RS STEGANALİZDE MASKELEME YÖNÜNÜN GİZLİ BİLGİNİN SEZİLMESİNE ETKİLERİ

Andaç ŞAHİN MESUT[1], Ercan BULUŞ[2], M. Tolga SAKALLI[1], H.Nusret BULUŞ[1]

[1]Trakya Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü
[2]Namık Kemal Üniversitesi, Çorlu Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü
andacs@trakya.edu.tr

ABSTRACT

Steganography is a very important hiding information technique and is commonly used on digital objects together with the developing technology in the last few years. One of the common methods used for hiding information on image files is LSB (Least Significant Bit Insertion) method. On the other hand, RS steganalysis is used in LSB method to find out hidden information on 8-bit and 24-bit colored images. In this study, we examine the effect of direction (from left to right or from top to bottom) of shift mask function used in mask process on detecting the information hidden on the image.

Keywords: Information Hiding, LSB Insertion Method, RS Steganalysis

1. GİRİŞ

Bilgi gizleme yönteminin önemli bir alt disiplini olan Steganografi, bir nesnenin içerisine bir verinin gizlenmesi olarak tanımlanabilir [1]. Steganografi'nin amacı gizli mesaj yada bilginin varlığını saklamaktır. Taşınmak istenen mesaj bir başka masum görünüşlü ortamda saklanarak, üçüncü şahısların iletilen mesajın varlığından haberdar olması engellenir. Steganografi; metin, resim ve ses steganografi olmak üzere üç alanda uygulanmaktadır.

Bu yaklaşımla ses, sayısal resim, video görüntüleri üzerine veri saklanabilir. Görüntü dosyaları içine saklanacak veriler metin dosyası olabileceği gibi, başka bir görüntü dosyası da olabilir [2].

Gizli bilgiyi bir resim içine gizleme işleminde iki dosya söz konusudur. Kapak resim ya da örtü verisi (cover image) olarak adlandırılan ilk dosya, gizli bilgiyi saklayacak olan resim dosyasıdır. İkinci dosya ise stego-text adı verilen gizlenecek olan mesajdır. Gizleme işlemi sonucunda kapak resim ve gizli mesajın oluşturduğu dosyaya "stego resim" adı verilir [3].

Görüntü steganografisinde bilgiyi resmin içine gizlemek için çeşitli yöntemler vardır. Bunlar şu şekilde sınıflandırılabilir.

- En önemsiz bite ekleme
- Maskeleme ve filtreleme
- Algoritmalar ve dönüşümler [4].

Steganaliz, bir örtü verisi (cover data) içerisinde herhangi bir bilgi olup olmadığını bulmayı ve eğer var ise bu bilgiyi elde etmek amacıyla steganografik algoritma kullanılan sisteme karşı yapılan saldırı yöntemleridir. Genelde saldırı yapan kişinin (steganalist) kullanılan steganografik sistemi bildiği varsayılır (Kerchoffs'un prensibi) [5].

Eğer steganalist kullanılan sistemi bilmiyorsa, bu onun işini zorlaştıracaktır. Steganalist bir steganografik sisteme saldırabilmesi için sahip olması gereken veriler vardır. Bu sahip olduğu verilere göre saldırı modellerinden birini seçebilir. Bu saldırı modelleri 5 kategoriye ayrılır [6]:

1. Sadece stego saldırısı: Analiz için sadece stego-nesnesi (Stego-object) (Görüntü dosyası) bilinmektedir.
2. Bilinen cover (örtü) saldırısı: Görüntünün mesaj gizlenmeden önceki ve sonraki hali bilinmektedir.
3. Bilinen mesaj saldırısı: Saklanan mesaj bilinmektedir.
4. Seçilmiş stego saldırısı: Steganografik algoritma ve stego-nesnesi bilinmektedir.
5. Seçilmiş mesaj saldırısı: Steganalist bu yöntemde stego-nesnesini analiz edebilmek için çeşitli mesajlar seçer, steganografik araçlar kullanır ve algoritmayı bulmaya çalışır.

Öncelikle resmin içinde veri gizlenip gizlenmediğini anlamak için sezme (detection) saldırıları yapılır. Bu saldırı yöntemleri;

- Histogram Analizi
- $\chi 2$ Testi
- RS Steganalizi

- RQP Yöntemi
- Görsel Ataklar

şeklinde sınıflandırılabilir [7].

Resmin içinde veri olduğu anlaşılırsa, bu veriyi elde etmek amacıyla çekme (extraction) saldırısı yapılır [8].

Bu çalışmada RS Steganalizde yapılan maskeleme işleminde doğru maske seçiminin [9] yanı sıra maske yönünün resmin içindeki gizli bilginin varlığının sezilmesinde önemli olup olmadığı incelenmiştir.

2. RS STEGANALİZ

Bu analiz, görüntülerde uzaysal korelâsyonlardan üretilen duyarlı ikili istatistiklerini kullanmaktadır. RS Steganalizi 24 bit renkli ve 8 bit gri seviye görüntülerde kullanılmaktadır. RS Steganaliz, görüntü dosyaları üzerinde En Önemsiz Bite Ekleme Yöntemine (LSB Insertion Methods) göre bilgi gizlenip gizlenmediğini anlamak için kullanılmaktadır. RS steganalizinde, bir görüntünün piksellerinin 3 bağımsız gruba: Düzenli (regular), Tekil (singular) ve Kullanılmayan (unused) olarak ayrılması esastır [10]. Fridrich tarafından geliştirilmiştir.

Test edilen görüntü (R), P kümesinden değer alan M x N piksel'lerden oluşmaktadır. Örnek olarak, 8-bit gri seviyeli bir görüntüde, P= {0,…, 255}'dir. Yapılacak ilk işlem olarak R, n komşu pikselden oluşan G ayrı gruplara bölünmektedir:

$$f(G) = f(x_1, x_2, ..., x_n) \in R \qquad (1)$$

Ayırıcı fonksiyon şu şekilde belirlenmiştir.

$$f(x_1, x_2, ..., x_n) = \sum_{i=1}^{n-1} |x_{i+1} - x_i| \qquad (2)$$

Örneğin $n = 4$ olarak seçildiğinde ayırma fonksiyonu aşağıdaki şekilde tanımlanabilir. (3)

$$G = (x_1, ..., x_4)$$
$$f(x_1, x_2, x_3, x_4) = |x_2 - x_1| + |x_3 - x_2| + |x_4 - x_3|$$

RS steganaliz için iki adet kaydırma fonksiyonu da kullanılmaktadır. Bu kaydırma fonksiyonları da şu şekilde tanımlanmaktadır.

$$F_1 : \quad 0 \leftrightarrow 1, 2 \leftrightarrow 3, 4 \leftrightarrow 5, ..., 254 \leftrightarrow 255$$
$$F_{-1} : \quad -1 \leftrightarrow 0, 1 \leftrightarrow 2, 3 \leftrightarrow 4, ..., 255 \leftrightarrow 256 \qquad (4)$$

$f(G)$ değerleri hesaplandıktan sonra bir maskeleme işlemi uygulanır. Maske (M), $(-1,0,1)$ değerlerinden oluşmaktadır. Bu maske G'ye uygulanır ve $F_M(G)$ değerleri hesaplanır. Maskenin değeri 1 ise F_1 kaydırma fonksiyonu, maske değeri -1 ise F_{-1} kaydırma fonksiyonu kullanılır. Daha sonra $-M$ maskesi içinde $F_{-M}(G)$ değerleri hesaplanır. Hesaplanan bu değerler aşağıdaki şartlara göre değerlendirilerek R_M , R_{-M} , S_M , S_{-M} , U_M ve U_{-M} sayıları hesaplanır.

- Eğer $f(F(G)) > f(G)$ ise G piksel grubu düzenlidir (R).
- Eğer $f(F(G)) < f(G)$ ise G piksel grubu tekildir (S).
- Eğer $f(F(G)) = f(G)$ ise G piksel grubu kullanılmayan (U) dır. [11]

Tüm G grupları için pozitif ve negatif maskeler kullanılarak R , S ve U gruplarının sayısı belirlenir.

Daha sonra resmin tüm piksellerinin son bitleri değiştirilir ve yukarıdaki işlemler tekrar edilir [12]. R_M , R_{-M} , S_M ve S_{-M} sayıları karşılaştırılarak bir sonuç elde edilir.

$$R_M \cong R_{-M}$$
$$S_M \cong S_{-M} \qquad (5)$$

Sıfır-mesaj hipotezine göre eğer yukarıdaki şart sağlanıyorsa resmin içine bilgi saklanmamış demektir. Değerlerin 0'a yakın çıkması resmin içinde bilgi olmadığını göstermektedir [11].

3. RS STEGANALİZ UYGULAMASI

RS Steganaliz uygulaması Microsoft Visual Basic 6.0 ortamında geliştirilmiştir. Program 24 bit renkli bmp yada gif formatında resmi alıp seçilen maske değerine göre her renk kanalı için ayrı ayrı olmak üzere Düzenli (Regular), Tekil (Singular) ve Kullanılmayan (Unused) grupların sayılarını belirlemektedir. Daha sonra elde edilen değerleri karşılaştırarak bir sonuca varmaktadır. Uygulamanın sözde programı (pseudo code) aşağıda verilmektedir.

Adım 1. Resmi seç
Adım 2. Maske değerlerini gir.
Adım 3. Her renk kanalı için ayrı ayrı uygulanmak üzere;
  i. Resmi 4'lü G gruba böl.
  ii. $f(G)$ ayırma fonksiyonu değerini hesapla.
  iii. Maske (M) değerlerine göre uygun kaydırma fonksiyonlarını kullanarak $f(F(G))$ değerini hesapla.
  iv. Ayırma ve kaydırma fonksiyonlarından elde edilen değerleri karşılaştırarak Düzenli (R- Regular), Tekil (S- Singular) ve Kullanılmayan (U- Unused) grupların sayılarını belirle.
  v. $-M$ için de Adım 3i, 3ii, 3iii ve 3iv'ü tekrarla.

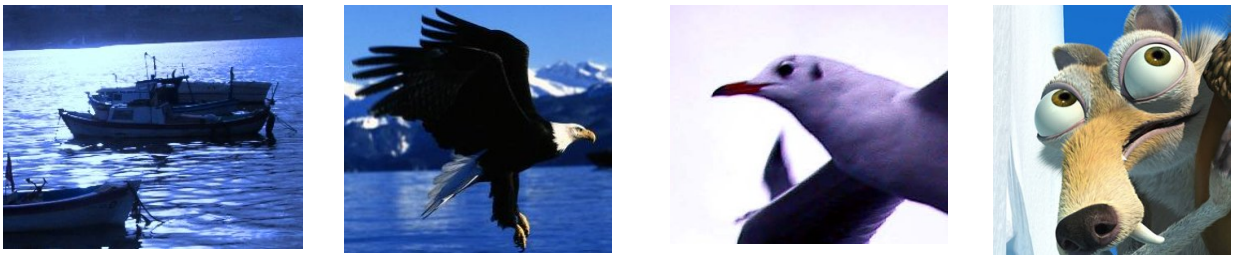
Adım 4. Resmin tüm piksellerinin her byte'nın son bitlerini değiştir ve Adım 3'ü tekrarla.
Adım 5. Her renk kanalı için orijinal resim ve son bitleri değiştirilmiş resimden elde edilen R_M , S_M ve U_M sayıları arasındaki farkı hesapla.

Programın çalışması sonucunda elde edilen fark değerleri 0'a ne kadar yakınsa resmin içinde bilgi yoktur denilebilir.

Maskeleme işleminde yönün önemini belirlemek için iki durumda değerlendirilme yapılmıştır. I. Durumda Adım 3.i'de yapılan 4'lü G gruba bölme işlemi soldan sağa doğru yapılmış ve maskeler de buna uygun şekilde soldan sağa doğru uygulanmıştır. II. Durumda ise Adım 3.i'deki resmi bölme işlemi yukarıdan aşağıya doğru yapılmış, maske değeri de yukarıdan aşağıya doğru uygulanmıştır. İki durumda da elde edilen RS Steganaliz sonuçları karşılaştırılmıştır.

Ölçümler için kullanılan resimler şekil 1'de verilmiştir. Maskeleme işleminde uygun bir maske olması dolayısıyla $M = (0,-1,1,-1)$ maskesi kullanılmıştır [9]. Maske yönünün önemli olup olmadığını anlamak amacı ile içinde bilgi olmayan resimler kullanılmıştır. Bu şekilde 0'a en yakın sonuç veren maske yönünün en etkin olduğu gözlenebilecektir.

Durum I ve Durum II'dan elde edilen sonuçlar Tablo 1'de verilmiştir.



(a) sandal.bmp (b) kartal.bmp (c) martı.bmp (d) scrat.bmp

Şekil 1. Ölçümler için kullanılan orijinal resimler

Tablo 1. $M = (0,-1,1,-1)$ kullanılarak elde edilen Durum I ve Durum II sonuçları. Değerler R (Red-Kırmızı), G (Gren-Yeşil) ve B (Blue-Mavi) renk kanalları için ayrı ayrı hesaplanmıştır.

		sandal.bmp		kartal.bmp		martı.bmp		scrat.bmp	
		I. Durum	II. Durum	I. Durum	II. Durum	I. Durum	II. Durum	I. Durum	II. Durum
R (Kırmızı) renk kanalı için	R	30	13	23	20	29	47	7	39
	S	30	13	23	20	29	47	7	39
	U	0	0	0	0	0	0	0	0
G (Yeşil) renk kanalı için	R	43	6	19	35	13	15	36	46
	S	43	6	19	35	13	15	36	46
	U	0	0	0	0	0	0	0	0
B (Mavi) renk kanalı için	R	22	32	6	6	9	31	9	45
	S	22	32	6	6	9	31	9	45
	U	0	0	0	0	0	0	0	45

$M = (0,-1,1,-1)$ kullanılarak yapılan ölçümler sonucu elde edilen Düzenli (Regular), Singular (Tekil) ve Kullanılmayan (Unused) grupların fark sayıları neticesinde II. Durum'un, yani resmin yukarıdan aşağıya doğru gruplanıp bu şekilde maskelenmesinin RS Steganaliz'de resmin içindeki bilginin sezilmesinde ters yönde etkili olduğu görülmüştür. Yukarıdan aşağıya doğru maskelemenin sandal.bmp'de daha iyi neticeler verdiği görülse de farklı maske seçimlerinde sağdan sola maskelemenin her zaman daha iyi olduğu yapılan ölçümler sonucunda görülmüştür.

4. SONUÇLAR

Teknolojinin çok hızlı bir şekilde gelişmesi ve internetin hızlanması ve yaygınlaşması neticesinde bilgisayar sistemlerinin güvenliği ve özellikle bilgi güvenliği oldukça önemli bir konu halini almıştır. İnternetin yaygınlaşması sonucunda veri alışverişi ve paylaşımı da artmıştır. Değişik türde verileri içeren farklı tipteki dosyalar dünyanın birçok yerindeki insanlar tarafından paylaşılabilir hale gelmiştir. Bu sayede dijital ortamların içine gönderilmek istenilen bilgilerin gizlenip diğer kişilere aktarılması oldukça kolaylaşmıştır. Bu yöntemin kötü amaçlı kişiler tarafından kullanılması toplum ve çevre güvenliğini tehlikeye sokmaktadır. Son yıllardaki birçok terör olaylarının planlanmasının bu şekilde yapıldığı bilinmektedir. Bu nedenle dijital ortamdaki verilerin içinde gizli bilgi olup olmadığının incelenmesi oldukça önemli bir konu haline gelmiştir. Bunu sezebilmek için çeşitli steganaliz yöntemleri geliştirilmiştir.

Bu çalışmada RS Steganaliz yöntemi için geliştirilmiş olan program ile yatay ve dikey olarak resimler maskelenmiş ve elde edilen sonuçlar neticesinde soldan-sağa doğru yapılan maskeleme işleminin daha iyi sonuçlar verdiği gözlemlenmiştir.

KAYNAKLAR

[1] Petitcolas F.A.P., Anderson R.J., Kuhn M.G., Information Hiding–A Survey, Proceedings of the IEEE, Special Issue on Protection of Multimedia Content, 87(7):1062-1078, July 1999.

[2] 86. Wang H., Wang S., "Cyber Warfare: Steganography vs. Steganalysis", Communications of the ACM, vol. 47, no. 10, October 2004.

[3] 44. Kharrazi M., Sencar H.T., Memon N, "Image Steganography: Concepts and Practice", WSPC/Lecture Notes Series, April 22, 2004.

[4] Sellars D., An Introduction to Steganography, Student Papers, 1999. http://www.cs.uct.ac.za/courses/CS400W/ NIS04/papers99/dsellars/index.html.

[5] Kerckhoffs A., La cryptographie militaire, Journal des Sciences Militaires, Feburary 1883.

[6] Lin, E. T., and Delp, E. J., A Review of Data Hiding in Digital Images, April 1999.

[7] Fridrich J., Goljan M., "Practical Steganalysis of Digital Images – State of the Art", In Proceedings of SPIE, Security and Watermarking Multimedia Contents IV (San Jose, CA, Jan. 21–24). International Society for Optical Engineering, 2002, 1–13.

[8] Phan R.C.W., Ling H.C., "Steganalysis of Random LSB Insertion Using Discrete Logarithms Proposed At Cıta03", M2USIC03, PJ, Malaysia, 2-3 October 2003.

[9] Şahin A, Buluş E., Sakallı M.T., Buluş H.N., "24-bit Renkli Resimler Üzerine Uygulanan RS Steganalizde Maske Seçimlerinin Etkileri",

Elektrik Elektronik Bilgisayar Mühendisliği Sempozyumu (ELECO 2006), Bursa-TÜRKİYE, Aralık 2006.

[10] Fridrich J., Goljan M., Du R., Reliable Detection of LSB Steganography in Color and Grayscale Images, Proc. of the ACM Workshop on Multimedia and Security, Ottawa, Canada, October 5, 2001, pp. 27-30.

[11] Fridrich J., Goljan M. and Du R., Detecting LSB Steganography in Color and Gray-Scale Images, Magazine of IEEE Multimedia Special Issue on Security, October-November 2001, pp. 22-28.

[12] Chandramouli R., Li G. And Memon N., Adaptive Steganography, Proc. Security and Watermarking of Multimedia Contents III, Special session on Steganalysis, SPIE Photonics West, Calif. 2002.