

RESİM İÇERİSİNDEKİ GİZLİ BİLGİNİN RQP STEGANALİZ YÖNTEMİYLE SEZİLMESİ

Andaç ŞAHİN* , Ercan BULUŞ* , M. Tolga SAKALLI* ve H. Nusret BULUŞ*

(*) Trakya Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü,
22030, EDİRNE

andacs@trakya.edu.tr, ercanb@trakya.edu.tr, tolga@trakya.edu.tr, nusretb@trakya.edu.tr

ÖZET

Steganografi önemli bir bilgi gizleme yöntemidir ve son yıllarda teknolojinin gelişmesiyle birlikte dijital nesnelere üzerinde sıklıkla kullanılmaya başlanmıştır. Steganaliz ise bir örtü verisi içinde gizli veri olup olmadığını anlamaya yarayan saldırı yöntemleridir. Bu çalışmada RQP Steganaliz yöntemi açıklanmış ve RQP Steganaliz yapabilen bir uygulama geliştirilmiştir. Program sonucunda elde edilen değerlerin nasıl yorumlanması gerektiği incelenmiştir.

Anahtar Kelimeler: Steganografi, RQP Steganaliz, Bilgi Gizleme.

THE GRASP OF THE HIDDEN INFORMATION ON IMAGES WITH THE RQP STEGANALYSIS METHOD

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. On the other hand, steganalysis the group of the attack methods to understand information whether it is hidden on cover object or not. In this study, RQP steganalysis method is explained and an application for RQP steganalysis is developed. As a result, we express the results of our application.

Keywords: Steganography, RQP Steganalysis, Information Hiding.

1. GİRİŞ

Bilgi gizleme yönteminin önemli bir alt disiplini olan Steganografi, bir nesnenin içerisine bir verinin gizlenmesi olarak tanımlanabilir [1]. Steganografi kelimesi kökleri “στεγανος” ve “γραφειν”den gelen Yunan alfabesinden türetilmiştir. Tam olarak anlamı “kaplanmış yazı” (covered writing) demektir [2]. 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. 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.

Gizli bilgiyi bir resme gizleme işleminde iki dosya söz konusudur. Kapak resim ya da örtü verisi (cover image) olarak adlandırılan ilk dosya, gizli bilgiyi saklayacak resim dosyasıdır. İkinci dosya ise gizlenecek bilgi olan mesajdır. Bu mesaj da stego olarak isimlendirilmektedir. Mesaj; açık metin (plain text), şifreli metin (cipher text), başka resimler veya bit dizisi içinde saklanabilecek başka bir şey olabilir. Gömme işlemi sonucunda kapak resim ve gömülü mesajın oluşturduğu dosyaya “stego resim” adı verilir.

Görüntü dosyaları üzerinde bilgi gizlemek için çeşitli steganografik yöntemler geliştirilmiştir. Bunlar 3 başlık altında sınıflandırılabilir.

- En önemsiz bite ekleme
- Maskeleye ve filtreleme
- Algoritmalar ve dönüşümler [3].

En önemsiz bite ekleme en yaygın kullanılan bilgi gizleme yöntemlerinden biridir. Taşıyıcı ortamın en az önemli bitlerini insan gözünün fark edemeyeceği şekilde gizli veriyi saklamak amacıyla değiştirmeyi temel alır.

Maskeleme ve filtreleme yöntemleri genellikle 24 bit resimler için kullanılmakta olup resmin en önemsiz alanlarının tespit edilerek buralarda saklama yapılmasını temel almaktadır. Bu yöntemler genelde filigran uygulamalarında karşımıza çıkmaktadır. Maskeleme teknikleri JPEG formatındaki resim dosyaları için daha uygundur.

Dönüşümler ise yine daha çok JPEG dosyalar üzerinde kullanılmaktadır. En yaygın olarak kullanılan dönüşümler ise DCT (Discrete Cosine Transform) ve DFT (Discrete Fourier Transform)'dir.

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) [4].

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 [5][6][7]:

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 [8].

Resmin içinde veri olduğu anlaşılırsa, bu veriyi elde etmek amacıyla çekme (extraction) saldırısı yapılır [9].

Eğer resmin içindeki gizli veri bozulmak isteniyorsa resmin içinden bir parçayı kesip çıkarmak ya da resme başka bir veri daha gizlemek gibi saldırı yöntemleriyle de resim içindeki gizli bilgi etkisiz ve işe yaramaz hale getirilebilmektedir.

Bu çalışmada 24 bit renkli resimler içerisinde bilginin sezilmesi için kullanılan steganaliz yöntemlerinden biri olan RQP Steganaliz incelenmiş ve bir RQP Steganaliz uygulaması geliştirilmiştir.

2. RQP STEGANALİZ

RQP yöntemi Fridrich tarafından geliştirmiştir [10]. 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 resmin 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'nin 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.

Bu iki oran arasındaki farkın büyük olması resminin içinde gizlenmiş bilgi olmadığını göstermektedir. Bu iki oranın birbirine yakın olması ise resmin içinde gizlenmiş bilgi olduğunu göstermektedir. Fakat bu büyüklük ve küçüklük göreceli bir kavramdır. Aradaki farkın nasıl yorumlanması gerektiğini tam olarak belirleyebilmek için birçok resim üzerinde ölçümler yapılmıştır.

Programın çalışmasını incelemek amacıyla örnek olarak 10 adet resim seçilmiş ve Şekil 1’de gösterilmiştir. Öncelikle içinde bilgi gizli olmayan resimlere RQP Steganaliz uygulanmış ve elde edilen sonuçlar Tablo 1’de verilmiştir. Daha sonra aynı resimlerin içerisine bir metin gizlenmiştir ve tekrar RQP Steganaliz uygulanmıştır.

Resmin içine bilgi gizleme işlemi tarafımızdan geliştirilen Stego_LSB isimli program tarafından yapılmıştır [11]. Bunun sonucunda elde edilen değerler ise Tablo 2’de gösterilmiştir. İçinde bilgi gizli olan ve olmayan resimler için O_1 ve O_2 değerleri arasındaki farklar incelenmiştir.

Programın sahte kodu aşağıda verilmiştir.

- Adım 1:** Resmi seç.
- Adım 2:** Yakın renk çiftlerinin sayısını hesapla (renk çiftleri arasındaki fark 3’ten küçük olanlar yakın renk çifti olarak seçilmiştir.)
- 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.



(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



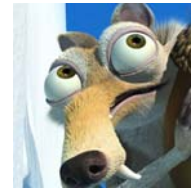
(g) meyve.bmp
217x238 piksel



(h) oyuncak.bmp
240x192 piksel



(i) resim.bmp
336x240 piksel



(j) scrat.bmp
292x308 piksel

Şekil 1. RQP Steganaliz için kullanılan örnek resimler

Tablo 1. İçine bilgi gizlenmemiş resimlere uygulanan RQP steganaliz sonuçları

	<i>O1</i>	<i>O2</i>	<i>Fark</i>
ataturk.bmp	0,30413	0,28312	0,02101
bahce.bmp	0,10332	0,09098	0,01235
balik.bmp	0,23569	0,22222	0,01347
cicek.bmp	0,35365	0,32045	0,03320
kalp.bmp	0,91485	0,91125	0,00360
kartal.bmp	0,68488	0,65845	0,02643
meyve.bmp	0,31941	0,28589	0,03352
oyuncak.bmp	0,12483	0,11404	0,01079
resim.bmp	0,39259	0,37610	0,01649
scrat.bmp	0,40881	0,38609	0,02272

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

	<i>O1</i>	<i>O2</i>	<i>Fark</i>
ataturk.bmp	0,28615	0,28312	0,00302
bahce.bmp	0,09311	0,09098	0,00213
balik.bmp	0,22408	0,22222	0,00186
cicek.bmp	0,32547	0,32045	0,00502
kalp.bmp	0,91182	0,91125	0,00057
kartal.bmp	0,66287	0,65845	0,00442
meyve.bmp	0,29172	0,28589	0,00583
oyuncak.bmp	0,11612	0,11404	0,00208
resim.bmp	0,37729	0,37610	0,00119
scrat.bmp	0,38988	0,38609	0,00379

Burada renk çiftlerinin arasındaki yakınlığın ne kadar olacağı da önemlidir. Bu çalışmada renk çiftleri arasındaki yakınlık 3 olarak alınmıştır. Kırmızı, yeşil ve mavi renk kanalları için ayrı ayrı olmak üzere pikselleri arasındaki renk farkları değerlendirilmiştir.

Tablo değerlerinden de görüleceği gibi içinde 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.

Yapılan denemeler sonucunda programın, görüntüdeki yakın renk çiftlerinin sayısının piksellerin sayısının %50'sini geçtiği durumlarda da doğru sonuçlar verdiği görülmüştür.

4. SONUÇLAR

Son yıllarda bilgisayar sistemlerinin güvenliği ve özellikle bilgi güvenliği oldukça önemli bir konu olarak karşımıza çıkmaktadır. Özellikle son 10 yılda internetin yaygınlaşmasıyla veri alışverişi ve paylaşımı da artmıştır. Metin, resim, ses vb. gibi birçok veriyi içeren dosyalar, etkin bir şekilde dünyanın birçok yerindeki 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. 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 resmin içinde bilgi olup olmadığını sezme amacıyla geliştirilmiş olan RQP Steganaliz yöntemi açıklanmış ve yöntemi anlatabilmek amacıyla BMP formatında 24 bitlik renkli resimler üzerinde çalışan bir uygulama geliştirilmiştir. Uygulamanın sonucunda elde edilen O_1 ile O_2 değerleri arasındaki farkın yüzde seviyesinde çıkmasının resmin içinde bilgi olmadığını, binde seviyesinde çıkması ise resmin içinde bilgi olduğunun göstergesi olduğu sonucuna varılmıştır.

5. 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., Burchfield R.W (eds.), “The Oxford English Dictionary: Being a Corrected Re-issue”, Oxford, England: Clarendon Press, 1933.
- [3] Sellars D., “An Introduction to Steganography”, Student Papers, 1999. <http://www.cs.uct.ac.za/courses/CS400W/NIS04/papers99/dsellars/index.html>
- [4] Kerckhoffs A., “La cryptographie militaire”, Journal des Sciences Militaires, February 1883.
- [5] Biryukov A., “Methods of Cryptanalysis”, PhD Thesis, 1999.
- [6] Rijmen V., “Cryptanalysis and Design of Iterated Block Ciphers”, PhD Thesis, October 1997.
- [7] Stinson D.R., “Cryptography: Theory and Practice, Second Edition”, CRC Press, 2002.
- [8] 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.
- [9] Phan R.C.W., Ling H.C., “Steganalysis of Random LSB Insertion Using Discrete Logarithms Proposed At Cita03”, M2USIC03, PJ, Malaysia, 2-3 October 2003.
- [10] 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.
- [11] Şahin A., Buluş E., Sakallı M.T., “24-Bit Renkli Resimler Üzerinde En Önemli Bite Ekleme Yöntemini Kullanarak Bilgi Gizleme”, Trakya Üniversitesi Fen Bilimleri Dergisi, Edirne-Türkiye, 2006.