24-Bit RENKLİ RESİMLER ÜZERİNDE UYGULANAN RS STEGANALİZDE MASKE SEÇİMLERİNİN ETKİLERİ

Andaç ŞAHİN[1] Ercan BULUŞ[2] H. Nusret BULUŞ[3] M. Tolga SAKALLI[4]

[1,2,3,4]Bilgisayar Mühendisliği Bölümü
Mühendislik Mimarlık Fakültesi
Trakya Üniversitesi, 22030, Edirne

[1]e-posta: andacs@trakya.edu.tr
[2] e-posta: ercanb@trakya.edu.tr
[3] e-posta: nusretb@trakya.edu.tr
[4] e-posta: tolga@trakya.edu.tr

Anahtar sözcükler:Bilgi Gizleme, Steganografi, RS Steganaliz

ABSTRACT

LSB (Least Significant Bit Insertion) method is one of the important information hiding methods. 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 examined the efficiency of mask values chosen by us used in RS steganalysis. For this aim, we developed a computer program to evaluate the efficiency of these mask values on 24-bit colored unhidden images. According to the obtained results, we determined mask values which gives more correct results.

1. GİRİŞ

Steganografi önemli bir bilgi gizleme yöntemidir [1]. Bu yaklaşım, bir nesnenin içerisine bir verinin gizlenmesi olarak tanımlanabilir. Bu yaklaşımla ses, sayısal resim, video görüntüleri üzerine veri saklanabilir. Görüntü dosyaları içerisine saklanacak veriler metin dosyası olabileceği gibi, herhangi bir görüntü içerisine gizlenmiş başka bir görüntü dosyası da olabilir. Bu yaklaşımda içine bilgi gizlenen ortama örtü verisi (cover-data), oluşan ortama da stego-metin (stego-text) veya stego-nesnesi (stego-object) denmektedir.

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

- En önemsiz bite ekleme
- Maskeleme ve filtreleme
- Algoritmalar ve dönüşümler [2].

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) [3].

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 [4]:

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

- χ^2 Testi
- RS Steganalizi
- RQP Yöntemi
- Görsel Ataklar

şeklinde sınıflandırılabilir [5]. Resmin içinde veri olduğu anlaşılırsa, bu veriyi elde etmek amacıyla çekme (extraction) saldırısı yapılır.

Bu çalışmada RS Steganalizde kullanılan maske değerlerinin etkinliği incelenmiştir. Yöntemin doğru sonuçlar vermesi maske değerinin doğru seçilmesiyle sağlanabilir. Değerin yanlış seçilmesiyle bir resmin içinde bilgi saklı olmadığı halde saklıymış gibi sonuçlar üretmesi mümkün olmaktadır.

2. RS STEGANALİZ

Bu analiz, görüntülerde uzaysal korelasyonlardan üretilen duyarlı ikili istatistiklerini kullanmaktadır. RS steganalizi 24 bit renkli ve 8 bit gri seviye görüntülerde kullanılmaktadır. RS Steganaliz, görüntü dosyaları üzerinde Son 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 [6]. 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:

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

Ayırıcı fonksiyon şu şekilde belirlenmiştir.

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

Örneğin $n = 4$ olarak seçildiğinde ayırma fonksiyonu aşağıdaki şekilde tanımlanabilir:

$$G = (x_1, ..., x_4)$$

$$f(x_1, x_2, x_3, x_4) = |x_2 - x_1| + |x_3 - x_2| + |x_4 - x_3| \quad (3)$$

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

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

$f(G)$ 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. [7]

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 [8]. R_M, R_{-M}, S_M ve S_{-M} sayıları karşılaştırılarak bir sonuç elde edilir.

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

Sıfır-mesaj hipotezine göre eğer yukarıdaki şart sağlanıyorsa resmin içine bilgi saklanmamış demektir. Değerlerin 0'a yakın çıkması resmin içinde bilgi olmadığını göstermektedir [7].

3. GELİŞTİRİLEN 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 diyebiliriz.

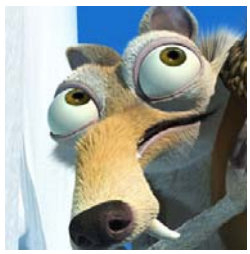
Seçilen maske değerlerinin etkinliğini araştırmak için içinde bilgi gizlenmemiş resimler kullanılmıştır.

Bu şekilde 0'a en yakın sonuç veren maske değerlerinin en etkin olduğu gözlenebilecektir. Şekil 1'de verilen ve içine bilgi gizlenmemiş olan çeşitli örnek resimler üzerinde değişik maske değerleri denenmiş ve elde edilen sonuçlar tablo 1'de verilmiştir. Örnek olarak 4 farklı maske denenmiştir.

(a) sabah.bmp

(b) kalp.bmp

(c) cicek.bmp



(d) scrat.bmp

Şekil 1 Ölçümler için kullanılan orijinal resimler

Tablo-1. (1,0,-1,1), (1,0,1,-1), (0,1,1,-1) ve (0,-1,1,-1) maske değerleri kullanılarak elde edilen Düzenli (Regular-R), Tekil (Singular-S) ve Kullanılmayan (Unused-U) gruplar arası fark değerleri. Değerler R (Red-Kırmızı), G (Gren-Yeşil) ve B (Blue-Mavi) renk kanalları için ayrı ayrı hesaplanmıştır.

(a) sabah.bmp için elde edilen değerler

Maske değerleri→		(1,0,-1,1)	(1,0,1,-1)	(0,1,1,-1)	(0,-1,1,-1)
R (Kırmızı) renk kanalı için	R	10	21	35	12
	S	9	32	35	12
	U	1	53	0	0
G (Yeşil) renk kanalı için	R	9	15	79	4
	S	15	29	79	4
	U	24	44	0	0
B (Mavi) renk kanalı için	R	15	19	17	7
	S	18	20	17	7
	U	33	39	0	0

(b) kalp.bmp için elde edilen değerler

Maske değerleri→		(1,0,-1,1)	(1,0,1,-1)	(0,1,1,-1)	(0,-1,1,-1)
R (Kırmızı) renk kanalı için	R	97	119	1132	23
	S	299	299	1132	23
	U	202	180	0	0
G (Yeşil) renk kanalı için	R	128	166	1147	7
	S	335	257	1147	7
	U	207	91	0	0
B (Mavi) renk kanalı için	R	140	179	949	12
	S	306	195	949	12
	U	166	16	0	0

(c) cicek.bmp için elde edilen değerler

Maske değerleri→		(1,0,-1,1)	(1,0,1,-1)	(0,1,1,-1)	(0,-1,1,-1)
R (Kırmızı) renk kanalı için	R	3	115	340	13
	S	21	189	340	13
	U	18	304	0	0
G (Yeşil) renk kanalı için	R	36	139	546	5
	S	77	228	546	5
	U	113	367	0	0
B (Mavi) renk kanalı için	R	71	125	280	29
	S	54	160	280	29
	U	125	285	0	0

(d) scrat.bmp için elde edilen değerler

Maske değerleri→		(1,0,-1,1)	(1,0,1,-1)	(0,1,1,-1)	(0,-1,1,-1)
R (Kırmızı) renk kanalı için	R	45	37	351	7
	S	165	163	351	7
	U	210	200	0	0
G (Yeşil) renk kanalı için	R	32	51	366	36
	S	66	95	366	36
	U	98	146	0	0
B (Mavi) renk kanalı için	R	165	172	343	9
	S	209	232	343	9
	U	374	404	0	0

Maske değerlerinin seçimi oldukça önemlidir. Örnek olarak seçilen 4 resim üzerinde (1,0,-1,1), (1,0,1,-1), (0,1,1,-1) ve (0,-1,1,-1) maske değerleri kullanılarak RS steganaliz uygulanmıştır. Tabloda bulunan fark değerlerinin 0'a yakın olması resmin içinde bilgi olmadığını ve bizim doğru bir maske seçtiğimizi göstermektedir. Tablodan da görülebileceği gibi fark değeri en az olan maske, tüm resimler için (0,-1,1,-1)'dir. Aradaki farkın en fazla olduğu maske değerinin ise (0,1,1,-1) olduğu görülmüştür.

4. SONUÇ

Internet üzerinden haberleşmenin hızlanması ve artmasıyla önemli bilgilerin bu ortamdan gizli bir şekilde gönderebilmesi oldukça önem kazanmıştır. Bununla birlikte gizli bilgi gönderme işlemi kötü amaçlar için de kullanılabilmektedir. Kötü amaçlı bilgi saklayan kişi, kurum, kuruluş veya terör örgütlerinin, kanunların izin verdiği ölçüde, iletişim bilgilerini ele geçirip önlem almak halkının güvenliğini sağlamaya çalışan güvenlik güçleri için büyük önem arz etmektedir. Bu yüzden gönderilen resimlerin içerisinde bilgi olup olmadığını anlamak ta önemli bir konu haline gelmiştir. Bunu anlamak amacıyla çeşitli steganaliz yöntemleri geliştirilmiştir. Yapılan çalışmada öncelikle RS steganaliz yöntemi detaylı olarak incelenmiş ve bu yöntemi kullanan bir yazılım geliştirilmiştir. Yazılım yardımıyla içine bilgi saklanılmış ve saklanılmamış pek çok resim incelenilmiştir. İncelemeler esnasında bu steganaliz yönteminde maske değerlerinin çok önemli bir rol oynadığı deneysel olarak ispatlanmıştır. Yanlış maske değerleri seçildiğinde içinde bilgi olmayan resimlerinde içinde bilgi olduğu sonucu elde edilebilmektedir. En doğru sonucu almak için şüpheli resim en uyun maske değeriyle incelenilmelidir.

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

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

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

[5] 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.

[6] 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.

[7] 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.

[8] 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.