Düzce Üniversitesi Bilim ve Teknoloji Dergisi

Yazılı Metni Şifreleyip LSB Yöntemi ile Gizleme

Ferdi ÖZBİLGİN [a,*], Fatih DURMUŞ [a], Serap KARAGÖL [a]

[a] *Elektrik Elektronik Mühendisliği Bölümü, Mühendislik Fakültesi, Ondokuz Mayıs Üniversitesi, Samsun, TÜRKİYE*

** Sorumlu yazarın e-posta adresi: ozbilginferdi@gmail.com*

ÖZET

Teknolojinin gelişmesi ile birlikte sayısal verilerin güvenli bir şekilde iletilmesi önemli bir hale gelmektedir. Şifreleme ve steganografi ile birlikte iletilecek veri alıcıya daha güvenli bir şekilde iletilebilmektedir. Bu çalışmada da yazılı bir metne ilkel şifreleme tekniklerinden Vigenere şifreleme uygulanmış ve elde edilen şifreli veri görüntü içerisine 3 farklı algoritma ile gizlenmiştir. Mesaj metni iletilirken steganografi de kullanıldığından ilkel şifreleme tekniklerinden Vigenere şifreleme tercih edilmiştir. Şifrelenmiş veri ile birlikte verinin boyut bilgisi görüntü içerisindeki piksellerin mavi bileşenine LSB (Least Significant Bit) yöntemiyle gizlenmiştir. Görüntü içerisine satırlara, sütunlara ve diagonal şekilde olmak üzere 3 farklı algoritma ile veri gizleme gerçekleştirilmiştir. Orijinal görüntü ile şifreli verinin gizlendiği taşıyıcı arasındaki değişim oranının tespit edilmesi amacıyla MSE (Mean Squared Error) kullanılmış ve 3 farklı algoritmada MSE değerleri karşılaştırılmıştır.

Anahtar Kelimeler: *Şifreleme, Veri Gizleme, LSB, Steganografi*

Encrypting Written Text and Hiding it with LSB Method

ABSTRACT

With the development of technology, the transmission of digital data in a secure manner becomes important. The data to be transmitted together with encryption and steganography can be transmitted more securely. In this study, a written text is applied to Vigenere encryption from primitive coding techniques and the obtained encrypted data is hidden in 3 different algorithms in an image. Since steganography is used when transmitting the message text, Vigenere encryption is preferred from the primitive coding techniques. The size information along with the encrypted data is hidden in the blue component of the pixels in the image by the LSB (Least Significant Bit) method. Data hiding has been performed in three different algorithms, namely rows, columns and diagonal within the image. MSE (Mean Squared Error) was used to determine the rate of change between the original image and the carrier where the encrypted data is hidden, and MSE values were compared in 3 different algorithms.

Keywords: *Encryption, Data Hiding, LSB, Steganography*

Geliş: 31/12/2017, Düzeltme: 01/03/2018, Kabul: 16/03/2018

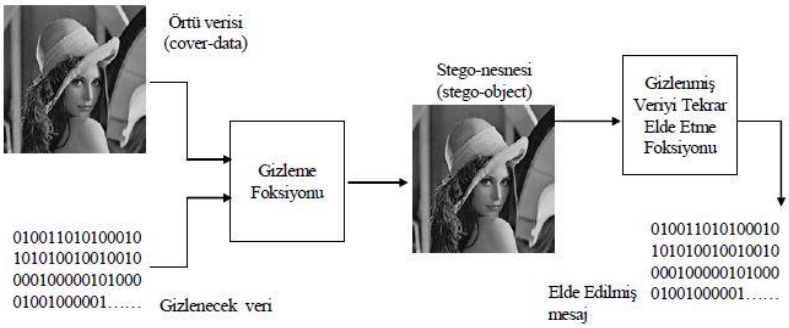
I. GİRİŞ

Bilişim teknolojilerinin günlük hayatımıza daha fazla girmesi ve kullanımının yaygınlaşmasıyla birlikte yapılan işlemler ve işlemlerin sonucunda elde edilen verilerin büyük çoğunluğu elektronik ortamlarda saklanmaktadır. Bu ortamlarda saklanan, işlenen ve ihtiyaç duyulduğunda transfer edilen bilgilerin korunması veya güvenliğinin sağlanması son derece önemlidir. Veri iletişiminin sayısal olarak gerçekleştirildiği bir ortamda, göndericiden alıcıya veya alıcıdan göndericiye iletilen veriye izinsiz erişim, zarar vermek, yok etmek, veride değişiklik yapmak ve yeniden üretmek gibi birçok tehdit mevcuttur. Bu tehditlerin alınan önlemlere rağmen her geçen gün arttığı bilinmektedir [1,2].

Bu tehditlerin ortaya çıkmasına karşılık olarak bunların giderilmesi için çeşitli teknikler geliştirilmiştir. Şifreleme de bunların başında gelen çözüm yolları arasındadır. Şifreleme, veriyi başka kişiler tarafından anlaşılamaz bir yapıya dönüştürüp veriyi çözmeyi zorlaştırsa da yapılacak herhangi bir kripto-analiz atağını önleyemediği durumlar olabilmektedir. Ayrıca elektronik ortamlarda iki uç arasında şifreli bir iletişim yapıldığı anlaşıldığında ise iletişimi engelleme yoluna gidilebilmektedir. İşte bu noktada steganografi bilimi gündeme gelmektedir [3].

Steganografi, temelleri çok eskiye dayanan bir bilim dalıdır [4]. Kelime anlamı olarak "gizlenmiş yazı" veya "örtülü yazı" anlamına gelmektedir [5]. Bir verinin dijital ortamda bulunan büyük boyutlardaki dosyalara gizlenmesiyle anlaşılmayacak şekilde iletilmesi sağlanmaktadır. Bu işlem, başka bir deyişle veri gizleme olarak da adlandırılabilir [6]. Sayısal veri dosyası formatlarının (ses, fotoğraf ve video gibi) çeşitliliği sayesinde steganografik yöntemlerle birçok dosya türü içerisine veri gizlenebilmektedir [7-12]. Bu veriler metin dosyası olabileceği gibi, herhangi bir görüntü içerisine gizlenmiş başka bir görüntü dosyası veya ses dosyası da olabilir [13]. Gizli verinin varlığını saklamak amacıyla gizleme işlemi sonucunda özgün verinin en az bozulmaya uğraması hedeflenir. Ayrıca özgün veriye, boyutu çok değiştirmeyecek şekilde, maksimum büyüklükte gizli veri saklamaya çalışılır [14,15].

Steganografi tekniklerinin temel mantığı, sayısal veri dosyası formatlarındaki gerek olmayan veya çok önemli olmayan bölümlerde kullanılması veya insan duyularının algılayamaması prensibine dayanmaktadır [3]. Resim içerisine uygulanacak genel bir steganografik sistem Şekil 1'deki gibidir. Gizlenecek veri gizleme fonksiyonu ile bir örtü verisi içerisine stego-nesnesine dönüştürülür. Gizlenmiş veri çözme fonksiyonu vasıtasıyla tekrar elde edilir.



Şekil 1. *Bir Veri Gizleme Sistemi*

Görüntü içerisine veri gizlemek için en çok kullanılan bazı yöntemler aşağıdaki gibidir.

- En önemsiz bite ekleme (LSB)
- Maskeleme ve filtreleme
- Algoritmalar ve dönüşümler

İletilecek verinin önemine göre gizleme ile birlikte şifreleme de yapılmaktadır. Şifreleme veri güvenlik seviyesini artırmak için tercih edilir. Şifreleme ve veri gizleme ile birlikte veri güvenlik seviyesi daha da artmaktadır. Sezar, Vigenere gibi ilkel şifreleme ve DES (Data Encryption Standart, Veri Şifreleme Standardı) ve AES (Advanced Encryption Standard, Gelişmiş Şifreleme Standardı) gibi modern şifreleme metotları şifrelemenin türleri olarak adlandırılabilir.

Son yıllarda steganografi ile ilgili birçok yöntem kullanılmıştır. LSB ile veri şifreleme yöntemlerinin birleştirilmesiyle resim içine resim gizlenmiştir [16]. Başka bir çalışmada Sezar şifreleme yöntemi ile ilk aşama şifrelemesinin ardından kaos teori şifrelemesi kullanılmıştır. Şifreli metin LSB yer değiştirme algoritmasıyla gizlenmiştir [17]. Uygun kenarın seçilmesi prensibine dayalı bir çalışmada kırmızı kanalın 1, yeşilin 4 ve mavinin 8 biti gizli mesaj bitlerinin gizlemek için kullanılmıştır. Yine bu çalışmada da LSB ile gizleme yapılmıştır [18]. LSB'nin daha az gizleme kapasitesi, daha fazla veriyi gizledikten sonra görüntü kalitesini ve gizli verilerin güvenliğini bozması gibi bazı sorunları aşmak için bir çalışma yapılmıştır. Çalışmada, görüntü kalitesini artıran ve yüksek yerleştirme kapasitesine ulaşan bilgileri üç boyutlu RGB görüntülerine yerleştirerek, renkli görüntüler için geliştirilmiş bir LSB tekniği önerilmiştir [19]. 2013 yılında kousik Oas Gupta ve arkadaşları [20], video dosyasını mesajı gizlemek için kullanan bir steganografi tekniğini önermiş ve 3, 3, 2 LSB değiştirme algoritması kullanılarak gizli veriler gömülmüştür. Bu teknik de, yüksek gizlilik elde etmek için genetik algoritma kullanırmıştır.

Bu çalışmada ise .txt uzantılı mesaj dosyasının güvenliği ve gizliliği artırabilmek için gizli bir anahtarın ardından ASCII kodunun teklik ve çiftlik durumuna göre değişen, dinamik bir Sezar şifreleme yöntemi kullanılmıştır. Ayrıca veri, insan gözünün en az duyarlı olduğu, piksellerin mavi bileşenlerine gizlenmiştir. Gizleme şeklinin satır, sütun ya da köşegenlerden uygun olanını bulmak için karşılaştırmalar yapılmıştır.

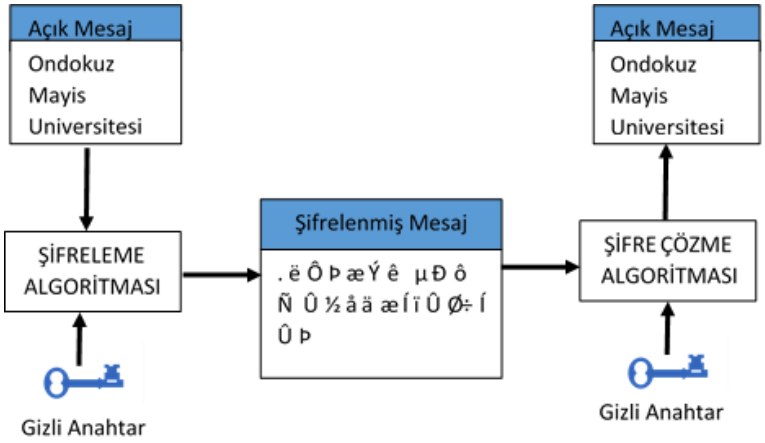
II. YÖNTEM

A. ŞİFRELEME

Bilgi aktarımı ve bilgi alımı yapan taraflar arasında bilgi güvenliğini sağlayan en temel sistem şifrelemedir. Aktarım yapılan bilgi alıcı tarafın da bilgisinin bulunduğu bir sistemle değiştirilir. Bu sistem basit matematiksel yöntemlerle yapılabildiği gibi modern yöntemlerle de oluşturulabilmektedir. Böylelikle verinin istenmeyen kişiler tarafından muhtemel bilgi çalınmasının önüne geçilir [21].

Verinin şifreleme ve şifrelenen verinin çözülmesi genel anlamda şekil 2'de diyagram olarak gösterilmektedir. Gönderilen bilgi ve şifre için kullanılan anahtar algoritma kullanılarak şifreli mesaj elde edilir. Bu kripto veri genel kullanım ortamından geçirilir. Ortam düşük maliyetli olmasına rağmen yetkisiz kullanıcıların ulaşımına açıktır. Gerçek mesaj, alıcı tarafından kripto veri ve şifre anahtarı kullanılmasıyla elde edilir. Kripto veri gerçek mesajdan çok farklı olduğundan yetkisiz kullanıcılar bu

veriye ulaşsalar dahi şifre çözme anahtarı kendilerinde olmadığı için gerçek veriyi elde etmeleri zordur [22].



Şekil 2. *Genel Bir Şifreleme Sistemi*

Bu çalışmada düz yazılı bir metinin ASCII kod karşılığı bulunarak öncelikle blok şifreleme ile anahtar yardımıyla şifrelenmiştir. Örneğin;

Tablo 1. *Metin, anahtar ve şifleri mesaj*

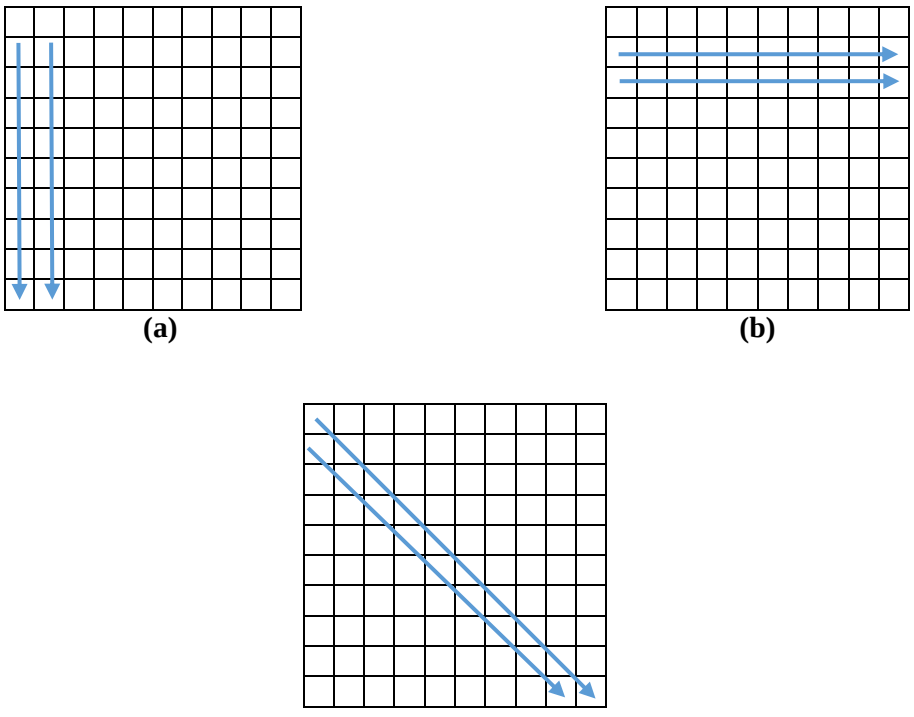
Mesaj	ASCII Karşılığı		Anahtar	ASCII Karşılığı		Şifreli Mesaj	ASCII Karşılığı
O	79		a	97		·	183
n	110		n	110		ë	235
d	100		a	97		Ô	212
o	111		h	104		Þ	222
k	107		t	116		æ	230
u	117		a	97		Ý	221
z	122		r	114		ê	234
	32						157
M	77					µ	181
a	97					Ð	208
y	121					ô	244
i	105					Ñ	255
s	115					Û	219
	32						157
U	85					½	189
n	110					å	229
i	105					ä	228
v	118					æ	230
e	101					Í	205
r	114					ï	239
s	115					Û	219
i	105					Ø	216
t	116					÷	247
e	101					Í	205

s	115															Û	219		
i	105															Þ	222		

B. EN ÖNEMSİZ BİTE EKLEME İLE VERİ GİZLEME

Görüntü içerisinde en anlamsız bite ekleme ile yapılan veri gizleme yöntemi en yaygın kullanılan yöntemlerden birisidir. Görüntüyü oluşturan her bir pikselin her baytının en anlamsız bitine ikilik sistemdeki verinin eklenmesi ile yapılmaktadır. Bir bitlik değişim göz ile görülür bir fark yaratmayacaktır.

Bu çalışmada şifreli ve ikilik sistemdeki veri, görüntü içerisinde satıra, sütuna ve diagonal şekilde mavi pikselin son bitine yerleştirilerek gizlenmiştir. Gizlenecek verinin boyut bilgisi ilk satıra yine mavi pikselin son bitine yerleştirme yapmak suretiyle alıcının veriyi çözerken kullanması için gizlenmiştir. İlk algoritmada şifreli veri 2. satırdan itibaren sütunlara mavi pikselin son bitine yerleştirilerek gizlenirken ikinci algoritmada şifreli veri yine 2. satırdan itibaren satırlara ekleme yaparak gizleme işlemi yapılmıştır. Son algoritmada ise ilk olarak köşegenden başlayarak gizlenen veri köşegenin son elemanına geldikten sonra bir alttaki köşegene geçerek gizleme işlemi devam etmektedir. İşlem bu şekilde şifreli verideki tüm bitler gizlenene kadar devam etmektedir. Veri yerleştirme algoritmaları Şekil 3'teki gibi gerçekleştirilmiştir. Son bite yerleştirilen şifreli verinin, gizlenen resmin bazı piksellerinin son biti ile aynı olmasından dolayı görüntü üzerindeki değişim, veri boyutundan daha az olmuştur.



Şekil 3. *Veri gizleme algoritmaları* ***(a)****Sütuna gizleme,* ***(b)*** *Satıra gizleme ve* ***(c)*** *Köşegene gizleme*

III. BULGULAR VE TARTIŞMA

Genel olarak, görüntü steganografi, görüntünün görsel kalitesinin algılanamaz şekilde değiştirilemeyeceği şekilde görüntüde gizli bir mesajın içeriğini yerleştirmelidir. Veri gizlendikten sonra görüntüde oluşan farklılığın azlığı steganografi algoritmasının kalitesini gösterir. Taşıyıcıda meydana gelen bozuklukların ya da değişim oranının tespit edilmesi amacıyla kullanılabilecek MAD (Mean Absolute Deviation, Ortalama Mutlak Sapma), MSE (Mean Square Error, Ortalama Karesel Hata), MAPE (Mean Absolute Percentage Error, Ortalama Mutlak hata Yüzdesi), MPE (Mean Percentage Error, Ortalama Yüzde Hata) gibi bir çok yöntem vardır. Hataların kareleri alındığı ve büyük öngörülü hataları cezalandırdığı için bu çalışmada MSE yaklaşımı kullanılmıştır. MSE'nin hesaplanması Denklem (1) de verilmiştir.

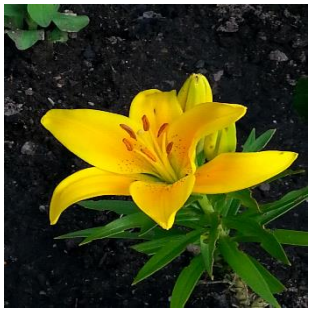
$$MSE = \frac{1}{M\ x\ N}\sum_{i=1}^{M}(P(i,j) - S(i,j))^2 \quad (1)$$

Burada MSE, hataların kareleri toplamının ortalaması, M ve N satır ve sütun sayıları, P(i,j) örtü verisi ve S(i,j) stego nesnesidir. Mavi piksel için yapılan hesaplamalarda elde edilen MSE değerleri Tablo 2 de verilmiştir. Kırmızı ve yeşil piksellerde değişim olmadığı için üç farklı veri boyutunda da MSE sıfır çıkmıştır.

Tablo 2. *Mavi piksel için MSE değerleri*

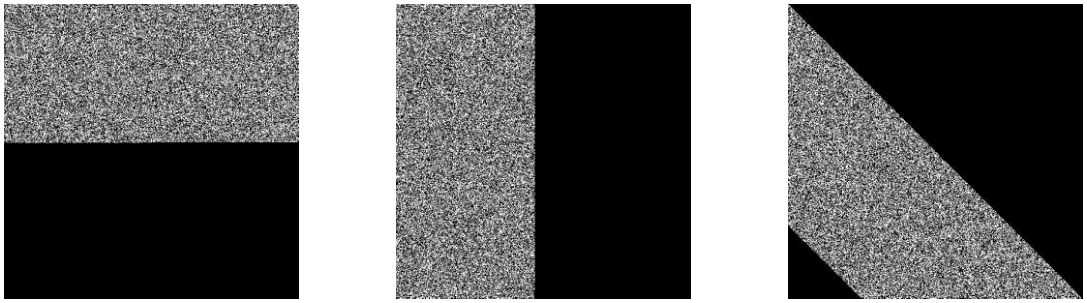
Veri boyutu	MSE hatası		
	Sütuna Gizleme	**Satıra Gizleme**	**Diagonal Gizleme**
26 bayt	0.00026	0.00027	0.000074
1000 bayt	0.0021	0.0022	0.0019
15000 bayt	0.03	0.03	0.0302

Şekil 4'te orijinal resim ile şifrelenmiş verinin resme gizlenmiş hali gösterilmektedir. Şifrelenmiş verinin boyutu 15000 bayttır. Gizlenen veri göndericiye güvenli bir şekilde ulaştırılmıştır. Görüntüyü alan alıcı, birinci satır ikinci sütundan başlayarak birinci satırdan veri boyutunu tespit edip Şekil 3'teki algoritmalardaki gibi ok yönünde mavi piksellerin son bitlerindeki verileri alarak şifreli veriyi elde eder.



(a) **(b)**

Şekil 4. (a) *Orijinal görüntüler* ***(b)*** *Şifreli veri gizlenmiş görüntüler*

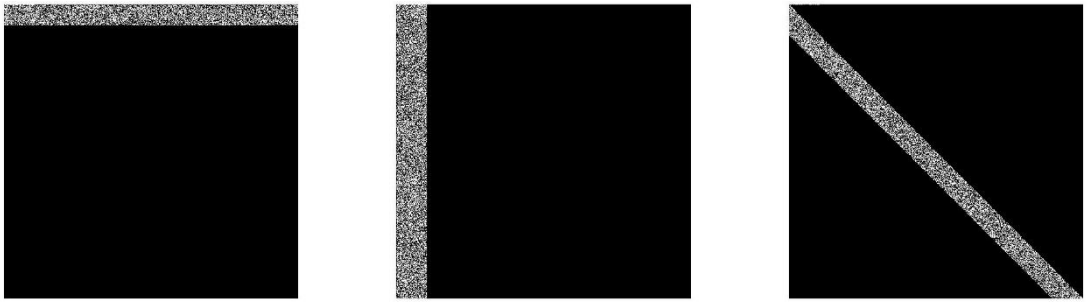


Şekil 5. *Kullanılan üç algoritmada 15000 baytlık veri için orijinal görüntü ile şifreli veri gizlenmiş resim arasındaki fark*

15000 baytlık aynı veri Şekil 6'daki gibi 3500 x 2333 piksellik daha yüksek çözünürlüklü görüntülere uygulandığında MSE değerleri Tablo 3'deki gibi elde edilmiştir.

(a) **(b)**

Şekil 6. *Yüksek çözünürlüklü* ***(a)*** *Orijinal görüntü* ***(b)*** *Şifreli veri gizlenmiş görüntü*



Şekil 7. *Kullanılan üç algoritmada 15000 baytlık veri için orijinal görüntü ile şifreli veri gizlenmiş resim arasındaki fark*

Şekil 7'de de görüldüğü gibi taşıyıcı görüntüde çözünürlük değeri yükseldiğinde, aynı veri gizli normal boyutlu görüntülere göre MSE değerleri küçük çıkmaktadır. Ayrıca taşıyıcıdaki çözünürlük değerinin artması ile daha çok veri gizlenebilmektedir.

Tablo 3. *15000 bayt veri için resim çözünürlüğüne göre kıyaslama*

	MSE hatası		
Çözünürlük	**Sütuna Gizleme**	**Satıra Gizleme**	**Diagonal Gizleme**
Düşük	0.03	0.03	0.0302
Yüksek	0.00093	0.001	0.00095

IV. SONUÇ

Bu çalışmada MATLAB programlama dili kullanılarak veri şifreleme ve en anlamsız bite ekleme ile veri gizleme yapan bir uygulama gerçekleştirilmiştir. Görüntü içerisindeki gizleme işlemi piksellerin satırına, sütununa ve köşegenlerine uygulanmıştır. Piksellerin son bitine ekleme yapıldığı için görüntü üzerinde değişim göz ile fark edilemeyecektir. Ayrıca şifreli veri kullanıldığından gizlenen veri bulunsa dahi veriyi çözmek gerekecektir.

26 bayt, 1000 bayt ve 15000 baytlık veriler kullanılarak Vigenere ve Sezar şifreleme ile şifrelenen veriler görüntü içerisinde satır, sütun ve köşegene olmak üzere üç farklı algoritmada gizlenmiştir. Bu üç algoritmada da veriler hatasız olarak alınmıştır.

Bu çalışmadaki dezavantaj gizlenecek veri görüntünün boyutu ile orantılı olmasıdır. Veri sıkıştırma ile bu dezavantaj kaldırılabilir. Ayrıca DES ve AES gibi modern şifreleme yöntemleri kullanılarak güvenlik seviyesi artırılabilir.

V. KAYNAKLAR

[1] G. Canbek, Sağıroğlu, Ş., "Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri'', Grafiker Yayınları, Ankara, ss. 01-50, 2006.

[2] Ş. Sağıroğlu, Alkan, M., "Her Yönüyle Elektronik İmza (e-İmza)'', Grafiker Yayınları, Ankara, s 3, s 5, ss 33, 2005.

[3] M. A. Atıcı, "Steganografik Yaklaşımların İncelenmesi, Tasarımı Ve Geliştirilmesi'', Yüksek Lisans Tezi, Gazi Üniversitesi, Ankara, 2007.

[4] 2nd Lt. J. Caldwell, "Steganography", Crosstalk The Journal of Defense Software Engineering, 25-27, 2003.

[5] J. Cummins, P. Diskin, S. Lau, R. Parlett, "Steganography and Digital Watermarking", School of Computer Science, The University of Birmingham, 2004.

[6] S. Öksüzoğlu, "Radyografik Görüntülere Veri Gizleme Uygulaması", SAÜ. Fen Bil. Der. 17. Cilt, 2. Sayı, ss. 277-286, 2013.

[7] K. Gopalan, "Audio steganography using bit modification", 2003 InternationalConference on Multimedia and Expo, Baltimore, Maryland, 629-632, 2003.

[8] M. Niimi, H. Noda, E. Kawaguchi, R.O. Eason, "High capacity and secure digital steganography to palette-based images", Image Processing 2002. Proceedings 2002 International Conference, Rochester, New York, USA,2: 917-920, 2002.

[9] S. Sağıroğlu, M. Tunckanat, ″A Secure Internet Communication Tool'', Turkish Journal of Telecommunications, 1(1):40-46, 2002.

[10] S. Shahreza, "Stealth steganography in SMS" Wireless and Optical Communications Networks, 2006 IFIP International Conference, Bangalore, 2006.

[11] X.G. Sui, H. Luo, "A new steganography method based on hypertext" Radio Science Conference, 2004. Proceedings. 2004 Asia-Pacific, Qingdao, China, pp. 181-184, 2004.

[12] H.W. Tseng, C.C. Chang, "Steganography using JPEG-compressed images", The Fourth International Conference, Wuhan Computer and Information Technology, CIT '04., China, pp. 12- 17, 2004.

[13] A. Sahin, E. Buluş, M.T. Sakallı, "Gri Seviye Resimler Üzerinde Rasgele Lsb Yöntemini Ve Sayi Teorisini Kullanarak Bilgi Gizleme Ve Steganaliz" Akademik Bilişim Konferansları 2006-AB2006, Denizli-TÜRKİYE, 2006.

[14] S. Atawneh, A New Algorithm for Hiding Gray Images Using Blocks, IEEE 2006, Information Systems Security, Vol.15, Issue 6, 2006.

[15] Kh. Manglem Singh, L. Shyamsudar Singh, A. Buboo Singh, Kh. Subhabati Devi, Hiding Secret Message in Edges of the Images, Information and Communication Technology Conferance, 2007.

[16] X. Zhou, W. Gong, W. L. Fu, L. J. Jin, "An Improved Method for LSB Based Color Image steganography Combined with Cryptography", ICIS 2016, Okayama, Japan, June 26-29, 2016.

[17] G. S. Charan, N. Kumar S S V, B. Karthikeyan, V. Vaithiyanathan, D. Lakshmi K, "A Novel LSB Based Image Steganography With Multi-Level Encryption", IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems ICIIECS'15, India, 2015.

[18] D. Singla, Dr. M. Juneja, "New Information Hiding Technique using Features of Image", Journal of Emerging Technologies in Web Intelligence, 6(2): 237-242, May 2014.

[19] A. Singh, H. Singh, "An Improved LSB based Image Steganography Technique for RGB Images", IEEE International Conference on Electrical Computer and Communication technologies, pp. 1-4, 2015.

[20] K. Dasguptaa, J. Kumar Mondal, P. Dutta," Optimized video Steganography using Genetic Algorithm (GA)" First International Conference on Computational Intelligence:Modelling Techniques and Applications, vol: l0 pp. 131 – 137, 2013.

[21] Y. Yalman, D. Ertürk, "Sayısal Ses İçerisinde Gizli Veri Transferinin Kablosuz Ortamda Gerçekleştirilmesi", Politeknik Dergisi, 11(4): 319–327, 2008.

[22] T. Akbal, Y. Yalman, A. T. Özcerit, "Gerçek Zamanlı Sayısal Ses İçerisinde Sıkıştırılmış ve Şifrelenmiş Veri Transferi", III. Ağ ve Bilgi Güvenliği Sempozyumu, Çankaya Üniversitesi, Ankara, 5–6 Şubat, 2010.