Edward Lorenz'in ortaya attığı kelebek etkisi teorisine göre Afrika'da kanat çırpın bir kelebeğin, Amerika'da fırtına oluşturabileceği belirtilmiştir. Kelebek etkisi, bir sistemdeki başlangıç verilerinin çok küçük miktardaki değişimi sonucu, tahmin edilemeyen ve çok büyük değişikliklerin meydana gelmesi olarak tanımlanmıştır. Kaotik sistemlerin belirli bir frekans aralığında bulunduğu ve bu sınırlar içerisinde hareketlerinin belirlenemez olduğu Lorenz tarafından saptanmıştır.

Kaotik sistemleri, belirli bir alana çeken bu yapılara kaotik çekerler adı verilmektedir. Bu çekerlere bakıldığında bu çekerleri meydana getiren eğrilerin, belirli sayıdaki parametreler dizisinin, zaman düzleminde hiçbir zaman iki kez aynı rotayı izlemediği ve bu rotalar arasında kesinlikle küçük de olsa bir farklılık olduğu görülmüştür. Çekerlerin oluşturduğu eğrilerin bu özelliğinden dolayı fraktal yapıda olduğu söylenebilir. Kaotik sistemler görüntü şifreleme uygulamalarında oldukça yoğun kullanılmaktadır. Bilinen kaotik sistemlerin kullanıldığı başarımlar ve güvenlik bakımından oldukça iyi sonuçlar elde edildiği 4 görülmektedir. Ayrıca birden fazla kaotik sistem kullanılması, bu sistemlerin başlangıç değerlerine hassas bağıllığı ve şifrelemede kullanılan parametrelerin fazla olması güvenlik seviyesini oldukça artırmaktadır. Bu sayede şifrelenen görüntünün istenmeyen şahıslar tarafından ele geçirilmesi, şifrelemede kullanılan parametreleri bilmediği takdirde, neredeyse imkânsız hale gelmektedir. Kaotik sistemler, ayrık zamanlı ve sürekli zamanlı olmak üzere ikiye ayrılmaktadır. Diferansiyel denklemlerden meydana gelen kaotik sistemlerin boyutu, yani denklem sayısı arttıkça, parametrelerin ve başlangıç değerlerinin sayısı da artmaktadır. Artan parametre ve başlangıç değerlerine bağlı olarak bilinmeyen değişken sayısını da artıracaktır. Şifreleme ve şifre çözme işlemlerinde kullanılan kaotik sistemlerde bilinmeyen değerlerin fazla olması üçüncü bir şahıs tarafından anahtarın veya şifrelenen bilgilerin ele geçirilmesini çok zor hale getirecektir. Ayrıca, parametreler ve başlangıç değerlerinin algoritmada kullanıldığı yerler de önemlidir. Denklem sayısı şifrelemede karıştırma ve yayılma özelliklerini artırır, fakat şifreleme hızını negatif yönde etkileyebilir. Ayrıca veri güvenliği ve kriptoloji gibi alanlarda yeni olan karmaşık kaotik sistemlerin kullanılmasının çok daha önemli olduğunu vurgulamaktadır. Görüntü şifrelemede kaotik sistemlerin kullanılması, sağladığı bazı üstünlüklerden ve analiz yöntemlerine karşı gösterdiği yüksek dayanıklılıktan kaynaklanmaktadır. Bu analizler anahtar güvenliği, histogram analizi, anahtar hassaslığı, görüntüdeki bitişik piksellerin birbiri ile olan ilişki katsayısı, bilginin düzensizlik analizi, şifreleme ve şifre çözme hızıdır. Bu sayede, yapılan her analize karşı doğrudan daha başarılı olduğu söylenemese de genel anlamda kullanılan geleneksel simetrik ve asimetrik şifreleme algoritmalarına karşı üstünlük sağladığı görülmektedir.

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 May 1976 tarafından 1976 tarihli bir makalede popüler hale getirilmiştir. Lojistik harita denklemi Denklem (3.1) de verilmiştir. Bu şekilde adlandırılır çünkü herhangi bir zaman adımındaki nüfus değerini bir sonraki adımdaki değerine eşler:

$$x_{i+1} = \lambda * x_i * (1 - x_i) \quad (3.1)$$



Şekil 3. 1 Lojistik harita çatallanma gösterimi: Yatay eksen λ , düşey eksen x değerleridir. (WikiPedia 2021)

x_{i+1} kaotik sistemin bir sonraki değeri, bu çalışmada λ için, [3.9- 4] arası sistem daha çok kaotik davrandığı (Şekil 3.1) 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 (Yayla 2019).

Algoritma 1 Veri Saklama Algoritması

INPUT: input_video, input_text

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

Algoritma 2 Veri Çıkartma Algoritması

INPUT: Stego_video, text_size

30. **INITIAL ASSIGNMENTS:** $x = 0.418$; $\lambda = 3.995$; $\alpha = 10^{14}$; text_size = 20000;

31. **for** j=1 to text_size do

32. S = frame_count * video_height * video_width;

33. $x = \lambda * x * (1 - x)$;

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_height)) / video_width);

37. n_width = floor(mod(value,(video_width * video_height)) / 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)==frame_pointer),:);

43. hided_size = size(hided_in_frame);

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)

Kasapbaşı ve Elmasry (2018) çalışmaya göre Sıkıştırılmış ve orijinal görüntü arasındaki kümülatif kare hatasını temsil eder. Anlaşılır şekilde açıklamak gerekirse, ortalama kare hatası, bir regresyon eğrisinin bir noktaya ne kadar yakın olduğunu anlatmaktadır. MSE, her zaman pozitifdir. Ve performans ölçer. Sıfıra yakın olan değerler çok daha iyi performans gösterdiği anlaşılmaktadır. Denklem (3.2) de gösterilmiştir.

$$\frac{1}{MN} \sum_{j=1}^M \sum_{k=1}^N (X_{j,k} - X'_{j,k})^2 \quad (3.2)$$

3.2.2 PSNR (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. Kasapbaşı ve Elmasry (2018) çalışmaya göre PSNR ne kadar yüksekse, sıkıştırılmış veya yeniden yapılandırılmış görüntünün kalitesi o kadar iyidir. Denklem (3.3) te gösterilmiştir.

$$PSNR = 10 \log \frac{(2^n - 1)^2}{MSE} = 10 \log \frac{255^2}{MSE} \quad (3.3)$$

3.2.3 SNR (Signal Noise Ratio)

Bir sinyalin seviyesini arka planda bulunan gürültü seviyesiyle karşılaştıran bir ölçüm yöntemidir. SNR, sinyal gücünün, gürültü gücüne oranıdır, çoğunlukla desibel cinsi ile ifade edilmektedir. 0 Db' den büyük bir oran gürültüden daha fazla sinyal olduğunu göstermektedir. Denklem (3.4) de gösterilmiştir (Wikipedia 2021).

$$SNR = \frac{\sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f'(x,y)^2}{\sum_{x=0}^{M-1} \sum_{y=0}^{N-1} [f(x,y) - f'(x,y)]^2} \quad (3.4)$$

3.2.4 Entropi

Güvenoğlu ve Razbonyalı (2019) çalışmaya göre Entropi, bir sistemdeki rastgele oluşum ve bozukluk olarak tanımlanır. P (mi) bir görüntüdeki her bir pikselin olasılık durumlarını temsil eder ve M × N toplam piksel sayısıdır. Gri seviyeli bir görüntüde (m0 = 0, m1 = 1, ... m255 = 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 (3.5) te gösterilmiştir.

$$H(m) = \sum_{i=0}^{M*N-1} P(m_i) \log_2 \frac{1}{P(m_i)} \quad (3.5)$$

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. Dalal ve Juneja (2019) çalışmasına göre 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 (3.6) de gösterilmiştir.

$$SSIM(x,y)=\frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \quad (3.6)$$

μ_x =x in ortalaması

μ_y = y nin ortalaması

σ^2 = x in varyansı

σ_y^2 = y nin varyansı

σ_{xy} = x ve y nin kovaryansı

$c_1 = (k_1L)^2$, $c_2 = (k_2L)^2$ =Zayıf payda ile bölünmeyi dengelemek için iki değişken

$k_1=0.01$; $k_2=0.03$

4.BULGULAR VE TARTIŞMA

Bu çalışmada üretilen gizli verilerin saklanması için sıkıştırılmamış biçimde olan 0.09sn uzunluğunda bir avi video seçilmiştir. Çeşitli uzunluklarda metinler hazırlanarak Algoritma 1'deki yöntemle 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.

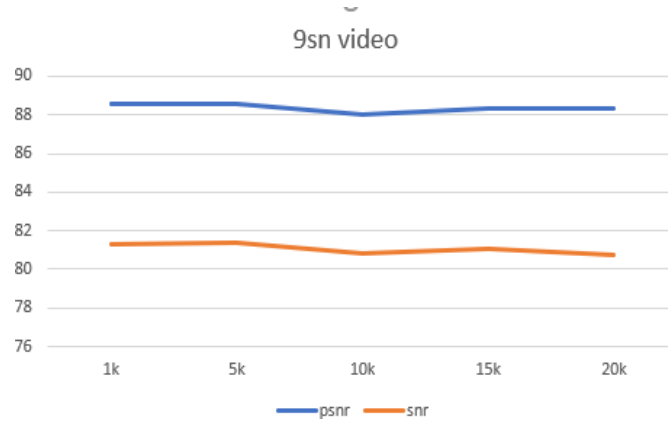
Çizelge 4. 1 0.09sn Video içinde saklanan verilerin Kalite Ölçümleri

Metin Büyükliği	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

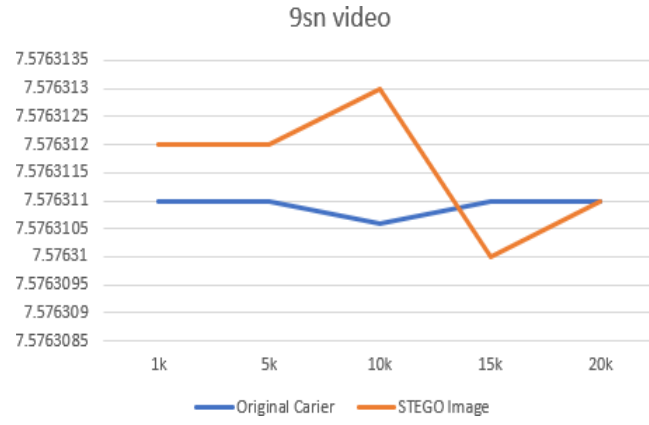
Çizelge 4.1 de çeşitli büyüklükteki verilerin gizlenmesi durumunda oluşacak kalite farkını göstermek için PSNR (Peak Signal Noise Ration), SNR(Signal Noise Ratio), Entropi, SSMI (Structural Similarity) ve MSE (Mean Squared Error) dan yararlanılmıştır.

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 gözükmemektedir. Bu ölçüm değerlerinden çıkarılabilecek sonuç, video kalitesinde bir değişiklik olmadığı bu sebeple gizli mesajın anlaşılamayacağı söylenebilir.

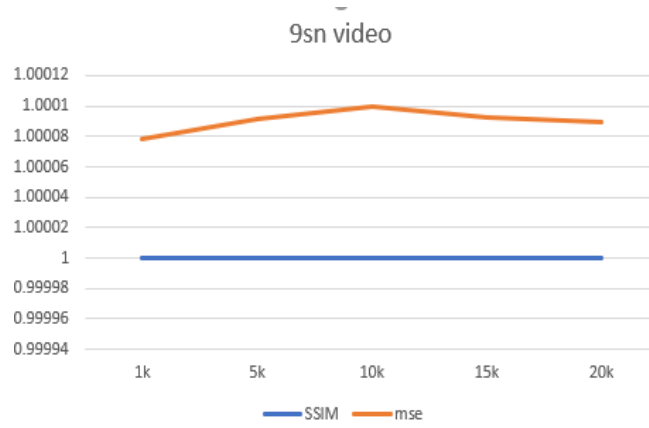
Şekil 4.1 de farklı büyüklükteki gizli mesaj büyüklüklerine göre ölçüm değerleri grafik olarak gösterilmiştir. Burada da izlendiği gibi değerler istenilen aralıktadırlar.



(a)

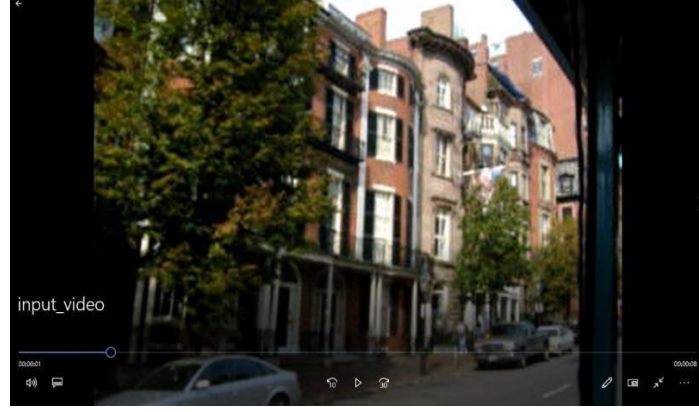


(b)

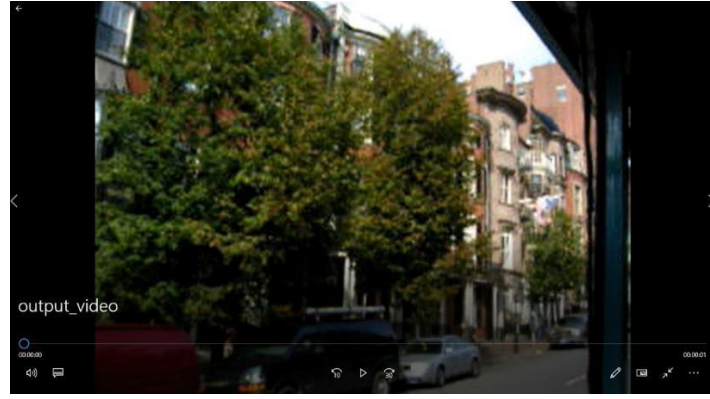


(c)

Şekil 4. 1 (a) PSNR SNR (b) Orijinal ve Stego görüntü Entropi (c) SSIM MSE



(d)



(e)

Şekil 4. 2 (d) input avi video görüntüsü (e) output avi video görüntüsü



(f)



(g)

Şekil 4. 3 (f) orjinal frame1 görüntüsü (g) changed frame1görüntüsü

Şekil 4.2 ve Şekil 4.3'te çalışmamızda kullandığımız input avi video, output avi video örnek olması açısından ise oluşturulan frameler içinden bir adet frame1 görüntülerinden orjinal frame1 ve changed frame1görüntüleri gösterilmiştir. Buradan da izleneceği gibi görüntü kalitesindeki farklar gözle görünmeyecek kadar azdır.

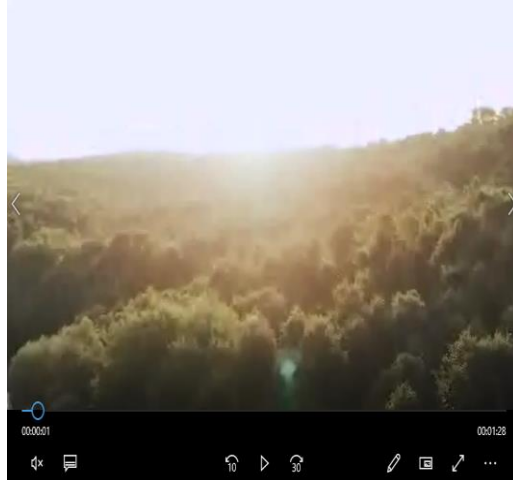
Ek olarak sıkıştırılmamış biçimde olan 1dk 29sn uzunluğunda bir avi video seçilmiştir. Çeşitli uzunluklarda metinler hazırlanarak Algoritma 1'deki yönteme göre video içine saklanmıştır. Metin uzunluğu 1KByte, 5KByte, 10KByte ve 20KByte olacak şekilde testler yapılmıştır.

Çizelge 4. 2 1.29sn Video içinde saklanan verilerin Kalite Ölçümleri

Metin Büyükülüğü	PSNR	SNR	Orijinal Entropi	STEGO Entropi	SSIM	MSE
1k	90.9638	80.6044	6.218868	6.218869	1	0
5k	90.9637	80.6042	6.218868	6.218869	1	0
10k	90.6015	80.5844	6.218868	6.218869	1	0
15k	90.6088	80.5442	6.218868	6.218869	1	0
20k	90.6125	80.4518	6.218868	6.218869	1	0

Çizelge 4.2 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.

Çizelge 4.2 de izlendiği gibi yüksek SNR, PSNR değerleri elde edilmiştir. Entropi de 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 Sıfıra yakın veya eşit olan değerler çok daha iyi performans gösterdiği anlaşılmaktadır. Burada da performansın başarılı olduğu görünmektedir. Bu ölçüm değerlerinden çıkarılabilecek sonuç, video kalitesinde bir değişiklik olmadığı bu sebeple gizli mesajın anlaşılamayacağı söylenebilir.



(d)



(e)

Şekil 4. 4 (d) 1.29sn input avi video görüntüsü (e) 1.29sn output avi video



(f)



(g)

Şekil 4. 5 (f) 1.29sn orjinal frame1 görüntüsü (g) 1.29sn changed frame1

Şekil 4.4 ve Şekil 4.5 'te çalışmamızda kullandığımız 1.29sn lik video ya ait input avi video, output avi video örnek olması açısından oluşturulan frameler içinden alınan bir adet orjinal frame1 ve changed frame1 görüntüleri gösterilmiştir. Buradan da gözlemleneceği üzere görüntü kalitesindeki farklar gözle görünmeyecek kadar azdır.

Çizelge 4. 3 Benzer çalışmaların sonuçları

Referans	MSE	PSNR	Açıklama
Deshmukh ve Rahangdale (2014) çalışmasına göre	0.1999	55.1217	Videoya 623 karakter LSB yöntemi ile saklanmıştır.
Kar ve Aman ve Mandal e Bhattacharya (2017) çalışmasına göre	[0-0.3]	[35-74]	Thinkerbelle Kaotik harita ile piksel seçimi, LSB yöntemi ile Video içine metin gizleme
Gambhir ve Mandal (2020) çalışmasına göre	0.01550	59.2377	Kaotik seçimli OpenMP uygulamalı Görüntü steganografi uygulaması
Tanveer ve Ashish (2020) çalışmasına göre	-	[43-64]	Arnold Haritası kullanılarak, Frekans Domaininden DCT, Video içine görüntü saklama
WikiPedia (2021)	-	78.84	Video Stegonografisi (Resim)
Manisha1 ve Sharmila2 (2019) çalışmasına göre	-	36.8	HD görüntüye, 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

Benzer çalışma sonuçları kıyaslanmak istenmiş, diğer çalışmaların sonuçları ile karşılaştırma yapılmak istendiğinde Çizelge 4.3 oluşturulmuştur. Karşılaştırılan çalışmalardaki kullanılan taşıyıcı videolar aynı olmadığı için sonuçları kendi içinde değerlendirilmesi daha doğru olacaktır. Bu çizelge de benzer metriklerin sonuçları kıyaslanmaktadır. Çalışmamızda kalite düşüşü olmamıştır ve çok yüksek PSNR değerleri elde edilmiştir. Bu sonuçlara dayanarak Gizli mesajın asla anlaşılamayacağı sonucuna varılmaktadır. Göz kontrolünde ise yeni stego video da gizli veri olduğu asla anlaşılmamaktadır.

5. SONUÇLAR VE ÖNERİLER

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 Çizelge 4.1 ve Çizelge 4.2 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 anlaşılacak 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

- Abdulla, AA., 2015. Exploiting similarities between secret and cover images for improved embedding efficiency and security in digital steganography, The University of Buckingham, Tez, 235p, Birleşik Krallık.
- Alwabhani, S. M. H., Elshoush, H.T., 2018. Chaos-Based Audio Steganography and Cryptography Using LSB Method and One-Time Pad, B.S. Abdur Rahman University Chennai, 768p, Hindistan.
- 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, 200p, Hong Kong, Çin.
- Chan, C-S., 2009. On using LSB matching function for data hiding in pixels. Fundamenta Informaticae, Department of Information Science and Applications Asia University Wufeng, 59p, Tayvan.
- Chan, Y-T., Lin, G-S., 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, Da-Yeh University, 357, Shan-Jiau Rd., Da-Tsuen, Changhua, 515p, Tayvan, R.O.C.
- Chaudhary, P., 2020. Novel Image Encryption Method Base on LSB Technique and AES Algorithm, Jaypee Institute of Information Technology Noida , 546p, Hindistan.
- Chen, P-Y., Lin, H-J., 2006. A DWT base approach for image steganography. International Journal of Applied Science and Engineering, National Changhua University of Education, 290p, Shi-Da Road, Changhua City 500, Tayvan, R.O.C.
- Dalal, M., Juneja, M. 2019. A robust and imperceptible steganography technique for SD and HD videos, Panjab University, Chandigarh, 5788p, Hindistan.
- Deshmukh, P. R., Rahangdale, B., 2014. Data Hiding using Video Steganography, Sipna COET, Amravati, 860p, Hindistan.
- Dey S., Abraham, A., Sanyal, S., 2007. An LSB Data Hiding Technique Using Prime Number. Third International Symposium on Information Assurance and Security, Third International Symposium on, 285p, Manchester, UK.
- 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, 165p, Kaohsiung, Tayvan.
- 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, The International Society of Optical Engineering, 34p, San Jose.

Gambhir, G., Mandal, J.K., 2020. Multicore implementation and performance analysis of a chaos based LSB steganography technique. Université de Nantes, CNRS UMR ,6164p, Nantes, Fransa.

Güvenöğlu, E., Razbonyalı, C., 2019. The Creation of Maze in Order to Hide Data, and the Proposal of Method Based on AES Data Encryption Algorithm, Research Paper, Maltepe University,679p, Istanbul.

Kasapbaşı, MC., Elmasry, W., 2018. New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check, Istanbul Commerce University, 68p, Istanbul.

Katzenbeisser, S. & Petitcolas, F.A.P.,1999. Information Hiding Techniques for Steganography and Digital Watermarking, George Mason University,114p, Fairfax.

Ker, AD., 2005. A general framework for structural steganaly of LSB replacement. International Workshop on information hiding, Oxford University,315p, İngiltere.

Kar, N., Aman, M. A. A. A., Mandal, K. and Bhattacharya, B., 2017. Chaos- based video steganography, 162p, Amman.

Ker, AD., Bohme, R ., 2008. Revisiting weighted stego-image steganalysis. Proc. SPIE Electronic Imaging Security Forensics Steganography and Watermarking of Multimedia Content ,Oxford University, 117p, İngiltere.

Ker, AD., 2005. Improved detection of LSB steganography in grayscale image. International Workshop on information hiding. Springer, Oxford University Computing Laboratory Oxford, 115p, İngiltere.

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 , Taiwan Information Security Center, Academia Sinica, Taipei, 211p, Tayvan.

Luo, W., Huang, F., Huang, J., 2010. Edge adaptive image steganography based on LSB matching revisited. IEEE Transactions on Information Forensic and Security, Sun Yat-Sen Univ., Guangzhou, 214p, Çin.

Manisha¹, S.,& Sharmila², T. S., 2019. A two-level secure data hiding algorithm for video Steganography, SSN College of Engineering, Chennai, Tamil Nadu, 542p, Hindistan.

May, R., 1976. Simple mathematical models with very complicated dynamics,

Princeton University,459p, Princeton.

Selvaraj, P., Varatharajan, R., 2018. Whirlpool Algorithm with Hash Function Based Watermarking Algorithm for the Secured Transmission of Digital Medical Images, United States Military Academy, Batı Noktası NY 10996, 67p, USA.

Şahin, A., Buluş, E., Sakallı, M.T., 2006. 24-Bit Renkli Resimler Üzerine en Önemsiz Bite Ekleme Yöntemini Kullanarak Bilgi Gizleme, Trakya Üniversitesi, 342p,Edirne.

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., Image team -site of Nantes, Nantes,616p, Fransa.

Tunçer, S., 2016. Kaotik Sistem Tabanlı Görüntü Şifreleme, Maltepe.

WikiPedia, Logistic Map, 2021, Erişim Tarihi: 08.01.2021. https://en.wikipedia.org/wiki/Logistic_map

WikiPedia, Logistic Map, 2021, Erişim Tarihi: 08.01.2021. <http://www.halic.edu.tr>

Wikipedia, 2021, Erişim Tarihi: 08.01.2021. https://tr.wikipedia.org/wiki/Sinyal_Gürültü_Oranı

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

EKLER

EK A. Uygulama Kodları

EK A. Uygulama Algoritmaları

Algoritma 1 Veri Saklama Algoritması

INPUT: input_video, input_text

```
4. INITIAL ASSIGNMENTS:  $x = 0.418$ ;  $\lambda = 3.995$ ;  $\alpha = 10^{14}$ ;  
5. for j=1 to text_size do  
6.   S = frame_count *  
video_height * video_width; 4.  
    $x = \lambda * x * (1 - x)$ ;  
13.  value = j + floor ( mod((  $\alpha * x$ ), S));  
14.  n_frame = floor(value / (video_width * video_height));  
15.  n_height = floor(mod(value,(video_width * video_height)) /  
video_width);  
16.  n_width = floor(mod(value,(video_width * video_height)) /  
video_height);  
17.  pixel_values(j,:) = [n_frame n_height n_width f(j)];  
18. end for  
19. array_size = size(pixel_values,1);  
20. frame_pointer = 0;  
29. while hasFrame(vidObj)  
30.   frame_pointer=frame_pointer+1;  
31.   Extracted = pixel_values((pixel_values(:,1)==frame_pointer),:);  
32.   vidFrame = readFrame(vidObj);  
33.   fname=fullfile('path\orj_frames',strcat('frame-  
' ,num2str(frame_pointer),'.png'));  
34.   imwrite(vidFrame,fname);  
35.   if (size(Extracted,1) > 0)  
36.     vidFrame = hide_function(vidFrame,Extracted);  
37.     fname=fullfile(path\changed_  
frames',strcat('frame-  
' ,num2str(frame_pointer),'.png'));  
38.     imwrite(vidFrame,fname);  
39.   end if  
40.   writeVideo(videoOut,vidFrame);  
41. end while  
42. close(videoOut);  
43. status=1;  
44. OUTPUT: 1; (Stego Video
```

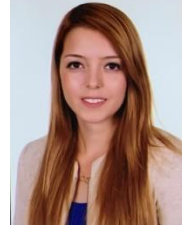
Algoritma 2 Veri Çıkartma Algoritması

INPUT: Stego_video, text_size

```
30. INITIAL ASSIGNMENTS:  $x = 0.418$ ;  $\lambda = 3.995$ ;  $\alpha = 10^{14}$ ; text_size = 20000;
34. for j=1 to text_size do
35.     S = frame_count *
video_height * video_width;
36.      $x = \lambda * x * (1 - x)$ ;
61.     value = j + floor ( mod(( alfa * x), S));
62.     n_frame =(value / (video_width * video_height));
63.     n_height = floor(mod(value,(video_width * video_height)) /
video_width);
64.     n_width = floor(mod(value,(video_width * video_height)) /
video_height);
65.     pixel_values(j,:) = [n_frame n_height n_width f(j)];
66. end for
67. while hasFrame(vidObj)
68.     frame_pointer=frame_pointer+1;
69.     hided_in_frame = pixel_values((pixel_values(:,1)==frame_pointer),:);
70.     hided_size = size(hided_in_frame);
71.     if (hided_size > 0)
72.         for c=1:hided_size
73.             i = hided_in_frame(c,2);
74.             j = hided_in_frame(c,3);
75.             index = hided_in_frame(c,4);
76.             r1=current_frame(i,j,1);
77.             r2=current_frame(i,j,2);
78.             r3=current_frame(i,j,3);
79.             R(index)=extract_text(r1,r2,r3);
80.         end for
81.     end if
82. end while
83. fid = fopen('out_text.txt','wb');
84. fwrite(fid,char(R),'char');
85. fclose(fid);
86. status=1;
OUTPUT: 1; (Video)
```

ÖZGEÇMİŞ

Adı Soyadı : Damla AKYÜZ
Doğum Yeri ve Yılı : PAZAR, 14/09/1991
Medeni Hali : (Evli)
Yabancı Dili : İngilizce
E-posta : damlas.senkul@gmail.com



Eğitim Durumu

Lise: : Ertuğrulgazi Anadolu Lisesi, 2009
Lisans : Trakya Üniversitesi, Mühendislik Fakültesi,
Bilgisayar Mühendisliği Bölümü, 2014
Yüksek Lisans : İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü,
Bilgisayar Mühendisliği Bölümü

Yayınları

Akyüz, D, Kasapbaşı, M.C. (2021). Yeni Kaotik Video Şifreleme Methodu. Haliç Üniversitesi Fen Bilimleri Dergisi tarafından kabul edilmiştir.