RENKLİ GÖRÜNTÜ DOSYALARI ÜZERİNDE GİZLİLİK PAYLAŞIMI UYGULAMASI

ANDAÇ ŞAHİN MESUT **DERYA ARDA**

Trakya Üniversitesi Mühendislik Mimarlık Fakültesi Bilgisayar Mühendisliği Bölümü, 22180, EDİRNE

andacs@trakya.edu.tr **deryaa@trakya.edu.tr**

Özet

İnternetin ve teknolojinin gelişmesiyle birlikte dijital ortamda bulunan verilerimizi koruma ihtiyacımız artmıştır. Verilerimiz metin, ses ya da görüntü dosyalarımız olabilir. Verilerin güvenliğinin nasıl sağlanacağı da önemli bir konu haline gelmiştir. Verilerimizi koruyabilmek için şifreleme ve steganografi gibi teknikler kullanılabilir. Gizlilik paylaşımı ise veriyi n kişiye dağıtarak ve tekrar elde edilmesi için en az k kişinin bir araya gelmesini gerektiren bir eşik şemasıdır. Gizli bilgi tek bir taşıyıcı ortam ile değil birçok taşıyıcı ortama dağıtılmış şekilde alıcıya iletilir. Böylelikle bilginin ele geçirilmesi amacıyla yapılabilecek saldırılara karşı önlem arttırılmış olur. Bu çalışmada gizli bir bilgi ya da önemli bir şekil içeren renkli görüntü dosyasının, (k,n) olarak oluşturulan bir eşik şemasına göre nasıl parçalara ayrıldığı ve alıcı tarafından nasıl tekrar elde edilebileceği gösterilmiştir.

Anahtar Kelimeler: Gizlilik Paylaşımı, Görüntü İşleme, Bilgi Güvenliği

1. Giriş

Önemli ve hassas verilerin etkin bir şekilde korunması ve güvenliğinin sağlanması konusu özellikle ticaret, iletişim, sağlık ve askeri alanlarda oldukça dikkat edilmesi bir konudur. Güvenliği sağlamak amacıyla şifreleme ve steganografi (bilgi gizleme) yöntemleri ayrı ayrı ya da bir arada kullanılabilir. Bu yöntemlerin etkinliğini arttırmak içinse gizlilik paylaşım şemaları geliştirilmiş böylelikle saklanan ya da şifrelenen verinin saldırılara karşı daha dayanıklı olması sağlanmıştır. Gizlilik paylaşım şemaları text veriler ya da görüntü dosyaları üzerine uygulanabilmektedir.

İlk gizlilik paylaşım şeması (secret sharing scheme- *SSS*) Blakley [1] ve Shamir [2] 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.

Karnin ve arkadaşları [3] mükemmel gizlilik paylaşımı (perfect secret sharing- *PSS*) kavramını ortaya atmıştır. Mükemmel gizlilik paylaşımı yaklaşımında alıcılar nitelikli ve niteliksiz olarak adlandırılan iki gruba ayrılmaktadır. Bilginin önemli kısımları nitelikli grup arasında paylaştırılır. Niteliksiz gurubun elinde önemsiz bilgi parçaları bulunmaktadır. Bu şekilde sadece nitelikli grubun belli sayıda üyesi bir araya gelerek gizliliği elde edebilmektedir. Fakat bu yöntemde bilginin hangi kısımlarının önemsiz olduğunu belirlemek önemli bir konudur.

PSS yaklaşımından sonra ortaya atılan bir diğer yaklaşım da niteliksiz grubun büyüklüğü oranında gizli bilginin belirli sayıda niteliksiz grup alıcısına da paylaştırılmasıdır. Bu gizlilik paylaşımı şemasına da düzenlenmiş gizlilik paylaşımı (ramp secret sharing- *RSS*) adı verilmektedir [4][5][6].

Daha sonraları PSS ve RSS yaklaşımları çeşitli araştırmacılar tarafından daha da geliştirilmiştir [7][8][9].

Naor ve Shamir gizlilik paylaşımı kavramını görüntü alanına genişletmiş ve görsel kriptografi olarak adlandırmıştır [10][11]. Görsel Kriptografi aslında bir PSS uygulamasıdır. Fakat bu yöntemde kayıpsız görüntü dosyalarına uygulama esnasında sorunlar ve kalite kayıpları ortaya çıkmaktadır.

Bu sorunları ortadan kaldırmak amacıyla daha iyi bir görüntü gizlilik paylaşımı Thien ve Lin tarafından sunulmuştur [12].

Bu çalışmada gizli bir bilgi ya da önemli bir şekil içeren renkli görüntü dosyasının, (k,n) olarak oluşturulan bir eşik şemasına göre nasıl parçalara ayrıldığı ve alıcı tarafından nasıl tekrar elde edilebileceği gösterilmektedir. Eşik şeması Thien ve Lin tarafından geliştirilen yaklaşıma göre hazırlanmıştır.

2. 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 [13].

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 [12].

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

Bu yöntemde oluşturulan görüntü dosyalarının boyutu, gizli resmin $\frac{1}{k}$'sı büyüklüğündedir.

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

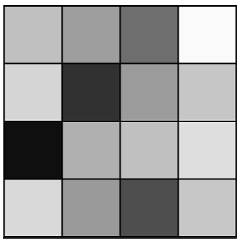
Alıcıların en az k'sı bir araya geldiğinde orijinal görüntünün elde edilmesi için Lagrange İnterpolasyon yöntemi kullanılmaktadır. Lagrange İnterpolasyon formülü de aşağıdaki şekilde tanımlanmaktadır [14][15].

$$h(x) = \sum_{k=1}^{t} y_k \prod_{\substack{j=1 \\ j \ne k}}^{t} \frac{x - x_j}{x_k - x_j} \pmod p \quad (2)$$

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 yada çeşitli algoritmalarla yapılabilmektedir. Bu şekilde güvenlik ve saldırılara karşı dayanıklılık arttırılmış olmaktadır [12].

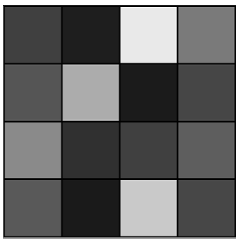
Örnek: Yöntemin nasıl çalıştığını göstermek amacıyla $4x4$ boyutunda gri renkli bir deneme görüntüsü seçilmiş olsun (Şekil 1). Renk değerlerinin görülebilmesi için pikseller büyük gösterilmiş ve renk değerleri yanındaki matriste verilmiştir. Seçilen görüntünün 4 alıcıya bölünmesi istensin ve görüntünün tekrar oluşturulabilmesi için en az 2 kişinin bir araya gelmesi gereksin. Bu durumda eşik şeması $(2,4)$ olarak seçilir.



$$I = \begin{bmatrix} 192 & 158 & 110 & 250 \\ 213 & 49 & 155 & 198 \\ 15 & 176 & 192 & 222 \\ 217 & 154 & 78 & 199 \end{bmatrix}$$

Şekil 1. $4x4$ boyutunda gri renkli bir deneme görüntüsü ve piksel değerleri

Permütasyon işlemi için 123 değeri anahtar olarak seçilmiştir ve mod 251'e göre modüler toplama yapılmıştır. Permüte edilmiş görüntü şekil 2'de gösterilmektedir.



$$I_P = \begin{bmatrix} 64 & 30 & 233 & 122 \\ 85 & 172 & 27 & 70 \\ 138 & 48 & 64 & 94 \\ 89 & 26 & 201 & 71 \end{bmatrix}$$

Şekil 2. Permüte edilmiş deneme görüntüsü ve piksel değerleri

Görüntünün Parçalara Bölünmesi:

Eşik şemamız $(2,4)$ olarak seçilmiştir bu durumda $k = 2$ ve $n = 4$'tür. Verilen sınır şartlarına göre $0 \le i \le 2$ ve $1 \le j \le 4$'tür.

Tekniğe göre 1. Dereceden polinomsal fonksiyon denklem 1 uygulanarak şu şekilde elde edilmektedir:

$$S_x(i,j) = I(ix2+1,j) + I(ix2+2,j)x \pmod{251} \quad (3)$$

251 değeri gri renkli resmin renk aralığı içindeki en büyük asal sayı olması sebebiyle seçilmiştir.

Paylaşım için oluşturulacak parçaların hangi pikselinin değeri hesaplanmak isteniyorsa i ve j değerleri ona göre konularak işlemler yapılmaktadır. Tüm işlemler permüte edilmiş görüntünün renk değerleri üzerinden yapılmaktadır.

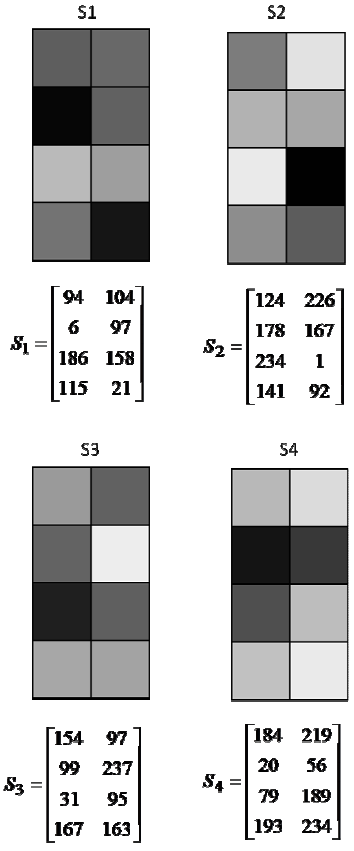
Örneğin alıcılara gönderilecek parçaların $(0,1)$. piksel değerleri hesaplanmak istensin, $i=0, j=1$ değerleri denklem 3'de yerine konulduğunda aşağıdaki denklem elde edilmektedir.

$$S_x(0,1) = I(0x2+1,1) + I(0x2+2,1)x \pmod{251}$$
$$S_x(0,1) = I(1,1) + I(2,1)x \pmod{251}$$
$$S_x(0,1) = 64 + 30x \pmod{251}$$

Bu denklemde de x yerine 1, 2, 3 ve 4 konularak oluşturulacak 4 parçanın $(0,1)$ pikselinin değeri hesaplanmış olur.

$$S_1(0,1) = 64 + 30x1 \pmod{251} = 94$$
$$S_2(0,1) = 64 + 30x2 \pmod{251} = 124$$
$$S_3(0,1) = 64 + 30x3 \pmod{251} = 154$$
$$S_4(0,1) = 64 + 30x4 \pmod{251} = 184$$

Diğer piksellerin hesaplanması için gerekli tüm denklemler kurularak değerler yerine konulduğunda $4x4$ boyutundaki görüntüden elde edilen $4x2$ boyutundaki görüntüler ve piksel renk değerleri Şekil 3'de gösterilmektedir.



Şekil 3. Seçilen örnek görüntüden elde edilen ve alıcılara paylaştırılacak görüntü dosyaları ve renk değerleri

Görüntünün Tekrar Elde Edilmesi:

2. ve 3. alıcıların ellerinde bulunan görüntü parçaları birleştirerek orijinal görüntüyü elde etmek istesinler.

2. ve 3. alıcıların kendilerine ait S_2 ve S_3 görüntü parçalarının renk matrisleri olan $S_2 = \begin{bmatrix} 124 & 226 \\ 178 & 167 \\ 234 & 1 \\ 141 & 92 \end{bmatrix}$, $S_3 = \begin{bmatrix} 154 & 97 \\ 99 & 237 \\ 31 & 95 \\ 167 & 163 \end{bmatrix}$ matrisleri denklem 2'deki lagrange interpolasyon formülüne sokulmaktadır.

Seçilen eşik şemasına göre orijinal görüntünün boyutu parçaların iki katı olduğu için her işlem sonucunda yan yana iki pikselin değeri elde edilmektedir. Orijinal görüntünün $(0,1)$ ve $(0,2)$. piksellerini oluşturmak için parçaların $(0,1)$. pikselleri kullanılmaktadır. İlk olarak 124 ve 154 değerleri denklem 2'de kullanılacaktır.

$$\begin{aligned} Ip(0,1-2) &= \left(124\frac{x-3}{2-3} + 154\frac{x-2}{3-2}\right) \mod 251 \\ &= \left(-124x + 372 + 154x - 308\right) \mod 251 \\ &= \left(30x + 64\right) \mod 251 \\ &= 30x + 64 \end{aligned}$$

Burada elde edilen sabit sayı permüte edilmiş görüntünün $(0,1)$. pikselini, x'li terimin katsayısı da permüte edilmiş görüntünün $(0,2)$. pikselini vermektedir.

Benzer şekilde görüntünün $(0,3)$ ve $(0,4)$. piksellerini oluşturmak için parçaların $(0,2)$. pikselleri kullanılmaktadır.

$$\begin{aligned} Ip(0,3-4) &= \left(226\frac{x-3}{2-3} + 154\frac{x-2}{3-2}\right) \mod 251 \\ &= \left(-226x + 678 + 97x - 194\right) \mod 251 \\ &= \left(-129x + 484\right) \mod 251 \\ &= 122x + 233 \end{aligned}$$

Bütün piksel değerleri kullanılarak I_p matrisi elde edilir ve daha sonra ters permütasyon işlemi uygulanarak seçilen görüntümüz olan I oluşturulmuş olur.

3. Geliştirilen Uygulama

Geliştirilen uygulama renkli görüntü dosyaları üzerinde seçilen bir eşik şemasına göre görüntü paylaştırma işlemi yapmaktadır. Uygulamada Thien ve Lin tarafından geliştirilen (k,n) eşik-tabanlı görüntü paylaşımı şeması kullanılmaktadır. Uygulama C++ dili ile geliştirilmiştir.

Görüntüyü paylaştırmak için yukarıda anlatılan işlemler her renk kanalı (Red-R, Green-G, Blue-B) için ayrı ayrı uygulanmaktadır. Öncelikle görüntü seçilmekte, permüte edilmekte ve seçilen eşik şemasına göre oluşturulan polinomsal fonksiyona göre alıcılara gönderilecek görüntüler elde edilmektedir.

Görüntü paylaşımı işleminin pseudo kodu aşağıda verilmiştir.

Adım 1: Seçilen resim üzerinde istenilen bir permütasyon yöntemine göre işlem yaparak I_p görüntüsünü oluştur.

Adım 2: Belirlenen (k,n) eşik şemasına göre kullanılacak polinomsal fonksiyonu hesapla.

Adım 3: Alıcılara gönderilecek olan görüntülerin boyutlarını hesapla. (Alıcılara gönderilecek görüntüler orijinal görüntünün $\frac{1}{k}$ 'sı büyüklüğündedir.)

Adım 4: Her renk kanalı için ayrı ayrı olmak üzere polinomsal fonksiyonu kullanarak alıcılara gönderilmek için oluşturulacak görüntülerin piksellerini hesapla.

Adım 5: R, G, B değerlerini kullanarak alıcılara gönderilecek görüntüleri oluştur.

En az sayıda alıcı bir araya geldiğinde ellerindeki görüntülerden resmi elde etmesi için de Lagrange interpolasyon yöntemi kullanılmaktadır. Bu işlemin pseudo kodu ise şu şekildedir.

Adım 1: Eşik şemasında belirlenen sayıda orijinal görüntüyü elde etme amacıyla kullanılacak görüntüleri al.

Adım 2: Her renk kanalı için ayrı ayrı olmak üzere renk değerlerini lagrange interpolasyon formülüne sokarak yeni piksel değerlerini hesapla.

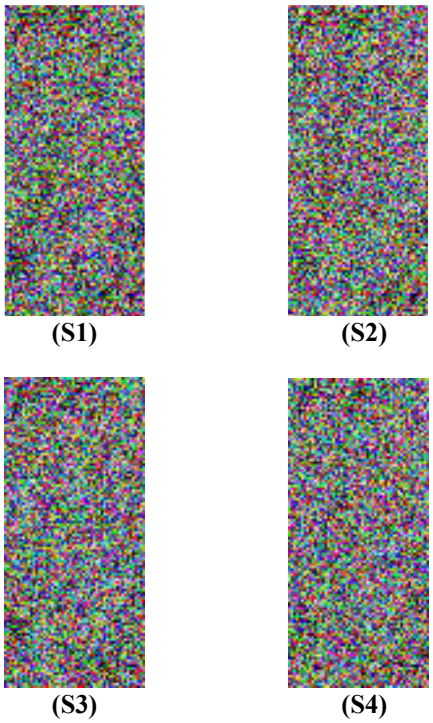
Adım 3: R, G, B değerlerini birleştirerek I_p görüntüsünü oluştur.

Adım 4: Oluşturulan I_p görüntüsüne ters permütasyon işlemi uygulayarak orijinal görüntü olan I 'yı elde et.

Uygulamanın çalışmasını göstermek amacıyla seçilen resim ve permüte edilmiş hali şekil 4'te gösterilmektedir. Seçilen görüntü dosyası 218x238 piksel boyutundadır. Elde edilen görüntülerin boyutları ise 109x238 pikseldir. Eşik şemamız $(2,4)$ olarak seçilmiştir. Orijinal görüntü 4 alıcı için bölünecek ve en az 2'si bir araya gelerek orijinal resmi oluşturabilecektir. Orijinal resimden oluşturulan görüntüler de şekil 5'te gösterilmiştir.

(a) **(b)**

Şekil 4. (a) Seçilen örnek görüntü meyveler.bmp ve **(b)** permüte edilmiş görüntü



(S1) **(S2)**

(S3) **(S4)**

Şekil 5. Permüte edilmiş resimden elde edilen görüntüler.

Oluşturulan görüntüler alıcılara gönderildikten sonra hangi iki alıcı olursa olsun bir araya geldiğinde orijinal resmi herhangi bir bozulma olmadan elde edebilmektedirler.

4. Sonuçlar

Gelişen teknoloji hayatımızı kolaylaştırsa da kişisel ve gizlilik taşıyan verilerin korunması 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. Verileri global ağda korumak için şifreleme yada bilgi gizleme teknikleri kullanabilmektedir. Gerektiği durumlarda bu iki yöntem birlikte de kullanılabilir. Gizlilik paylaşımı şemaları ise güvenliğin daha da arttırılmasını sağlayabilmektedir. Örneğin bir askeri harita başka bir yere gönderilmek istendiğinde önce şifrelenebilir ve daha sonra bir gizlilik paylaşımı şeması uygulanarak parçalara bölünerek güvenliği arttırılabilir. Ya da önemli bir bilgi içeren veri dosyası masum görünüşlü bir görüntü dosyası içerisine gizlenebilir, steganografik saldırılardan korunması amacıyla da gizlilik paylaşımı şemasına tabi tutulabilir. Oluşturulan parçalar farklı kişilere gönderildiği için kötü amaçlı kişilerin bilgileri ele geçirmesi daha da zorlaştırılmış olur. Oluşturulan parçalar istenilirse tek bir alıcıya da gönderilebilir. Saldırganın bu durumda tüm parçaları ele geçirmesi daha kolaydır fakat eşik şemasını tahmin etmek ve permütasyon işleminin nasıl yapıldığını da çözmek zorundadır.

Bu çalışmada bir gizlilik paylaşımı şeması kullanılarak renkli görüntü dosyasının parçalara nasıl bölünebileceği ve alıcılara gönderildikten sonra belirlenen eşik şemasına göre en az sayıdaki alıcının bir araya gelerek renkli görüntüyü nasıl elde edebileceği gösterilmiştir. Yapılan birçok deneme neticesinde seçilen görüntü dosyaları belirlenen eşik şemasına göre parçalara ayrılmış ve en az sayıda kişi bir araya gelerek orijinal görüntüye hiçbir kayıp ya da bozulma olmadan ulaşabilmiştir. Bu yöntem tek başına ya da diğer güvenlik yöntemleriyle birleştirilerek veriler üzerinde daha etkin bir koruma sağlamaktadır.

Kaynaklar

1. Blakley GR. Safeguarding cryptographic keys. Proceedings AFIPS 1979 National Computer Conference, vol. 48, New York, USA, 4–7 June 1979. p. 313–7.
2. A. Shamir, “How to share a secret,” Communications of the ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979.
3. E. D. Karnin, J. W. Greene, and M. E. Hellman, “On secret sharing systems,” vol. IT-29, no. 1, pp. 35–41,Jan. 1983.
4. K. Kurosawa, K. Okada, K. Sakano, W. Ogata, and S. Tsujii, “Nonperfect secret sharing schemes and matroids,” Lecture Notes in Computer Science, vol.765, pp. 126–141, 1994. [Online]. Available: citeseer.ist.psu.edu/article/kurosawa94nonperfect.html
5. W. Ogata and K. Kurosawa, “Some basic properties of general nonperfect secret sharing schemes,” J.UCS:Journal of Universal Computer Science, vol. 4,no. 8, pp. 690–704, 1998. [Online]. Available: citeseer.ist.psu.edu/article/ogata98some.htm
6. P. Paillier, “On ideal non-perfect secret sharing schemes,” in Security Protocols Workshop, 1997, pp. 207–216. [Online]. Available:citeseer.ist.psu.edu/paillier98ideal.html
7. C. Asmuth and J. Bloom, “A modular approach to key safeguarding,” vol. 29, no. 2, pp. 208–210, Mar. 1983.
8. G. R. Blakley and C. Meadows, “Security of ramp schemes,” presented at the Advances in Cryptology – Crypto ’84, G. R. Blakley and D. Chaum, Eds., Aug.1984.
9. A. De Santis and B. Masucci, “Multiple ramp schemes,” vol. 45, no. 5, pp. 1720–1728, July 1999.
10. M. Naor and A. Shamir. (1996, June) Visual cryptography II: Improving the contrast via the cover base. [Online]. Available: http://philby.ucsd.edu/cryptolib/1996/96-07.html.
11. M. Naor and A. Shamir, “Visual cryptography,” presented at the Proceedings of the Conference on Advances in Cryptology – Eurocrypt ’94, A. De Santis, Ed., Berlin, Germany, 1994, pp. 1–12.
12. C.-C. Thien and J.-C. Lin, “Secret image sharing,” Computers & Graphics, vol. 26, no. 5, pp. 765–770,2002.
13. 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