T.C.
TRAKYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SAYISAL DAMGALAMA KULLANIMI VE TELİF HAKLARINI KORUMADA GÜVENİLİRLİĞİ

SİNAN SERBESTOĞLU

YÜKSEK LİSANS TEZİ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

Tez Danışmanı: Dr. Öğr. Üyesi Andaç ŞAHİN MESUT

EDİRNE-2019

SİNAN SERBESTOĞLU'nun hazırladığı "SAYISAL DAMGALAMA KULLANIMI VE TELİF HAKLARINI KORUMADA GÜVENİLİRLİĞİ" başlıklı bu tez, tarafımızca okunmuş, kapsam ve niteliği açısından Bilgisayar Mühendisliği Anabilim Dalında bir Yüksek lisans tezi olarak kabul edilmiştir.

Jüri Üyeleri (Ünvan, Ad, Soyad):	İmza
Dr. Öğr. Üyesi Andaç MESUT (Danışman)	.....
Doç. Dr. M. Tolga SAKALLI	.....
Dr. Öğr. Üyesi H. Nusret BULUŞ	.....

Tez Savunma Tarihi: 23/08/2019

Bu tezin Yüksek Lisans tezi olarak gerekli şartları sağladığını onaylarım.

İmza

Dr. Öğr. Üyesi Andaç MESUT

Tez Danışmanı .....

Trakya Üniversitesi Fen Bilimleri Enstitüsü onayı

.....

Prof. Dr. Murat YURTCAN

Fen Bilimleri Enstitüsü Müdürü

T.Ü. FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ YÜKSEK LİSANS PROGRAMI

DOĞRULUK BEYANI

Trakya Üniversitesi Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında, tüm verilerin bilimsel ve akademik kurallar çerçevesinde elde edildiği, kullanılan verilerde tahrifat yapılmadığını, tezin akademik ve etik kurallara uygun olarak yazıldığını, kullanılan tüm literatür bilgilerinin bilimsel normlara uygun bir şekilde kaynak gösterilerek ilgili tezde yer aldığını ve bu tezin tamamı ya da herhangi bir bölümünün daha önceden Trakya Üniversitesi ya da farklı üniversite tez çalışması olarak sunulmadığını beyan ederim

23/08/2019

Sinan SERBESTOĞLU

İmza

Tezli Yüksek Lisans

Sayısal Damgalama Kullanımı ve Telif Haklarını Korumada Güvenilirliği

Trakya Üniversitesi Fen Bilimleri Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

ÖZET

Analog teknolojilerden sayısal teknolojilere geçiş sayısal ortamda saklanan dosyaların içeriklerinin korunmasını ve aynı zamanda içeriğin değiştirilmemesi için önlemler alınması konusunu beraberinde getirmiştir. Her türlü sayısal içerik sahipleri, telif haklı multimedya içeriğinin korunması için yeni teknolojiler istemektedir. Multimedya koruması son yıllarda gündeme gelmiş ve bu konuyla ilgilenmek için araştırmacılar, sürekli olarak yeni, verimli ve etkin teknolojiler araştırmakta ve keşfetmektedirler. Sayısal ortamın getirdiği avantajla gelen çoğaltma ve kopyalama gibi işlemlerle bu sorun daha da önem kazanmıştır. Görüntüler üzerinde yapılan işlemlerde çoğaltma, kopyalama ve diğer tüm değişiklikler kolay bir hal almıştır. Görüntüye hak sahibinin imzası, eserin sahibinin logosu veya yapıldığı tarih gibi bir bilginin damgalanması sayısal görüntülerdeki telif haklarını korumak için yapılan uygulamalardandır. Damgalama, görüntü üzerine insan gözünün görebileceği veya göremeyeceği şekilde bir yöntem seçilerek uygulanır.

Bu çalışmanın amacı, sayısal ortamındaki görüntülere gizli bir bilgi damgalanması (filigran) ile telif haklarını korumada güvenirliğini ortaya çıkarmaktır. Bu amaçla damga eklemek için kullanılan yöntemler açıklanacak ve yöntemlerin içeriği korumada ne kadar başarılı oldukları değerlendirilecektir.

Yıl: 2019

Sayfa Sayısı: 72
Anahtar Kelimeler: Damgalama, Sayısal imge damgalama, Telif hakkı koruma

Master Thesis

The Use of Watermarking and it's Reliability in Copyright Protection

Trakya University Institute of Natural Sciences

Computer Engineering Department

ABSTRACT

The transition from analogue technologies to digital technologies has brought about the protection of the contents of files stored in digital media and at the same time taking measures to prevent the content from being changed. All kinds of digital content owners are seeking new technologies to protect copyrighted multimedia content. Multimedia protection has come up in recent years and researchers are constantly exploring and exploring new, efficient and efficient technologies to address this issue. In particular, the replication and replication operations provided by the digital environment have further increased the importance of this problem. Making changes, copying and duplication of images has become extremely easy. One of the works for the protection of copyright in digital images is the stigmatization of images such as the signature of the work owner, the date of the work or the logo of the company. This information can be imprinted visually on the carrier image or by a technique that the human eye cannot detect.

The aim of this study is to reveal the reliability of copyright protection by watermarking confidential information on images in digital media. For this purpose, the methods used to add stamps will be explained and how successful the methods are in preserving the content.

Year: 2019

Number of Pages: 72

Keywords: Watermarking, Digital Image Stamping, Copyright Protection

TEŞEKKÜR

Eğitimim süresince her zaman güler yüzüyle bana destek olan hiçbir konuda yardımlarını esirgemeyen, tez çalışmasının planlanması ve yürütülmesinde bilgisinden yararlandığım sevgili danışmanım Dr. Öğr. Üyesi Andaç MESUT hocama, diğer dersini aldığım ve tanışabildiğim tüm Bilgisayar Mühendisliği Anabilim Dalı öğretim üyelerine, tezim için bana hep destek olan biricik eşim Gülseren SERBESTOĞLU ve kızım İnci'ye, eğitim için her zaman beni motive eden canım anneme sonsuz teşekkürler.

İÇİNDEKİLER

ÖZET iv

ABSTRACT vi

TEŞEKKÜR viii

İÇİNDEKİLER ix

KISALTMALAR VE SİMGELER DİZİNİ xii

ŞEKİLLER DİZİNİ xiii

ÇİZELGELER DİZİNİ xiv

BÖLÜM 1 1

GİRİŞ 1

BÖLÜM 2 4

DAMGALAMA HAKKINDA GENEL BİLGİLER 4

2.1 Damgalama Nedir? 4

2.2 Steganografinin ve Damgalamanın Tarihçesi 8

2.3 Steganografi ile İlgili Yapılmış Çalışmalar 10

2.4 Sayısal Damga ile İlgili Yapılmış Çalışmalar 11

2.5 Damgalama Gereksinimleri 13

2.6 Damgalama Uygulamaları ve Kullanım Alanları 14

BÖLÜM 3 17

DAMGALAMA YÖNTEMLERİ ve SINIFLANDIRILMASI 17

3.1. Algıya Göre Sınıflandırma 18

1.1.1. Görünür Damgalama 20

1.1.2. Görünmez Damgalama 22
1.1.3. Yarı Saydam Damgalama 26
3.2. Veri Ortamına Göre Sınıflandırma 26
3.2.1. Metin Damgalama 27
3.2.2. Ses Damgalama 28
3.2.3. Görüntü Damgalama 30
3.2.4. Video Damgalama 30
3.3. Algoritma Düzlemine Göre Sınıflandırma 31
3.3.1. Uzay Düzlemi 31
3.3.2. Frekans Düzlemi 31
BÖLÜM 4 34
GÜVENLİK VE DAYANIKLILIK 34
4.1. Basit Saldırılar 35
4.2. Kaldırma Saldırıları 36
4.3. Geometrik Saldırılar 36
4.4. Kriptografik Saldırılar 37
4.5. Protokol Saldırıları 37
BÖLÜM 5 38
SAYISAL ÇAĞDA TELİF HAKKI KORUMASI 38
5.1. Fikri Mülkiyet Haklarına (IPR) Genel Bakış 38
5.1.1. Tanımlı Fikri Mülkiyet Hakları 39
5.2. SAYISAL ÇAĞDA TELİF HAKKI 39
5.2.1. Telif Hakkı ve İnternet 40
5.2.2. İnternette telif hakkı ihlali 40
5.2.3. ABD Telif Hakkı Yasası 41

5.2.4. Avrupa Birliği (AB) Telif Hakkı Yasası 41
5.3. İNTERNET TELİF KANUNU VE KORSANLIĞI 43
5.4. SAYISAL TELİF HAKKI KORUMASINDA DAMGALAMA 44
BÖLÜM 6 47
SONUÇ VE ÖNERİLER 47
KAYNAKLAR 50
ÖZGEÇMİŞ 58

KISALTMALAR VE SİMGELER DİZİNİ

DCT	: Discrete Cosine transform
DWT	: Discrete Wavelet Transform
DFT	: Discrete Fourier Transform
FFT	: Fast Fourier Transform
LSB	: Least Significant Bit
SVD	: Singular Value Decomposition
HVS	: Human Visual System
DVD	: Digital Compact Disk
IPR	: Intellectual Property Rights
IP	: Intellectual Property
DMCA	: Digital Millennium Copyright Act
RIAA	: Recording Industry Association of America
IFPI	: International Federation of the Phonographic Industry
SNR	: Signal to Noise Ratio
PNSR	: Peak Signal to Noise Ratio
LAN	: Local Area Network
PAN	: Personal Area Network
WAN	: World Area Network
DRM	: Digital Rights Management
PDA	: Personal Digital Assistant
CD	: Compact Disk

ŞEKİLLER DİZİNİ

Şekil 2.1 Sayısal Damga Gömme İşlemi.....5

Şekil 2.2 Sayısal Damgayı Elde Etme İşlemi.....5

Şekil 2.3 Kağıt Filigran Uygulaması.....10

Şekil 3.1 Sayısal Damganın Sınıflandırılması 20

Şekil 3.2 Görünür Damga Uygulaması 21

Şekil 3.3 Görünmez Damga Uygulaması.....191

Şekil 4.1 Sayısal Damga Güvenliği 37

ÇİZELGELER DİZİNİ

Çizelge 3.1 Algıya Göre Sınıflandırma Özellikleri 19

Çizelge 3.2 DFT, DCT ve DWT algoritmaları 32

BÖLÜM 1

GİRİŞ

Bilgisayarların hayatımıza girmesiyle birlikte farklı türdeki birçok bilgi sayısal ortamda saklanmaya başlamıştır. Kullanıcılar çeşitli programlar vasıtasıyla metin, görüntü, video ve değişik multimedya dosyalar yaratabilir hale gelmişlerdir. İnternet ile birlikte yarattıkları bu içerikleri başkaları ile paylaşmaya başlamışlardır. İnternetin çok yaygın hale gelmesi ve multimedya teknolojilerindeki başarılı teknikler, yaratıcılık konusunda öncülük etse de kullanıcılar için içeriklerini güvence altına alma konusunda bir takım sorunlar yaratmıştır. Multimedya teknolojisini kullanmanın tehditleri arasında telif hakkı koruması, multimedya genel güvenliği ve multimedya içeriğinin doğrulanması bulunur. Ancak, telif hakkı koruması multimedya içeriğine tehdit oluşturan en önemli sorunlardan biridir (Barni, Bartolini, Cox, Hernandez & Perez-Gonzalez, 2001).

Yarı iletkenlerin kullanımı ile başlayıp hızla gelişen ve hayatımızı kolaylaştıran ürünler bugün hayal edemeyeceğimiz bir noktaya gelmiştir. Sayısal kamera ve fotoğraf makineleri, cep telefonları, tabletler, drone'lar ve giyilebilir teknolojiler maliyetlerin ve internet hızlarının artması sonucu hayatımızın her noktasına girmiştir. Ses, resim ve video gibi bu ürünlerin artması sonucu üretimi ve paylaşımı kolaylaşan içeriklerin telif haklarının korunması sorunuyla karşılaşılmıştır (Emek, Pazarcı & Yücel, 2004).

İnternetin hızlı bir şekilde genişlemesi, kullanıcıların ses, görüntü ve video formatındaki sayısal verilere erişimini kolaylaştırmış ve sayısal verilerin yayılmasını hızlandırmıştır. Yayıncıların, sanatçıların ve fotoğrafçıların, güvenlik eksikliği nedeniyle internette eserlerini paylaşmak istemediği durumlar olmuştur.

Multimedya bilgilerinin güçlendirilmesi sorunu gittikçe daha önemli hale gelmiş ve birçok telif hakkı sahibi, verilerinin veya çalışmalarının yasadışı olarak çoğaltılmasını engellemek için çeşitli önlemler almak zorunda kalmıştır.

Çalışma sahiplerinin telif haklarının korunması amacıyla yapılan araştırmalarda, steganografi uygulamalarına benzer bilgi saklama yöntemleri geliştirilmiştir. Bunlardan bazıları, çalışma ya da sahibinin hakkında bilgi içeren sayısal imza (digital signature), etiket (label) ya da sayısal damga (watermark) olarak gösterilebilir (Mohanty, Barni, Bartolini, Cappellini, & Piva, 1998).

Sayısal damgalama, multimedya içerikleri içinde görünmez veya duyulamayan verileri gömmek için kullanılan bir tekniktir. Sayısal damgalama bir kimlik koduna sahip sayısal bir belgenin kaynağını, yazarını, yaratıcısını, sahibini ve dağıtımcısını veya yetkili tüketicisini tanımlamayı mümkün kılar. Sayısal damgalama, içerik kullanıcılarının yasadışı kopyalama, çoğaltma ve bir ağ ortamında dağıtımını engellemenin etkili bir yolu olarak ele alınmaktadır.

Genelde telif hakkı koruması için bir sayısal damgalama tekniğinin iki özelliği sağlaması gerekmektedir. Birinci özellik gömülen damganın, imge verisini görünür bir şekilde ve ses verisini duyulur bir şekilde bozmamasıdır. Yani damga; imge için görülemez, ses için duyulamaz olmalıdır. İkinci özellik ise damganın yetkisiz kişiler tarafından elde edilemez olmasıdır. Damganın şekilsel bozulmalara ve genel işaret işlemeye karşı dayanıklı olması beklenir (Erçelebi, Tokur & Bayık, 2002).

Görsel verileri korumak için mümkün olan birçok yaklaşımdan, sayısal damgalama, muhtemelen en çok ilgi çeken alanlardan biridir. Görüntülerin sağlam bir şekilde damgalanması fikri, görüntü içindeki bilgi verisini insan görsel sistemi için anlaşılmaz bir biçime, ama ortak görüntü işleme operasyonları gibi saldırılardan elde edilen verilere gömmek şeklindedir. Amaç, bir insan gözü için tamamen aynı görünen bir görüntü üretmektir; ancak, eğer gerekli ise, sahibinin anahtarı ile karşılaştırıldığında, pozitif doğrulamaya izin verir.

2007 yılında yapılan bir araştırmada 131 milyon $ bir paya sahip bu teknolojinin 2018 yılı için 1 milyar $ değere sahip olacağı söylenmiş ve

damgalamanın gelecekte önemli bir teknoloji olacağı düşünülmektedir (Anonim, 2008).

Bu çalışmanın amacı, sayısal ortamındaki görüntülere gizli bir bilgi damgalanması (filigran) alanını incelemektir. Ayrıca damgalama gereksinimleri, yöntemleri, sınıflandırması, saldırı türleri ve sayısal çağda telif hakkı kanunları incelenip bunların telif haklarını korumada güvenirliğini ortaya çıkarmak amaçlanmaktadır.

BÖLÜM 2

DAMGALAMA HAKKINDA GENEL BİLGİLER

2.1 Damgalama Nedir?

Damga genellikle resim, sayfa, kağıt gibi nesnelerin üzerine yerleştirilmiş özel işaret veya simgedir. İçerik koruma ve telif hakkı koruma amacıyla yapılmaktadır. Damga kullanım yeri açısından ikiye ayrılır.

Kağıt Damga (filigran): Sadece kağıtlar üzerinde uygulanan ve özel ışıkla görünen ya da daha belirgin olan filigranlar.

Sayısal Damga (Dijital Filigran - Digital Watermark): Sayısal dosyalarda kullanılan filigranlar. (Metin, Görüntü, Video, Ses dosyaları) (Mesut,2019)

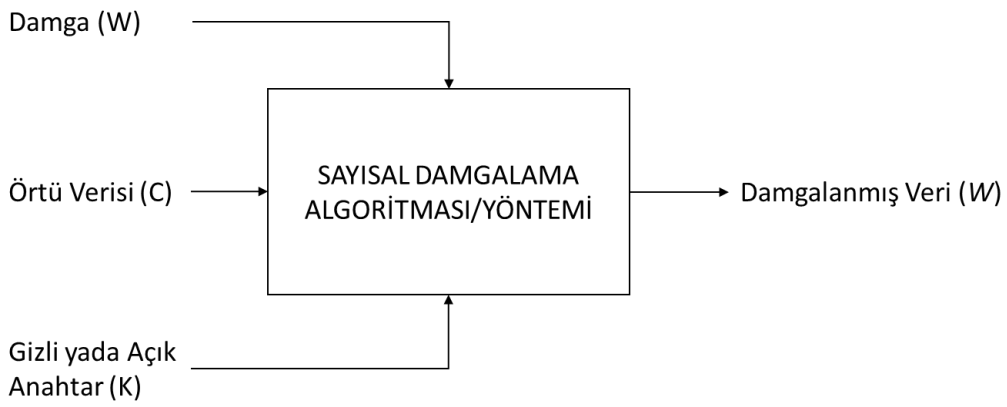
Damgalama, orijinal sinyalin kalitesini bozmadan güvenli bilginin taşındığı bir tekniktir (Ravula, 2010). Bu yöntem iki parçadan oluşur:

- Gömme Bloğu
- Çıkarma Bloğu

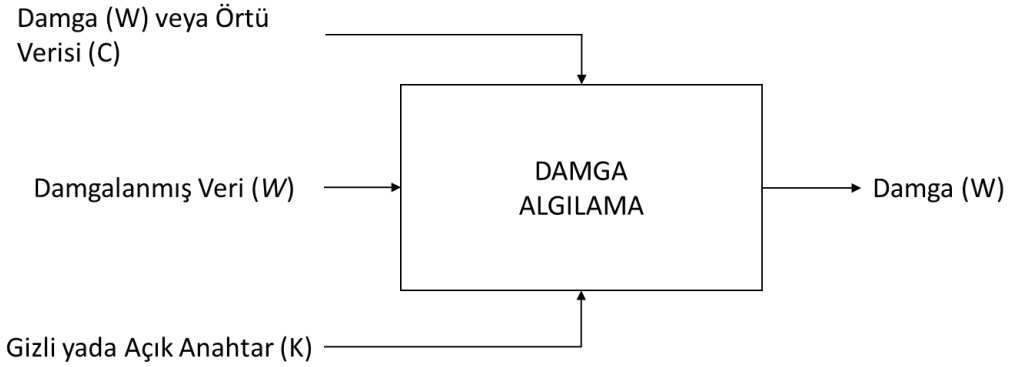
Sistem bir steganografi sisteminde olduğu gibi bir gömme anahtarına sahiptir. Anahtar, yetkisiz kullanıcıların verileri değiştirmesine veya çıkarmasına izin vermemek adına güvenliği artırmak için kullanılmıştır. Gömülecek nesne damga olarak bilinir. Damga; metin, rakamlar ya da bir görüntü olabilir. Damga yapılacak gömme ortamı orijinal sinyal veya örtü nesnesi olarak adlandırılır ve değiştirilmiş nesne gömülü sinyal veya damgalanmış veriler olarak adlandırılır (Kumar, 2004).

Şekil 2.1'de gösterilen gömme bloğu, giriş olarak damga, orijinal sinyal (veya kapak nesnesi) ve damgalama anahtarından oluşur. Sonuç olarak gömülü

sinyal veya damgalı veri oluşturulur. Şekil 2.2'de verilen çıkarma bloğu için girişler gömülü nesne, anahtar ve bazen damgadır (Kumar, 2004).



Şekil 2.1 Sayısal Damga Gömme İşlemi



Şekil 2.2 Sayısal Damgayı Elde Etme İşlemi

Başka bir tanıma göre damgalama, sayısal multimedya içeriğine bilgi katma işlemidir (Memon, Holliman, & Yeung, 1999). Sayısal damga basma, bilginin (damga dediğimiz) daha sonra kopya önleme ve kontrolü de dâhil olmak üzere çeşitli amaçlar için çıkarılabileceği veya algılanabileceği şekilde sayısal

multimedya içeriğine gömme işlemidir. Sayısal damgalama, damga basma tekniklerinin geliştirilmesi ve ticarileştirilmesi, sayısal içeriğin hızlı bir şekilde yayılmasının önündeki bazı zorlukların üstesinden gelmeye yardımcı olmak için aktif ve önemli bir araştırma alanı haline gelmiştir (Swanson, Kobayashi, & Tewfik, 1998).

Genel anlamda bakacak olursak, damgalama, şifreleme ve şifre çözme işlemlerinde bir gelişmedir. Sayısal damgalama, içeriğe doğrudan gizlenen ve insan tarafından duyusal olarak algılanamayan bir bilgi parçasıdır. Ancak, bilgisayar tarafından okunabilir. Bunun en büyük avantajı, içeriğin damgadan ayrılmaz olmasıdır. Damganın birkaç formu vardır (Srivadana, 2013);

İmzalar : Damga, içeriğin sahibini saptar. Bu bilgi, bir kullanıcı tarafından içeriği sahibinden yayınlamak için yasal haklar elde etmek için kullanılır.

Parmak İzi : Damgalar, parmak izi ile bu içeriğin alıcılarını belirlemede yardımcı olur, ayrıca yasadışı kopyaların kaynağının izlenmesinde de yardımcı olur. Parmak izi ve imzalar arasındaki tek fark, damgayı imzalamada içerik sahibini tanımlamasıdır. Parmak izinde, bilgisayarlar ve diğer görsel kanallar olan otomatik sistemler içeriği tanımlar. İçeriğin sahibine yasal olarak dağıtılmasını sağlar.

Kopya kontrolü : Damga, içerik sahibinin istediği kullanım ve kopyalama kuralları hakkında bilgiler içerir. Bu bilgileri içeren cümleler kopyalanamayacaktır.

İçerik korumak için çeşitli algoritmalar geliştirilmektedir fakat gürültü ve sağlamlık en büyük sorunlardır. Bu nedenle içerik korumak amacıyla sayısal damgalama teknikleri önem kazanmaktadır. Bu teknikle sayısal formata şifrelenmiş bilgilere sadece yetkili kişilerce ulaşılabildiğinden emin olabiliriz. Diğer tarafların orijinal verileri yok etmeden bu verilere erişmesi zorlaşır. Bu neredeyse görünür, kırılgan, desen eşleştirme, steganografi gibi damgalama olarak bilinen birçok yaklaşıma benzer.

Görünür damga basma tekniği, içeriği kodlamayan, böylece herkes tarafından kolayca okunabilen veya kopyalanabilen, oldukça tanıdık bir tekniktir. Gizlilik bu yöntemle sürdürülemez. İçerikle birlikte, görünür damgalar oluşturulmaktadır.

Steganografi, yalnızca uygun bir kanaldan erişilebilen şifreli içeriği gizleyen başka bir gizli damgalama yöntemidir. Bu iletişim kanalları da geri çekilebilir, böylece onu işe yaramaz hale getirir. Kırılgan damgalar bir şekilde, kodlanmış verilerin kolayca okunamadığı yerlere kıyasla en iyisidir, imzalar aracılığıyla içeriğe yalnızca kimliği doğrulanmış taraflarca erişilebilmektedir (Srivadana, 2013).

Steganografinin temel amacı m mesajını d örtü verisinin içine saklayarak d' verisini elde etmek ve insanlar tarafından d' içinde m'in tespit edilmemesini sağlamaktır. Damgalama işleminin ana amacı ise m mesajını d örtü verisinin içine saklayarak d' verisini elde etmek ve insanlar tarafından d' içinde m'in değiştirilmemesini ve kaldırılmamasını sağlamaktır. (Mesut,2019).

İhlal edilen telif hakkı içeriğini belirleme yeteneği ile kodlanan içeriğin konuşlandırılmasına karşı çalışan sayısal damga, telif hakkı materyaline kimliği doğrulanmış kullanıcılar tarafından kolayca erişilebilmesini sağlar. Bu, kolayca dönüştürülemeyen ve işlenemeyen sayısallaştırılmış veri olarak adlandırılabilir. Metin, resim gibi tüm formatlara gömülebilirler. Sesler ve videolar gibi damgalar, verilerin kendi aralarında tanımlanmasına izin verir ve içerik arasında bilgiyi sağlar. Bu damga insan tarafından algılanmaz, ancak bilgisayarlar tarafından okunabilir (Anderson, 1996). Makine tarafından okunabilen damgalar daha çok tercih edilir. Daha iyi kodlama için kendinden tanımlı olarak adlandırılabilecek eylemlerin okunmasına yardımcı olan aktif işaretlemenin yapılmasına izin verdiği için genel olarak gerekli olmayan okunabilir ve insandan daha iyidir. Herhangi bir içerik kaybı olmadan damga çıkartılamaz. Bayraklar, tetikleme bitleri, kopya kontrol bilgileri, seri numaraları, içerikle ilgili bazı kodlar gibi pek çok ilgili bilgiden oluşur. Bu sayısal damgaların yakın zamanda FBI'da filmlerin ve müziğin telif hakkı koruması konusunda birçok uygulaması vardır. Bunların damga yapımında yardımcı olması için seri numaraları vardır.

Veri kaybına, değişikliklere ve alt seçim türündeki problemlere dayanabilecek deneysel analizlerle onaylanmış birçok iyileştirme ve alternatif teknik vardır (Srivadana, 2013).

2.2 Steganografinin ve Damgalamanın Tarihçesi

Veri gizleme yöntemlerinin tarihi veri iletişimi kadar eskilere dayanmaktadır. MÖ 485-425 yıllarında yaşayan ilk yunan tarihçisi Heredot, Pers İmparatorluğu ve Yunan şehir devleti arasında yapılan savaşta gizli bir iletişim yöntemini anlatmıştır. Pers kralına gizli bir planı götürecek olan kişinin saçları tıraş edildikten sonra mesaj dövme ile kazınmış daha sonra saçlarının tekrar uzaması beklenmiş ve mesaj için doğal kamuflaj oluşturulmuştur. Taşıyıcı bu sayede yanında hiçbir şey bulunamadığı için rahatça seyahat etmiş ve hedefine vardığında saçlarını tekrar tıraş edip mesajını göstermiştir (Anonim, 2007).

Günümüzde de kullanılan görünmez mürekkep uygulamaları bilinen tarih kadar eskidir. MS 23-29 yılları arasında yaşamış Pliny bir yazı için bir bitkiye ait süt kullanarak saydam bir yazı yazdığını ve ardından kâğıt ısıtıldığında bu sütün kağıt üstünde koyu bir renk aldığını anlatmıştır. Bu da tarihte kullanılan ilk görünmez mürekkep uygulaması olarak karşımıza çıkmıştır (Anonim, 2007).

Rönesans döneminde yaşayan Johannes Trithemius ilk kriptoloji kitabını yazmıştır. Aynı dönemde Giovanni Battista Porta, gizli bir mesajın çok kaynamış bir yumurta ile nasıl taşınabileceğini tanımlamıştır (Anonymous, 2007). Bunların yanında steganografi alanında bilinen ilk eser, Johannes Trithemius tarafından yazılmış kitaptır (Johson ve Jajoda, 1998).

"Örtülü yazı" anlamındaki Steganography kelimesi, eski Yunanca'dan gelen bir kelimedir (Johson ve Jajoda, 1998). Steganographia terimi ilk olarak Trithemius'un el yazması kitabında geçmiştir (Katzenbiesser ve Petitcolas., 2007).

Steganografik yöntemler 1. ve 2. Dünya Savaşında da kullanılmıştır. Gizli bir mürekkep geliştiren kimyagerler bununla zararsız görünen bir mektupta birçok gizli mesaj gönderilebilir. Belge olarak görünen bilgi de gizli mesaj içerebilir. Belge açık şekilde gönderilir ve 3.şahıslar bunun normal bir bilgi olduğunu düşünür. Örnek olarak aşağıda 2. Dünya savaşında bir Alman casus tarafından gönderilen bir mesaj vardır (Kutucu ve Kaya, 2002).

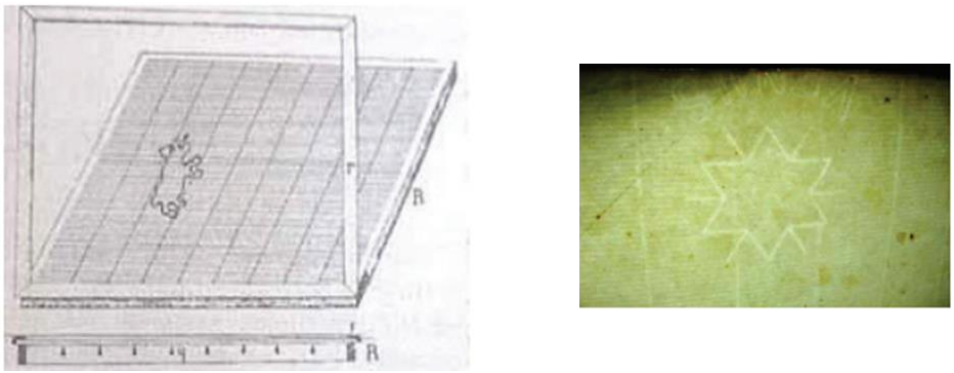
Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-product, ejecting suets and vegetable oils.

Her kelimeye ait 2. harfi seçersek "Pershing sails from NY June 1" mesajı karşımıza çıkmaktadır (Kutucu ve Kaya, 2002).

Kâğıt üzere uygulanan filigran ilk kez 1293 yılında İtalya'nın Fabriano kentinde kullanılmıştır. Damga bir pirinç telin değişik şekiller verilerek (daire, üçgen, haç vb.) bükülmesiyle oluşturulurdu. Şekil verilip bükülen tel kâğıt hamuru kalıbına konur ve hamura basılırdı. Basılan kısımdaki yoğunlaşma ile kâğıdı ışığa tuttuğumuzda bu kısım koyu bir şekilde görünürdü.

Banknot kâğıdı gibi elle yapılan kâğıtların üretiminde filigran yöntemi bugün de uygulanmaktadır. Bank of England, 1697 yılında damga içeren banknotları kullanmaya başlamıştır.

19.yüzyılda daha karmaşık ya da ayrıntılı desenli damgaların yapımına başlanmıştır. Bu tarz damgalarda, model bir mum üzerine çıkarılıp elektriksel bir yöntemle metal kalıplara aktarılırdı. Bu kalıpların birinde desen metalin içine oyulmuştur; diğerinde desen kalıpta kabartma biçiminde bulunur. Pirinç tel ile sıkça örülmüş bir kafes bu kalıplar arasına konur ve bunların üzerindeki model, bu tel kafese çıkıncaya dek kalıplar basınç altında tutulur. Ardından bu model kalıplar vasıtasıyla tel kafeste elde edilmiş olurdu. Elle kâğıt yapımında ise bu kâğıt hamuru tel kafes üzerine serilir ve suyu bu kafesten süzdürülür; sonuç olarak kafesteki modelin içerdiği desen, kâğıtta elde edilir. Bu tarz damga sadece elle yapılan kağıtlarda kullanılır ve çok net bir şekilde görülebilir. Şekil 2.3 bu uygulamayı ve sonuçta elde edilen damgayı göstermektedir. (Mesut,2019)



Şekil 2.3 Kağıt Filigran Uygulaması

Bilgisayar ve bilgisayar ağlarının gelişmesiyle ortaya çıkan güvenlik ve telif hakları sorunu için sayısal damgalama fikri ilk olarak 1990 yılının başında ortaya atılmıştır. O günden beri artan bir ilgi ile konu üzerinde araştırmalar yapılmaktadır.

Sayısal görüntülerin damgalanması üzerine ilk akademik konferans 1996 yılında organize edilmiştir. Bu konudaki ilk yayınlar TANAKA ve arkadaşları tarafından 1990 yılında yapılmıştır. 1995 yılından itibaren yayınlanan araştırmaların sayısında büyük bir artma görülmüştür. Sayısal görüntülerdeki damgalama çalışmaları, sonradan, ses ve video görüntüleri üzerine de yapılarak genişleyerek artmıştır (Chen, 1999).

2.3 Steganografi ile İlgili Yapılmış Çalışmalar

Kurak ve McHugh (1992), piksel değerlerindeki en önemsiz bitte değişiklik yaparak görüntü dosyaları üzerinde bir Steganografi yöntemi gerçekleştirmişlerdir.

Bender ve diğ. (1996), yazı, ses ve görüntü gibi farklı ortam türlerine bilgi gizlenebileceğini bildirmişlerdir.

Marvel, Bonceleti & Retter (1999), yayılı spektrum, hata kontrol kodlaması ve görüntü işleme yöntemleri ile bir veri gizleme işlemi gerçekleştirmişlerdir. Bu çalışmada alıcı ve göndericide anahtar bulunması durumunda, orijinal resim olmaksızın gizlenmiş veri elde edilebilmektedir.

Lee ve Chen (2000), LSB (Least Significant Bit) isimli teknik ile gri ton resimlerde piksellerin ilk dört biti ile yapılan değişiklik sonucu yüzde elliye yakın bir kapasite artışı sağlamış bir veri gizleme yöntemi geliştirmişlerdir.

Tseng ve Chang (2004), jpeg uzantılı resimleri kullanarak klasik yöntemlerde olduğu gibi Ayrık Kosinüs Dönüşümü (AKD) bileşenleri sabit büyüklükte veri gizlemek yerine, kapasite tahmin tablosuna göre gizledikleri yüzde yirmi daha yüksek kapasiteli bir yöntem önermişlerdir.

Reddy ve Raja (2009), çalışmalarında Ayrık Dalgacık Dönüşümü (ADD) alınıp güçlendirme temelli, yüksek kapasiteli ve güvenli bir veri gizleme yöntemi geliştirmişlerdir.

2.4 Sayısal Damga ile İlgili Yapılmış Çalışmalar

Son yıllarda sayısal multimedya teknolojilerindeki gelişmeler, internette bu teknolojilerin daha hızlı ve daha kolay kullanılması nedeniyle önem kazanmıştır. Daha fazla büyüme ve multimedya teknolojilerindeki başarılı teknikler, kullanıcılar için içeriklerini güvenceye alma konusunda birtakım sorunlar yaratırken önemli değişiklikler getirmiştir. Multimedya teknolojisini kullanmanın tehditleri arasında telif hakkı koruması, multimedya genel güvenliği ve multimedya içeriğinin doğrulanması multimedya içeriği için tehdit oluşturan en önemli problemler olarak görülmektedir. Bununla birlikte, telif hakkı koruması, multimedya içeriği için tehdit oluşturan en önemli sorunlardan biridir. (Barni vd., 2001).

Sayısal damgalama, verilerini güvence altına almak ve telif hakkı sorunlarını önlemek için operatörler tarafından kullanılan tekniklerden biridir. Damgalama, telif hakkı ve kimlik doğrulama ihlallerinden korunmak için verinin içine gizli bir kod veya sinyal yerleştirilen bir tekniktir (Langelaar, Gerhard, Setyawan & Lagendijk, 2000). Kod, içeriği güvenli hale getirirken içeriğin kalitesini etkilemeyecek şekilde gömülür. Sayısal damgalar, veri içine gömülü telif hakkı veya kimlik doğrulama sayısal kodundan oluşur. Bu kod, içerik kodu tespit etmek için belirli bir dedektörden geçinceye kadar sayısal içerikte görünmeden kalır (Zhang, Zhu & Fu, 2004).

Sayısal damgalama Müzik Şirketi'nin, almış olduğu patentle tarihteki yerini almıştır. Gerçekleştirilen bu patent çalışmasında müzik dosyalarına, telif haklarını korumak amacıyla bir kimlik kodu yerleştirilebileceği gösterilmiştir (Hembrooke, 1954).

Schyndel, Tirkel & Osborne (1994), uzay düzleminde gerçekleştirilen görüntünün en önemsiz bitinde değişiklik yaparak kolay gerçekleştirilen bir yöntem geliştirmişlerdir, fakat bu yöntem saldırılar karşısında oldukça zayıftır.

Koch, Rindfrey & Zhao (1996), orijinal görüntüyü 8x8'lik bloklara bölüp her bloğun AKD'sini alıp damga bilgisine göre orta frekans bölgesinde değişiklik yaparak çoklu ortam çalışmalarının telif hakkını koruma amaçlı bir çalışma gerçekleştirmişlerdir.

Cox, Kılıan, Leıghton & Shamoon (1997), sağlamlığı oldukça yüksek birçok çoklu ortam türünde uygulanabilecek bir veri gizleme yöntemi önermişlerdir.

Kutter, Jordan & Bosson (1997), renkli bir görüntü içerisine sadece mavi piksel değerlerinde değişiklik yaparak orijinal görüntüye gerek olmadan gizli verinin bulunabileceği bir yöntem geliştirmişlerdir.

Yeung ve Mintzer (1997), doğrulama amaçlı bir görünmez damgalama geliştirmişlerdir. Böylece damgalanan verinin üzerinde herhangi bir değişiklik olup olmadığı kolayca tespit edilebilecekti.

Mohanty ve diğ. (1999), görünür ve görünmez damgalamanın birlikte kullanıldığı, telif haklarını korumak amacıyla bir yöntem kullanmışlardır.

Hsu ve Wu (1999), imgenin doğruluğunu kanıtlamak amacıyla frekans düzleminde DCT tabanlı bir damgalama algoritması önermişlerdir.

Takai ve Mifune (2002), Fourier hologram tekniği ile bir damgalama yöntemi önermişlerdir.

Shih ve Wu (2003), görüntü kalitesi üzerinde daha az bozulma sağlayan frekans ve uzay düzlemi yöntemleri ile bir damgalama yöntemi önermişlerdir. Damga iki parçaya ayrıldıktan sonra ilk bölümü uzay düzlemde az önemsiz bitlerde, ikinci bölümü ise frekans düzleminde damgalanır.

Shieh, Huang & Wang (2004), DCT yöntemi ile değişiklik yapılacak frekans seçimi için genetik algoritma kullanan bir çalışma yapmışlardır. Dayanıklı ve görünmez bir damgalama işlemi yapılmıştır.

Cai, He, Liu & Yang (2004), yüksek güvenlik için oluşturulan faz kaydırmalı interferometre kullanarak gerçekleştirilmiş bir damgalama çalışması sunmuşlardır.

2.5 Damgalama Gereksinimleri

Sayısal içeriğin niteliğine ve güvenlik seviyesine bağlı olarak bir dizi damgalama tekniği veya uygulaması mevcuttur. Her damgalama tekniği veya uygulamasının, tasarımın geliştirilmesine dayanan kendi gereksinimleri vardır. Her damgalama tekniği ve uygulaması incelenemez; Bununla birlikte, çeşitlilik göz ardı edilemez. Bununla birlikte, her damgalama tekniğinde yerine getirilmesi gereken çok sayıda gereksinim vardır (Pu, Liao, Zhou & Zhang, 2004). Bunlar aşağıdaki gibidir:

Sağlamlık: Bir damgalama algoritması işlemi, farklı saldırı türlerine karşı sağlam olmalıdır, yani kapak görüntüsünün içindeki işaret kolayca kaldırılamamalıdır. Alternatif olarak, işaretin kaybı yalnızca kapak görüntülerinin bozulması pahasına elde edilebilir olmalıdır.

Damga Kırılganlığı: Damgalama algoritması, bir işaret veya logo gibi kapak görüntüsünün içindeki kırılgan bir gizli veriyi, kapak görüntü özelliklerinden hiçbirini etkilemeyecek şekilde işlemelidir. Bu, kapak görüntüsüne değişiklik yapıldığında, işaretin veya logonun bir kısmının kaybedilmesi durumunda damgalama algoritmasının sağlamlığının arttırılması için yardımcı olabilir.

Görünmezlik: Bir damga gömme aslında algılanamaz, yani insanlar orijinal verileri enjekte edilen damgayla verilerden ayırt edemezler. Ayrıca, gömülen işaret orijinal kapak görüntüsünün gerçek görsel niteliğini bozmayacak şekilde bir damgalama algoritması işleme işlemi gereklidir.

Kapasite: Kapasite, görüntünün taşıyabileceği dahil edebilecek veri miktarıdır, mevcut kapasiteyi daha yüksek kullanabilme yeteneği algoritmanın gücünü arttırır;

ancak bu, algoritmalarda kalite ya da sağlamlık yönünden kayıplara yol açmamalıdır.

2.6 Damgalama Uygulamaları ve Kullanım Alanları

Damgalama, telif hakkı korumasına yöneliktir; Bununla birlikte, damgala kullanımını sınırsız hale getiren başka birçok uygulama vardır.

Damgalama uygulama alanı sınırlı değildir; bunun yerine, damga basma tekniklerinin veya planlarının uygulanabileceği birkaç alan vardır. Bunlar arasında (Alasafi, 2016):

- Fikri mülkiyet haklarını geliştirmek için kullanılan telif hakkı koruması
- Reklam ve reklamlarda kullanılan yayın izleme
- İyileştirilmiş mülkiyet konularında kullanılan kimlik doğrulama
- İllegal Yasadışı çoğaltma kaynaklarının izlenmesinde kullanılan parmak izi
- Güvenli iletişim amacıyla kullanılan gizli iletişim iki taraf arasındaki bilgi
- Güvenli olmayan uygulamalar için diğer nesnelerin arkasındaki bilgilerin gizlendiği tarih

Damgalama, şunlar için de kullanılabilir (Alasafi, 2016):

- Tıbbi bilgilerin içine hasta bilgilerini yerleştirmek gibi tıbbi uygulamalarda kullanılan tıbbi güvenlik
- Filmlerin ve haber öğelerinin veya herhangi bir multimedya nesnesinin endekslenmesi gibi birçok alanda indekslemede kullanılan indeksleme

Damgalama uygulamaları ve kullanım alanları kısaca aşağıdaki gibi özetlenmiştir:

Parmak İzi: Yasadışı kopyaların kaynağını bulmak için, sahip farklı müşterilere verilen kopyalara farklı damgalama anahtarları yerleştirebilir. Sahibi için, benzersiz bir seri numarası benzeri damgayı gömmek, korunan verileri kopyalayıp üçüncü bir tarafa sağlayarak lisans sözleşmesini kesen müşterileri tespit etmenin iyi bir yoludur (Tokur, 2004).

İndeksleme: Damgalama, multimedya uygulamalarına geniş bir yelpazede yeni yetenekler sunmaktadır. Video içeriğinde yorumların eklenmesini, ayrıca filmlerin veya haber öğelerinin endekslenmesini, arama motorlarında kullanılabilecek işaretleyicilerin kullanımını mümkün kılarak, video postanın indekslenmesini sağlar (Cox vd., 2000). Çevrimiçi görüntü ve video içeriğinin sayısı, günümüzün arama motorunun özelliklerinden çok daha hızlı arttığından, multimedya verilerine hızlı erişim sağlamanın yeni yollarını önceden planlamak önemlidir ve damgalamanın kesinlikle yapılması için umut verici bir yol olmuştur.

Telif Hakkı Koruması ve Sahip Kimliği: Kendi mülkünü korumak için, veri sahibi, verilerinin Telif hakkı bilgisini temsil eden bir damgayı yerleştirebilir. Bu uygulama, mahkemede telif hakkı anlaşmazlıkları çözümünde gerçekten yararlı bir araç olabilir. Muhtemelen sayısal görüntülerin damgalanması en yaygın kullanımıdır (Tokur, 2004).

Yayın İzleme: Yayınlanmış programların otomatik olarak tanımlanmasına yardımcı olmak için, orijinal damgalamalar, bir ağda geniş bir şekilde yayınlanacak her türlü veriye eklenebilir. Reklam verenlerin ödedikleri parayı aldıklarını veya müzisyenlerin mülkünün korsan istasyonları tarafından yeniden yayınlanmadığını ya da en azından, eğer tespit edilebileceğini belirttiklerinden emin olabilmektedir (Cox vd., 2000).

Kopya koruması: Damgalı bilgiler doğrudan sayısal kayıt cihazını kontrol edebilir. Gömülü anahtar, kayıt cihazı tarafından algılanır ve sonra kopyalama işleminin devam edip etmeyeceğine karar veren bir kopya izin biti akışı kontrol etmektedir (Cox vd., 2000).

Veri Doğrulama: Kırılgan damgalama, bir görüntünün veya herhangi bir başka türde verinin herhangi bir şekilde bozulmasını algılamak için kullanılır. Damga tespit edilirse, veriler orijinaldir, değilse; veriler yeniden düzenlenmiştir ve dikkate alınamaz (Tokur, 2004).

Veri Gizleme (Gizli İletişim): Özel verilerin iletimi muhtemelen en eski damgalama uygulamalarından biridir. Muhtemelen daha önce anlaşılacağı gibi, herhangi bir yetkisiz kişinin bunu tespit etmesini engelleyecek şekilde bir stratejik mesajın zararsız hale getirilmesinden ibarettir (Tokur, 2004).

Tıbbi Güvenlik: Tarihi ve hastanın adını medikal görüntülere katmak, tıbbi bilgilerin yanı sıra güvenliğin de mahremiyetini artırabilir. Yukarıda zikredilen uygulamalardan, damgalama iki farklı tipe bölünebilir: sağlamlık için ilk beşi, kırılganlık için son üçü. Kırılgan damgalama, kullanılan görüntü veya diğer veriler bozulduğunda kaybolur. Örneğin kullanılan verinin orijinal olmasının kesin olması zorunlu durumlarda değerlendirme sürecinde gerçekten yararlı olabilir (Wolfgang, Podilchuk & Delp, 1999). Aksine, sağlam damgalar, anahtarın bunlardan geçtikten sonra hala algılanabilmesi için saldırılara karşı koymak üzere tasarlanmıştır. Telif hakkı korumasını içeren uygulama aralıkları, yani üzerinde çalıştığımız uygulama çok farklı spesifik özellikler ister. Yine de, sağlam damgalar için bir dizi temel gereksinimi listelemek mümkündür. Bunlar genel bir iz düşümdür, ancak okuyucunun sistem tasarımında yer alan ana zorlukları bir kez daha anlayabilmesini sağlamalı ve aynı zamanda bu teknolojinin zorluklarını tartışan aşağıdaki paragrafın doğal ön hazırlıklarını yapmalıdır (Tokur, 2004).

Algısal Şeffaflık: Damganın tipik görüntüleme koşulları altında görünmediğinden emin olmak için insan görsel sisteminin özelliklerini kullanır (Tokur, 2004). Temel olarak, damga bir görüntünün orijinalinden farklı görünmemesi gerektiği anlamına gelir; yani, algılanan kalitede herhangi bir bozulma fark edilmemelidir. Diğer damga türleri görünür olmakla birlikte, uygulamada birçoğu görünür değildir ve bu yüzden saydamlık sayısal damgalanmanın temel bir gereği olarak ele alınmaktadır.

BÖLÜM 3

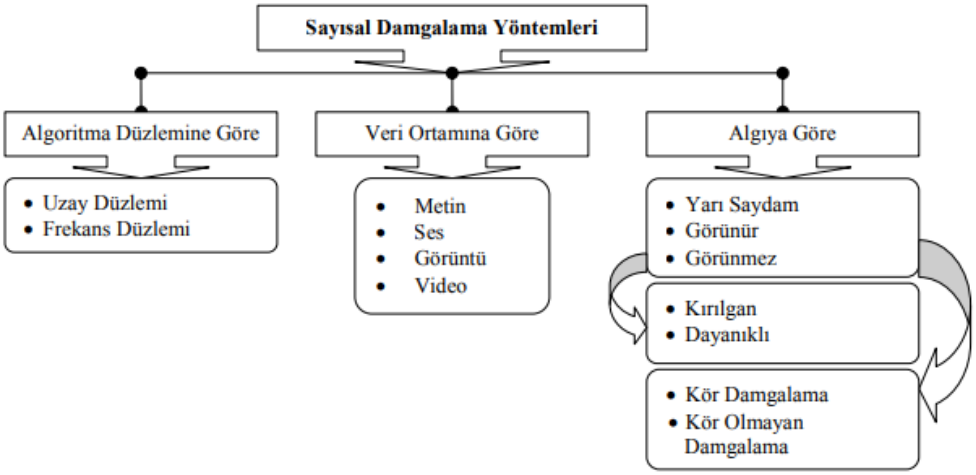
DAMGALAMA YÖNTEMLERİ ve SINIFLANDIRILMASI

Damga oluşturma tekniği, verileri veya görüntüyü (işaret veya logo olarak adlandırılır) multimedya dosyası gibi sayısal bir nesneye yerleştiren işlemdir. Bu işaret veya logo daha sonra gömme işleminde kullanılan aynı damgalama tekniğini tersine çevirerek çıkarılabilir veya algılanabilir. Kaynak görüntüsü, kapak resmi veya orijinal görüntüler olarak adlandırılan bu işareti veya logoyu gerçekleştirmek için kullanılır. Bir damga basma tekniği yalnızca görüntünün telif hakkını korumak için kapak görüntüsünün içine bir işaret veya logo koymak için kullanılan bir işlemdir (Alasafi, 2016).

Damgalama tekniğinin sağlam olduğu düşünülen en önemli şartlardan biri, bir işaretin veya logonun saldırganlar tarafından kolayca tespit edilememesi veya çıkartılamaması veya bir kapak görüntüsünün içindeki işaret veya logonun harici saldırılardan daha az etkilenmesidir.

Damgalama teknikleri, çalışma alanı, işaret türü veya logo türü ve kullanılan kapak görüntüsü gibi bu gömülü işlemin modüle edilmiş veya modüle edilmiş doğasını işlemek için kullanılan farklı yöntemlere göre sınıflandırılır; Ayrıca, insan algısına ve kullanılan tüm uygulamalara göre sınıflandırılabilirler (Le, Nguyen & Le, 2010).

Bilgisayar ortamındaki verilerin damgalanması için birçok yöntem geliştirilmiştir. Damgalama yöntemleri, algoritma düzlemine göre, çalışmanın türüne göre ve algıya göre olmak üzere öncelikle üç ana başlıkta incelenebilir. Bunlar da kendi içerisinde alt gruplara ayrılır. Buna göre aşağıda sayısal damgalamanın çeşitleri görülmektedir (Şekil 3.1).



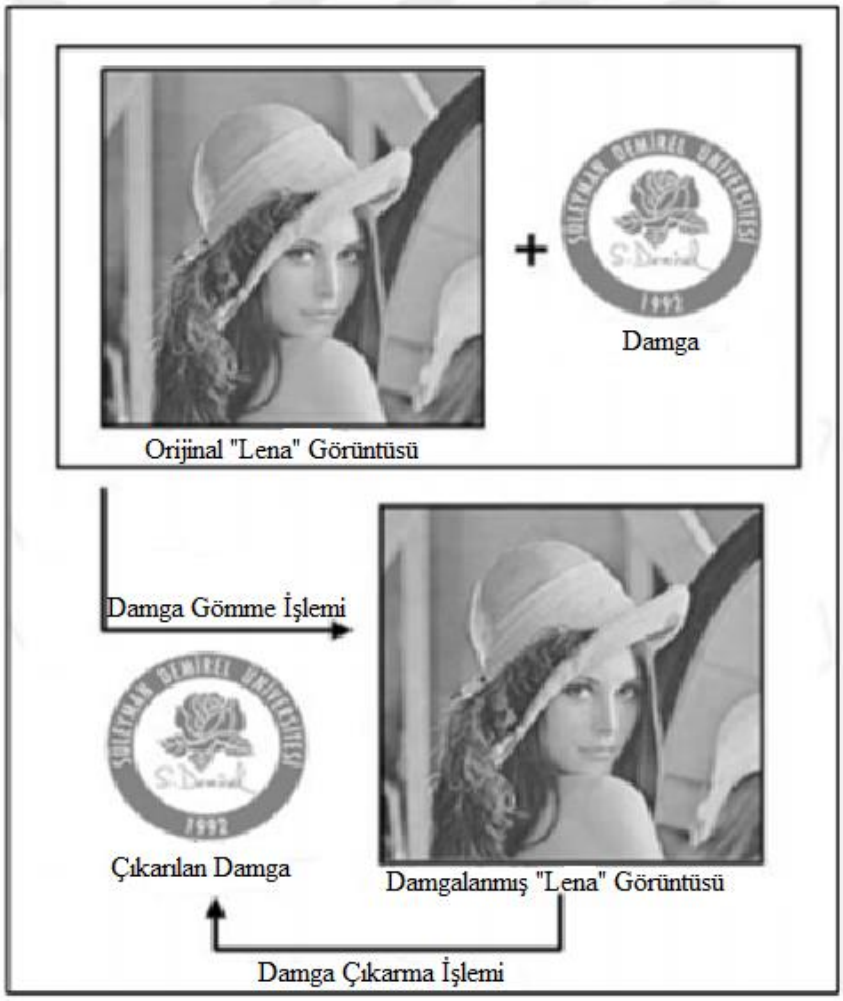
Şekil 3.1 Sayısal Damganın Sınıflandırılması

3.1. Algıya Göre Sınıflandırma

Sayısal Damgalama teknikleri algıya göre "görünür", "görünmez" ve "yarı saydam" olarak sınıflandırılır.

Şekil 3.2 görünür damgalama tekniklerini gösterirken, Şekil 3.3, görünmez damgalama tekniklerini göstermektedir.

Şekil 3.2 Görünür Damga Uygulaması



Şekil 3.3 Görünmez Damga Uygulaması

Çizelge 3.1, bir damgalama algılayıcısına göre özellikleri göstermektedir (Cox vd., 1997; Kutter vd., 1997; Hsu ve Wu, 2000; Fidrich, 1998).

Çizelge 3.1 Algıya Göre Sınıflandırma Özellikleri

Görünür Damgalama	
Özellik	-Medyada Telif Hakkı ihlalleri için kullanılır. -Telif hakkı yasa dışı olarak kaldırılamaz.

	-Kimlik doğrulamayı sağlar. -Esas olarak logo ve marka etiketinde kullanılır
Avantajları	-doğrudan doğruya damgalama ekleme olasılığı -hızlı işlem
Dezavantajlar	-Saldırgan kırılganlığı -Onur kırıcı orijinal kalite
Görünmez Damgalama	
Özellik	-Genellikle görünmez damgalama tercih edilir. -İnsan gözünün algılayamayacağı şekilde olur. -Ticari gereklilik durumunda tercih edilir.
Avantajları	-Orijinali küçültmede dayanıklılık.
Dezavantajlar	-Orijinal görüntü değiştirilebilir.

1.1.1. Görünür Damgalama

Görüntünün herhangi yerine gözle görülebilecek bir şekilde, damgalanacak damganın yerleştirilmesine "görünür damgalama" denir. Yasal olmayan yöntemler kullanılarak çıkarılamaz, görüntüyü veya içeriği doğrulama amacıyla genellikle logo ve tescil etiketleri şeklinde kullanılmaktadır. Görünür damgalama teknikleri, bir işaretin veya logonun gözle görülebildiği her türlü tekniği içerirken, bu teknik günümüzde medya kanalı logoları gibi medya kanallarında yaygın olarak kullanılır (Swanson vd., 1998). Bazı yeni çalışmalar hem görünebilir hem de görünmeyen damgaları kullanarak görünmez damganın görünür damganın yedeği olarak kullanılacağını göstermiştir (Amit Kumar, 2015). Televizyon ekranındaki kanal

logosu ve Internet'te yayınlanan imgelerin bir köşesinde yer alan yayınlandığı site adresi gibi uygulamaları vardır.

Direk olarak uygulandığından dolayı kolay ve hızlı olmasına karşılık, asıl görüntü kalitesini azaltır ve saldırılara karşı kırılgandır.

Görünür damgaların kullanımı, eserlerin mülkiyetini tanımlamak ve izleyicilerin sınırlı kopya haklarının ötesinde izinsiz kullanım yapmalarını önlemek içindir (Hu ve Kwong, 2001). Özel damgalar, özel bir araç gerekmediğinden, sayısal içeriğin yaratıcısının mülkiyet bilgilerini damgadan çıkarmak için içeriği tanımlamanın en kolay yoludur.

Genel olarak, görünür damga basma teknikleri iki türe ayrılabilir: ayrılmaz ve çıkarılabilir. İlki esas olarak aşağıdaki iki faktörü göz önünde bulundurur. Birincisi, damganın kaynak görüntüye veya videoya uyumlu olması gerektiğidir. Yani, uygun damga gerekir. Damga sayısal içeriğin içinde görünebilir ancak orijinal resmin görsel kalitesini etkilememelidir. Diğeri, gömülü damganın, istenmeyen düzenleme ve kötü amaçlı saldırılara karşı güçlü bir şekilde dayanıklı olması gerektiğidir (Pei ve Zeng, 2006). Buna karşın, çıkarılabilir görünen damgalama teknikleri, telif hakkı koruma sorunlarına başka etkili bir çözüm sunar. Orijinal sayısal içerik, dağıtımdan önce telif hakkı bildirimi gibi silinebilir bir desenle işaretlenir veya internette ücretsiz görüntüleme şeklinde bırakılır. Referansta açıklandığı gibi yalnızca çıkarılabilir görünen damga basma teknikleri, aşağıdakiler gibi bazı uygulamalar için uygundur (Yang vd., 2008):

1. Sayısal görüntüler ve videolar insanların yaşamında önemli bir rol oynamaktadır ve yavaş yavaş klasik analog ürünlerin yerini almaktadır. İçerik sağlayıcıları bilgisayar ağları üzerinden ücretsiz ön izleme ve indirmeleri dağıtma veya paylaşma yolu ile görünür telif hakkı bilgisi ile alabilir. İçeriği ile ilgilenen herkes, telif hakkı bilgilerini kaldırmak için üreticiden gizli anahtarı satın alarak daha iyi sürümleri elde edebilir.

2. Ticari bir ortamda bir şirket, ücretsiz deneme yazılımını kullanıcılara sınırlı bir süre için serbest bırakarak kar elde edebilir, ancak deneme süresi sona erdiğinde çalışmayı durdurabilir. Bu amaçla, yazılım bağımlı sayısal içerik, örneğin, normal kullanımını etkilemek için mühendislik çizimi çıkarılabilir bir

görünür damga ile kısıtlanabilir. Devam etmek için kullanıcının, yazılımı etkinleştirmesi ve damgayı sayısal içerikten lisans anahtarıyla kaldırması gerekmektedir.

Çıkarılabilir görünür damgalamayı gerektiren birçok potansiyel uygulama olmasına rağmen, literatürdeki çoğu makale geri alınamaz tekniklerin geliştirilmesine odaklanmaktadır. Birçok geri dönüşümlü, tersinir veya bozulmasız yöntemler olarak da adlandırılır. Ancak iki damgalama algoritması türü farklı uygulama senaryoları için farklı sağlamlık gerekliliklerini karşılamak üzere tasarlandığından, sadece birkaç görünür damga programı çıkarılabilmektedir (Yang vd., 2008).

1.1.2. Görünmez Damgalama

Etkilenmeyen damga veya görünmez damga, bir işaret veya logonun görsel olarak algılanamayacağı her tür damgalama tekniğini içerir. Özel bir yazılım kullanılmadan, DCT ve DWT teknikleri kullanılarak damga gibi işaret veya logolar çıkartılamaz. Görünmez damgalama yöntemleri dayanıklılığına göre kendi içinde "dayanıklı" ve "kırılgan" olmak üzere ikiye ayrılır. Sağlam damgalar veri doğrulama için kullanılabilirken, kırılgan damgaların sayısal içeriğin bütünlüğünü ve orijinalliğini kontrol etmesi amaçlanmıştır (Vleeschouwer vd., 2002;Petitcolas vd., 1999).

Dayanıklı Damga: Dayanıklı damgalama yönteminde, taşıyıcı görüntüye gizli olarak damgalanan bilginin, görüntün kalitesinde ciddi bir bozulmaya neden olmadan, farklı görüntü işleme saldırılarına karşı dayanıklı ve geri çıkarıldığında tanınabilir nitelikte olması amaçlanmaktadır.

Sağlam (dayanıklı) damga, gömülü işaretin veya logonun piksel bitlerinde değişiklik yaptığı ve gözlenemediği anlamına gelir. Ayrıca, veri çıkarma işlemi sadece uygun kod çözme mekanizmaları kullanılarak yapılmalıdır (Petitcolas vd., 1999).

Kırılgan Damga: Marka veya logonun gömülü olduğu kapak görüntüsü üzerinde meydana gelen herhangi bir değişiklik veya herhangi bir saldırı işleminin,

markanın veya logonun tahrip olmasına neden olacak herhangi bir teknik anlamına gelir (Stein, 2000).

Görüntü değiştirilmişse, değiştirilmiş bloklara karşılık gelen görüntü içeriği ve damga eşleştirilemez, böylece değiştirilmiş bloklar algılanır. Bazı kırılgan damgalama şemaları, bir konak görüntüsünü küçük bloklara böler ve işareti her bir bloğa yerleştirir. Gömülü veriler, her kapak bloğunun ana içeriğinin bir karması olabilir. Görüntü değiştirilmişse, değiştirilen bloklara karşılık gelen görüntü içeriği ve damga, değiştirilen blokların algılanması için eşleştirilemez. Saldırgan, sahte bir damgayı içeren yasadışı bir görüntüyü sahtekarlık yapmak için birçok damgalı görüntüden uygun blokları seçebilse dahi, tarif edilen damgalama yöntemi, bu tip saldırılara karşı güvenlik sağlamak amacıyla her blok için kırılgan bir damga üretmek üzere iki adet aynı endeks bilgisini kullanır (Zhang ve Wang, 2009).

Blok şeklinde kırılgan damgalama şemaları, yalnızca değiştirilmiş blokları tanımlayabilir ancak değiştirilmiş pikselleri tanımlayamaz. Başka bir deyişle, değişikliğin ayrıntılı modelini bulamazlar. Bu dezavantajın üstesinden gelmek için, ana piksellerin gri değerlerinden türetilmiş olan damga bilgisinin ana piksellere kendi içine gömüldüğü bazı piksel bazında kırılgan damga şemaları önerilmiştir (Vleeschouwer vd., 2002). Dolayısıyla, değiştirilmiş pikseller, taşıdıkları damga bilgisinin bulunmamasından dolayı tanımlanabilir. Bununla birlikte, bu yöntemlerde, yeni piksel değerlerinden türetilen bazı bilgiler damgayla çakışabildiğinden, değiştirilmiş piksellerin yerleri tamamlanmamış ve değiştirme modelinin tespiti yanlıştır. Bu sorunu çözmek için, hassas bir damga düzenleme şeması, bir konak görüntüsüne bir dizi özel kimlik doğrulama verisi yerleştirir ve görüntü doğrulama için istatistiksel bir mekanizma sunar. Değişiklik mukavemetini tahmin ederek, değiştirilmiş pikselleri tam olarak bulmak için değiştirilmiş ve orijinal piksellere karşılık gelen iki farklı dağılım kullanılabilmektedir (Zhang ve Wang, 2009).

Görünmez damga (sağlam veya kırılgan olabilir), piksel değerinde yapılan modifikasyonların algısal olarak fark edilmeyecek ve yalnızca uygun bir kod çözme mekanizması ile geri kazanılabilecek şekilde gömülür (Mohanty, 2008). Çoklu damgalarda, telif hakkı koruması, içerik doğrulaması veya resim yazısı için

iki veya üç damga gömülüdür. IBM'in Vatikan Kütüphanesi projesi ile başladığından beri, görünür damgalama teknolojisi önemli ölçüde ilerlemiştir. Görünmez sağlam damga, Cox'un (1997) araştırma ekipleri tarafından başlatılmıştır.

Görünmez bir damga basma tekniği için, sadece sağlamlık özelliği içerik korumasını garanti etmek için yeterli değildir. Uygulamaya özel damgalama teknikleri, multimedya cihazlarında bulunan standart kodlayıcı-kod çözücü sistemleri ile geliştirilmelidir. Gelişimleri standart bir kurumun kurulmasını gerektirir (Eskicioğlu ve Delp 2001). Dijital video disklerde (DVD) depolanan içerikle ilgili iyi bilinen bir teknik grup, Kopya Koruması Teknik Çalışma Grubu'dur. Ses için, Güvenli Sayısal Müzik Girişimi damgalama teknolojisini standartlaştırıyor. Görünmez dayanıklı damgalamanın uygulanabilirliği için sağlanan yasal çerçeve damganın kasıtlı olarak çıkarılmasını veya saldırılara karşı korunmasını sağlayan Dijital Binyıl Telif Hakkı Yasası ile belirlenmiştir (Mohanty, 2008).

Sayısal multimedya çağı, görüntü içeriğinin yaratılması ve dağıtılmasında birçok avantaj sağlamıştır, ancak kopyalama ve düzenleme kolaylığı da yetkisiz kullanım, yanlış kullanım ve yanlış beyanı kolaylaştırmaktadır. İçerik sağlayıcılar bu konular hakkında doğal olarak endişelenmektedirler ve bir görüntüye başka bir sinyal (damga) yerleştirme eylemi olan damga, sahip haklarını korumak için önerilmiştir (Lin and Delp, 2005).

Görünmez veya saydam işaretler, damgalanmış görüntüdeki algısal bozulmayı en aza indirmek için insan görsel sisteminin özelliklerini kullanmaktadır (Lin and Delp, 2005; Wolfgang vd., 1999).

Şeffaf damgaların sınıfında, teknikler sağlam veya kırılgan olarak da sınıflandırılabilir. Sağlam bir işaret, işareti çıkarmaya veya imha etmeye çalışan saldırılara karşı koymak için tasarlanmıştır. Bu tür saldırılar arasında kayıplı sıkıştırma, filtreleme ve geometrik ölçeklendirme bulunur. Damgalı görüntüdeki yüksek olasılıklı hafif değişiklikleri belirlemek için kırılgan bir işaret tasarlanmıştır. Kırılgan damgaların ana uygulaması içerik doğrulamasıdır. Literatürde bildirildiği gibi damga basma çalışmalarının çoğu sağlam teknikler

alanındadır. Birçok önemli uygulama kırılgan damgaların kullanımından faydalanabilir (Wolfgang vd., 1999).

Kırılgan damgalar, sayısal görüntülerin telif hakkı sahipliğini zorlamak için uygun değildir; bir saldırgan gömülü damgayı imha etmeye çalışır ve kırılgan damgalar kolayca imha edilebilir. Kırılgan damgaların modifikasyona duyarlılığı, görüntü doğrulamada kullanımlarına yol açar. Yani, tarafların bir görüntünün işaretlendiğinden beri düzenlenmemiş, zarar görmemiş veya değiştirilmemiş olduğunu doğrulaması için ilgi çekici olabilir (Yeung ve Mintzer, 1998).

Görüntü doğrulama sistemleri hukuk, ticaret, savunma ve gazetecilikte uygulanabilirliğe sahiptir. Sayısal görüntüler değiştirilebildiğinden beri, görüntünün güvenilirliğinin sorgulanabileceği durumlarda herhangi bir değiştirme olmadığını göstermek için güvenli bir kimlik doğrulama sistemi kullanışlıdır. Yaygın örnekler, değiştirmeyi saptamak için bir veri tabanındaki görüntülerin işaretlenmesidir, "güvenilir bir kamerada" kullanılması haber ajanslarının bir görüntünün olayları tahrif etmek için hazırlanmamasını veya düzenlenmemesini sağlayabilir. Ticari amaçlı görüntülerin işaretlenmesiyle, alıcı aldığı görüntülerin orijinal olduğundan emin olabilir. Diğer durumlara mahkeme salonu kanıtlarında kullanılan görüntüler, gazetecilik fotoğrafçılığı veya casuslukla ilgili görüntüler örnek verilebilir (Lin and Delp, 2005).

Sayısal bir çalışmanın gerçekliğini doğrulamanın başka bir yöntemi, imza sisteminin kullanılmasıdır. Bir imza sisteminde, kimliği doğrulanacak verilerin bir özeti, kriptografik karma işlevlerinin kullanılmasıyla elde edilir. Daha sonra özet, orijinal verilere bağlı olan imzayı üretmek için şifreli olarak imzalanır. Daha sonra, bir alıcı (muhtemelen değiştirilmiş) verilerin özetini inceleyerek ve verilerin doğru olup olmadığını belirlemek için bir doğrulama algoritması kullanarak imzayı doğrular. Kırılgan damgalama ve sayısal imza sistemlerinin amacı benzer olsa da, damgalama sistemleri, görüntü verilerinde bir miktar değişiklik (damga ekleme) yapılması pahasına imza sistemlerine kıyasla çeşitli avantajlar sunar (Lin and Delp, 2005).

Bir damga doğrudan görüntü verilerine gömülü olduğundan, kimlik doğrulama doğrulaması için ek bilgi gerekmez. (İmza kendisinin iletilen verilere

bağlı olması gerektiğinden, bu sayısal imzalara benzemez.) Bu nedenle, orijinallik testi sürecinde ihtiyaç duyulan kritik bilgiler sıkı bir şekilde gizlenmiştir ve sayısal imzayı kaldırmaktan daha zordur. Ayrıca, sayısal imza sistemleri görüntüyü keyfi bir bit akışı olarak görür ve benzersiz yapısından faydalanmaz. Bu nedenle, bir imza sistemi bir görüntünün değiştirildiğini algılayabilir ancak değişiklikleri niteleyemez. Birçok damgalama sistemi, işaretlenmiş bir görüntünün hangi alanlarının değiştirildiğini ve hangi alanların değiştirilmediğini belirleyebilir, ayrıca değişikliklerin yapısını tahmin edebilir (Lin and Delp, 2005).

Ek olarak, görünmez damganın damgayı tespit prosesine göre sınıflandırılması da aşağıdaki gibidir (Le vd., 2010), örneğin:

Kör Damgalama: Bu tip damgalama tekniğinde, işaretleme veya logoyu çıkartmak için tespit işleminde orijinal verilere ihtiyaç duyulmaz. Geniş bir uygulama alanına sahiptir, ancak daha yüksek bir damgalama teknolojisi gerektirir ve zaman ve paraya mal olur.

Kör Olmayan Damgalama: Bu tip damga basma tekniğinde, tespit işlemi için hem orijinal görüntü hem de işaret veya logo gereklidir.

Yarı kör damgalama: Bu tip damga basma tekniğinde, algılama işlemini tamamlamak için orijinal görüntüye veya işaret ya da logoya ihtiyaç duyar.

1.1.3. Yarı Saydam Damgalama

Görünür ya da görünmez damgalamanın yanında sayılabilecek üçüncü bir yöntem ise, görüntünün büyük bir bölümü üzerine, logonun yarı saydam olarak eklenmesidir. Bu yolla eklenen logonun görüntüden ayrılması, görüntüyü anlamsız kılacağından avantajlıdır. Ancak görüntüyü kullanıcıya bu şekilde sunmak bir dezavantajdır.

3.2. Veri Ortamına Göre Sınıflandırma

Damga basma teknikleri, gömme için kullanılan nesnenin türüne, ana bilgisayar nesne türüne bağlı olarak da “metin”, “ses”, “görüntü” ve “video” olarak sınıflandırılabilir (Alasafi, 2016).

3.2.1. Metin Damgalama

Sayısal damgalama, bilgi güvenliği araştırma alanında 1990'larda önerilen bir sayısal ürün telif hakkı koruma teknolojisidir. Multimedya verileri, sayısal, seri numarası, metin, resim, logo ve diğer bilgi türlerinde yerleşiktir ve telif hakkı korumasında rol oynar, ürünü işaretler, gizli iletişim kurar, ait olduğu verileri onaylar, veri doğruluğunu tespit eder (Ruia ve Jinqiaob, 2013).

Günümüzde, ana metin damga algoritmaları 4 şekilde sınıflandırılabilir:

- formata dayalı metin damgası,
- içeriğe dayalı metin damgası,
- gösterilen önemsiz biti temel alan damga
- doğal dile dayalı metin damgası (Zhao, 2009).

Biçime (formata) dayalı metin damgası en yaygın kullanılan algoritmadır. Satır kaydırma, başlangıçtan karakter kaydırma, daha sonra yazı tipi boyutunu, rengini ve diğer yöntemleri değiştiren ilerlemeye kodlama özelliği ve formata dayalı metin damgalaması araştırması çok etkindir.

İçeriğe dayalı metin damgası, daha iyi sağlamlığa ve güvenliğe sahip olan damga gömme amacına ulaşmak için karakter kodlamasıyla değiştirilir (Ruia ve Jinqiaob, 2013). Edebiyat, İngilizce harflerin yerine benzer Yunanca harfleri kullanmaktadır, ancak bu yöntem sadece İngilizce için uygundur. Damgalama alanı küçüktür ve daha fazla damga bilgisi içeremez. Edebiyat Çince karakter ifadesine dayalı metin damgası, Çince metin için en iyi damgalama algoritması türü olmaktadır (Zhao, 2009).

Temsil edilemeyen esaslara dayanarak yapılan metin damgası, LSB'ye benzerdir. Damgayı gömmek için önemsiz noktaları veya boşlukları kullanan görüntü damgası kararsızdır ve iletim sürecinde damga bilgisini kaybedebilmesi mümkündür. Ayrıca sağlamlık ve güvenlik, format temelli daha sonraki metin damgalama kadar iyi değildir (Ruia ve Jinqiaob, 2013).

Atallah ve ark. (2002)'de Amerika Birleşik Devletleri'nde; Damgalama bilgisi, cümle yapısını, eş anlamlı ikamesini değiştirerek ve diğer yöntemlerle gömdüler. Doğal olarak dil sayısal damgayı metin içeriğini değiştirdi ancak metin

ve biçimin anlamını pek değiştirmedi. Damga ekledikten sonra, damga bilgisini dosyada tespit etmek neredeyse imkânsızdı. Ayrıca damgayı yok etmekte kolay değildi. Ancak standart bir dosyada bu yöntem anlamı değiştirebilir, çünkü format şekli katıdır. Bu nedenle, bu yöntem katı formatları biçimlendirmek için geçerli değildir. Bilgisayarların doğal dil işleme yetenekleri yeteri kadar olgun olmadığı için bu, doğal dil teknolojisine dayalı metin damgalamanın darboğazıdır.

Mevcut damgalama algoritmalarının aşağıdakiler gibi birçok sorunu bulunmaktadır (Ruia ve Jinqiaob, 2013):

- Düşük sağlamlık: damga bilgilerini değiştirmek için doğrudan WORD menüsü üzerinden çalışabiliriz;
- Yetersiz güvenlik: damgalama algoritmasını biliyorsanız, damgayı çıkarabilirsiniz;
- Düşük damga kapasitesi;
- Çince ve İngilizce karışık metinler için geçerli olamaması.

Çince ve İngilizce karışık metinler için çoklu damgalama algoritmaları, karakter kodlamasına dayalı özniteliklerdir. Bu algoritma damgalama güvenliğini, sağlamlığı ve kapasiteyi mevcut olandan daha iyi hale getiren damgalama algoritmasıdır.

3.2.2. Ses Damgalama

Bilgi sistemlerindeki ve ağ tabanlı veri tabanlarındaki gelişmeler, sayısal medyada, örneğin ses, görüntü ve video gibi hızlı büyümeyi hızlandırmaya devam ediyor. Bu, kısmen, sayısal ortamın sağladığı yüksek verimli manipülasyon, çoğaltma ve erişime bağlıdır.

Veri gizleme, verilerde küçük değişiklikler yaparak video, görüntü veya ses gibi sayısal verilerdeki ekstra bilgileri kodlama işlemleridir. Bir görüntü veya sesi, ek bilgilerle desteklemek veya görüntü veya sesin bütünlüğünü doğrulamak için seslerdeki veya görüntülerdeki bilgilerin gizlenmesi kullanılabilmektedir. Gizli bilgilerin kendisi metin, ses veya görüntü verileri veya köprüler olabilir. Örneğin, bir resimdeki yüzleri ve binaları etiketlemek için metin başlıkları kullanılabilmektedir. Kısa bir ses klipi, bir tren düdüğünü bir lokomotifin

görüntüsü ile ilişkilendirebilmektedir. Bir köprü, bir görüntü bölgesini başka bir belgeye veya veri kaynağına bağlayabilmektedir (Boney, Tewfik & Hamdy, 1996).

Gömülü veriler tipik olarak saklandığında veya iletildiğinde görüntüde kalır. Gömülü verilerin bir son kullanıcı tarafından çıkarılması veya son kullanıcıya gizlenmesi amaçlanabilir. Örneğin, bir önceki örnekte, bir tüketici gömülü verileri çıkarabilir ve bunu bir bilgi ihtiyacını karşılamak için kullanabilir. İkinci durumda, gömülü veriler bir damga olabilir. Damga, telif hakkını veya diğer bilgileri temel verilere gizleyerek sayısal medyayı etiketlemek için kullanılan bir tekniktir. Şifrelemenin aksine, örneğin, verilere erişimi kısıtlamak için kullanılır, yazarlığın sağlam bir şekilde ispatlanması için damga kullanılmaktadır. Genel olarak veri gizleme gibi, damga medyada kalır. Bununla birlikte, genel olarak saklanan verilerin aksine, damgayla kullanıcı gömülü bilgiye erişemez (Boney vd., 1996).

Genel olarak veri gizleme ve özellikle damga kullanma, yararlı olmak için tipik olarak aşağıdaki gereklilikleri karşılamalıdır: duyulmuyor olmalı ve sağlam olmaları gerekir. Her ne kadar diğer kriterler önemli olsa da (örneğin istatistiksel olarak duyulmazlık, çoklu veri yerleştirme ve kendi kendine zamanlama desteği), elde edilemezlik ve elde edilen verilerin sağlamlığı en önemli olanıdır. İlk gereksinim, ana verinin sağlam veri olması durumunda gizli verilerin duyulamamasıdır. Aksi takdirde, ses kalitesi düşebilir. İkinci gereklilik, sağlamlık, içine gömüldüğü ortamın manipülasyonu ışığında gizli verilerin hayatta kalması ile ilgilidir.

Tipik olarak, ses verileri, filtreleme, yeniden örnekleme, sıkıştırma, gürültü, kırpma, ses-sayısal ve müteakiben sayısal-ses dönüşümü gibi sinyal işleme işlemlerine tabidir. Çünkü, ana bilgisayar verileri her zaman bu manipülasyona tabi olacaktır, gömülü veri sağlam olmalıdır. Yani, gömülü veriler, host verileri sinyal işleme işlemlerine tabi tutulduktan sonra hayatta kalabilmelidir (Boney vd., 1996).

3.2.3. Görüntü Damgalama

Renkli ya da siyah beyaz görüntülerin damgalanmasında, damga doğrudan orijinal görüntüye eklenir. Görünmezliği arttırmak için damganın asıl işaretine bağlı olarak ölçeklenmesi gerekir. Görüntü damgalamada damga, sıkıştırma, filtreleme, kırpma, döndürme, ölçeklendirme, geometrik bozulma, A/D dönüşüm, D/A dönüşüm gibi yaygın işaret işleme saldırılarına karşı dayanıklılığını korumalıdır.

3.2.4. Video Damgalama

Multimedya uygulamalarının temel popülaritesi, yasadışı kopyalamayı ve sayısal video dağıtımını önlemek için telif hakkı koruması sağlamayı zorunlu kılmıştır. Telif hakkı koruması, korumak istediğiniz sayısal videoya sahiplik bilgileri ve logo gibi verileri kimlik doğrulama verisi olarak eklemek anlamına gelmektedir. Kimlik doğrulama verileri videodan çıkarılabilir ve mülkiyeti kanıtlamak için yetkili kanıt olarak kullanılabilir. Bu nedenle Sayısal Video Damgalama, araştırma alanında yeni ortaya çıkan telif hakkı koruma tekniğidir. (Chimanna ve Khot, 2013).

Video damgalama, bilgileri videonun karelerine yerleştirmeyi içerir. Görüntü damgalamanın bir uzantısıdır ve bu nedenle görüntü damgalama için kullanılan teknikler de video damgalama içeriğine uygulanabilir.

Video damgalama uzaysal boyutta ya da frekans boyutunda yapılabilir. Uzaysal boyutta video damgalama, frekans boyutta video damgalamadan çok daha basittir ancak frekans boyutta damgalama nispeten daha sağlamdır ve istenmeyen saldırıların çoğuna dayanabilir. Yaygın olarak kullanılan frekans dönüşümleri, DFT (Ayrık Fourier Dönüşümü), FFT (Hızlı Fourier Dönüşümü), DCT (Ayrık Kosinüs Dönüşümü) ve DWT'dir (Ayrık Dalgacık Dönüşümü). DWT, diğer dönüşümlerden daha hızlı ve hesaplama açısından daha verimlidir (Chimanna ve Khot, 2013).

DWT mükemmel uzamsallık özelliklerine sahiptir, bu nedenle damganın algılanamayan şekilde gömülebileceği alanları tanımlamak için kullanılır. Damga,

insan görsel sistemine (HVS) daha az duyarlı olduğu için çıkarılan çerçevelerin parlaklık bileşenine gömülüdür (Chimanna ve Khot, 2013).

Damga bitleri gömülmek için kullanılan alt bantlar üzerine dağıtılarak, hemen hemen tüm saldırılara karşı dirençli olan daha sağlam damga düzenine sahip olur.

3.3. Algoritma Düzlemine Göre Sınıflandırma

Damgalama için kullanılan algoritmalar örtü nesne olarak kullanılan ortam ve istenen algı düzeyi için "Uzay düzlemi" ve "frekans düzlemi" olarak ta sınıflandırılmaktadır.

3.3.1. Uzay Düzlemi

Uzay düzlemindeki damgalama işlemlerinde, damgalanacak çalışmanın bilgisi üzerinde değişiklik yapılır. Damganın algılanmasının zor olması amaçlanmıştır. Bu sebeple görüntü piksellerinin parlaklık değerlerine küçük değişiklikler eklenmiştir. Damga pikselin parlaklık değerine direk eklenebilir ya da parlaklık değerinin en düşük anlamlı bitine eklenebilir (Oğuz, 2006).

Uzaysal alan teknikleri, piksellerdeki değiştirilmiş bitler veya bu piksellerin sayısının ağırlığının değiştirilmesi gibi, görüntünün içindeki karakteristik özellikleri değiştirerek damgalama tekniklerinin kapak görüntüsüne bir işaret veya logo yerleştirmek üzere kullanılan tekniklerdir (Le vd., 2010).

En Önemsiz Bit (LSB) teknikleri ve Yayılı Spektrum Modülasyonu (Spread-Spectrum Modulation-SSM) tabanlı teknikler gibi bu açıdan birçok teknik kullanılmıştır. Bu türler, bir işareti gizlemek için kullanılan en güçlü tekniklerden biridir; ancak, görüntünün genel görselleştirmesini olumsuz etkileyebilir.

3.3.2. Frekans Düzlemi

Damgalama araştırmalarının önemli bir bölümünü de frekans düzleminde yapılan araştırmalar oluşturmaktadır. Frekans düzleminde yapılan damgalama işlemlerinde ise, damgalanacak çalışma öncelikle frekans bileşenlerine ayrılır.

Görüntü bilgisinin frekanslarına ayrılmasında Ayrık Kosinüs Dönüşümü (Discrete Cosine Transform), Ayrık Dalga Dönüşümü (Discrete Wavelet Transform), Ayrık Fourier Dönüşümü (Discrete Fourier Transform), Hızlı Fourier Dönüşümü (Fast Fourier Transform) gibi dönüştürme araçları kullanılmaktadır.

Damgalanan bilginin görüntü içinde JPEG gibi kayıplı sıkıştırmaya karşı dayanıklılığının sağlanması amacıyla birçok çalışmada Ayrık Dalgacık Dönüşümü kullanılmıştır. Bu düzlemde elde edilen frekanslar ve katsayıları üzerinde değişiklik yapıldıktan sonra ters dönüşüm formülü kullanılarak damgalanmış ürün elde edilmektedir (Oğuz, 2006).

Ayrıca, DCT ve DWT veya DWT ve SVD gibi bu tekniklerden ikisini veya daha fazlasını birleştirmeye dayanan bazı yeni teknikler vardır (Le vd., 2010). Bağlama uzaysal alan teknikleri ve frekans alanı teknikleri, günümüzde daha fazla uygulanmaktadır. Çünkü piksel bitini değiştiren kapak görüntüsü örneğinin spektral katsayılarını kullanmaktadırlar. Bu, işaret veya logoyu tespit etmek veya çıkarmak için özel araçlar kullanmaksızın çıplak gözle gömülü herhangi bir işaret veya logoyu tespit etmeyi zorlaştırır (Alasafi, 2016).

Aşağıda çizelge 3.2'de DFT, DCT ve DWT algoritmaları arasındaki ana farklar gösterilmektedir (Alasafi, 2016).

Çizelge 3.2. DFT, DCT ve DWT algoritmaları

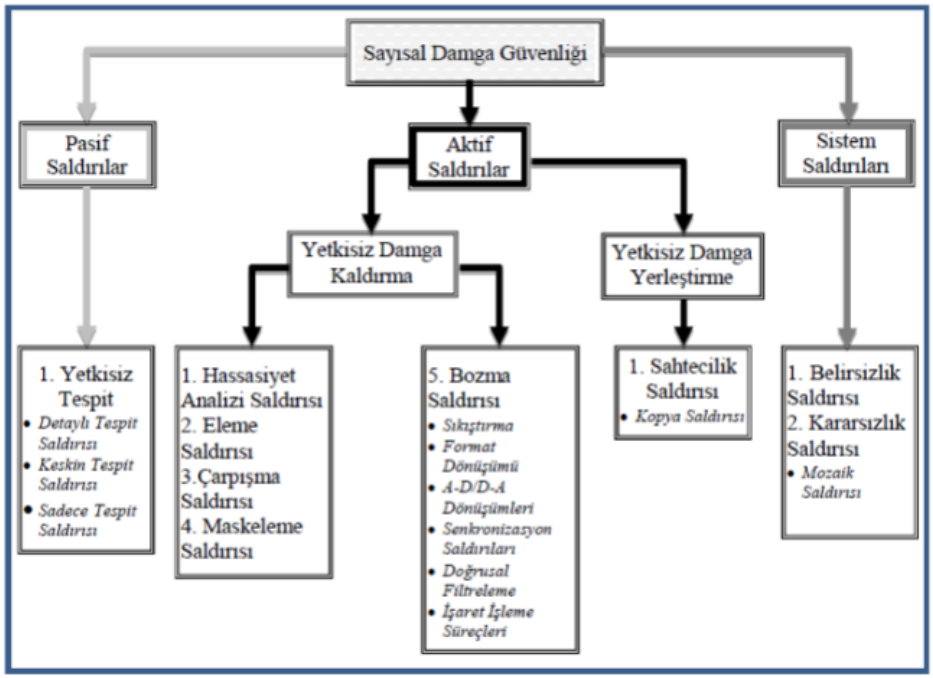
Algoritmalar	**Artıları**	**Eksileri**
DFT	DFT, döndürme, ölçekleme ve çevirmedir. Bu nedenle, geometrik bozulmalardan kurtulmak için kullanılabilir.	Zor bir işlem ve hesaplama maliyeti karmaşık olabilir.
	Sayısal işlemlere karşı daha sağlam. İşaret, yerleştirme nedeniyle hiçbir saldırı	Kuantalama işlemi sırasında bazı yüksek frekanslı bileşenler baskılanabilir. Kırpma ve

DCT	tarafından kaldırılamaz. İşaret orta frekans katsayısı içindedir.	ölçeklendirmeye karşı hassastır.
DWT	İnsan algısıyla anlaşılmayacak daha yüksek sıkıştırma oranı. Hem zaman hem de uzaysal frekans alanında iyi lokalizasyon sağlar. Kırpma, ölçeklendirmeye karşı hassastır.	Hesaplama başına maliyet daha yüksek olabilir. Daha karmaşık olabilir. Sıkıştırma süresi daha yüksek olabilir. Gürültü görüntünün köşelerinde gözle görülebilir.

BÖLÜM 4

GÜVENLİK VE DAYANIKLILIK

Sayısal Damganın güvenliği sayısal damganın kasıtlı olarak bozulması ya da başka işlemlere karşı ne kadar kuvvetli olduğunu incelemektedir. Kötü niyetli bu işlem genellikle damganın ortadan kaldırılarak ya da zarar verilerek işlevini yerine getirememesini amaçlamaktadır. Damga güvenliğini tehdit eden bu kötü niyetli işlemler üç grupta toplanmaktadır. Damga ekleyeceğimiz ortam ve eklenecek damganın türü dikkatlice seçilerek dayanıklı bir damga eklenmesiyle güvenlik sağlanabilmektedir (Cevdet, 2018).



Şekil 4.1 Sayısal Damga Güvenliği

Damgalama yönteminin dayanıklılık açısından değerlendirilmesi de oldukça önemlidir. Daha önceki bölümlerde anlatılmış olan “Dayanıklı Damga” kavramından ayrı olarak “Damganın Dayanıklılığı” çeşitli müdahale ve saldırılara karşı dayanıklı olmasını ifade eder.

İşlenmiş damgalı veriye "saldırıya uğramış veri" denir. Herhangi bir damgalama şemasının önemli bir yönü, saldırılara karşı sağlamlığıdır. Sağlamlık kavramı sezgisel olarak açıktır. Saldırıya uğrayan verileri işe yaramaz hale getirecek kadar bozulmamışsa damga sağlamdır. Damganın bozulması, eksiklik olasılığı, bit hatası olasılığı veya kanal kapasitesi gibi kriterlerle ölçülebilir. Multimedya için, saldırıya uğrayan verinin kullanışlılığı, algısal kalitesi veya doğal sesin değişimi (distorsiyonu) dikkate alınarak ölçülebilir. Bu nedenle, sağlamlık, damganın bozulması ve saldırıya uğramış verilerin bozulması göz önüne alınarak eşzamanlı olarak değerlendirilebilir.

Bir saldırı, saldırıya uğrayan verinin algısal kalitesini korurken, damgayı kabul edilebilir sınırların ötesinde bozmaya zorlarsa bir damgalama düzenini yenmeyi başarır (Patel ve Alpesh, 2014).

Damgalama saldırıları farklı kaynaklarda değişik şekillerde sınıflandırılmaktadır. Fakat temel olarak iki grupta yer almaktadırlar. Bunlardan ilki damgayı bozmayı amaçlarken, diğeri damgayı elde etmeyi amaçlamaktadır.

Literatürdeki mevcut saldırılar 5 sınıfta ele alınır:

- Basit Saldırılar
- Kaldırma Saldırıları
- Geometrik Saldırılar
- Kriptografik Saldırılar
- Protokol Saldırıları

4.1. Basit Saldırılar

Bu başlık altında yapılan saldırılar aslında sıkıştırma ve genel görüntü, ses, video işleme yöntemleridir. Yapılan bu işlemlerin amacı damgalanmış nesne üzerinde değişiklik yaparak damganın algılanmasını engellemektir. Sıkıştırma işlemleri, görüntü,

video ve ses dosyalarına gürültü ekleme, görüntü dosyalarının boyutları üzerinde kırpma yapma gibi işlemler bu sınıfa örnek olarak verilebilir (Yavuz, 2008).

4.2. Kaldırma Saldırıları

Kaldırma Saldırıları, filigran algoritmasının tamamen kaldırılmasını amaçlamaktadır. Yani, hiçbir işlem, karmaşık bir şekilde bile olsa filigran bilgilerini saldırıya uğrayan verilerden kurtaramaz. Bu kategori gürültü giderme, remodülasyon, çakışma ve ortalama alma yöntemlerini içerir. Bu yöntemlerin tümü her zaman tam filigran temizleme hedeflerine yaklaşmaz, ancak yine de filigran bilgisine önemli ölçüde zarar verebilir.

Gelişmiş temizleme saldırıları, filigranı işlemlerini yeterince optimize etmeye çalışır. Genellikle, filigran için istatistiksel modeller ve orijinal veriler optimizasyon sürecinde kullanılır. Gizleme saldırıları, her biri bir anahtar veya farklı bir filigranla imzalanan belirli bir veri kümesinin birçok kopyası bir saldırgan veya bir saldırgan grubu tarafından alınabildiğinde uygulanabilir. Böyle bir durumda, tüm kopyaların ortalaması alınarak veya her farklı kopyadan yalnızca küçük parçalar alarak başarılı bir saldırı gerçekleştirilebilir (Patel ve Alpesh, 2014).

4.3. Geometrik Saldırılar

Kaldırma saldırılarının aksine, geometrik saldırılar aslında gömülü damganın kendisini kaldırmaz ancak gömülü bilgilerle damga dedektörü eşitlemesini deforme etmeyi amaçlar. Mükemmel senkronizasyon yeniden elde edildiğinde dedektör gömülü damga bilgisini geri kazanabilir. Bununla birlikte, gerekli senkronizasyon işleminin karmaşıklığı pratik olamayacak kadar büyük olabilir. Bununla birlikte, en yeni damgalama yöntemleri, özel senkronizasyon tekniklerinin kullanılması nedeniyle bu saldırılara dayanmaktadır.

Global geometrik çarpıtmalara karşı sağlamlık çoğu zaman, ya değişmeyen bir alanın (Fourier-Melline) ya da ek bir şablonun ya da otomatik kovaryans işlevi (ACF) geometrik çarpıklıkların tahmin edilmesini sağlayan özel olarak tasarlanmış periyodik damgaların kullanımına dayanır. Bununla birlikte, aşağıda tartışıldığı gibi, saldırgan, senkronizasyon şeması bilgisini kullanan özel saldırılar tasarlayabilir. Küresel afin

dönüşümlerine sağlamlık az çok çözülmüş bir konudur. Bu nedenle, pikseller yerel olarak kaydırılır, ölçeklenir ve önemli görsel bozulma olmadan döndürülür. Bununla birlikte, bazı yeni yöntemlerin bu saldırıya karşı koyabildiğini belirtmekte fayda var (Patel ve Alpesh, 2014).

4.4. Kriptografik Saldırılar

Kriptografik saldırılar damga düzenlemelerindeki güvenlik yöntemlerini kırmayı ve böylece gömülü damga bilgisini kaldırmanın veya yanıltıcı damgaları gömmenin bir yolunu bulmayı amaçlar. Böyle bir teknik gömülü gizli bilgi için kaba kuvvet aramasıdır. Bu kategorideki bir başka saldırı, bir damga dedektörü cihazı mevcut olduğunda damga içermeyen bir sinyal oluşturmak için kullanılabilecek Oracle saldırısıdır. Pratik olarak, bu saldırıların uygulanması, yüksek işlemsel karmaşıklıkları nedeniyle sınırlandırılmıştır (Patel ve Alpesh, 2014).

4.5. Protokol Saldırıları

Protokol saldırıları, filigran uygulamasının tüm kavramına-içeriğine saldırmayı amaçlamaktadır. Bir tür protokol saldırısı, tersinir filigranlar kavramına dayanmaktadır. Tersine çevirmenin arkasındaki fikir, saldırganın filigran verisinden kendi filigranını çıkarması ve filigran verisinin sahibi olduğunu iddia etmesidir. Bu, verilerin gerçek mülkiyeti ile ilgili olarak belirsizlik yaratabilir. Telif hakkı koruma uygulamaları için filigranların değiştirilemez olması gerektiği gösterilmiştir. Filigran teknolojisinin ters çevrilemez olması şartı, filigran olmayan bir belgeden filigran çıkarmanın mümkün olmaması gerektiği anlamına gelir. Bu soruna bir çözüm, filigranları tek yönlü işlevler kullanarak sinyale bağımlı hale getirmek olabilir. Başka bir protokol saldırısı kopya saldırısıdır. Bu durumda amaç, filigranı tahrip etmemek ya da tespitini bozmamak, ancak filigranı veriden filigranı tahmin etmek ve hedef veri adı verilen başka bir veriye kopyalamaktır.

Tahmini filigran, algılanamazlığını gidermek için hedef verilerin yerel özelliklerine uyarlanmıştır. Kopyalama saldırısı, hedef verilerdeki geçerli bir filigran, ne filigran teknolojisi hakkında ne algoritmik bilgi ne de filigranın anahtarı bilgisi ile üretilemediğinde uygulanabilir. Yine, sinyale bağlı filigranlar kopya saldırısına karşı dirençli olabilir (Patel ve Alpesh, 2014).

BÖLÜM 5

SAYISAL ÇAĞDA TELİF HAKKI KORUMASI

Yeni binyıl, daha geniş bir internet kullanımıyla daha yaygın ve yoğun bir Sayısal Çağ getirmiştir. Nikolai Kondratiev (bir sovyet ekonomisti), dünya sanayi ülkelerinin sanayi devrimlerinin başlangıcından bu yana art arda büyüme ve gerileme yaşadıklarını varsaymıştır (Stutz ve Warf, 2005). Daha sonra bilim adamları, şu anda bir bilgi teknolojisi dalgasında (Kondratiev'in 5. Dalgası olarak bilinir) yaşadığımızı iddia etmişlerdir. Bu nedenle, sayısal çağ bugün iş dünyasını önemli ölçüde etkilemiş ve e-ticaret faaliyetlerine yol açmıştır.

İletişim ve bilgisayar teknolojisi bir araya gelmiş ve bilgi depolama, işleme ve iletişim maliyetlerinin düşük olması ile karakterize edilen "yeni bir tekno-ekonomik paradigmaya" yol açmıştır (Stutz ve Warf, 2005). Sonuç olarak, fikirlerin ifadesini koruyan daha kapsamlı ve uygulamalı bir sayısal telif hakkı korumasına ihtiyaç duyulmakta olduğu tespit edilmiştir.

5.1. Fikri Mülkiyet Haklarına (IPR) Genel Bakış

Son yıllarda, Fikri Mülkiyet (IP) koruması küresel olarak daha fazla önem kazanmış ve politika yapıcı, analist ve yatırımcıların ilgisini çekmiştir. Bowyer (1996), asıl amacın, insanların topluma fayda sağlayabilecek yeni ve faydalı şeylerin geliştirilmesini üstlenmesi ve iş dünyasında adalet kavramlarını uygulamak için gerekli motivasyonu korumak olduğunu belirtmiştir. Bu nedenle, güçlü fikri mülkiyet koruması, yatırım koşullarını artırarak, yerel sanayideki kalkınmayı teşvik ederek ve ekonomik büyüme sağlayan daha fazla yatırım sağlayarak bir ülkeyi geliştirmektedir (WIPO, 2007). Ayrıca, bir araştırmalarda yatırımcı ülkelerin %86 ile %100'ünün bir ülkede Fikri Mülkiyet Hakları (IPR)'nın gücünün yatırım kararını etkilediğine inandığını açıklamaktadır. Çünkü

yatırımcıların karlı olması için korumalı bir sayısal iş ortamına ihtiyaçları bulunmaktadır (Davies ve Withers, 2009). Ayrıca, bilginin sayısallaştırılması ve araştırma ağlarının büyümesi bilim ve fikri mülkiyet korumada teknoloji topluluklarının eğilimini hızlandırmıştır (Chareonwongsak, 2002).

5.1.1. Tanımlı Fikri Mülkiyet Hakları

Fikri Mülkiyet, fikri mülkiyet koruması almaya hak kazanabilmesi için maddi forma indirgenmesi gereken maddi olmayan mülkiyet haklarıyla ilişkilendirilir. Fikri mülkiyet hukuku, ortak yasa (içtihat veya "yargılayan" yasalardan türetilmiş yazılı olmayan yasalar) ve tüzükler (Parlamento Yasası) ile yönetilir. E-ticaret için fikri mülkiyet haklarının ana formları 4 patente bölünebilir; Patentler, Ticari Sır, Telif Hakkı ve Ticari Markalar (Bowyer, 1996).

Patent, mucitler ve toplum arasında, genellikle yeni ürün ve teknoloji ve bilimsel buluşlar veya yenilikler alanındaki işlemler için verilen bir koruma şekli olan bir sözleşmedir (Bowyer, 1996). Ticari Sırlar, sahibine diğerlerine kıyasla bir işin "nasıl yapıldığını bilme (know how)" olarak adlandırılan rekabet avantajı sağlar. Sözleşmeli olarak tescil ettirilmesi ve korunmasına gerek yoktur. Telif hakkına gelince, siber uzayda önemli bir fikri mülkiyet sorunu olan fikirlerin ifadesini ve insan yaratıcılığının ürününü korur. Koruması belirli bir süre devam eder ve yaratılan iş oluştuğu anda etkilidir. Ve son olarak ticari marka, ticari işlem sırasında mallarını veya hizmetlerini tanımlamak için işletmeler tarafından kullanılan bir kelime, sembol veya grafik işaretidir, web siteleri alan adları buna bir örnektir. Yasal koruma sağlamak için ülkede kayıtlı olmak zorundadır ve diğer üçünden farklı bir ömre sahip değildir (Nasir, Ponnusamy & Lee., 2008).

5.2. SAYISAL ÇAĞDA TELİF HAKKI

Telif hakkı, internet çağında gittikçe önem kazanan birçok fikri mülkiyet hakları formunun dalıdır. Peterson telif haklarının geliştirilmesinin, korunmaya değer olanın, korunmaya değer ilk model olduğu ilkesine dayandığını iddia etmiştir (Longdin, 2005). Telif hakkı 16. yüzyılda matbaa endüstrisinde yer almakta olup, modern haliyle Bern Sözleşmesinden geliştirilmiştir. Bugün, Dijital

Binyıl Telif Hakkı Yasası 1998 ABD Telif Hakkı mevzuatı ve 1987 Telif Hakkı Yasası ve 1997 Telif Hakkı (Değişiklik) Yasası olarak karşımıza çıkmıştır.

5.2.1. Telif Hakkı ve İnternet

İnternet, ABD'de ARPANET adı verilen askeri ağın belirli bir kısmının sivil kullanıma açılmasıyla ortaya çıkmıştır. Başlangıçta (1950-1975), bu ağ "salyangozun hızı" ile tabir edilebilecek bir yavaşlıkta çalışıyordu. Daha sonra belirli bir protokol mimarisiyle daha hızlı hale getirilmiştir. 1980'li yıllarda daha geniş bir kullanım oranına ulaşmış ve günümüzde tüm dünyaya yayılmıştır. Şimdi, ortak bir iletişim protokolünü paylaşan dünya çapında bir bilgisayar ağıdır, dolayısıyla coğrafi konumdan bağımsızdır ve dünya küresel topluluğunu bütünleştirir (Nasir vd., 2008).

İnternet kullanıcıları 1994'te 13 milyardan 2000'de 300 milyona yükselmiş (Cerf, 2000), böylece ticari kuruluşların katılımı ve yeni bir sosyal alan olması daha cazip hale gelmiştir (Martin, 2004). Yaygın büyümesine ve kullanımına rağmen, telif hakkı ihlallerini engellemede en büyük zorluk ortaya çıkmakta ve siber alanda arttırılmış ve zorunlu bir telif hakkı koruması gerektirmektedir.

5.2.2. İnternette telif hakkı ihlali

İnternet, metinlerin, görüntülerin, fotoğrafların ve seslerin iletimi için kullanıldığından dolayı, telif hakkının uygulanması kaçınılmazdır (Nasir vd., 2008).

Birçoğunun genel kavramı ve içeriği (nosyon), internette bulunan herhangi bir şeyin kamuya açık olduğu ve yazar / sahibin izni olmadan alınabileceği ve böylece milyarlarca dolar gelir kaybına neden olabileceği yönündedir. Temelde, İnternet küresel bir korsanlık endüstrisine olanak sağlamıştır (Friedman, 1997). Milyonlarca insan aynı anda herhangi bir sayısal belgeyi okuyabilir ve ayrıca çalabilir. Dolayısıyla durum dünya çapında mevcut mevzuatın yetersizliğine işaret ediyor gibi görünmektedir.

5.2.3. ABD Telif Hakkı Yasası

1976 Telif Hakkı Yasası ve sonraki tüm telif hakkı değişikliklerini fikri mülkiyet haklarının tescil edilmesinden Telif Hakkı Bürosu sorumludur. Amerika Birleşik Devletleri telif hakkı yasası, Amerika Birleşik Devletleri Kanunu'nun 17'nci başlığının 17'den 8'e ve 10'undan 12'nci bölümlerinde bulunmaktadır. Mevcut telif hakkı yasası için temel çerçeveyi sağlayan 1976 tarihli Telif Hakkı Yasası, 19 Ekim 1976'da Pub olarak çıkarıldı. L. No. 94-553, 90 Stat. 2541. 1976 Yasası, 17. başlıktaki telif hakkı yasasının kapsamlı bir revizyonuydu. Aralık 2011'de bu genel basımın son baskısından bu yana yürürlüğe giren önemli telif hakkı mevzuatı, Kilit Açılan Tüketici Seçimi ve Kablosuz Rekabet Kanunu ve 2014 STELA Yeniden Yetkilendirme Yasasını içermektedir.

ABD Telif Hakkı yasası, baskı grupları ve lobiciler tarafından yapılan büyük baskılara yanıt olarak, Dijital Binyıl Telif Hakkı Yasası (DMCA) adıyla 1998 yılında çıkarılmıştır. Özellikle, ABD Telif Hakkı yasası, İnternet konularını çoğu ülkeden daha iyi ele almaktadır.

Kapsanan ana konular arasında aşağıdakiler yer alır;

a) kar amacı gütmeyen amaçlar için muafiyetin adil kullanımı; ve
b) ISS'nin sorumluluğunu sınırlamak (1976 Telif Hakkı'nın 107. Maddesi).

Telif hakkıyla ilgili sorunları çevreleyen birçok görüş ve eleştiri barındırmaya çalıştığı görülmesine rağmen yine de başarısı hala devam etmektedir (Nasir vd., 2008).

5.2.4. Avrupa Birliği (AB) Telif Hakkı Yasası

Fikri Mülkiyet Antlaşması AB Direktifi, Roma Antlaşması'nın (2004) iç pazar hükümleri uyarınca yapılmıştır. Tüm üye devletlerin, sahtecilik ve korsanla mücadelede etkili, caydırıcı ve orantılı çözümler ve cezalar uygulamalarını gerektirir. Sayısal telif haklarının uygulanmasında ilave birçok önlem var gibi görünmektedir. Bundan önce 2002 yılında, bilgi ekonomisinden ziyade bilgi toplumu üzerine vurgu yapan AB Telif Hakkı Direktifi uygulanarak, ekonomik kaygıların yalnızca böyle bir toplumun gelişimini teşvik etmek için tasarlanan

hükümet eyleminde dikkate alınması gerektiği vurgulanmıştır. Yönerge aynı zamanda yaratıcılığın ve canlı kültürel alanın önemini korurken, AB içindeki güvenlik alanında "yüksek teknoloji" araştırmalarını teşvik etmektedir (Nasir vd., 2008).

İnternet'in özelliği yasayı geçersiz kılmıştır. Bu nedenle soru, telif hakkı teknolojinin ilerlemesiyle sarsılıp sarsılmadığı ve sayısal çağda önemli olup olmadığı sorusudur. Kuşkusuz, mevcut Telif Hakkı yasaları Telif Hakkı sahiplerine koruma sağlar, ancak bazı dezavantajlara sahiptir. Telif hakkı korumasının insanlara uygulanmasının etkinliği konusunda bazı şüpheler ortaya atılmıştır. İnternetin sınırsız doğası, diğer yargı alanlarıyla daha yakın bir ilişki ve uluslararası örgütlerle yakın iş birliği çağrısında bulunmaktadır. Herhangi bir yetkisiz kullanımı önlemek için toplum Telif Hakkı koruması gerekliliği konusunda eğitilmelidir (Nasir vd., 2008). Mevzuat, Telif Hakkı sahiplerinin ihlal veya ihlal durumunda tazminat talep etmeleri veya bir eylemde bulunmaları için bir temel oluşturabilir. Bu, toplumda değerleri göz ardı eden sembolik bir güce sahip olan Kanun'dan kaynaklanmaktadır; Toplum artık fikri mülkiyet korumasını, ifade yaratmanın benzersiz bir nedeni olarak kabul etmediğinde, ahlaki altyapı daha önce yasalaştırılan düzenlenmelere aykırı hale gelmiştir.

Bazı kullanıcılar, yazılım kopyalamanın, veri indirmenin ve internetten izinsiz müzik kopyalamanın kabul edilebilir olduğunu ve anlaşılabilir bir kültür olduğunu görebilmektedirler. Yine de bunun bir Telif Hakkı ihlali olduğunun farkındadırlar. Bu, etik eksikliğini ve yerleşen ciddi bir tutum sorununu göstermektedir. Bazıları Telif Haklarını korumak için teknolojik araçlarla korunmasına çalışmış olsa da teknolojinin nihai çözüm olmadığı iddia edilmektedir. Bu amaçla, Telif Hakkı sahipleri İnternet'te hayatta kalacaktır, ancak gelecekte kullanıcılara makul miktarda özgürlük verilmesi ve Telif Hakkı sahiplerinin çoğaltma haklarının korunması arasında bir denge sağlanması gerekmektedir. Bu başarılırsa, Telif Hakkı amacına hizmet etmiş olmaktadır (Nasir vd., 2008).

5.3. İNTERNET TELİF KANUNU VE KORSANLIĞI

Telif hakkıyla korunan eserlerin, özellikle de müziğin korsanlığı, internet tabanlı suçun temel taşıdır ve fikri mülkiyeti korumak için tasarlanan modern mevzuat için en önemli itici güçtür. Wall (2003) "siber korsanlığı", "görüntüler, müzik, ofis yardımcıları veya etkileşimli deneyimler" dâhil olmak üzere, internette "yaratılmış veya popüler hale getirilmiş yeni fikri mülkiyet biçimlerinin tahsis edilmesi" olarak tanımlamaktadır. Bu suçlar çoğu zaman böyle sayılmaz. Telif hakkı yasası, "fikirler, buluşlar, işaretler, bilgiler ve ifade" de dahil olmak üzere "maddi olmayan" mülk ile ilgili olduğu için, bu mülkiyet biçimlerinin diğer biçimlerden daha az "özel" olduğuna inanmak için genellikle sebep vardır (Bently, Davis & Ginsburg, 2010). Bu yazar bunun böyle olmadığını savunmaktadır.

Fikri mülkiyet algısının, diğer mülkler gibi daha az somut olarak algılanmasının, bu mülkleri korumanın daha az gerekli olmasının nedeni olduğunu savunmak, etik boyutu olarak çok önemli bir husustur. Lysonski ve Durvasula (2008) tarafından yapılan kapsamlı bir çalışmada, bu araştırmacılar internetteki müzik korsanlığının durumunu düşündüklerini, "yasal işlem ile caydırıcı" olduklarını iddia etmişlerdir (Lyonski ve Durvasula, 2008). 300'den fazla üniversite öğrencisinin yaptığı bir çalışmada, telif hakkı kapsamındaki eserlerin ve katılımcıların fikri mülkiyete sahip olmadığı eserlerin yasa dışı indirilmelerinin "etik olarak yanlış olmadığına dair güçlü bir inanca dayandırıldığını" iddia etmişlerdir (Lyonski ve Durvasula, 2008). Sonuç olarak, bu araştırmacılar, bu tür bir etkinliği engellemek için olumsuz sonuçların yanı sıra daha etkili bir yol bulmanın gerekli olduğunu savunmaktadırlar.

İnternetteki telif hakkı ve fikri mülkiyet haklarını bilerek ihlal eden kişiler, "eşler arası dosya paylaşımı" ile korsanlıkla mücadele etmektedir. 2011 yılında "İnternetin % 28'i kullanıcılar dünya genelinde aylık olarak yetkisiz servislere erişiyorlar" (IFPI, 2012). Bu korsanlığın yayılmasında etkili olan bir diğer unsur ise, 2003'te 605 milyon kullanıcıyı 2008'de 1 milyarın üzerine çıkaran "internetin kendisinin hızlı genişlemesi" ve 2008'de "genişbant" internet erişimindeki kullanıcıları "büyük miktarda sayısal içeriği sıkıştırılmış biçimde hızlı bir şekilde indirmek için" hızlı büyüme gerçekleşmiştir (Bently vd., 2010).

İnternetteki korsanlığı ve fikri mülkiyeti ve telif hakkı ihlallerini yasaklama ya da azaltma yasasının en büyük savunucularından biri, müzik endüstrisi, özellikle Amerika Kayıt Endüstrisi Birliği (RIAA) ve Uluslararası Fonografik Endüstrisi Federasyonu (IFPI) olmuştur. Pfanner (2010), bu endüstrilerin internet korsanlığının bir sonucu olarak, geleneksel medya satışlarında, özellikle de kompakt disklerin satışında sürekli bir düşüş olduğunu ortaya çıkardığını bildirmektedir. IFPI'nin sayısal korsanlığın 2004 ve 2009 yılları arasında "küresel müzik satışlarında yüzde 30'luk bir düşüş" ile sonuçlandığını savunmuştur (Pfanner, 2010). iTunes gibi hizmetleri kullanan meşru (genellikle sayısal haklara sahip) müzik dosyalarının satışında bir genişleme ve Pandora ve Spotify gibi yayın hizmetlerinde bir genişleme olsa da, kayıt endüstrisi gelirlerini kaybetmeye devam etmiş ve bu suçu devam ettirmiştir.

Meşru sayısal satışlar 2009-10 yıllarında yüzde 27 oranında artarken, kompakt disklerin (çok daha karlı bir ürün olan) satışı aynı yıllarda %16 azalırken, sanayi gelirinin 2009 yılında 17,5 milyar dolardan 2010 yılında 15,8 milyar dolara düşmesiyle sonuçlanmıştır (Pfanner, 2010).

Rekor endüstrisinin iddialarıyla tartışmak zordur. Sayısal müziğin meşru satışındaki dünya çapındaki artışa rağmen, internetten indirilen tüm müziğin yüzde 95'i, son yıllarda değişmeyen bir rakam olarak korsanlaştırılmaktadır (IFPI, 2009). Ne olursa olsun kaydın, sayısal alanın potansiyeline uygun bir şekilde adapte olmuş, bu sektörün neden katı mevzuat için savunuculuk yaparak çıkarlarını korumak zorunda kaldığını anlamak zor değildir.

Sayısal Haklar Yönetimi'ni uygulamak çok zordur. Analog boşluk, şunu belirtir, bir kullanıcı tarafından gözlemlenebilecek her şey de kopyalanabilir. Bu nedenle güvenliğini sağlamak imkânsızdır. Telif hakkı ihlallerine karşı içerik, yine de dağıtımını yaparken. Damgalama ve diğer sayısal güvenlik biçimlerinin her zaman düzeltilebilir olduğu kanıtlanmıştır.

5.4. SAYISAL TELİF HAKKI KORUMASINDA DAMGALAMA

İnternetin yaygın kullanımı ve akış ortamı ve sıkıştırma teknolojisindeki gelişmeler, sayısal müzik, resim, video, kitap ve oyunlar Internet üzerinden anında

son kullanıcılara dağıtılabilmektedir. Çoğu sayısal servis sağlayıcı, sayısal içeriklerini yalnızca CD'ler aracılığıyla değil, aynı zamanda bilgisayar ağları üzerinden de satmaktadır. Bununla birlikte, sayısal hakların korunması ve yönetimi olmadan, sayısal içerik kolayca kopyalanabilir, değiştirilebilir ve medya şirketlerinde gelir kaybına neden olabilecek çok sayıda alıcıya dağıtılabilmektedir.

Dünyanın en büyük ikinci tüketici elektroniği üreticisi olan Sony, müzik sektöründe 2002 yılında üç ay içinde 10,3 milyar yen (160 milyon $) zarar verip kar kaybına neden olduğu için "sayısal korsanlığı" suçlamıştır (Suzuki, 2002). Ticari sayısal fikri mülkiyeti korumak ve sayısal korsanlığı önlemek için, sayısal içeriğe yetkisiz erişimi engelleyen ve yöneten bir sisteme ihtiyaçları olduğunu savunmuştur.

Sayısal Hak Yönetimi (Digital Rights Management-DRM) sistemleri, yüksek değerli sayısal varlıkları korumak ve dağıtım ve kullanımlarını kontrol etmek için kullanılabilir. Bir DRM sistemi, sayısal içeriğe yetkisiz erişime karşı kalıcı bir içerik koruması sunmalı ve yalnızca uygun yetkiye sahip kişilere erişimi sınırlandırmalıdır. DRM sistemi bu işlemleri yapmak için şifreleme, filigran ve hak yönetimi dillerini kullanmaktadır (Karlıdağ, 2010).

Farklı platformlarda (örneğin PC'ler, dizüstü bilgisayarlar, PDA'lar, mobil cihazlar) farklı türlerde sayısal içeriklerin (örneğin müzik dosyaları, video akışları, sayısal kitaplar, görüntüler) kullanım haklarını yönetmek daha esnek olmalıdır.

DRM'deki temel kavram, sayısal lisansların kullanılmasıdır. Sayısal içeriği satın almak yerine, tüketici kendisine belirli haklar veren bir lisans satın alır. Lisans, sayısal içerik için belirli kullanım kurallarını belirten bir sayısal veri dosyasıdır. Kullanım kuralları, erişim sıklığı, son kullanma tarihi, diğer cihazlara aktarımın kısıtlanması, izinlerin kopyalanması vb. gibi bir dizi kriterle tanımlanabilir. Genellikle sayısal içerik ve lisanslar ayrı ayrı depolanır, bu da sistemi korumalı içeriğin kullanıcılar arasında serbestçe dağıtılabileceği şekilde daha esnek hale getirir ve lisans talepleri daha sonra gerçekleşebilir.

Sayısal damgalama, altyazı ve telif hakkı kontrolü de dâhil olmak üzere çeşitli amaçlarla sayısal içeriğe eklenebilecek algılanamayan bir sinyaldir. Damgaların önemli bir özelliği, dosya filtreleme ve sıkıştırma gibi ortak sinyal

dönüşümlerine karşı sağlamlık ve kurcalamaya karşı dirençtir (Cox ve Miller 1997).

DRM sistemlerinde damgalar ciltleme için kullanılabilir. İçerik sahipleri, içeriğin alıcısı ve ödeme bilgileri gibi sayısal içeriğe ilişkin bilgiler, içeriğin telif hakkını kontrol etmek ve belirlemek için özel damgalama okuma yazılımıyla kurtarılabilir olmaları gerekmektedir.

Damgalar, sayısal korsanları izlemek için adli olarak da kullanılabilir. Birçok şirket webde düzenli olarak arama yapan ve damgası alınmış sayısal dosyaları test eden bir web örümcek hizmeti sağlar. Bu hizmetin amacı, kayıtlı içerik sahiplerinin telif hakkı ihlallerini tespit etmektir. Telif hakkı ihlali tespit edildiğinde, içerik sahiplerine bildirilecek ve ihlal eden kişi muhtemelen mahkemeye gönderilecektir.

BÖLÜM 6

SONUÇ VE ÖNERİLER

Damgalama, birçok uygulama içeren çok aktif bir araştırma alanıdır. Nispeten yeni bir alan olmasına rağmen, mesajları sayısal sinyallere gizlemek için önemli algoritmalar üretilmiştir. Bunlar birçok farklı model ile tanımlanabilmektedir. Bu yazıda bu modeller için iki geniş kategori tanımlanmıştır. Bunlar iletişim tabanlı modeller ve geometrik modellerdir. İletişim tabanlı modeller, yan bilgiyi kullananlara ve kullanmayanlara da ayrılabilir. Bir örnek yan bilgi modellerini göstermek için bu sistemlerin her birinin kendi sistemi ve yan bilgi modellerini göstermek için iki örnek sistem kullanılmıştır.

Avantajlar ve dezavantajlar ve hangisinin kullanılacağının seçimi, alttaki uygulamanın her biri, bir başkası için önemli bazı damgalama özelliği satmaktadır.

Elbette bu yazıda verilen örnekler, damga basmaya yönelik birçok farklı yaklaşımın yalnızca küçük bir örneğidir. Bahsedilmemiş diğer yaklaşımların örnekleri, frekans alanında çalışan ve DCT katsayısı ve dalgacık katsayılarından yararlananları içermektedir.

Sayısal damgaların kullanımı, benzersiz bir tanımlayıcı için bir izleme ve yayın içerik hakları sahibini ve dağıtıcılarını içermektedir. Günümüzde kullanılan sayısal damgalara bir örnek, bir takip altyapısı, bir izleme istasyonu olabilir. Gömülü damga çevrimiçi olarak algılanabilmektedir. Bu nedenle, bilginin uygunsuz kullanımı tespit edildiğinde, bu eylem içerik sahibine bir rapor gönderir ve bu da bilginin uygun şekilde lisanslanmasında yardımcı olmaktadır.

Telif haklarının sağlanmasında faydalanmanın yanı sıra dağıtım gelirini de arttırarak daha iyi ve verimli bir teknoloji sunmaktadır. İşaret işleme operasyonlarında kurcalamaya karşı direnç elde etmek zordur. Tüm bu işlemlerin yardımı ile damga kullanımı potansiyel bir çözüm görevi gördüğü için açık

kaynaklı ağlar için içerik sağlanmaktadır. Verilerin yanlış tahsis edilmesi, birden fazla damga, şifreleme gibi başka teknikler kullanılarak azaltılabilse de, bu içeriği daha iyi korurken çeşitli problemler çıkabilmektedir.

Bu araştırma boyunca, sayısal damgalamanın önemi, çeşitli ortamlar için (metin, görüntü, hareketli görüntü, ses) damgalama gereklilikleri ve damgalama tekniklerinin en önemli uygulama alanlarından bahsedilmiştir. Ek olarak, damgalama tekniklerinin sınıflandırılması ve damgalama teknikleri ile güvensiz iletişim problemi arasındaki ilişkileri ve damgalama tekniklerinin atak sınıflandırmalarını incelenmiştir. Ayrıca sayısal damgalama ile ilgili çalışmalar incelenmiş ve konumuzla ilgili birçok araştırmacının yaptığı önceki çalışmalar taranmıştır.

Modern yaşamımızda, bilgi ve iletişim teknolojisine bağlılık giderek artmaktadır ve bilgi teknolojilerinin kullanımına olan bu artan ihtiyaç, yaşamımızı birçok açıdan olumlu ya da olumsuz şekillerde etkileyebilir. Bu nedenle, sayısal ortamın Internet gibi güvenli olmayan ortamlardan veya Yerel Alan Ağları (LAN), Kişisel Alan Ağları (PAN) ve Geniş Alan Ağları (WAN) gibi özel ağlar üzerinden iletilmesi basit olmamaktadır.

İletilen sayısal multimedya sahipliğini kanıtlamak, telif hakkı korumasını ve mülkiyet haklarını geliştirmek için sağlam bir damga düzenine sahip olma gerekliliğini ortaya koymaktadır. Çeşitli bilim adamları tarafından önerilen ve tanıtılan teknikler vardır, ancak en belirgin ve ünlü teknik damgalamadır. Damgalama, verileri doğrudan multimedya içeriğine karıştırır ve bu işlem genellikle damganın konumunu belirleyen bir anahtar içermektedir.

Görüntü işleme ile ilgili bilim ve teknoloji, hızlandırılmış bir evrim şeklidir. Modern teknolojinin kullanımına olan güven ve sayısal nesnelerin çoklu iletişim türleriyle aktarılması gerekliliği nedeniyle Kanallarda, bu tür kanalların bazıları, damgalama tekniklerini telif hakkı koruması ve çalışmaların geliştirilmesinde çalışmayı destekleyen araçlar olarak içeren çok çeşitli uygulamalara ek olarak çeşitli şekillerde güvensiz olabilmektedir. Gelecekteki çalışmalar için aşağıda bazı öneriler verilmiştir:

- Yeni damgalama tekniklerinin önerisi ile bir ana görüntüye gömülebilecek bilgi miktarını artırmak;
- Ana görüntüye daha fazla bilgi eklerken görünürlüğünü etkilemeyen daha fazla şeffaflık sağlamak;
- Daha yüksek SNR ve PNSR değerleri elde ederek görüntü kalitesi açısından daha iyi değer veren yeni damgalama teknikleri önermek;
- Görüntü karıştırma teknikleri gibi mevcut olanlara ek özellikler ekleyerek algoritmaların sağlamlığını artırmak.

KAYNAKLAR

Alasafi, L. (2016). *Güvensiz Haberleşme Ortamlarında Telif Hakkı Koruma Amaçlı Dayanıklı İmge Damgalama*. (Yüksek Lisans Tezi). Süleyman Demirel Üniversitesi/Fen Bilimleri Enstitüsü/Elektrik Elektronik Mühendisliği Anabilim Dalı, Isparta.

Amit Kumar, S. (2015). Robust and Imperceptible Dual Watermarking for Telemedicine Applications. *Wireless Personal Communications*, 80(4), 1415-1433.

Anderson, R. (Ed.) (1996). *Information Hiding*. Berlin: Springer-Verlag.

Anonim, (2008). Beyond traditional DRM: Moving to Digital Watermarking & Fingerprinting in Media Monetization. 24 Eylül 2008 tarihinde http://www.multimediaintelligence.com adresinden erişildi.

Anonim, 2007. Image Steganography and Steganalisys. 24 Mart 2019 tarihinde http://www.ims.nus.edu.sg/Programs/imgsci/files/memon/sing_stego.pdf adresinden erişildi.

Atallah, M., Raskin, V., Hempelmann, CF., Karahan, M., Sion, R., Topkara, U., Triezenberg, KE. (2002). Natural language watermarking and tamperproofing. *Proceedings of the 5th information hiding workshop*, 196-212.

Barni, M., Bartolini, F., Cox, I.J., Hernandez, J., and Perez-Gonzalez, F. (2001). Digital Watermarking for Copyright Protection: A Communications Perspective. *IEEE Communications Magazine*, 39(8), 90-133.

Bender, W., Gruhl, D., Morimoto, N., Lu, A. (1996). Techniques for data hiding. *IBM Systems Journal*, 35(3&4), 313-336.

Bently, L., Davis, J., and Ginsburg, J.C. (2010). *Copyright and Piracy: An Interdisciplinary Critique*. England: Cambridge University Press.

Boney, L., Tewfik, A., Hamdy, K. (1996). Digital Watermarks for Audio Signals. *IEEE Int. Conf. on Multimedia Computing and Systems*, 473- 480.

Bowyer, K. (1996). *Ethics & Computing*. California: IEEE Computer Society Press.

Cai, L., He, M. Z., Liu, Q. ve Yang, X. L. (2004). Digital Image Encryption and Watermarking by Phase-Shifting Interferometry. *Applied Optics*, 43(15), 3078-3084.

Cerf, V. (2018). Internet in the 21st Century ISOC Luxembourg. *Communications of the acm*, 61(10), 5.

Cevdet, A. (2018). Dayanıklı Sayısal Damgalama ve Damga Güvenliği. 24 Mart 2019 tarihinde https://docplayer.biz.tr/104733466-8-dayanikli-sayisal-damgalama-ve-damga-guvenligi.html adresinden erişildi.

Chareonwongsak, K. (2002). Globalisation and Technology: How will they change society. *Technology in Society*, 24(3), 191-206.

Chen, C. (1999). *On the Study of Watermarking Application in www Modeling, Performance Analysis and Application of Digital Image Watermarking Systems*. (Yüksek lisans tezi). National Tsing Hua Üniversitesi, Hesinchu/Taiwan.

Cox, I. J., Miller, M.L., Bloom, J.A. (2000). Watermarking Applications and their Properties. *Proc. of International Conference on information Technology*, 6-10.

Cox, I. J., Kılıan, J., Leıghton, T., And Shamoon, T. (1997). Secure Spread Spectrum Watermarking for Multimedia. *IEEE Transactions on Image Processing*, 6(12), 1673–1687.

Cox, I.J. and Miller, M.L. (1987). A Review of Watermarking and The Importance of Perceptual Modeling. *roc. SPIE Conf. on Human Vision and Electronic Imaging II*, 3016, 92-99.

Davies, W. & Withers, K. (2009). *Public Innovation: Intellectual Property in a Digital Age United Kingdom*. Institute for Public Policy Research.

Emek, S., Pazarcı, M., Yücel, M. (2004). Sabit İmgeler İçin ADD-AKD Tabanlı Sayısal Damgalama Yöntemi. *IEEE Sinyal İşleme ve İletişim Uygulamaları*, SIU'04, 34-36.

Erçelebi E., Tokur Y., Bayık B. (2002). Geometrik Şekiller ile Frekans Bölgesinde Sayısal İmge Damgalama. *Bursa ELECO'2002 Elektrik, Elektronik ve Bilgisayar Mühendisliği Sempozyumu ve Fuarı*, 319-323.

Eskicioğlu A. M., Delp, E. J. (2001). An Overview of Multimedia Content Protection in Consumer Electronics Devices. *Elsevier Signal Processing : Image Communication 16*, 681–699.

Fidrich, J., Baldoza, A., Simard, R. (1998). Robust Digital Watermarking Based on Key-Dependent Basis Functions. *In Proc. of International Information Hiding Workshop*, 1525, 143-157.

Friedman, M.S. (1997). Infojacking: Crimes in the Information Superhighway. *Computer Forensics Online*, 24 Temmuz 2007 tarihinde http://www.shk-dplc.com/cfo adresinden erişildi.

Hembrooke, E. F. (1954). *United States Patent 3,004,104*. 24 Mart 2019 tarihinde https://patents.google.com/patent/US3004104A/en adresinden erişildi.

Hsu, C. T., Wu, Ja-L. (2000). Image Watermarking By Wavelet Decomposition. *Academy of Information and Management Sciences Journal*, 3(1), 70- 86.

IFPI . (2009). IFPI Digital Music Report 2009. 24 Mart 2019 tarihinde www.ifpi.org/content/library/dmr2009.pdf adresinden erişildi.

IFPI. (2012). IFPI Digital Music Report 2012. 24 Mart 2019 tarihinde http://www.ifpi.org/content/library/DMR2012_key_facts_and_figures.pdf adresinden erişildi.

Johson, N. F., Jajoda, S. (1998). Exploring Steganography: Seeing the Unseen. *IEEE Computing Practices*, 2, 26-34.

Karlıdağ, S. (2010). *Fikirlerimizin Sahibi Kim? - Türkiye Müzik Endüstrisinde Telif Hakları Politikaları*. İstanbul: Kalkedon Yayınları.

Katzenbiesser, S., Petitcolas, F. (2007). *Information Hiding Techniques for Steganography and Digital Watermarking*. London: Artech House.

Koch, E., Rindfrey, J., Zhao, J. (1996). Copyright Protection for Multimedia Data. *Digital Media and Electronic Publishing*, 203-213.

Kumar, M. N. (2004). *Watermarking Using Decimal Sequences*. (Yüksek lisans tezi). Louisiana State Üniversitesi, Louisiana.

Kurak, C., McHugh, J. (1992). A Cautionary Note on Image Downgrading. *Proceedings of the IEEE 8th Annual Computer Security Applications Conference*, Texas.

Kutter, M. Jordan, F., Bosson, F. (1997). Digital Signature of Color Images Using Amplitude Modulation. *Proc. of the SPIE*, 3022, 518-526.

Kutter, M., S. Voloshynovskiy, M., Herrigel, A. (1997). The Watermark Copy Attack. *Security and Watermarking of Multimedia Content, 3971, 371-380*.

Kutucu, H. ve Kaya, M. (2002). *Kriptografi ve Ağ Güvenliği Steganografi*. (Yüksek lisans tezi). Ege Üniversitesi/Uluslararası Bilgisayar Enstitüsü, İzmir.

Langelaar, Gerhard C., Setyawan, I., Lagendijk, R.L. (2000). Watermarking Digital Image and Video Data: A State-of-the-Art Overview. *IEEE Signal Processing Magazine*, 17(5), 20-47.

Le, T.H.N., Nguyen, K.H., Le, H.B. (2010). Literature Survey on Image Watermarking Tools, Watermark Attacks and Benchmarking Tools. *Second International Conferences on Advances in Multimedia (MMEDIA)*, 67-73.

Lee, Y., Chen, L. (2000). High Capacity Image Steganographic Model. *IEEE Proceedings - Vision, Image and Signal Processing*, 288 – 294.

Lin, E.T., Delp, E.J. (2005). A Review of Fragile Image Watermarks. *Video and Image Processing Laboratory (VIPER) School of Electrical and Computer Engineering Purdue University West Lafayette*, Indiana.

Longdin, L. (2005). Copyright Protection for Business Systems and Surveys. *20th BILETA Conference: Over-Commoditised; Over-Centralised; Over-Observed: the New Digital Legal World?*, Queen's University of Belfast, Malaysia.

Lysonski, S., and Durvasula, S. (2008). Digital piracy of MP3s: Consumer and Ethical Predispositions. *Journal of Consumer Marketing*, 25(3), 167-178.

Martin, P. (2004). Community & Identity in Cyberspace: An Introduction to Key Themes and Issues. *Human Affairs*, 2, 116-125.

Marvel, L. M., Bonceleti C. G., Retter, C. T. (1999). Spread Spectrum Image Steganography. *IEEE Transactions on Image Processing*, 8(8), 1075-1083.

Memon, N., Holliman, M., Yeung. M. (1999). On the Need for Image Dependent Keys in Watermarking. *Proceedings of the Second Workshop on Multimedia*.

Mesut, A.Ş. (2019). Bilgi Gizleme Teknikleri Yüksek Lisans Dersi Notları. 1 Ağustos 2019 tarihinde https://personel.trakya.edu.tr/andacs#.XRjIz-gzY2w adresinden erişildi.

Mohanty, S. P., Barni, M., Bartolini, F., Cappellini, V., Piva, A. (1998). A DCT-Domain System for Robust Image Watermarking. *Signal Processing*, 66(3), 357-372.

Mohanty, S. P., Ramakrishnan, K., Kankanhalli, M. (1999). A Dual Watermarking Technique for Images. *Proceedings of the 7th ACM International Multimedia Conference (ACMMM)*, 49-51.

Mohanty, S.P. (2008). Invisible Watermarking Based on Creation and Robust Insertion-Extraction of Image Adaptive Watermarks. *Article in ACM Transactions on Multimedia Computing Communications and Applications*, 5(2), 12:1-12:22.

Nasir, R., Ponnusamy, V., Lee, K.M. (2008). Copyright Protection In The Digital Era: A Malaysian Perspective. *Munich Personal RePEc Archive*, 8253, 1-16.

Patel, M., Alpesh, S. (2014). The Study of Various Attacks on Digital Watermarking Technique. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, 3(5), 1567-1570.

Petitcolas, F., Anderson, R., Kuhn, M. (1999). Information Hiding – a Survey. *Proc. of the IEEE*, 87(7), 1062-1078.

Pfanner, E. (2010). Music Industry Counts the Cost of Piracy. 24 Mart 2019 tarihinde http://www.nytimes.com/2010/01/22/business/global/22music.html?_r=0 adresinden erişildi.

Pu, Y., Liao, K., Zhou, J., Zhang, N. (2004). A Public Adaptive Watermark Algorithm for Color Images Based on Principal Component Analysis of Generalized Hebb. *Proc. Of IEEE Int. Conference on Information Acquisition*, 690-695.

Ravula, R. (2010). *Audio Watermarking Using Transformation Techniques*. (Yüksek lisans tezi). Louisiana State Üniversitesi, Louisiana.

Reddy, H. S. M., Raja, K. B. (2009). High Capacity and Security Steganography Using Discrete Wavelet Transform. *International Journal of Computer Science and Security*, 3(6), 462-472.

Ruia, X., Jinqiaob, C.X.S. (2013). A multiple watermarking algorithm for texts mixed Chinese and English. *Proc. Comput. Sci.*, 17, 844-851.

Schyndel, R. G., Tirkel, A. Z., Osborne, C. F. (1994). A Digital Watermark, *Image Processing Conference ICIP-94*, 2, 86-90.

Shieh, C., Huang, H., Wang, F., Pan, J. (2004). Genetic Watermarking Based on Transform-Domain Techniques. *Pattern Recognition*, 37(3), 555-565.

Shih, F. Y., Wu, S. Y. (2003). Combinational Image Watermarking in The Spatial and Frequency Domains. *Pattern Recognition*, 36(4), 969 – 975.

Srivadana, N. (2013). Digital Watermarking. *International Journal For Technological Research In Engineering*, 1(3), 13-17.

Stein, J.Y. (2000). *Digital Signal Processing: a Computer Science Perspective*. New York: Wiley-Interscience.

Stutz, F., Warf, B. (2005). *World Economy: Resources, Location Trade & Development* (4.Baskı), USA: Pearson.

Suzuki, H. (2002). Sony Innovation Guards Content. 5 Şubat 2002 tarihinde http://australianit.news.com.au/articles/0,7204,4874591%5E16681%5E%5Enbv%5E,00.html adresinden erişildi.

Swanson, M.D., Kobayashi, M., Tewfik, A.H. (1998). Multimedia Data Embedding and Watermarking Technologies. *Proc. of the IEEE*, 86(6), 1064-1087.

Takai, N., Mifune, Y. (2002). Digital Watermarking by a Holographic Technique, *Applien Optics*, 41(5), 865-873.

Tokur, Y. (2004). Sayısal Ses Verisinin ve Sayısal Görüntü Verisinin Telif Hakkının Korunması için Sayısal Damgalama. (Yüksek lisans tezi). Gaziantep Üniversitesi/Elektrik ve Elektrik Mühendisliği, Gaziantep.

Tseng, H., Chang, C. (2004). Steganography Using JPEG Compressed Images. *The Fourth International Conference on Computer and Information Technology*, China.

Wall, D. (2003). *Crime and the Internet*. New York: Routledge.

WIPO. (2007). IP Strategies and Innovation. 20 Şubat 2019 tarihinde http://www.wipo.int/ipdevelopment/en/strategies/national_ip_strategies.html#why adresinden erişildi.

Wolfgang, R. B. Podilchuk, C. I., Delp, E. J. (1999). Perceptual Watermarks for Digital Images and Video. *Proceedings of the IEEE*, 87(7), 1108- 1126.

Wu, C.T., Ja-Ling, H. (1999). Hidden Digital Watermarks in Images. *IEEE Transactions on Image Processing*, 8(1), 58-68.

Yavuz, E. (2008). *Duruk İmgelerde Damgalama ve Veri Saklama*. (Doktora tezi). Ankara Üniversitesi/Fen Bilimleri Enstitüsü Elektronik Mühendisliği Anabilim Dalı, Ankara.

Yeung, M., Mintzer, F. (1997). An Invisible Watermarking Technique for Image Verification. *International Conference on Image Processing*, 1, 680-683.

Yeung, M., Mintzer, F. (1998). Invisible Watermarking for Image Verification. *Journal of Electronic Imaging*, 7(3), 578-591.

Zhang, W., Zhu, W., Fu, Y. (2004). An Adaptive Digital Watermarking Approach. *Proc. of IEEE Int. Conference on Mechatronics and Automation*, 690-695.

Zhao, L., Cui, D.W. (2009). Text watermark algorithm based on tone of Chinese characters. *Comput. Eng.* 35(10), 142–144.

ÖZGEÇMİŞ

Sinan SERBESTOĞLU, 28 Şubat 1988 tarihinde M. Kemalpaşa/BURSA'da doğdu. Lise eğitimini Bursa'da tamamladıktan sonra 2014 yılında H. Ahmet Yesevi Uluslararası Türk Kazak Üniversitesi, Bilişim Teknolojileri ve Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü'nünden mezun oldu. 2015 yılında Trakya Üniversitesi Fen Bilimleri Enstitüsünde Bilgisayar Mühendisliği Anabilim Dalında yüksek lisans eğitimi almaya başladı. Halen Sağlık Bakanlığına bağlı Çerkezköy Devlet Hastanesinde çalışan Sinan SERBESTOĞLU evli ve bir çocuk babasıdır.