Journal of the Faculty of Engineering and Architecture of Gazi University 31:3 (2016) 781-789

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

Göktürk Alfabesi Tabanlı Görsel Sır Paylaşımı Metodu ile Veri Gizleme Uygulaması

Türker Tuncer[1*], Engin Avcı[2]

[1]Fırat Üniversitesi, Teknoloji Fakültesi, Adli Bilişim Mühendisliği Bölümü, 23119, Elazığ, Türkiye
[2] Fırat Üniversitesi, Teknoloji Fakültesi, Yazılım Mühendisliği Bölümü, 23119, Elazığ, Türkiye

Ö N E Ç I K A N L A R

- Yeni bir harf tabanlı görsel sır paylaşımı şeması
- Veri gizlemeyle harf tabanlı görsel sır paylaşımı şeması
- Yeni bir çok seviyeli bilgi güvenliği uygulaması

Makale Bilgileri
Geliş: 28.08.2015
Kabul: 25.01.2016

DOI:
10.17341/gummfd.79458

Anahtar Kelimeler:
Veri gizleme, harf tabanlı görsel sır paylaşımı, damgalama, bilgi güvenliği, imge işleme

ÖZET

Günümüzde birçok sır paylaşımı ve görsel sır paylaşımı(GSP) tabanlı veri gizleme metodu önerilmiştir. GSP karmaşık matematiksel işlemler kullanmadan bilgi güvenliğini sağlayan bir yöntemdir ancak GSP metotları gürültü benzeri veriler ürettiği için, saldırganların dikkatini çekmektedir. Bu problemi çözebilmek için harf tabanlı GSP metotları önerilmiştir. Harf tabanlı GSP metotları, harflerin morfolojik özelliklerine bağımlı oldukları için istenilen performansı sağlayamamaktadır. Bu problemi çözmek için toplama tabanlı sır paylaşımı yöntemini kullanan yeni bir harf tabanlı GSP metodu geliştirilmiştir. Önerilen harf tabanlı GSP metodu harflerin morfolojik özelliklerinden bağımsızdır ve tüm doğal diller için kullanılabilmektedir. Bu makalede önerilen harf tabanlı GSP metodu, Göktürk alfabesinde bulunan harfler kullanılarak gerçekleştirilmiştir. Gizli veri önerilen Göktürk alfabesi tabanlı GSP metodu kullanılarak sır parçalarına ayrılmış ve RGB imgelerinin katmanlarına gömülmüştür. Deneysel sonuçlar, önerilen GSP tabanlı veri gizleme uygulamasının başarılı olduğunu göstermiştir.

Data Hiding Application with Gokturk Alphabet Based Visual Cryptography Method

H I G H L I G H T S

- A novel letter based visual cryptography scheme
- Data hiding algorithm with letter based visual cryptography scheme
- A new secure multi-level information security application

Article Info
Received: 28.08.2015
Accepted: 25.01.2016

DOI
10.17341/gummfd.79458

Keywords:
Data hiding, letter based visual cryptography, watermarking, information security, image processing

ABSTRACT

Nowadays, a lot of secret sharing and visual cryptography (VC) based data hiding methods have been proposed. VC provides perfectly information security without using complex mathematical operations but VC methods generates noise-like data. Thus, this methods attract attention of attackers. To solve this problem, letter based VC methods are proposed. However, letter based VC methods are dependent on morphological features of letters. To solve this problem, a new letter based VC which used additive based secret sharing. The proposed letter based VC method is independent on morphological features of letters and this method can be used all of the letters. The proposed letter based VC method used letters of Gokturk in this paper. The secret data is divided into secret shares by using Gokturk Alphabet based VC and these secret shares are embedded into R, G and B layers of color images respectively. The experimental results show that the proposed VC based data hiding application is successfully.

1. GİRİŞ (INTRODUCTION)

İnternetin yaygınlaşması ve bulut teknolojisinin kullanımının artmasıyla birlikte, bilgi güvenliğinin önemi hissedilmeye başlamıştır. Bilgi güvenliğini sağlayabilmek için çeşitli metotlar ve protokoller kullanılmaktadır. Yaygın olarak kullanılan güvenlik yöntemlerinin başında şifreleme ve veri gizleme gelmektedir. Şifreleme, bir verinin içeriğini değiştirmeye yönelik kullanılırken; veri gizleme veri içeriğini değiştirmez, o veriyi bir örtü nesnesine gizler. Veri

* Sorumlu Yazar/Corresponding author: turkertuncer@firat.edu.tr / 0531 669 3070

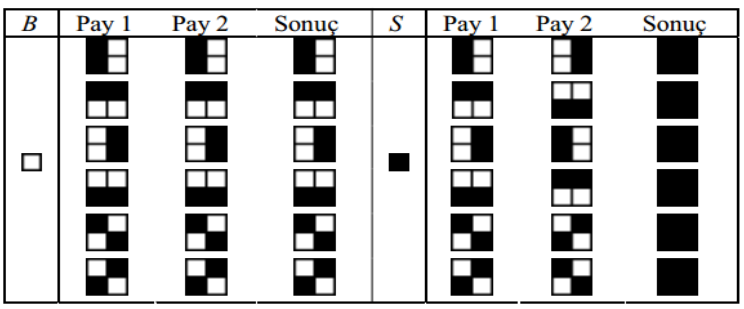
gizlemenin temel amacı ise, gizli verinin sezilememesidir [1-3]. Veri gizlemede en sık kullanılan yöntemler steganografi ve sayısal damgalamadır. Steganografide verinin güvenilir olarak alıcı tarafa iletilmesi hedeflenirken sayısal damgalama da verinin telif haklarının korunması hedeflenmektedir [4-5]. Kısacası, şifreleme verinin içeriğini korumayı amaçlarken, veri gizleme verinin sezilememesini amaçlamaktadır. Verilerin güvenilir olarak parçalara ayrılması ve dağıtılması için sır paylaşımı algoritmaları kullanılmaktadır [6]. Sır paylaşımı kriptolojik bir protokol olarak literatürdeki yerini almaktadır. Sır paylaşımı algoritmaları, ilk olarak 1979 yılında Blakley ve Shamir tarafından önerilmiştir [7, 8]. Bu yöntemlerin temel amacı gizli veriyi sır parçalarına ayırmak ve güvenilir bir dağıtıcı ile sır parçalarını dağıtmaktır. Sır parçaları bir araya geldiğinde ise gizli veri elde edilecektir. GSP metotları ilk olarak 1994 yılında Naor ve Shamir tarafından önerilmiştir [9]. GSP metotları kullanılarak görsel formda bulunan gizli veriyi, 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. Naor ve Shamir' in GSP metoduna ait kodlama tablosu Şekil 1' de verilmiştir. Ayrıca, imge kimliklendirmek ve gizli verinin güvenliğini arttırmak için GSP metotlarıyla veri gizleme metotlarının bir arada kullanılması önerilmiştir. Lee vd. PNG imgeleri kimliklendirmek için Shamir'in (k, n) GSP yöntemini kullanmışlardır [10]. Yuan sır paylaşımı algoritmalarını kullanarak çoklu örtü imgesi tabanlı uyarlamalı staganografi algoritmasını önermiştir. Önerilen algoritmada, Shamir'in sır paylaşımı metodu ile ±1 veri gizleme operatörü kullanılmaktadır. Bu algoritmayla, yüksek görsel kalite elde edilmiştir [11]. Ayrıca günümüzde sır paylaşımı ve GSP tabanlı birçok veri gizleme algoritması önerilmiştir [12-15]. Bu makalenin organizasyonu; İkinci bölümde motivasyon ve tasarım, üçüncü bölümde önerilen algoritma, dördüncü bölümde deneysel sonuçlar ve beşinci bölümde ise sonuç ve önerilerden bahsedilmiştir.

2. MOTİVASYON VE TASARIM (MOTIVATION AND DESIGN)

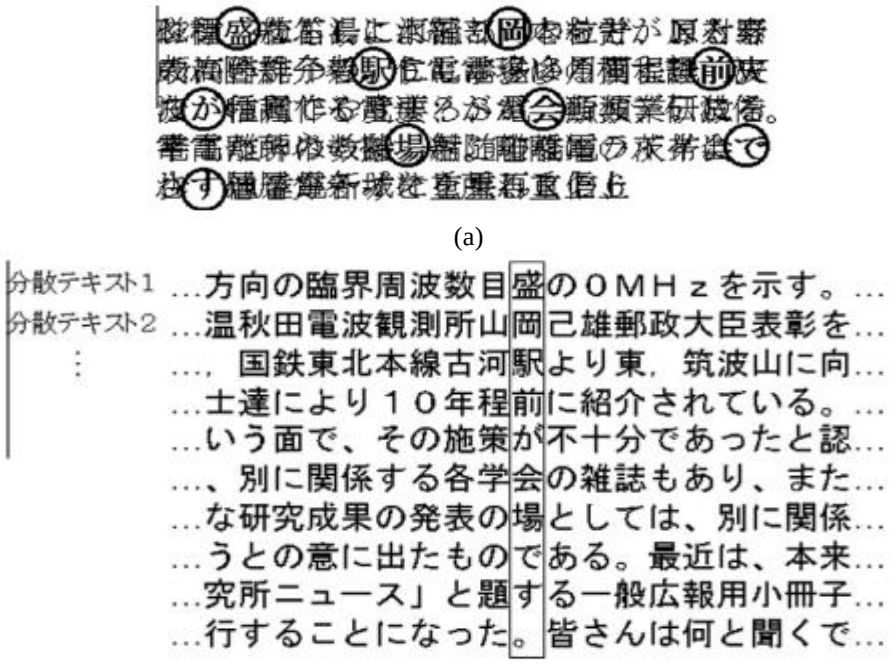
Takizawa vd. Japoncada bulunan harflerini kullanan iki adet sır paylaşımı metodu önermiştir. İlk metotta bir veritabanı oluşturulmuştur. Oluşturulan veritabanı kullanılarak harflerin morfolojik analizi gerçekleştirilmiştir. Belirlenen harfler döndürülerek, sır parçaları elde edilmiştir (Şekil 2). Takizawa vd. ikinci yaklaşımında ise, harfler kullanılarak anlamlı cümleler elde edilmiştir. Anlamlı cümleler sır parçaları olarak kabul edilmişti. Birden fazla anlamlı cümlenin bir araya gelmesiyle mesaj elde edilmiştir [16]. Lin vd. Çince, Korece, Japonca ve Latince harfleri tabanlı bir GSP metodu önermiştir. Bu metot, Naor ve Shamir'in (k,n) GSP metodunu kullanmaktadır. Önerilen metotta alt pikseller, harflerden oluşmaktadır. Oluşturulan şemanın örneği Şekil 3' de verilmiştir [17]. Literatürde önerilen harf tabanlı GSP şemaları incelendiğinde, oluşturulan sır paylaşım şemalarının harflerin morfolojik özelliklerini kullandığı gözlemlenmiştir. Doğal dillerde kullanılan harflerin morfolojik özelliklerinin farklı olmasından dolayı harf tabanlı görsel sır paylaşım şemalarının tüm alfabelerde uygulanamadığı, uygulansa dahi belirli bir harf kümesinin kullanıldığı gözlemlenmiştir. Bu makalede, tüm doğal dillerde bulunan harfleri kullanılabilecek yeni bir GSP önerilmiştir. Önerilen GSP metodunun hesapsal karmaşıklığı diğer metotlara göre düşüktür. Ayrıca bu makalede veri gizleme kullanılarak elde edilen sır parçaları gizlenmiş ve sır parçalarının hilecilik saldırılarından korunması hedeflenmiştir.

3. ÖNERİLEN METOT (THE PROPOSED METHOD)

Önerilen yöntemde harf tabanlı yeni bir görsel sır paylaşım şeması önerilmiştir. Gizli mesajı ifade edebilmek ve saldırganların dikkatini çekmeden bilgi güvenliğini sağlayabilmek için doğal dillerde kullanılan harfler ve veri gizleme kullanılmıştır. Bu yöntemin temel amacı karmaşık matematiksel işlemler kullanmadan sahtecilik saldırılarından korunabilmek, harf tabanlı GSP şemalarında var olan çalışma zamanı, piksel genişlemesi ve harfler eşit olasılıkta kullanılması problemlerini giderebilmektir. Önerilen yöntemde anlamlı görsel sır paylaşım şeması ve veri gizleme algoritması bir arada kullanılarak çok seviyeli bir bilgi güvenliği uygulaması oluşturulmuştur. Bu çalışmada Göktürk alfabesine ait 38 adet harf kullanılmıştır. Bu harfler kullanılarak anlamlı sır parçalarının oluşturulması hedeflenmektedir. Göktürk alfabesine ait harfler Şekil 4'te verilmiştir [18]. Önerilen metot kullanılarak gizli veri, anlamlı alt piksellerden oluşan sır parçalarına ayrılmaktadır. Bu metot kullanılarak hem anlamlı görsel sır parçaları elde edilmektedir hem de elde edilen sır parçaları kullanılarak RGB imgelerin kimlik doğrulaması yapılabilmektedir.



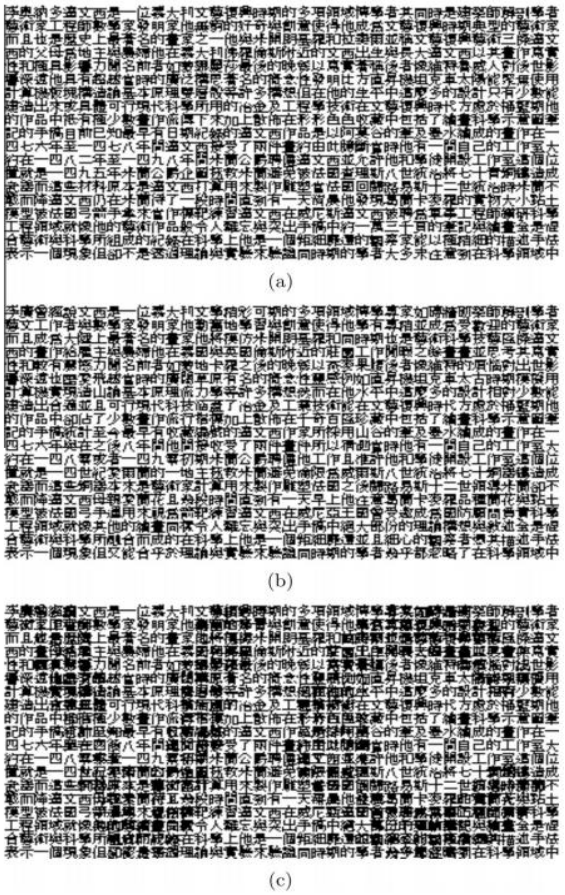
Şekil 1. Piksellerin kodlanması [6] (Coding pixels [6])



(a)

(b)

Şekil 2. Takizawa vd. (a) ilk şeması (b) ikinci şeması [16] (Takizawa et al.'s (a) first scheme (b) second scheme)



(a)

(b)

(c)

Şekil 3. (a) Pay 1 (b) Pay 2 (c) Yeniden yapılandırılmış imge [17]
((a) Secret share 1 (b) Secret share 2 (c) Reconstructed image [17])

Adım 1: Harflere ID numarası atanır. Harflere ID numarası atamak için çevrimsel asal döngüsü kullanılır [19].

$$CG = a^i \bmod p,\ p>38,\ i=\{1,2,\ldots,p\} \tag{1}$$

Adım 2: Gizli veri 3 x 2 boyutundaki bloklara ayrılır ve her blok için hedef değeri hesaplanır [$\log_2 38$] = 6. Bloklardan değerlerin elde edilmesinin en temel amacı piksel genişleme oranın azaltılmasıdır. Örneğin Liu vd.' nin önerdiği GSP metodunda kullanılan alt piksellerin boyutu 9 x 9' dur [17]. Bu durumda piksel genişleme değeri 81 olarak elde edilmektedir. Ancak Eşitlik 2 kullanılarak elde edilecek piksel genişleme değeri 9 x 9 / 6 olarak elde edilmektedir.

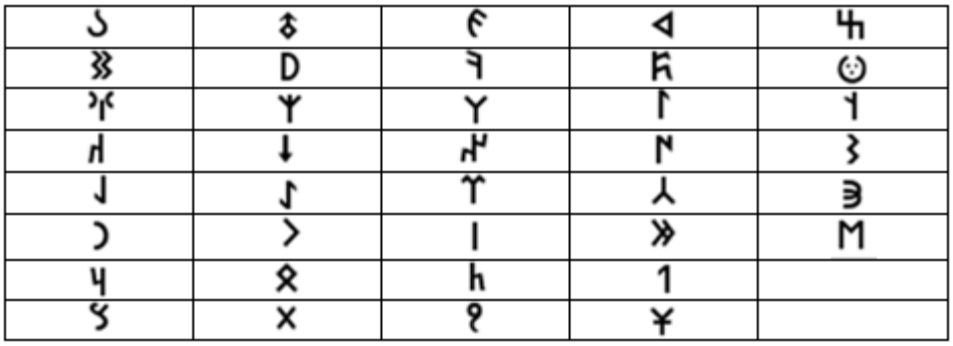
$$\begin{aligned} T = {} & WI_{i,j}2^5 + WI_{i,j+1}2^4 + WI_{i+1,j}2^3 + \\ & WI_{i+1,j+1}2^2 + WI_{i+2,j}2^1 + WI_{i+2,j+1} \\ T = {} & T \pmod{38} \end{aligned} \tag{2}$$

T hedef değeri, *WI* gizli imge *i* ve *j* ise indis değerlerini temsil etmektedir.

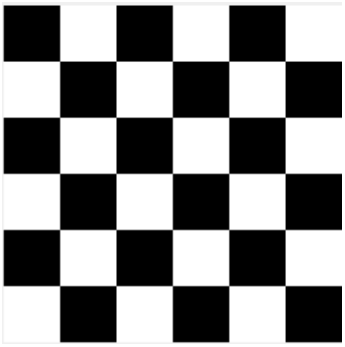
Adım 3: Oluşturulan (n, n)' lik GSP şemasının n-1 adet parçası rastgele sayı üreteci kullanılarak oluşturulmaktadır. Eşitlik 3 ve 4' te lineer eşiksel rastgele sayı üreteci [20] ve lojistik harita tabanlı rastgele sayı üretecinin [21] denklemleri verilmiştir.

$$x_{i+1} = [(cx_i + d \bmod p) \bmod 38] \tag{3}$$

$$\begin{aligned} & x_{i+1} = \mathrm{round}\left(37 r x_i (1 - x_i)\right), \\ & 3.5 \le r \le 4,\ x \ne 0.5,\ x \in [0,1] \end{aligned} \tag{4}$$



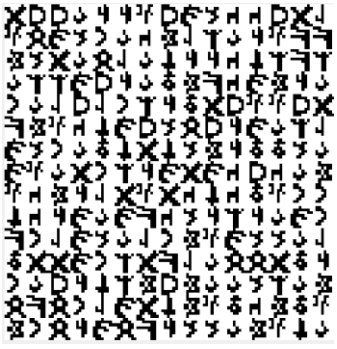
Şekil 4.Göktrük alfabesine ait harfler (Letters of Gokturk alphabet)



(a) Dama Tahtası

(b) Pay 1

(c) Pay 2



(d) Pay 3

Şekil 5. (3, 3) GSP şeması ((3,3) visual cryptography scheme)

c rastgele sayı üreteci çarpanı, *d* artım miktarı, *r* kaos katsayısı ve *x* ise elde edilen rastgele sayı dizisidir.

Adım 4: n. sır parçasını üretebilmek için Eşitlik 5-6 kullanılmaktadır [22].

$$sum = \sum_{i=1}^{n-1} id_i \tag{5}$$

$$id_n = T\text{-}sum \ (mod\ 38), \quad 0 \leq id_n \leq 37 \tag{6}$$

Adım 5: Oluşturulan sır parçaları örtü nesnesinin katmanlarına gizlenir. Şekil 5' te önerilen metot kullanılarak oluşturulan sır parçaları gösterilmektedir. Şekil 5' te dama tahtası imgesi ve bu imgeye ait 3 adet sır parçası verilmektedir Dama tahtası imgesinin özelliği, her bir blokta bulunan piksel değerlerinin birbirine eşit olmasıdır. Bu imgeye ait bloklar aynı özellikte olmasına rağmen üretilen sır parçaları Şekil 5'te görüldüğü gibi farklı özellikler göstermektedir. Önerilen veri çıkarma ve yeniden yapılandırma algoritmasının adımları aşağıda verilmiştir.

Adım 1: Çevrimsel asal döngüsünün parametreleri kullanılarak harflere ait kimlik numaraları elde edilir.
Adım 2: Örtü imge R,G ve B katmanlarına ayrılır.
Adım 3: Veri çıkarma algoritması uygulanarak sır parçaları elde edilir.
Adım 4: Örüntü eşleştirme kullanılarak harflere ait kimlik değerleri elde edilir.

Adım 5: Eşitlik 7, 8 ve 9 kullanılarak orijinal piksel değerleri hesaplanır.

$$T = \sum_{i=1}^{n} id_i \,(mod\ 38) \tag{7}$$

$$value = dec2bin(T,6) \tag{8}$$

$$WI_{i,j} = value_1,\ WI_{i,j+1} = value_2\ WI_{i+1,j} = value_3$$
$$WI_{i+1,j+1} = value_4,\ WI_{i+2,j} = value_5\ WI_{i+2,j+1} = value_6$$
$$i = \{1,3,5,\ldots,m-1\},\ j = \{1,3,5,\ldots,n-1\} \tag{9}$$

Value elde edilen değerler dizisi olarak nitelendirilmektedir.

Adım 6: Hesaplanan değerler Şekil 6' da gösterildiği gibi yerleştirilerek gizli veri elde edilir.

$value_1$	$value_2$
$value_3$	$value_4$
$value_5$	$value_6$

Şekil 6. Elde edilen değerlerin yeniden yapılandırılmış imgeye yerleştirilme
(Placing the obtained values to reconstructed image)

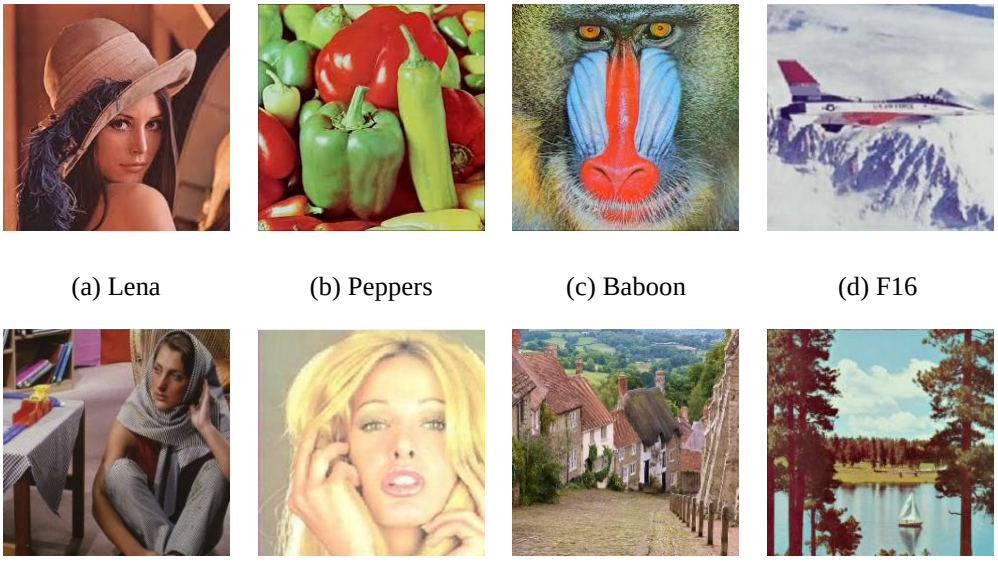
4. SONUÇLAR VE TARTIŞMA
(RESULTS AND DISCUSSIONS)

Önerilen Göktürkçe tabanlı GSP metodunu kullanana veri gizleme uygulamasını test edebilmek için SIPI [23] imge veritabanında bulunan renkli imgeler kullanılmıştır. Kullanılan imgeler 512 x 512 x 3 boyutundadır ve Şekil 7' de gösterilmiştir. Şekil 7' de verilen örtü imgelerine Şekil 8' deki damgalar gömülmüştür. (3,3) harf tabanlı görsel sır paylaşım yönteminin örneği Şekil 9' da, (2,3) harf tabanlı GSP örneği ise Şekil 10'da verilmiştir. Elde edilen sır parçaları örtü nesnesinin R, G ve B katmanlarına gizlenmiştir. Veri gizlemenin görsel kalitesini test edebilmek için MSE (mean square error, ortalama karesel hata) ve PSNR (peak signal-to-noise rate, tepe sinyal gürültü oranı) [24] ölçüm metrikleri kullanılmıştır. Bu metriklerin formülleri, Eşitlik 10 ve 11' de verilmiştir.

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(CI_{i,j} - SI_{i,j})^2 \tag{10}$$

$$\text{PSNR} = 10\log\frac{\text{Max}(CI_{ij}^2)}{\text{MSE}} \tag{11}$$

Test imgelerine 2 bpp (bit per pixel, piksel başına bit) kapasitede veri gizlenmiştir. Önerilen metoda ait PSNR değerinin diğer metotlarla karşılaştırılması Tablo 1'de verilmiştir. Önerilen harf tabanlı GSP metodunda alfabede bulunan harflerin kullanılma olasılığının birbirine yakın olması gerekmektedir. Harflerin kullanılma olasılıklarının hesaplanması için frekans analizi yapılmıştır. Frekans analizini yapabilmek için "Fırat" imgesi (2, 2) GSP metodu kullanılarak sır parçalarına ayrılmıştır.



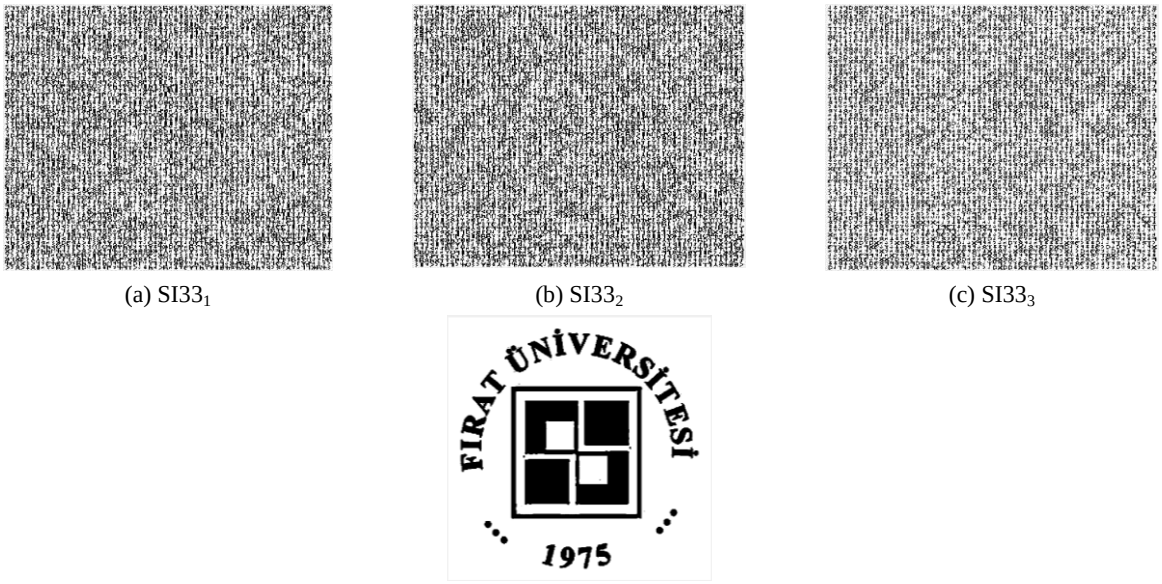
(a) Lena (b) Peppers (c) Baboon (d) F16

(e) Barbara (f) Tiffany (g) Goldhill (h) Sailboat

Şekil 7. Test imgeleri. (The test images)

(a) Fırat (b) Tübitak

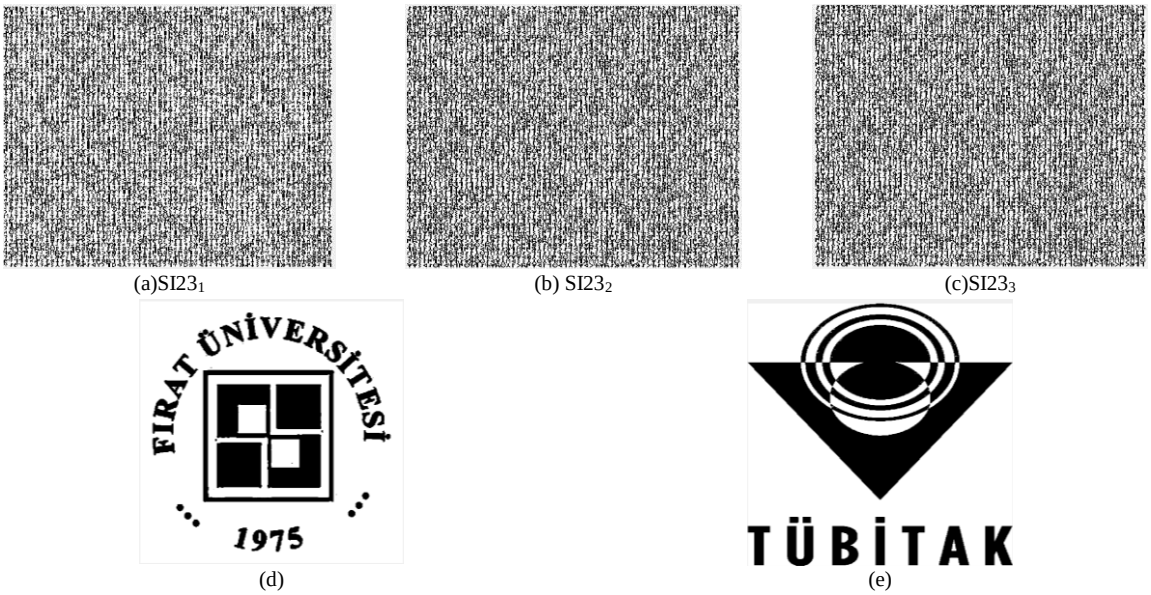
Şekil 8. Test için kullanılan damgalar (Watermarks used for test)



(a) $SI33_1$ (b) $SI33_2$ (c) $SI33_3$

(d) Gizli veri

Şekil 9. (3, 3) harf tabanlı GSP metodu uygulaması (Application of (3, 3) letter based visual cryptography)



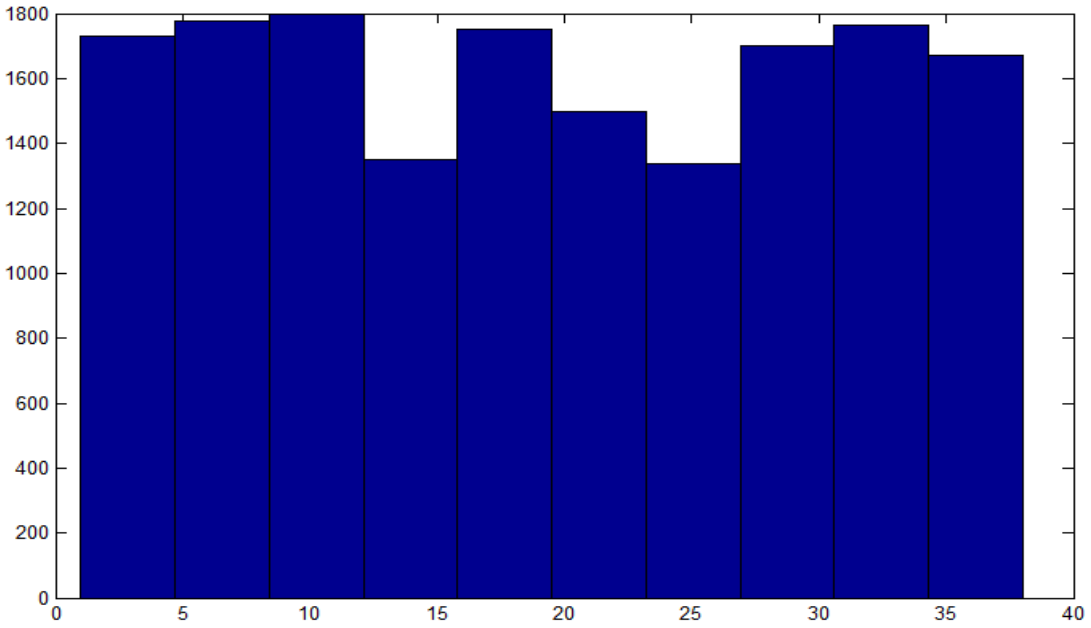
(a)$SI23_1$ (b) $SI23_2$ (c)$SI23_3$

(d) $SI23_1$ve $SI23_2$yeniden yapılandırılması. (e) $SI23_1$ve $SI23_3$yeniden yapılandırılması

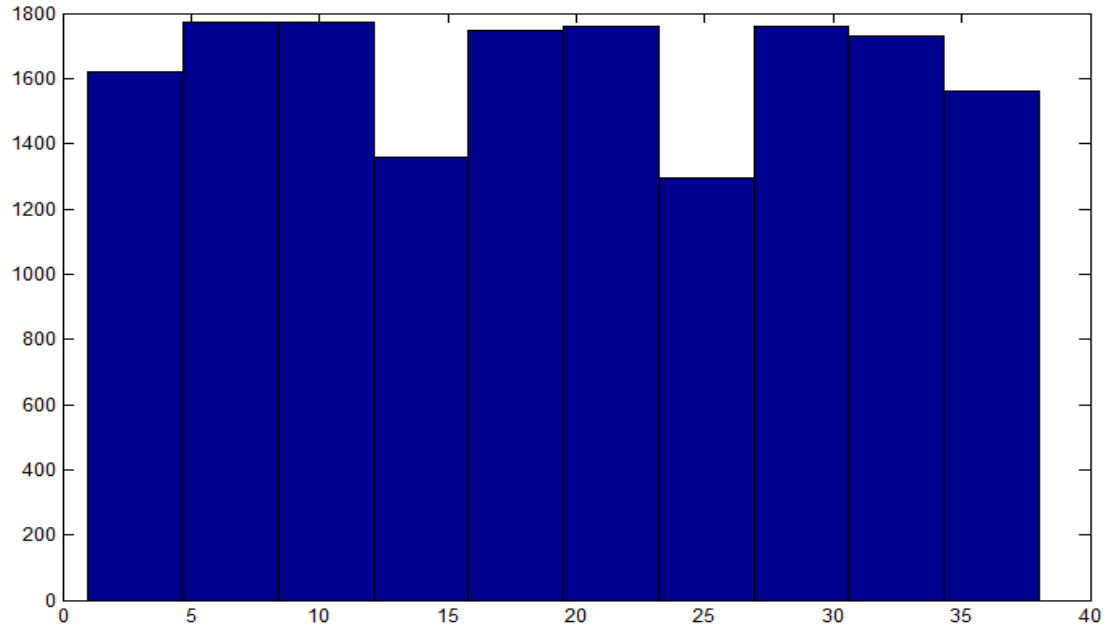
Şekil 10. (2, 3) harf tabanlı GSP metodu uygulaması (Application of (2, 3) letter based visual cryptography)

Tablo 1. Önerilen metoda ait PSNR değerinin diğer metotlarla karşılaştırılması
(Comprasion of the proposed method's PSNR values with other methods)

Stego İmge	Lin ve Tsai'nin metodu [25]	Yang vd.'nin metodu [26]	Chang vd.'nin metodu [27]	Wu vd.'nin metodu [28]	Önerilen Metot
Lena	39,20	41,60	40,37	43,54	43,58
Jet	39,25	41,66	40,73	43,53	43,56
Peppers	39,17	41,56	39,30	43,56	43,56
Baboon	39,18	41,55	39,94	43,54	43,58
Ortalama	39,2	41,59	40,08	43,54	43,57



(a)



(b)

Şekil 11. Harflere ait frekans analizi (a) İlk sır parçası (b) İkinci sır parçası
(Frequency analysis of letters (a) First secret share (b) Second secret share.)

Tablo 2. Önerilen harf tabanlı GSP metodunun Lin vd.' nin metoduyla [11] karşılaştırılması
(Comparision of the proposed letter based visual cryptography method with Lin et al.'s [11] method)

Şema	Özellik				
	Sır sayısı	Piksel Genişlemesi (m)	Olasılık	Yeniden Yapılandırma	Hesapsal Karmaşıklık
Liu vd.[17]	n	9 x 9	Harflerin şekillerine bağımlı	Gürültülü, gizli mesajı yeniden elde edebilmek için ekstra işlem gerektirir.	O(n)
Önerilen Metot	n	$\frac{9x9}{3x2}$	Harflerin şekillerinden bağımsız	Gürültüsüz, gizli mesajı elde etmek için ekstra işleme gerek yoktur.	O(1)

Sır parçalarına ayırma işleminde Matlab R2013a yazılımının rand fonksiyonu kullanılmıştır. Elde edilen sır parçalarının harf frekans analiz sonuçları Şekil 11'de verilmiştir. Şekil 11' de gösterildiği gibi, alfabede bulunan tüm harfler kullanılmıştır ve harflerin kullanılma olasılıkları birbirine yakındır. Harflerin kullanılma olasılıkları, GSP şemasında kullanılan rastgele sayı üreticine bağımlıdır. Ayrıca Liu vd.' nin [17] önerdiği harf tabanlı GSP metodu ile önerilen metodun karşılaştırılması Tablo 2'de verilmiştir.

5. SONUÇLAR (CONCLUSIONS)

Bu makalede yeni bir harf tabanlı GSP metodu önerilmiştir ve önerilen metot veri gizleme ile birlikte kullanılarak çok katmanlı güvenlik uygulaması oluşturulmuştur. Bu makalede, literatürde ilk kez toplama tabanlı sır paylaşımı kullanılarak harf tabanlı GSP şeması önerilmiştir. Önerilen algoritmanın uygulamasını gerçekleştirebilmek için Göktürk alfabesindeki harfler kullanılmıştır. Önerilen metotta lojik toplama operatörü olan VEYA' nın yerine cebirsel toplama ve mod operatörü kullanılmıştır. Gizli veri gürültüsüz ve genişlemesiz olarak yeniden yapılandırılmıştır. Önerilen metodun hesapsal karmaşıklığı O (1)' dir.

Bu makalede harf tabanlı GSP ile veri gizleme metotları birlikte kullanılarak imgeler için kimlik doğrulama yapılabileceği gösterilmiştir. Deneysel çalışmaların ilk bölümünde veri gizleme sonuçları analiz edilmiştir. Elde edilen veri gizleme sonuçları literatürdeki diğer metotlarla karşılaştırılmış ve önerilen metodun sonuçları başarılı bulunmuştur. Ayrıca deneysel çalışmaların 2. Bölümünde ise önerilen harf tabanlı GSP şeması incelenmiş ve istenilen başarım parametreleri elde edilmiştir. Bu çalışma ile harf tabanlı GSP metotlarında var olan piksel genişlemesi, harf frekans dağılımı ve çalışma zamanı gibi problemler çözülmüştür. Önerilen harf tabanlı GSP şemasının en önemli özelliği harflerin morfolojik özelliklerinden bağımsız olmasıdır. Veri gizleme kullanılarak sahtecilik saldırılarından korunmak için çok seviyeli güvenlik uygulaması gerçekleştirilmiştir. Veri gizleme ile GSP bir arada kullanılarak hızlı, yüksek kapasitede mesaj taşıma yeteneğine sahip, uygulanabilir ve güvenilir bir metot elde edilmiştir. Gelecekteki çalışmalarda, anlamlı görsel şifreli görüntüler oluşturmak için bu metot kullanılacaktır. Ayrıca veri tabanında bulunan harf ve karakter sayısı genişletilip, yeni bir GSP tabanlı imge kimliklendirme algoritmasının önerilmesi planlanmaktadır.

KAYNAKLAR (REFERENCES)

1. Deng C., Gao X., Li X., Tao D., A local Tchebichef moments-based robust image watermarking, Signal Process. 89 (8), 1531-1539, 2009.
2. Fridrich J., Soukal D., Matrix embedding for large payloads, IEEE Trans. Inf. Forensics Secur. 1 (3), 390-395, 2006.
3. Gao X., Deng C., Li X., Tao D., Geometric distortion insensitive image watermarking in affine covariant regions, IEEE Trans. Syst. Man Cybern. Part C Appl. Rev. 40 (3), 278-286, 2010.
4. Atıcı M.A., Sağıroğlu Ş., Development of a New Folder Lock Appraoch and Software Based on Steganography, Journal of the Faculty of Engineering and Architecture of Gazi University, 31 (1), 129-144, 2016.
5. Elibaşı E., Özdemir S., Secure Data Aggregation in Wireless Multimedia Sensor Networks Via Watermarking, Journal of the Faculty of Engineering and Architecture of Gazi University, 28 (3), 587-594, 2013.
6. Nabiyev V.V., Ulutas M., Ulutas G., Doğruluk oranı iyileştirilmiş (2, n) olasılıklı görsel sır paylaşımı şeması, 3. Information Security & Cryptology Conference with International Participation, 2008.
7. Blakley G.R., Safeguarding Cryptographic Keys, Proceedings of the National Computer Conference, American Federation of Information Processing Societies Procedings, New York, USA, pp. 313-317, June 1979.
8. Shamir A., How to Share a Secret, Communications of ACM, 22 (11), 612-613, 1979.
9. Naor M., Shamir A., Visual cryptography, in: A. DeSantis (Ed.), Advances in Cryptology-EUROCRYPT'94, Lecture Notes in Computer Science, Perugia, Italy, 950, 1-2, 1994.
10. Lee C., Tsai W., A data hiding method based on information sharing via PNG images for applications of color image authentication and metadata embedding, Signal Processing, 93, 2010-2025, 2013.
11. Yuan H., Secret sharing with multi-cover adaptive steganography, Information Sciences, 254, 197-212, 2014.
12. Huang H.C., Lu Y.Y., Lin J., Ownership protection for progressive image transmission with reversible data

hiding and visual secret sharing, Optik, 127, 5950-5960, 2016.

13. Avci E., Tuncer T., Avci D., A Novel Reversible Data Hiding Algorithm Based on Probabilistic XOR Secret Sharing in Wavelet Transform Domain, Arabian Journal for Science and Engineering, 41 (8), 3153-3161, 2016.

14. Liu Y., Ju L., Hu M., Zhao H., Jia S., Jia Z., A new data hiding method for H.264 based on secret sharing, Neurocomputing, 188, 113-119, 2016.

15. Tuncer T., Avci E., A reversible data hiding algorithm based on probabilistic DNA-XOR secret sharing scheme for color images, Displays, 41, 1-8, 2016.

16. Takizawa O., Yamamura A., A proposal of secret sharing using natural language text, in: IPSJ Computer Security Symposium, 343-348, 2001.

17. Lin H.C., Yang C.N., Laih C.S., Lin H.T., Natural language based visual cryptography scheme, J. Vis. Commun. Image R., 24, 318-331, 2013.

18. Göktürkçe. http://turkcesivarken.com/gokturkce. Erişim Tarihi Temmuz 1, 2016.

19. Pomerance C., Finite cyclic groups, https://math.dartmouth.edu/~carlp/rademacherlecture2.pdf, 2010. Erişim Tarihi Temmuz 14, 2016.

20. Sezgin F., Sezgin T.M., Finding the best portable congruential random number generators, Computer Physics Communications 184, 1889-1897, 2013.

21. Özkaynak F., Özer A. B., Lojistik Harita ile Rastgele Sayı Üretilmesi ve İstatistiki Yöntemlerle Sınanması, Journal of Istanbul Kültür University, 129-133, 2006.

22. Karaoğlan D., A Key Establishment Scheme for Wireless Mesh Networks using Identity-based Cryptography and Threshold Secret Sharing, Master of Science Thesis, Sabanci University, 15-16, 2009.

23. SIPI Image Database. http://sipi.usc.edu/database. Erişim Tarihi Temmuz 1, 2016.

24. Al-Domur H., Al-Ani A., A steganography embedding method based on edge identification and XOR coding, Expert Systems With Applications, 46, 293-306, 2016.

25. Lin C.C., Tsai W.H., Secret image sharing with steganography and authentication, Journal of Systems and Software, 73 (3), 405-414, 2004.

26. Yang C.N., Chen T.S., Yu K.H., Wang C.C., Improvements of image sharing with steganography and authentication, Journal of Systems and Software, 80 (7), 1070-1076, 2007.

27. Chang C.C., Hsieh Y.P., Lin C.H., Sharing secrets in stego images with authentication, Pattern Recognition, 41 (10), 3130-3137, 2008.

28. Wu C.C., Kao S.J., Hwang M.S., A high quality image sharing with steganography and adaptive authentication scheme, Journal of Systems and Software, 84 (12), 2196-2207, 2011.