Journal of the Faculty of Engineering and Architecture of Gazi University 32:3 (2017) 877-886

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

Tekil değer ayrışımı tabanlı yeni bir imge kimliklendirme yöntemi

Türker Tuncer*
Fırat Üniversitesi, Teknoloji Fakültesi, Adli Bilişim Mühendisliği Bölümü, 23119, Elazığ, Türkiye

ÖNEÇIKANLAR

- TDA tabanlı özellik çıkarımı
- Damga üretmek için güvenilir sözde rastgele sayı üreteçleri kullanımı
- Blok tabanlı imge kimliklendirme için yeni bir yaklaşım

Makale Bilgileri
Geliş: 31.05.2016
Kabul: 28.04.2017

DOI:
10.17341/gazimmfd.337637

Anahtar Kelimeler:
İmge kimliklendirme, tekil değer ayrışımı, kırılgan damgalama, veri gizleme, bilgi güvenliği

ÖZET

İmgelerde kimlik doğrulama için kırılgan damgalama yöntemleri yaygın olarak kullanılmaktadır. Sayısal damgalama tekniklerinin kırılganlığını arttırmak için genellikle özet fonksiyonları, parite bitleri ve sır paylaşımı gibi yöntemler kullanılmaktadır. Bu makalede tekil değer ayrışımı (TDA) ve blok tabanlı yeni bir veri gizleme tekniğiyle imge kimlik doğrulama işlemi önerilmiştir. Önerilen yöntemde blok boyutu kullanıcı tarafından belirlenebilmektedir. Bu uygulama da 2 x 2, 4 x 4, 8 x 8 veya M x M boyutunda bloklar kullanılmıştır. Her bir bloktan TDA kullanılarak özellik çıkarılmıştır. Elde edilen özellikler blok büyüklüğüne göre basamaklandırılmış. Damga üretme aşamasında güvenilir sözde rastgele üreteçleri kullanılarak damga üretilir. Özellikler ile damga şifrelenir ve şifrelenmiş damga önerilen damga gömme yöntemi kullanılarak örtü imgeye gömülür. Bu yöntem ön işlem, özellik çıkarımı, basamaklama, damga üretme, damga şifreleme, damga gömme, damga çıkarma, damga deşifreleme ve saldırı tespiti aşamalarından oluşmaktadır. Yöntemin görsel kalitesi tepe sinyal gürültü oranı (TPGO - PSNR) ve saldırı tespiti yeteneği bit hata oranı (BER) ile ölçülmüştür. Deneysel sonuçlar önerilen metodun başarılı olduğunu göstermiştir.

A novel image authentication method based on singular value decomposition

HIGHLIGHTS

- SVD based feature extraction.
- Usage secure pseudo random number generators for watermark generation.
- A novel approach for block based image authentication

Article Info
Received: 31.05.2016
Accepted: 28.04.2017

DOI:
10.17341/gazimmfd.337637

Keywords:
Image authentication, singular value decaomposition, fragile watermarking, data hiding, information security

ABSTRACT

Fragile watermarking methods have been widely used for image authentication. In order to increase the fragility of digital watermarking techniques, cryptologic hash functions, parity bits and secret sharing methods are generally used. In this article, a new image authentication method based on singular value decomposition (SVD) with a new block-based data hiding technique is proposed. The block size can be determined by the user in the proposed method. In this work, 2 x 2, 4 x 4, 8 x 8 or M x M size of blocks are used. Features are extracted from each block using SVD. Extracted features are quantizated by block size. In the stage of watermark generation, watermarks are generated by using secure pseudo random generators. The generated watermark is encrypted by extracted features and encrypted watermark is embedded into cover image using the proposed data hiding function. This method consists of preprocessing, feature extraction, quantization, watermark generation, watermark encryptiom, watermark embedding, watermark extraction, watermark decryption and tamper detection. The visual quality of the suggested method is measured by peak signal to noise ratio (PSNR) and tamper detection capability is measured by bit error rate (BER). Experimental results have demonstrated that the proposed method is successful.

*Sorumlu Yazar/Corresponding Author: turkertuncer@firat.edu.tr / Tel: +90 531 669 30 70

1. GİRİŞ (INTRODUCTION)

Son yıllarda bilişim teknolojileri insan hayatının her alanında kullanılmaktadır. Son zamanlarda ortaya çıkan nesnelerin interneti teknolojisiyle artık tüm cihazlar için internet kavramı meydana çıkmıştır. Bu teknolojilere paralel olarak multimedya teknolojisi de hızlı bir gelişim ve değişim geçirmiştir [1]. Sosyal paylaşım platformlarının yaygınlaşması, sağlık hizmetlerinin bilişim alt yapısını kullanması, uzaktan eğitim platformalarının yaygın olarak kullanılmasıyla birlikte multimedya veri iletimi ve multimedya verilerimim paylaşılması yaygın hale gelmiştir [2]. Multimedya verilere kolayca erişilmesinden dolayı, bu verileri değiştirebilecek araçlar da geliştirilmiştir. Adobe photoshop, Strimark, Microsoft Paint gibi araçlarla multimedya veriler özellikle imgeler kolaylıkla değiştirilebilmektedir [3]. Bu durum, imgeler için bilgi güvenliği konusunun sıcak başlıklı konular arasında yer almasını sağlamıştır [4]. Günümüzde karşılışılan en büyük problemlerden birisi de imgelerin kimlik doğrulamasının yapılmasıdır. İmgeler için kimlik doğrulama genel olarak iki başlıkta incelenmektedir. Bunlar, aktif imge kimlik doğrulama ve pasif imge kimlik doğrulamasıdır [5]. Pasif imge kimlik doğrulamasında kopyala yapıştır sahteciliği ve diğer sahtecilik ataklarının tespit edilmesi amaçlanmaktadır. Pasif imge kimliklendirme yöntemlerinde, orijinal imge bilinmeden veya önceden herhangi bir işlem yapılmadan kimlik doğrulama işleminin yapılması hedeflenir. Aktif imge doğrulama yöntemleri ise imza tabanlı kimlik doğrulama yöntemleri ve kırılgan damgalama teknikleri olarak iki alt grupta incelenmektedir. İmza tabanlı imge kimlik doğrulama yöntemlerinde kriptolojik özet fonksiyonları ve açık anahtar tabanlı şifreleme yöntemleri kullanılmaktadır. Kırılgan damgalama yöntemlerinde ise damga imgeyle ilişkilendirilir. Bu tür yöntemlerde ya damga üretme aşaması vardır, ya da damga dışardan girilmektedir. Damgayı imgeye gizlemek için damga gömme yöntemleri kullanılmaktadır. Damga gömme yöntemlerinin asıl amacı, minimum bozulmayla damgayı imgenin içerisine gizlemektir. Kırılgan damgalama yöntemleri genellik kör damgalama yöntemleridir. Kör damgalama yöntemlerinde, damgayı çıkarmak için orijinal imgeye veya ekstra bir veriye gerek duyulmaktadır. Kırılgan damgalama yöntemlerinin diğer bir özelliği de saldırı tespiti yapabilmeleri ve saldırı yapılan bölgeyi tespit edebilmeleridir [6]. Ayrıca sayısal damgalama teknikleri uzaysal alan ve frekans alanını kullanmaktadır. Uzaysal alan kullanan sayısal damgalama tekniklerinde piksel değerleri doğrudan değiştirilmektedir. Frekans alanını kullanan sayısal damgalama teknikleri ise Ayrık Fourier Dönüşümü (AFD) [7], Ayrık Kosinüs Dönüşümü (AKD) [8], Ayrık Dalgacık Dönüşümü (ADD) [9] gibi frekans dönüşüm tekniklerini kullanarak frekans katsayılarını elde etmek kullanılmaktadır. Bu çalışmada Tekil Değer Ayrışımı (TDA) tabanlı yeni bir imge kimlik doğrulama yöntemi önerilmiştir. Önerilen yöntem blok tabanlı bir kimlik doğrulama yöntemidir ve bu yöntem ön işlem, özellik çıkarma, basamaklama, anahtar üretme, damga şifreleme, damga gömme, damga çıkarma, veri doğrulama ve saldırı tespiti aşamalarından oluşmaktadır. Önerilen yöntemin öne çıkan yönleri aşağıda verilmiştir. Bu çalışmada LSB (En Anlamsız Bit, Least Significant Bit) eliminasyon yöntemi kullanıldıktan sonra özellik çıkarılmıştır. Bu sayede veri doğrulama işlemi kolaylıkla yapılabilmektedir. Önerilen yöntemde özellik çıkarmak ve damga gömmek için farklı boyutta bloklar kullanılabilmektedir. Özellik çıkarma aşamasında TDA kullanılmaktadır. Önişlem aşamasıyla bloktaki tüm pikseller ya tek ya da çift hale dönüştürülmektedir. Bu işlem ile önerilen yöntemin imge kimlik doğrulama arttırılmıştır. Bu yöntem düşük maliyetli ve efektif bir yöntemdir. Önerilen yöntem genişletilebilir bir yöntemdir. Damga üretme aşamasında çalışmada önerilen yöntem dışındaki yöntemler de kullanılabilmektedir. Önişleme aşamasında ve damga gömme fonksiyonunda ±1 operatörü kullanılmıştır. Bu operatör sayesinde yüksek görsel kalite elde edilmiştir. Damga üretiminde, güvenilir sözde rastgele sayı üreteçleri kullanılmıştır. Üretilen damga ile özellikler şifrelenerek, damga ile örtü imge ilişkilendirilmiştir. Güvenilir sözde rastgele sayı üreteçlerinin kullanılmasıyla, önerilen yöntem olasılıksal bir forma dönüştürülmüştür. Bu çalışmanın diğer bölümleri şu şekilde organize edilmiştir. İlgili çalışmalar ikinci bölümde, önerilen yöntem üçüncü bölümde, deneysel sonuçlar dördüncü bölümde, sonuç ve öneriler beşinci bölümde anlatılmıştır.

2. İLGİLİ ÇALIŞMALAR (RELATED WORKS)

İmgelerde kimlik doğrulamak için kullanılan yöntemlerin başında kırılgan sayısal damgalama yöntemleri gelmektedir. Bu bölümde bazı kırılgan damgalama yöntemlerine yer verilmiştir. Bu yöntemler şu şekildedir. Walia ve Suneja [10] medical imgeler için Weber kanunu tabanlı kör ve kırılgan bir sayısal damgalama yöntemi önermişlerdir. Bu çalışmada pikseller yoğunluklarına göre sınıflandırılmış ve çalışmada belirlenen şartlara sahip olan piksellere sayısal damga gömülmüştür. Roldan vd. [11] basamaklandırılmış indis modülasyonu, AKD ve ADD kullanan bir imge kimlik doğrulama yöntemi önermişlerdir. Bu yöntem frekans uzayını kullanan bir sayısal damgalama yöntemidir ve imge kurtarma özelliğine sahiptir. Saldırı tespiti yapılan bölgelerdeki imgeyi kurtarmak için çok katmanlı yapay sinir ağları kullanılmıştır. Preda ve Vizireanu [12] AKD uzayını kullanan bir sayısal damgalama yöntemi sunmuşlardır. Sundukları yöntemin temel amacı imgeler için kimlik doğrulamasının yapılmasıdır. Bu yöntemde AKD kullanılmasını en temel amacı yöntemin, JPEG sıkıştırmalara karşı dayanıklı olmasıdır. El'arbi ve Amar [13] AKD ve yapay sinir ağları tabanlı bir imge kimlik doğrulama yöntemi önermişlerdir. AKD sayısal damgalama için, 3 katmanlı geri ve beslemeli yapay sinir ağı ise saldırı durumunda imgeleri onarmak için kullanılmıştır. Lin vd. [14] dağıtık kaynak kod kullanan bir imge kimlik doğrulama yöntemi önermilerdir. Patra vd. [15] imge kimlik doğrulaması yapabilmek için Çin Kalan Teoremi (ÇKT) tabanlı bir sayısal damgalama yöntemi önermişlerdir. Bu yöntem uzaysal alanı kullanan bir yöntemdir ve bu yöntemde

temel olarak yeni bir damga yöntemi önerilmiştir. Bu yöntem TDA tabanlı damgalama yöntemleriyle karşılaştırılmış ve performans olarak başarılı sonuçlar elde edilmiştir. Patra vd. [16] önerdikleri ÇKT tabanlı sayısal damga gömme yöntemini AKD katsayılarına uygulayarak JPEG sıkıştırmaya karşı dayanıklı bir sayısal damgalama yöntemi önermişlerdir. Shao vd. [17] kaotik harita ve ortagonal Fourier-Mellin momentleri tabanlı dayanıklı bir sayısal damgalama tekniği önermişlerdir. Önerilen yöntem çift imgeler üzerinde uygulanmıştır. Bu yöntem içerik kimliklendirme ve doğrulama aşamalarından oluşmaktadır. Bu yöntemde, Fourier-Mellin momentleri özellik çıkarma için kaos ise damgayı karıştırmak için kullanılmıştır. Wang ve Men [18] tersine çevrilebilir kırılgan bir sayısal damgalama yöntemi önermişlerdir. Bu yöntemde imge kimliklendirme için açık anahtar şifreleme ve sayısal damgalama kullanılmıştır ve önerilen yöntem bu yönüyle aktif kimliklendirme yöntemlerini hibrit olarak kullanan bir yöntemdir. Huo vd. [19] blok tabanlı bir kırılgan damgalama önermişlerdir. Önerilen yöntem damga üretme ve damga gömme indisini tespit edebilmek için iki farklı anahtar kullanmaktadır. Wójtowicz ve Ogiela [20] biyometrik imgelerin kimlik doğrulamasını yapabilmek için bir sayısal damgalama yöntemi önermişlerdir ve yöntemlerinde iris ve parmak izi imgelerini kullanmışlardır. Tuncer ve Avcı [21] imgelerde kimlik doğrulama yapabilmek için kaos tabanlı bir kırılgan damgalama yöntemi önermişlerdir. Bu yöntemlere ek olarak sır paylaşımı ve veri gizleme kullanarak imge kimlik doğrulaması yapan birçok yöntem önerilmiştir. Bunlardan birkaçı şu şekildedir. Lin ve Tsai [22] (k,n) eşiksel sır paylaşımı yapısını kullanan bir steganografik imge kimlik doğrulama yöntemi önermişlerdir. Önerilen yöntem sır paylaşımı ve LSB veri gizleme fonksiyonunu kullanmaktadır. Yang vd. [23] Lin ve Tsai'nin [22] yöntemini geliştirip, daha efektif bir imge kimlik doğrulama yöntemi önermişleridir. Chan vd. [24] Lin ve Tsai [22] ve Yang vd.'nın [23] yöntemlerinde gördükleri eksiklikleri gidererek, daha efektif bir sır paylaşımı tabanlı imge kimlik doğrulama yöntemi önermişlerdir. Eslami ve Ahmadabadi [25] literatürdeki sır paylaşım tabanlı imge kimlik doğrulama analiz etmişler ve imge kimlik doğrulama yeteneği daha yüksek bir sır paylaşımı tabanlı imge kimlik doğrulama yöntemi önermişlerdir. Yang vd. [26] parite bitlerini kullanmayan sır paylaşımı tabanlı yüksek görsel kaliteye ve yüksek imge kimlik doğrulama yeteneğine sahip bir metot önermişlerdir. Avcı vd. [27] ADD tabanlı veri gizleme yönteminin başarımını arttırmak için XOR tabanlı sır paylaşımı yöntemini kullanmıştır.

3. ÖNERİLEN İMGE KİMLİKLENDİRME YÖNTEMİ
(THE PROPOSED IMAGE AUTHENTICATION METHOD)

Bu makalede TDA tabanlı yeni bir imge kimliklendirme yöntemi önerilmiştir. Önerilen yöntem aşağıdaki kısımlardan oluşmaktadır.

1. Bloklara bölme,
2. LSB eliminasyon,
3. Özellik çıkarma,
4. Damga üretme,
5. Damga şifreleme,
6. Ön işlem,
7. Damga gömme,
8. Damga çıkarma,
9. Damga deşifreleme,
10. Saldırı tespiti aşamalarından oluşmaktadır.

Önerilen yöntemin ilk aşamasında örtü imge 2 x 2, 4 x 4, 8 x 8 veya b x b boyutundakini bloklara bölünür. Özellik çıkarmak için tüm imgeye LSB eliminasyon işlemi uygulanır. LSB elimine edilmiş imgenin tüm bloklarına TDA uygulanarak U, S ve V matrisleri elde edilir. Özellikler, tekil değerleri barından S matrisinden elde edilir. S matrisinin en büyük değeri blok boyutuna göre basamaklandırılır. Örneğin 512 x 512 boyutundaki gri seviyeli bir imge 4 x 4 boyutunda bloklara bölündüğünde özellik matrisinin boyutu 128 x 128 olacaktır. Basamaklama aşaması alt blokların boyutuna bağımlıdır. Örneğin 4 x 4 boyutundaki bloklar için özellikler [0, 4x4-1] arasında basamaklanır. Basamaklama işlemini gerçekleştirmek için Normalizasyon eşitliği kullanılmaktadır ve bu eşitlik Eş. 1' de verilmiştir.

$$X' = round\left(\frac{X - X_{max}}{X_{max} - X_{min}}\left(b^2 - 1\right)\right) \quad (1)$$

Yukarıdaki eşitlikte X değeri özellik vektörü, X' değeri normalize edilmiş özelliklerin değeri, X_{max} özelliklerin maksimum değeri , X_{min} özelliklerin minimum değeri, b alt blok boyutu örneğin 4 x 4 boyutundaki blok için b 4 değerini alacaktır ve $round$ ise yuvarlama fonksiyonudur. Ardından normalize edilmiş değerler örtü imgeye tekrar ±1 operatörü kullanılarak veri gizlenir. Önerilen imge doğrulama yönteminin blok diyagramı Şekil 1'de verilmiştir. Önerilen yöntemin veri gizleme adımları aşağıda verilmiştir.

Adım 1: Örtü imgenin tüm pikselleri çift veya tek sayı yapılır. Bunun seçimi kullanıcıya aittir. Ön işlem aşamasında ya tüm pikseller çift yâda teke dönüştürülür.

Adım 2: Tüm bloklara LSB eliminasyon uygulanır. LSB eliminasyon eşitliği aşağıdaki Eş. 2' de verilmiştir.

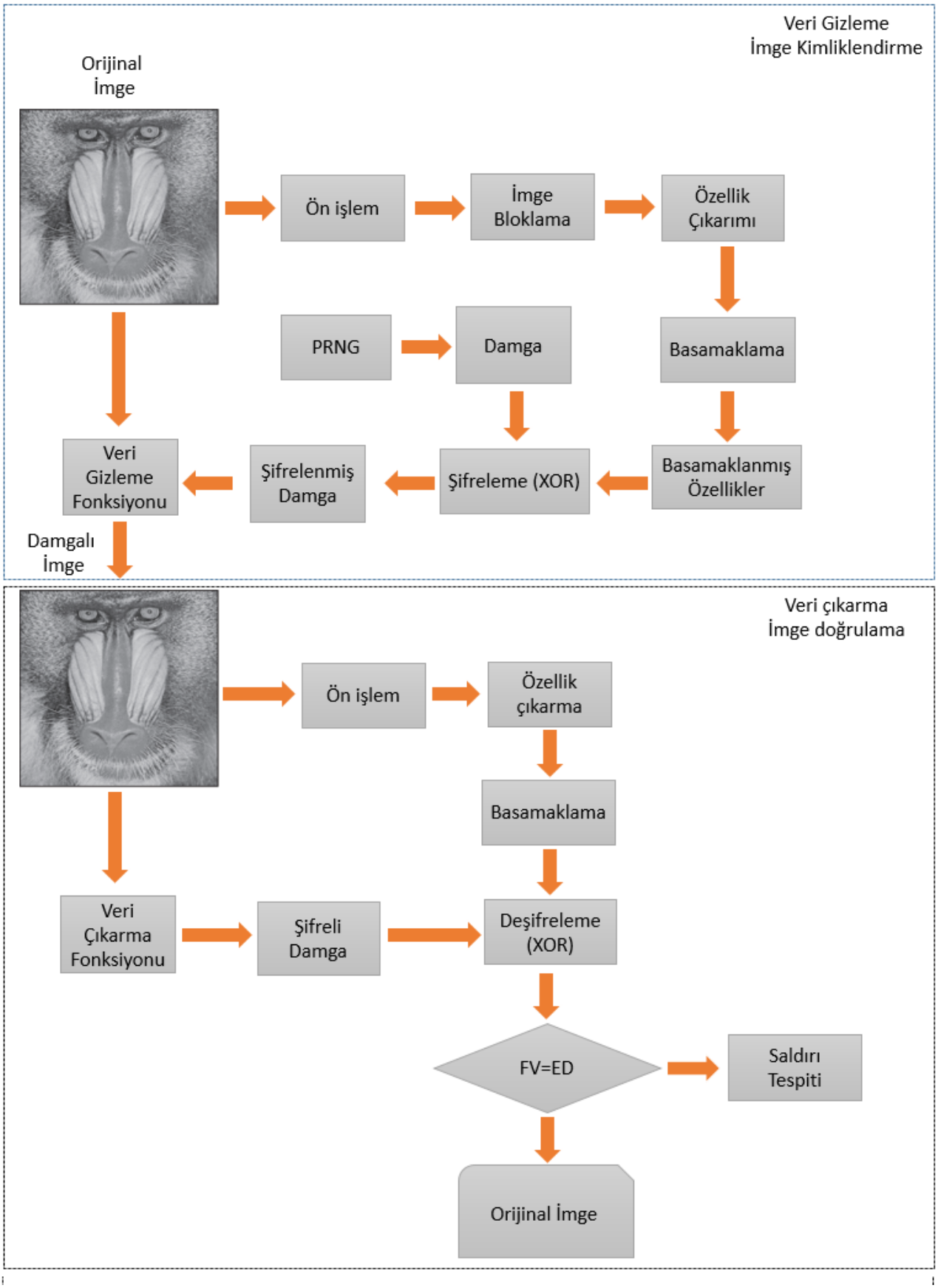
$$X = \left\lfloor \frac{X}{2} \right\rfloor \quad (2)$$

Adım 3: LSB elimine edilmiş blok değerlerine TDA uygulanır ve S matrisinin en büyük değeri özellik olarak kaydedilir. TDA' nın Eş. 3' de verilmiştir.

$$TDA(X) = \begin{bmatrix} u_1 & u_2 & u_3 \\ u_4 & u_5 & u_6 \\ u_7 & u_8 & u_9 \end{bmatrix} \text{x} \begin{bmatrix} s_1 & 0 & 0 \\ 0 & s_2 & 0 \\ 0 & 0 & s_3 \end{bmatrix} \text{x} \begin{bmatrix} v_1 & v_2 & v_3 \\ v_4 & v_5 & v_6 \\ v_7 & v_8 & v_9 \end{bmatrix} \quad (3)$$

Adım 4: W x H boyutundaki imgeden W/b x H/b boyutunda özellik matrisi elde edilir.

Adım 5: Elde edilen özellikler, Eşitlik 1 kullanılarak normalize edilir.



Şekil 1. Önerilen imge kimliklendirme yönteminin blok diyagramı (Block diagram of the proposed image authentication method)

Adım 6: W/b x H/b x $\log_2(b^2)$ boyutunda damga üretilir. Damgayı üretmek için sözde rastgele sayı üreteçleri kullanılmaktadır. Eş. 4, Eş. 5'te lojistik harita ve lineer eşiksel tabanlı sözde rastgele sayı üreteçlerinin denklemleri verilmektedir.

$$rv_{i+1} = h \text{ x } rv_i \text{ x } (1 - rv_i)(mod\ b^2)\ 3.57 \leq r \leq 4$$
$$rv = (0,1)\ ve\ rv \neq \{0.25, 0.5, 0.75\} \quad (4)$$

$$rv_{i+1} = a \text{ x } rv_i + c\ (mod\ b^2) \quad (5)$$

h lojistik harita çarpanı, rv rastgele sayı dizisi, a rastgele sayı çarpanı, c artırım miktarı, i ise indis değeridir ve $i = \{1,2,3,\ldots,\frac{WxH}{b^2}\}$ olarak tanımlanmaktadır.

Adım 7: Çıkarılan özellikler ve rastgele üretilen damga ile şifrelenir. Şifreleme yönteminin eşitliği Eş. 6'da verilmiştir.

$$WM = rv \oplus fv \quad (6)$$

Adım 8: Damga bloktaki indis değerini göstermektedir. Gösterilen indis değeri tek ise çift yapılır çift ise tek hale dönüştürülür.

Bu işlemi gerçekleştirmek için ±1 operatörü kullanılır. İmge kimlik doğrulamayla ilgili örnek aşağıdaki Şekil 2'de verilmiştir. Veri çıkarma ve saldırı tespit aşamasında, damgalı imgeye LSB eliminasyon yöntemi uygulanır. LSB eliminasyon yöntemi uygulanan imge b x b boyutunda bloklara ayrılır ve her bir bloğa TDA uygulanır. Elde edilen S matrisinin en büyük değerleri özellik vektörüne atanır ve elde edilen özellik vektörü basamaklanır. Bu işlemin ardından veri çıkarma işlemi gerçekleştirilir. Bloklara ayırma işlemi tekrardan gerçekleştirilir. Blokta bulunan aykırı pikselin lokasyonu belirlenir. Bu işlemin sonucunda damgalı imgeden şifreli damga çıkarılır. Damgayı deşifrelemek için özellik değerleriyle çıkarılan damga XOR işlemine tabi tutulur ve böylece damga elde edilir. Önerilen yöntemin veri çıkarma algoritması Algoritma 1'de verilmiştir. Saldırı tespit aşamasında kullanıcı tohum değerlerini kullanarak damgayı üretir. Elde edilen damga ve üretilen damga karşılıştırılır. Eğer tüm değerler aynı ise imge kimlik doğrulama işlemi gerçekleştirilmiştir. Eğer farklı değerler varsa blok bazlı saldırı tespiti yapılır. Ayrıca, saldırı tespitinde blokta bulunan tek ve çift piksellerin sayısı da kontrol edilmektedir. Önerilen yöntemin saldırı tespit algoritması Algoritma 2'de verilmiştir.

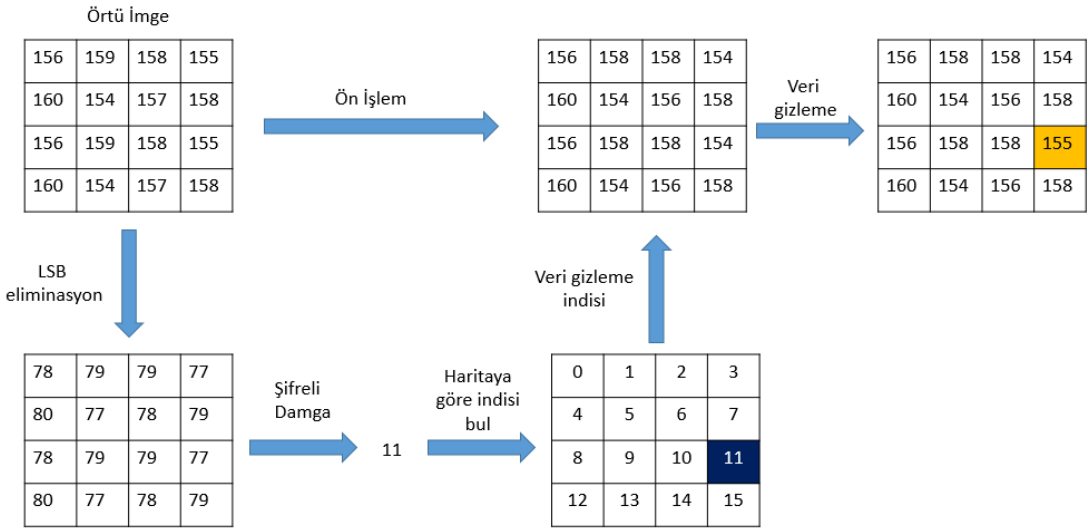
4. DENEYSEL SONUÇLAR (EXPERIMENTAL RESULTS)

Bu bölümde, önerilen yöntem kullanılarak elde edilen deneysel sonuçlar gösterilmektedir. Önerilen yöntemin performansını ölçmek için kapasite, görsel kalite ve imge kimlik doğrulama yeteneği kullanılmıştır. Deneysel sonuçları elde etmek için literatürde sıklıkla kullanılan ve Şekil 3'te gösterilen gri seviyeli test imgeleri kullanılmıştır [28]. *Kapasite:* Bu yöntemde örtüşmeyen bloklar kullanılmıştır ve önerilen yöntemin kapasitesi blok boyutuna bağlıdır. Örneğin 2 x 2 boyutunda bloklar kullanıldığında her bir bloğa 2 bit, 4 x 4 boyutunda bloklar kullanıldığında her bir bloğa 4 bit, 8 x 4 boyutundaki bloklar kullanıldığında her bir bloğa 5 bit ve 8 x 8 boyutundaki boyutunda bloklar kullanıldığında her bir bloğa 6 bit damga gizlenmektedir. Yöntemin kapasitesini Eş. 7 genel olarak ifade etmiştir.

$$C = \frac{log_2(b^2)}{b^2} \quad (7)$$

C, bpp (bit per pixel, bit başına piksel) olarak kapasiteyi ifade etmektedir. Tablo 1'de 512 x 512 boyutundaki imgeler için elde edilen özellik vektörünün uzunluğu verilmektedir.

Görsel Kalite: İmge kimliklendirme yöntemlerinin performansını değerlendirmek için kullanılan en önemli parametrelerden birisi de görsel kalitedir. Görsel kaliteyi sayısal olarak ifade etmek için genellikle ortalama karesel hata (MSE) [29] ve PSNR [30] ölçütleri kullanılmıştır. MSE ve PSNR Eş. 8, Eş. 9'da tanımlanmıştır.



Şekil 2. Önerilen yöntemin veri gizleme örneği (Example of the proposed data hiding)

Algoritma 1. Önerilen yöntemin veri çıkarma algoritması

Girdi: W x H boyutunda stego imge WI, Blok boyutu b.
// ÖZELLİK ÇIKARMA
1: $FI = \left\lfloor \frac{WI}{2} \right\rfloor$ // FI LSB eleminasyon işleminden geçirilmiş imge.
2: row=0;
3: for i= 1 to W step by b do
4: cols=0;
5: for j=1 to H step by b do
6: [U S V]=SVD(FI(i:i+b-1,j:j+b-1));
7: FV(row+1, cols+1)=S(1,1); // Özellik vektörünün elde edilmesi
8: cols++;
9: endfor
10: rows++;
11: endfor
12: // Eşitlik 1 kullanılarak Normalizasyon işlemi gerçekleştirilir.
13: // VERİ ÇIKARMA
14: row=0;
15: for i= 1 to W step by b do
16: cols=0;
17: for j=1 to H step by b do
18: for ii=0 to b-1 do
19: for jj=0 to b-1 do
20: if WI(i+ii,j+jj) (mod 2) ==1 then
21: ED(row+1,cols+1)=ii*b+jj; // ED çıkarılan veri.
22: break;
23. endif
24: endfor
25: endfor
26: cols++;
27: endfor
28: rows++;
29: endfor
30: WM= FV $\oplus$ ED // Damgayı elde etmek için Eşitlik 6 kullanılmıştır.
Çıktı: W/b x H/b boyutundaki damga WM.

Algoritma 2. Önerilen yöntemin saldırı tespit algoritması

Girdi: W x H boyutunda stego imge WI, Güvenilir sözde rastgele sayı üretecinin tohum değerleri, Blok boyutu b.
1: Algoritma 1 kullanılara imgeden çıkarılan damga WM elde edilir.
2: Güvenilir sözde rastgele sayı üretecine tohum değerleri girilerek GWM elde edilir.
3: row=0;
4: for i= 1 to W step by b do
5: cols=0;
6: for j=1 to H step by b do
7: say_tek=0; say_cift=0;
8: for k=0 to b-1 do
9: for l=0 to b-1 do
10: if WI(i+k,j+l) (mod 2)=0 then
11: say_cift=say_cift+1;
12: else
13: say_tek=say_tek+1;
14: endif
15: endfor
16: endfor
17: if say_tek!=1 or say_cift!=b^2-1 or WM(rows+1,cols+1)!= GWM(rows+1,cols+1) then
18: tampered(i:i+b-1,j:j+b-1)=1; // Saldırı tespiti yapıldı
19: else
20: tampered(i:i+b-1,j:j+b-1)=0;
21: endif
22: cols++;
23: endfor
24: rows++;
Çıktı: W x H boyutundaki saldırı tespit haritası, tampered.

Şekil 3. Test imgeleri a) Baboon b) Boat c) Elaine d) House e) Lena f) Peppers g) F16 h)Tiffany i) Barbara
(Test images (a) Baboon (b) Boat (c) Elaine (d) House (e) Lena (f) Peppers (g) F16 (h)Tiffany (i) Barbara)

$$MSE = \frac{1}{WH}\sum_{i=1}^{W}\sum_{j=1}^{H}(OI_{i,j} - WI_{i,j})^2 \quad (8)$$

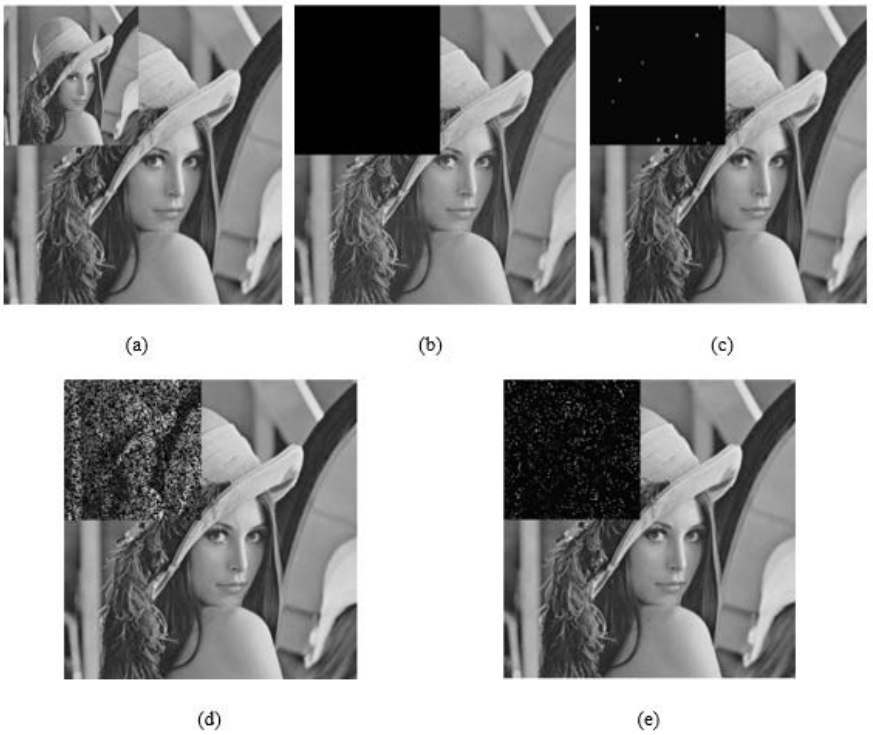
$$PSNR = 10\log_{10}\frac{Max(OI_{i,j}^2)}{MSE} \quad (9)$$

Yukarıdaki eşitliklerde OI orijinal imgeyi, WI damgalı imgeyi, W ve H ise imgenin genişliğini ve yüksekliğini ifade etmektedir. Farklı blok boyutları için elde edilen PSNR değerleri Tablo 2'de gösterilmiştir. Tablo 2'de görüldüğü gibi, farklı blok boyutlarında hemen hemen aynı görsel kalite değerleri elde edilmiştir. Bunun en önemli sebebi ise ön işlem aşamasıdır. Yöntemin görsel kalitesini daha net anlayabilmek için önerilen yöntem literatürdeki diğer yöntemlerle karşılaştırılmıştır ve elde edilen değerler Tablo 3'te gösterilmiştir.

İmge Kimlik Doğrulama Yeteneği: İmge kimliklendirme yeteneği veya saldırı tespiti yeteneği olarak ifade edilen parametre, yöntemin saldırı tespiti yeteneğini ölçmek için kullanılmaktadır. Bu yeteneği ölçmek için imgelere genellikle kolaj saldırıları uygulanmaktadır. Bu performans parametresi görsel ve sayısal olarak ölçülmektedir. İmge kimliklendirme yeteneğini test etmek için Bit hata oranı (BER) kullanılmaktadır [31]. BER' in formülü Eşitlik 10'da verilmiştir.

$$BER = \frac{Toplam\ değişen\ bit\ sayısı}{Toplam\ bit\ sayısı} \quad (10)$$

İmge kimliklendirme yeteneğini ölçmek için imgelere saldırı yapılmıştır. Şekil 4'te saldırı yapılmış imgenin kimlik doğrulama yeteneği diğer yöntemlerle karşılaştırılmıştır. İmgenin küçültülmüş versiyonu, orijinal imgenin sol üst köşesine eklenmiştir. Saldırının diğer kolaj saldırılardan farkı, yapısal olarak orijinal imgeye benzeyen imgenin eklenmesidir [26]. Karşılaştırma için 4 x 4 boyutunda bloklar kullanılmıştır ve sonuçlar Şekil 4'te gösterilmiştir. Şekil 4'te görüldüğü gibi 4 x 4 boyutunda alt bloklar kullanıldığında BER değeri 1 olarak elde edilmiştir.



Şekil 4. Önerilen yöntemin ile literatürde daha önceden önerilmiş yöntemlerin imge kimliklendirme yeteneklerinin karşılaştırılması a) Saldırıya uğramış imge b) önerilen yöntem c) Yang vd.'nın [26] yöntemi d) Yang vd.'nın yöntemi [23] (e) Chang vd.'nın [24] yöntemi (Comprasion of the image authentication ability of the proposed method with previously proposed methods in the literature (a) attacked image (b) Yang et al.'s [26] method (c) Yang et al.'s [23] method (d) Chang et al.'s [24] method)

Şekil 5. Farklı boyutta bloklar kullanılarak elde edilen kimlik doğrulama sonuçları a) 2x2 b) 4x4 c) 8x8 d) 16x16 e) 32x32 (Authentication results obtained using blocks of different sizes (a) 2x2 (b) 4x4 (c) 8x8 (d) 16x16)

Tablo 2. Farklı blok boyutları için elde edilen PSNR (dB) değerleri
(The obtained PSNR values (dB) for variable block sizes)

	2 x 2	4 x 4	8 x 8	16 x 16	32 x 32
Baboon	51,15	51,14	51,15	51,15	51,15
Boat	51,13	51,14	51,15	51,14	51,13
Elaine	51,15	51,15	51,15	51,15	51,16
House	51,14	51,14	51,15	51,13	51,14
Lena	51,15	51,14	51,13	51,14	51,13
Peppers	51,15	51,14	51,15	51,15	51,14
F16	51,14	51,15	51,14	51,13	51,13
Tiffany	51,14	51,14	51,15	51,14	51,14
Barbara	51,13	51,14	51,13	51,12	51,13

Tablo 3. Önerilen Yöntem ile diğer yöntemlerin PSNR değerlerinin karşılaştırılması
(Comparison of PSNR values of the proposed method with other methods)

	Lin vd. [22]	Yang vd. [23]	Chang vd. [24]	Eslami vd. [25]	Wu ve Lin'in 1. Yöntemi [1]	Wu ve Lin'in 2. Yöntemi [1]	Önerilen Yöntem
Lena	43,82	46,11	42,28	47,59	51,10	51,15	51,15
Pepper	43,78	46,14	42,30	47,53	51,10	51,12	51,14
Baboon	43,81	46,14	42,31	47,55	51,10	51,15	51,15
Elaine	43,77	46,12	42,29	47,50	51,11	51,14	51,15
Boat	43,80	46,10	42,22	47,51	51,12	51,12	51,15

BER değerinin 1 elde edilmesi mükemmel kimliklendirme yeteneğinin varlığını ispat etmiştir. Aynı saldırının farklı boyutta bloklar kullanılarak yapılmış hali ve elde edilen BER değerleri Şekil 5'te verilmiştir.

5. SONUÇLAR VE TARTIŞMALAR
(RESULTS AND DISCUSSIONS)

Bu makalede yeni bir imge kimliklendirme yöntemi önerilmiştir. Bu yöntem ön işlem, özellik çıkarımı, basamaklama, damga üretme, damga gömme, damga çıkarma, veri doğrulama ve saldırı tespiti basamaklarıdır. Ön işlem aşamasında tüm piksel değerleri tek veya çift hale getirilir. Özellik çıkarımı aşamasında ise LSB eliminasyon işlemi ve tekil değer ayrışımı yöntemleri kullanılmaktadır. Elde edilen özellikler blok boyutuna göre normalize edilir. Damga üretmek için güvenilir sözde rastgele üreteçleri kullanılmaktadır. Damga ile çıkarılan özellikler XOR işlemine tabi tutularak damga şifrelenir ve damga ile imge ilişkilendirilir. Veri gizleme işleminde ise ±1 operatörü kullanılarak veri gizlenir. Veri çıkarma işleminde ise bloktaki tek veya çift olan pikselin konumu belirlenir ve veri çıkarılır. Saldırı tespiti aşamasında ise, damgalı imgeden özellik çıkarılır, çıkarılan özellik ile damga XOR işlemine tabi tutulur. Rastgele sayı üretecinin tohum değerleri kullanılarak orijinal damga üretilir. Üretilen damga ve elde edilen damga karşılaştırılarak saldırı tespiti yapılır. Buna ek olarak, bloktaki tek ve çift piksellerin sayısı göz önüne alınarak da saldırı tespiti yapılmaktadır. Önerilen yöntem görsel kalite, kapasite ve kimlik doğrulama yeteneği parametreleri kullanılarak test edilmiştir.

Blok boyutu değişmesinin görsel kaliteyi değiştirmediği görülmüştür. PSNR değeri 51 dB' den yüksek elde edilmiştir. Blok boyutuna göre elde edilen özellik vektörlerinin uzunlukları makalede verilmiştir ve önerilen yöntemin saldırı tespit yeteneğinin yüksek olduğu gözlemlenmiştir. İlerleyen çalışmalarda bu yöntem ve algısal imge özet fonksiyonları kullanılarak imge kimlik doğrulama, saldırı tepiti ve imgeyi yeniden elde etmeyle ilgili çalışmalar yapılabileceği gösterilmiştir.

KAYNAKLAR **(REFERENCES)**

1. Atici 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.
2. Tuncer T., Avcı D., Avcı E., A new data hiding algorithm based on minesweeper game for binary images, Journal of the Faculty of Engineering and Architecture of Gazi University, 31 (4), 951-959, 2016.
3. Wu W.-C., Lin Z.-W., SVD-based self-embedding image authentication scheme using quick response code features, J. Vis. Commun. Image R. 38, 18–28, 2016.
4. 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.
5. Hu Y.-C., Lo C.-C., Chen W.-L., Probability-based reversible image authentication scheme for image demosaicking, Future Generation Computer Systems 62, 92–103, 2016.
6. Christian R., Jean-Luc D., A survey of watermarking algorithms for image authentication, EURASIP J. Appl. Signal Process., 6, 613–621, 2002.
7. Lin Y.K., A data hiding scheme based upon DCT coefficient modification, Computer Standards & Interfaces, 36 (5), 855-862, 2014.
8. Liu Y., Zhao J., A new video watermarking algorithm based on 1D DFT and Radon transform, Signal Processing, 90 (2), 626-639, February 2010.

9. Lee S. H., DWT based coding DNA watermarking for DNA copyright protection, Information Sciences, 273, 263-286, 2014.

10. Walia E., Suneja A., Fragile and blind watermarking technique based on Weber's law for medical image authentication, IET Computer Vision, 7 (1), 9-19., 2013.

11. Roldan L. R., Hernández M. C., Chao J., Miyatake M. N., Meana H. P., Watermarking-based Color Image Authentication with Detection and Recovery Capability, IEEE Latin America Transactions, 14 (2), 2016.

12. Preda R.O., Vizireanu D.N., Watermarking-based image authentication robust to JPEG compression, Electronics Letters, 51 (23), 1873-1875, 2015.

13. El'arbi M., Amar C. B., Image authentication algorithm with recovery capabilities based on neural networks in the DCT domain, IET Image Processing, 8 (11), 619-626, 2014.

14. Lin Y.-C., Varadoyan D., Girod B., Image Authentication Using Distributed Source Coding, IEEE Transactions on Image Processing, 21 (1), 273-283, 2012.

15. Patra J. C., Kathik A., Bornand C., A novel CRT-based watermarking technique for authentication of multimedia contents, Digital Signal Processing, 20, 442-453, 2010.

16. Patra J. C., Phua J. E., Bornand C., A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression, Digital Signal Processing, 20, 1597-1611, 2010.

17. Shao Z., Shang Y., Zhang Y., Liu X., Guo, G., Robust watermarking using orthogonal Fourier–Mellin moments and chaotic map for double images, Signal Processing, 120, 522–531, 2016.

18. Wang N., Men C., Reversible fragile watermarking for 2-D vector map authentication with localization, Computer-Aided Design 44, 320–330, 2012.

19. Huo Y., He H., Chen F., Alterable-capacity fragile watermarking scheme with restoration capability, Optics Communications 285, 1759–1766, 2012.

20. Wójtowicz W., Ogiela M. R., Digital images authentication scheme based on bimodal biometric watermarking in an independent domain, J. Vis. Commun. Image R. 38, 1–10, 2016.

21. Tuncer T., Avcı E., Block based Fragile Watermarking Algorithm for Image Authentication and Tamper Detection, 9th International Conference on Information Security and Cryptology, 5-10, 25-26 Nov. 2016.

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

23. 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, 1070-1076, 2007.

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

25. Eslami Z., Ahmadabadi J.Z., Secret image sharing with authentication-chaining and dynamic embedding, Journal of Systems and Software, 84,803-809, 2011.

26. Yang C.N., Ouyang J.F., Harn L., Steganography and authentication in image sharing without parity bits, Optics Communications, 285, 1725-1735, 2012.

27. 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.

28. University of Southern California, Signal and Image Processing Institute, SIPI Image Dataset, http:// http://sipi.usc.edu/database/ (15.03.2017)

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

30. Abd-Eldayem M.M., A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine, Egyptian Informatics Journal, 14,1–13, 2013.

31. Guo J., Zheng P., Huang J., Secure watermarking scheme against watermark attacks in the encrypted domain, Journal of Visual Communication and Image Representation, 30, 125-135, July 2015.