mühendislikdergisi
Dicle Üniversitesi Mühendislik Fakültesi
Cilt: 8, Sayı: 3,525-534
Temmuz 2017

İkili imgeler için blok tabanlı yeni bir kimlik doğrulama yöntemi

Türker TUNCER

Fırat Üniversitesi, Adli Bilişim Mühendisliği Bölümü, Elazığ

Makale Gönderme Tarihi: 20.12.2016 Makale Kabul Tarihi: 13.02.2017

Öz

İkili imge kimlik doğrulamada genellikle sayısal damgalama teknikleri kullanılmaktadır. İkili imgelerin için önerilen sayısal damgalama teknikleri diğer damgalama tekniklerinden farklıdır çünkü ikili imgelerin piksel değerleri 0 ve 1'dir. İnsan görme sisteminin ikili imgelerde yapılan küçük değişimleri algılayabilmesinden dolayı, ikili imgelerde damgalama gri seviyeli veya renkli imgelerde damgalamadan daha zordur. Bu makalede ikili imgelerde kimlik doğrulama için yeni bir kırılgan damgalama yöntemi önerilmiştir. Önerilen kırılgan damgalama yöntemi bloklara bölme, gömülebilir blok belirleme, özellik çıkarma, veri gizleme, veri çıkarma, veri doğrulama ve saldırı tespiti aşamalarından oluşmaktadır. Öncelikle, ikili görüntü bloklara bölünür. Kurallara göre yerleştirilebilir bloklar belirlenir. Gömülebilir bloklar, 3 öznitelik çıkarma blokları ve bir veri gizleme bloğu olmak üzere 4 alt bloğa ayrılmıştır. Özellik değeri, özellik çıkarma blokları kullanılarak elde edilir. Filigran gömme yeri (indis) ve doğrulama biti, özellik değeri kullanılarak hesaplanır. Veri gizleme bloklarının piksel değerleri, özellik kullanılarak belirlenir ve bu değerler, kimlik doğrulama bitleriyle değiştirilir. Filigran çıkarma aşamasında, özellik değerleri, özellik çıkarımı kullanılarak hesaplanır. Bloğun özellik değeri pikselin değeri ile aynı ise, kimlik doğrulama işlemi tamamlanır. Aksi halde saldırı tespit yapılır. Önerilen yöntemin performansını ölçmek için değişken boyuttaki bloklar, kullanılmıştır. Deneysel sonuçlar, önerilen yöntemin yüksek görsel kalite, kapasiteye sahip olduğunu ve bu yöntemin pratikte kullanılabileceğini göstermektedir.

Anahtar Kelimeler: *İkili imge kimlik doğrulama; Kırılgan damgalama; Özellik çıkarma; Veri gizleme; Bilgi güvenliği.*

*Yazışmaların yapılacağı yazar: Türker TUNCER. turkertuncer@*fırat.edu.tr*; Tel: (424) 237 00 00 (3485)

Giriş

Bilişim teknolojilerinin gelişmesiyle birlikte, dokümanlar hızlı bir şekilde sayısal ortama aktarılmaya başlamıştır. Sayısallaşan verilerin erişim kontrolünün sağlanması için genellikle elektronik imzalar kullanılmaktadır. Günümüzde belge yönetimi sistemlerinde kâğıt ortamının yerine elektronik belge yönetimi sistemleri yaygınlıkla kullanılmaktadır. Sayısallaşan doküman verileri ikili imgeler halinde de bulunmaktadır. Bu verilerin kimlik doğrulaması ve inkâr edilememesinin sağlanması için ikili imge kimlik doğrulama yöntemlerinin kullanılması gerekmektedir. İkili imge kimlik doğrulama için sıklıkla veri gizleme ve sayısal damgalama yöntemleri kullanılmaktadır (Ma vd., 2015; Furon, 2005; Fridrich, 2005; Shropshire vd., 2015; Lavanya vd., 2013; Liu ve Zhao, 2010).

İkili imgelere veri gizlemek, gri seviyeli veya renkli imgelere veri gizleme işleminden daha zor bir işlemdir. Çünkü ikili imgenin pikselleri yalnızca 0 veya 1 değerlerini almaktadır. Bu sebepten dolayı, ikili imgelere veri gizlemek veya bu imgeleri kimlik doğrulama için blok tabanlı veri gizleme veya damgalama yöntemleri kullanılmaktadır. Doküman imgeleri de ikili imgeler olduğu için, ikili imgeler için kullanılan imge kimlik doğrulama yöntemlerinin doküman imgeleri için kullanılabileceği gösterilmiştir.

Bu makalede ikili imgelerde kimlik doğrulama için yeni bir yöntem önerilmiştir. Önerilen yöntem blok tabanlıdır. Bu yöntemin temel amacı gömülebilir blokları alt bloklara bölerek yüksek görsel kaliteye sahip yeni bir imge kimlik doğrulama yöntemi elde etmektir. Bu özelliğinden dolayı bu yönteme makro blok tabanlı imge kimlik doğrulama yöntemi de denilebilir. Makro bloklar 3 adet özellik bloğu ve bir adet veri gizleme bloğuna ayrılmaktadır. Özellik çıkarma blokları kullanılarak veri gizleme indisi ve kimlik doğrulama biti elde edilir. Bu çalışmada basit matematiksel yöntemler kullanılarak efektif bir imge kimlik doğrulama yöntemi elde edilmiştir. Bu çalışmada önerilen teknik, yüksek görsel kalite ve kapasiteye sahip, saldırı tespiti yapabilen yöntemdir. Ayrıca bu çalışma genişletilebilir bir yöntemdir. Damga üretme aşamasında farklı kurallar veya fonksiyonlar kullanılarak yeni imge kimlik doğrulama yöntemlerinin oluşturulabileceği makale içerisinde gösterilmiştir. Önerilen yöntemin özellikleri aşağıdaki gibi verilmiştir.

- Önerilen yöntem herhangi bir veriye ihtiyaç duymadan veriyi geri çıkarabilmektedir.
- Bloklar veri özellik çıkarma ve veri gizleme bloğu olarak ikiye ayrılmıştır.
- Özellik çıkarma blokları kullanılarak doğrulama biti elde edilmektedir.
- Özellik çıkarma blokları kullanılarak veri gizleme indisi elde edilmektedir.
- Özellik çıkarma, veri gizleme ve veri çıkarma işlemlerinin maliyetleri düşüktür.
- Önerilen yöntem veri gizleme ve kimlik doğrulama yöntemi olarak kullanılabilmektedir.
- Önerilen yöntem genişletilebilir bir yöntemdir. (Kullanıcı farklı özellikler tanımlayabilmektedir).
- Önerilen yöntem değişken boyuttaki alt blokları kullanabilmektedir.
- Gömülebilir alanlar kullanılarak anahtar elde edilmektedir.
- Anahtar kullanılarak sahtecilik tespiti işlemleri gerçekleştirilmektedir.
- Önerilen yöntem kullanılarak yüksek veri gizleme kapasitesi ve yüksek görsel kaliteye sahip imge kimlik doğrulama yöntemi elde edebilmektir.
- Önerilen yöntem kullanılarak ikili formda bulunan sayfaların da kimlik doğrulaması yapılabilmektedir. Bu yöntem kullanılarak eğitim alanında bilgi güvenliği uygulamalarının gerçekleştirilebileceği gösterilmiştir.

Önerilen yöntem herhangi bir örüntü veya maske kullanmadan imge kimlik doğrulama işlemini gerçekleştirebilmesidir. Bu çalışma, ikili imge kimlik doğrulama veya doküman kimlik doğrulama alanlarında efektif olarak kullanılabilir. Bu konuyla literatürde birçok çalışma yapılmıştır. Yapılan çalışmalar aşağıdaki gibi verilmiştir.

Wu ve Liu (2004), ikili imgeleri ve dokümanları kimlik doğrulama için blok tabanlı bir yöntem önermişlerdir. Önerilen yöntemde blokların ilişkileri hesaplanarak imge özellikleri çıkarılmıştır. Çıkarılan özellikler karıştırma işleminden geçirilip örtü nesnesine gizlenmek-

tedir. Gömülen veriyi çıkarmak için orijinal örtü nesnesine ihtiyaç duyulmamaktadır. Yang ve Kot (2006), çift katmanlı kör ikili imge kimlik doğrulama şemasını önermişlerdir. İlk katmanda imgenin tümünün kimlik doğrulaması hedeflenirken ikinci katmanda saldırı tespiti yapmak için gerekli işlemler bulunmaktadır. Görüntüde değişebilir pikseller tespit edilerek makro bloklar halinde kodlanır. Makro bloklar kullanılarak özellik çıkarma ve veri gizleme işlemi yapılmaktadır. Guo ve Zhang (2003), ikili dokümanlar, taranan şekiller ve ikili imgeler için yüksek veri gizleme kapasitesine sahip imge kimlik doğrulama yöntemini önermişlerdir. Sayılan bu metotların en önemli eksikleri, uygulama alanında sıklıkla kullanılamamalarıdır. Tzeng ve Tsai'nin (2003) yönteminde kimlik doğrulaması yapılacak imge n adet bloğa ayrılır. Kimlik doğrulama bitlerini oluşturmak için paylaşılmış simetrik anahtar kullanılır. Kimlik doğrulama bitleri n adet bloğa sırasıyla gömülerek imge kimlik doğrulama işlemi yapılır. Wu ve Liu'nun (2004) yönteminde değiştirilebilir pikseller tespit edilir ve bu piksellere kimlik doğrulama bitleri gömülür. Wu ve Liu'nun (2004) yöntemi bu yönüyle pratikte uygulanabilir bir yöntemdir. Kim vd.'nin (Kim, 2003; Kim ve Afif, 2004) ilk yöntemi sözde rastgele sayı üreteci kullanarak veri gizleme indisini belirlemektedir. Belirlenen piksel 0 yapılmaktadır. Sayısal imza ve Mesaj kimlik doğrulama kodları (MAC) kullanılarak kimlik doğrulama bitleri üretilir. Üretilen kimlik doğrulama bitleri örtü imgeye gömülür. Kim'in (Kim, 2005) ikinci yönteminde ise ilk yöntemde meydana gelen görsel bozulmayı indirgemektir. Lee vd. (2007) görsel bozulmayı minimize eden bir imge kimlik doğrulama yöntemi önermiştir. Yang ve Kot (2007), Kim vd.'nin (Kim, 2003; Kim and Afif, 2004) yöntemlerinin görsel kalitesini geliştirmek için ikili imge kimlik doğrulama yöntemi önermiştir.

Bu makalede, ikili imgeler için blok tabanlı yeni bir imge kimlik doğrulama yöntemi önerilmiştir. Makalenin organizasyonu şu şekildedir. 2. bölümde önerilen kimlik doğrulama yöntemi, 3. bölümde deneysel sonuçlar ve 4. bölümde sonuç ve öneriler sunulmuştur.

Önerilen Kimlik Doğrulama Yöntemi

Bu makalede ikili imge kimlik doğrulama için önerilen yöntem 4 ana kısımdan oluşmaktadır. Bunlar;

- Nokta belirleme
- Özellik çıkarma
- Veri gizleme
- Veri çıkarma ve saldırı tespiti aşamalarından oluşmaktadır.

Önerilen imge kimlik doğrulama yönteminin adımları aşağıdaki gibidir;

Adım 1: İmge elde edilir.

Adım 2: Blok boyutu belirlenir. İmge örtüşmeyen alt bloklara ayrılır.

Adım 3: Veri gizlenebilir bloklar belirlenir. Veri gizlenebilir blokları tüm elemanları 0 veya 1'lerden oluşmayan bloklardır. Bu makalede, bloklar 2M x 2M boyutunda seçilmiştir.

Adım 4: n. blokta bir bit veri gizlenir. n-1 adet bloğun değerleri elde edilir ve buradan elde edilen değerler kullanılarak özellikler elde edilir. Bu makalede kullanılan alt bloklar M x M boyutundadır. 3 adet alt blok özellik çıkarmak için, 1 adet alt blok ise veri gizlemek için kullanılır. Özellik çıkarma ve veri gizleme için aşağıdaki eşitlikler kullanılmaktadır.

$$T = \sum_{i=1}^{2M}\sum_{j=1}^{2M} sb_{i,j} \quad (1)$$

$$E = \sum_{i=M+1}^{2M}\sum_{j=M+1}^{2M} sb_{i,j} \quad (2)$$

$$F = T - E \quad (3)$$

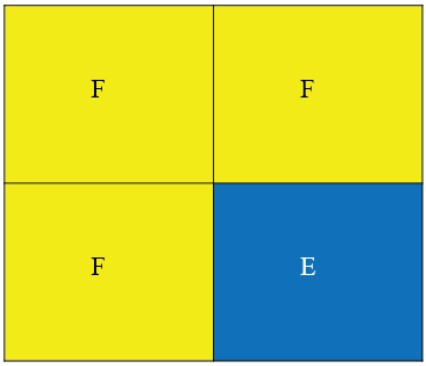
$$indis = F \ (mod\ M^2) \quad (4)$$

$$satir = \left\lfloor \frac{indis}{M} \right\rfloor \quad (5)$$

$$sutun = indis\ (mod\ M) \quad (6)$$

T değeri makro blokta bulunan piksellerin toplamı, E değeri veri gizlenecek blokta bulunan piksel değerlerinin toplamını, F değeri özellik değerini, indis verinin nereye gömüleceğini, *satir* veri gizlenecek noktanın satır değerini, *sutun* değişkeni ise veri gizlenecek pikselin sütun değerini belirtmektedir. *Satır* ve *sutun*

değişkenleri veri gizlenecek pikselin veya noktanın lokasyonunu oluşturmaktadır. Bu lokasyon veya indis kullanılarak doğrulama biti gömme ve saldırı tespiti işlemleri gerçekleştirilmektedir. Özellikler sadece özellik çıkarma bloklarından elde edilmektedir. Veri gizleme bloklarındaki değerler değiştirildiği için özellik değeri hesaplanırken işleme tabi tutulmazlar çünkü önerilen yöntem kör sayısal damgalama yöntemidir. Kör sayısal damgalama yöntemlerinde damgayı çıkarmak için ek veriye ihtiyaç duyulmamaktadır. Eşitlik 1-6 kullanılarak doğrulama bitinin indis belirlenmektedir. Şekil 1' de özellik çıkarma ve veri gizleme blokları gösterilmiştir.



Şekil 1. Özellik çıkarma ve gizleme blokları.

Şekil 1' de F ile gösterilen bloklar özellik çıkarma blokları E ile gösterilen blok ise veri gizleme bloğudur.

Doğrulama bitini hesaplamak için Eşitlik 7 kullanılmaktadır.

$$db = \sum_{i=M+1}^{2M} \sum_{j=M+1}^{2M} sb_{i,j} - sb_{i+satir,j+sutun} \, (mod2) \quad (7)$$

Eşitlik 7' de sb siyah beyaz imgeyi ifade etmektedir.

Adım 5: Elde edilen özellikler n. blokta gösterilen yere gömülür. Bu pikselin değeri ve indisi kimlik doğrulama kodunu vermektedir. Kimlik doğrulama kodunu daha güvenilir bir formda saklayabilmek için anahtar verisi de kullanılabilmektedir. Kimlik doğrulama bitinin gömülmesi Eşitlik 8' de verilmiştir.

$$sb_{i+satir,j+sutun} = db \quad (8)$$

Önerilen kimliklendirme yönteminin veri çıkarma ve saldırı tespit basamağında ise M değeri kullanılarak blok tabanlı özellik çıkartılır. Elde edilen özellikler ile kimlik doğrulama değeri birbirine eşit ise kimlik doğrulama işlemi doğrudur, eğer bu iki değer birbirine eşit değilse saldırı tespiti yapılır. Önerilen veri çıkarma ve saldırı tespiti yönteminin adımları aşağıdaki gibi verilmiştir.

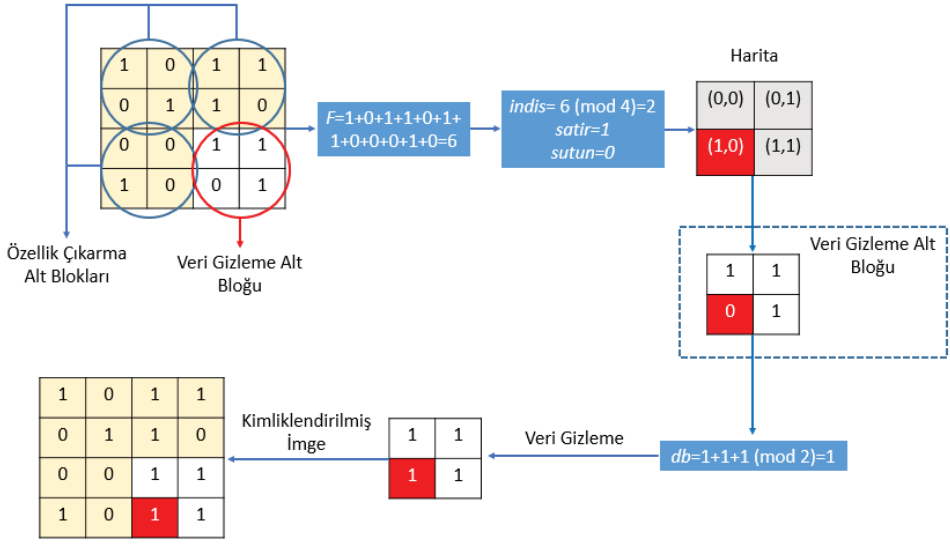
Adım 1: Alıcı tarafa M değeri yollanır.

Adım 2: M değeri ve Eşitlik 1-7 kullanılarak özellik çıkarılır ve kimlik doğrulama değeri elde edilir.

Adım 3: Eğer kimlik doğrulama değeriyle gösterilen değer birbirine eşit ise kimlik doğrulama işlemi başarılıdır.

Adım 4: Eğer kimlik doğrulama değeriyle gösterilen değer birbirine eşit değilse ilgili bloklara saldırı yapılmıştır.

Önerilen yöntemle ilgili örnek Şekil 2'de verilmiştir.



Şekil 2. Önerilen yöntemin özellik çıkarma, doğrulama biti üretme ve veri gizleme örneği.

Şekil 2'deki örnekte özellik çıkarma bloklarının piksel değerleri toplanarak özellik değeri elde edilir. Özellik değeri kullanılarak veri gizleme indisi tespit edilir. Veri gizleme bloğunda, veri gizlenecek piksel değerinin dışındaki değerler kullanılarak doğrulama biti elde edilir. Doğrulama bitinin hesaplanması için veri gizleme bloğundaki veri gizlenecek piksel haricindeki tüm değerler toplanır ve mod 2 işlemi uygulanır. Şekil 2' deki örnekte 4 x 4 boyutundaki bloklar ve 2 x 2 boyutundaki alt bloklar kullanılmıştır. Bu sebepten dolayı, indis değerinin gösterdiği indise db değeri gömülerek imge kimliklendirme işlemi tamamlanır. İmge kimlik doğrulama işleminde özellik blokları kullanılarak doğrulama biti ve indis değerleri elde edilir. Veri gizleme alt bloğunda indis değerinin gösterdiği değer ile hesaplanan db değeri aynı ise imge kimlik doğrulama işlemi başarılıdır, değilse saldırı tespiti yapılır. Bu kimlik doğrulama işlemi sadece gömülebilir bloklar için geçerlidir. Şekil 2'deki örnek blok tabanlı saldırı tespitini de özetlemektedir. Tüm imgede kimlik doğrulama işlemini gerçekleştirmek için anahtar üretilmesi gerekmektedir. Anahtar üretilmesinin sözde kodu Algoritma 1' de verilmiştir.

Algoritma 1. Anahtar üretilmesinin sözde kodu.

Giriş: W x H boyutunda orijinal imge (OI), blok boyutu M
Çıkış: W/M x H/M boyutunda anahtar (key)

```
1:row=0;
2:for i=1 to W step by M do
3:   col=0;
4:   for j=1 to H step by M do
5:      tpl=0;
6:      for k=0 to M-1 do
7:         for l=0 to M-1 do
8:            tpl=tpl+OI(i+k,j+l);
9:         endfor
10:     endfor
11:     if tpl=0 then
12:        key(row+1,col+1)=0;
13:     elseif tpl=M^2
14:        key(row+1,col+1)=1;
15:     else
16:        key(row+1,col+1)=2;
17:     endif
18:     col=col+1;
19: endfor
20: row=row+1;
21:endfor
```

Saldırı tespiti aşamasında Algoritma 1 kullanılarak anahtar üretilir. Üretilen anahtar

orijinal imgenin anahtarıyla karşılaştırılır. Eğer anahtar değerleri farklıysa saldırı tespiti yapılır. Eğer iki anahtarın ilgili indisi 2 ise blok tabanlı saldırı tespiti yapılır. Saldırı tespitinin şartları Eşitlik 9' da verilmiştir.

$$tamper(i{:}\,i+M-1, j{:}\,j+M-1) = \begin{cases} Wkey(row,col) \neq Okey(row,col) \\ Wkey(row,col) = Okey(row,col) = 2 \; and \; WI_{i+satir,j+sutun} \neq db \end{cases} \quad (9)$$

$$i = \{1,2,\dots,W\}, j = \{1,2,\dots,H\}, row = \left\{1,2,\dots,\left\lfloor\frac{W}{M}\right\rfloor\right\}, col = \left\{1,2,\dots,\left\lfloor\frac{H}{M}\right\rfloor\right\},$$

Eşitlik 9' da *Wkey* damgalı imgenin veya değiştirilmiş imgenin anahtarı, *Okey* orijinal imgenin anahtarı, *row* ve *col* anahtarlara ait indisler, *i* ve *j* ikili imgelerin indisleri, *satir* ve *sutun* ise özellik çıkarma işlemi sonucu elde edilen veri gizleme indisini oluşturan yükseklik ve genişlik parametreleridir.

Deneysel Sonuçlar

Önerilen metodun performansını ölçmek için PSNR (tepe sinyal gürültü oranı, peak signal to-noise ratio) ve kapasite kullanılmıştır. PSNR ve kapasite metriklerinden sonuç elde edebilmek için Şekil 3'de gösterilen imgeler kullanılmıştır.

Şekil 3. Deneylerde kullanılan test imgeleri (a) Baboon, (b) Lena, (c) Text, (d) Goldhill, (e) Peppers, (f) Cameraman.

Önerilen algoritmanın görsel kalitesini ölçebilmek için ortalama karesel hata (MSE) ve PSNR kullanılmıştır. MSE ve PSNR' nin formülleri aşağıdaki Eşitlik 9 ve 10'da verilmiştir (Tanchenko, 2014).

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(CI_{i,j} - SI_{i,j})^2 \quad (9)$$

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

Veri gizleme kapasitesini ölçmek için ise gömülen bit sayısı hesaplanmıştır. Veri gizlemek için 4 x 4, 6 x 6, 8 x 8 ve 10 x 10'luk makro bloklar kullanılmıştır. Elde edilen kapasite ve PSNR değerleri Tablo 1'de verilmiştir. Şekil 3'te literatürde sıklıkla kullanılan test imgeleri verilmiştir. Bu imgeler önerilen yöntemin diğer yöntemlerle karşılaştırılması için gereklidir.

Tablo 1. Blok boyutuna göre elde edilen PSNR ve kapasite değerleri.

Örtü İmgeleri	4 x 4		6 x 6		8 x 8		10 x 10	
	Kapasite	**PSNR**	**Kapasite**	**PSNR**	**Kapasite**	**PSNR**	**Kapasite**	**PSNR**
Baboon	8483	18.06	4578	20.34	2909	22.69	1955	24.36
Lena	3464	21.74	2645	23.04	1996	23.94	1629	25.31
Text	5355	20.92	3490	20.98	2534	24.16	1871	23.93
Goldhill	3295	21.34	2215	22.67	1713	24.21	1365	25.04
Peppers	3315	21.81	2013	23.86	1377	25.45	1035	26.55
Cameraman	2411	23.78	1830	25.92	1269	27.05	909	29.29

Tablo 2. Sonuçların karşılaştırılması.

Örtü İmgeleri	Vankatesan ve ark.'nın yöntemi (Vankatesan et al., 2007)		Tseng ve ark.'nın yöntemi (Tseng et al., 2007)		Tuncer ve ark.'nın yöntemi (Tuncer et al., 2016)		Önerilen yöntem	
	Kapasite (bit)	PSNR (dB)	Kapasite (bit)	PSNR (dB)	Kapasite (bit)	PSNR (dB)	Kapasite (bit)	PSNR (dB)
Baboon	9441	16.36	11,806	16.83	10,800	17.00	11,599	16.71
Airplane	3293	21.25	3292	21.74	3414	21.90	3486	21.91
Lena	3657	20.45	4198	20.70	4268	21.02	4129	21.03
Gatbawi	7273	17.13	9551	17.11	10610	17.11	9694	17.44
Peppers	2880	21.59	3015	20.50	3008	22.31	3315	21.81
Epitaph	8953	17.23	9360	17.34	9641	17.40	9413	19.18

Önerilen yöntemle, önceki yöntemlerin PSNR/Kapasite karşılaştırılması Tablo 2'de verilmiştir. Kapasiteleri arttırmak için 2 x 2 ve 4 x 4 boyutunda makro bloklar hibrit olarak kullanılmıştır. Bu işlemin temel amacı yüksek kapasitelerde görsel kaliteyi ölçebilmektir.

Sonuç ve Öneriler

Bu makalede makro blok tabanlı yeni bir ikili imge kimlik doğrulama algoritması önerilmiştir. Önerilen algoritmada bir makro bloktan 4 adet blok elde edilebilmektedir. Bu bloklardan 3 tanesi özellik çıkarma 1 tanesi ise veri gizleme için kullanılmaktadır. Bu makalede 2 x 2, 3 x 3, 4 x 4 ve 5 x 5 boyutundaki alt bloklardan oluşan 4 x 4, 6 x 6, 8 x 8 ve 10 x 10 boyutundaki makro bloklar kullanılmıştır. Önerilen yöntemin performansı görsel kalite, kapasite metrikleri kullanılarak ölçülmüş ve başarılı sonuçlar elde edilmiştir. Önerilen yöntemin doküman imgelerinin kimlik doğrulamasında kullanılabileceği gösterilmiştir.

İlerleyen çalışmalarda bu yöntemin uygulamada kullanılması ve farklı özellik çıkarma yöntemleriyle denenmesi planlanmaktadır. Özellik elektronik belge yönetim sistemlerinde dokümanların kimlik doğrulamasını sağlayabilmek için bu yöntemin kullanılması öngörülmektedir.

(a) Baboon (b) Airplane

(c) Lena (d) Gatbawi

(e) Peppers (f) Epitaph

Şekil 3. Karşılaştırma için kullanılan ikili test imgeleri (Yung and Yoo, 2014).

Kaynaklar

Fridrich, J., (2005). Steganography in digital media: Principles, algorithms, and applications, Cambridge University Press, 2005.

Furon, T., (2005). A survey of watermarking security International workshop on digital watermarking, Lecture notes on computer science, Vol. 3710, *Springer,* 201–215.

Guo M., Zhang H., (2010). High Capacity Data Hiding for Binary Image Authentication, International Conference on Pattern Recognition,.

Kim H., (2005). A new public-key authentication watermarking for binary document images resistant to parity checks, in: Proc: IEEE International Conferences on Image Processing (ICIP), vol. 2, pp. 1074–1077.

Kim, H., Afif, A., (2003). Secure authentication watermarking for binary images, in: Proc. Brazilian Symposium on Computer Graphics and Image Processing, pp. 199–206.

Kim, H., Afif, A., (2004). A secure authentication watermarking for halftone and binary images, *International Journal of Imaging Systems and Technology* 14 (4), 147–152.

Lavanya, B., Smruthi, Y., Elisala, S. R., (2013). Data hiding in audio by using image steganography technique, IJETTCS, Volume 2, Issue 6.

Lee, Y., Hur, J., Kim, H., Park, Y., Yoon H., (2007). A new binary image authentication scheme with small distortion and low false negative rates, IEICE Transactions on Communications E90-B (11) 3259–3261.

Liu, Y. Zhao, J., (2010). A new video watermarking algorithm based on 1D DFT and Radon transform, *Signal Processing*, Volume 90, Issue 2, 626-639.

Ma, X., Pan, Z., Hu, S., Wang, L., (2015). Reversible data hiding scheme for VQ indices based on modified locally adaptive coding and double-layer embedding strategy, J. Vis. Commun. Image R. 28, 60–70.

Shropshire, J., Warkentin, M., Sharma, S., (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior, *Computers & Security*, Volume 49, 177-191.

Tanchenko A., (2014). Visual-PSNR measure of image quality, J. Vis. Commun. Image R. 25,874–878.

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

Tuncer, T., Avcı, D., Avcı, E., (2016). İkili imgeler için mayın tarlası oyunu tabanlı yeni bir veri gizleme algoritması, *Journal of the Faculty of Engineering and Architecture of Gazi University* 31:4, 951-959.

Tzeng, C., Tsai, W., (2003). A new approach to authentication of binary images for multimedia communication with distortion reduction and security enhancement, IEEE Communications Letters 7 (9) 443–445.

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

Wu, M., Liu, B., (2004). Data hiding in binary images for authentication and annotation, IEEE Transactions on Multimedia 6 (4), 528–538.

Wu, M.,Liu, B., (2004). Data Hiding in Binary Image for Authentication and Annotation, IEEE Transactions on Multimedia, Vol 6, No 4.

Yang, H. Kot, A. C., (2006). Binary Image Authentication With Tampering Localization by Embedding Cryptographic Signature and Block Identifier, IEEE Signal Processıng Letters, Vol. 13, no. 12.

Yang, H., Kot, A.C., (2007). Pattern-based data hiding for binary image authentication by connectivity-preserving, IEEE Transactions on Multimedia 9 (3), 475–486.

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

A Novel Block Based Authentication Method for Binary Images

Extended Abstract

Digital watermarking techniques have been commonly used for binary image authentication. The digital watermarking techniques for binary images are different from other watermarking techniques because the pixel values of the binary images are 0 and 1. Digital watermarking techniques for binary images is more difficult than watermarking in gray-level or colored images, because the human vision system can perceive small changes in binary images. In this article, a new fragile watermarking method is proposed for authentication for binary images. In this paper, a new fragile block based watermarking method for binary images authentication is proposed. The proposed method consists of dividing into blocks, determining embeddable blocks, feature extraction, data hiding, data extraction, data verification and tamper detection steps. Firstly, the binary image is divided into blocks. According to rules, embeddable blocks are determined. Embeddable blocks are divided into 4 sub-blocks which are 3 feature extraction blocks and a data hiding block. The feature value is obtained by using the feature extraction blocks. Watermark embedding location (index) and authentication bit is calculated by using feature value. The pixel values of the data hiding blocks are determined by using feature and these values modified with authentication bits. In watermark extraction phase, feature values are calculated by using feature extraction. If the feature value of the block is the same as the value of the pixel, the authentication process is completed. Otherwise, the attack is detected. Blocks in variable sizes are used to measure the performance of the proposed method. Experimental results have shown that the proposed method has high visual quality, capacity and this method can be used in practice.

Authentication bit generation and watermark embedding steps are given below.
Step 1: Obtain image.
Step 2: Determine block size
Step 3: Divide image to sub-blocks by using non-overlapping blocks.
Step 4: Determine embeddable blocks. Pixels of embeddable blocks which are not all 0 and 1. In the proposed method, feature extractor blocks and data hiding block are used.
Step 4: I used Eq. 1-7 to generate embeddable bit and data hiding indices. To extract feature, Eq. 1-7 are used.
Step 5: The obtained authentication bit and index are used for data hiding. Data hiding process is described in Eq. 8.
Data extraction and tamper detection steps are given below.
Step 1: Use Eq. 1-7 for feature extraction.
Step 2: If determined pixel value is equal to authentication bit, image authentication is successful.
Step 3: If determined pixel value is not equal to authentication bit, go to tamper detection. In this method, 2M x 2N sized blocks are used for image authentication. 4 M x N sized blocks are obtained from 2M x 2N blocks. The first 3 blocks are used for feature extraction. The last block is used for data hiding. In the proposed method, 4 x 4, 6 x 6, 8 x 8 and 10 x 10 sized macro blocks are used for performance testing. 2 x 2, 3 x 3, 4 x 4 and 5 x 5 size blocks are also used for feature extraction and data hiding in these macro blocks.

The characteristics of the proposed method are given below.
The proposed method can extract authentication bits without any map or data. This method is blind watermarking and image authentication method.
In a macro block, blocks are divided into feature extraction blocks and data hiding block.
Authentication bit and its index are determined by using feature extraction blocks.
Execution cost of the proposed method is low.
The proposed method is an extensible method. (The users can define different features.)
The proposed method can use sub-blocks in various sizes.
The key is obtained by using embeddable pixels.
The proposed method has tamper detection ability by using the key.
The proposed method has high visual quality and high payload capacity.
Visual quality and data hiding capacity are used for performance test. PSNR (Peak Signal Noise-to Ratio) and payload capacity are used in this test.

Experimental results showed that the proposed method resulted successfully and the proposed method obtained higher capacity and visual quality than previously proposed methods in the literature.

Keywords: *Binary image authentication; Fragile watermarking; Feature extraction; Data hiding; Information security.*