

GÜVENLİ İLETİŞİM İÇİN VERİ GİZLEME TEKNİKLERİNİN KULLANIMI

Pınar ÇİVİCİOĞLU¹

Mustafa ALÇI²

¹Erciyes Üniversitesi, Sivil Havacılık YO, Uçak Elektroniği Bölümü, 38039, Kayseri

²Erciyes Üniversitesi, Mühendislik Fakültesi, Elektronik Mühendisliği Böl., 38039, Kayseri

¹e-posta: civici@erciyes.edu.tr

²e-posta: malci@erciyes.edu.tr

Anahtar sözcükler:Güvenli veri iletişimi, steganografi

ÖZET

Bu bildiride, güvenli veri iletişimini sağlamak için yararlanılan steganografi teknikleri tanıtılmış, bu teknikler kullanılarak, bir görüntünün içerisine bir başka görüntünün ya da bir metnin saklanabileceği gösterilmiştir. Bu amaç için kullanılacak oldukça fazla sayı ve çeşitte hazır program bulunmaktadır ancak bu çalışmada, hazır programlara gerek kalmadan herhangi bir uygun programlama dili kullanılarak da bilgi gizleme konusunda başarılı olunabileceği gösterilmiştir.

dijital ortamda gönderilmesi mümkün herhangi bir dosya olabilir [4].

Bilgi gizleme yöntemleri değerlendirildiğinde steganografi ve kriptografinin akraba olduklarından bahsedilebilir. Kriptografi, bir mesajı anlaşılacak bir şekle dönüştürmek için şifrelerken steganografi, mesajı görünmemesi için saklar. Steganografi yöntemlerinin çoğu, gizlenen mesajı şifreleyerek steganografi ve kriptografiyi birlikte kullanılır. Steganografi, kriptografi için bir tamamlayıcı durumundadır çünkü fazladan bir güvenlik katmanı daha eklenmesini sağlamaktadır.

1. GİRİŞ

Steganografi, bir bilgiyi, bir başka bilgi içerisinde saklama sanatı olarak tanımlanabilir [1]. Klasik steganografi, bir seri numarası, telif hakkına ait bir işaret gibi gizli bir mesajı, bilgisayar kodu, video filmi veya bir müzik kaydı gibi bir kılıf mesajı içerisine gömme yollarıyla ilgilenir. Gömme işlemi, genellikle bir parola kullanılarak yapılır ve bu parola bilinmeksizin üçüncü bir kişinin gizlenen bilgiyi bulması ya da yok etmesi çok zordur. Bilgi, kılıf işaretine gömüldükten sonra elde edilen işaret, stego-ışareti olarak adlandırılır. Mesela, bir marka, bir metnin içerisine gömüldükten sonra bu metin, stego-metni olarak adlandırılır. Aynı şekilde bir metin bir görüntü içerisine gömüldüğünde bu durumda da bir stego-görüntüsü elde edilir [2].

Steganografinin genel olarak amacı, gizlenen bilgiyi, istenmeyen kişilerin eline geçirmesi durumunda, bilginin gizlendiği ortam içerisinde bir bilgi sakladığına dair şüphelenmelerine meydan vermeyecek şekilde iyi saklayabilmektir. Yani steganografinin amacı, diğer kişilerin bir bilginin gizlendiğini öğrenmelerine engel olmaktır. Bir steganografi yöntemi, taşıyıcı ortamla ilgili şüphe yaratıyorsa, bu durumda yöntem başarılı olarak kabul edilemez [3]. Gizli mesajları taşıyan kılıflar, dijital olarak sıkça kullanılan ve masum görünümde olan görüntüler, resimler, sesler veya metinler olabilir. Gizlenen bilgi de düz bir yazı, şifreli bir yazı veya

Steganografinin diğer bir şekli, filigran oluşturma olarak adlandırılmaktadır ve ticari alanda gittikçe artan bir hızla kullanılmaktadır. Filigran oluşturmada taşıyıcı ortam dikkat çekecek şekilde değiştirilmeden küçük bir bilgi gömülür. Filigran oluşturma genellikle, telif hakkı alınan web sayfaları ya da ses dosyaları gibi dijital ortamların korunmasında kullanılır [3]. Filigran oluşturma ve steganografi arasındaki tek fark şudur: Filigran oluşturmada kılıf, haberleşme nesnesiyken steganografide, gizlenen mesaj haberleşme nesnesidir.

Dijital filigranların bir kısmı insan gözüyle görülebilirken diğer kısmı görülmeyebilir. Görülebilen filigranlar, genellikle görüntünün küçük bir alanıyla sınırlandırılmıştır ve kağıtlar üzerindeki ya da TV yayın istasyonlarında görülen geleneksel logolarla kıyaslanabilir. Bu filigranları kaldırmak isteyen kişiler, resimlerin ilgili kısmını keserek rahatlıkla kaldırabilir. Bu sebeple görünebilen filigranlar teknik olarak steganografi şeklinde değerlendirilmezler. Bu durumda görünmeyen filigranlar, görünen filigranlara göre daha fazla avantaj sağlamaktadır çünkü nerede bulundukları bilinmemektedir. Filigran oluşturma işleminde genel bir uygulama, filigranı tüm görüntü üzerinde yaymaktır. Böylece kırpmaya girişimlerine karşı koruma sağlanmış olacaktır [5].

Steganografi ve bilgi gizlemeyle ilgili kavramlar, çok yeni sayılmazlar. Steganografinin ilk kez

Yunanistan'da Altın Çağ döneminde kullanıldığı düşünülmektedir. Bu çağda insanlar, tabletler üzerine yazılar yazmışlar ve bu yazıların üzerini balmumuyla kapatarak yazıyı görünmez hale getirmişlerdir ve böylece o tableti gören kişiler üzerinde yazı olduğunu anlayamamışlardır.

Ustaca kullanılan diğer bir yöntem, bilgiyi taşıyacak kişinin başını traş ederek bilgiyi dövme şeklinde başına yazmaktır. Saçların uzamasıyla yazılan bilgi görünmez hale gelmekte ve bilgiyi taşıyacak kişinin başı tekrar traş edildiğinde saklanan bilgiye ulaşılabilir [6].

İkinci dünya savaşının başlarında steganografi teknolojisi hemen hemen sadece görünmeyen yazıların yazılabildiği “görünmeyen mürekkepleri” kapsamaktaydı. Bu mürekkepler genellikle, sirke, meyve suları ve süt gibi ısıtıldıkları zaman koyu renk alan maddelerden oluşmaktaydı. Ayrıca görünmeyen mürekkeplerin elde edilmesinde bazı kimyasal maddelerden de yararlanılmıştır. Masum bir mektup görünümündeki bir yazı, satır aralarına bu tip mürekkepler kullanılarak yazılan değişik yazılarla çok farklı mesajlar verebilmekteydi.

Steganografinin meşhur bir başka kullanımı, Margaret Thatcher'ın İngiltere başbakanı olduğu dönemde gerçekleşmiştir. 1980 yıllarında Margaret Thatcher, bakanlar kurulu dokümanlarının basına sızmasına çok sinirlenmiş ve kelime aralarında, bakanların kimliklerini şifrelemek için kelime işlemcileri programlatmıştır. Böylece bilgiyi sızdıran bakanların kim olduğunu tespit etmeye çalışmıştır [2].

Son yıllarda, bilgi gizleme konularına duyulan ilgi büyük oranda artmıştır [1-13]. Bunun sebebi, radyo, televizyon ve kitap yayıncılarının, dijital filmler, telif hakkı alınmış markalar, kitaplar ve ses kayıtlarındaki şifreli seri numaralarını gizleyen yöntemlere olan ilgilerinin artmış olmasıdır [2].

Bu çalışmada, gizlenecek bilgi olarak iki farklı mesaj işareti kullanılmıştır. Yapılan ilk deneyde, işaret işleme uygulamalarında sıkça kullanılan Peppers (Biberler) görüntüsü Mandrill görüntüsünün içerisine, ikinci deneyde de içerisinde “Erciyes Üniversitesi” yazılarının bulunduğu bir metin dosyası Lena görüntüsünün içerisine gizlenmiştir. Böylece steganografi ve kriptografinin ikisi de aynı anda kullanılmıştır.

2. STEGANOĞRAFI TEKNİKLERİ

Günümüzde, bilgiyi gizlemek için çok çeşitli teknikler kullanılmaktadır. Bu sebeple, kılıf ortamı seçildikten sonra, mesajı gizlemek için hangi yöntemin kullanılacağına karar verilmelidir. Görüntülerde bilgiyi saklamak için başvuru tekniklerden birçoğu, aşağıdaki yöntemleri kullanmaktadır [6]:

- Bilginin en düşük değerlikli bitte (LSB) saklanması
- Maskeleye ve filtreleme
- Algoritmalar ve dönüşümler

Bilginin ses veya video dosyalarında saklanmasıyla ilgili en sık başvuru yöntem, bilgiyi LSB içerisine yerleştirmektir. Bu yöntem kılıf dosyalarında çok küçük de olsa değişikliklere sebep olmaktadır. Eğer kılıf dosyası bir ses dosyası ise düşük seviyede yankılanmalar meydana gelir; eğer video dosyası ise, gözle ayırt edilemeyecek kadar küçük değişiklikler meydana gelir. Dijital görüntüler genellikle 24 bitlik ya da 8 bitlik dosyalar halinde kaydedilir. 24 bitlik bir görüntü, bilgiyi gizlemek için daha çok alan sağlar ancak oldukça büyük bir yer kaplar.

Pikseller için tüm renk değerleri, üç temel renkten elde edilir: kırmızı, yeşil ve mavi. Her temel renk, 1 bayt ile temsil edilir ve 24 bitlik görüntüler, bir renk değerini temsil etmek için piksel başına 3 bayt kullanır. 24 bitlik bir görüntünün her bir baytının LSB'sinde bir başka görüntüyü saklamak için her pikselin 3 biti kullanılır. Mesela, A harfini 3 pikselin içine saklamak isteyelim. 3 piksel için orijinal bilgi aşağıdaki şekilde olsun:

00100111	11101001	11001000
00100111	11001000	11101001
11001000	00100111	11101001

A'nın ikilik sistemdeki değeri, 10000011'dir. A'nın ikilik sistemdeki değerini 3 pikselin içine yerleştirdiğimiz zaman aşağıdaki bit düzemi elde edilir:

00100111	1110100 <u>0</u>	11001000
0010011 <u>0</u>	11001000	1110100 <u>0</u>
11001000	00100111	11101001

Kullanılan 8 bayt içerisinde sadece altı çizili bitler değiştirilmiştir. Bilgiler LSB'ye ya da LSB'den bir önceki bite yerleştirilse bile göz, aradaki farkı güçlüğüle ayırt edebilir.

3. KRİPTOLAMA VE STEGANOĞRAFI İÇİN KULLANILAN YÖNTEM

Steganografi yöntemlerinin çoğu, mesajın varlığının tespit edilmesi durumunda bir de deşifre için uğraşılmasını sağlamak amacıyla gizlenen mesajı şifreler. Yani steganografi ve kriptografi birlikte kullanılır. Steganografi, kriptografi için bir tamamlayıcı durumundadır çünkü fazladan bir güvenlik katmanı daha eklenmesini sağlamaktadır. Bu sebeple çalışmamızda steganografi ve kriptografi tekniklerinin her ikisi de kullanılmıştır.

Kullanılan algoritma, bilgilerin LSB'de gizlenmesi prensibine göre hazırlanmıştır: Bilgileri LSB'de saklamak için öncelikle nümerik bir anahtar seçilir. Seçilen bu anahtara bağlı olarak görüntüdeki

piksellerin yerleri değiştirilir ve ilgili pikseller bu yeni pozisyonlara yerleştirilir. Böylece kriptolama işlemi gerçekleştirilmiş olur. Bu dağılan pikselleri eski konumuna döndürebilmek için en başta seçilen anahtarın ne olduğunun bilinmesi gerekir. Son işlem olarak, kriptolanan veri, kılıf görüntüsünün LSB'lerinde saklanır.

4. GÖRÜNTÜ KALİTE ÖLÇÜTLERİ (IQM'ler)

Tanıtılan yöntemin başarısını değerlendirebilmek amacıyla işaret işlemede sıkça kullanılan kalite ölçütlerinden yararlanılmıştır: Karesel Ortalama Hata: *MSE* [14], Pearson korelasyon katsayısı: *Corr* [15] ve Tepe Sinyal-Gürültü Oranı: *PSNR*.

Kıyaslamada kullanılan *PSNR* ölçütü şöyle tanımlanır:

$$PSNR = 10 \log_{10} \left(\frac{I_{\max}^2}{MSE} \right) \text{ dB} \quad (1)$$

$I_{\max}$ değeri, referans görüntünün en büyük griton değeridir. *PSNR* karşılaştırmalarında standart sağlamak için bu değer genellikle 255 olarak kullanılır. Bu çalışmada $I_{\max}$ değeri olarak Şekil-1(a) ve 3(a)'daki görüntünün en büyük griton değeri kullanılmıştır. *MSE* değerinin hesaplanmasında,

$$MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (Y_{i,j} - S_{i,j})^2 \quad (2)$$

ifadesi kullanılır. Burada M görüntünün yatay boyutundaki, N ise dikey boyutundaki toplam piksel sayısıdır. $S_{i,j}$ orijinal görüntü pikselleri, $Y_{i,j}$ ise stego-görüntü pikselleridir [16]. Pearson korelasyon katsayısı *Corr*,

$$Corr = \frac{\sum \sum (S - \bar{S}) (Y - \bar{Y})}{\sqrt{\sum \sum (S - \bar{S})^2 \sum \sum (Y - \bar{Y})^2}} \quad (3)$$

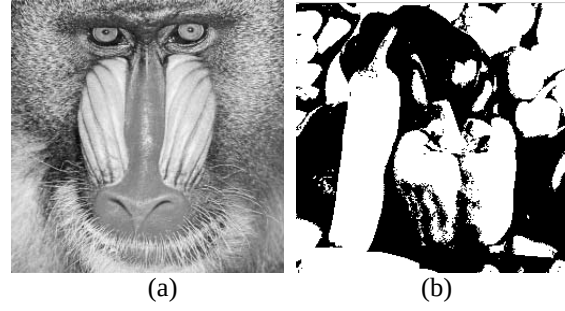
ile verilir. Burada,

$$\bar{S} = \frac{\sum \sum S}{M N} \text{ ve } \bar{Y} = \frac{\sum \sum Y}{M N} \quad (4)$$

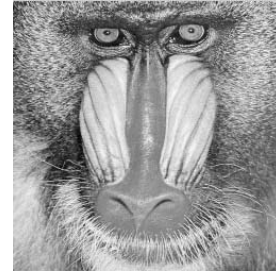
kullanılarak hesaplanır. S orijinal görüntü pikselleri, Y ise stego-görüntü pikselleridir.

5. GERÇEKLEŞTİRİLEN DENEYLER

Deneyler Şekil-1 ve Şekil-3'te verilen test görüntüleri üzerinde gerçekleştirilmiştir. Şekil-1(a) ve 3(a)'da verilen görüntüler, kılıf işareti olarak, Şekil-1(b) ve 3(b)'de verilen görüntüler ise mesaj işareti olarak kullanılmıştır. Sunulan yöntemin başarısı, Tablo-1 değerlendirilerek rahatlıkla görülebilmektedir.



Şekil-1. (a) Kılıf işareti olarak kullanılan Mandrill görüntüsü
(b) Mesaj işareti olarak kullanılan Peppers görüntüsü



Şekil-2. Tanıtılan yöntemin Şekil-1'deki işaretler için kullanılmasıyla elde edilen stego-görüntü



Şekil-3. (a) Kılıf işareti olarak kullanılan Lena görüntüsü
(b) Mesaj işareti olarak kullanılan metin



Şekil-4. Tanıtılan yöntemin Şekil-3'teki işaretler için kullanılmasıyla elde edilen stego-görüntü

Tablo 1. Elde edilen stego-görüntüler için hesaplanan IQM'ler

	<i>MSE</i>	<i>Corr</i>	<i>PSNR</i>
Mandrill içerisinde gizlenerek oluşturulan stego-görüntü için IQM'ler	0.49663	0.99983	51.17
Lena içerisinde Metin gizlenerek oluşturulan stego-görüntü için IQM'ler	0.50499	0.99992	51.098

6. SONUÇ

Bu bildiride, steganografi teknikleri kullanılarak bir görüntünün ve bir metin dosyasının önce kriptolanması, sonra da bir başka görüntü içerisinde gizlenmesi sağlanmıştır. Kullanılan yöntemi, uygun herhangi bir programlama diliyle kodlamak mümkündür. Şekil-2'de, Peppers görüntüsünün Mandrill kılıf görüntüsüne gizlenmesi sonucu elde edilen stego-görüntü, Şekil-4'te ise metin dosyasının Lena kılıf görüntüsüne gizlenmesi sonucu elde edilen stego-görüntü verilmiştir. Şekil-2 ve Şekil-4 incelendiğinde, Mandrill ve Lena görüntülerinin değişiminin görsel olarak fark edilemediği görülmektedir. Tablo-1'de, elde edilen stego-görüntüler için kullanılan kalite ölçütleri verilmiştir. Görüldüğü gibi, önerilen yöntemin bilgi saklamada kullanılmasıyla oldukça başarılı sonuçlar elde edilmektedir.

KAYNAKLAR

- [1] Cachin C., An Information-Theoretic Model for Steganography, PROCEEDINGS OF 2ND WORKSHOP ON INFORMATION HIDING, LECTURE NOTES IN COMPUTER SCIENCE, pp. 1-12, Springer, 1998.
- [2] Anderson R.J., Petitcolas F.A.P., On the Limits of Steganography, IEEE JOURNAL OF SELECTED AREAS IN COMMUNICATIONS, Vol. 16, No. 4, pp. 474-481, 1998.
- [3] Artz D., Digital Steganography: Hiding Data within Data, IEEE INTERNET COMPUTING, Vol. 5, No.3, pp. 75-80, 2001.
- [4] Johnson N.F., Jajodia S., Steganalysis: The Investigation of Hidden Information, IEEE INFORMATION TECHNOLOGY CONFERENCE, pp. 113-116, New York, USA, 1998.
- [5] Johnson N.F., An Introduction to Watermark Recovery from Images, PROCEEDINGS OF THE SANS INTRUSION DETECTION AND RESPONSE CONFERENCE, San Diego, CA, 1999.
- [6] Johnson N.F., Jajodia S., Exploring Steganography: Seeing the Unseen, IEEE COMPUTER, pp. 26-34, 1998.
- [7] Xia X.G., Boncelet C.G., Arce G.R., A Multiresolution Watermark for Digital Images, IEEE INTERNATIONAL CONFERENCE ON IMAGE PROCESSING, 1997.
- [8] Anderson R.J., Stretching the Limits of Steganography, Information Hiding, SPRINGER LECTURE NOTES IN COMPUTER SCIENCE, Vol. 1174, pp. 39-48, 1996.
- [9] Bender W., Gruhl D., Morimoto N., Lu A., Techniques for Data Hiding, IBM SYSTEMS JOURNAL, Vol. 35, No. 3-4, pp. 313-336, 1996.
- [10] Boland F.M., Ruanaidh O., Dautzenberg C., Watermarking Digital Images for Copyright Protection, PROCEEDINGS OF IEEE INTERNATIONAL CONFERENCE ON IMAGE PROCESSING AND ITS APPLICATIONS, Edinburgh, 1995.
- [11] Marvel L.M., Boncelet C.G., Retter C.T., Reliable Blind Information Hiding for Images, PROCEEDINGS OF INFORMATION HIDING WORKSHOP, Portland, Oregon, 1998.
- [12] Swanson M.D., Kobayashi M., Tewfik A.H., Multimedia Data-Embedding and Watermarking Technologies, PROCEEDINGS OF THE IEEE, Vol. 86, No. 6, pp. 1064-1087, 1998.
- [13] Moskowitz I.S., Longdon G.E., and Chang L.W., A New Paradigm Hidden in Steganography, NEW SECURITY PARADIGMS WORKSHOP PROCEEDINGS, pp. 41-50, 2000.
- [14] Greene N., Heckbert P.S., Creating Raster Omnimax Images from Multiple Perspectives Views Using the Elliptical Weighted Average Filter, IEEE COMPUTER GRAPHICS AND APPLICATIONS 6, pp.21-27, June 1986.
- [15] Umbaugh S. E., Computer Vision and Image Processing, Prentice Hall Inc., London, pp.153-171, 1998.
- [16] Eng H.L., Ma K.K., Noise Adaptive Soft-Switching Median Filter, IEEE TRANSACTIONS ON IMAGE PROCESSING, Vol.10, pp.242-251, 2001