VERİ SAKLAMA YÖNTEMLERİ: SAYISAL GÖRÜNTÜLERİN DAMGALANMASI, AMAÇLARI VE UYGULAMA ALANLARI

Mustafa ORAL[1] **Murat FURAT**[2]

[1]Elektrik ve Elektronik Mühendisliği Bölümü, Mustafa Kemal Üniversitesi, Hatay
[2]Elektrik ve Elektronik Mühendisliği Bölümü, Çukurova Üniversitesi, Adana

[1]e-posta: moral@mku.edu.tr [2]e-posta: mfurat@cu.edu.tr

Anahtar Sözcükler: Veri Saklama, Sayısal Görüntülerin Damgalanması, Telif Hakları ve Güvenlik

ABSTRACT

In this paper, an overview of information hiding methods in general and digital watermarking of images in particular are presented. The terminology of information hiding systems, the goal of digital watermarking and its application areas are explained in detail.

1. GİRİŞ

Veri saklama yöntemlerinin tarihi, veri iletişimi kadar eskilere dayanmaktadır. Bilginin değeri ile doğru orantılı olarak onun güvenli bir şekilde iletilmesinin önemi de artmıştır. Tarih boyunca bu konuda çeşitli araştırmalar yapılmış, bilginin iletilmesinde ve saklanmasında önemli gelişmeler yaşanmıştır.

İletişim teknolojilerinde yaşanan gelişmelere paralel olarak bu konudaki çalışmalar da çeşitlilik göstermiştir. Özellikle bilgisayarların ve depolama birimlerinin sağladığı kolaylık ve avantajlar nedeniyle bilgi, hızlı bir şekilde sayısal ortamda saklanmaya ve işlenmeye başlamıştır. Bilgisayarlar ile birlikte gelen Internet'in sağladığı bilgi aktarım kolaylığı, iletişimde yeni bir çığır açmıştır.

Bilginin saklanmasının ve iletilmesinin biçim değişmesi, onun korunması ve güvenli iletilmesindeki yeni yöntemleri de beraberinde getirmiştir. Sayısal teknolojinin sağladığı kolaylık kadar getirdiği güvenlik sorunlar da mevcuttur. Bu sorunların türüne göre ve farklı amaçlara göre birçok yöntem geliştirilmiştir. Her biri farklı yönleri ile bu konuda yaşanan çeşitli sorunlara çözümler getirmektedir. Bu çalışmada, veri saklama yöntemleri genel olarak açıklanmış, bunlar arasında literatürde önemli yer tutan sayısal damgalamanın amaçları ve uygulama alanları hakkında bilgi sunulmuştur.

2. VERİ SAKLAMA YÖNTEMLERİ

2.1. Veri Saklama Yöntemlerinin Tarihçesi

Bilginin değeri kadar onun güvenli olarak iletilmesi ve saklanması da önemlidir. Bu konuda yapılan çalışmalar arasında günümüze ulaşan ilk bilgiler milattan önceki yıllara dayanır. M.Ö. 485–525 yıllarında yaşayan Yunan tarihçisi Heredot, bir çalışmasında Pers İmparatorluğu ile bir Yunan şehir devleti arasında geçen savaş sırasında gerçekleşen gizli bir iletişim metodunu anlatmıştır. Pers kralına ulaştırılacak gizli plan, taşıyacak kişinin kafası tıraş edilerek dövme ile yazılmış ve taşıyıcının saçları tekrar uzayıncaya kadar beklenmiştir. Böylece mesaja bir çeşit doğal kamuflaj hazırlanmıştır. Görünürde yanında hiçbir şey bulunmayan taşıyıcı, özgürce seyahat edebilmiş ve ulaşması gereken yere vardığında kafasını tıraş edip taşıdığı mesajı göstermiştir [1].

Bilinen tarih kadar eski bir veri saklama yöntemi de günümüzde görünmez mürekkep diye tanımladığımız yöntemdir. MS 23 – 79 yıllarında yaşayan Pliny the Elder, saydam bir yazı için, bir bitkinin sütü kullanılarak kağıda yazı yazıldığını ve sonradan kağıdın ısıtıldığında uygulanan sütün kağıt üzerinde kahverengiye doğru koyulaştığını anlatmıştır. Gizli veri iletişimi amacıyla kullanılan bu yöntem, bilinen ilk görünmez mürekkep uygulaması olarak karşımıza çıkmaktadır [1].

Bu konuda geçmişte kullanılan çok sayıda tekniği rapor eden Æneas the Tactician, gizli mesajları taşıyan mektupların, kadınların küpelerinde saklanıp taşındığını bildirmiştir. Bildirilen diğer bir yöntem de ise, mektuptaki yazı karakterlerinin boyunun değiştirerek gizli mesajın kodlanması veya mektubun üstüne ya da altına küçük delikler açarak mesajın saklanmasıdır. Bu yöntem, 17. yüzyılda Wilkins (1614–1672) tarafından geliştirilerek küçük delikler yerine görünmez mürekkep kullanılarak mikro noktalar ile işaretlenmiştir [2]. Görünmez mürekkep yöntemi II. Dünya Savaşı'nın başlarında kullanılmıştır. Görünmez mürekkep ile masum gibi görünen mektupların satır aralarında farklı mesajlar taşınmıştır. Ayrıca şifrelenmemiş bir mektubun metni, taşınacak mesajı gizlemek için bir ortam olarak kullanılmıştır. II. Dünya Savaşı'nda bir Alman ajanı tarafından gönderilen mektupta bu yöntem

kullanılmıştır [3,4]. Mesaj, mektubun metni içine gizlenmiştir. Normal cümle düzenindeki mektubun aşağıdaki metni, masum bir metin olarak görünmektedir:

Apparently neutrals protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.

Metnin sakladığı asıl bilgi, metindeki her kelimenin ikinci harflerinin birleştirilmesi ile ortaya *"Pershing sails from NY June 1"* olarak çıkmaktadır.

2.2. Terminoloji

Bilgi, bir taşıyıcıya saklanıp iletilebileceği gibi çeşitli yöntemlerle anlaşılmaz bir biçime dönüştürülerek de iletilebilmektedir. Her iki yöntemde de sadece ilgili kişilerin saklı bilgiyi elde etmesi amaçlanır.

Sayısal alanda yaşanan gelişmeler ile birlikte veri saklama teknolojilerinde de gelişmeler olmuştur. Sayısal ortamın sağladığı kolaylıkların yanında verinin saklanmasında, iletilmesinde ve sahibinin telif haklarının korunması gibi konularda büyük sorunları da beraberinde getirmiştir. Bu nedenle, birçok yöntem geliştirilmiş, her biri çeşitli sorunlara farklı çözümler önermiştir.

2.2.1. Steganography

Örtülü yazı anlamına gelen "Steganography", bir taşıyıcıya gizli mesajın eklenmesi yoluyla yapılan iletişim türüdür. Mesajın taşıyıcı üzerinde yapılacak değişikliklere karşı dayanıklı olması beklenmez. Buradaki amaç, taşıyıcıya fark edilmeyecek bir yöntem ile mesajı saklamak ve iletmektir.

Örtülü mesaja örnek olarak, hapishanedeki iki mahkumun durumu modellenmiştir [2]. Mahkumlar hapishaneden kaçmak istemektedirler ancak aralarındaki iletişim gardiyan tarafından sağlanmaktadır. Bu durumda, mahkumlar birbirlerine gönderecekleri mesajları şifrelemek zorunda ve bunun gardiyanın anlamayacağı bir biçimde yapmaları gerekmektedir. Dolayısıyla, birbirlerine gönderilecekleri mesajın masum bir resim içine gizlenmesi uygun çözüm olarak ortaya çıkmaktadır.

2.2.2. Kriptoloji

Kriptoloji, gizlenmesi gereken mesajın bir algoritma kullanarak şifrelenmesidir. Anlamlı bir yapıya sahip olan mesaj şifrelendikten sonra anlamsız bir biçime dönüştürülür. Örtülü mesajın aksine bu mesaj, herhangi bir taşıyıcı kullanılmadan alıcıya gönderilir. Alıcı, aldığı mesajı deşifre ederek asıl mesaja ulaşır. Üçüncü kişiler, şifrelenmiş mesajı elde etse bile deşifre algoritmasını bilmedikçe mesajın aslını elde edemezler. Bu yöntem, Rönesans döneminden itibaren geliştirilmeye başlanmıştır. Günümüzde ise bilgisayarların da etkin rol oynadığı iletişim alanında geniş çapta kullanılmaktadır [5].

2.2.3. Sayısal Damgalama (Digital Watermarking)

Günümüz teknolojisinin sunduğu sayısal ortamın avantajları nedeniyle her türde bilgi artık sayısal ortama aktarılabilmekte, kolayca düzenlenebilmekte ve uzak mesafelere hızlı bir şekilde iletilebilmektedir. Bilgisayarların ve bilgisayar ağlarının gelişmeye başlaması ile birlikte yeni güvenlik ve telif haklarının korunması sorunları ortaya çıkmıştır [7]. Bu sorunlara çözüm olması amacıyla önerilen sayısal damgalama yöntemleri, steganography uygulamalarıyla benzerlik gösterir. Hem örtülü yazıda hem de sayısal damgalamada, taşıyıcı üzerinde görünmez bir bilgi taşımayı amaçlanır. Ancak örtülü yazıda taşıyıcı saklanan bilginin iletilmesi amacıyla kullanılırken, sayısal damgalama da ise taşıyıcıya kendisiyle ilgili bilgi saklanır. Amaç bakımından sayısal damgalama yöntemlerinde, çalışma ile birlikte çalışmaya damgalanan bilginin her zaman taşınması da istenir. Bu nedenle bilgisayar ortamındaki çalışmalara telif hakkı, lisans, logo vb. bilgiler damgalanır. Damgalama yöntemlerinin geliştirilmesinde, sayısal çalışmalara damgalanan bilginin çeşitli saldırılara karşı dayanıklı olması da öncelikli amaçlardan biri olarak göz önünde tutulurken örtülü yazı uygulamalarında böyle bir beklenti yoktur [2].

2.2.4. Parmak İzi Ekleme, Etiketleme (Fingerprinting, Labelling)

Etiketleme olarak da adlandırılan parmak izi ekleme, bir sayısal çalışmayı diğerlerinden ayırmak amacıyla kullanılan yöntemlerden biridir. Örneğin, sayısal bir ürünün müşteriye verilmesi öncesinde, telif haklarının korunması amacıyla, yalnızca o müşteriyi temsil eden bir bilginin ürüne görünmez bir şekilde damgalanmasıdır. Etiketleme için kullanılan yöntemde bilgi, dışardan yapılan çeşitli saldırılara karşı dayanıklıdır. Böylece her müşteriye, içinde kendisine özel bir bilginin saklandığı bir ürün verilir [8]. Sayısal ürünlerin kopyalanarak çoğaltılmasının çok kolay olduğu bilgisayar dünyasında, yasadışı olarak ürünlerin kullanılmasında ve takibinde bu yöntem önemli avantajlara sağlamaktadır. Parmak izi ekleme, amaç bakımından sayısal damgalamadan farklı ancak yöntem olarak sayısal damgalama ile aynı özellikleri gösterir.

2.2.5. Sayısal İmzalama (Digital Signature)

Sayısal imzalama, bir doküman sahibinin kendi kişisel anahtarı (private key) ile dokümanı imzalaması yani şifrelemesidir. Bu kişisel anahtardan üretilen kamusal anahtar (public key), dokümanın gönderileceği alıcı tarafında bulunur ve dokümanı açmakta kullanılır. Sayısal imzalama, kişisel ve kamusal anahtarın kullanıldığı damgalama olarak tanımlanabilir. Bir kişisel anahtar ile imzalanan doküman, sahibi hakkında bilgi de birlikte taşımış olur [9]. Kişisel anahtardan üretilen bir kamusal anahtar, dokümanın açılmasında kullanılır ve doküman sahibinin erişim yetkisi kontrolünü de elinde tutmasını sağlar. Sayısal imzalama bilgisayarlar kullanılarak yapılan iletişimde,

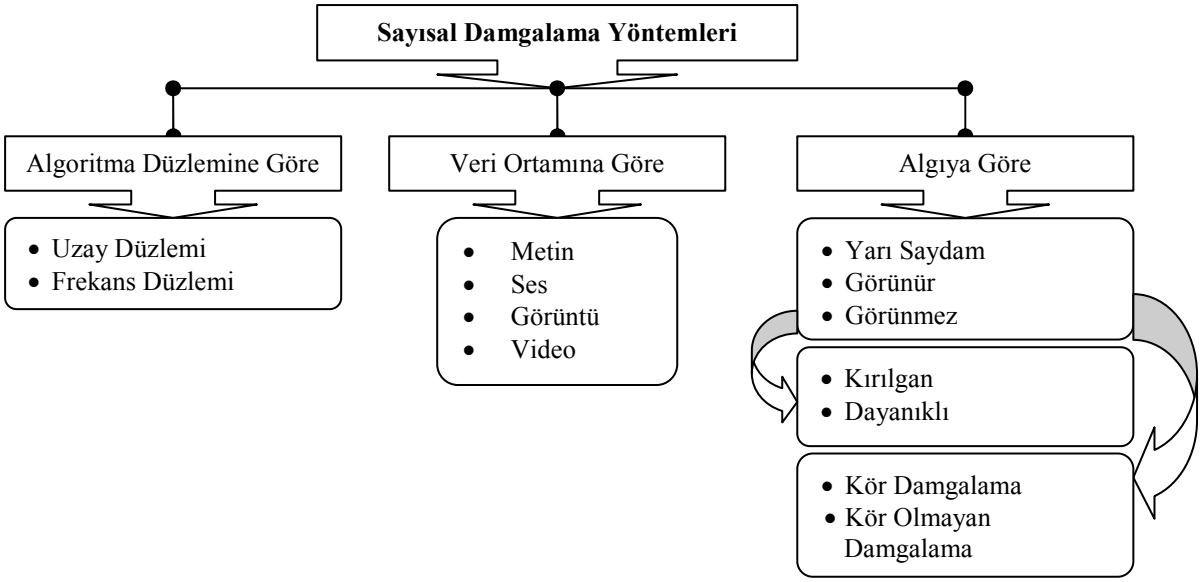
MD5 gibi şifreleme algoritmalarında sıklıkla kullanılmaktadır [10].

3. SAYISAL DAMGALAMA

Sayısal damgalama; sayısal ürünlerin yasadışı kopyalama yoluyla çoğaltılmasına ve Internet altyapısının sunduğu imkanlarla dağıtılmasına karşı ürün sahibinin haklarının korunması için önerilen yöntemlerin içinde ilk sıralarda yer almaktadır.
Sayısal damgalama kullanarak sayısal ürünün içeriğine çeşitli amaçlarla bilgi saklanır. Saklanan bilginin, ürün ile birlikte taşınması, gerektiğinde geri elde edilerek kullanılması amaçlanır. Özellikle telif haklarının korunmasının amaçlandığı sayısal damgalama yöntemleri, sayısal ürünün içeriğinin doğrulanması gibi çeşitli alanlarda da kullanılmaktadır.

3.1. Sayısal Damgalama Yöntemleri

Literatürde çeşitli amaçlara yönelik birçok damgalama yöntemi önerilmiştir. Bu yöntemler, algoritmalarının gösterdiği çeşitli özellikler bakımından birbirinden ayrılır.



Sayısal damgalama yöntemleri ilk olarak damgalama algoritmasının çalıştığı düzleme göre iki ana grupta incelenebilir. Uzay düzleminde çalışan algoritmalarda damgalama işlemi doğrudan pikseller üzerinde değişiklikle yapılırken frekans düzlemindeki damgalama için öncelikle görüntü frekanslarına ayrılır. Dönüştürme araçları olarak Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), Fast Fourier Transform (FFT) literatürde kullanılmıştır. Bunlar arasında özellikle DCT, çeşitli avantajlarından dolayı görüntü damgalama yöntemlerinde öncelikli tercih edilen dönüştürme aracıdır [7,9,11,12,17,18]. Frekans düzleminde damgalama için gerekli değişiklerin yapılmasının ardından ters dönüştürme yapılarak yeni piksel yoğunlukları hesaplanarak damgalama işlemi tamamlanır.
Literatürde, her iki düzleminde birlikte kullanıldığı sayısal görüntülerin damgalanması için önerilen bir yöntemde, damga için seçilen filigran ikiye ayrılmakta, bir kısmı uzay düzleminde bir kısmı da DCT kullanılarak elde edilen frekans bileşenlerine damgalanmaktadır [24]. Böylece, görüntüye daha fazla bilgi damgalanması amaçlanmaktadır.
Damgalanan veri türüne göre algoritmalar metin, ses, görüntü ve video olmak üzere 4 grupta toplanabilir, Bunlar arasında görüntü, hem kopyalanması hem de değişiklik yapılması en kolay veri türü olduğundan, sayısal görüntüler üzerine literatürde birçok damgalama yöntemi önerilmiştir.
Damgalama yöntemleri, algılanma derecesine göre yarı saydam, görünür ve görünmez olarak üçe ayrılabilir. Yarı saydam damgalama işleminde damga bilgisi yarı saydam olarak görüntü ya da video üzerinde yer alır. Görünür olarak damgalama yöntemleri ise, damga net bir şekilde görülür. Buna örnek olarak televizyon kanallarının ekran üzerindeki logosu gösterilebilir. Ancak görünmez olarak yapılan damgalamalarda, damga bilgisi gözle görülemeyecek derecede değişiklikle yapılır.
Görünmez damgalama algoritmaları kendi içinde ikiye ayrılır: dayanıklı ve kırılgan. Dayanıklı damgalama algoritmalarında damganın kendisini yok edecek saldırı niteliğindeki değişikliklere karşı dayanıklı olması, tanınabilir nitelikte geri elde edilebilmesi amaçlanır. Kırılgan damgalama algoritmalarında ise damga en küçük değişiklikte zarar görecek bir yapıya sahiptir. Kırılgan yapılı damgalama yöntemleri, veri üzerinde değişiklik olup olmadığının tespiti (content authentication) için önerilmektedir [13].
Damgalama yöntemleri genel olarak iki ana algoritmadan oluşur. Bunlar damgalama algoritması ve geri elde etme algoritmasıdır. Damgalanacak veri,

damga ve isteğe bağlı olarak özel ve kamusal anahtarlar damgalama algoritmasında kullanılır.
Görünmez damgalama yöntemleri geri elde algoritmasına göre iki ayrı gruba ayrılır. Damgalanmış görüntüden damganın geri elde edilmesinde asıl görüntünün kullanıldığı yöntemler "kör olmayan damgalama" olarak adlandırılır. Asıl görüntünün kullanılmadığı geri elde etme algoritmasının olduğu yöntemler "kör damgala" yapmaktadır.
Görünmez damgalama algoritmalarında sayısal görüntüdeki değişikliğin ölçülmesinde genellikle üç ölçü biriminden faydalanılmaktadır. Bunlardan MSE (Mean-Square Error) damgalanmış görüntü ile asıl görüntü arasındaki hatayı gösterirken, PSNR (Peak-to-Signal Noise Ratio) damgalanmış görüntünün kalitesinin ölçümünde kullanılmaktadır. Damgalanmış görüntünün kalitesi 30–40 dB arasında olan görüntüler kaliteli olarak kabul edilirken bunun üzerindeki değerler yüksek kaliteli damgalanmış görüntülerdir [18]. Ayrıca geri elde edilen damganın aslına olan benzerliğinin ölçümünde NC (Normalized Correlation) sıklıkla tercih edilmektedir. NC ölçümü 1 çıkan damga aslı ile aynı olarak kabul edilir. Bunların dışında, piksel tabanlı kalite ve bozulmanın ölçüldüğü birçok ölçü tekniği de mevcuttur [19].

3.2. Sayısal Görüntülerde Damgalama Uygulamaları

Sayısal görüntüler üzerine yapılan ilk damgalama çalışmaları, bilgisayar ve bilgisayar ağlarının gelişmesiyle ortaya çıkan telif haklarının korunması amacıyla yapılmıştır [14]. Daha sonra yapılan çalışmalarda, geliştirilen yöntemlerin farklı sorunlara çözüm olarak önerildiği görülmektedir.

3.2.1. Telif Haklarının Korunması (Copyright))

Telif hakkı bilgisinin açıkça ortaya konması amacıyla yapılan damgalama yöntemlerinde bilgi, kolaylıkla fark edilebilecek bir şekilde damgalanır. Buna örnek olarak televizyon kanallarının logosu yada haber ajanslarının çektiği görüntülerde yer alan ajans logosu gösterilebilir. Bu yöntem, sabit görüntülerde logonun kırpma yoluyla ayrılmasının kolaylığı nedeniyle dezavantajlıdır. Buna yakın olarak, yarı saydam şekilde logonun görüntünün anlamlı bölümü üzerine yerleştirilmesi de tercih edilen yöntemlerden biridir. Bu yöntemle yapılan damgalama sonunda logonun kırpılma yoluyla yok edilmesi görüntüyü de anlamsız yapacağından başarılı olarak değerlendirilebilir. Ancak, görüntünün anlam bütünlüğü üzerindeki olumsuz etkisi nedeniyle dezavantajlıdır.
Görünür ve görünmez damgalama algoritmalarından başka bunların beraber kullanıldığı bir çalışmada sayısal görüntü önce görünür bir algoritma ile damgalanmakta, ardından görünmez olarak damgalanmaktadır [23].
Sayısal görüntü ve video gibi ürünlerde telif haklarının korunması amacıyla yapılan çalışmalarda görünmez damgalama yöntemleri daha sık görülmektedir. Bunun nedeni, damgalama sonucunda elde edilen ürünün aslıyla olan farkının belli olmaması, bilginin saklanmasında kullanılan algoritmanın bilinmemesi ve bilginin saklandığı yerin belli olmaması gibi avantajlara sahip olmasıdır [7].
Literatürde yer alan birçok görünmez damgalama algoritmasında frekans düzlemi kullanılmıştır. Özellikle sabit görüntüler için sıklıkla tercih edilen kayıplı JPEG sıkıştırmasından gizlenen damga bilgisini korumak amacıyla DCT tercih edilmektedir [7,11,16,17,18]. DCT ile yapılan damgalama algoritmalarında görüntü öncelikle frekans bileşenlerine ayrılır. Bunun için görüntü 8×8 piksel boyutlarında bloklara ayrılarak her bloğun frekansları ayrı ayrı hesaplanır. Buradan elde edilen bir DC ve 63 AC frekansın katsayılarında önerilen yönteme göre değişiklikler yapıldıktan sonra ters dönüştürme uygulanarak damgalanmış görüntü elde edilir. Değişikliklerin yapılacağı frekansların seçiminde, JPEG kayıplı sıkıştırmasının etkisi ve görüntüde oluşacak bozulmanın da minimumda tutulması önemli rol oynar. Bunun için sadece orta frekans bandından seçimin yapıldığı çalışmalar [7,11,17] kadar bu seçimin genetik algoritma ile yapıldığı çalışmalar da literatürde mevcuttur [18].

3.2.2. *Yasadışı Kopyalamaya Karşı Koruma*

Damgalama algoritmalarının kullanım alanlarından biri de kopyalama yoluyla ürünlerin çoğaltılmasıdır. Özelikle sayısal içeriğin korunması ve takibinde önemli bir uygulama olan damgalama, hareketli görüntü (video) kayıtlarında kopyalamanın takibinde ve kısıtlanmasında kullanılmaktadır. Örnek olarak DVD (Digital Versetile Disk) içeriğinde mevcut alan damga gösterilebilir. DVD kayıt cihazları damga tespit eden bir mekanizma içerdiği takdirde, DVD içinde kayıtlı olan görüntülerin kopyalama iznini kontrol edebilir. Bu çözüm daha da ilerletilirse, "Kopyalanabilir", "Bir kez kopyalanabilir", "Kopyalanamaz" bilgilerini simgeleyen bir verinin video görüntüsünün çeşitli bölümlerine eklenmesiyle de yapılabilir [20].

3.2.3. İçerik Doğrulama (Authentication)

Sayısal damgalama, sayısal ürünün içeriğinde yapılacak değişikliğin tespiti amacıyla kullanılabilir. Bu amaçla kırılgan yapılı damgalama algoritmaları seçilir. Sayısal ürün, üzerinde yapılacak en küçük değişiklikte bozulacak şekilde ürün damgalanır. Damganın bozulması, ürünün değiştirildiğini gösterir. Literatürde, medikal görüntülerde değişiklik olup olmadığı üzerine yapılan bir çalışmada yüksek kaliteli kırılgan yapılı damgalama yöntemi önerilmiştir [21]. LSB (Least Significant Bit) tabanlı yöntemde, damga bilgisi görüntü piksellerinin son bitlerine damgalanır. Böylece görüntüdeki bozulma minimumda olurken yüksek kalitede damgalanmış görüntü elde edilmiştir. Damgalanmış görüntüdeki damganın benzerlik ölçümü 1 çıktığı takdirde medikal görüntü hiçbir değişikliğe uğramamış, aksi takdirde değiştirilmiş olduğunu göstermektedir.

Bu konuda yapılan başka bir çalışmada, çeşitli amaçlarla kullanılan görüntüler için kişisel ve kamusal anahtar kullanımına dayalı içerik doğrulama yöntemi önerilmiştir [22]. Görüntü sahibinin kendi kişisel anahtarıyla damgaladığı görüntüden herhangi bir kişi kamusal anahtar kullanarak damgayı görüntüden geri uygun damgayı elde edebilir.

3.2.4. Bilgi Saklama

Gizli damgalama yöntemlerinde, damga bilgisi iletilecek bilgi olarak seçildiğinde örtülü yazıda (steganography) olduğu gibi görüntü ya da başka bir sayısal veri taşıyıcı olarak kullanılabilir. Görünmezliğin ve geri elde algoritmansın sadece alıcı ve gönderenin bildiğinden güvenli ve gizli bir iletişim yoludur.

3.3. Sayısal Görüntülerde Damgaya Yapılabilecek Saldırılar

Sayısal görüntüler için önerilen damgalama yöntemleri algıya göre incelendiğinde yarı-saydam, görünür ve görünmez olarak sınıflandırılır. Görünür damgalama da görüntünün üzerinde yer alan damga bilgisi kırpma yoluyla kolaylıkla görüntüden ayrılabilir ya da başkası ile değiştirebilir. Bu durum yarı-saydam olarak görüntünün anlamlı bölümüne yapılacak damgalamayla aşılabilir ancak literatürde, bu yöntemle yapılan damgalamadaki yarı-saydam damganın yok edilmesi amacıyla yöntem mevcuttur [15]. Telif haklarının korunması amacıyla yarı-saydam bir logo damgalanmış sabit görüntülere saldırı niteliğindeki bu yöntemle, logo görüntüden kaldırılıp orijinal görüntüye yakın nitelikte bir görüntü elde edilebilmektedir.

Görünmez damgalamalar, görünür ve yarı-saydam damgalamalara göre damganın yerinin bilinmemesi açısından kırpma ya da değişiklik yoluyla yapılacak saldırılar karşı daha dayanıklıdır. Ancak görünmez damgayı yok etmeye ya da tanınamayacak derecede bozmaya yönelik saldırılar da mevcuttur [19]. Bu saldırılar görüntünün kalitesinde olumsuz değişikliğe yol açmadan doğrudan damgayı hedef alan değişikliklere dayanır.

- JPEG kayıplı sıkıştırması,
- Geometrik saldırılar: açılı, yatay ve dikey eksende döndürme, ölçeklendirme, satır ve sütun silme, rasgele geometrik bozma
- Kalite üzerinde saldırılar: filtreleme, keskinleştirme, gürültü ekleme, yazdırma-tarama
- Stirmark: Sayısal görüntülerin damgalanması sonucunda dayanıklılığın tespiti için birçok saldırı tekniğini uygulayan bir uygulamadır. Stirmark saldırısı sonrasında elde edilen görüntülerdeki damganın benzerliği ölçülerek damgalama algoritmasının bu saldırıya karşı başarısı ölçülür [5].

4. SONUÇ

Bu çalışmada, veri saklama yöntemleri, sayısal alanda bu konuda yapılan önceki çalışmalar ve özellikle sayısal görüntülere uygulanan damgalama algoritmaları incelenmiştir. Literatürde önerilen bazı yöntemler örnek olarak sunulmuştur.

Çeşitli amaçlarla yapılan görüntü damgalama algoritmaları ayrıntılarıyla açıklanmış ve damgayı yok etmeye veya bozmaya yönelik değişiklikler sıralanmıştır. Literatürdeki çalışmalarda sayısal görüntüler için, tüm saldırılara karşı dayanıklı bir damgalama algoritması beklenmemekte, hedef doğrultusunda başarılı bir yöntem geliştirme amaçlanmaktadır.

5. KAYNAKLAR

[1] ANONİM, 2007. Image Steganography and Steganalisys. http://www.ims.nus.edu.sg/Programs/imgsci/files/memon/sing_stego.pdf

[2] KATZENBIESSER, S., PETITCOLAS, F., 2000. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, 237, London.

[3] CHEN, P. C., 1999. On the Study of watermarking Application in WWW–Modeling, Performance Analysis and Application of Digital Image Watermarking Systems. Master Thesis, National Tsing Hua University, 127 s, Hesinchu, Taiwan.

[4] JOHNSON, N. F., JAJODA, S., Exploring Steganography: Seeing the Unseen. IEEE Computing Practices, 2: 26-34, 1998.

[5] PETITCOLAS, A. P., ANDERSON, R. J., KUHN, M. G., Attacks on Copyright Marking Systems, Second International Workshop, IH'98, 1998, 219-239, Oregon, USA.

[6] PETITCOLAS, A. P., ANDERSON, R. J., KUHN, M. G. Information Hiding – A Survey, Proceedings of the IEEE, 87(7):1062-1078, July 1999.

[7] HSU, C. T. and WU, J.W. Hidden Digital Watermarks in Images, IEEE Transaction on Image Processing, 8 (1): 58-68, 1999.

[8] ARNOLD, M., SCHMUCKER, M., WOLTHUSEN, S. D., 2003. Techniques and Applications of Digital Watermarking and Content Protection, Artech House, 273, London.

[9] MOHANTY, S. P., Digital Watermarking: A Tutorial Review, Technical Report, Dept. of Electrical Engineering, Indian Inst. of Science, Bangalore, India, 1999 (Yayınlanmamış).

[10] TIPTON, H. F., KRAUSE, M., 2006. Information Security Management Handbook. Auerbach Publications, 3280, New York.

[11] PAI, Y. T., RUAN, S. J., Low Power Block-Based Watermarking Algorithm, IEICE Trans. Inf. & Syst. Vol. E89-D, No.4, April 2006.

[12] PODILCHUK, C. I., DELP, E. J. Digital Watermarking: Algorithms and Applications, IEEE Signal Processing Magazine, Vol. 18 (4): 33–46, July 2001.

[13] KONG, X., FENG, R., Watermarking Medical Signals for Telemedicine, IEEE Trans. on Information Technology in Biomedicine, Vol. 5, No. 3, 195-201, 2001.

[14] WOLFGANG, R. B., DELP, E. J., A Watermark for Digital Images, IEEE International Conference on Image Processing, ICIP'96, Lausanne, Switzerland.

[15] HUANG, C. H., WU, J. L., Attacking Visible Watermarking Schemes, IEEE Transaction on Multimedia, Vol. 6, No. 1, 16-30, 2004

[16] PAI, Y. T., RUAN, S. J., A High Quality Robust Digital Watermarking by Smart Distribution Technique and Effected Embedded Scheme, IEICE Trans. Fundamentals, Vol.E90–A, No.3 March 2007.

[17] WANG Q., SUN, S., DCT-Based Image-Independent Digital Watermarking, WCCC-ICSP 2000. 5th Int. Conference on Signal Processing, Vol. 2, 942 - 945 21-25 Aug. 2000.

[18] SHIEH, C. S., HUANG, H. C., WANG, F. H., PAN, J. S., Genetic Watermarking Based on Transform Domain Techniques, The Journal of the Pattern Recognition, 37, 555-565, 2004.

[19] KUTTER, M., PETITCOLAS, F. A. P., A Fair Benchmark for Image Watermarking Systems, Electronic Imaging'99 Security and Watermarking of Multimedia Contents, Vol. 3657, January 1999, USA.

[20] MUHAREMAGIC, E., FURHT, B., Survey of Watermarking Tecniques and Applicayions, http://www.cse.fau.edu/~borko/Chapter7,%20Hdbk%20of%20MM%20Security.pdf

[21] WANG, G., RAO, N., A Frigile Watermarking Scheme for Medical Image, IEEE Engineering in Medicine and Biology 27th Annual Conference, September 2005, Shanghai, China.

[22] WANG, P. W., A Public Key Watermark for Image Verification and Authentication, Proc. In IEEE Int. Conference on Image Processing, Vol. I, October 1998, 455-459, Chicago, USA.

[23] MOHANTY, S. P., RAMAKRISHNAN, K. R., KANKANHALLI, M., A Dual Watermarking Technique for Images, Proceedings of 7th ACM International Multimedia Conference, ACMM-MM'99, 1999, 49-51, Orlando, USA.

[24] SHIH, F. Y., WU, S. Y. T., 2003. Combinational Image Watermarking in the Spatial Domain and Frequency Domains, The Journal of Pattern Recognition, 36 (2003): 969-975.