Fırat Üniv. Müh. Bil. Dergisi
30(1), 151-159, 2018

Science and Eng. J of Fırat Univ.
30(1), 151-159, 2018

Goldbach Sanısı Tabanlı Yeni Bir Matematiksel Sayısal İmge Damgalama Yöntemi

Türker TUNCER
Fırat Üniversitesi Teknoloji Fakültesi Adli Bilişim Mühendisliği Bölümü, Elazığ, Türkiye
turkertuncer@firat.edu.tr

(Geliş/Received: 15.08.2017; Kabul/Accepted: 08.01.2018)

Özet

Bu makalede Goldbach sanısı kullanılarak yeni bir sayısal damgalama yöntemi önerilmiştir. Goldbach sanısına göre 2'den büyük tüm çift sayılar iki asal sayının toplamından oluşmaktadır. Bu makalede elde edilen asal sayıların oranları kullanılarak sayısal damgalama işlemi gerçekleştirilmiştir. Bu yöntemde imge bloklara ayrılmış ve veri gizlenecek piksel rastgele sayı üreteci kullanılarak seçilmiştir. Önerilen yöntemi test etmek için görsel kalite, dayanıklılık ve çalışma zamanı kullanılmıştır. Bu yöntem Çin Kalan Teoremi tabanlı sayısal damgalama algoritmalarıyla karşılaştırılmıştır. Deneysel sonuçlar, goldbach sanısı tabanlı sayısal damgalama yöntemini doküman, video ve imge içeriğini korumak için kullanılacak pratik ve başarılı bir yöntem olduğunu göstermiştir.

Anahtar Kelimeler: Goldbach Sanısı; Sayısal Damgalama; Telif Hakkı Koruma; Bilgi Güvenliği.

A New Mathematical Digital Image Watermarking Method Based on Goldbach Conjecture

Abstract

In this paper, a new digital watermarking method is proposed by using Goldbach conjecture. All even numbers which are greater than 2 are consist of sum of two primes numbers according to Golbach conjecture. We used rate of the used prime numbers to implement digital watermarking in this paper. In this method, image is divided into blocks and the proposed method is selected embeddable pixel by using pseudo random number generator. Visual quality, robustness and execution time are used to evaluate the proposed method. The proposed method is compared to Chinese remainder theorem based digital watermarking methods. The experimental results showed that, Goldbach based digital watermarking method can be used to protect document, video and images contents. This method is successful and practically.

Keywords: Collatz Conjecture; Digital Watermarking; Copyright Protection; Information Security.

1. Giriş

Bilgi teknolojileri ve multimedya teknolojilerinin gelişmesiyle birlikte imge paylaşımı çok kolay ve hızlı bir hale gelmiştir ancak aynı teknoloji imgelerin bilgi güvenliğinin sağlanmasını zorunlu bir hale getirmiştir [1-3]. Günümüzde çok gelişmiş multimedya düzenleme araçları bulunmaktadır. Bu araçlar kullanılarak imgeler bireylerin fark edemeyeceği şekilde değiştirilebilmektedir. Bu durumda imgelerin sahipliği ispat edilememekte ve çok büyük maddi ve manevi kayıplar yaşanmaktadır [1-4] İmgelerin sahipliğini doğrulayabilmek için kriptolojik özet fonksiyonları ve sayısal damgalama teknikleri kullanılmaktadır. Sayısal damgalama tekniklerinin temel amacı imgede minimum bozulma oluşturarak sahiplik doğrulaması yapabilmektir. İmgelerin sahipliğini belirlemek için genellikle görünmez damgalama teknikleri kullanılmaktadır. Bu teknikler uzaysal alanı kullanabildikleri gibi, sayısal dönüşümleri de kullanabilmektedirler. Sayısal damgalamada genellikle, Ayrık Kosinüs Dönüşümü (AKD), Ayrık Dalgacık Dönüşümü (ADD) ve Tekil Değer Ayrışımı (TDA) gibi dönüşümler kullanılmaktadır [5-9]. Sayısal damgalama yöntemini oluşturan bileşenler aşağıda verilmiştir.

- Örtü imge
- Damga
- Anahtar
- Veri gömme fonksiyonu

- Damgalanmış imge
- Veri çıkarma fonksiyonu

Örtü imge, damganın gömüleceği imgedir. Damga, telif hakkı koruması otomatik üretilen veya kullanıcı tarafından oluşturulan gizli mesajdır. Anahtar kullanımı kullanıcının tercihine bırakılmıştır. Genellikle anahtarlar güvenliği sağlamak için kullanılmaktadır. Anahtar, damganın gömüleceği indisleri belirlemekle beraber damgayı veya örtü nesnesini şifrelemede de kullanılabilirler. Veri gömme fonksiyonu kullanılarak damga örtü nesnesinin içerisine gömülür ve böylece damgalanmış imge elde edilir. Veri çıkarma fonksiyonu kullanılarak damgalanmış imgeden damga elde edilir. Literatürde yer alan bazı sayısal damgalama yöntemleri aşağıda verilmiştir [1-9].

Mir [10] web içeriklerinin telif hakkını korumak için sayısal damgalama tabanlı bir yöntem önermiştir. Önerdiği yöntemde HTML kodlarını örtü nesnesi olarak kullanmaktadır. Damga semantik ve sentetik kurallar kullanılarak HTML kodlarına şifrelenmiş bir şekilde gömülmekte ve böylece telif hakkını koruma amaçlanmaktadır. Zheng vd. [11] TDA ve en küçük kareler destek vektör makinesi kullanarak hem sayısal damga gömme hem de sayısal damgayı tespit etmek için bir algoritma önermişlerdir. Bu yöntem TDA alt bloklara uygulanarak katsayılar elde edilir. Elde edilen katsayılara damga gömülür. İmgenin içerisinde damganın olup olmadığını tespit edebilmek için en küçük kareler destek vektör makinesi kullanılmıştır. Hu ve Hsu [12] ADD, TDA ve AKS kullanarak dayanıklı bir sayısal damgalama yöntemi önermiştir. Damga gömme aşamasında basamaklandırılmış indis modülasyonu ve Arnold dönüşümü kullanılmıştır. Abdallah vd. [13] TDA tabanlı homomorfik imge damgalama yöntemi önermiştir. Xiang-yang vd. [14] geometrik ataklardan korunmak için yerel kutupsal harmonik dönüşüm tabanlı bir sayısal damgalama yöntemi önermiştir. Önerilen yöntemin SURF yönteminden daha dayanıklı olduğunu göstermişlerdir. Damga, gizli anahtar kullanılarak üretilmiştir. Khalili [15] AKD ve Arnold kaotik dönüşümünü tabanlı bir sayısal damgalama yöntemi geliştirmiştir. Bu yöntemde JPEG-YCbCr kanalları kullanılarak sayısal damgalama yöntemi dayanıklı hale getirilmiştir. Mehto ve Mehra [16] AKD ve ADD tabanlı uyarlanabilir kayıpsız bir sayısal damgalama yöntemi önermişlerdir. Bu yöntem medikal imgelerde uygulanmıştır. Botta vd. [17] renkli imgeler için kırılgan bir sayısal damgalama çerçevesi oluşturmuştur. Bu çerçevede kayıpsız dönüşümler, genetik algoritma, sendrom kodlama gibi yöntemler kullanılmıştır. Nguyen vd. [18] imgelerin kimlik doğrulamasını gerçekleştirmek için ADD tabanlı bir kırılgan damgalama yöntemi sunmuşlardır. Bu yöntemde gizli anahtar kullanılarak damga üretilmiş belirlenen kurallara göre ADD katsayılarına gizlenmiştir. Teorik olarak mükemmel görsel kalite sağlasa da pratik uygulanması zordur çünkü piksel değerleri ondalıklı sayılardan oluşmaktadır. Shih ve Zhong [19] medikal imgeler için yüksek kapasiteli bir sayısal damgalama yöntemi sunmuşlardır. Önerilen yöntemde medikal imgenin teşhisle ilgili alanlar ve ilgili olmayan alanları kullanılmıştır. Patra vd. [20] çin kalan teoremi tabanlı bir sayısal damgalama yöntemi geliştirmiştir. Yazarlar bu yöntemin imge kimlik doğrulama yöntemi olarak kullanılabileceğini söylemiştir. Yöntem kırılgan bir yapıya sahiptir ancak kimlik doğrulama yöntemi olarak pratikte kullanılamayacağı görülmektedir. Patra vd. [21] çin kalan teoremi tabanlı sayısal damgalama yönteminin JPEG sıkıştırmalara karşı dayanıklı olabilmesi için AKD katsayılarına damga gömmüştür. Thlasidharan ve Nair [22] QR kod tabanlı kör bir sayısal damgalama yöntemi sunmuştur. Bu yöntemde saldırı tespiti yapmak için özellik çıkarma ve QR oluşturma aşamaları kullanılmıştır. Gizliliği sağlamak için Arnold dönüşümü kullanılmıştır. QR kod ADD katsayılarına gömülmüştür.

Bu makalede Goldbach sanısı tabanlı yeni bir imge damgalama yöntemi önerilmiştir. Önerilen yöntemin karakteristiği aşağıdaki gibi verilmiştir.

- Goldbach sanısına göre tüm çift sayılar en az iki asal sayının toplamından oluşmaktadır ancak bu sanı tüm doğal sayılar için ispatlanamamaktadır. Bu makalede, piksel değerleri 8 bitten oluşan imgeler kullanılmıştır. Bu piksellerin alabileceği değerler 0 ile 255 arasında değişmektedir. Bu sonlu uzayda Goldbach sanısı ispatlanmış bir sanıdır. Tek değerler için -1 operatörü kullanılarak, tek değerler çifte dönüştürülmüştür. Bu sayede Goldbach sanısı 8 bitlik imgede uygulanabilir hale

dönüştürülmüştür. Bu makale, başka matematiksel kullanılarak damgalama yöntemlerinin elde edilebileceğini göstermektedir ve bu makalede literatürde ilk kez Goldbach sanısı tabanlı bir imge damgalama yöntemi önerilmiştir.

- Goldbach sanısı sonucu elde edilen asal sayıların oranı elde edilerek piksel değerleri normalize edilir. Normalize edilmiş değerler bir sabitle çarpılarak oranın tam kısmı elde edilir ve mod operatörü kullanılarak damga gizleme ve damga çıkarma işlemi gerçekleştirilmiştir. Sabitle çarpma ve mod operatörü kullanılması sayesinde eşit (uniform) dağılım elde edilmiştir. Bu durumda Önerilen yöntemin güvenilir damgalama için uygun olduğunu göstermektedir.
  - Önerilen yöntem blok tabanlı bir yöntemdir. İmge öncelikle bloklara bölünür. Her bir blokta sadece bir piksele damga gömülmektedir. Damga gömülecek pikseli seçmek rastgele sayı üreteçler kullanılmaktadır. Rastgele sayı üreteçleri sayesinde önerilen damgalama yönteminin güvenilirliği sağlanmaktadır.
  - Önerilen yöntem yüksek görsel kalitede ve yüksek kapasitede damgalama imkânı sağlamaktadır. Ayrıca deneysel sonuçlar önerilen yöntemin fonksiyonel programlama sayesinde, hızlı bir algoritma olduğunu göstermektedir. Önerilen yöntem kırılgan bir yöntemdir ve bu yöntem kullanılarak imge damgalama yöntemlerinin geliştirilebileceği gösterilmiştir.

Bu makalenin organizasyonu şu şekildedir. Makalenin 2. Bölümünde Goldbach Sanısı, 3. Bölümde önerilen sayısal damgalama yöntemi, 4. bölümde deneysel sonuçlar ve 5. bölümde sonuç ve önerilerden bahsedilmiştir.

2. Goldbach Sanısı

Bu sanı 1742 yılında Christian Goldbach'ın Leonhard Euler'e yazdığı mektupla ortaya çıkmıştır. Goldbach sanısına göre 2'den büyük tüm çift sayılar 2 asal sayının toplamından oluşmaktadır. Bu sanı günümüzde hala ispatlanamamıştır. Goldbach sanısı kolay anlaşılan ancak 274 yıldır çözülemeyen milenyum problemleri arasında yerini almaktadır [23].

3. Goldbach Sanısı Tabanlı İmge Damgalama Yöntemi

Bu çalışmada, imgelere veri gizlemek için Goldbach sanısı kullanılmıştır. Goldbach sanısına göre 2'den büyük tüm doğal sayılar 2 asal sayının toplamı şeklinde ifade edilebilmektedir. Goldbach sanısı sadece çift sayılar için önerilmiştir. Bu makalede Goldbach sanısının tüm sayılarda kullanılabilmesi için yeni bir yöntem önerilmiştir. Önerilen yöntemde elde edilen asal sayıların oranı alınmaktadır ve damga gömme işlemi için bu oranlar kullanılmaktadır. Goldbach sanısına göre, bir çift sayı birden fazla asal çiftinden oluşabilmektedir. Goldbach sanısını kullanarak çift sayıyı oluşturan tüm asal sayıları bulmak algoritmanın karmaşıklığını arttıracağı için önerilen yöntemde sayıyı oluşturan ilk asal sayı çifti kullanılmıştır. Bu işlemi gerçekleştirmek için 2 adet algoritma çalışmaktadır. İlk algoritma asal sayıyı bulan algoritma ikincisi ise asal sayıların oranlarını bulan algoritmadır. Hassasiyeti arttırmak için elde edilen oranların virgülden sonraki iki hanesi kullanılarak sayısal damgalama işlemi gerçekleştirilmektedir. Asal sayıların oranlarını bulan fonksiyonun sözde kodu Algoritma 1' de verilmiştir.

Algoritma 1. Goldbach sayılarının oranlarını bulan algoritmanın sözde kodu.

Giriş: Piksel değeri p.
Çıkış: Oran değeri

```
1: if p<8 then
2:     r=0.5;
3:     return r;
4: else
5:    if p (mod 2)=1 then
6:        p=p-1;
7:        endif
8:       for k=2 to p-2 do
9:           if asal(k)=true and asal(p-k)=true then
10:              r=k/(p-k);
11:              return r;
12:              break;
13:          endif
14:      endfor
15: endif
```

Algoritma 1'de verilen r değeri kullanılarak sayısal damgalama işlemi gerçekleştirilecektir. Bu algoritma Goldbach oranlarını verdiği için GO adında bir fonksiyon olarak tanımlanmaktadır. Önerilen damga gömme yönteminin algoritması aşağıdaki gibidir.

Adım 1: Örtü imge m x n boyutunda örtüşmeyen alt bloklara ayrılır. Blok sayısı veya veri gizleme kapasitesi Eşitlik 1'de verilmiştir.

$$BS = \left\lfloor \frac{W}{m} \right\rfloor \left\lfloor \frac{H}{n} \right\rfloor \quad (1)$$

Eşitlik 1' de W imgenin genişliği, H imgenin uzunluğunu temsil etmektedir.

Adım 2: Rastgele sayı üreteci kullanılarak P adındaki piksel seçilir.

Adım 3: Goldbach oranını elde etmek için GO fonksiyonu kullanılır.

$$r = GO(P) \quad (2)$$

Eşitlik 2'de kullanılan r değişkeni Golbach oranını ifade etmektedir.

Adım 4: r değerinin virgülden sonraki iki basamağını elde etmek için T değeri Eşitlik 3 kullanılarak hesaplanır.

$$T = \lfloor 100.r \rfloor \quad (3)$$

Adım 5: Veri gizleme değeri E' yi elde etmek için Eşitlik 4 kullanılır.

$$E = T \ (mod\ 2) \quad (4)$$

Adım 6: Eğer damga değeri D=0 ve E=1 ise P değeri değiştirme prosedürü kullanılarak P değeri değiştirilir.

Adım 7: Eğer damga değeri D=1 ve E=0 ise P değeri değiştirme prosedürü kullanılarak P değeri değiştirilir.

Adım 8: Damga boyutunca Adım 2-7 tekrarlanır.

Adım 6 ve 7'de kullanılan değiştirme prosedürünün sözde kodu Algoritma 2'de verilmiştir.

Algoritma 2. Değiştirme prosedürünün sözde kodu.

Giriş: Piksel değeri P, Damga değeri D, Veri gizleme değeri E.
Çıkış: Değiştirilmiş piksel değeri P'

```
1: if D=0 and E=1 then
2:     for i=1 to 255 do
3:         if P+k<256 then
4:             P=P+k;
5:             if GO(P)=0 then
6:                 P'=P;
7:                 break;
8:             endif
9:         elseif P-k≥0 then
10:            P=P-k;
11:            if GO(P)=0 then
12:                P'=P;
13:                break;
14:            endif
15:        endif
16:    endfor
17: elseif D=1 and E=0 then
18:    for i=1 to 255 do
19:        if P+k<256 then
20:            P=P+k;
21:            if GO(P)=1 then
22:                P'=P;
23:                break;
24:            endif
25:        elseif P-k≥0 then
26:            P=P-k;
27:            if GO(P)=1 then
28:                P'=P;
29:                break;
30:            endif
31:        endif
32:    endfor
33: endif
```

Önerilen sayısal damgalama yönteminin veri çıkarma adımları aşağıdaki gibi verilmiştir.

Adım 1: İmge m x n boyutundaki bloklara ayrılır.

Adım 2: Tohum değerleri kullanılarak rastgele sayı dizisi oluşturulur.

Adım 3: Rastgele sayı dizisi kullanılarak P' değeri elde edilir.

Adım 4: Eşitlik 5 kullanılarak damga verisi D elde edilir.

$$D = \lfloor GO(P') \text{ x } 100 \rfloor \ (mod\ 2) \quad (5)$$

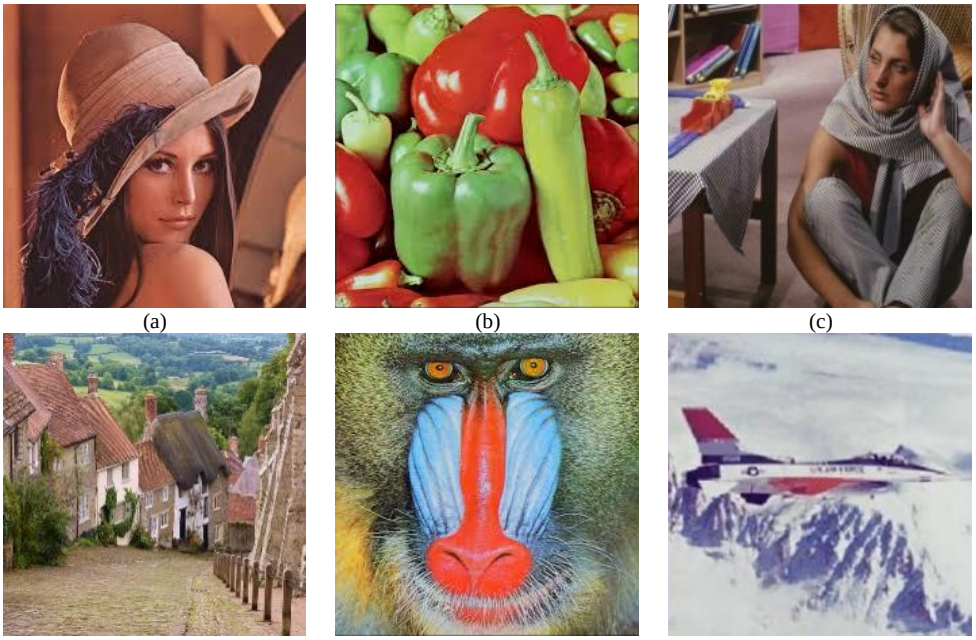
Adım 5: Damga boyutunca adım 3-4 tekrarlanır.

Önerilen sayısal damgalama algoritmasının kapasitesini arttırmak için Eşitlik 4, 5 ve değiştirme prosedüründe kullanılan mod değerleri değiştirilebilmektedir. Örneğin Örneğin 2 bit veri gizlenecek ise mod 4, 3 bit veri gizlenecek ise mod 8 değeri kullanılabilmektedir.

4. Deneysel Sonuçlar

Önerilen sayısal damgalama yöntemini test etmek için; Kapasite, Görsel Kalite, Dayanıklılık, Çalışma zamanı, Güvenilirlik değerlendirme ölçümleri kullanılarak önerilen yöntemin performansı test edilmiştir.

Bu parametreleri sayısal olarak ifade edebilmek için Tepe Sinyal Gürültü Oranı (TSGO, PSNR), bit, Bit Hata Oranı (BHO, BER) ve milisaniye ölçüm birimleri kullanılmıştır. Bu sayısal değerleri elde edebilmek için literatürde sıklıkla kullanılan 512 x 512 boyutundaki renkli test imgeleri kullanılmıştır [25].



(a) (b) (c)

(d) (e) (f)

Şekil 1. Test imgeleri [25]. (a) Lena (b) Peppers (c) Barbara (d) Goldhill (e) Baboon (f) Jet

Kapasite: Önerilen yöntem, kapasite açısından esnek bir yöntemdir. Bu makalede 8 x 8 bloklara 1 bitlik veri gizlenmiştir. Kullanılan imgeler 512 x 512 x 3 boyutunda olduğu için veri gizleme kapasitesi $\frac{512}{8}.\frac{512}{8}.3$ bit elde edilir. Önerilen yöntemin kapasitesi genel olarak Eşitlik 6'da verilmiştir.

$$Kapasite = \left\lfloor \frac{M}{w} \right\rfloor . \left\lfloor \frac{N}{h} \right\rfloor . katman.bit \qquad (6)$$

Eşitlik 5'te M örtü imgesinin satır sayısı, N örtü imgesinin sütun sayısı, w kullanılan alt bloğun satır sayısı, h kullanılan alt bloğun sütun sayısı ve bit değer seçilen piksele kaç bit veri gizlendiğini göstermektedir. Katman değişkeni gri seviyeli imgeler 1, RGB imgeler için 3 değerini almaktadır.

Görsel Kalite: Önerilen yöntemin performansını test edebilmek için kullanılan en önemli başarım parametrelerinde birisi de görsel kalitedir. Görsel kaliteyi test edebilmek için ise MSE (mean square error, ortalama karesel hata) ve PSNR ölçütleri kullanılmaktadır. Algoritmanın başarımını test etmek için rastgele üretilmiş veriler kullanılmıştır. MSE ve PSNR' nin denklemleri formül 7 ve 8'de verilmiştir.

$$MSE = \sum_{i=1}^{M}\sum_{j=1}^{N}\left(CI_{i,j} - WI_{i,j}\right)^2 / (M\ x\ N) \qquad (7)$$

$$PSNR = 10\ x\ log_{10}(1/MSE) \qquad (8)$$

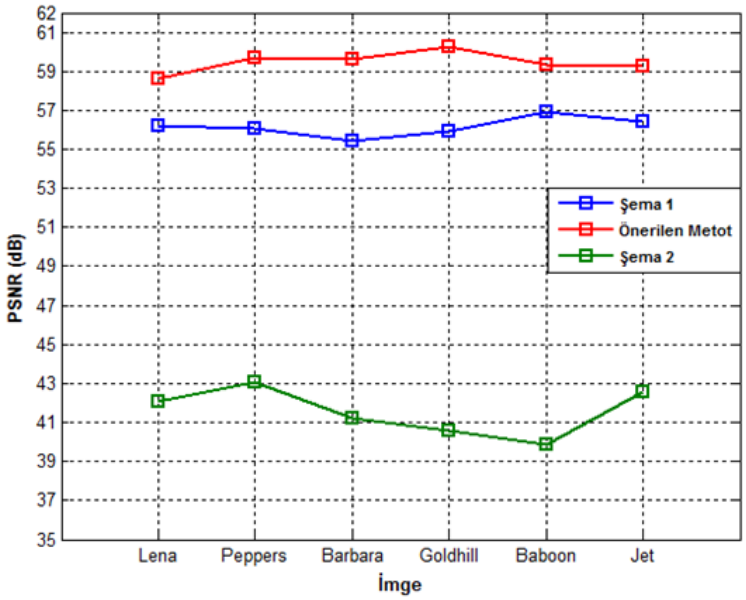
Eşitlik 3'te kullanılan *CI* örtü imgesi, *WI* damgalı imgedir.

Aşağıdaki tabloda blok boyutuna göre elde edilen PSNR değerleri verilmiştir. Bu karşılaştırmada seçilen piksele bir bit veri gizlenmiştir.

Tablo 1. Blok boyutlarına göre elde edilen PSNR değerleri.

İmge	2 x 2	3 x 3	4 x 4	5 x 5	6 x 6	7 x 7	8 x 8
Lena	45.78	49.30	51.82	53.84	55.09	57.09	58.63
Peppers	47.36	50.84	53.31	55.46	57.03	58.25	59.69
Barbara	46.63	50.62	53.03	55.13	56.48	57.80	59.62
Goldhill	48.02	50.89	53.42	55.69	57.03	58.61	60.24
Baboon	47.38	50.01	52.78	54.64	56.17	57.45	59.35
Jet	46.41	50.18	52.34	55.01	56.19	58.21	59.24

Önerilen yöntem ile literatürde daha önceden önerilmiş Şema 1[20] ve Şema 2[21]'nin PSNR değerleri karşılaştırılmıştır. Karşılaştırma sonuçları Şekil 2'de verilmiştir. Bu karşılaştırma için 8 x 8 boyutundaki bloklar kullanılmıştır.



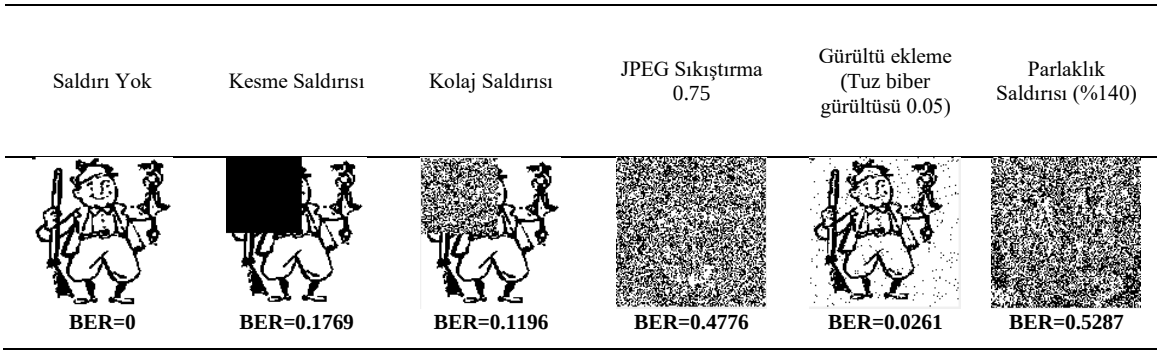
Şekil 2. PSNR değerlerinin karşılaştırılması.

Dayanıklılık: Önerilen yöntemin dayanıklılığını ölçmek için damgalı imgeye çeşitli saldırılar yapılmıştır. Önerilen yöntem uzaysal alanı kullandığı için imgelerde kimlik doğrulama amacıyla kullanılabilmektedir. Kesme, kolaj, gürültü ekleme, JPEG sıkıştırma ve parlaklık atakları gibi ataklar uygulanarak yöntemin dayanıklılığı test edilmiştir. Dayanıklılık testi yapılırken 8 x 8 boyutunda bloklar kullanılarak damga gömülmüştür. 512 x 512 boyutundaki imgeye 64 x 64 boyutundaki damga gömülmüştür. Damgadaki değişimi ölçmek için BER kullanılmıştır. BER' in eşitliği Eşitlik 9'da verilmiştir.

$$BER = \sum_{i=1}^{W}\sum_{j=1}^{H}\frac{D_{i,j} \oplus D'_{i,j}}{W * H} \qquad (9)$$

Yukarıdaki denklemde D orijinal damga, D' saldırıdan sonra elde edilen damga, W damganın genişliği ve H damganın yüksekliğini temsil etmektedir.

Saldırı yapılmış imgeden elde edilen damgalar ve BER değerleri Şekil 3'te verilmiştir.



Şekil 3. Saldırı yapılmış Baboon imgesinden damganın çıkarılması ve elde edilen BER değerleri.

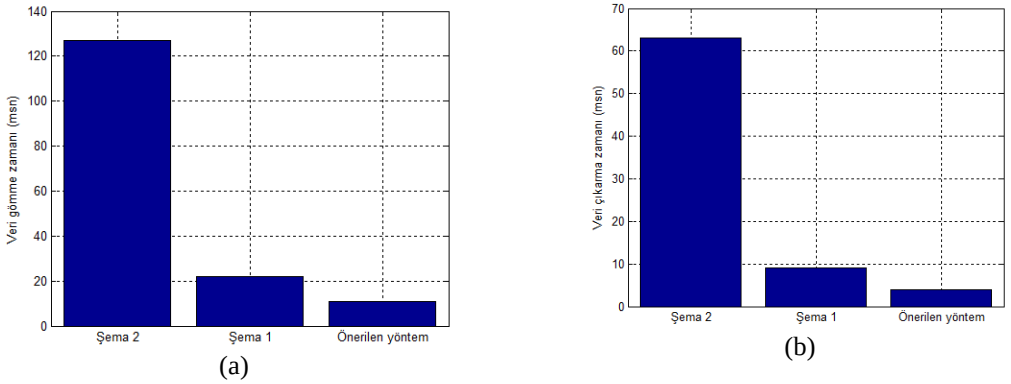
Çalışma Zamanı: Önerilen yöntemin çalışma zamanını hesaplamak için farklı boyutlarda at bloklar kullanılmıştır. Testler Intel Pentium i5-4570 3.20 GHz işlemci, 8 GB RAM'e sahip bir masaüstü bilgisayarda MATLAB 2015a yazılımı kullanılarak gerçekleştirilmiştir. Örtü nesnesi olarak kullanılan imgeler 256 x 256 boyutunda gri seviyeli imgelerdir. Bu imgelerin kullanılmasının temel sebebi, literatürdeki diğer yöntemlerle karşılaştırmanın yapılabilmesidir. [20] ve [21]' de sunulan yöntemlerin çalışma zamanını ölçmek için 256 x 256 boyutunda gri seviyeli imgeler kullanılmıştır. Bu sonuçları elde etmek için [25]' te verilen veritabanındaki gri seviyeli imgeler 256 x 256 olarak boyutlandırılmıştır ve elde edilen ortalama damga gömme ve damga çıkarma süreleri Tablo 2'de gösterilmiştir.

Tablo 2. Blok boyutlarına göre elde çalışma süreleri (ms)

2 x 2		3 x 3		4 x 4		5 x 5		6 x 6		7 x 7		8 x 8	
GZ	ÇZ	GZ	ÇZ	GZ	ÇZ	GZ	ÇZ	GZ	ÇZ	GZ	ÇZ	GZ	ÇZ
147	54	66	24	36	15	28	9	19	6	14	5	11	4

Tablo 2'de GZ veri gizleme zamanını, ÇZ veri çıkarma zamanını temsil etmektedir. Şekil 4'de önerilen yöntemin literatürdeki diğer yöntemlerle karşılaştırılması verilmiştir.

Bu karşılaştırmada 8 x 8 boyutundaki örtüşmeyen bloklar kullanılarak 256 x 256 boyutundaki gri seviyeli imgeye tam kapasitede damga gömülmüştür.



Şekil 4. Önerilen yöntem ve diğer yöntemlerin çalışma zamanlarının karşılaştırılması (a) ortalama veri gömme zamanları (b) ortalama veri çıkarma zamanları.

Güvenilirlik: Önerilen yöntem blok tabanlı bir yöntemdir. Damga gömmek için bloktan rastgele bir piksel seçilmektedir. Damga gömülecek pikseli seçmek için rastgele sayı üreteçleri kullanılmaktadır. Yöntemin güvenilir bir yöntem olması için kriptolojik rastgele sayı üreteçleri kullanılması gerekmektedir. Bu rastgele sayı üreteçlerinin özellikleri [26]' da sunulan makalede net bir şekilde açıklanmıştır. Kriptolojik özellik taşıyan rastgele sayı üreteçlerinin herhangi biri kullanılarak önerilen yöntemin güvenilirliği sağlanabilmektedir [27]. Yöntem bu yönüyle genişletilebilir bir yöntemdir. Örneğin 256 x 256 boyutunda bir imgeye 8 x 8 boyutunda bloklar kullanarak damga gömmek için $\frac{256}{8}.\frac{256}{8} = 1024$ bit uzunluğunda bir anahtarın kullanılması gerekmektedir. Kullanılan rastgele sayı üreteci kriptolojik özelliklere sahip ise saldırganın bu büyüklükteki anahtarı elde edebilmesi için 2^{1024} saldırı gerçekleştirmesi gerekmektedir. Bu durumda yöntemin güvenilir bir yöntem olduğunu doğrulamaktadır. Özetle, önerilen yöntem anahtar tabanlı bir damgalama yöntemidir ve damgalama anahtarı üretmek için kriptolojik rastgele sayı üreteçleri kullanılmaktadır. Kullanılan anahtar boyutu, imgenin boyutuna ve kullanılan blok boyutuna bağlıdır. Rastgele sayı üreteci kullanılarak üretilen anahtarın boyutu Eşitlik 10' da gösterilmiştir.

$$anahtar_{boyutu} = \left\lfloor \frac{M}{w} \right\rfloor . \left\lfloor \frac{N}{h} \right\rfloor . katman \quad (10)$$

Yeterli büyüklükte anahtar kullanılarak önerilen yöntemin güvenilirliği sağlanmaktadır.

5. Sonuç ve Öneriler

Bu çalışmada, Goldbach sanısı tabanlı yeni bir sayısal damgalama yöntemi önerilmiştir. Goldbach sanısı kullanılarak yeni bir dönüşüm elde edilmiştir. Elde edilen dönüşüm kullanılarak uzaysal alanda yeni bir damgalama yöntemi geliştirilmiştir. Önerilen damgalama yönteminin başarımını ölçmek için kapasite, görsel kalite, dayanıklılık ve çalışma zamanı kullanılmıştır. Önerilen yöntemin kapasitesinin esnek olduğu ve yüksek kapasitede damgalama imkanı verdiği matematiksel olarak gösterilmiştir. 8 x 8 blok boyutunda 60 dB civarında PSNR değeri elde edilmiştir. Dayanıklılık testinde önerilen algoritmanın parlaklık saldırısı ve JPEG ataklarına karşı dayanıklı olmadığı ancak gürültü ekleme saldırısına karşı dayanıklı olduğu gözlemlenmiştir. Önerilen sayısal damgalama yöntemi kırılgan bir yapıya sahiptir ve bu yöntemin imge kimlik doğrulama yöntemi olarak kullanılabileceği gösterilmiştir. Bu yöntemin çalışma zamanı ölçülmüş ve hızlı çalıştığı görülmüştür. Bloktaki veri gizlenecek piksel rastgele sayı üreteci kullanılarak seçilmektedir. Güvenilir rastgele sayı üreteçleri sayesinde veri güvenliği de sağlanmıştır.

Gelecekteki çalışmalarda bu yöntem AKD ve ADD gibi dönüşümlerle birlikte kullanılarak daha dayanıklı sayısal damgalama yöntemleri ve imge kimlik doğrulama yöntemlerinin önerilebileceği gösterilmiştir.

6. Kaynaklar

1. Doğan, Ş. (2016). A new data hiding method based on chaos embedded genetic algorithm for color image. *Artificial Intelligence Review*, *46*(1), 129-143.
2. Akter, A., E-Tajnina, N., Ullah, M.A. (2014). Digital image watermarking based on DWT-DCT: evaluate for a new embedding algorithm, in: Third Int. Conf. On Informatics, Electronics & Vision, May 2014, Dhaka,Bangladesh, pp. 1–6.
3. Su, Q., Niu, Y., Wang, Q., Sheng, G. (2013). A blind color image watermarking based on DC component in thespatial domain, Optik 124 (23), 6255–6260.
4. Lang, J., Zhang, Z.-G. (2014). Blind digital watermarking method in the fractional Fourier transform domain, Opt. Lasers Eng. 53, 112–123.
5. Musrrat, A., Ahn, C.W., Pant, M. (2014). A robust image watermarking technique using SVD and differential evolution in DCT domain, Optik 125 (1), 428–434.
6. Tuncer, T., Avcı, E. (2016). Göktürk Alfabesi Tabanlı Görsel Sır Paylaşımı Metodu ile Veri Gizleme Uygulaması, Journal of the Faculty of Engineering and Architecture of Gazi University, 31, 3, 781-789.
7. Dogan, S. (2017). A reversible data hiding scheme based on graph neighbourhood degree. Journal of Experimental &

Theoretical Artificial Intelligence, 29(4), 741-753.
8. Elibaşı E., Özdemir S. (2013). Kablosuz Çoklu Ortam Algılayıcı Ağlarında Damgalama İle Güvenli Veri Kümeleme, Journal of the Faculty of Engineering and Architecture of Gazi University Cilt 28, No 3, 587-594, Vol 28, No 3, pp. 587-594.
9. Dogan, S., Tuncer, T., Avci, E., Gulten, A. (2011). A robust color image watermarking with Singular Value Decomposition method. *Advances in* Engineering Software, 42(6), 336-346.
10. Mir, N. (2014). Copyright for web content using invisible text watermarking, Computers in Human Behavior, 30, 648–653.
11. Zheng, P.-P., Feng, J., Li, Z., Zhou, M.-Q. (2014). A novel SVD and LS-SVM combination algorithm for blind watermarking, Neurocomputing, 142, 520–528.
12. Hu, H.-T., Hsu, L.-Y. (2015). Exploring DWT–SVD–DCT feature parameters for robust multiple watermarking against JPEG and JPEG2000 compression, Computers and Electrical Engineering, 41, 52–63.
13. Abdallah, H. A., Ghazy, R. A., Kasban, H., Faragallah, O. S., Shaalan, A. A., Hadhoud, M. M., Dessouky, M. I., El-Fishawy, N. A., Alshebeili, S. A., Abd El-samie, F. E. (2014). Homomorphic image watermarking with a singular value decomposition algorithm, Information Processing and Management, 50, pp. 909–923.
14. Xiang-yang, W., Yu-nan, L., Shuo, L., Hong-ying, Y., Pan-pan, N., Yan, Z. (2015). A new robust digital watermarking using local polar harmonic transform, Computers and Electrical Engineering, 46, 403–418.
15. Khalili, M. (2015). DCT-Arnold chaotic based watermarking using JPEG-YCbCr, Optik, 126, 4367–4371.
16. Mehto, A., Mehra, N. (2016). Adaptive Lossless Medical Image Watermarking Algorithm Based on DCT & DWT, International Conference on Information Security & Privacy (ICISP2015), 78, 88-94.
17. Botta, M., Cavagnino, D., Pomponiu, V. (2016). A modular framework for color image watermarking, Signal Processing, 119, 102–114.
18. Nguyen, T.-S., Chang, C.-C., Yang, X.-Q. (2016). A reversible image authentication scheme based on fragile watermarking in discrete wavelet transform domain, Int. J. Electron. Commun. (AEÜ), 70, 1055–1061.
19. Shih, F. Y., Zhong, X. (2016). High-capacity multiple regions of interest watermarking for medical images, Information Sciences, 367–368, 648–659.
20. Patra, J. C., Karthik, A., Bornand, C. (2010). A novel CRT-based watermarking technique for authentication of multimedia contents, Digital Signal Processing, 20 , 442-453.
21. Patra, J. C., Karthik A., Bornand, C. (2010). A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression, Digital Signal Processing, 20, 1597-1611.
22. Thulasidharan, P. P., Nair, M. S. (2015). QR code based blind digital image watermarking with attack detection code, Int. J. Electron. Commun. (AEÜ), 69, pp. 1074–1084.
23. Idowu, M. A. (2015). A Novel Theoretical Framework Formulated for Information Discovery from Number System and Collatz Conjecture Data, Procedia Computer Science, 61, pp. 105 – 111.
24. Copot, M. (2016). Collatz Conjecture reverse-tree, https://codepen.io/towc/pen/mEaJjq, (Son Erişim Tarihi: 29/09/2016).
25. SIPI Image Dataset (2017). University of Southern California, Signal and Image Processing Institute, http://sipi.usc.edu/database/, (Son Erişim Tarihi: 16/10/2017)
26. Özkaynak, F. (2015). Kriptolojik Rasgele Sayı Üreteçleri. Türkiye Bilişim Vakfı Bilgisayar Bilimleri Ve Mühendisliği Dergisi, 8(2).
27. Özkaynak, F. (2014). Cryptographically secure random number generator with chaotic additional input. Nonlinear Dynamics, 78(3), 2015-2020.