Journal of the Faculty of Engineering and Architecture of Gazi University 31:4 (2016) 951-959

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

İkili imgeler için mayın tarlası oyunu tabanlı yeni bir veri gizleme algoritması

Türker Tuncer[1*], Derya Avcı[2], Engin Avcı[3]

[1]Fırat Üniversitesi, Teknoloji Fakültesi, Adli Bilişim Mühendisliği Bölümü, 23119, Elazığ, Türkiye
[2]Fırat Üniversitesi, Mühendislik Fakültesi, Elektrik-Elektronik Mühendisliği Bölümü, 23119, Elazığ, Türkiye
[3]Fırat Üniversitesi, Teknoloji Fakültesi, Yazılım Mühendisliği Bölümü, 23119, Elazığ, Türkiye

Ö N E Ç I K A N L A R

- Yeni bir veri gizleme yöntemi
- İkili imgeler için mayın tarlası oyunu kuralları
- İkili imgeler için yeni bir mayın tarlası tabanlı veri gizleme algoritması

Makale Bilgileri

Geliş: 07.08.2015
Kabul: 08.09.2016

DOI:
10.17341/gazimmfd.278450

Anahtar Kelimeler:
İkili imge,
veri gizleme,
mayın tarlası oyunu,
sayısal damgalama,
steganografi,
bilgi güvenliği

ÖZET

Günümüzde ikili imgeler için birçok veri gizleme algoritması önerilmektedir. Önerilen algoritmaların temel amacı yüksek kapasitede ve yüksek görsel kalitede veri gizlemeyi sağlamaktır. Bu amacı gerçekleştirmek için genellikle örüntü tabanlı veri gizleme algoritmaları kullanılmaktadır. Bu makalede, ikili imgeler için mayın tarlası oyunu tabanlı yeni bir veri gizleme algoritması önerilmiştir. Mayın değeri 0 veya 1 seçilerek komşuluk dereceleri hesaplanmaktadır. Komşuluk derecelerini belirlemek için 3x3 boyutundaki örtüşmeyen bloklar kullanılmıştır. Elde edilen komşuluk derecelerini değiştirerek veri gizleme işlemi gerçekleştirilmektedir. Bozulmanın minimum seviyede olması için hamming uzaklığı hesaplanmıştır. Komşuluk dereceleri farklı, benzer blokların seçiminde ise rastgele sayı üreteçleri kullanılarak algoritmanın gizliliği sağlanmıştır. Deneysel sonuçlar, önerilen veri gizleme algoritmasının başarılı sonuçlar elde ettiğini göstermiştir.

A new data hiding algorithm based on minesweeper game for binary images

H I G H L I G H T S

- A new data hiding method
- Minesweeper rules for binary images
- A new data hiding algorithm based on minesweeper for binary images

Article Info

Received: 07.08.2015
Accepted: 08.09.2016

DOI:
10.17341/gazimmfd.278450

Keywords:
Binary image,
data hiding,
minesweeper game,
digital watermarking,
steganography,
information security

ABSTRACT

Nowadays, a lot of data hiding algorithms for binary images have been proposed in the literature. The main purpose of these algorithms is to provide data hiding with high capacity and high visual quality. The pattern based data hiding algorithms are commonly used to achieve this purpose. In this paper, a new data hiding algorithm is suggested. This algorithm is based on minesweeper game for binary images. Neighborhood degree is calculated by selecting mine value as 0 or 1. The size of 3x3 non overlapping blocks have been used to determine neighborhood degree. Data hiding process is implemented by modifying the obtained neighborhood degree. Hamming distance is calculated to keep distortion in minimum level. In the selection of similar blocks with different neighborhood degrees, privacy of the algorithm is provided by using random number generators. The experimental results showed that the proposed data hiding algorithm resulted successfully.

* Sorumlu Yazar/Corresponding author: turkertuncer@firat.edu.tr / Tel: +90 531 669 3070

1. GİRİŞ (INTRODUCTION)

Bilgi güvenliğini sağlayabilmek için veriyi yetkisiz erişimlerden korumak gerekmektedir [1]. İnternetin yaygın olarak kullanılması ve akıllı cihazların taşınabilir hale gelmesiyle birlikte kişisel veriler hızlı bir şekilde sayısal ortama aktarılmaya başlamıştır. Sayısal ortamda bulunan verilerin güvenliğinin sağlanması ise çok önemli bir konu haline gelmiştir. Günümüzde, siber saldırı ve savunma yöntemlerinin ülkelerin milli savunma politikaları içerisinde yer almaya başlamıştır. Bilgi güvenliğini sağlamak için birçok yöntem bulunmaktadır ancak bu yöntemlerden en sık kullanılanları şifreleme ve veri gizlemedir. Şifreleme yöntemleri mesajın içeriğini değiştirerek veri gizliliğini sağlamayı hedeflemektedir. Şifreleme yöntemleri şifreleme algoritması, şifre çözme algoritması ve açık/gizli anahtardan oluşmaktadır. Şifreleme biliminde simetrik güven modeli, asimetrik güven modeli ve protokoller kullanılarak bilgi güvenliği sağlanmaktadır. Veri gizleme, gizli mesajı örtü nesnesi içerisine fark edilmeyecek şekilde gizlenmesi işlemidir. Veri gizlenmiş sinyale stego-sinyal denilmektedir. Veri gizlemedeki temel amaç, güvenilir olmayan bir veri iletim hattında güvenilir bir kanal açarak, saldırganların dikkatini çekmeden mesajı alıcı tarafa göndermek ve multimedya verilerinin telif haklarının korunmasını sağlamaktır [2-7]. Veri gizlemenin en sık kullanılan alt dalları steganografi ve sayısal damgalamadır. Steganografi, gizli mesajın saldırganların dikkatini çekmeden alıcı tarafa gönderilmesini hedeflerken, sayısal damgalama telif hakkı koruma ve kimlik doğrulama işlemlerini gerçekleştirmek için kullanılmaktadır [8, 9]. Veri gizleme yöntemleri yalnız kullanılabilecekleri gibi kaos, şifreleme, veri sıkıştırma, sır paylaşımı ve görsel sır paylaşımı yöntemleriyle birlikte de sıklıkla kullanılmaktadır [10-15]. Veri gizlemeyi oluşturan bileşenler ise aşağıdaki gibi verilmiştir.

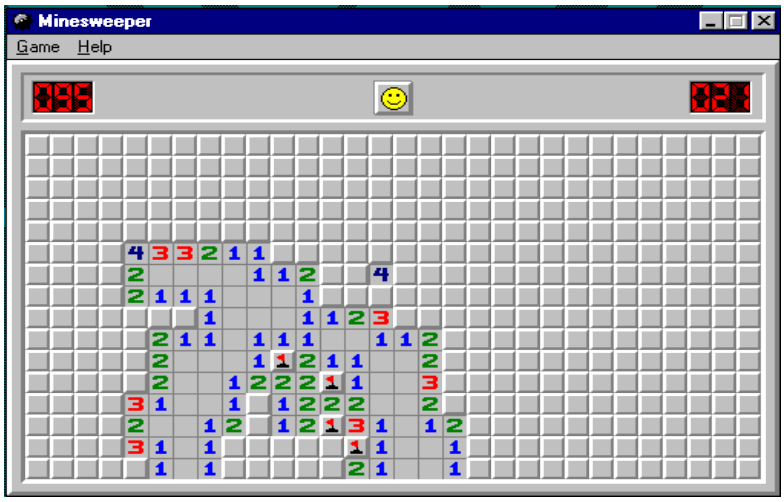
- Örtü nesnesi
- Gizli mesaj
- Veri gizleme fonksiyonu
- Veri gizleme anahtarı
- Veri gizlenmiş nesne
- Veri çıkarma fonksiyonu

Veri gizleme fonksiyonu örtü nesnede gizli mesajın nasıl gizleneceğini, veri gizleme anahtarı ise gizli mesajın örtü nesnesinin hangi konumlarına gizleneceğini belirlemektedir. Veri gizleme fonksiyonu ve veri gizleme anahtarı kullanılarak gizli mesaj örtü nesnesine gömülür. İçerisine veri gizlenmiş nesne stego nesne olarak adlandırılır. Veri gizlenmiş nesnede gizli mesajı çıkarabilmek için ise veri çıkarma fonksiyonu ve veri gizleme anahtarı kullanılır [16]. Literatürde birçok veri gizleme algoritması önerilmiştir. Önerilen algoritmalar genellikle gri seviyeli veya renkli imgeleri kullanmaktadır. Gri seviyeli imgeler için önerilen veri gizleme algoritmaları renkli imgeler için de rahatlıkla kullanılmaktadır. Ancak ikili imgeler için bu durum söz konusu değildir. İkili imgelere veri gizlemek için daha farklı yöntemlerin kullanılması gerekmektedir. İkili imgeler için önerilen çalışmalardan bazıları aşağıdaki gibi verilmiştir. Matsui ve Tanaka titrek faks imgelerine veri gizlemek için bit değiştirme tabanlı yeni bir metot önermiştir [17]. Low ve ark. satır aralığı ve karakter boşluklarını değiştirerek ikili imgeler için veri gizleme metodu önermiştir ve bu metot metin imgelerinde kullanılmıştır [18, 19]. Bunların yanı sıra tüm ikili imgeler için genel veri gizleme metotları da önerilmiştir. Koach ve Zao ikili imgelere veri gizlemek için blok tabanlı yeni bir metot önermiştir ve bu metot genel ikili imgelere veri gizlemek için kullanmıştır [20]. Ancak bu metotla yapılan veri gizlemelerde problemler meydana gelmektedir. Bu problemlerin üstesinden gelebilmek için Wu ve ark. imgenin belirli karakteristik özellik gösteren örüntülerine veri gizlemeyi önermiştir [21]. Liu ve ark. 2 x 2 boyutunda bloklar kullanarak ikili imgelere veri gizleyen yeni bir metot önermiştir [22]. Wu ve Liu örtü imgesinin piksellerine karıştırma algoritması uygulayarak blok tabanlı veri gizleme metodu önermiştir. Bu metot yüksek görsel kaliteye sahiptir ve gizlenen veri gözle fark edilmez [23]. Venkatesan ve ark. blokların paritesini kullanarak yeni bir veri gizleme metodu önermiştir. Önerilen bu metotla blok başına bir bit veri gizlenmiştir [24]. Yung ve Yoo anahtar kimlik doğrulaması için blok maske tabanlı veri gizleme algoritması sunmuştur. Kenar uyarlamalı olan bu veri gizleme algoritmasında Canny kenar çıkarma algoritmasının maskesi kullanılmıştır ve bu metotla yüksek kapasitelerde yüksek görsel kalite değerleri elde edilmiştir [25]. Jung ve Yoo ikili imgelere veri gizlemek için yeni bir algoritma sunmuştur. Yapılan çalışmada ikili imgelere veri gizlemenin diğer imgelere veri gizlemeden daha zor olduğu ve bundan dolayı ikili imgelerde kalite kontrolünün yapılması gerekliliği ortaya konmuştur. Önerilen metot blok tabanlı bir veri gizleme metodudur ve kalite kontrolünün yapılabilmesi için parite biti kullanılmıştır [26]. Wang ve ark. ikili imgeler için yüksek kapasiteli bir veri gizleme algoritması önermiştir. Sunulan algoritma blok örüntüleri kullanmaktadır. Kullanılan bloklar 2 x 2 boyutundadır. Deneysel sonuçlar, önerilen algoritmanın literatürde daha önce önerilen algoritmalarla karşılaştırılmış ve başarılı sonuçlar elde edilmiştir [27].

Bu çalışmada, ikili imgeler için mayın tarlası oyunu tabanlı yeni bir veri gizleme algoritması önerilmiştir. Mayın tarlası oyununda yer alan komşuluk dereceleri kullanılarak veri gizleme kuralları tanımlanmıştır. 3 x 3 boyutundaki bloklar kullanılarak veri gizleme işlemi gerçekleştirilmiş ve her bir bloğa 1 bit gömülmüştür. Bu çalışmanın 2. Bölümünde Mayın Tarlası oyunu, 3. Bölümünde önerilen veri gizleme algoritması, 4. Bölümünde deneysel sonuçlar 5. bölümde ise sonuçlara yer verilmiştir.

2. MAYIN TARLASI OYUNU (MINESWEEPER GAME)

Mayın tarlası oyununun ilk örnekleri 1960 ve 1970' li yılların başlarında ortaya çıkmıştır. Mayın tarlası oyunu günümüzdeki haliyle 1983 yılında piyasaya sürülmüştür. Mayın tarlası tek kullanıcılı bir video oyunudur. Oyunun amacı mayına rastlamadan tüm boş alanları bulmaktır [28].



Şekil 1. Mayın tarlası oyunu ekran görüntüsü [30] (Screenshot of minesweeper game [30])

Mayınsız alanlara tıklayınca karşımıza gelen sayılar ise, o alan etrafında bulunan mayın sayısını vermektedir. Mayın tarlası oyunu, Windows işletim sistemleriyle birlikte gelen, gelmiş geçmiş en popüler mantık ve hafıza oyunlarından biridir [29]. Oyunun amacı, mayınlı arazide mayınlardan kaçmak ve mayınsız alanları bulmaktır. Şekil 1'de oyunun ekran görüntüsü verilmiştir.

3. ÖNERİLEN METOT (THE PROPOSED METHOD)

Önerilen veri gizleme algoritması ikili görüntüler için geliştirilmiştir. Komşuluk analizi yapabilmek için 3 x 3 boyutunda komşuluk matrisi kullanılmıştır. Komşuluk matrisi Şekil 2' de verilmiştir.

$P_{i,j}$	$P_{i,j+1}$	$P_{i,j+2}$
$P_{i+1,j}$	$P_{i+1,j+1}$	$P_{i+1,j+2}$
$P_{i+2,j}$	$P_{i+2,j+1}$	$P_{i+2,j+2}$

Şekil 2. 3 x 3 komşuluk matrisi
(Neighbor matrix which size of 3 x 3)

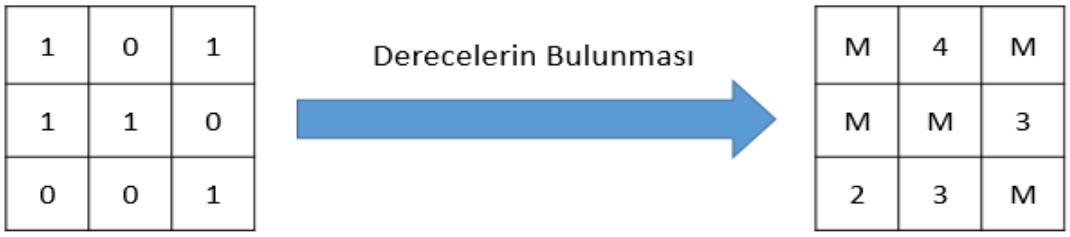
Önerilen metot ile mayınların belirlenmesi gerekmektedir. 0 veya 1 değerindeki pikseller mayın olarak seçilmektedir. Eğer 1 değeri mayın olarak seçilirse, 0 değerinde bulunan piksellerin dereceleri hesaplanmaktadır. Tüm değerleri 0 veya 1 olan 3 x 3 boyutundaki örtüşmeyen alt bloklar veri gizleme işlemi için kullanılmamaktadır. Şekil 3' te mayın derecesinin bulunmasıyla ilgili örnek verilmiştir. Yukarıdaki örnekte 1 pikseli mayın olarak seçilmiştir ve 0 olan piksellerin dereceleri bulunmuştur. Elde edilen komşuluk dereceler toplanarak matrisin değeri elde edilmektedir. Şekil 3'deki matrise ait komşuluk derecelerinin toplamı 4+3+2+3=12'dir. Örtüşmeyen alt blok olarak kullanılan matrise ait derecelerin toplamını hesaplamak için Eşitlik 1 kullanılmaktadır.

$$V = \sum_{i=1}^{n} kd_i \tag{1}$$

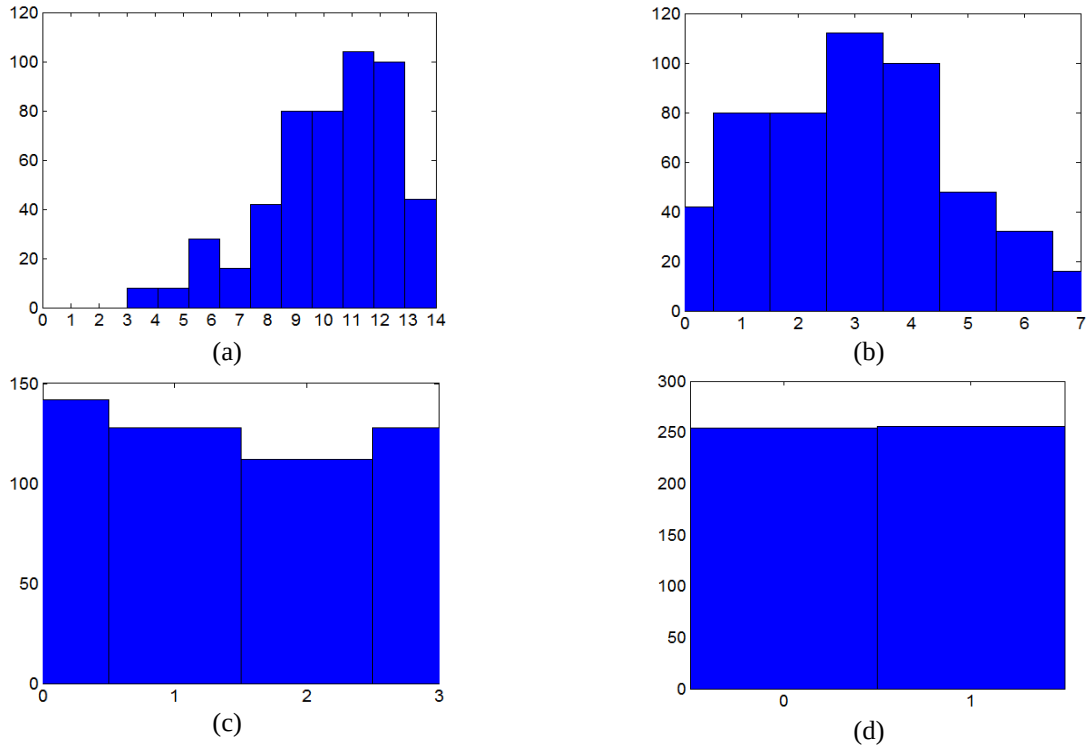
kd matristeki mayın olmayan elemanların mayınlara olan komşuluk derecesi, *V* ise alt bloğa ait komşuluk derecelerinin toplamı olarak ifade edilmektedir. Alt blok olarak kullanılan 3 x 3 boyutundaki matrisin alabileceği tüm değerler hesaplanmış ve en yüksek *V* değeri 14 olarak elde edilmiştir. Bu makalede 3 x 3 boyunda örtüşmeyen bloklar kullanılmıştır. Hesapsal karmaşıklığı indirgemek için bloktaki değerler onluk tabana çevrilmiştir. Önerilen algoritma tüm elemanları 0 veya 1 olan alt bloklara veri gizleyememektedir. Bu sebepten dolayı onluk değeri 1 ile 510 arasında olan matrislere veri gizlenmektedir. 3 x 3 boyutundaki alt bloğun onluk değeri Eşitlik 2 kullanılarak hesaplanmaktadır. Eşitlik 2' nin formülü aşağıdaki gibidir.

$$od = p_{i,j}\ x\ 2^8 + p_{i,j+1}\ x\ 2^7 + \cdots + p_{i+1,j+1}\ x\ 2^0 \tag{2}$$

od alt bloğa ait onluk değer. Ancak hesaplanan onluk değerlerin dağılımı eşit olasılıkta değildir. Bu sebepten dolayı, mod operatörü kullanılmıştır. Değerlerin dağılım histogramları Şekil 4' te verilmiştir. Şekil 4' te olası tüm alt bloklara ait komşuluk derecelerinin toplamına ait histogramlar verilmiştir ve görüldüğü gibi en iyi olasılıkta dağılım V (mod 2) işleminde görülmektedir. Komşuluk değerleri V (mod 2) işlemine göre hesaplanmaktadır. Olası tüm onluk değerler 3 x 3 boyutundaki alt bloklara dönüştürülür ve bu alt bloklar arasındaki benzerlikler hesaplanarak benzer matrisler adında bir listede tutulur. Benzerlik hesaplanırken, bit değişimi dikkate alınır ve minimum bit değişimine sahip bloklar benzer bloklar olarak kabul edilir. Örneğin 4 sayısı 9 bitte (000000100) olarak ifade edilmektedir. 4 sayısının benzerleri ise 5

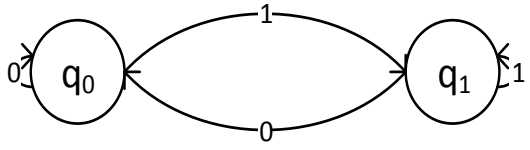


Şekil 3. Mayın=1 için komşuluk derecelerin hesaplanması (Calculating neighbor degrees for mine=1)



Şekil 4. Olası tüm onluk değerlerin komşuluk derecelerinin toplamlarına ait histogram çizelgeleri (a) V (b) V (mod 8) (c) V (mod 4) (d) V (mod 2)
(Histogram charts of sum of neighbor degrees of all possible decimal values (a) V (b) V (mod 8) (c) V (mod 4) (d) V (mod 2))

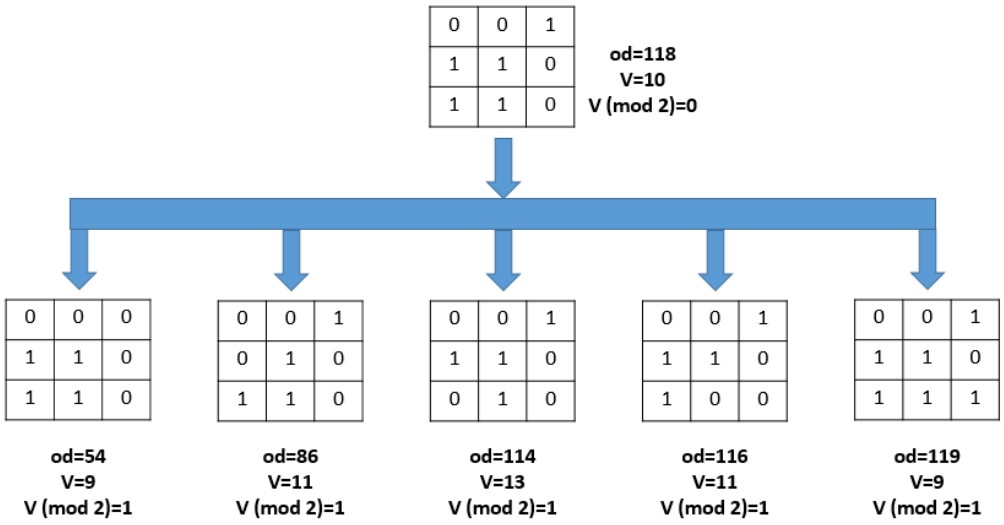
(000000101), 6 (000000110), 12 (000001100), 36 (000100100), 68 (001000100), 132 (010000100) ve 260 (10000100)'dır. Bu benzerler arasından V (mod 2) işleminin sonucu 4'ün V (mod 2) sonucuna eşit olmayan bloklar benzer adlı tabloya kaydedilir ve veri gizleme işleminde bu bloklar kullanılır. Bu işlem matrisler için bir kereliğine yapılacaktır. Veri gizleme işlemi ise Şekil 5' te gösterilen otomata kullanılarak gerçekleştirilmiştir.



Şekil 5. V (mod 2) için veri gizleme diyagramı
(Data hiding diagram for V (mod 2))

Veri gizleme algoritmasının adımları aşağıdaki gibidir.

Adım 1: Mayın olarak 0 veya 1 seç.
Adım 2: Eğer seçilen örtüşmeyen alt blok boyutu 3 x 3 ise bu alt bloğa ait onluk değer [1,510] aralığında ise adım 3'e geç değilse pencereyi bir sonraki piksellere kaydır. 3 x 3 boyutundaki alt blok 9 bitle kodlanmaktadır. Önerilen algoritma tüm elemanları 0 veya 1' den oluşan alt bloklara veri gizleyememektedir. Bu sebepten dolayı 2^0 ve $2^{3 \times 3}$ -2 arasında onluk değer alan alt bloklar kullanılmaktadır.
Adım 3: Seçilen mayına göre komşuluk dereceleri hesapla.
Adım 4: Eşitlik 1'i kullanarak V değerini hesapla.
Adım 5: Eğer V (mod 2) =0 ve gizli veri $SD_{i,j}$=1 ise V (mod 2) =0 olan ve matrise en yakın benzerlikte olan matris seçili matrisin yerine yerleştir ve adım 2'ye git. En yakın benzerlikte olan matrisleri hesaplamak için hamming uzaklığı kullanılmaktadır. İlgili bloğa hamming uzaklığı 1 olan bloklar benzer bloklar olarak adlandırılmaktadır. En



Şekil 6. Benzer bloklar (Similar blocks)

yakın benzerlikte olan matris daha önceden oluşturulmuş ve tüm olasılıkların tutulduğu liste kullanılarak seçilir. Veri gizlemek için benzer bloklardan rastgele herhangisi bir tanesi seçilerek ilgili bloğun yerine yerleştirilir. Benzer bloklar derecelerinin toplamı ilgili alt bloktan farklı olan bloklardır. Şekil 6' da benzer bloklarla ilgili bir örnek verilmiştir. Eğer Şekil 6' da gösterilen bloğa 0 verisi gömülecekse blokta değişiklik yapılmaz, eğer 1 verisi gömülecek olursa benzer bloklardan herhangi biri ilgili bloğun yerine yerleştirilir. Benzer blokları bulmak için kullanılan algoritma Tablo 1' deki algoritmada verilmiştir.

Tablo 1. Benzer blokların bulunması. (Finding similar blocks)

Algoritma 1. [1, 2^{b^2}-2] arasında bulunan tüm değerlere ait benzer blokların bulunması

Giriş: b x b boyutunda örtüşmeyen bloklar
1: say=0;
2: for i=1 to 2^{b^2}-2 do
3: for j=1 to 2^{b^2}-2 do
4: i değerini b x b bit olarak kodla
5: j değerini b x b bit olarak kodla
6: blok1 ve blok2' yi b x b boyutundaki matrise çevir
7: sayaç=0
8: for m=1 to b do
9: for n=1 to b do
10: if blok1(m,n)!=blok2(m,n) then
11: sayaç=sayaç+1;
12: endif
13: endfor
14: endfor
15: Eşitlik 1'i kullanarak V_{blok1} ve V_{blok2}' yi elde et.
16: if sayaç=1 and V_{blok1} (mod 2) != V_{blok2} (mod 2) then
17: benzer(i,say)=j;
18: say=say+1;
19: endif
20: endfor
21: endfor
Çıkış: Tüm değerlere ait benzer bloklar listesi, benzer

Adım 6: Eğer V (mod 2) =0 ve $SD_{i,j}$=1 ise V (mod 2) =1 olan ve matrise en yakın benzerlikte olan matrisi seçili matrisin yerine yerleştir ve adım 2' ye git.
Adım 7: Adım 2-6' i gizli veri boyutunca tekrarla. SD gizli veri olarak tanımlanmaktadır.

Veri çıkarma işleminde derecelerinin toplamı kullanıldığı için benzer bloklar arasında rastgele seçim yapılabilmektedir. Bir bloğa ait birden fazla benzer bloğun varlığı Şekil 6' da da gösterilmiştir. Böylece hem veri çıkarma işlemi kolaylıkla gerçekleştirilebilir hem de rastgele seçim sayesinde veri güvenliği sağlanır. Veri çıkarma algoritmasının adımları ise aşağıda verilmiştir.

Adım 1: Mayın olan piksel değerini elde et.
Adım 2: Eğer seçilen 3 x 3 matrisine ait değer [1, 510] aralığında ise adım 3'e geç değilse pencereyi bir sonraki 3 x 3 boyutundaki piksellere kaydır.
Adım 3: Seçilen mayına göre komşuluk dereceleri hesapla.
Adım 4: Formül 1'i kullanarak V değerini hesapla.
Adım 5: $SD_{i,j}$=V (mod 2) bir sonraki 3 x 3 boyutundaki matrisi seç ve adım 2'ye git.
Adım 6: Adım 2-5'i gizli veri boyutunca tekrarla.

4. SONUÇLAR VE TARTIŞMALAR
(RESULTS AND DISCUSSIONS)

Bu çalışmanın performansının test edebilmek için 512 x 512 boyutunda 6 adet ikili imge kullanılmıştır. Örtü verisi olarak kullanılan ikili imgeler Şekil 7'de gösterilmiştir. Algoritmanın performansını test edebilmek için kapasite ve görsel kalite metrikleri kullanılmıştır. Maksimum kapasite $\lfloor M/3 \rfloor x \lfloor N/3 \rfloor$ iken, ikili imgenin yapısına göre bu kapasite değişmektedir. Görsel kaliteyi test edebilmek için ise MSE (mean square error, ortalama karesel hata) ve PSNR (peak signal-to-noise rate, tepe sinyal gürültüsü) ölçütleri kullanılmaktadır. Algoritmanın başarımını test etmek için rastgele üretilmiş veriler kullanılmıştır. MSE ve PSNR' nin formülleri Eşitlik 3 ve 4'te verilmiştir [31].

Şekil 7. Test imgeleri [25] (Test images [25])

$$MSE = \sum_{i=1}^{M}\sum_{j=1}^{N}\left(CI_{i,j} - SI_{i,j}\right)^2/(M\ x\ N) \quad (3)$$

$$PSNR = 10\ x\ log_{10}(1/MSE) \quad (4)$$

Eşitlik 3'te kullanılan *CI* örtü imgesi, *SI* stego imge, *M* imgenin satır sayısı, *N* imgenin sütun sayısıdır. Önerilen metodun literatürde var olan önceki yöntemlerle karşılaştırılması Tablo 2'de verilmiştir. 3 x 3 blok boyutu için en yüksek kapasitede elde edilecek teorik PSNR değeri *10 x* log_{10} *(3 x 3 x 2)* dB olarak hesaplanmaktadır. PSNR değeri kapasiteyle ters orantılıdır.

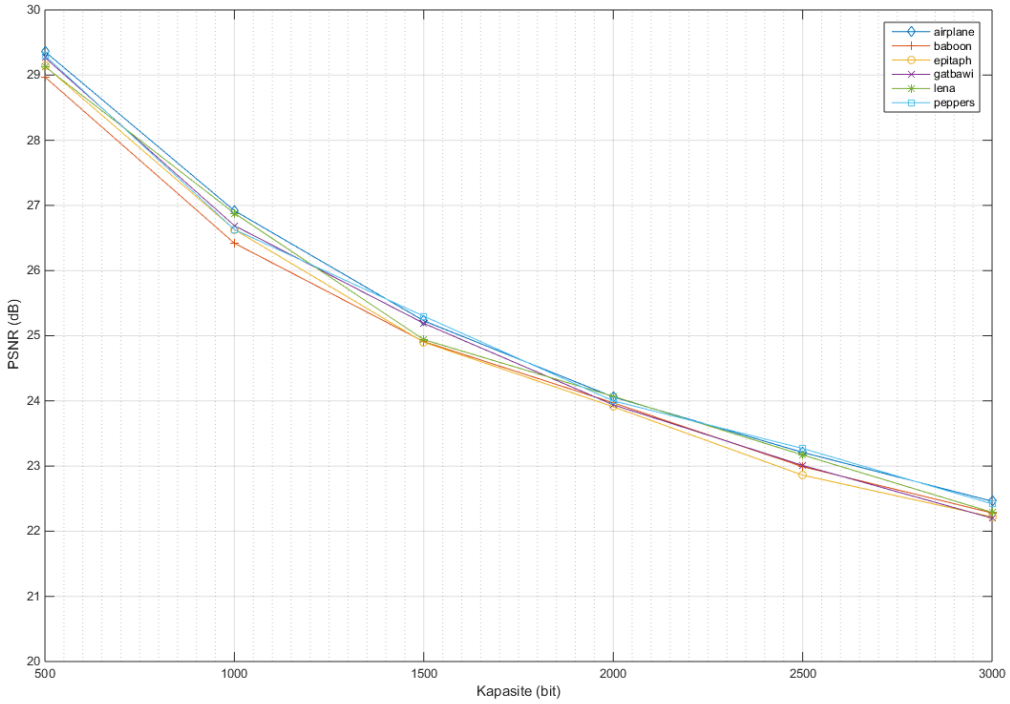
Şekil 8'de 512 x 512 boyutunda farklı yapısal özelliklere sahip ikili imgelere önerilen algoritmanın uygulanması ve elde edilen sonuçlar verilmiştir. Şekil 9'da ise kullanılan test imgelerinin PSNR/kapasite değişimleri verilmiştir.

Tablo 2. Sonuçların karşılaştırılması (Comparison of the results)

Örtü imgesi	Vankatesan ve ark. yöntemi [24]		Tseng ve ark. yöntemi [32]		Önerilen yöntem	
	Kapasite (bit)	PSNR (dB)	Kapasite (bit)	PSNR (dB)	Kapasite (bit)	PSNR (dB)
Baboon	9441	16,36	11,806	16,83	10,800	17,00
Airplane	3293	21,25	3292	21,74	3414	21,90
Lena	3657	20,45	4198	20,70	4268	21,02
Gatbawi	7273	17,13	9551	17,11	10,610	17,11
Peppers	2880	21,59	3015	20,50	3008	22,31
Epitaph	8953	17,23	9360	17,34	9641	17,40

Şekil 8. Yapısal olarak farklı özelliklere sahip ikili imgelere önerilen algoritmanın uygulanması (a) çince (b) kameraman (c) metin (d) pirinçler (e) panda (f) discover

(Implementation of the proposed method to structurally different characteristic binary images (a) chinese (b) cameraman (c) text (d) rice (e) panda (f) discover)



Şekil 9. Test imgelerinin PSNR/ kapasite değişimleri (PSNR/Capacity change rates of test images)

5. SONUÇLAR (CONCLUSIONS)

Bu çalışmada, ikili imgeler için mayın tarlası tabanlı yeni bir veri gizleme algoritması önerilmiştir. Mayın olarak 0 veya 1 değeri seçilmiştir. Mayınsız bölgelerin derecelerini hesaplamak için komşuluk analizi kullanılmış ve bu dereceler toplanarak bloğa ait değer elde edilmiştir. Blok değerleri değiştirilerek veri gizleme işlemi gerçekleştirilmiştir. Önerilen veri gizleme algoritmasının başarımı kapasite ve görsel kalite parametreleri kullanılarak değerlendirilmiştir. Önerilen algoritma literatürde daha önceden önerilmiş yöntemlerle karşılaştırılmış ve başarılı sonuçlar elde edilmiştir. Ayrıca eşit olasılıkta dağılım ve benzer eleman seçiminde kullanılan rastgele sayı üreteci sayesinde veri güvenliği sağlanmıştır. Önerilen metodun ilerleyen çalışmalarda, gri seviyeli ve renkli imgelerde veri gizleme için kullanılabileceği gösterilmiştir. Gelecekteki çalışmalarda, farklı oyunlara ait kurallar kullanılarak veri gizleme işlemlerinin yapılabileceği gösterilmiştir.

TEŞEKKÜR (ACKNOWLEDGEMENT)

Bu çalışmaya değerli tavsiyeleriyle katkı sağlayan hakemlere, okumalarıyla çalışmanın gelişmesini sağlayan Arş. Gör. Yunus Korkmaz ve İlknur Tuncer'e teşekkür ederiz.

KAYNAKLAR (REFERENCES)

1. Ni Z., Shi Y.Q., Ansari N., Su W., Reversible Data Hiding, IEEE Transactions on Circuits and Systems for Video Technology, 16 (3), 354–362, 2006.

2. Begum M.B., Venkataramani Y., LSB Based Audio Steganography Based on Text Compression, Procedia Engineering, 30, 703-710, 2012.

3. Perez-Gonzlez F., Balado F., Quantized projection data hiding, in Proc. IEEE Int. Conf. Image Process., 2, 889–892, 2002.

4. Shi Y.Q., Ni Z., Zou D., Liang C., Lossless data hiding: fundamentals, algorithms and applications, IEEE Int. Symp. Circuits Syst., 33–36, 2004.

5. Mao Q., A fast algorithm for matrix embedding steganography, Digital Signal Processing, 25, 248-254, 2014.

6. Von Ahn, L., Hopper N.J., Public-key steganography, in Advances in Cryptology-Eurocrypt, Berlin, Germany: Springer-Verlag, 3027, 323–341, 2004.

7. Lin G.S., Chang Y.T., Lie W.N., A framework of enhancing image steganography with picture quality optimization and anti-steganalysis based on simulated annealing algorithm, IEEE Trans. Multimedia, 12 (5), 345–357, 2010.

8. 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.

9. Elbaşı 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.

10. Çavuşoğlu, Ü., Uyaroğlu, Y., Pehlivan, İ., Design of A Continuous-Time Autonomous Chaotic Circuit and

Application of Signal Masking, Journal of the Faculty of Engineering and Architecture of Gazi University, 29 (1), 79-87, 2014.

11. Bouslimi D., Coatrieux G., Cozic M., Roux C., Data hiding in encrypted images based on predefined watermark embedding before encryption process, Signal Processing: Image Communication 47, 263–270, 2016.

12. 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.

13. 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.

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., Avcı E., Data Hiding Application with Gokturk Alphabet Based Visual Cryptography Method, Journal of the Faculty of Engineering and Architecture of Gazi University, 31 (3), 781-789,2016.

16. Avci E., Tuncer T., Ertam F., Çok katmanlı görüntü steganografi, 7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 2014.

17. Matsui K., Tanaka K., Video-steganography: how to secretly embed a signature in a picture, in: Proc. IMA Intellectual Property Project, 187–206, 1994.

18. Low S.H., Maxemchuk N.F., Lapone A.M., Document identification for copyright protection using centroid detection, IEEE Trans. Commun., 372–383, 1998.

19. Brassil J.T., Low S.H., Maxemchuk N.F., Copyright protection for the electronic distribution of text documents, in: Proc. of IEEE, 1181-1196, 1999.

20. Koch E., Zhao J., Embedding robust labels into images for copyright protection, in: Proc. of the International Congress on Intellectual Property Rights for Specialized Information, Knowledge & New Technologies, 242–251, 1995.

21. Wu M., Tang E., Liu B., Data hiding in digital binary images, in: IEEE Inter. Conf. on Multimedia & Expo, 393–396, 2000.

22. Liu C., Dai Y., Wang Z., A novel information hiding method in binary images, J. Southeast Univ., 98-101, 2003.

23. Wu M., Liu B., Data hiding in binary image for authentication and annotation, IEEE Trans. Multimedia, 528–538, 2004.

24. Venkatesan M., Meenakshidevi P., Duraiswamy K., Thiagarajah K., A new data hiding scheme with quality control for binary images using block parity,in: 3rd Inter. Symposium on Information Assurance and Security, 468–471, 2007.

25. Yung K.H., Yoo K.Y., Data hiding method in binary images based on block masking for key authentication, Information Sciences, 277, 188-196, 2014.

26. Yung K.H., Yoo K.Y., Data hiding method with quality control for binary images, J. Software Engineering & Applications, 2, 20-24, 2009.

27. Wang C.C., Chang Y.F., Chang C.C., Jang J.K., Lin C.C., A high capacity data hiding scheme for binary images basedon block patterns, The Journal of Systems and Software, 93, 152–162, 2014.

28. Mayın Tarlası, http://www.bilgisayamiyorum.com/question/252.aspx, Erişim Tarihi: 06/08/2015.

29. Minesweeper, http://windows.microsoft.com/tr-tr/windows/minesweeper-how-to#1TC=windows-7, Erişim Tarihi: 07/08/2015.

30. Minesweeper, https://aidanjreid.com/2014/12/30/why-dating-is-like-minesweeper/, Erişim Tarihi: 06/08/2015.

31. 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.

32. Tseng H.W., Wu F.R., Hsieh C.P., Data hiding for binary images using weight mechanism, IIHMSP, 307–310, 2007.