RENKLİ İMGELERDE KİMLİK DOĞRULAMASI VE SALDIRI TESPİTİ İÇİN GÖRSEL SIR PAYLAŞIM TABANLI YENI BIR KIRILGAN DAMGALAMA ALGORITMASI

Turker Tuncer[1], Engin Avcı[2]

Original scientific paper

Adli bilişim, bilişim sistemleri üzerinden genellikle veri olarak elde edilen delillerin toplanması, saklanması, derlenmesi ve analizi konusunda standartları oluşturulan çok disiplinli bir yapıdır. Adli bilişim sanılan aksine özel bir alan değil, geniş alan disiplinidir. Bu makalede adli bilişim uygulamalarında sıklıkla kullanılan özet fonksiyonlarının yerine kırılgan damgaların kullanılması önerilmiştir. Özet fonksiyonları saldırının yapıldığı bölgeyi tespit edemezler bu sebepten dolayı sayısal verilerde kimlik doğrulama için kırılgan damgaların kullanılması önerilmiştir. Bir damgayı kırılgan hale getirebilmenin en iyi yolu sır paylaşım tabanlı algoritmaları kullanmaktır. Bu makalede Wu ve Chen' in görsel sır paylaşımı algoritması kullanılarak, RGB imgeler için kimlik doğrulama ve saldırı tespiti yapılmıştır. Önerilen kırılgan damgalama algoritması yüksek görsel kaliteye sahip, kırılgan, güvenilir ve yüksek veri gizleme kapasitesine sahip bir algoritmadır. Wu ve Chen görsel sır paylaşımı algoritması sayesinde açısal ataklara karşı hassas, yeni bir kırılgan damgalama sistemi önerilmiştir.

Anahtar Kelimeler: *Veri Gizleme; Damgalama; Görsel Sır Paylaşımı; Adli Bilişim; Kriptolojik Özet Fonksiyonları; Bilgi Güvenliği; Görüntü İşleme.*

1 Giriş

Bilgi güvenliğini sağlayabilmek için veriyi yetkisiz erişimlerden korumak gerekmektedir. [1]. İnternetin yaygın olarak kullanılması, 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 sağlamanın iki yolu vardır. Bunlar şifreleme ve veri gizlemedir. Şifreleme biliminde simetrik şifreleme, asimetrik şifreleme ve görsel sır paylaşımı kullanılmaktadır. Şifrelemenin sağlanabilmesi için güvenilir anahtar üretme, karıştırma ve seçme gibi işlemlerin gerçekleştirilebilmesi için rastgele sayı üreteçlerine ihtiyaç duyulmaktadır.

Veri gizlemenin ilk örneklerine antik çağlarda rastlanmaktadır. Bu bilim dalının ilk bilinen uygulaması antik çağlarda gerçekleşen kafa derisine mesajı dövme olarak çizdirip, saçları uzatarak kafa derisindeki mesajı gizlemektir. Bu örnekten de anlaşılacağı gibi, veri gizlemenin temel amacı, veri için güvenilir bir veri iletim hattı oluşturmaktır. Günümüzde, birçok veri gizleme uygulaması geliştirilmektedir [2]. Veri gizleme biliminin en sık kullanılan alt dalları ise steganografi ve damgalamadır (watermarking). Steganografi, gizlenen verinin sezilememesini hedeflemektedir. Günümüzde birçok firma ve kurum steganografiyi kullanarak veri gizliliğinin sağlamayı hedeflemektedir[3-7]. Damgalamada da ilgili multimedya mesajın kimlik doğrulamasının yapılması hedeflenmiştir.

Veri gizleme algoritmalarını oluşturan öğeler aşağıdaki gibi verilmiştir [8].

- Örtü nesnesi (Cover object)
- Gizli mesaj (Secret message)
- Veri gizleme fonksiyonu (Data hiding function)
- Veri gizlenmiş nesne (Stego object)
- Veri gizleme anahtarı (Stego key)
- Veri çıkarma fonksiyonu (Data extraction function)

Örtü nesnesi metin, ses, imge ve video gibi multimedya verilerden oluşmaktadır [6]. Gizli mesaj, örtü nesnesinin içerisine veri gizleme fonksiyonu kullanılarak gömülür ve çıktı olarak veri gizlenmiş nesne elde edilir. Veri çıkarma aşamasında ise, veri gizleme anahtarı kullanılarak veri gizlenmiş nesnede bulunan veri gizleme indisleri tespit edilir. Veri çıkarma fonksiyonu kullanılarak gizli mesaj elde edilir [9-10]. Bu konuyla ilgili literatürde bulunan birkaç çalışma aşağıda verilmiştir.

Qi vd. [11] imge kimlik doğrulaması için, tekil değer tabanlı yarı kırılgan yeni bir damgalama şeması sunmuşlardır. Bu metot içerik bağımlı olarak güvenilir bir damga üretir ve bu damgayı tekil değer dizisine mantıksal operatörler kullanarak gömer. Botta vd. [12] kendi çalışmalarından önce tespit edilmeyen atakları tespit edebilmek ve saldırının lokasyonunu bulabilmek için yeni bir kırılgan damgalama sistemi önermiş ve başarılı sonuçlar elde etmişlerdir. Yu vd. [13] imge kimlik doğrulaması ve saldırı tespiti yapabilmek için yeni bir kırılgan damgalama algoritması geliştirmiştir. Düşük gömme kapasitesi kullanılarak saldırı tespiti yapılır. Bu sebepten dolayı önerilen algoritmanın görsel kalitesi yüksek elde edilmiştir. Ghosal vd. [14] binom dönümüşümü tabanlı kırılgan damgalama algoritması önermiştir ve elde edilen sonuçlar başarılı bulunmuştur. Tong vd. [15] kaos tabanlı saldırı tespit etme ve yeniden yapılandırma yeteneğine sahip bir kırılgan damgalama algoritması önermiştir. Deneysel sonuçlar bu algoritmanın daha güvenilir, daha iyi saldırı tespiti yapabilen ve kendini onarabilen bir algoritma olduğunu ortaya koymuştur. Tu vd. [16] doküman koruyabilmek için sır paylaşımı ve steganografi tabanlı yeni bir algoritma önermiştir. (k,n) sır paylaşımı şeması tabanlı bu algoritmada k<n ve gizli veri n parçaya ayrılmaktadır. Bu n adet sır parçasının k adeti bir araya geldiğinde mesaj elde edilmektedir. Deneysel sonuçlar bu metodun güvenilir ve uygulanabilir olduğunu göstermiştir. Lee vd. [17] tarafından Shamir'in (k,n) eşiksel sır paylaşım modeli tabanlı PNG imgelerde kimlik doğrulama algoritması önerilmiştir. Bu veri gizleme algoritma yüksek veri gizleme kapasitesine sahip, güvenilir, verimli ve yüksek görsel kaliteli bir veri gizleme algoritmasıdır.

Bu makalenin 2. bölümünde kriptolojik özet fonksiyonları, 3. bölümünde görsel sır paylaşım modelleri, 4. bölümünde önerilen yöntem, 5. bölümünde deneysel

sonuçlar 6. ve son bölümünde ise sonuçlardan bahsedilecektir.

2 Kriptolojik Özet Fonksiyonları

Kriptografik özet fonksiyonları değişken uzunluktaki herhangi bir veriden sabit veya genellikle daha küçük uzunlukta özet değerleri çıkartmak için kullanılır [18-22].

Özet bilgi sabit uzunluğa sahiptir. Özet fonksiyonlarında, tek yönlü (one-way) fonksiyonlar kullandığı için özet değerinden giriş verisine ulaşılması veya giriş verisi ile ilgili bilgi edinme teorik olarak imkânsızdır. Çünkü özet değeri, veri ile ilişki kurulamayan, anlam bütünlüğü içermeyen ve rastgele seçilmiş sayılar gibi görünmektedir.

Özet değeri elde edilen veriye özeldir. Özetleme işlemi her tekrarlandığında aynı sonucu verir. Veride gerçekleşen 1 bitlik değişiklik özet bilgisini de değiştirmektedir. Bu yüzden bu değere genellikle verinin dijital parmak izi veya özet değeri denilmektedir.

Özet fonksiyonları çok çeşitli alanlarda kullanılmaktadır. Asimetrik şifrelemede, elektronik imza şemalarında, rastgele sayı üreteçlerinde ve adli bilişim alanında kullanılmaktadır.

Kriptografik özet fonksiyonlarında aranan özellikler aşağıdaki gibidir [22-24]:

- Bilinen ve ispat edilebilir bir özet fonksiyonu algoritması kullanılmalıdır.
- Bir özet fonksiyonu herhangi bir uzunluktaki veriyi girdi olarak alabilmeli ve sabit uzunlukta çıktı üretmelidir.
- Verilen herhangi bir x değeri ve h özet fonksiyonu için $h(x)$ değerini hesaplamak kolay olmalıdır.
- Ters görüntü direnci (Preimage resistance): $h(x)$ değerini veren x değerinin bulunması zor olmalıdır.
- İkinci ters görüntü direnci (Second preimage resistance): x ve $h(x)$ verildiği zaman $h(x') = h(x)$ olacak şekilde x ten farklı bir x' bulmak zor olmalıdır.

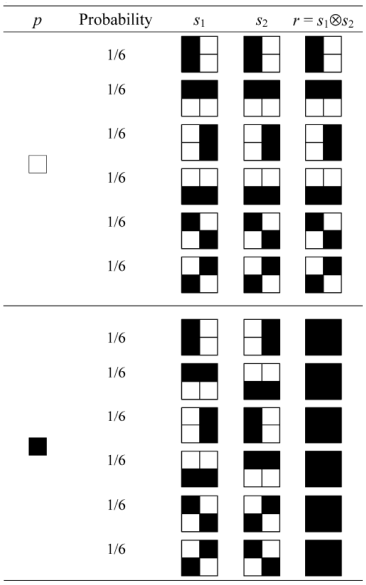
Çakışma direnci (Collision resistance): Herhangi bir x için $h(x') = h(x)$ olacak şekilde x ten farklı bir x' bulmak zor olmalıdır.

Adli bilişim uygulamalarında blok şifreleme tabanlı özet fonksiyonları kullanılmaktadır. Bu özet fonksiyonlar ise MD4, MD5, SHA0, SHA1, SHA256, SHA-3 vb. algoritmalardır.

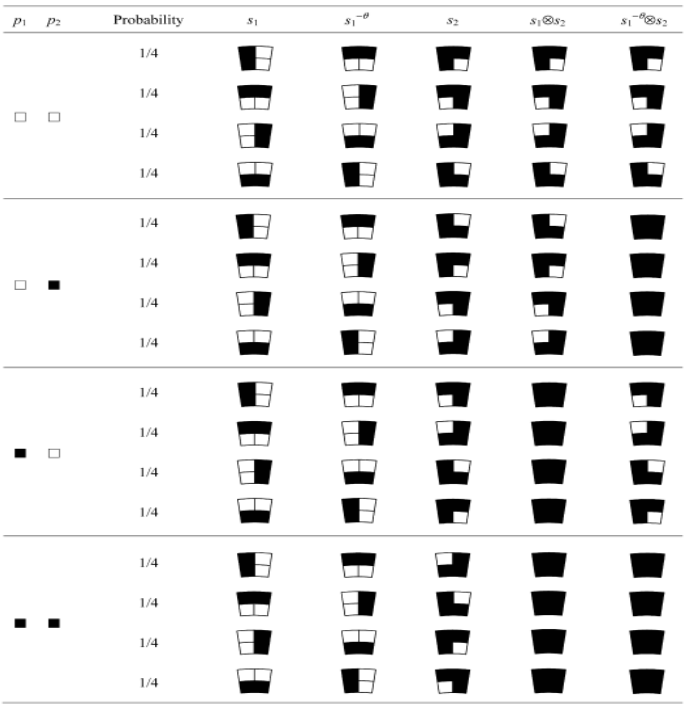
Adli bilişim uygulamalarında özet fonksiyonları bir verinin değiştirilip değiştirilmediğinin doğrulanması için kullanılmaktadır.

3 Görsel Sır Paylaşımı Modelleri

Görsel sır paylaşımı kavramı ilk kez 1996' da Moni Naor ve Adi Shamir tarafından ortaya atılmıştır [25]. Sır paylaşımını en basit şekliyle ifade etmek için 0 ve 1'lerden oluşan ikilik görüntüler kullanılmıştır.



Şekil 1. Genişletilmiş GSP modeli



Şekil 2. Wu ve Chen kodlama tablosu

Naor ve Shamir' in önerdiği metodun genişletilmiş görsel sır paylaşımı (2, 2) algoritması şekil 1'de verilmiştir.

Bu modelin açısal olarak daha da geliştirilmiş hali, Wu ve Chen tarafından 2005 yılında geliştirilmiştir. Önerilen algoritmada 3 adet sır parçası ve 2 bitlik veri gizleme fonksiyonu kullanılacağı için Wu ve Chen' nin modelinin kullanılması öngörülmüştür [26,27]. Wu ve Chenin kodlama tablosu şekil 2' de verilmiştir.

Önerilen yöntemde rastgele sayı üreteçleri kullanılarak sır parçaları seçilebilir. 3 adet sır parçası kullanılmıştır ve kullanılan sır parçalarından 2 bit çıkış üretilmiştir. Şekil 2' de gösterilen p1 ve p2 çıkış bitleri, s1, s1-ɵ ve s2 ise sır parçaları olarak kabul edilmiştir.

4 Önerilen metot

Bu makalenin en temel amacı, adli bilişimde sıklıkla kullanılan özet fonksiyonlarının yetersiz kaldığı yerlerde kırılgan damgaları kullanmaktır. Önerilen metot ile öncelikle damga sır paylaşımı şeması kullanılarak parçalarına ayrılacak ve ardından damga 2LSBs (Least Significant Bits Insertion – En anlamsız bit yerleştirme) veri gizleme fonksiyonu kullanılarak veri gizlenecektir.

Önerilen veri gizleme algoritmasında görsel sır paylaşımı algoritması olarak Wu ve Chen'in görsel sır paylaşımı algoritmasının kullanılması önerilmiştir. Şekil 2'de verilen tablo kullanılarak damga gürültüsüz olarak elde edilmektedir. Önerilen veri gizleme algoritmasının blok diyagramı şekil 3' deki gibidir.

Önerilen veri gizleme algoritmasının adımları da aşağıdaki gibidir.

(1) Renkli RGB imge sırasıyla R, G ve B kanallarına ayrılır.

(2)Wu-Chen algoritması kullanılarak damga 3 sır parçasına ayrılmıştır.

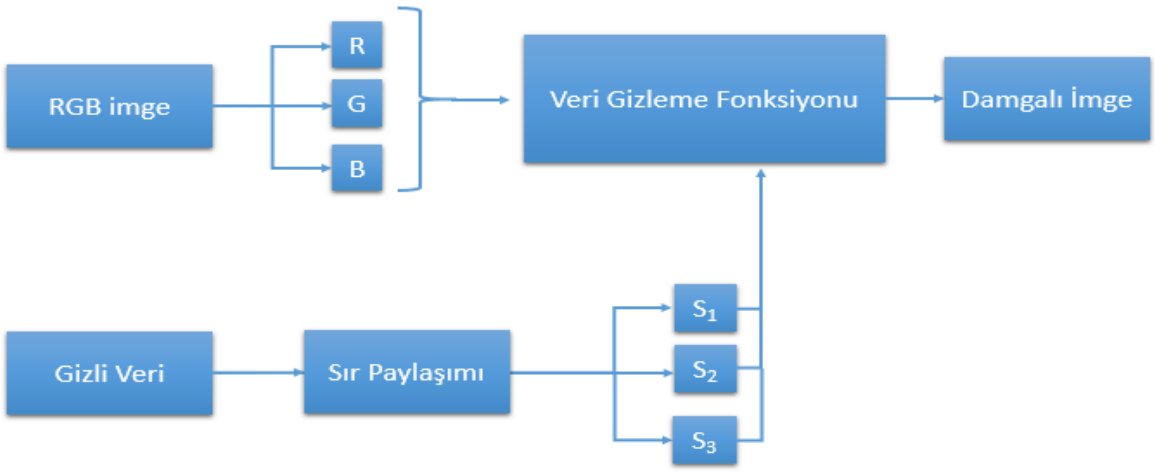
(3) Sır parçası olacak elemanları seçebilmek için ise sözde rastgele sayı üreteçleri kullanılmıştır. Bu makalede lineer eşiksel sayı üreteci kullanılmıştır.

$$X_{i+1}=(aX_i+c)\,mod\,m \qquad (1)$$

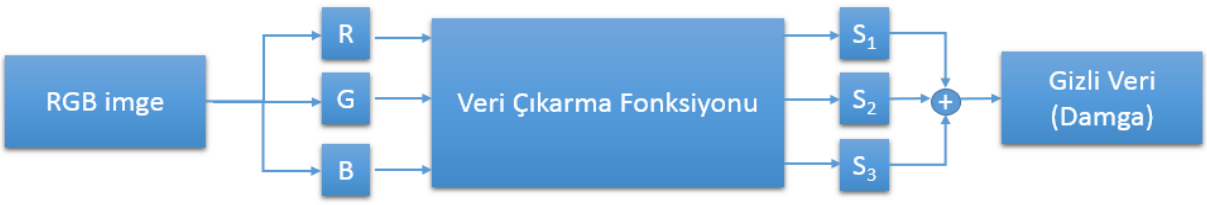
X rastgele sayı dizisi, a çarpan, c artım ve m modül katsayılarıdır. Bu formül kullanılarak istenilen uzunlukta 0 ile m-1 arasında rastgele sayı üretilebilmektedir.

(4) Elde edilen 3 sır parçası 2LSBs veri gizleme algoritması kullanılarak örtü imgesine gömülür.

Yukarıdaki adımlar gerçekleştikten sonra damgalanmış imge elde edilir. Damgalanmış imgeden, damgayı elde etmek için ise kullanılacak adımların blok diyagramı şekil 4' de verilmiştir.



Şekil 3. Önerilen veri gizleme algoritmasının blok diyagramı.



Şekil 4. Önerilen veri çıkarma algoritmasının blok diyagramı.

Önerilen algoritma kullanılarak damgayı yeniden elde etmek için aşağıdaki adımlar kullanılır.

(1) Damgalanmış imge katmanlarına ayrılır.

(2) Veri çıkarma fonksiyonu kullanılarak S1, S2 ve S3 kümleri oluşturulur. Bu çalışmada 2LSBs veri gizleme algoritması kullanıldığı için aşağıdaki formül kullanılarak veri çıkarma işlemi gerçekleştirilir.

$$S_{1i,j}=R_{i,j}(mod\ 4),\ i=\{1,2,...,m\},\ j=\{1,2,...,n\} \quad (2)$$

$$S_{2i,j}=G_{i,j}(mod\ 4),\ i=\{1,2,...,m\},\ j=\{1,2,...,n\} \quad (3)$$

$$S_{3i,j}=B_{i,j}(mod\ 4),\ i=\{1,2,...,m\},\ j=\{1,2,...,n\} \quad (4)$$

(3) Şekil 2' deki kurallar kullanılarak sır parçalarından damga elde edilir.

Önerilen metodun avantajları aşağıdaki gibi verilmiştir.

- Toplanan veriler için kimlik doğrulama işlemi yapabilmek.
- Toplanan verinin orijinal olduğunu anlayabilmek.
- Eğer veri saldırıya uğramışsa, verinin hangi bölgesine saldırı yapıldığı kolaylıkla tespit edebilmek.

5 Deneysel Sonuçlar

Bu makalede kullanılan yöntemi değerlendirebilmek için veri gizleme algoritmalarını değerlendirebilmek için önerilmiş 6 adet gereksinimi sağlaması gerekmektedir. Bu gereksinimler ise aşağıdaki gibi verilmiştir. Bu gereksinimleri test etmek için SIPI imge veri tabanından 8 adet imge seçilmiştir ve seçilen imgeler 512 x 512 x 3 boyutunda imgelerdir. Örtü imgelere 512 x 512 boyutunda damgalar gizlenmektedir. Örtü verisi olarak kullanılan imgeler şekil 5' de verilmiştir.

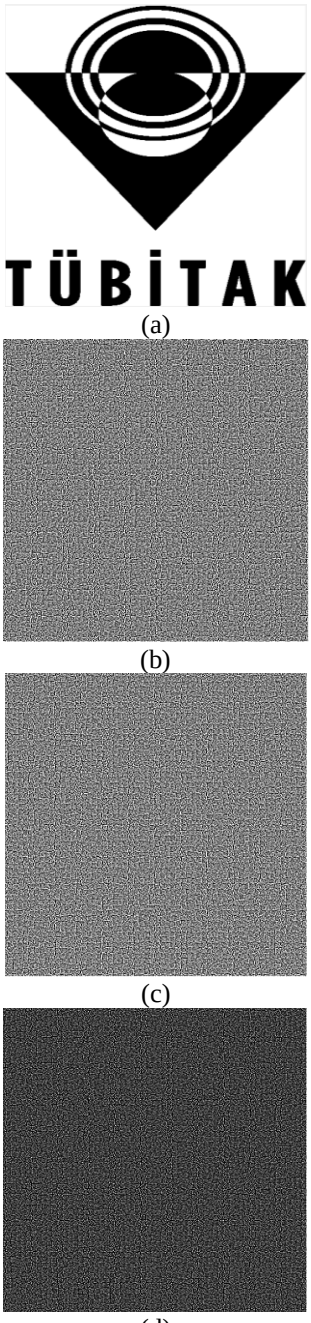
Optimum veri gizleme fonksiyonu: Bu makalede veri gizleme fonksiyonu olarak 2LSBs kullanılmıştır. LSB veri gizleme algoritmalarında en sık kullanılan ve en çok bilinen veri gizleme fonksiyonlarıdır. Bu fonksiyonların uygulaması kolaydır ve bu fonksiyonlar kullanılarak veri gizleme işlemi hızlı bir şekilde yapılmaktadır. Şekil 2' de verilen tablo kullanılarak damga sır parçalarına ayrılır ve 2LSBs fonksiyonu kullanılarak renkli imgeye gömülür.

Optimum veri çıkarma fonksiyonu: Önerilen metotla veri çıkarabilmek için (mod 4) işlemi kullanılarak sır parçaları elde edilmektedir. Sır parçaları elde edildikten sonra mantıksal veya işlemi veya Şekil 2 ' de verilen Wu ve Chen' in kodlama tablosu kullanılarak damga elde edilir.

Şekil 5. Deneysel sonuçlar için kullanılan test imgeler (a) Orijinal imge (b) Stego-imge

Kapasite: Önerilen algoritma kullanılarak renkli imgenin her bir katmanına 2bpp (bit per pixel – piksel başına bit) kapasitede veri gizlenmektedir.

Gizlilik: Wu ve Chen' in görsel sır paylaşımı metodu kullanılarak damganın gizliliği sağlanmaktadır. Aynı zamanda sır parçalarının rastgele seçimi sayesinde güvenilir bir dağılım sağlanacaktır. Rastgele sayı üreticinin en büyük avantajlarından birisi ise elemanların tekrarlanma sayısını birbirine yakınlaştırmasıdır. Şekil 6'da, ikilik bir imge ve imgeye önerilen görsel sır paylaşım şemasının uygulanmasının ardından elde edilen sır parçaları verilmiştir.



Şekil 6. Wu ve Chen görsel sır paylaşımı yönteminin uygulanması (a) Orijinal imge (b) İlk sır parçası (c) ikinci sır parçası (d) üçüncü sır parçası

Elde edilen 3 adet sır parçası sırasıyla R,G ve B katmanlarına gömülmektedir. Veri çıkarma fonksiyonu bilinse de damgaya doğrudan ulaşılamayacaktır. Wu ve Chen' in görsel sır paylaşımı yöntemi kullanılarak damganın gizliliği sağlanmaktadır.

Ataklara Karşı Dayanıklılık: Bu makalede, kırılgan ve atağın hangi bölgeye yapıldığını tespit edebilen yeni bir algoritma önerilmiştir. Test resimleri olarak şekil 5' de gösterilen renkli imgeler kullanılmıştır. Bu imgelerin 100 x 100' lük kısmına aşağıdaki ataklar uygulanmıştır[28-30]. Saldırıları tespit edebilmek için tüm elemanları 1 olan beyaz damganın gömülmesi öngörülmüştür.

- Kesme atağı
- Kolaj atağı
- Döndürme atağı
- JPEG sıkıştırma atağı
- Medyan filtre atağı
- Boyutlandırma atağı

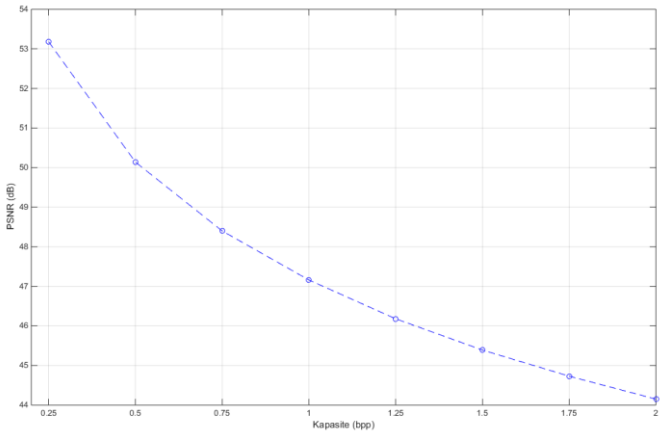
Tablo 1' de gösterildiği gibi özet fonksiyonlar kullanılarak saldırı tespiti yapılamamaktadır. Saldırının, imgenin hangi bölgesine yapıldığını tespit edebilmek için önerilen metot kullanılmalıdır. Elde edilen sonuçlar, önerilen metodun yüksek kırılganlığa sahip olduğunu göstermektedir.

Yüksek Görsel Kalite: Bir veri gizleme algoritmasının sağlaması gereken en önemli özelliklerden birisi de yüksek görsel kalitedir. Gizlenen verinin gözle ve kulakla fark edilememesi gerekmektedir. Görsel kaliteyi ölçmek için MSE (mean square error – ortalama karesel hata), PSNR (peak signal-to-noise ratio – tepe sinyal gürültü oranı) vb. ölçüm parametreleri kullanılmaktadır. MSE ve PSNR formülleri denklem 5 ve 6' da verilmiştir.

$$MSE = \frac{1}{mn}\sum_{i,j}(CI_{i,j} - SI_{i,j})^2 \qquad (5)$$

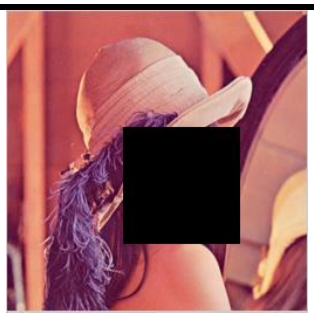
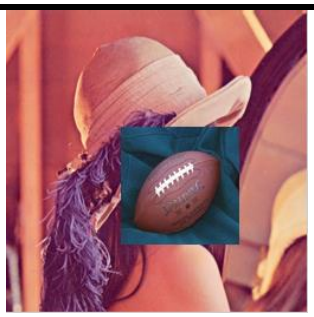
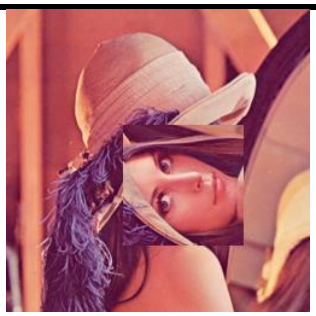
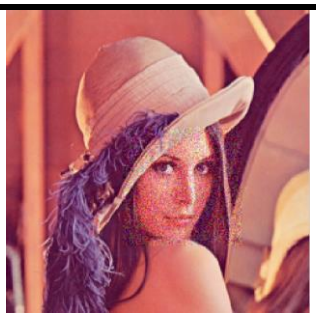
$$PSNR = 10\log\frac{Max(CI_{i,j}^2)}{MSE} \qquad (6)$$

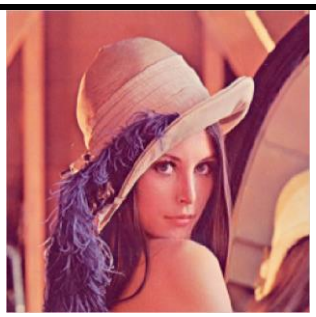
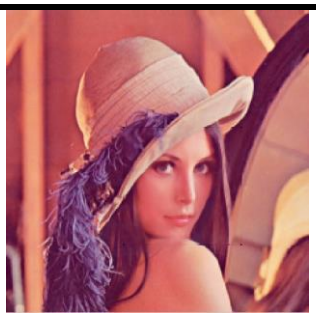
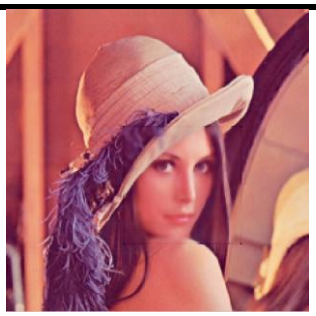
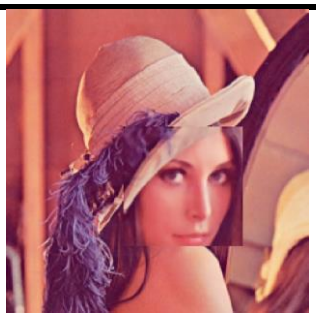
Şekil 7' de önerilen algoritmanın test resimlerine uygulanmasının ardından elde edilen PSNR kapasite değişim eğrisi verilmiştir.



Şekil 7. Test resimlerinden elde edilen ortalama PSNR/ Kapasite değişim oranı.

Tablo 1. Saldırı tespiti ve MD5 özet fonksiyonları.

Atak	Saldırı Yapılan İmge	Elde Edilen Damga	Özet Fonksiyonları (MD5)
Kesme Atağı			Orijinal imge: CB18648237B3DA26440D7F233AC503FE Kesme atağı uygulanmış imge: 7623195870C23B9E6AC11A0E947666B7
Kolaj Atağı			Orijinal imge: CB18648237B3DA26440D7F233AC503FE Kolaj atağı uygulanmış imge: 45385D2B552542C7A72DB42B0AD5D61D
Döndürme (90 derece)			Orijinal imge: CB18648237B3DA26440D7F233AC503FE Döndürme atağı uygulanmış imge: 31E01399DCB3C56904815AB7F377E663
Gaussian Gürültü (M=0.01, V=0.01)			Orijinal imge: CB18648237B3DA26440D7F233AC503FE Gürültü atağı uygulanmış imge: FC6FD9D3D494D0873907A9CA0D747A34

JPEG Sıkıştırma (%90)			Orijinal imge: CB18648237B3DA26440D7F233AC503FE JPEG sıkıştırma atağı uygulanmış imge: 0075BE44A271BE390B844504AB74BEB8
Medyan Filtre Atağı (3 x 3)			Orijinal imge: CB18648237B3DA26440D7F233AC503FE Medyan filtre atağı uygulanmış imge: 91EB75A75852D15BAF97E8E476BA601C
Wiener Filtre Atağı (3 x 3)			Orijinal imge: CB18648237B3DA26440D7F233AC503FE Wiener Filtre atağı uygulanmış imge: D8375C73852E20756471A5EEAB624C79
Boyutlandırma Atağı (150 x 150)			Orijinal imge: CB18648237B3DA26440D7F233AC503FE Boyutlandırma atağı uygulanmış imge: 40DDD296B5B7C7ACF8624F776AC8311E

6 Sonuç

Bu makalede, toplanan verileri doğrulama ve bu verilere yapılan saldırıları tespit edebilmek için rastgele sayı üreteçleri, özet fonksiyonları, görsel sır paylaşım algoritmaları ve veri gizleme algoritmaları kullanılmıştır ve bu algoritmanın adli bilişim uygulamalarında da kullanılabileceği gösterilmiştir. Birbirinden ayrı 3 alan kullanılarak veri doğrulama yapılmıştır. Özet fonksiyonlarının değiştirilen verileri tespit edebilmektedir ancak verinin hangi bölgesinin saldırıya uğradığını tespit edememektedir. Bu sebepten dolayı görsel sır paylaşımı tabanlı yeni bir kırılgan damgalama önerilmiştir. Wu-Chen görsel sır paylaşım modeli ve 2LSBs veri gizleme fonksiyonu kullanılarak oluşturulan bu algoritma, veri gizleme ölçütlerinin tümünü sağladığı gibi, saldırı tespiti yapabilmede de yüksek performansa sahiptir. Özellikle açısal saldırılara karşı oldukça hassas bir damgalama yöntemi önerilmiştir. Bu işlem adli bilişimde sadece toplanan verilerin doğrulanması kısmında kullanılacaktır. Bu makale, adli bilişimin geniş alan bilgisine sahip olduğunu göstermekle beraber, veri gizlemenin tüm başarım ölçütlerini sağlamış, kırılgan ve adli bilişimde uygulanabilir bir damgalama sistemi önerilmiştir

.

7 Kaynaklar

[1] Z. Ni, Y.-Q. Shi, N. Ansari, W. Su, Reversible Data Hiding, IEEE Transactions On Circuits And Systems For Video Technology, 16 (3), 2006.

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

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

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

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

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

[7] G.S. Lin, Y.T. Chang, W.N. Lie, 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] C. Cachin, An information-theoretic model for steganography, Information and Computation, 192 (1), 41-56, 2004.

[9] Y.-H. Yu, C.-C. Chang, A new edge detection approach based on image context analysis, Image and Vision Computing, 24 (10), 1090–1102, 2006.

[10] A. Westfeld, Detecting low embedding rates, In: Proceedings of information hiding workshop. LNCS, 2578, 324-339., 2003.

[11] X. Qi, X. Xin, A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization, Journal of Visual Communication and Image Representation, 30 (2015), 312-327, 2015.

[12] M. Botta, D. Cavagnino, V. Pomponiu, A successful attack and revision of a chaotic system based fragile watermarking scheme for image tamper detection, International Journal of Electronics and Communications (AEÜ), 69 (1), 242-245, 2015.

[13] M. Yu, J. Wang, G. Jiang, Z. Peng, F. Shao, T. Luo, New fragile watermarking method for stereo image authentication with localization and recovery, International Journal of Electronics and Communications (AEÜ), 69 (1), 361-370, 2015.

[14] S.K. Ghosal, J. K.Mandal, Binomial transform based fragile watermarking for image authentication, Journal of Information Security and Applications, 19 (4&5), 272-281, 2014.

[15] X. Tong, Y. Liu, M. Zhang, Y. Chen, A novel chaos-based fragile watermarking for image tampering detection and self-recovery, Signal Processing: Image Communication, 28 (3), 301-308, 2013.

[16] S.Tu, C. Hsu, Protecting secret documents via a sharing and hiding scheme, Information Sciences, 279 (20), 52-59, 2014.

[17] C. Lee, W. Tsai, A data hiding method based on information sharing via PNG images for applications of color image authentication and metadata embedding, Signal Processing, 93 (7), 2010-2025, 2013.

[18] Vassil Roussev, An evaluation of forensic similarity hashes, Digital Investigation, Volume 8, Supplement, August 2011, Pages S34-S41

[19] Ç. Koç, (2009). Cryptographic Engineering, Springer-Verlag.

[20] J. Kartz, Y. Lindell, (2008). Introduction to modern cryptography : principles and protocols, Chapman & Hall.

[21] C. Paar, J. Pelzl, (2010). Understanding Cryptography A Textbook for Student and Practitioners, Springer.

[22] K. Kırkıl, A. B. Özer, F. Özkaynak, (2012). Kaos Tabanlı Kriptolojik Özetleme Fonksiyonları, Akıllı Sistemlerde Yenilikler ve Uygulamaları Sempozyumu, Trabzon.

[23] A. Menezes, P. Van Oorschot, S Vanstone. (1996). Handbook of Applied Cryptography. CRC Press.

[24] B. Preneel, (1993). Analysis and Design of Cryptographic Hash Functions. PhD thesis, Katholieke Universiteit Leuven.

[25] M. Naor, A. Shamir, (1995)Visual Cryptography, EUROCRYPT'94 – Springer.

[26] C.C. Wu, L.H. Chen, A study on visual cryptography, Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.

[27] H.-C. Wu, C.-C. Chang, Sharing visual multi-secrets using circle shares, Comput. Stand. Interfaces 134 (28) (2005) 123–135.

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

[29] M. Tanha, S. D. S. Torshizi, M. T. Abdullah, F. Hashim, An overview of attacks against digital watermarking and their respective counter measures. Paper presented at Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on, Kuala Lumpur, 265–70, 26–28 June 2012.

[30] P. P. Thulasidharan, M. S. Nair, QR code based blind digital image watermarking with attack detection code, International Journal of Electronics and Communications (AEÜ), In Press, Uncorrected Proof, Available online 11 April 2015.

Authors' addresses

Dr. Türker Tuncer[1], Asistant Research
Fırat University
Technology Faculty, Forensic Engineering
ttuncer@firat.edu.tr

Dr. Engin Avci[2], Professor
Fırat University
Technology Faculty, Software Engineering
eavci@firat.edu.tr