Trakya University Journal of Engineering Sciences
http://dergipark.gov.tr/tujes
ISSN 2147–0308 *Research Article / Araştırma Makalesi*

VİDEO DOSYALARI ÜZERİNDE LSB YÖNTEMİYLE BİLGİ GİZLEME İŞLEMİNİN SIRALI VEYA RASTGELE YAPILMASININ GÜVENLİĞE ETKİLERİNİN İNCELENMESİ

Egemen TEKKANAT[1], Andaç ŞAHİN MESUT[2]

[1] *Trakya Üniversitesi, Keşan Yusuf Çapraz Uygulamalı Bilimler Yüksekokulu, Bilişim Sistemleri ve Teknolojileri Bölümü, Keşan / Edirne / Türkiye*

[2] *Trakya Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Edirne / Türkiye*

Makale Künye Bilgisi: Tekkanat, E., Mesut, A.Ş. (2022). Video dosyaları üzerinde LSB Yöntemiyle Bilgi Gizleme İşleminin Sıralı veya Rastgele Yapılmasının Güvenliğe Etkilerinin İncelenmesi. *Trakya Üniversitesi Mühendislik Bilimleri Dergisi*, 23(1), 37-49.

Öne Çıkanlar

- Bilgi Gizleme ve Şifreleme teknikleri veri güvenliği için önemlidir.
- Veri gizleme farklı özellikteki dijital ortamlara uygulanarak veri güvenliği, telif hakkı, kimlik kanıtlama gibi işlevleri sağlamak amacıyla kullanılabilir.
- Video dosyalarında veri gizlemek için en sık kullanılan yöntemlerden olan LSB yöntemi sıralı veya rastgele uygulanabilir.

Makale Bilgileri

Makale Tarihçesi:

Geliş:
13 Mayıs 2022

Kabul:
6 Haziran 2022

Anahtar Kelimeler:

Video steganografi;
En önemsiz bite ekleme yöntemi;
Steganaliz

Öz

Teknolojinin hızlı gelişimi ile birlikte bilgi güvenliği kavramı önemli bir konu haline gelmiştir. Özellikle dijital ortamda gerçekleştirilen veri transferleri sırasında verilerin güvenliğini sağlayabilmek için Kriptoloji ve Steganografi kavramına ihtiyaç duyulmaktadır. Kriptoloji bilgiyi anlamsız hale getirmek için kullanılırken Steganografi var olan bilgiyi taşıyıcı dosyalar üzerine saklamak için kullanılmaktadır. Bu araştırmada video dosyaları üzerine LSB yöntemi kullanılarak sıralı ve rastgele bilgi gizleme işlemleri gerçekleştirilmiş ve analizleri yapılmıştır.

INVESTIGATION OF THE EFFECTS OF SEQUENTIAL OR RANDOM HIDING OF INFORMATION ON VIDEO FILES USING THE LSB METHOD ON SECURITY

Article Info

Article History:

Received:
May 13, 2022

Accepted:
June 6, 2022

Keywords:

Video Steganography;
LSB Insertion Method;
Steganalysis

Abstract

With the rapid development of technology, the concept of information security has become an important issue. The concept of Cryptology and Steganography is needed to ensure the security of data, especially during data transfers in digital environment. While cryptography is used to render information meaningless, Steganography is used to store existing information on carrier files. In this research, sequential and random information hiding processes were performed on video files by using the LSB method, and their analyzes were made.

*Sorumlu Yazar: egementekkanat@trakya.edu.tr

1. Giriş

Kişisel bilgilerin gizlenmesi ve gizli haberleşme insanlığın en eski dönemlerinden beri var olan bir kavramdır. Çağın gereksinimleri doğrultusunda insanoğlu çeşitli sebeplerden dolayı gizli haberleşme yöntemlerini tercih etmişlerdir. İnternet ve paralel teknolojik gelişmeler çağımızın en önemli getirilerindendir. Özellikle İletim hızının artması ile bilgisayar sistemlerinin güvenliği ve bilgi güvenliği konuları oldukça önem kazanmıştır. İnternetin birçok kişi tarafından kolayca erişilebilmesi nedeniyle metin, resim, ses, video vb. gibi birçok bilgi ve mesajlar içeren dosyaların ağ üzerinden paylaşımı önemli ölçüde artmıştır. Paylaşılan bu ortamların güvenliğini sağlayabilmek için bilgileri şifreleme ve bilgileri gizleme teknikleri güvenlik açıklarını kapatmak için geliştirilmiş ve uygulanmaya başlanmıştır.

Birbiri ile haberleşen kişiler arasındaki iletişime dışarıdan üçüncü kişiler tarafından erişilebilmekte ve bu süreç sırasında eriştiği verileri değiştirebilmektedir. Bu da haberleşme sürecinin hatalı olmasına sebep olabilmektedir. Bu süreçte bilgi güvenliği konusu oldukça ciddi bir konudur. Bilgilere erişip bunları değiştirebilme süreçlerine karşılık çeşitli koruma ve önleme mekanizmaları geliştirilmiştir. Şifreleme ve bilgi gizleme bu mekanizmalarının en önemli parçalarından birileridir.

Şifreleme gizlenecek verilerin anahtarlar yardımı ile anlaşılması zor hale getirilmesini ifade ederken bilgi gizleme ise bilgileri elde etmek isteyen üçüncü kişilerden bilgileri saklamak amacı ile kullanılmaktadır. Bu iki mekanizma başlı başına güvenlik sağlayabildikleri gibi birlikte kullanıldıklarında ise güvenlik özellikleri artmaktadır. Bu iki mekanizma birlikte kullanıldığında iletişim güvenli bir hale gelebilmektedir.

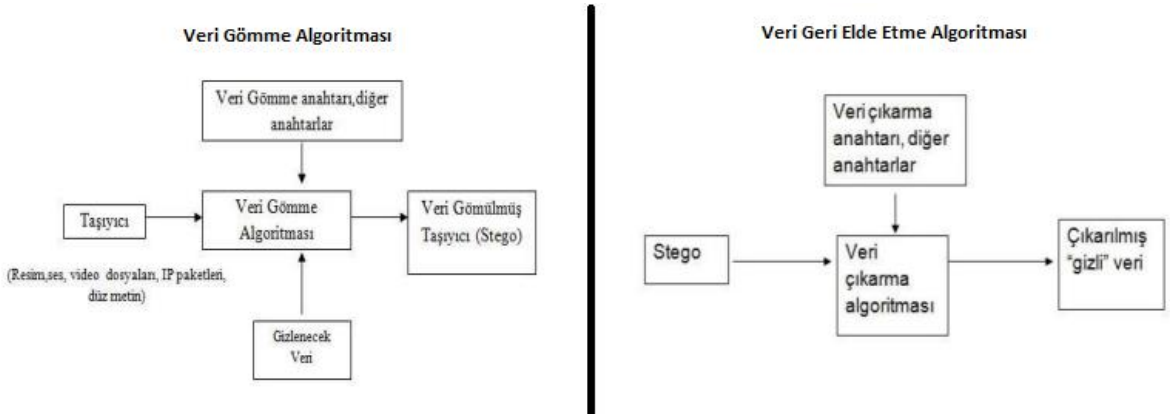
Bilgi gizleme birçok alt alandan oluşmaktadır. Bu sınıflandırma bilgi gizleme alanında yapılan ilk bilimsel toplantıda kabul edilmiştir (Pfitzmann B, 1996)

Bu çalışmada bilgi gizlemenin bir alt disiplini olan steganografi yöntemlerinin video dosyaları üzerinde uygulanması incelenmiştir. Hareketli görüntü dosyaları (video) üzerinde bilgi gizlemek amacıyla kullanılan LSB yöntemi incelenmiş ve bunun için bir uygulama geliştirilmiştir. Veri gizleme işlemleri sıralı ve rastgele şekilde yapılmış ve bunların etkinlikleri değerlendirilmiştir.

2. Steganografi

Temeli antik çağlara kadar dayanan eski bir bilgi gizleme sanatı olan Steganografi biliminin temel çıkış amacı, gizli haberleşmenin üçüncü kişiler tarafından fark edilmeden iletilmesidir. Steganografi iki parçadan oluşan Yunanca bir kelimedir. “Steganos” örtülü/gizli, “graphy” ise yazım/çizim anlamına gelmektedir (Cox, I. J., Miller, M. L., Bloom, J. A ,2000). Kelime kökeni Yunancadan gelmektedir ve tam olarak anlamı “örtülmüş yazı” demektir (Neil F.Johnson,1998). Steganografi bilgi gizlemenin bir alt dalıdır.

Steganografi tekniklerinde içine bilgi gizlenen ortama örtü verisi (cover-data) veya örtü nesnesi (cover-object) ve oluşan ortama ise stego-metin (stego-text) ya da stego-nesnesi (stego-object) denilmektedir. Bilginin saklanması işlemi ve aynı zamanda saklanan bilginin geri elde edilmesini zorlaştırmak adına bir stego-anahtarı kullanılmaktadır. (Hu, S. D. ,2011).



Şekil 1. Steganografik Sistem

Steganografi ses, metin, görüntü vb. ortamdaki verilerin korunması için kullanılan bir disiplin olarak tanımlanmaktadır. Metin Steganografide bilgi gizlemek için kullanılan ortam basılı ya da dijital ortamdaki metin dosyalarıdır. Metin dosyasındaki verileri gizlemek için farklı yöntemler kullanılabilir (Akyüz, D., & Kasapbaşı, M. C. 2021). Genellikle, bu yöntemlerin veri saklama kapasiteleri düşük seviyededir. Ayrıca metin dosyaları üzerindeki değişikliklerin kolay algılanabilmesi nedeniyle dikkatlice uygulanması gerekmektedir. Bu sebeple uygulanması zor bir veri gizleme şeklidir.

Resim Steganografi tekniğinde gizleme işleminde görüntü dosyaları kullanılmaktadır**.** Görüntü dosyaları iletim ortamlarında oldukça fazla kullanıldığı için ve iletimleri özellikle internet üzerinden kolay olduğu için steganografik sistemlerde en sık uygulandığı formatlardır. İletiminin kolay olmasının yanı sıra yaygın olarak kullanılmasını bir sebebi de kapasite özelliğidir (Avcı, E., Tuncer, T., & Ertam, F. , 2014).

Görüntü dosyaları üzerinde bilgi işleme sırasında kullanılan anahtar kavramı gizlenecek mesajın güvenilirliği sağlamaktadır. Kullanılan bu anahtar ile gizlenilmesini istediğimiz verinin gömülme noktaları tespit edilmektedir. Güvenirliliği sağlamak amacı ile kullanılan bu anahtar şifreleme amacı ile kullanılabilmektedir (Şahin Mesut A., Mesut A., Sakallı M.T.,2010).

Ses Steganografi tekniğinde ses dosyaları üzerinde bilgi gizleme işlemi yapılmaktadır**.** İnsan işitme sistemi frekans aralığı sebebi ile ses sinyalleri içine bilgi gizleme işlemi uygulanması uğraş gerektiren bir alandır (Şahin, A., 2007).

İnsan işitme sistemi sesleri 109:1'den büyük bir güç aralığında ve 103:1'den büyük bir frekans aralığında algılar. HAS (Human Auditory System)'in beyaz Gauss gürültüsüne (AWGN) duyarlılığı da yüksektir; bir ses dosyasındaki bu gürültü, ortam seviyesinin altında 70 dB kadar düşük tespit edilebilir (Nosrati, M., Karimi, R., & Hariri, M., 2012).

Ses Steganografinin dikkatli şekilde gerçekleştirilmesi gerekmektedir. Ses steganografide kullanılan yöntemler diğer alanlarda kullanılan yöntemlere göre daha karmaşıktır (Al-Othmani, A. Z., Manaf, A. A., & Zeki, A. M.,2012).

3. Video Steganografi

Video Steganografi, bir videonun içinde bazı gizli bilgileri gizleme işlemidir. Bu bilgilerin videoya eklenmesi, piksel rengindeki değişiklik ihmal edilebilir düzeyde olduğundan insan gözü tarafından tanınmaz.

Video steganografi resim steganografinin genişletilmiş hali gibidir. Farklı noktaları olarak ise video dosyası dinamiktir. Veri gizlenen resmi video içerisinde bulmak bu yüzden daha zordur. Video steganografide

daha fazla saldırı olanağı bulunmaktadır. Bunlar kayıplı sıkıştırma, çerçeve (frame) oranı değiştirme, format değişimi, video işleme sırasında çerçeve ekleme ve çıkarma gibi yöntemlerdir. Video dosyaları çok sayıda resim dosyasının birleştirilmiş hali olduğu için veri saklama kapasitesi daha fazladır.

Video steganografi yöntemleri sıkıştırılmış ve Sıkıştırılmamış (ham) videolar üzerinde uygulanabilir. Video üzerinde veri gizleme yapan algoritmalar gömme alanı açısından da iki şekilde uygulanır. Bunlar Mekânsal Alan teknikleri ve Alan dönüştürme teknikleridir (Hacımurtazaoğlu. M, 2022).

Sıkıştırılmamış videolar üzerinde uygulanan Düzensiz dikdörtgen bölümlemesi (Non - Uniform rectangular partition) yönteminde ana video içerisine sıkıştırılmamış bir video saklanması şeklindedir. Bu aşamada dikkat edilmesi gereken nokta ise gizlenecek video ile örtü videosunun aynı boyutlarda olmasıdır. Bu yöntemin uygulanmasında ayrıştırılan kodlar şifrelenerek örtü videosunda yer alan her karenin en önemsiz dört bitine saklanarak gerçekleştirilmektedir (Hu, S. D. ,2011).

Sıkıştırılmış videolar üzerinde uygulanan yöntemlerde veriler I çerçevesi alanına P, B alanlarındaki maksimum hareket vektörleri ve maksimum kare değişimiyle gömülebilir. En yüksek performans olarak ise AVC kodlama tekniği ile oluşturulan videolarda ulaşılmaktadır (Misman, C. ,2018).

Mekânsal Alan tekniklerinin en yaygın olarak kullanılanı En Önemsiz Bite Ekleme (Least Significant Bit Insertion – LSB) yöntemidir. Uygulanması en kolay ve yaygın olarak kullanılmakta bir teknik olmakla beraber dikkatsiz kullanılması durumunda veri kayıpları ortaya çıkabilmektedir. Bu yöntemde; resim yapısı içerisinde yer alan piksellerdeki byte' ların en önemsiz bitlerinin yerine gizlenecek olan bilgilerin bitleri sırasıyla başlangıcından itibaren teker teker yerleştirilmektedir (Şahin, A., Buluş, E., & tolga Sakallı, M. ,2006). İletişimin daha güvenli olması adına saklanacak olan veriler RSA ve AES gibi şifreleme metotları ile de desteklenebilmektedir. Bu yöntemin tek dezavantajı kapasite sınırı olmasıdır yani gönderilecek mesaj ya da dokümanın uzunluğu taşıyıcı medya uzunluğuna bağlıdır. Bu yöntemde gizli bilgi bilgiler sıralı ya da rastgele şekilde saklanabilir. Bunlardan birincisinde resim üzerinde sıralı şekilde gizleme yapma işlemi, ikincisinde ise rasgele gizleme fonksiyonu üreterek belirlenen bir pikselde gizleme yapmak şeklindedir. Güvenliği arttırmak için ise Stego-anahtar (stego-key) kullanılmaktadır. Anahtar kullanmanın avantajı Şifre çözme işlemi esnasında ortaya çıkmaktadır. Anahtara sahip olmayan kimse gizli mesaj elde edilememektedir.

Alan dönüştürme tekniklerinde de çeşitli dönüşüm fonksiyonları kullanılmakta ve frekans düzlemde veri gizleme işlemleri gerçekleştirilmektedir.

4. Gereç ve Yöntem:

Bu çalışmada AVI formatındaki video dosyaları üzerine bilgi gizleme işlemi için MATLAB programı ile bir uygulama geliştirilmiştir. Gerçekleştirilen uygulamada en önemsiz bite ekleme yöntemi kullanılmış ve güvenliği arttırmak için AES ve RSA şifreleme teknikleri kullanılmıştır. Video üzerinde gizlenecek bilgiler sıralı ve rastgele olarak iki farklı şekilde gizlenmektedir.

Sıralı gizleme yönteminde veri her bite 0. bitten başlayarak bit uzunluğu kadar saklanır. Rastgele gizleme yönteminde ise bir algoritma mevcuttur.

Bu algoritma:

$f = (ax + b) \bmod c$ şeklindedir.

x: gizlenecek bit

c: frame sayısı

a ve b: asal sayılar

Bu algoritma ile gizlenecek olan veriler video çerçeveleri üzerinde rastgele olarak dağıtılmaktadır.

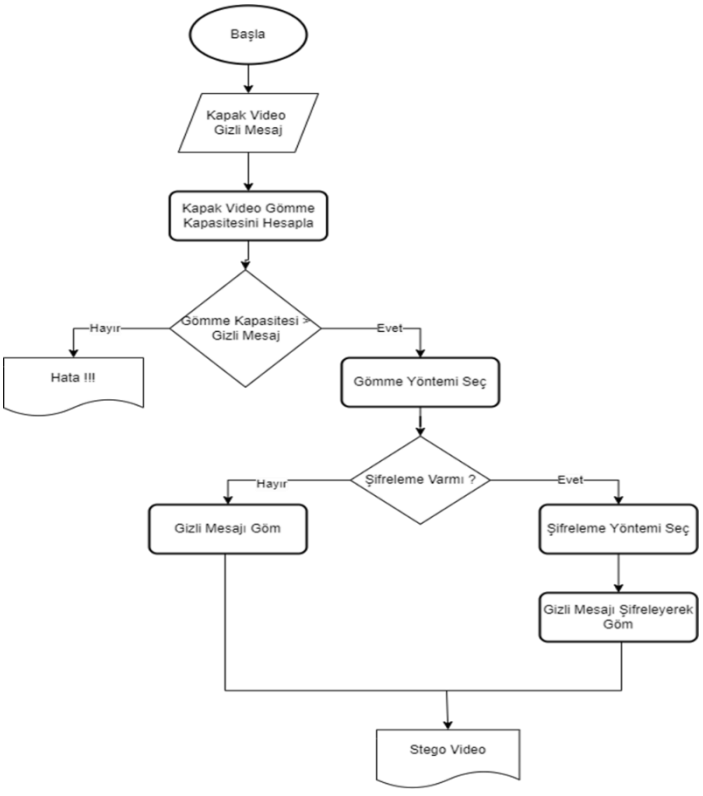
Gizleme işlemleri içerisinde var olan algoritmayı güçlendirmek ve gizlenen bilginin anlaşılır olmasını engellemek amacıyla şifreleme yöntemleri kullanılmıştır. Bu yöntemler simetrik şifreleme algoritması olan AES ve asimetrik şifreleme algoritması olan RSA şifrelemesidir.

RSA şifreleme algoritması asimetrik bir şifreleme algoritmasıdır ve 1978 yılında Ron Rivest, Adi Shamir ve Leonard Adleman tarafından geliştirilmiştir. RSA nın mantığı iki asal sayının çarpımından oluşan tamsayılara dayanmaktadır. Bu algoritmanın güvenliği ise kullanılan iki asal sayının büyüklüğü ile ilgilidir (Rivest, R. L., Shamir, A., & Adleman, L. (1978).).

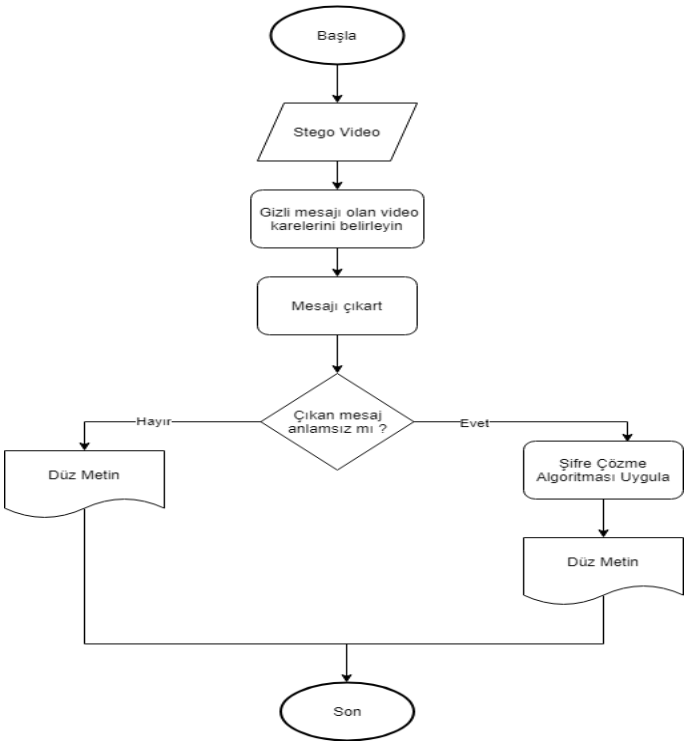
Simetrik bir şifreleme algoritması olan AES, kabul edilmiş bir şifreleme standardıdır. AES algoritması şifreleme ve şifre çözme işlemlerinde aynı anahtarı kullanmaktadır. DES algoritmasına göre daha hızlı ve güvenli olan AES algoritmasında girdi ve çıktı matrisleri her zaman 128 bit olmak zorundadır. Anahtar uzunlukları 128, 192 veya 256 bit olabilmektedir. AES algoritmasının yapısı genel anlamda iki farklı bloktan oluşmaktadır. Bu bloklardan ilki tur dönüşüm diğer blok ise anahtar üretim bloğudur. Algoritma tekrarlı bir yapıya sahiptir (Doğan, A. Y. , 2008).

Yapılan gizleme işlemleri sırasında orijinal video ile bilgi gizlenmiş videolar arasında bir boyut farkı oluşmamaktadır.

Şekil 2'de video dosyaları üzerinde önerilen gömme algoritmasının uygulanması gösterilmiştir. Şekil 3'te ise video dosyaları üzerinde önerilen veri çıkartma algoritmasının uygulanması gösterilmiştir.



Şekil 2. Önerilen Gömme İşleminin Algoritması



Şekil 3. Gizli Veriyi Elde Etme İşleminin Algoritması

Steganografik bir algoritma incelenirken genellikle üç temel unsur göz önünde bulundurulur. Bu unsular dayanıklılık, saklanabilen veri miktarı ve değişimin fark edilememesidir (Çimen, C., Akleylek, S. ve Akyıldız, E. ,2007). Taşıyıcıda ne kadar değişim olduğu steganografi bir algoritma için oldukça önemlidir. Taşıyıcıdaki değişimi ya da verideki bozulma oranının belirlenmesi için çeşitli ölçme yöntemleri mevcuttur.Bunlar arasında en bilinenleri; MSE, RMSE ve PSNR'dır. MSE hataların kareleri toplamının ortalamasıdır. Görüntü dosyalarında gerçek ve ideal piksel değerleri arasındaki ortalama kare farkını ölçmek için kullanılmaktadır.

MSE genellikle σ^2 olarak gösterilir. MSE değerinin sıfıra yakın olması iyi bir performans olduğunu ifade eder MSE'nin karekökü ise RMSE'dir (Sayood, 1996).

$$\sigma^2 = \frac{1}{N}\sum_{n=1}^{N}(x_n - y_n)^2$$

PSNR tanım olarak en yüksek sinyal gürültü oranı anlamına gelmektedir. Bir sinyalin sahip olduğu maksimum gücü ile sinyalin gürültüsü arasındaki oranı hesaplamak için kullanılan bir metriktir. Bazı durumlarda Ortalama Kare Hata (MSE) yerine bu metrik tercih edilebilmektedir, PSNR, genel olarak sıkıştırılmış görüntülerin kalitesini ölçmek için tercih edilmektedir (Sayood, 1996).

$$PSNR(dB) = 10\log_{10}\frac{x_{peak}^2}{\sigma_d^2}$$

Steganografik sistemlerde bilgi gizlenen görüntü dosyalarında RGB değerleri değiştirildiği için renk yoğunlukları da değişmekte ve bu da önemli bir konu haline gelmektedir. Histogram kavramı piksellerdeki renk bileşenlerinin dağılımları göstermektedir. Histogram analizleri bilgi gizlendikten önceki ve bilgi gizlendikten sonraki görüntüler arasındaki bu farkı ortaya koyabilmektedir.

5. Bulgular ve Tartışma

Video dosyaları üzerinde gizleme işlemleri birçok farklı video dosyasında uygulanmıştır. Sıralı ve rastgele bilgi gizleme işlemlerinin değerlendirilmesi amacıyla taşıyıcıdaki değişim ölçülmüş ve histogram analizi yapılmıştır.

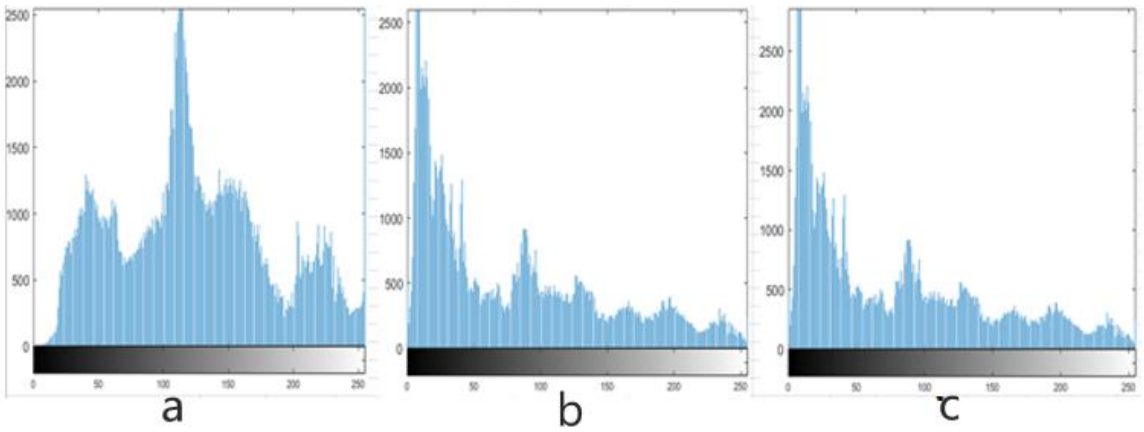
Örnek olarak iki adet video seçilmiş ve taşıyıcıdaki değişimleri ölçebilmek amacıyla MSE ve PSNR değerleri ede edilmiştir. Bu sonuçlar tablo 1 ve tablo 2 de gösterilmiştir. Video dosyaları üzerinde bilgi gizleme işlemlerindeki metinlerin boyutları 0,1 KB ile 450 KB arasında değişmektedir.

Tablo 1. Video 1 için elde edilen MSE ve PSNR değerleri

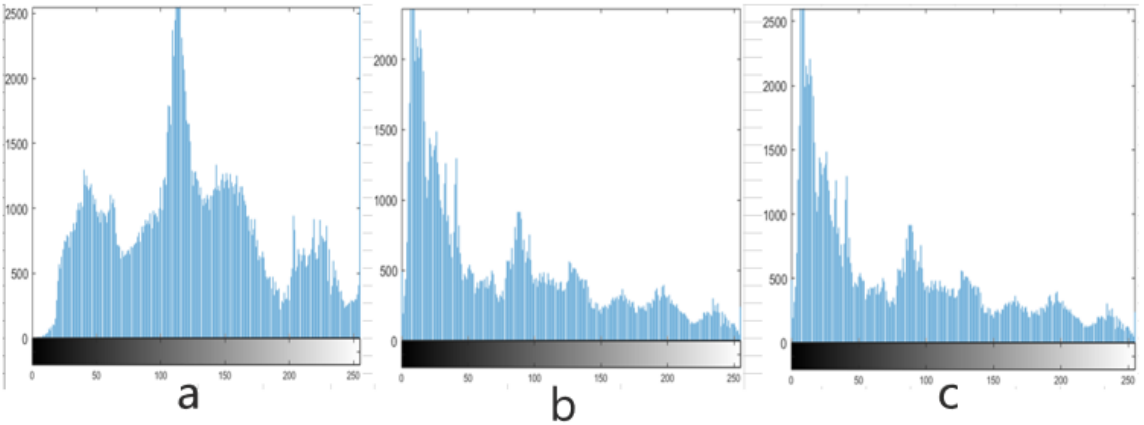
Sıralı Gizleme			**Rastgele Gizleme**		
	MSE	**PSNR**		**MSE**	**PSNR**
450 KB	5.553	55,3612	**450 KB**	5.581	55.352
200 KB	5.552	55,3611	**200 KB**	5.580	55.351
116 KB	3.258	57.668	**116 KB**	3,217	57.660
60 KB	1.621	60.687	**60 KB**	1.634	60.672
30 KB	0.7759	63.886	**30 KB**	0.7798	63.881
12 KB	0.4721	66.056	**12 KB**	0.4735	66.055
10 KB	0.2803	68.323	**10 KB**	0.2807	68.331
7.5 KB	0.2196	69.384	**7.5 KB**	0.2195	69.394
6 KB	0.1818	70.200	**6 KB**	0.1825	70.202
4 KB	0.1118	72.306	**4 KB**	0.1116	72.327
3 KB	0.0998	72.794	**3 KB**	0.0999	72.812
2 KB	0.0562	75.264	**2 KB**	0.0565	75.289
1 KB	0.0310	77.836	**1 KB**	0.0321	77.780
0.6 KB	0.0175	80.334	**0.6 KB**	0.1795	80.289
0.3 KB	0.0095	82.961	**0.3 KB**	0.0098	82.942
0.1 KB	0.0035	87.226	**0.1 KB**	0.0035	87.408

Tablo 1'de Video 1 dosyası üzerine yapılan gizleme işlemi sonucunda girilen veri boyutu değiştikçe MSE ve PSNR değerlerindeki değişim gözükmektedir. Veri boyutu büyüdükçe MSE değeri artmakta PSNR değeri ise azalmaktadır. Video 1 dosyasının boyutu 7.99 MB'dir.

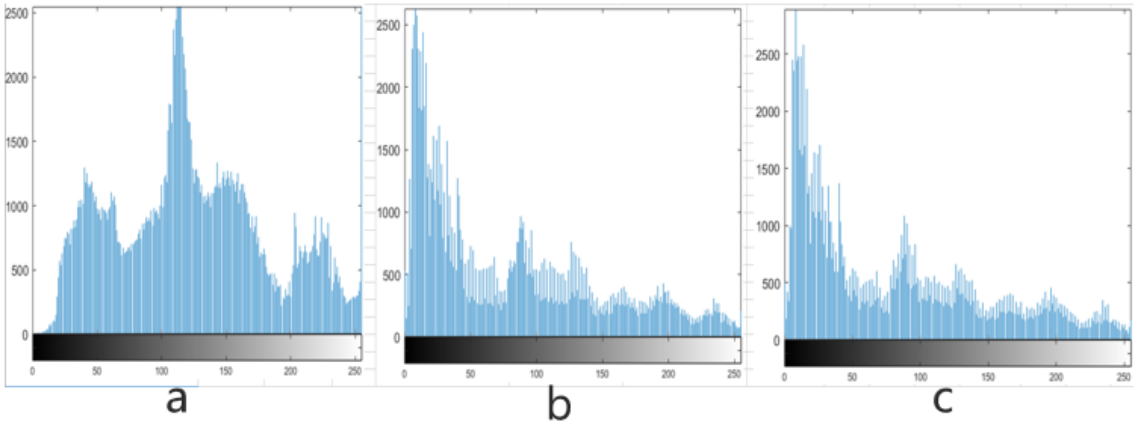
Aşağıda Video1 dosyasına sırasıyla 0,1 KB, 30 KB, 120 KB ve 400 KB gizlendiğinde oluşan histogram grafikler verilmiştir. Gizleme işlemi sıralı ve rastgele olacak şekilde ayrı ayrı gerçekleştirilmiştir.



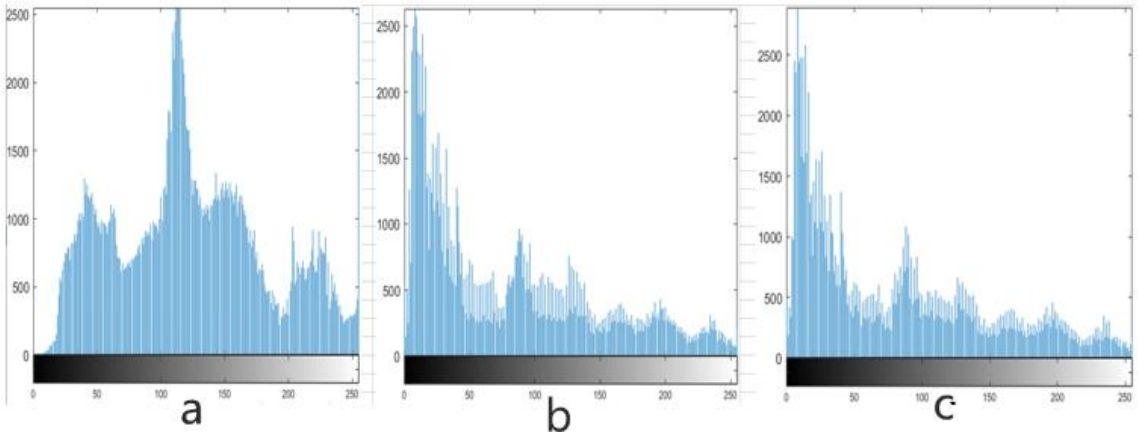
Şekil 4. (a) Veri gizlenmemiş orijinal Video1 dosyasının histogram grafiği **(b)** Video 1 doyasına sıralı olarak 0,1 KB veri gizlendiğinde oluşan histogram grafiği **(c)** Video 1 doyasına rastgele olarak 0,1 KB veri gizlendiğinde oluşan histogram grafiği



Şekil 5. (a) Veri gizlenmemiş orijinal Video1 dosyasının histogram grafiği **(b)** Video 1 doyasına sıralı olarak 30 KB veri gizlendiğinde oluşan histogram grafiği **(c)** Video 1 doyasına rastgele olarak 30 KB veri gizlendiğinde oluşan histogram grafiği



Şekil 6. (a) Veri gizlenmemiş orijinal Video1 dosyasının histogram grafiği **(b)** Video 1 doyasına sıralı olarak 120 KB veri gizlendiğinde oluşan histogram grafiği **(c)** Video 1 doyasına rastgele olarak 120 KB veri gizlendiğinde oluşan histogram grafiği



Şekil 7. (a) Veri gizlenmemiş orijinal Video1 dosyasının histogram grafiği **(b)** Video 1 doyasına sıralı olarak 450 KB veri gizlendiğinde oluşan histogram grafiği **(c)** Video 1 doyasına rastgele olarak 450 KB veri gizlendiğinde oluşan histogram grafiği

Şekil 4'te Video 1 üzerinde 0,1 KB lık veri gizleme işlemi gerçekleştirilmiştir. Gizlenen veri miktarı çok düşük olduğu için orijial dosya ile sıralı veya rastgele gizleme sonucunda elde edilen histogram grafiklerinde farkedilebilir bir değişim olmadığı gözlenmiştir.

Şekil 5'te ise Video 1 üzerinde 30 KB lık veri gizleme işlemi gerçekleştirilmiştir. Gizleme işlemi yapıldıktan sonra orijinal dosyanın histogramı ile Sıralı veya rastgele gizleme sonucunda elde edilen histogramlar arasında fark olduğu gözükmektedir. Orijinal dosyanın elimizde olduğu durumda yapılan bir histogram analizi soncunda gizli bilginin var olduğu anlaşılabilmektedir. Sıralı yada rastgele gizleme histogramları arasında çok gözle görülür bir fark yoktur.

Şekil 6'da Video 1 üzerindeki 120 KB lık veri gizleme işlemi gerçekleşmiştir. Orijinal ve veri gizlenmiş videoların histogramları arasındaki fark iyice belirginleşmiştir. Bu büyüklükte bir veri gizlendiğinde sıralı ya da rastgele gizleme soncunda oluşan histogram grafikleri de farklılaşmaya başlamaktadır.

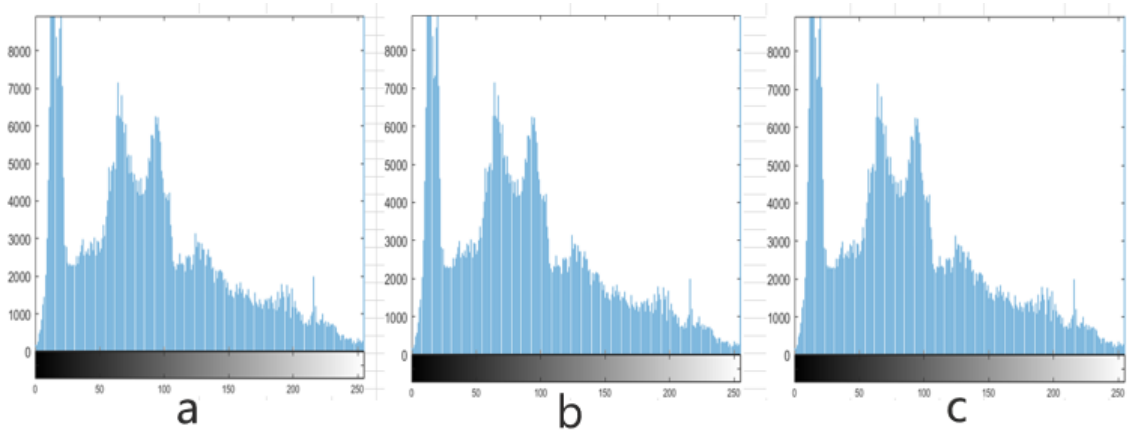
Şekil 7'de ise video 1 üzerinde 450 KB lık veri gizleme işlemi gerçekleştirilmiştir. Elde edilen histogram grafiklerindeki değişimlerin çok fazla olduğu gözlemlenmiştir.

Gizleme işlemlerinde 120 KB lık ve üzeri veri gizleme yapıldıktan sonra histogram grafiklerindeki değişim daha net gözükmektedir.

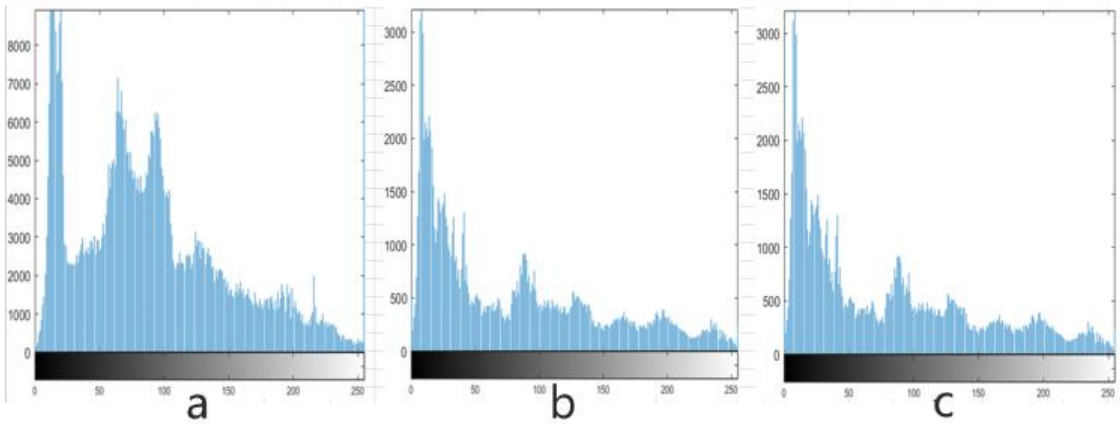
Tablo 2 de örnek olarak seçilen bir diğer video dosyası olan Video 2 dosyası üzerine yapılan gizleme işlemi sonucunda elde edilen PSNR ve MSE değerleri verilmiştir. Artan veri miktarı nedeniyle bu değerlerdeki değişimler gözlenmiştir. Veri boyutu büyüdükçe MSE değeri artmakta PSNR değeri ise azalmaktadır. Video 2 dosyasının boyutu 5.99 MB dır.

Tablo 2. Video 2 için elde edilen MSE ve PSNR değerleri

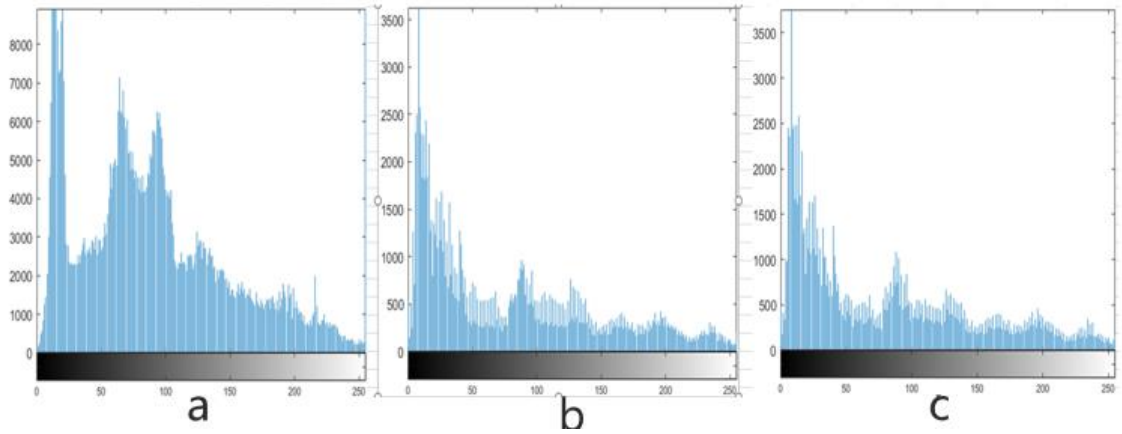
Sıralı Gizleme			**Rastgele Gizleme**		
	MSE	**PSNR**		**MSE**	**PSNR**
450 KB	5.553	55,3612	**450 KB**	5.581	55.352
200 KB	5.552	55,3611	**200 KB**	5.580	55.351
116 KB	3.258	57.668	**116 KB**	3,217	57.660
60 KB	1.621	60.687	**60 KB**	1.634	60.672
30 KB	0.7759	63.886	**30 KB**	0.7798	63.881
12 KB	0.4721	66.056	**12 KB**	0.4735	66.055
10 KB	0.2803	68.323	**10 KB**	0.2807	68.331
7.5 KB	0.2196	69.384	**7.5 KB**	0.2195	69.394
6 KB	0.1818	70.200	**6 KB**	0.1825	70.202
4 KB	0.1118	72.306	**4 KB**	0.1116	72.327
3 KB	0.0998	72.794	**3 KB**	0.0999	72.812
2 KB	0.0562	75.264	**2 KB**	0.0565	75.289
1 KB	0.0310	77.836	**1 KB**	0.0321	77.780
0.6 KB	0.0175	80.334	**0.6 KB**	0.1795	80.289
0.3 KB	0.0095	82.961	**0.3 KB**	0.0098	82.942
0.1 KB	0.0035	87.226	**0.1 KB**	0.0035	87.408



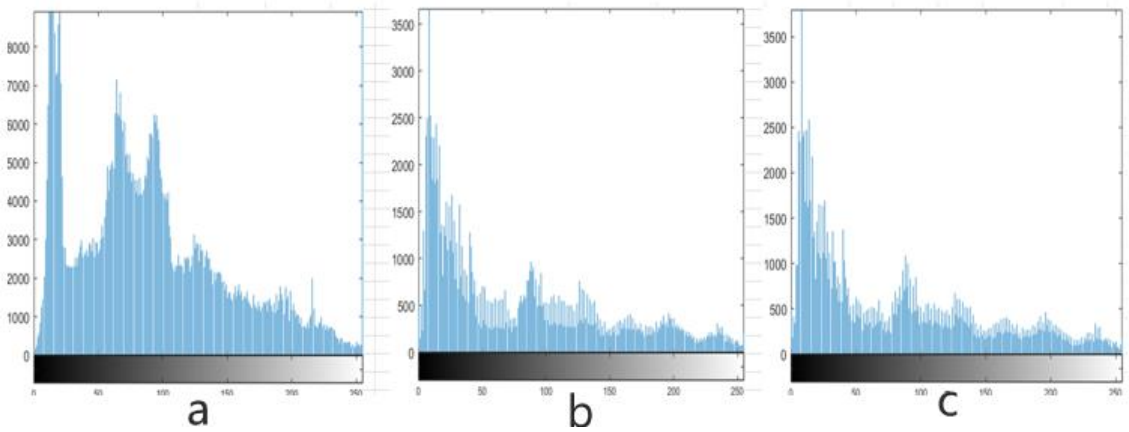
Şekil 8. (a) Veri gizlenmemiş orijinal Video2 dosyasının histogram grafiği **(b)** Video 2 doyasına sıralı olarak 0,1 KB veri gizlendiğinde oluşan histogram grafiği **(c)** Video 2 doyasına rastgele olarak 0,1 KB veri gizlendiğinde oluşan histogram grafiği



Şekil 9. (a) Veri gizlenmemiş orijinal Video2 dosyasının histogram grafiği **(b)** Video 2 doyasına sıralı olarak 30 KB veri gizlendiğinde oluşan histogram grafiği **(c)** Video 2 doyasına rastgele olarak 30 KB veri gizlendiğinde oluşan histogram grafiği



Şekil 10. (a) Veri gizlenmemiş orijinal Video2 dosyasının histogram grafiği **(b)** Video 2 doyasına sıralı olarak 120 KB veri gizlendiğinde oluşan histogram grafiği **(c)** Video 2 doyasına rastgele olarak 120 KB veri gizlendiğinde oluşan histogram grafiği



Şekil 11. (a) Veri gizlenmemiş orijinal Video2 dosyasının histogram grafiği **(b)** Video 2 doyasına sıralı olarak 450 KB veri gizlendiğinde oluşan histogram grafiği **(c)** Video 2 doyasına rastgele olarak 450 KB veri gizlendiğinde oluşan histogram grafiği

Şekil 8 de Video 2 üzerinde 0,1 KB lık veri gizleme işlemi gerçekleştirilmiştir. Sıralı ve rastgele şekilde yapılan gizleme işlemi sonrasında oluşan histogram ile orijinal videodan elde edilen histogram arasında çok fark olmadığı gözlemlenmiştir. Şekil 9 da Video 2 üzerinde 30 KB lık veri gizleme işlemi gerçekleştirilmiştir. Orijinal histogram ile sıralı ve rastgele şekilde yapılan gizleme işlemi sonrasında videodan elde edilen histogramlarda farkın arttığı görülmüştür. Şekil 10'da Video 2 üzerine 120 KB lık veri gizleme işlemi gerçekleşmiştir. Şekil 11'de video 2 üzerinde 450 KB lık veri gizleme işlemi gerçekleştirilmiştir. Sıralı ve rastgele şekilde yapılan gizleme işlemi sonrasında histogram değişiklikleri gösterilmiştir.

Gizleme işlemlerinde 120 KB lık ve üzeri veri gizleme yapıldıktan sonra histogram grafiklerindeki değişim daha net gözükmektedir.

Sıralı ve rastgele gizleme sonrasında ortaya çıkan histogram grafikleri arasındaki farkın daha küçük boyuttaki veri gizleme işlemlerine göre daha fazla olduğu gözlemlenmektedir.

6. Sonuçlar ve Değerlendirme

Kişisel ya da kurumsal veri güvenliği günümüzde çok önemli bir konudur. Veri güvenliğini sağlamak için çeşitli yöntemler geliştirilmiştir. Bu çalışmada hareketli görüntü olarak tanımlanan video dosyaları üzerinde veri gizlemek için kullanılan LSB yöntemi incelenmiştir. Bu gizleme işleminin sıralı bir şekilde ya da bir fonksiyona bağlı olarak rastgele bir şekilde yapılmasının güvenlik açısından etkisi olup olmadığı incelenmiştir. Bunun için bir uygulama geliştirilmiş, veri gizleme analiz işlemleri bu uygulama aracılığıyla yapılmıştır. Taşıyıcıdaki değişimi ölçme amacıyla PSNR ve MSE değerleri hesaplanmış, dayanıklılık için de Histogram analizi yapılmıştır. Farklı büyüklükteki dosyalara çeşitli büyüklükteki veriler sıralı ve rastgele şekilde gizlenmiştir. Elde edilen sonuçlar sayesinde düşük miktarda saklanan verinin PSNR, MSE ve Histogram analizinde bilgi varlığının sezilmesi konusunda ayırıcı olmadığı görülmüştür. Bu yöntem ile düşük miktarda veri saklamanın oldukça güvenli olduğunu göstermektedir. Gizlenen veri miktarı arttıkça bir fonksiyona bağlı olarak rastgele şekilde yapılan gizleme yöntemindeki analiz değerlerinin yani orijinal dosya ile veri gizlenmiş dosya arasındaki fark ve benzerlik oranlarının daha iyi olduğu sonucuna varılmıştır. Bu durum da rastgele veri gizleme işleminin daha iyi olduğunu ortaya çıkartmaktadır. Sıralı gizleme işleminde gizli bilginin yerleştirilmesi işleminin ilk pikselden başlayarak sona doğru yapılması nedeniyle gizli verinin varlığının rastgele yönteme göre daha kolay anlaşılabileceği sonucuna varılmıştır.

7. Kaynakça

Akyüz, D., Kasapbaşı, M. C. (2021). Yeni kaotik video steganografi metodu. *Haliç Üniversitesi Fen Bilimleri Dergisi*, 4(1), 25-40.

Al-Othmani, A. Z., Manaf, A. A., & Zeki, A. M. (2012). A Survey On Steganography Techniques İn Real Time Audio Signals And Evaluation. *International Journal of Computer Science Issues* (IJCSI), 9(1), 30.

Avcı, E., Tuncer, T., Ertam, F. (2014). Çok Katmanlı Görüntü Steganografi. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı*.

Cox, I. J., Miller, M. L., Bloom, J. A (2000). Watermarking Applications And Their Properties. *Int. Conf. On Information Technology*, Las Vegas, USA.

Çimen, C., Akleylek, S., Akyıldız, E. (2007). Şifrelerin Matematiği: Kriptografi, *ODTÜ Geliştirme Vakfı Yayıncılık*, İstanbul.

Doğan, A. Y. (2008). AES Algoritmasının FPGA Üzerinde Düşük Güçlü Tasarımı *Doktora Tezi*,

İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

Hacımurtazaoğlu. M. (2022). Video Steganografisine Yenilikçi Bir Yaklaşım, *Doktora Tezi*, Selçuk Üniversitesi Fen Bilimleri Enstitüsü, Konya.

Hu, S. D. (2011). A Novel Video Steganography Based On Non-Uniform Rectangular Partition. *In 2011 14th IEEE International Conference on Computational Science and Engineering* (pp. 57-61). IEEE.

Misman, C. (2018). Mobil Haberleşme Güvenliğinin Steganografi İle Arttırılması, *Doktora Tezi*, Necmettin Erbakan Üniversitesi, Konya.

Johnson N.F., Jajoida S. (1998). Exploring Steganography: Seeng the Unseen, *IEEE Computing Practices*, 0018-9162/98, 26-34.

Nosrati, M., Karimi, R., Hariri, M. (2012). Audio steganography: A Survey On Recent Approaches. *World applied programming*, 2(3), 202-205.

Pfitzmann B., (1996). Information Hiding Terminology, *In: Anderson, R. (eds) Information Hiding. IH 1996. Lecture Notes in Computer Science, vol 1174*. Springer, Berlin, Heidelberg. In Anderson [3], pp. 347-350, ISBN 3-540-61996-8.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A Method For Obtaining Digital Signatures And Public-Key Cryptosystems. *Communications of the ACM*, 21(2), 120-126.

Şahin Mesut A., Mesut A., Sakallı M.T. (2010). Görüntü Steganografide Gizlilik Paylaşım Şemalarının Kullanılması ve Güvenliğe Etkileri, *III Ağ ve Bilgi Güvenliği Sempozyumu*, Ankara.

Şahin, A., Buluş, E., Sakallı M.T. (2006). 24-Bit Renkli Resimler Üzerinde En Önemsiz Bite Ekleme Yöntemini Kullanarak Bilgi Gizleme. *Trakya Üniversitesi Fen Bilimleri Dergisi*, 7(1), 17-22.

Şahin, A. (2007). Görüntü Steganografide Kullanılan Yeni Metodlar ve Bu Metodların Güvenilirlikleri. Doktora Tezi, Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Edirne.

Sayood K. (1996) Introduction to Data Compression, *Morgan Kauffman Publishers*, Inc. 340 Pine Street, Sixth Floor, San Francisco, CA 94104-3205, USA, 1996.