RQP STEGANALİZDE RENK ÇİFTLERİ ARASINDAKİ YAKINLIK DERECESİ SEÇİMİNİN RESMİN İÇİNDEKİ GİZLİ BİLGİNİN SEZİLMESİNE ETKİSİ

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 information hiding method which has been used since ancient times. By the development of technology it is started to be used on digital objects. Steganalysis is an attack method which is used to discover if there is a secret data on a cover data. In this study, RQP Steganalysis method used on colored images and how efficient choosing proximity degrees between color pairs on perceiving information are examined.

Key words: Information Hiding, Steganopraphy, RQP Steganalysis

1. GİRİŞ

Steganografi çok eski çağlara dayanan bir bilgi gizleme sanatıdır [1]. Steganografi kelimesi kökleri "στεγαυος" ve "γραΦειν"'den gelen Yunan alfabesinden türetilmiştir. Tam olarak anlamı "kaplanmış yazı" (covered writing) demektir [2]. Steganografi gizli bir iletişim sağlamaktadır. Amacı iki kişi arasındaki iletişimin bir üçüncü şahıs tarafından fark edilememesidir. Bilimsel ortamda Steganografi çalışmaları 1983 yılında Simmons tarafından "Prisoner Problem"'in [3] tanımlanması ile başlamaktadır. Steganografi'nin amacı gizli mesaj ya da bilginin varlığını saklamaktır. Taşınmak istenen mesaj bir başka masum görünüşlü ortamda saklanarak, üçüncü şahısların iletilen mesajın varlığından haberdar olması engellenir.

Sayısal steganografi kullanım alanları açısından genel olarak üçe ayrılmaktadır. Bunlar; Metin (text) steganografi, Görüntü (image) steganografi ve Ses (audio) steganografi'dir.

Sayısal resimler dağıtımı en kolay ve internette hemen her sayfada karşılaşılabilecek dosyalardır. Kullanıldıkları formatlara göre farklılık göstermekle birlikte steganografi uygulamalarında en yaygın kullanılan ortamlar resim dosyalarıdır. Bu nedenle steganografi konusunda yapılan çalışmalar ve geliştirilen teknikler ağırlıklı olarak resim steganografi çerçevesinde yer almaktadır.

Görüntü dosyalarının içerisine bir metin gizlenebileceği gibi bir resim dosyasının içine bir başka resmi de gizlemek mümkündür.

Bu yaklaşımda içine bilgi gizlenen ortama örtü verisi (cover-data) veya örtü nesnesi (cover-object), oluşan ortama da stego-metin (stego-text) veya stego-nesnesi (stego-object) denmektedir [4]. Bir bilgiyi başka bir ortamın içine gizlenerek yeni bir ortam yaratılması işlemi Steganografik Sistem olarak adlandırılmaktadır. Gönderici bir gizleme fonksiyonu kullanarak bir steganogram yaratır. Gizleme fonksiyonu, verinin saklanacağı taşıyıcı ortam ve gizlenecek veri olmak üzere iki parametreye sahiptir [5].

Herhangi bir steganografik sisteminin temelde şeffaflık (transparency) ve sağlamlık (robustness) şartlarını sağlaması gerekmektedir. Şeffaflık saklanan verinin tespit edilememesi ve fark edilememesini ifade ederken sağlamlık saklanan verinin çıkartma işleminde düzgün bir şekilde geri getirilmesini anlatmaktadır. Gizleme Fonksiyonu olarak adlandırılan ve bilgi gizlemede en çok kullanılan yöntemler aşağıda gösterilmiştir:

- En önemsiz bite ekleme
- Maskeleme ve filtreleme
- Algoritmalar ve dönüşümler [6].

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) [7].

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 [8][9][10]:

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 [11].

Resmin içinde veri olduğu anlaşılırsa, bu veriyi elde etmek amacıyla çekme (extraction) saldırısı yapılır [12].

Bu çalışmada 24 bit renkli resimler içerisinde bilginin sezilmesi için kullanılan steganaliz yöntemlerinden biri olan RQP Steganaliz'de renk çiftlerinin arasındaki yakınlık derecesi seçiminin analiz için bir etkisi olup olmadığını anlamak amacıyla bir RQP Steganaliz uygulaması geliştirilmiş ve denemeler yapılmıştır.

2. RQP STEGANALİZ

RQP yöntemi Fridrich tarafından geliştirmiştir [13]. Bu metod LSB gizlemesi tarafından yaratılan yakın renk çiftlerini analiz etmeye yöneliktir. Öncelikle seçilen resim için yakın renk çiftlerinin tüm renk çiftlerine oranı hesaplanır. Daha sonra bu resim içerisine bir test mesajı gizlenerek oran yeniden hesaplanır. Bu iki oran arasındaki fark büyük ise resminin içinde gizlenmiş bilgi yok demektir. Bu iki oranın birbirine yakın olması resmin içinde gizlenmiş bilgi olduğunu göstermektedir.
RQP, örtü verisindeki yakın renk çiftlerinin sayısı, piksellerin sayısının %30'undan küçük olduğu sürece gayet iyi sonuçlar vermektedir. Eğer görüntüdeki yakın renk çiftlerinin sayısı piksellerin sayısının %50'sini geçerse, verilen sonuçlar giderek güvensiz olmaktadır.

RQP'ın başka dezavantajı, gri seviyeli görüntülerde uygulanmamasıdır.

3. RQP STEGANALİZ UYGULAMASI

Program BMP formatındaki 24 bit renkli resimler üzerinde çalışmaktadır. Öncelikle seçilen resim için yakın renk çiftlerinin tüm renk çiftlerine oranı (O_1) hesaplanmaktadır. Daha sonra bu resim içerisine bir test mesajı gizlenerek oran (O_2) yeniden hesaplanır.

Programın sahte kodu aşağıda verilmiştir.

Adım 1: Resmi seç.
Adım 2: Yakın renk çiftlerinin sayısını hesapla (renk çiftleri arasındaki fark her denemede değiştirilmiştir.)
Adım 3: Yakın renk çiftlerinin tüm renk çiftlerine oranını hesapla ve O_1 olarak belirle.
Adım 4: Seçilen resmin içine bir test mesajı gizle ve oranı tekrar hesaplayıp O_2 olarak belirle.
Adım 5: O_1 ile O_2 arasındaki farkı hesapla.

Programın çalışmasını incelemek amacıyla örnek olarak 10 adet resim seçilmiş ve Şekil 1'de gösterilmiştir.

Yakın renk çiftlerindeki yakınlık derecesinin etkisini ölçmek amacı ile yakınlık dereceleri sırasıyla 1,2,3 ve 5 olarak seçilmiş ve hem içinde bilgi gizli olmayan resimlere hem de içine bilgi gizlenmiş resimlere RQP Steganaliz uygulanmıştır. Kırmızı, yeşil ve mavi renk kanalları için ayrı ayrı olmak üzere pikselleri arasındaki renk farkları değerlendirilmiştir.

Resmin içine bilgi gizleme işlemi tarafımızdan geliştirilen Stego_LSB isimli program tarafından yapılmıştır [14].

(a) ataturk.bmp 400x300 piksel | (b) bahce.bmp 335x192 piksel | (c) balik.bmp 379x253 piksel | (d) cicek.bmp 312x223 piksel | (e) kalp.bmp 313x292 piksel

(f) kartal.bmp 269x249 piksel | (g) meyve.bmp 217x238 piksel | (h) oyuncak.bmp 240x192 piksel | (ı) resim.bmp 336x240 piksel | (i) scrat.bmp 292x308 piksel

Şekil 1. RQP Steganaliz için kullanılan örnek resimler

Program öncelikle yakın renk çiftlerinin sayısının renk çiftlerine oranının %50'yi geçip geçmediğini kontrol etmektedir. Eğer %50'yi geçerse bir uyarı mesajı verilmektedir.

Programın çalışması sonucunda seçilen yakınlık derecelerine göre yöntemin güvenilir olmadığı mesajı verilen resimler tablolarda **G.D.** harfleri ile edilen fark değerlerinin yanında belirtilmiştir.

Tablo 1. İçine bilgi gizlenmemiş resimlere uygulanan RQP steganaliz sonuçları

Çiftler Arasındaki Yakınlık Derecesi	**5**	**3**	**2**	**1**
ataturk.bmp	0,01293 **(G.D)**	0,02101	0,01074	0,02747
bahce.bmp	0,00967	0,01235	0,00648	0,00992
balik.bmp	0,00926	0,01347	0,00294	0,0127
cicek.bmp	0,01912 **(G.D)**	0,03320	0,01454	0,02366
kalp.bmp	0,00121 **(G.D)**	0,00360 **(G.D)**	0,01011 **(G.D)**	0,02950 **(G.D)**
kartal.bmp	0,00987 **(G.D)**	0,02643 **(G.D)**	0,01071 **(G.D)**	0,08694
meyve.bmp	0,02099	0,03352	0,00466	0,03346
oyuncak.bmp	0,01028	0,01079	0,00479	0,01026
resim.bmp	0,01018 **(G.D)**	0,01649	0,00730	0,02302
scrat.bmp	0,01391 **(G.D)**	0,02272	0,00518	0,03531

Tablo 2. İçinde bilgi gizli olan resimlere uygulanan RQP steganaliz sonuçları

Çiftler Arasındaki Yakınlık Derecesi	**5**	**3**	**2**	**1**
ataturk.bmp	0,00212	0,00302	0,00110	0,00355
bahce.bmp	0,00156	0,00213	0,00059	0,00185
balik.bmp	0,00120	0,00186	0,00009	0,00119
cicek.bmp	0,00269 **(G.D)**	0,00502	0,00414	0,00466
kalp.bmp	0,00024 **(G.D)**	0,00057 **(G.D)**	0,00126 **(G.D)**	0,00555 **(G.D)**
kartal.bmp	0,00238 **(G.D)**	0,00442 **(G.D)**	0,00097 **(G.D)**	0,01059
meyve.bmp	0,00354	0,00583	0,00236	0,00515
oyuncak.bmp	0,00182	0,00208	0,00091	0,00078
resim.bmp	0,00126	0,00119	0,00109	0,00204
scrat.bmp	0,00189	0,00379	0,00051	0,00461

RQP Steganaliz'e göre elde edilen farkın büyük olması resminin içinde gizlenmiş bilgi olmadığını göstermektedir. Ve O_1 ile O_2 arasındaki farkın yakın olması ise resmin içinde gizlenmiş bilgi olduğunu göstermektedir. Fakat bu büyüklük ve küçüklük göreceli bir kavramdır. Seçilen yakınlık derecesine göre aradaki farkın dağılımları farklılık göstermektedir. Aradaki farkın nasıl yorumlanması gerektiğini tam olarak belirleyebilmek için birçok resim üzerinde ölçümler yapılmıştır.

Yakınlık derecesi 5 olarak seçildiğinde yöntemin birçok resim için güvenilir sonuçlar vermediği belirlenmiştir. Bu resimler ve değerler tablolarda yer almaktadır. Çiftler arasındaki yakınlık derecesinin büyük seçilmesi, yakın renk çiftlerinin sayısını arttıracağından yöntemin güvenilirliğini azaltmaktadır.

Yakınlık derecesinin 1 olarak seçilmesi de değerler arasında büyük farklılıklara neden olmakta ve herhangi bir sonuca ulaşmamızı zorlaştırmaktadır.

Yakınlık derecesinin 3 olarak seçildiği durumda bilgi gizli olmayan resim dosyalarına uygulanan RQP steganaliz sonucunda fark değerlerinin yüzde seviyesinde olduğu görülmektedir. İçinde bilgi gizli olan dosyalarda ise bu fark binde seviyesine düşmektedir. Bu nedenle programın çalışması sonucunda elde edilen değerler binde seviyesinde ise resim içinde bilgi gizlenmiştir denilebilir [15].

2 olarak seçildiğinde ise bilgi gizli olmayan resimlerde elde edilen fark değerlerinin 0,01500 ile 0,00300 arasında değer aldığı görülmektedir. İçine bilgi gizlenmiş resimlerde ise 0,00500 ile 0 arasında değer alabileceği hesaplanmıştır. Kalp.bmp isimli resmin renk değerleri açısından karmaşık bir resim olmadığı için yakınlık derecesi 1 olsa bile RQP Steganaliz'in bu resimde güvenilir sonuçlar vermediği görülmüştür.

4. SONUÇLAR

Teknolojinin, özellikle bilgisayar sektörünün ve internetin gelişmesiyle birlikte bilgi güvenliği oldukça önemli bir konu haline gelmiştir. İnternet sayesinde artan veri alışverişi ve paylaşımı neticesinde metin, ses, resim gibi birçok veriyi içeren dosyalar dünyanın çeşitli yerlerindeki insanlar tarafından paylaşılabilir hale gelmiştir. Bu sayede dijital ortamların içine gönderilmek istenilen bilgilerin gizlenip diğer kişilere aktarılması oldukça kolaylaşmıştır. Fakat bu yöntemin kötü amaçlı kişiler tarafından kullanılması toplum ve çevre güvenliğini tehlikeye sokmaktadır. Birçok terörist faaliyetin bilgi gizleme kullanılarak planlandığı bilinmektedir. Bu nedenle dijital ortamdaki verilerin içinde gizli bilgi olup olmadığının incelenmesi oldukça önemli bir konu olarak karşımıza çıkmaktadır. Dijital ortamdaki dosyaların içinde gizli bilgi olup olmadığı incelemek amacıyla çeşitli steganaliz yöntemleri geliştirilmiştir.

Bu çalışmada 24 bit renkli resimler içinde bilgi olup olmadığını sezmek amacıyla geliştirilmiş olan RQP Steganaliz yöntemi açıklanmış ve yakınlık renk

çiftleri arasındaki yakınlık derecesinin etkili olup olmadığı izlenmiştir.

Görüntüdeki yakın renk çiftlerinin sayısı piksellerin sayısının %50'sini geçerse, verilen sonuçlar giderek güvensiz olmaktadır. Yakınlık derecesi büyüdükçe, yakın renk çifterinin sayısı artacağından yöntemin güvenilirliği azalmaktadır.

Yapılan ölçümler neticesinde yakınlık derecesinin 2 yada 3 olarak seçilmesinin yöntemin güvenilirliği açısından daha doğru olduğu sonucuna varılmıştır.

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] Murray A.H., Burchfiled R.W (eds.), "The Oxford English Dictionary: Being a Corrected Re-issue", Oxford, England: Clarendon Pres, 1933.

[3] Simmons G., "The Prisoners' Problem and the Subliminal Channel", CRYPTO83 Advances in Cryptology, pp. 51-67, Aug 22 -24, 1984.

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

[5] Westfeld A., Pfitzmann A., "Attacks on Steganographic Systems", Information Hiding. Third International Workshop, IH'99, Dresden, Germany, September/October, 1999, Proceedings, LNCS 1768, Springer-Verlag Berlin Heidelberg 2000.

[6] Sellars D., "An Introduction to Steganography", Online book, 1999.

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

[8] Biryukov A., "Methods of Cryptanalysis", PHd Thesis, 1999.

[9] Rijmen V., "Cryptanalysis and Design of Iterated Block Ciphers", PHd Thesis, October 1997.

[10] Stinson D.R., "Cryptography: Theory and Practice, Second Edition", CRC Press, 2002.

[11] 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.

[12] 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.

[13] Fridrich J., Du R., Meng L., "Steganalysis of LSB Encoding in Color Images", Proceedings IEEE International Conference on Multimedia and Expo, New York City, NY, July 30–August 2, 2000.

[14] Şahin A., Buluş E., Sakallı M.T., "24-Bit Renkli Resimler Üzerinde En Önemsiz Bite Ekleme Yöntemini Kullanarak Bilgi Gizleme", Trakya Üniversitesi Fen Bilimleri Dergisi, Edirne-Türkiye, 2006.

[15] Şahin A., Buluş E., Sakallı M.T., Buluş H.N., "Resim İçerisindeki Gizli Bilginin RQP Steganaliz Yöntemiyle Sezilmesi", Akademik Bilişim Konferansları 2007-AB2007, Kütahya-Türkiye, Şubat-2007.