Çok Katmanlı Görüntü Steganografi

E. Avcı, T.Tuncer, F.Ertam

***Özet*—Bir steganografik metodu değerledirebilmek için örtü verideki değişim ve örtü verinin taşıma kapasite ele alınmalıdır. Steganografik metotlarda en temel amaç kapasiteyi arttırmak ve örtü verideki değişimi azaltmaktır. Ancak kapasiteyle örtü verisindeki değişim ters orantılı olduğu için bu iki amaç aynı anda gerçekleşemez. Örtü verisindeki değişimi sabit tutup kapasiteyi arttırmak için çok katmanlı steganografi kullanılmaktadır. Bu çalışmada çok katmanlı görüntü steganografi ele alınacak ve çok katmanlı olmayan metotlarla karşılaştırılacaktır.**

***Anahtar Kelimeler*—Görüntü Steganografi, Bilgi Güvenliği, Çok katmanlı steganografi, Veri Gizleme**

Multi-Layered Image Steganography

***Abstract*— Change of the cover object and capacity of the cover object should be addressed in order to appreciate a steganographic method. The main purpose of steganographic methods is increasing capacity and reduce the changes of cover object. However, capacity is inversely proportional to the change in cover object, these two goals cannot be realized simultaneously. Multi-layer steganography is used for change of the cover object was kept constant in order to increase capacity. In this study, a multi-layered image steganography will be discussed and this method will be compared with non-multi-layered methods.**

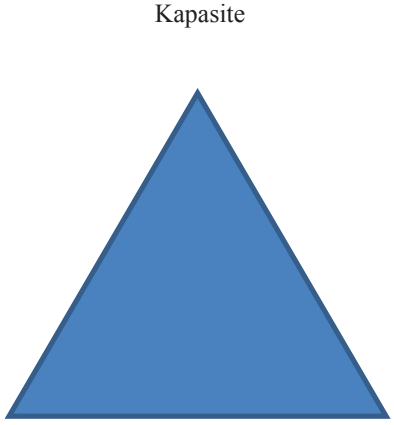
***Keywords*—Image Steganography, Information Security, Multi-Layer Steganography, Information Hiding**

I. GİRİŞ

Bilgi gizleme teknikleri eski çağlardan günümüze kadar kullanılan tekniklerdir. Bu tekniklerin temel amacı, gönderilecek verileri güvenilir bir kanal oluşturup o kanal vasıtasıyla aktarabilmektir. Günümüz dijital dünyasında birçok bilgi gizleme tekniği geliştirilmiştir ve geliştirilmeye devam edilmektedir [1]. Bilgi gizlemenin en önemli alt dallarından biri olan steganografi dijital medya verilerinin korunması için kullanılmaktadır. Steganografi; hem bilimsel olarak bilgi gizlemenin alt dalı hem de bilgiyi saklama sanatı olarak adlandırılır [8]. Steganaliz ise gizli iletişim kanalları dinleyip, yapılan iletişimi ele geçirmek için yapılan saldırıları ve analizleri içermektedir.

Engin Avcı, Fırat Üniversitesi Teknoloji Fakültesi Yazılım Mühendisliği Bölümü 23100 Elazığ, Türkiye (e-posta: enginavci@firat.edu.tr).
Türker Tuncer, Fırat Üniversitesi Teknoloji Fakültesi Adli Bilişim Mühendisliği Bölümü 23100 Elazığ, Türkiye (e-posta: turkertuncer@firat.edu.tr).
Fatih Ertam, Fırat Üniversitesi Bilgi İşlem Daire Başkanlığı, 23100, Elazığ, Türkiye (e-posta: faith.ertam@firat.edu.tr)

Bir steganografik sistem farklı bakış açılarıyla değerlendirilmektedir. Bunlar bilgi gizlenen örtü verisi (cover object) ne kadar değiştiği, bilgi saklama kapasitesinin ne kadar olduğu ve sistemin dayanıklılığının ne kadar olduğudur [2]. Bir steganografik sistemin başarımını değerlendirmek için bu üç kritere bakılması gerekmektedir. Bu kriterleri steganografi ve steganaliz alanında çalışmaları olan bilim insanı Jessica Fridrich ortaya atmıştır ve Fridrich üçgeni şekil 1'de belirtilmiştir.



Şekil 1. Fridrich Üçgeni

Günümüzde birçok steganografik metot vardır ve bu metotların başarımının ölçülmesi için yukarıdaki üçgen referans alınmalıdır.

Her steganografik yöntem algoritmik olarak farklı metotlar izlediği için farklı analiz metotları geliştirilmiştir. Bundan dolayı her metodun kendine özgü bir steganaliz metodu bulunmaktadır [4].

Bu makalede çok katmanlı görüntü steganografiden bahsedilecektir. Temel amaç görüntünün içerisine veri ve o verinin içerisinede aynı algoritmayla veri gizlemektir. Veri gizleme ve çıkarma işlemleri ilerleye bölümlerde ayrıntılı bir şekilde anlatılacaktır.

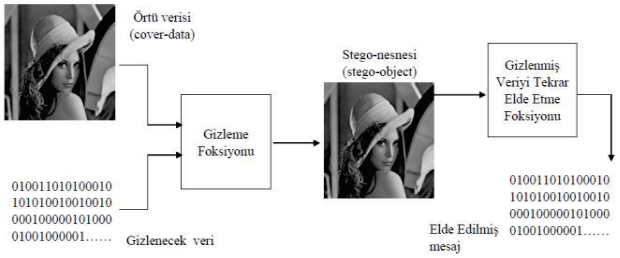
Çalışmanın 2. Bölümünde görüntü steganografi, üçüncü bölümde çok seviyeli katmanlı steganografi, dördüncü bölümde geliştirilen uygulama ve 5. ve son bölümde sonuç ve öneriler yer alacaktır.

II. GÖRÜNTÜ STEGANOGRAFİ

Steganografi tekniğinin en sık uygulandığı medya formatları görüntü formatlarıdır ve günümüzde yaygın şekilde kullanılmaktadır. Yaygın kullanılmasının en önemli sebeplerin biri ise kapasitedir.

Dijital görüntülerin dağıtımı kolay ve internette hemen hemen her sayfada bulundukları için steganografik iletişim açısında sıkça kullanılabilecek dosyalardır.

Görüntü dosyalarına steganografinin uygulanabilmesi için ön şart resmin dijitalleştirilmesidir. Piksel değerleri alındıktan sonra hangi gizleme fonksiyonun kullanılacağı seçilir. Gizleme fonksiyonu seçildikten sonra gömülecek verinin boyutu, tipi ve örtü nesnesinin neresine gömüleceği hakkındaki bilgiler alınarak Steganografi anahtar oluşturulmalıdır. Anahtar istenilirse şifrelenir. Ardından gömülecek veri gizleme fonksiyonu kullanılarak örtü nesnesine gizlenir ve Stego resmi veya steganogram oluşturulur.



Şekil 2.Görüntüler için kullanılan steganografik sistem diyagramı

Herhangi bir steganografik sistemin kabul edilebilmesi için Fridrich üçgeninde gösterilen üç temel şartı sağlaması gerekmektedir. Bunlar algılanabilirlik, sağlamlık ve kapasitedir. Algılanabilirlik; taşıyıcı nesnenin (Stego-object) içerisinde bilgi olup olmadığının sezilmesidir. Eğer bir sistemde bilgi varlığı ne kadar az sezilirse o sistem o kadar güvenilirdir. Sağlamlık koşulunda ise gizli verinin ne kadarlık kısmı iletim hattında bozulmadan alıcı tarafa iletilebildiğinin ölçütüdür. Gizli veri iletişim kanalındaki gürültü ve saldırılardan ne kadar az etkilenmişse sistem o kadar sağlamdır. Kapasite ise örtü verisinin (cover data) ne kadarlık bilgi taşıyabileceğiyle ilgilidir. Örtü verisi ne kadar çok bilgi taşırsa o kadarlık kapasiteye sahip demektir. Örneğin steganografın elinde here piksele bir bitlik bilgi saklayabileceği bir gizleme fonksiyonu olsun ve anahtar resme gömülmesin, böyle bir steganografik sistemin kapasitesi aşağıdaki gibi gösterilmiştir.

$$S = mnk \tag{1}$$

$$B = 8b \tag{2}$$

$$K = \frac{S}{8} \tag{3}$$

S resmin piksel sayısı veya kaç byte' tan oluştuğu temsil etmektedir. m satır sayısı, n sütun sayısı ve k katman sayılarını sembolize etmektedir. Her pikselin bir baytlık bilgi taşıdığı düşünülecek olursa formül 1 resmin kaç bytelık resim olduğu bilgisini vermektedir. Eğer resim RGB formatında ise k 3 değerini alacaktır, gri seviyeli bir resim ise k değeri 1 olacaktır. 1 baytın 8 bit olduğu formül 2' te gösterilmiştir. Gizleme fonksiyonun özelliği ve eldeki bilgilerden yola çıkılarak formül 3' deki kapasite denklemi elde edilmiş olur.

Kusursuz bir steganografik sistemin oluşturulması için algılanabilirlik, sağlamlık ve kapasite ölçütlerinin maksimize edilmesi gerekmektedir fakat taşıyıcının kapasitesi arttıkça algılanabilirliği artmakta ve algılanabilen bir sistem kabul edilmez bir hal almaktadır. Aynı zamanda kapasitesi arttırılan bir steganografik sistemde sağlamlıktan bahsetmekte zor olacaktır. Çünkü taşınan veri iletim kanalında gerçekleşen kayıp ve saldırılardan doğrudan etkilenecektir. Bu 3 ölçütü mükemmel kullanabilen bir saklama fonksiyonu halen geliştirilememiştir ve bu sebepten dolayı ölçütlerde kabul edilebilir kıstaslar konularak gizleme fonksiyonları değerlendirilmeye çalışılmaktadır. Bu ölçütlerin en iyi sağlandığı veriler görüntü verileri (resim ve videolar) olduğu için Görüntü Steganografi çok sık kullanılmaktadır[5].

Görüntü steganografide en sık kullanılan metotlar ise aşağıda verilmiştir

En önemsiz bit değiştirme
Maskeleme ve filtreleme
Algoritmalar ve dönüşümler [2]

III. ÇOK KATMANLI STEGANOGRAFİ

Çok katmanlı steganografik yöntemler taşıyıcının kapasitesini ve güvenliği arttırmak amacıyla ortaya atılmıştır[6]. Örneğin taşıma kapasitesi 10 Kb olan bir örtü verisinin kapasitesini 12 Kb' e çıkarılmak amaçlanmıştır. Çok katmanlı steganografinin bir diğer avantajı ise kapasiteyi artırırken taşıyıcıdaki değişim yok denecek şekilde artmaktadır veya hiç artmamaktadır[7]. Çok katmanlı steganografinin matematiksel modelli aşağıdaki gibidir.

$$s = log_{\left(\frac{b}{e}\right)}(MNk) \tag{4}$$

$$C = \sum_{n=1}^{s} \left(\frac{MNk}{\left(\frac{b}{e}\right)^n} \right) \tag{5}$$

$$C' = \frac{MNk}{\left(\frac{b}{e}\right)} \tag{6}$$

$$K = \frac{C - C'}{C'} 100 \tag{7}$$

$$r = \frac{C}{MNk} 100 \tag{8}$$

s seviye sayısını, b piksel değerlerinin kaç bitle ifade edildiğini, e bir piksele gömülecek bit sayısını, M resimdeki satır sayısını,N sütun sayısını, k katman sayısını, C' tek katmanlı steganografi kullanılarak yapılan gizlemede örtü verisinin kapasitesini, C çok katmanlı steganografi kullanılarak

yapılan gizlemede örtü verisinin kapasitesini, K kazancı ve r ise gizlenmiş verinin örtü verisine olan oranını ifade etmektedir.

TABLO I. Tek Seviyeli ve Çok Seviyeli (Soğan) Steganografi Veri Gizleme Kapasiteleri (LSB Tekniği, b=8, e=1)

Çok Katmanlı Steganografi Kullanılarak Elde Edilen Kazançlar (LSB Tekniği, b=8, e=1, 1 bpp)				
Boyut	64X64	256X256	512X512	1536X1536
Seviye	4	5	6	7
Kazanç (%)	14.2578	14.2822	14.2853	14.2857

Yukarıdaki tabloda LSB tekniğinin çok katmanlı uygulamasının kazanç değerleri verilmiştir. Sadece 2 seviyeli steganografi de dahi bant genişliğindeki artış %12.5 olarak gerçekleşmiştir. Çok katmanlı steganografi daha karmaşık olmasına ragmen, kapasiteyi ciddi şekilde arttırmaktadır.

Çok katmanlı görüntü steganografi yönteminin en büyük avantajlarından biride bant genişliği artmasına rağmen, resimdeki değişmenin hemen hemen aynı kalmasıdır.

Resimlerin bozulma oranı PSNR (Peak Signal Noise Rate) ve MSE (Mean Square Error) metrikleriyle hesaplanmaktadır. PSNR' nin yüksek çıkması resimdeki bozulmanın az olduğunu göstermektedir [9].

$$MSE = \frac{1}{MN}\sum_{i,j}(P_{i,j} - \bar{P}_{i,j})^2 \quad (9)$$

$$PSNR = 10.\log.\frac{Max(P_{i,j}^2)}{MSE} \quad (10)$$

rice adam cameraman Football

Şekil 3. Karşılaştırma İçin Kullanılacak Resimler

Şekil 3' teki resimlere önce klasik LSB yöntemi kullanılarak veri gömülmüştür, ardından ÇOK KATMANLI GÖRÜNTÜ STEGANOGRAFİ kullanılarak veri gömülmüş ve kapasitesi (bant genişliği) arttırılmıştır. İki seviyeli ÇOK KATMANLI GÖRÜNTÜ STEGANOGRAFİ yapısı kullanılmıştır ve bant genişliği %12.5 arttırılıp PSNR sonuçları aşağıdaki tabloda verilmiştir.

TABLO II. PSNR değerleri

Görüntü	LSB (%100 Kapasite- 1 bpp)	LSB (%114 Kapasite , 1.14 bpp)	4 katmanlı görüntü steganografi (%114 Kapasite)
rice	48.3568	44.8572	48.3648
adam	48.1875	36.7469	48.1263
cameraman	48.3374	44.6697	48.3600
football	48.3126	36.7448	48.3356

Tablo 2' de görüldüğü gibi PSNR sonuçları birbirine çok yakındır. Ortalama PSNR değişim miktarı %0.059 olarak gerçekleşmiştir. Bu oran ise çok küçük bir orandır ve bu oran ihmal edilebilir.

Yukarıdaki verilerden yola çıkacak olursak, çok katmanlı görüntü steganografi yöntemiyle gerçekleştirilen veri gizlemelerde örtü verisinin kalitesi bozulmadan bant genişliği (kapasite) arttırılmıştır.

Fakat klasik yöntemler kullanılarak taşıyıcı kapasitesi artırılmaya çalışıldığında, PSNR değişim miktarı ortalama %15.6275 olarak gerçekleşmiştir. Klasik yöntemlerle kapasite artırıldıkça, taşıyıcı resmin kalitesi düşmektedir. Klasik yöntemlerde, resmin kalitesi ile kapasite arasında negatif korelasyon vardır. Çünkü yukarıda ki uygulamada resmin kapasitesi %14 arttırıldı fakat resmin kalite metriği olan PSNR ise %15 değer kaybetmiştir.

IV. SONUÇ

Bu çalışmada çok katmanlı steganografiden bahsedilmiş olup, tek katmanlı steganografiye göre avantajlarından bahsedilmiştir. Özellikle bant genişliğini taşıyıcı kapasitesini arttırması önemli bir özellik olarak görülmüştür.

Örneğin tek katmanlı steganografik bir modelin karmaşıklığını O(n) olarak kabul edersek, aynı modelin 2 katmanlı uygulamasının karmaşıklığı O(nlogn) olarak karşımıza çıkacaktır. Ancak kapasite arttıkça örtü verisindeki bozulma artmaktadır. Çok Katmanlı metotlar kullanılarak örtü verisinde ki değişim sabit tutularak kapasite arttırılabilir.

Bu yöntem özellikle onion routing (soğan yönlendirme) ve çok seviyeli güvenlik uygulamalarında da kullanılabilir. Soğan yönlendirme de taşıyıcı (soğan) birden fazla mesaj taşımaktadır ve bu mesajlar çeşitli anahtarlarla şifrelenmiştir. İlgili anahtara sahip olan kullanıcı soğanı deşifre ederek ilgili mesajı elde edebilmektedir. Soğanın oluşturulabilmesi için çok katmanlı steganografi kullanılabilir. Örtü verinin altında gizlenecek alt örtü veriler sayesinde, birden fazla mesaj taşınabilir. Ayrıca çok seviyeli güvenlik uygulamalarında da bu metot kullanılabilir.

Modelin performansını arttırmak için paralel programlama metotlarına başvurulabilir. Örneğin threadler kullanılarak modelin perfomansı arttırılabilir. Ayrıca gömülü sistemlerde uygulaması yapılarak analiz edilebilir.

KAYNAKLAR

[1] Katzenbeisser, S., Petitcolas, F.A.P., 2000., Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, INC. 685 Canton Street Norwood, MA 02062.
[2] Şahin, A., 2007. Görüntü Steganografide Kullanılan Yeni Metotlar ve Bu Metotların Güvenilirlikleri, Doktora Tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne.
[3] N. Baykal, T. Beyan, "Bulanık Mantık Uzman Sistemler ve Denetleyiciler", Bıçaklar Kitabevi, 2004.
[4] Al-Najjar AJ. (2008) The Decoy: Multi-Level Digital Multimedia Steganography Model. In Proc. of 12th WSEAS International Conference on Communications, Heraklion, Greece, July 23-25, 2008
[5] Şahin Mesut A., Mesut A.,Saklı M.T.,"Görüntü Steganografide Gizlilik Paylaşım Şemalarının Kullanılması ve Güvenliğe Etkileri", III Ağ ve Bilgi Güvenliği Sempozyumu, Ankara-Türkiye, Feb 2010
[6] Fraczek W., Mazurczyk W., Szczypiorski K.,"Multi-Level Steganography: Improving Hidden Communication in Networks", Warsaw University of Technology, Apr 2012
[7] Al-Najjar AJ. ,The Decoy: Multi-Level Digital Multimedia Steganography Model. In Proc. of 12th,2008
[8] Popa, R., An Analysis of Steganogrphic Techniques, Master Thesis, Department of Computer Science and Software Engineering, Faculty of Automatics and Computers, The Politehnica University of Timisoara,1998.
[9] Sayood K., Introduction to Data Compression, Morgan Kauffman Publishers, Inc. 340 Pine Street, Sixth Floor, San Francisco, CA 94104-3205, USA,1996.

Engin Avcı, F.Ü. Yazılım Mühendisliği bölümünde çalışmaktadır. Doç. Dr. Engin Avcı görüntü işleme ve bilgi güvenliği alanında çok sayıda uluslararası yayına sahiptir

Türker Tuncer, F.Ü. Adli Bilişim Mühendisliği Bölümünde Araştırma görevlisi olarak çalışmaktadır, Yazılım Mühendisliği Bölümünde doktora öğrencisidir, bilgi güvenliği ve yazılım güvenliği alanında çalışmaktadır.

Fatih Ertam, Fırat Üniversitesi Enformatik Bölümünde okutman olarak görev yapmakta ve Bilgi işlem biriminde ağ ve sistem yöneticiliği görevini yürütmektedir. Yazılım Mühendisliği bölümünde doktora öğrencisidir, ağ güvenliği alanında çalışmaktadır.