GÖRÜNTÜ STEGANOGRAFİDE GİZLİLİK PAYLAŞIM ŞEMALARININ KULLANILMASI ve GÜVENLİĞE ETKİLERİ

Andaç ŞAHİN MESUT **Altan MESUT** **M. Tolga SAKALI**

Trakya Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, Edirne

e-posta: andacs@trakya.edu.tr, altanmesut@trakya.edu.tr, tolga@trakya.edu.tr

Abstract

Developing technology have raised the need of protecting our important data. For this aim, to increase the security of data needed for us, some techniques such as secret sharing schemes are used together with encryption or data hiding techniques. In this way, our important data becomes more reliable against malicious attacks. In this study, we examine how secret sharing schemes are used in image steganography and how that affects the security of the formed structure.

Keywords: Secret Scharing Scheme, Information Security, Image Steganography.

1. Giriş

Bilgi gizlemenin önemli bir alt disiplini olan Steganografi, bir nesnenin içerisine bir verinin gizlenmesi olarak tanımlanabilir [1]. 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. Steganografi; metin, resim ve ses steganografi olmak üzere üç alanda uygulanmaktadır.

İlk gizlilik paylaşım şeması (secret sharing scheme-*SSS*) Blakley [2] ve Shamir [3] tarafından 1979 yılında üretilmiştir. Bu gizlilik paylaşımı şemasına aynı zamanda (k,n) eşik şeması adı verilmektedir. Şemanın ana fikri gizli bilginin n kişiye dağıtılması ve k kişinin bir araya gelmesiyle gizli bilginin elde edilebilmesidir. k kişiden az kişinin bir araya gelmesiyle gizli bilgi elde edilememektedir.

Gizlilik paylaşım şemaları text veriler ya da görüntü dosyaları üzerine uygulanabilmektedir. Çeşitli araştırmacılar gizlilik paylaşımı şemaları için değişik yaklaşımlar sunmuşlardır. Kayıpsız görüntü dosyalarındaki kayıpları engelleyen bir görüntü gizlilik paylaşım şeması da Thien ve Lin tarafından sunulmuştur [4].

Bu çalışmada bir bilgi gizlenen renkli görüntü dosyasına Thien ve Lin tarafından geliştirilen gizlilik paylaşımı işleminin nasıl uygulandığı ve bunun sonucunda güvenliğin nasıl etkilendiği incelenmiştir.

2. Görüntü Steganografi

İstenilen bir bilgiyi bir görüntü içerisine gizleme işleminde iki dosya söz konusudur. Kapak resim ya da örtü verisi (cover image) olarak adlandırılan ilk dosya, bilgiyi saklayacak resim dosyasıdır. İkinci dosya ise gizlenecek bilgi olan mesajdır. Bu mesaj da stego olarak isimlendirilmektedir. Mesaj; açık metin (plain text), şifreli metin (chipher 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 sınıflandırılabilmektedir.

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

3. Thien ve Lin Gizlilik Paylaşımı Şeması

Thien ve Lin, Shamir tarafından 1979'da geliştirilen gizlilik paylaşımı şemasını akıllıca kullanarak (k,n) eşik-tabanlı bir görüntü paylaşımı sunmuştur [6].

Yöntemin ana fikri *lxl* boyutundaki *I* olarak adlandırılan gizli resimden n tane paylaştırılmış görüntü elde etmek için $(k-1)$. dereceden bir polinomsal fonksiyon kullanmaktır. $0 \le i \le \left(\frac{l}{k}\right)$ ve $1 \le j \le l$ olmak üzere polinomsal fonksiyon şu şekilde tanımlanmaktadır [4].

$$S_x(i,j) = I(ik+1,j) + I(ik+2,j)x + \ldots + I(ik+k,j)x^{k-1} \pmod p$$

Bu yöntemde alıcılara gönderilmek için oluşturulan görüntü dosyalarının boyutu, orijinal resmin $\frac{1}{k}$'sı büyüklüğündedir.

Elde edilen görüntü n adet görüntü parçası alıcılarına gönderilir. Alıcılardan en az k'sı bir araya gelerek orijinal görüntüyü elde edebilmektedir.

Alıcıların en az k'sı bir araya geldiğinde orijinal görüntünün elde edilmesi için Lagrange İnterpolasyon yöntemi kullanılmaktadır. Lagrange İnterpolasyon formülü de aşağıdaki şekilde tanımlanmaktadır [7][8].

$$h(x) = \sum_{k=1}^{t} y_k \prod_{\substack{j=1 \\ j \neq k}}^{t} \frac{x - x_j}{x_k - x_j} \pmod p$$

Formüldeki k, alıcıların numarasını, y değerleri de görüntü parçalarındaki renk değerlerini göstermektedir. Bölme işlemi için kullanılan mod değeri birleştirme işlemi için de kullanılmaktadır.

Thien ve Lin ayrıca alıcılara paylaştırma işleminden önce görüntünün permüte edilmesini tavsiye etmektedir. Permütasyon işlemi herhangi bir anahtar değer ile ya da çeşitli algoritmalarla yapılabilmektedir. Bu şekilde güvenlik ve saldırılara karşı dayanıklılık arttırılmış olmaktadır [4].

Thien ve Lin gizlilik paylaşımı şemasının parçalara bölme işlemi nasıl yaptığını gösteren bir örnek [9] numaralı kaynakta verilmiştir.

4. Bilgi Gizleme ve Görüntüyü Paylaştırma Uygulaması

Görüntü steganografide gizlilik paylaşımı şemalarının nasıl kullanıldığını göstermek amacıyla seçilen renkli görüntü dosyası şekil 1'de gösterilmiştir. Seçilen resim 216x237 boyutundadır. Öncelikle resmin içine bilgi gizlenmekte ve daha sonra görüntü paylaştırılmaktadır.

Bilgi gizleme işlemi tarafımızdan geliştirilen ve en önemsiz bite ekleme yöntemine göre çalışan Stego_LSB isimli program tarafından yapılmaktadır [10].

Resmin parçalara bölünmesi işlemi de tarafımızdan geliştirilen Thien ve Lin tabanlı görüntü paylaşımı programı ile yapılmaktadır [9].

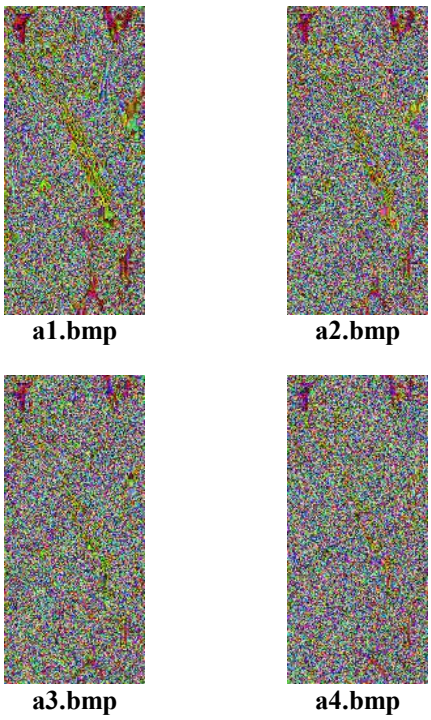
Şekil 1. Seçilen örnek renkli görüntü dosyası meyveler.bmp

meyveler.bmp isimli görüntü dosyasının içerisine 8,437 KB büyüklüğünde bir metin gizlenmiş ve oluşan yeni görüntü dosyası olan gizli_meyveler.bmp şekil 2'de gösterilmiştir.

Şekil 2. 8,437 Kb büyüklüğünde gizli veri içeren gizli_meyveler.bmp isimli görüntü dosyası

Gizli bilgi içeren görüntü dosyası daha sonra $(2,4)$ olarak seçilen Thien ve Lin eşik şeması ile alıcılarına paylaştırılmaktadır. gizli_meyveler.bmp dosyası 4 alıcı için bölünecek ve en az 2'si bir araya gelerek orijinal resmi oluşturabilecektir. 4 alıcıya gönderilecek parçalar ise Şekil 3'te verilmiştir. Oluşan görüntü dosyalarının boyutları 109x238 pikseldir.

Alıcılara gönderilen parçalardan herhangi ikisi bir lagrange interpolasyon formülüne sokularak orijinal görüntü elde edilmektedir. Görüntü paylaştırma esnasında görüntü dosyalarının boyutları da yarıya düştüğünden her bir parçada orijinal görüntü dosyasının yarı bilgisinin olduğu düşünülebilir. Yani oluşturulan yeni görüntü dosyalarında gizlenmiş bilginin parçaları da bulunmaktadır.



Şekil 3. Alıcılara gönderilecek görüntü dosyası parçaları.

Görüntü paylaştırma şeması kullanımının güvenliği nasıl etkilediğini incelemek amacıyla RS steganaliz uygulanmıştır. Bu yöntem resmin içinde gizli bilgi olup olmadığını sezmeye yönelik steganalitik saldırı yöntemlerinden biridir [11]. Resmin içinde bilgi olduğunun sezilmesiyle de çekme (extraction) saldırıları yapılmaktadır [12].

RS Steganaliz, görüntü dosyaları üzerinde En Önemsiz Bite Ekleme Yöntemine (LSB Insertion Methods) göre bilgi gizlenip gizlenmediğini anlamak için kullanılmaktadır. Fridrich tarafından geliştirilmiştir. RS steganalizinde, bir görüntünün piksellerinin 3 bağımsız gruba: Düzenli (regular), Tekil (singular) ve Kullanılmayan (unused) olarak ayrılması esastır [13]. Bu grupların sayıları belirlenir ve daha sonra bunlar arasındaki farklara bakılır. RS Steganaliz sonucunda elde edilen fark değerlerinin 0'a yakın çıkması resmin içinde bilgi olmadığını göstermektedir.

RS Steganaliz işlemi geliştirdiğimiz bir program tarafından yapılmaktadır [15]. Görüntü paylaşımı işleminin güvenlik açısından ne kadar etkili olduğunu göstermek amacıyla RS Steganaliz gizli_meyveler.bmp ve görüntü paylaştırma şeması ile oluşturulan a1.bmp, a2.bmp, a3.bmp ve a4.bmp isimli dosyalara uygulanmıştır.

RS Steganalizde maske değeri olarak M=(0,-1,1,-1) seçilmiştir. RS Steganaliz sonucunda elde edilen değerler Tablo 1'de verilmiştir.

Tablo 1. M= (0,-1,1,-1) maske değeriyle elde edilen RS Steganaliz sonuçları. RS steganaliz her renk kanalı; R (Red-Kırmızı), G (Green-Yeşil), B (Blue-Mavi); için ayrı ayrı yapılmıştır.

		gizli_meyveler.bmp	a1.bmp	a2.bmp	a3.bmp	a4.bmp
R	**R**	2	0	0	0	0
	S	2	0	0	0	0
	U	0	0	0	0	0
G	**R**	18	0	0	0	0
	S	18	0	0	0	0
	U	0	0	0	0	0
B	**R**	26	0	1	1	0
	S	26	0	1	1	0
	U	0	0	0	0	0

RS Steganalizde sonuçların 0 ya da 0'a çok yakın çıkması o görüntü dosyasının içinde bilgi olmadığını göstermektedir. Tablo 1'deki sonuçlardan da görülebileceği gibi görüntü dosyasının içine bilgi gizleyip yeni oluşan dosyayı alıcısına o şekilde gönderdiğimizde saldırgan RS steganaliz yaptığında gizli-meyveler.bmp dosyasının içinde bilgi olabileceği yönünde bir kanıya varacak ve bu bilgiye erişebilmek için çekme saldırılarına başlayacaktır. Bilgi gizlenmiş dosyayı 4 parçaya böldüğümüzde ve bu şekilde gönderdiğimizde ise saldırgan yaptığı RS steganaliz neticesinden bu dosyalarda herhangi bir bilgi olmadığı kanısına varacaktır.

Yapılan testler sonucunda bilgi gizlenmiş resim dosyasını o haliyle göndermek yerine görüntü paylaşımı şeması ile parçalara bölüp göndermenin steganaliktik saldırılar karşısında dosyanın daha güvenli iletilebilmesini sağladığı görülmektedir.

5. Sonuçlar

Son yıllarda bilgisayar sistemlerinin güvenliği ve özellikle bilgi güvenliği oldukça önemli bir konu olarak karşımıza çıkmaktadır. Büyük bir global ağ olan internetin de 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. Gelişen teknoloji neticesinde saldırganlar da önemli verilere daha kolay ulaşabilmektedirler. Önemli verilerimizi kötü amaçlı kişilerden koruyabilmek için çeşitli güvenlik tekniklerini birlikte kullanmak daha yararlı olmaktadır.

Bu çalışmada görüntü steganografi ile görüntü paylaşımı şemalarının birlikte nasıl kullanıldığı gösterilmiştir. Görüntü dosyasının içerisine bilgi saklayıp gönderdiğimizde steganaliktik saldırılara karşı daha savunmasız bir durumda olabiliriz. Saldırgan yapacağı bir steganalitik saldırı sonucunda resmin içinde bilgi olabileceği kanısına varacak ve bu bilgiyi çekmeye çalışacaktır. Görüntü dosyasını parçalara böldüğümüzde ise saldırgan 4 parçayı ayrı ayrı analiz edecek içinde bir bilgi olduğu kanısına varsa bile öncelikle eşik şemasının boyutunu ve mod değerini bulması gerekecektir. Bunları bulsa bile Lagrange İnterpolasyon formülü neticesinde elde edebileceği görüntü permüte edilmiş görüntü olacaktır. Bundan sonra da ters permütasyon işlemi yaparak bilgi gizlenmiş resim dosyasına ulaşacaktır. Son olarak ta çekme saldırısı yapmaya başlayacaktır. Böylelikle bir bilgiyi elde edebilmek için çok zaman ve emek sarf etmesi gerekecektir. İnternet üzerinde milyonlarca resmin gönderildiği düşünülürse bu işlemleri yapabilmesi oldukça zahmetli bir durum haline gelecektir.

Görüntü paylaşımı şemalarının görüntü steganografi ile birlikte kullanılmasının güvenliği arttırıcı bir durum olduğu görülmektedir.

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] Blakley GR. Safeguarding cryptographic keys. Proceedings AFIPS 1979 National Computer Conference, vol. 48, New York, USA, 4–7 June 1979. p. 313–7.

[3] Shamir A., "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979. 12.

[4] C.-C. Thien and J.-C. Lin, "Secret image sharing," Computers & Graphics, vol. 26, no. 5, pp. 765–770,2002.

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

[6] Lee Bai, "A Reliable (k, n) Image Secret Sharing Scheme", Proceedings of the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, Indianapolis, Indiana. USA: IEEE Press, 2006: 31-36, ISBN: 0-7695-2539-3.

[7] Dorothy Elizabeth Robling Denning, Cryptography and Data Security, Addison-Wesley Publishing Company, 1982.

[8] Trappe W., Washington L., Introduction to Cryptography with Coding Theory Second Edition, Pearson Prentice Hall, 2006.

[9] Şahin Mesut A., Arda D., "Renkli Görüntü Dosyaları Üzerinde Gizlilik Paylaşımı Uygulaması", IV İletişim Teknolojileri Sempozyumu, Adana-TÜRKİYE, Ekim-2009.

[10] 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-TÜRKİYE, Haziran-2006.

[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., 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.

[14] 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.

[15] Şahin A., "Görüntü Steganografide Kullanılan Yeni Metodlar ve Bu Metodların Güvenilirlikleri", Doktora Tezi, (2007).