BRAILLE ALFABESİ TABANLI OLASILIKSAL GÖRSEL SIR PAYLAŞIMI METODU

T.Tuncer ve E. Avcı

Özet **— Naor ve Shamir imgelerin ve şifreleme anahtarlarının gizliliğinin korumak için (k,n) görsel sır paylaşımı (GSP) metodunu önermiştir. Bu metot kullanılarak, gizli veri karmaşık hesaplamalar yapılmaksızın sır parçalarına ayrılabilmektedir. GSP metotları güvenilirliği sağlar ancak gürültü benzeri imgeler saldırganların dikkatini çekmektedir. Bu makalede alt pikseller, braille alfabesindeki harflerden oluşmaktadır yani sır parçaları anlamlı parçalardan oluşmaktadır. Bu çalışmada, olasılıksal bir yaklaşım kullanılarak yeni bir GSP önerilmiştir. Yeniden yapılandırma aşamasın özel veya (XOR) operatörü kullanılmıştır. Ayrıca, önerilen braille tabanlı GSP (BGSP) kullanılarak veri gizleme uygulaması gerçekleştirilmiştir. Böylece, sır parçaları saldırganların dikkatini çekmeden alıcı tarafa iletilebilecektir.**

Anahtar Kelimeler**— Braille tabanlı görsel sır paylaşımı, Olasılıksal görsel sır paylaşımı, Veri gizleme, Damgalama, Bilgi güvenliği, İmge işleme.**

Abstract**— (k,n) visual cryptography scheme is firstly proposed by Naor and Shamir to protected image contents and encryption keys. Secret data can be divided into secret shares without complex calculation by using this method. Visual cryptography methods are provided security but a lot of attack is developed for noise- like image by attacker. In this paper, subpixels are coded with braille coding. We created meaningful secret shares by using braille. In this study, we presented a new probabilistic braille based visual cryptography algorithm with XOR operator. The proposed method is used XOR for reconstruction. Also, we used data hiding for camouflage. Thus, the secret shares are sent to receiver without attracting attention of attackers.**

Keywords**— Braille based visual cryptography, Probabilistic visual cryptography, Data hiding, Watermarking, Information security.**

Türker Tuncer, Fırat Ünv. Teknoloji Fak. Adli Bilişim Müh. Böl. 23119 Elazığ/TÜRKİYE (turkertuncer@firat.edu.tr)

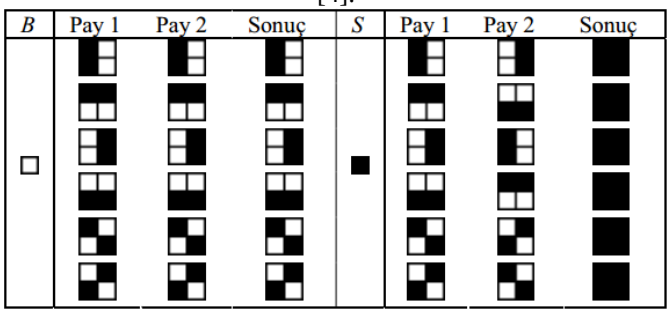
Engin Avcı, Fırat Ünv. Teknoloji Fak. Yazılım Müh. Böl. 23119 Elazığ/TÜRKİYE (enginavci23@hotmail.com)

I. GİRİŞ

Bulut teknolojisinin kullanımının artmasıyla birlikte, bilgi güvenliğinin de önemi artmıştır. Çünkü bulut, kullanıcılarının erişimine açık bir platformdur. Bulutta bulunan bilgilerinin güvenliğini ve gizliliğini sağlayabilmek için bilgi güvenliği yöntemlerinin kullanılması gerekmektedir. Bu güvenlik önlemlerinin başında ise şifreleme ve veri gizleme gelmektedir. Şifreleme, bir verinin içeriğini değiştirmeye yönelik kullanılırken; veri gizleme örtü nesnesinin içeriğini değiştirmez sadece gizli veriyi bir örtü nesnesine gizler. Veri gizlemedeki en temel amaç ise, gizli verinin sezilememesidir [1-3]. Kısacası, şifreleme verinin içeriğini korumayı amaçlarken, veri gizleme verinin sezilememesini amaçlamaktadır. Verilerin güvenilir olarak paylaşımı ve saklanması için sır paylaşımı algoritmaları önerilmektedir [4].

Sır paylaşımı algoritmaları, ilk olarak 1979 yılında Blakley ve Shamir tarafından önerilmiştir [5, 6]. Bu yöntemlerin temel amacı şifreleme anahtarı korumak ve güvenilir bir dağıtıcı ile sır parçalarını dağıtmaktır. Sır parçaları bir araya gelince anahtarı oluşturacaktır. GSP şemaları ise ilk olarak 1994 yılında Naor ve Shamir tarafından önerilmiştir [7]. Bu algoritmayla, gizli mesaj belirlenen kurallara göre sır parçalarına ayrılmaktadır. Gizli veriyi yeniden elde etmek için karmaşık matematiksel işlemlere gerek yoktur. Sır parçalarının üst üste gelmesiyle gizli mesaj elde edilebilmektedir. Shamir' in görsel sır paylaşımı algoritmasının kodlama tablosu Tablo 1' de verilmiştir.

Tablo 1. Shamir' in GSP şemasında piksellerin kodlanması [4].



Tablo 1' de de görüldüğü gibi, Shamir'in GSP şemasında imgenin yeniden yapılandırılması için mantıksal VEYA operatörü kullanılmıştır. Bu metodun yanı sıra olasılıksal GSP (OGSP) şemaları da mevcuttur. Wang' ın şeması XOR ve VE operatörü kullanan ve en yaygın kullanılan OGSP'lerden biridir [8]. Bu şemada sır parçalarının bir kısmı rastgele üretilmektedir. Diğer sır parçaları ise istenilen sonuca göre üretilmektedir.

İmge kimliklendirmek ve gizli verinin güvenliğini arttırmak için veri gizleme ve görsel şemalarının bir arada kullanılması önerilmiştir. Ayrıca GSP ve veri gizlemenin birlikte kullanıldığı çalışmalar şu şekilde sıralanmıştır. Lee vd. PNG imgeleri kimliklendirmek için Shamir'in (k,n) görsel sır paylaşımı şemasını kullanmışlardır [9]. Yuan sır paylaşımı algoritmalarını kullanarak çoklu örtü imgesi tabanlı uyarlamalı staganografi algoritmasını önermiştir. Önerilen algoritma

Shamir'in sır paylaşımı algoritmasını kullanmaktadır ve veri gizleme fonksiyonu olarak ±1 operatörü kullanılmaktadır. Bu algoritmayla, yüksek görsel kalite elde edilmiştir [10].

Ayrıca, literatürde harf tabanlı GSP şemaları da bulunmaktadır. Takizawa vd. Japon harflerini kullanan iki adet sır paylaşımı metodu önermiştir. İlk metotta bir veritabanı oluşturulmuştur. Oluşturulan veritabanı kullanılarak harflerin morfolojik analizi gerçekleştirilmiştir. Belirlenen harfler döndürülerek, sır parçaları elde edilmiştir. Takizawa vd. Ikinci yaklaşımında ise, harfler kullanılarak anlamlı cümleler elde edilmiştir. Anlamlı cümleler sır parçaları olarak kabul edilmiştir. Birden fazla anlamlı cümlenin bir araya gelmesiyle mesaj elde edilmiştir [11].

Lin vd. çince, korece, japonca ve latince harflerini tabanlı bir görsel sır paylaşımı metodu önermiştir. Bu metot temel olarak Shamir'in (k,n) görsel sır paylaşımını algoritmasını temel almaktadır. Alt pikseller, harflerden oluşmaktadır [12]. Wang vd. görsel şifreleme için Braille adlı bir makale yayınlamıştır ve bu makalede RGB imgelerin kimliklendirilmesiyle ilgili bir çalışma yapılmıştır [13].

Bu makalede Braille alfabesinde harflere karşılık gelen kodlar analiz edilmiştir ve XOR operatörü kullanılarak yeni bir GSP şeması oluşturulması öngörülmüştür.

Bu makalenin organizasyonu aşağıdaki gibi verilmiştir. İkinci bölümde motivasyon ve tasarım, üçüncü bölümde Braille alfabesi, dördüncü bölümde önerilen algoritma, beşinci bölümde deneysel sonuçlar ve altıncı bölümde ise sonuç ve önerilerden bahsedilmiştir.

II. MOTİVASYON VE TASARIM

Bu makalede çok seviyeli bir güvenliği metodu oluşturularak, gizli verinin güvenliği sağlanmıştır. Braille alfabesi kullanılarak anlamlı sır parçalarından oluşturulmuş yeni bir GSP şeması oluşturulmuştur. Ayrıca oluşturulan sır parçaları örtü nesnesinin içerisine gizlenmiştir, böylece sır parçaları için güvenilir veri iletim hattı oluşturulmuştur. Saldırgan steganaliz yöntemlerini kullanarak sır parçalarını elde etse dahi, sır parçaları Braille alfabesinde bulunan harflerden oluştuğu için, saldırgan sır parçasında bir şifre olduğu sanıp o şifreyi çözmeye çalışacaktır.

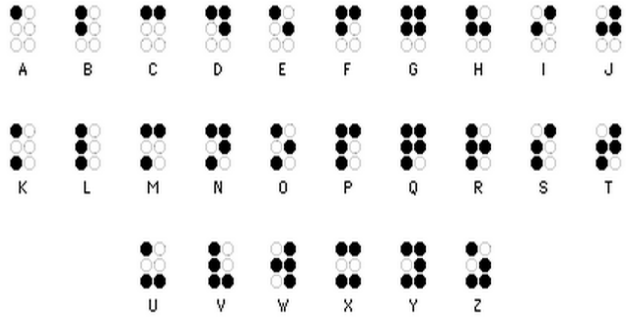
Kısacası bu makalede, saldırganın dikkatini çekmeden sır parçalarını alıcı tarafa gönderilmesi hedeflenmiştir. Çünkü gürültü benzeri sır parçaları saldırganların dikkatini çekmekte ve bu sır parçalarını elde eden saldırganlar, çeşitli saldırılar ve hileler düzenleyerek gizli veriyi değiştirebilmektedir. Eğer sır parçaları elde edilirse, Braille kodlar sayesinde saldırganın dikkati başka bir yöne doğru çekilecektir. Saldırgan ilk etapta Braille kodlarını anlamlandırmaya çalışacaktır.

Önerilen metodun motivasyonu, anlamlı alt parçalardan oluşan OGSP metodu tasarlamak ve bu metodu veri gizleme algoritmalarıyla birlikte kullanıp, yüksek seviyeli veri güvenliğini sağlamaktır.

III. BRAİLLE ALFABESİ

Görme engelli kişilerin kullanması için, 1829 yılında Louis Braille tarafından önerilmiştir. Louis Braille' in keşfettiği bu alfabe literatürde Braille alfabesi olarak adlandırılmaktadır. Braille alfabesi 6 adet noktadan oluşmaktadır ve bu noktalar 3 x 2 boyutundaki bir matrise yerleştirilmiştir. Alfabede yer alan işaretlerin tamamı bu 6 noktanın pozisyonuna göre oluşturulmuştur [14].

Harflerin Braille alfabesine göre kodlanması şekil 1' de verilmiştir.

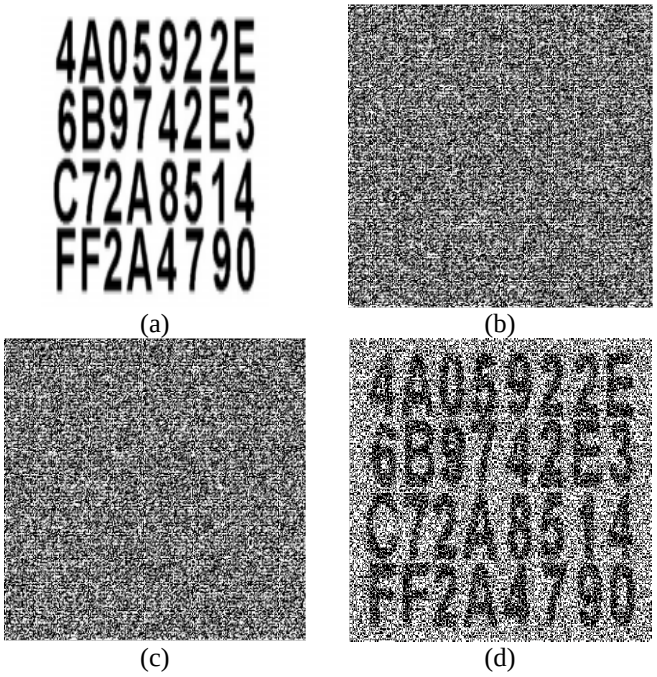


Şekil 1. Harflere Ait Braille kodları [15].

IV. ÖNERİLEN METOT

Bu makalede sır parçaları olarak, şekil 1' de gösterilen Braille harfleri kullanılmıştır. Önerilen yöntem Shamir' in (k,n) GSP şeması ve Wang' ın OGSP şemasından esinlenerek ileri sürülmüştür [7,8]. Olasılıksal BGSP oluşturulduğu için rastgele sayı üreteçleri kullanılmıştır. Sır paylaşımı gerçekleştirmek için XOR operatörü kullanılmıştır. Bu operatörün kullanılmasının temel sebebi ise 0 ve 1' in oluşmasından 0.5' e en yakın olasılığın oluşmasıdır. (2,2) BGSP şemasında, 26 adet harf kullanıldığı için toplam olasılık sayısı 26^2=676'dır. Bir bloğun siyah piksele eşit olması için en az 4 adet siyah pikselin olması gerekmektedir. Diğer durumlarda o blok beyaz (1) olarak ifade edilecektir. Bu koşullar altında 362 çift Braille koda XOR işlemi uygulanması sonucu 1, 314 çift Braille kodun XOR işlemi uygulanması sonucu 0 elde edilecektir. Bu makalede önerilen olasılıksal yöntemin, Yang' ın [16] sunduğu OGSP' ye göre en temel farkı alt piksellerin anlamlı olmasıdır. Yang' ın şemasında imgenin kontrastı söz konusuyken, önerilen metotta harflerin gelme olasılığı hesaplanmalıdır ve bu harflerin biraraya geldiğinde 0 ve 1' i elde etme olasılıklarının hesaplanması gerekmektedir. Ayrıca önerilen algoritmada kullanılan kural tablosu kontrast olasılığının gerçekleşmesi için de modifiye edilebilmektedir. Sözde rastgele sayı üreteçleri kullanılarak harflerin gelme olasılıkları uniform olarak ayarlanabilir. Kullanılan sözde rastgele sayı üreteçlerinin büyük bir kısmı üniform özellik gösterdiği için, bu yöntemde kullanılan rastgele sayı üretecinin türünün pek bir önemi yoktur. Uniform dağılım gösteren herhangi bir rastgele sayı üreteci kullanılabilmektedir. $P(0)=314/676=0.4645$ ve $P(1)=362/676=0.5355$ olacaktır. Olasılıkların 0.5' e yakın olmasından dolayı XOR operatörü kullanılmıştır. Önerilen olasılıksal BGSP' nin algoritması aşağıdaki gibidir. Ayrıca sır parçalarını gizlemek için veri gizleme algoritmalarından faydalanılmıştır.

Adım 1: 0 ve 1 kombinasyonlarını iki ayrı listeye kaydet.
Adım 2: İkili imgeyi gir.
Adım 3: İkili imgenin piksel değeri 0 ise sıfırlar listesinden rastgele Braille kodları seç.
Adım 4: İkili imgenin piksel değeri 1 ise birler listesinden rastgele Braille kodları seç.
Adım 5: Braille kodlarını sır parçası olan imgelere yerleştir.
Adım 6: İkili imgenin boyutu kadar adım 3-5' i tekrarla.
Adım 7: Elde edilen sır parçalarını örtü imgelerine veri gizleme fonksiyonunu kullanarak gizle.
Şekil 2' de (2,2) BGSP kullanılarak yapılan sır paylaşımı işlemi gösterilmiştir.



(a) (b) (c) (d)

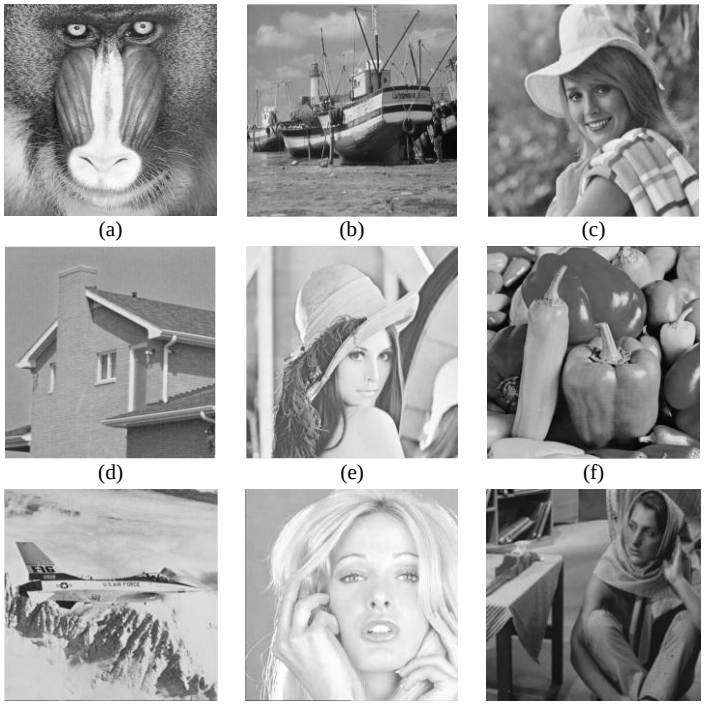
Şekil 2. (2,2) BGSP (a) Gizli veri (b) 1. Sır parçası (c) 2. Sır parçası (d) Yeniden elde edilmiş imge

İmgeyi yeniden elde etmek için, XOR operatörü kullanılmaktadır.

Horng vd. [17]' nin sunduğu makalede, GSP şemalarında meydana gelebilecek sahtekârlıktan bahsedilmiştir. Eğer herhangi bir sır parçası saldırganın eline geçerse ve saldırgan logonun ne olduğu bilirse, elde ettiği sır parçasını modifiye ederek farklı bir logonun oluşturulmasını sağlayabilmektedir. Bu tip sahtekârlıklardan korunabilmek için logonun saldırgandan gizlenmesi gerekmektedir. Horng vd. makalesinde kimlik doğrulama sistemi geliştirilerek bu tip sahtekârlıkların önüne geçilmeye çalışılmıştır. Bu makalede, sır parçalarını, bu tip saldırılardan koruyabilmek için veri gizleme uygulaması gerçekleştirilmiştir. Sır parçaları örtü nesnelerin içerisine gizlenerek, sır parçalarının sezilememesi ve elde edilememesi sağlanmıştır ve şemayı daha güçlü bir hale getirmek için veri gizleme uygulamaları kullanılmıştır. Sır parçalarını kamufle etmek için kullanılan veri gizleme algoritması ise 2LSBs (Least significant bits – En anlamsız bite gömme) algoritmasıdır. Bu algoritma kullanılarak, sır parçaları örtü nesnesinin en anlamsız iki bitine gömülmüştür.

V. DENEYSEL SONUÇLAR

Önerilen BSGP metoduyla sır parçalarına ayrılmış verileri veri gizleme uygulamasını test edebilmek için SIPI [18] imge veritabanı kullanılmıştır. Kamuflaj safhasında veri gizleme algoritmaları kullanılmıştır ve BGSP tabanlı veri gizleme algoritmasının görsel kalitesi test edilmiştir. Kullanılan imgeler 512 x 512 boyutundadır ve şekil 3' te gösterilmiştir.



(a) (b) (c) (d) (e) (f) (g) (h) (f)

Şekil 3' te gösterilen test imgelerinin görsel kalitesini test edebilmek için PSNR (peak signal-to noise ratio) ve MSE (mean square error) metrikleri kullanılmıştır. MSE ve PSNR' nin formülleri formül 1 ve 2'de verilmiştir.

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(CI_{i,j} - SI_{i,j})^2 \quad (1)$$

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

Şekil 3' te gösterilen imgeler 512 x 512 boyutundadır ve bu imgelere 524,288 bit veri gömülmüştür. Elde edilen PSNR sonuçları Tablo 2' de verilmiştir.

Örtü İmgesi	PSNR (dB)	
	Sır 1	Sır 2
Baboon	44.65	44.93
Boat	44.99	44.37
Elaine	45.52	45.11
House	45.36	45.54
Lena	44.01	44.75

Peppers	44.88	44.16
Airplane	43.97	44.61
Tiffany	45.32	45.88
Barbara	45.36	44.93

VI. SONUÇ

Bu makalede Braille alfabesinde bulunana harfler kullanılarak, yeni bir anlamlı sır paylaşımı metodu önerilmiştir. Önerilen metot kullanılarak gizli veri sır parçalarına ayrılmış ve her bir sır parçası bir örtü nesnesinin içerisine gizlenerek veri gizleme uygulaması gerçekleştirilmiştir. Önerilen BGSP algoritması olasılıksal metot ve XOR operatörünü kullanmıştır. Bu metotta XOR kullanılarak olasılıklar 0.5' e yaklaştırılmıştır. Rastgele sayı üreteci kullanılarak, Braille kodların sır parçası üzerinde uniform dağılımı sağlanmıştır. Kamuflaj aşamasında ise veri gizleme algoritmalarından faydalanılmış ve başarılı sonuçlar elde edilmiştir.

Gelecekteki çalışmalarda, biyometrik bilgi güvenliğini sağlayabilmek için ve yüksek görsel kaliteye sahip veri gizleme tabanlı imge kimlik doğrulama algoritmaları oluşturabilmek için önerilen algoritma kullanılacaktır.

KAYNAKLAR

[1] C. Deng, X. Gao, X. Li, D. Tao, A local Tchebichef moments-based robust image watermarking, Signal Process. 89 (8) (2009) 1531–1539.

[2] J. Fridrich, D. Soukal, Matrix embedding for large payloads, IEEE Trans. Inf. Forensics Secur. 1 (3) (2006) 390–395.

[3] X. Gao, C. Deng, X. Li, D. Tao, Geometric distortion insensitive image watermarking in affine covariant regions, IEEE Trans. Syst. Man Cybern. Part C Appl. Rev. 40 (3) (2010) 278–286.

[4] V.V. Nabiyev, M. Ulutas, G. Ulutas, Doğruluk oranı iyileştirilmiş (2,n) olasılıklı görsel sır paylaşımı şeması, 3. Information Security & Cryptology Conference with International Participation, 2008.

[5] G.R. Blakley, Safeguarding Cryptographic Keys, Proceedings of the National Computer Conference, American Federation of Information Processing Societies Procedings, New York, USA, pp. 313-317, June 1979.

[6] A. Shamir, How to Share a Secret, Communications of ACM, vol. 22, no 11, pp. 612-613, 1979.

[7] M. Naor, A. Shamir, Visual cryptography, in: A. DeSantis (Ed.), Advances in Cryptology – EUROCRYPT'94, Lecture Notes in Computer Science, Perugia, Italy, vol. 950, 1994, pp. 1–12.

[8] D. Wang, L. Zhang, N. Ma, and X. Li, Two secret sharing schemes based on Boolean operations. Pattern Recognition 40(10), 2776–2785, 2006.

[9] C. Lee, W. Tsai, A data hiding method based on information sharing via PNG images for applications of color image authentication and metadata embedding, Signal Processing, pp. 2010-2025, (93), 2013.

[10] H. Yuan, Secret sharing with multi-cover adaptive steganography, Information Sciences, pp. 197-212, (254), 2014.

[11] O. Takizawa, A. Yamamura, A proposal of secret sharing using natural language text, in: IPSJ Computer Security Symposium, 2001, pp. 343–348.

[12] H. Lin, C. Yang, C. Laih, H. Lin, Natural language based visual cryptography scheme, J. Vis. Commun. Image R. , pp. 318-331, (24), 2013.

[13] G. Wang, F. Liu, W. Q. Yan, Braille for visual cryptography, IEEE International Symposium on Multimedia, 2014.

[14] MEB, Özel eğitim okulları için Braille kabartma yazı kılavuzu, MEB devlet kitapları, pp. 4, 1991.
(URL:
http://orgm.meb.gov.tr/alt_sayfalar/yayimlar/ozelegitim/blair/blair.pdf)

[15] http://sanlitarihim.blogcu.com/braille-alfabesini-dunyada-ilk-kez-osmanli-kullandi/6593257 (Son Erişim Tarihi: 16/08/2015)

[16] C. -N. Yang, New visual secret sharing schemes using Probabilistic method, Pattern Recognition Letters, 25, pp. 481-494, 2004

[17] G. Horng, T. Chen, D., -S. Tsai, Cheating in visual cryptography, Designs, Codes and Cryptography, 25, pp. 219-236, 2006.

[18] SIPI Image Database, http://sipi.usc.edu/database/ (Access Date: 26/08/2015)