# 4. Ağ ve Bilgi Güvenliği Sempozyumu

# LSB Ekleme Yönteminde Bilgi Gizleme İçin Tek Renk Kanal Kullanımının Güvenliğe Etkileri

Emir ÖZTÜRK[1] Andaç ŞAHİN MESUT[2] Altan MESUT[3]

[1,2,3]Bilgisayar Mühendisliği Bölümü, Trakya Üniversitesi, Edirne

[1]e-posta: emirozturk@trakya.edu.tr [2] e-posta: andacs@trakya.edu.tr
[3] e-posta: altanmesut@trakya.edu.tr

## Özetçe

Teknolojinin gelişmesiyle birlikte dijital ortamdaki verilerin güvenliğini sağlamak gerekliliği ortaya çıkmıştır. Bilgi güvenliği sağlamak amacıyla genellikle şifreleme teknikleri ve steganografi teknikleri kullanılmaktadır. Bu iki yöntem tek başlarına kullanılabildikleri gibi güvenliği arttırmak amacıyla birlikte de kullanılabilmektedir. Şifrelemede amaç verinin içeriğinin korunması iken steganografinin amacı verinin varlığının gizlenmesidir. Steganografik yöntemler metin, görüntü ve ses dosyalarına uygulanabilmektedir. Bu çalışmada görüntü dosyalarına bilgi gizlemede yaygın olarak kullanılan bir steganografi yöntemi olan LSB yönteminin, 24 bitlik bmp formatındaki bir görüntü üzerinde tüm renk kanalları kullanılmayıp seçilen herhangi bir renk kanalı üzerinde uygulanması incelenmektedir.

Anahtar Kelimeler: Steganografi, Steganaliz, En Önemsiz Bite Ekleme Yöntemi

## 1. Giriş

Bilgi gizleme yönteminin önemli bir alt disiplini olan Steganografi, bir nesnenin içerisine bir verinin gizlenmesi olarak tanımlanabilir [1]. Steganografi kelimesi kökleri "στεγανός" ve "γραφειυ"'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 [3].

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 [4].

Görüntü dosyalarına bilgi gizlemek için geliştirilen çeşitli steganografik yöntemleri 3 başlıkta toplamak mümkündür.

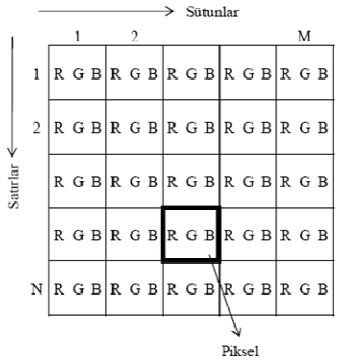
- En önemsiz bite ekleme
- Maskeleme ve filtreleme
- Algoritmalar ve dönüşümler [5].

En önemsiz bite ekleme yönteminde resmi oluşturan her pikselin her byte'nın en önemsiz biti olan son biti değiştirilerek o bitin yerine gizlenmesini istediğimiz verinin bitleri sırasıyla verinin başlangıcından itibaren birer birer yerleştirilmektedir. Bu yöntemde bilgi gizlemek amacıyla sayısal bir resmi oluşturan tüm renk kanalları (Kırmızı, Yeşil, Mavi – Red, Green, Blue) kullanılmaktadır.

Bu çalışmada 24 bitlik bmp formatındaki bir görüntü dosyasında tüm kanallar yerine sadece seçilen bir renk kanalının bilgi gizlenmesi amacıyla kullanılması durumunda bilginin sezilebilirliğinin değişip değişmediği incelenmektedir.

## 2. Sayısal Resmin Yapısı

Bir sayısal görüntü N satır ve M sütundan oluşan bir dizi şeklindedir. Dizinin her elmanı piksel olarak adlandırılır. En basit görüntülerde piksel değeri 1 veya 0 olabilir. Bu tip görüntülere ikili görüntü adı verilir. Genellikle 24 bitlik görüntüler üzerine veri gizleme işlemi yapılır. 24 bitlik görüntülerde bir piksel başına 3 byte kullanılmaktadır. Her pikselin rengi; Kırmızı (red), Yeşil (green), Mavi (blue) olmak üzere üç ana renkten elde edilmektedir. Buna pikselin RGB değeri denilmektedir [6].




*Şekil 1*: 24 bitlik renkli sayısal resmin yapısı.

24 bitlik bir görüntüde her renk 0 ile 255 arasında değer alabilen ikili kodlar olarak ifade edilir. Örneğin turkuaz renkli bir pikselin RGB kodu aşağıdaki gibidir.

R = 48 = 00110000
G = 214 = 11010110
B = 200 = 11001000

## 3. En Önemsiz Bite Ekleme Yöntemi

En önemsiz bite ekleme yöntemi (Least Significant Bit Insertion Methods) yaygın olarak kullanılan ve uygulaması basit bir yöntemdir. Fakat yöntemin dikkatsizce uygulanması durumunda veri kayıpları ortaya çıkmaktadır. Bu yöntemde; resmi oluşturan her pikselin her byte'nın en önemsiz biti olan son biti değiştirilerek o bitin yerine gizlenmesini istediğimiz verinin bitleri sırasıyla verinin başlangıcından itibaren birer birer yerleştirilmektedir. Burada her sekiz bitin en fazla bir biti değişikliğe uğratıldığından ve eğer değişiklik olmuşsa da değişiklik yapılan bitin byte'ın en az anlamlı biti olmasından dolayı, ortaya çıkan stego-resim (= örtü verisi + gömülü veri) değişimler insan tarafından algılanamaz boyutta olmaktadır. Son bite ekleme işlemi resmin başından ya da sonundan olmak üzere sıralı bir şekilde olabileceği gibi, bir rasgele fonksiyon üreteci (random function generator) kullanılarak belirlenen bir piksel üzerinde değişiklik yapılması şeklinde gerçekleştirilebilmektedir.

Bazı steganografik sistemler bazı gizli anahtarlar da kullanabilmektedir. Bu anahtarlar ikiye ayrılırlar:

1. Steganografik anahtarlar; mesajı resmin içine gizleme ve tekrar elde etme işlemini kontrol etme için kullanılırlar.
2. Kriptografik anahtarlar; Mesajın resmin içine gizlenmeden önce şifrelenmesi ve daha sonra deşifrelenmesinde kullanılırlar [7].

## 4. Steganografik Yöntemin Değerlendirilmesi

Bir steganografik yöntem ya da algoritma değerlendirilirken 3 temel kriter göz önünde bulundurulur. Bunlar

- Kapasite
- Taşıyıcıdaki değişim
- Dayanıklılık'tır.

Taşıyıcıdaki değişimi yada resimdeki bozulma oranının belirlenmesi için çeşitli ölçme yöntemleri vardır. Bunlar arasında en bilinenleri; MSE (Mean Squared Error), RMSE (Root Mean Squared Error) ve PSNR(Peak Signal to Noise Ratio)'dır [8]. MSE hataların kareleri toplamının ortalamasıdır. RMSE ise MSE'nin karekökü'dür. Bazen MSE yerine, hatanın büyüklüğünün orijinal piksel değerinin en büyüğü (peak-tepe) ile olan ilişkisi ile ilgilenilir. Bu gibi durumlarda PSNR yöntemi kullanılmaktadır.

Bir steganografik sistemin dayanıklılığını ölçmek için ise steganaliz yöntemleri kullanılmaktadır. 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 [9].

Kapasite kriterinde ise dosya türü önemli rol oynamaktadır.

## 5. Geliştirilen Uygulama ve Elde Edilen Sonuçlar

Uygulama Visual Studio.Net platformu kullanılarak geliştirilmiştir ve hem tüm kanallara son bite ekleme hem de seçilebilen tek bir renk kanalı üzerinde son bite ekleme yapabilmektedir. Geliştirilen program ayrıca orijinal ve bilgi gizlenmiş resimlerin histogramlarını çıkartabilmekte, resmin bozulma oranlarını ölçebilmekte ve görsel atak uygulayabilmektedir.

Bu yaklaşımın nasıl sonuçlar verdiğini inceleyebilmek amacıyla örnek olarak 4 resim seçilmiştir. Seçilen örnek resimler 24 bitlik bmp formatında görüntülerdir ve şekil 2'de verilmektedir. Daha sonra bu resimlere 3 KByte büyüklüğündeki Türkçe bir metin gizlenmiştir. Gizleme işlemi tüm renk kanallarında ve daha sonra ayrı ayrı renk kanalları üzerinde yapılmıştır. Bilgi gizleme işlemi sonucunda elde edilen bizli gizlenmiş resim dosyalarının sonuna hangi renk kanalının kullanıldığını belirten harfler eklenmiştir.


meyveler.bmp
210x230 piksel


deniz.bmp
210x230 piksel


nehir.bmp
210x230 piksel


çiçek.bmp
210x230 piksel

*Şekil 2*: Örnek olarak seçinle 24 bitlik bmp resimler

Yöntemi değerlendirebilmek amacıyla bilgi gizlenmiş resimlere sırasıyla bozulma oranlarını hesaplayabilmek için MSE ve PSNR ölçümleri, dayanıklılık kriterini ölçmek amacıyla RS Steganaliz ve Histogram analizi uygulanmış ve elde edilen değerler aşağıda verilmiştir.

PSNR ve MSE ölçümü için her kanal için ayrı hesaplama yapılmıştır. Elde edilen değerler Tablo 1'de verilmektedir. Genel görüş olarak PSNR değerlerinin yüksek MSE değerlerinin düşük olması resimde çok fazla bozulma olmadığını göstermektedir.

Tablo 1'deki değerlerden de görülebileceği gibi bilgi gizleme işlemi için tüm kanalların kullanılması durumunda MSE oranı üç renk kanalına yayılmakta fakat bilgi gizleme için tek renk kanalı kullanılması durumunda bozulma tek renk kanalında olduğu için MSE değeri bozulmanın olduğu renk kanalı için yüksek çıkmaktadır. Aynı durum PSNR değerleri için de geçerlidir. Bu durumda tek kanala gizlemenin kolaylıkla sezilebildiği düşünülebilir. Ancak bozulmayı ölçmek için orijinal resme ihtiyaç duyulduğu ve saldırganın elinde de orijinal resim olmadığı göz önünde bulundurulmalıdır. Genel olarak PSNR değerlerinin yüksek MSE değerlerinin düşük olması dolayısıyla bilgi gizlemek için tüm renk kanallarının kullanılması ya da sadece tek renk kanalının kullanılması durumlarının ikisinde de taşıyıcıdaki değişimin çok olmadığı söylenebilir.

*Tablo 1*:Bilgi gizlenmiş resimler ve orijinal resim arasındaki bozulma oranları (MSE ve PSNR)

| | MSE | | | PSNR | | |
|---|---|---|---|---|---|---|
| | **R** | **G** | **B** | **R** | **G** | **B** |
| meyveler-rgb.bmp | 0.08519669 | 0.08583851 | 0.08507247 | 58.82658 | 58.79398 | 58.83291 |
| meyveler-r.bmp | 0.2567081 | 0 | 0 | 54.03641 | Inf | Inf |
| meyveler-g.bmp | 0 | 0.2562526 | 0 | Inf | 54.04412 | Inf |
| meyveler-b.bmp | 0 | 0 | 0.2561284 | Inf | Inf | 54.04623 |
| deniz-rgb.bmp | 0.08440994 | 0.08509317 | 0.08457557 | 58.86687 | 58.83186 | 58.85835 |
| deniz-r.bmp | 0.256853 | 0 | 0 | 54.03396 | Inf | Inf |
| deniz-g.bmp | 0 | 0.2555694 | 0 | Inf | 54.05572 | Inf |
| deniz-b.bmp | 0 | 0 | 0.2558178 | Inf | Inf | 54.05149 |
| nehir-rgb.bmp | 0.08625259 | 0.08751553 | 0.08575569 | 58.77308 | 58.70995 | 58.79818 |
| nehir-r.bmp | 0.2570393 | 0 | 0 | 54.03081 | Inf | Inf |
| nehir-g.bmp | 0 | 0.2558592 | 0 | Inf | 54.05079 | Inf |
| nehir-b.bmp | 0 | 0 | 0.2559627 | Inf | Inf | 54.04904 |
| çiçek-rgb.bmp | 0.0852795 | 0.0842443 | 0.08608696 | 58.82236 | 58.8754 | 58.78143 |
| çiçek-r.bmp | 0.2550104 | 0 | 0 | 54.06522 | Inf | Inf |
| çiçek-g.bmp | 0 | 0.2547619 | 0 | Inf | 54.06946 | Inf |
| çiçek-b.bmp | 0 | 0 | 0.253913 | Inf | Inf | 54.08395 |

RS Steganalizde her renk kanalı için pikseller gruplara ayrılır. Seçilen maske değerine göre yapılan çeşitli kaydırma işlemleri sonucunda elde edilen değerlerin sıfır ya da sıfıra yakın çıkması o resim dosyasının içinde gizli bilgi olmadığını ya da steganografik algoritmanın çok iyi olduğunu ve bu analize karşı dayanıklı olduğunu göstermektedir. RS Steganalizde kaydırma işlemleri için kullanılan maske değeri daha önce yapılmış olan çalışmalarımız esnasında denenen ve en uygun sonuçları veren maskeler arasından seçilmiştir [10].

Tablo 2,3,4 ve 5'teki değerlere bakıldığında tüm renk kanallarına ya da seçilen bir renk kanalına bilgi gizlenmiş resimlere uygulanan RS steganaliz sonucunda anlamlı kabul edebileceğimiz seviyede farklı değerler elde edilmediği hatta nehir.bmp resminin kırmızı ve yeşil renk kanalı kullanılarak bilgi gizlenmesi sonucunda sıfır değerlerinin elde edilerek en iyi sonuçlara ulaşıldığı görülmüştür.

Bu durumda bilgi gizleme amacıyla tüm kanalların ya da tek bir renk kanalının kullanılmasının RS Steganaliz açısından çok fark etmediği görülmektedir.

*Tablo 2*: Bilgi gizlenmiş meyveler resmine $M = (0,-1,1,-1)$ kullanılarak elde edilen RS Steganaliz sonuçları

| | | meyveler-rgb.bmp | meyveler-r.bmp | meyveler-g.bmp | meyveler-b.bmp |
|---|---|---|---|---|---|
| R (Kırmızı) renk kanalı için | R | 7 | 12 | 10 | 10 |
| | S | 7 | 12 | 10 | 10 |
| | U | 0 | 0 | 0 | 0 |
| G (Yeşil) renk kanalı için | R | 8 | 5 | 2 | 5 |
| | S | 8 | 5 | 2 | 5 |
| | U | 0 | 0 | 0 | 0 |
| B (Mavi) renk kanalı için | R | 20 | 24 | 24 | 8 |
| | S | 20 | 24 | 24 | 8 |
| | U | 0 | 0 | 0 | 0 |

*Tablo 3*: Bilgi gizlenmiş deniz resmine $M = (0,-1,1,-1)$ kullanılarak elde edilen RS Steganaliz sonuçları

| | | deniz-rgb.bmp | deniz-r.bmp | deniz-g.bmp | deniz-b.bmp |
|---|---|---|---|---|---|
| R (Kırmızı) renk kanalı için | R | 27 | 18 | 27 | 27 |
| | S | 27 | 18 | 27 | 27 |
| | U | 0 | 0 | 0 | 0 |
| G (Yeşil) renk kanalı için | R | 33 | 35 | 20 | 35 |
| | S | 33 | 35 | 20 | 35 |
| | U | 0 | 0 | 0 | 0 |
| B (Mavi) renk kanalı için | R | 6 | 16 | 16 | 6 |
| | S | 6 | 16 | 16 | 6 |
| | U | 0 | 0 | 0 | 0 |

*Tablo 4*: Bilgi gizlenmiş nehir resmine $M = (0,-1,1,-1)$ kullanılarak elde edilen RS Steganaliz sonuçları

| | | nehir-rgb.bmp | nehir-r.bmp | nehir-g.bmp | nehir-b.bmp |
|---|---|---|---|---|---|
| R (Kırmızı) renk kanalı için | R | 2 | 1 | 0 | 0 |
| | S | 2 | 1 | 0 | 0 |
| | U | 0 | 0 | 0 | 0 |
| G (Yeşil) renk kanalı için | R | 2 | 4 | 6 | 4 |
| | S | 2 | 4 | 6 | 4 |
| | U | 0 | 0 | 0 | 0 |
| B (Mavi) renk kanalı için | R | 5 | 9 | 9 | 5 |
| | S | 5 | 9 | 9 | 5 |
| | U | 0 | 0 | 0 | 0 |

*Tablo 5*: Bilgi gizlenmiş çiçek resmine $M = (0,-1,1,-1)$ kullanılarak elde edilen RS Steganaliz sonuçları

| | | çiçek-rgb.bmp | çiçek-r.bmp | çiçek-g.bmp | çiçek-b.bmp |
|---|---|---|---|---|---|
| R (Kırmızı) renk kanalı için | R | 0 | 2 | 3 | 3 |
| | S | 0 | 2 | 3 | 3 |
| | U | 0 | 0 | 0 | 0 |
| G (Yeşil) renk kanalı için | R | 7 | 9 | 15 | 9 |
| | S | 7 | 9 | 15 | 9 |
| | U | 0 | 0 | 0 | 0 |
| B (Mavi) renk kanalı için | R | 2 | 5 | 5 | 3 |
| | S | 2 | 5 | 5 | 3 |
| | U | 0 | 0 | 0 | 0 |

.

Görsel ataklarda amaç dosyanın içinde veri olup olmadığını belirtmek ve varsa yeri hakkında da bilgi vermektir. Bu saldırı yöntemi Westfeld ve Pfitzmann tarafından geliştirilmiştir [7]. Genellikle LSB üzerinde etkili olan bu saldırı yönteminde amaç resim üzerindeki her pikselin LSB değerini arttırma üzerine kuruludur. Resim ilk pikselden son piksele kadar taranır, sadece son bit değerine göre işlem yapılır. Uygulaması çok basit olmakla beraber karmaşık yüzeylerde anlaşılırlığı zordur.

Meyveler resminin orijinal haline uygulanan görsel atak sonucu şekil 3'te ve bilgi gizlenmiş hallerine uygulanan görsel atak sonucu şekil 4'te gösterilmiştir.

meyveler.bmp

*Şekil 3*: Orijinal meyveler.bmp resmine uygulanan görsel atak sonucu

meyveler-rgb.bmp

meyveler-r.bmp

meyveler-g.bmp

meyveler-b.bmp

*Şekil 4*: Bilgi gizlenmiş meyveler resminlerine uygulanan görsel atak sonucu

Şekillerden de görüleceği üzere resmin karmaşık yüzeye sahip olmasından dolayı saldırgan kesin bir yargıya varamayacaktır.

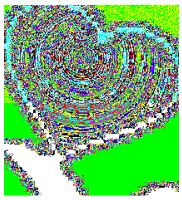
Genellikle düz yüzeyli renk geçişleri az olan resimlerde uygulanması daha iyi sonuçlar vermektedir. Bu durumu göstermek amacıyla 210x230 piksel boyutundaki kalp.bmp resmine 3 Kbyte bilgi tüm kanallarına ve seçilen kanalına gizlenmiş ve görsel atak uygulanmıştır. Orijinal resime uygulanan görsel atak sonucu şekil 5'te, bilgi gizlenmiş resimlere uygulanan görsel atak sonuçları ise şekil 6'da gösterilmiştir.

kalp.bmp
210x230 piksel

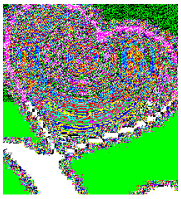
görsel atak yapılmış hali

*Şekil 5*: Orijinal kalp.bmp resmi ve uygulanan görsel atak sonucu

kalp-rgb.bmp



kalp-r.bmp



kalp-g.bmp

kalp-b.bmp

*Şekil 6*: Bilgi gizlenmiş kalp resimlerine uygulanan görsel atak sonucu

Arka yüzeyin düz ve renk geçişlerinin çok olmadığı bir resim dosyasına yapılan görsel ataklar daha iyi sonuçlar vermektedir. Burada yeşil renk kanalına saklanan bilginin diğer kanallara yada tüm renk kanallarına saklamaya nazaran daha çok sezilebildiği görülebilmektedir.

## 6. 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 çalışmada yaygın olarak kullanılan LSB yönteminde bilgi gizleme amacıyla tüm renk kanallarının değil de seçilen bir renk kanalının kullanılmasının güvenliği nasıl etkilediği incelenmiştir. Bu durum güvenliği negatif yönde etkilememekle birlikte saldırganın işini daha zorlaştırmak amacıyla kolaylıkla uygulanabilir. Saldırganın elinde orijinal resim olmadığı için bilgiyi sezmek ve elde etmek için daha fazla çaba sarf etmesi gerekmektedir. Ayrıca bilgi gizleme işleminin sıralı değil de bir anahtar değere göre rastgele yapılması steganalitik saldırılara karşı daha güçlü olmasını sağlayacaktır.

## 7. Kaynakça


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

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

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

[6] Morkel T., Eloff J.H.P., Olivier M.S., "An Overview of Image Steganography", Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005/

[7] 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. 70.

[8] Sayood K.: "Introduction to Data Compression", Morgan Kauffman Publishers, Inc. 340 Pine Street, Sixth Floor, San Francisco, CA 94104-3205, USA, 1996. 61.

[9] 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.

[10] Şahin A., Buluş E.,Buluş H.N., Sakallı M.T., "24-bit Renkli Resimler Üzerine Uygulanan RS Steganalizde Maske Seçimlerinin Etkileri" Elektrik Elektronik Bilgisayar Mühendisliği Sempozyumu (ELECO 2006), Bursa-TÜRKİYE, Aralık-2006.