# Bölüm 3

# SAYISAL FİLİGRAN[1]

**Hüseyin Bilal MACİT[2]**
**Arif KOYUN[3]**

## 1. TANIM

Elektronik sistemlerinin yaygınlaşması ile veri üretimi her geçen gün kolaylaşmaktadır. Fotoğraf, ses ve video gibi verileri yakalamak için kullanılan cihazlara erişimin kolaylaşması, akıllı telefonların günden güne gelişen görüntü yakalama teknolojileri, geliştirilen veri sıkıştırma teknikleri, yeni veri depolama yöntemleri ve donanımları ile artan kişisel veri depolama imkânları; insanların sayısal medya üretim hızını günden güne arttırmaktadır. Diğer taraftan, düşük maliyetli ve hızlı olması, stoklama gerektirmemesi nedeniyle internet, sayısal medyalar için iyi bir dağıtım aracı haline gelmiştir. Özellikle akıllı telefonların yaygınlaşması, mobil ağların genişlemesi ve buna paralel olarak sosyal medya araçlarının kullanımının günden güne artması ile mobil cihazlar en fazla sayısal medya üreten araçlar durumuna gelmiştir. İnternette her geçen gün artan sayısal medya sayısı, yeni sorunları da beraberinde getirmektedir. İletişim kolaylığı ve işlem güçlerinin artması ile sayısal veriler bu iletişim ve depolama ortamında kayıpsız olarak kopyalanabilmekte ve çok hızlı bir şekilde dağıtılabilmektedir. Bu durum mahremiyet ve güvenlik sorunlarını da arttırmıştır. Kolayca dinlenebilen iletişim kanallarınca bireylerin okudukları her metin, çektikleri her fotoğraf, dinledikleri her müzik ve izledikleri her video takip edilebilir hale gelmiş ve veri güvenliği önceki çağlara göre çok daha büyük bir problem hale gelmiştir. Ayrıca sayısal veri üreticilerinin haklarının korunması, verilerin kötü niyetli müdahalelere karşı korunması ve hassas veriler ile ilgilenilen uygulamalarda veri güvenilirliğinin sağlanması önemli problemler olarak karşımıza çıkmaktadır

[1] Bu çalışma "Mobil cihaz görüntüleri için entropi tabanlı kırılgan damgalama metodu geliştirilmesi" başlıklı doktora tez çalışmasının bir bölümünü içermektedir.

[2] Dr. Öğr. Üyesi, Mehmet Akif Ersoy Üniversitesi, Bucak Zeliha Tolunay Uygulamalı Teknoloji ve İşletmecilik Yüksekokulu, Bilişim Sistemleri ve Teknolojileri Bölümü, hbmacit@mehmetakif.edu.tr ORCID iD: 0000-0002-5325-5416

[3] Dr. Öğr. Üyesi, Süleyman Demirel Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü AD, arifkoyun@sdu.edu.tr ORCID iD: 0000-0001-6701-363X

(Baraklı, 2014; Boyacı, 2017). Kişisel ve kurumsal verilerin iletişiminde, güvenlik, gizlilik konularında geleneksel kriptografi araçları yaygın olarak kullanılmaktadır. İletim kanalında her veri, modern matematiksel yöntemler ile oluşturulmuş algoritma ve anahtarlar ile şifrelenip taşınmaktadır. Ancak şifresiz verinin bir defa elde edilmesi, onun çoğaltılıp dağıtılması için yeterli olmaktadır. Bu durum yasa dışı kullanımların önünü açmaktadır. Birçok kişi ve kurum, içerik koruması ve orijinal ürün satışı problemleri ile karşı karşıya kalmıştır. Yasa dışı veri dağıtımı, yüksek kapasiteli sayısal kayıt cihazlarının çoğalmasıyla daha da artmıştır. Sayısal ortamın bu denli yaygın olmadığı önceki dönemlerde, ortalama bir müşterinin bir şarkıyı veya videoyu analog teypte çoğaltmasının tek yolu, orijinalinden daha düşük kalitede bir ikinci kuşak korsan kopya kaydetmesiydi. Sayısal cihazlarının yaygınlaşması ile bu medyalar, çok daha az kalite kaybı ile çoğaltılabilir hale geldiler. Böylece, medyaların çoğaltımı için bu kayıt cihazlarını ve dağıtım için interneti kullanan korsan içerik üreticiler, telif hakkı korumalı veya kişisel mahrem medyayı gerçek telif hakkı sahiplerine hiçbir ödeme yapmaksızın ve izinsiz olarak kolaylıkla kaydedebilir ve dağıtabilir hale geldiler. Bu sorun yeni veri gizleme yöntemleri aranmasına sebep olmuştur. Bir veri gizleme sisteminin en önemli gereksinimleri, veri yükü, algılanamazlık ve sağlamlık olarak bilinmektedir. Veri yükü; orijinal verinin taşıyabildiği gizli veri miktarını, algılanamazlık; gizli verinin yetkisiz kişilerden korunması durumunu, sağlamlık ise gizli verinin yetkisiz kişiler tarafından yapılabilecek saldırılara dayanma durumunu göstermektedir (Şatır, 2013).

Sayısal medyanın içerisine, başka bir bilgi gizlemek için medya üzerinde büyük değişiklikler yapılabilir. Ancak orijinal medyadaki büyük değişiklikler, üçüncü şahıslar tarafından fark edilebilir olacaktır (Öztürk, 2009). İnsan İşitme Sistemi (İİS), İnsan Görme Sistemine (İGS) göre nesnelerdeki küçük değişiklikleri algılama konusunda daha hassastır. Örneğin; İİS 2 Kilohertz (kHz) altındaki ses frekanslarındaki küçük değişiklikleri kolayca algılayabilmektedir. Ancak bu durum İGS için geçerli değildir. Dolayısıyla, bir ses verisini korumak için kullanılan güvenli veri gizleme yöntemi, bir resim verisi için uygulanabilir olmayabilir. Farklı medya türleri için farklı yöntemler kullanmak kaçınılmazdır (Chore ve Tiwari, 2017).

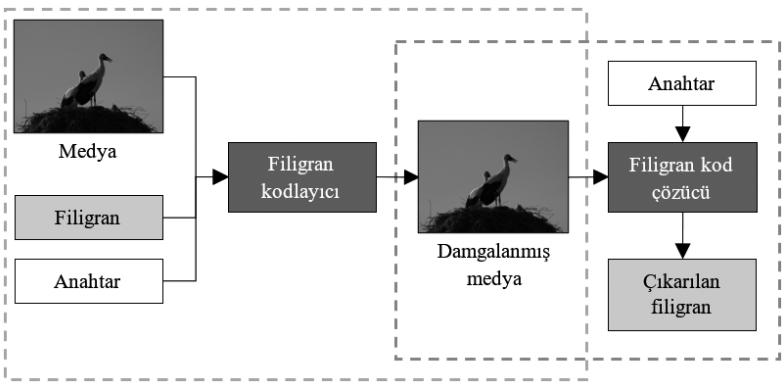
Temeli antik çağlara kadar dayanan veri gizleme yöntemleri, 21. yüzyıl sayısal ortamında etiketleme, sayısal imzalama, kriptoloji, damgalama ve steganografi olarak karşımıza çıkmaktadır (Yalman ve Ertürk, 2009). Parmak izi ekleme olarak da bilinen etiketleme; sayısal bir medyaya, tüketiciye dağıtılmadan önce medyanın telif haklarının korunması amacıyla yalnızca o tüketiciyi temsil eden

gizli bir bilginin tüketici tarafından algılanamayacak bir şekilde eklenmesi işlemidir (Arnold vd., 2003). Her tüketiciye verilen medya, içinde kendisine özel bir bilgi saklandığı için birbirinden farklıdır (Hamza, 2008). Etiketleme, amaç bakımından sayısal damgalamadan farklı olsa da yöntem olarak sayısal damgalama ile aynı özellikleri gösterir (Oğuz, 2006). Her ikisinin ortak yönü, korsan kopyaları engellemek ve yasal sürece yardımcı olarak telif hakları ihlallerinin önüne geçilmesi amacıyla uygulanmalarıdır (Kutucu vd., 2015). Sayısal imzalama, doküman sahibinin kendi kişisel anahtarı ile dokümanı imzalaması yani şifrelemesidir. Sayısal imzalama, kişisel ve kamusal anahtarın kullanıldığı damgalama olarak tanımlanabilir. Kişisel bir anahtar ile imzalanan doküman, sahibi hakkındaki bilgiyi de birlikte taşımaktadır (Fridrich, 2006). Herhangi biri için oluşturulan kamusal ve kişisel imzalar, o kişiye elektronik kartlarda verilir. Ancak birçok yerde yasal düzenlemelerin ve teknik altyapının tamamen sağlanmamış olmasından dolayı kullanımı yaygın değildir. Sayısal imza kullanılarak, gönderilecek dokümanın bütünlüğü sağlanır. Göndericinin kişisel imzası kullanılarak şifrelendiğinden gönderici tarafından inkâr edilemez ve göndericinin imzası taklit edilemeyeceğinden, dokümanın belirtilen göndericiden geldiği kesindir. Alıcı kendisine ait kamusal anahtarı kullanarak bu dokümanı açar, ancak göndericinin kişisel anahtarı olmadan doküman üzerinde değişiklik yapamaz (Oğuz, 2006). Kriptoloji, şifrelenmiş belgeler bilimi olarak nitelendirilir. Kriptografi ve kripto analiz olmak üzere iki alana ayrılır. Veriyi şifrelemek için kullanılan teknikleri inceleyen bilim dalına kriptografi denir. Şifrelenmiş bir verinin şifrelenmemiş hale getirilmesiyle ilgilenen bilim dalına ise kripto analiz denir (Şen, 2006; Ülker vd., 2006). Kriptografi; esas olarak verinin istenmeyen kişiler tarafından anlaşılamamasını ve iletim aşamasındaki bütünlüğün sağlanmasını amaçlar. Kriptoloji yöntemi, bir anahtar ile şifrelenmiş veriyi, umuma açık bir kanaldan anlaşılmadan alıcı tarafa iletir. Sayısal damgalama ile yakından ilişkili olan kriptoloji, günümüzde bazı sayısal bilgilerin korunmasında tek başına yeterli olamamaktadır. Çünkü kriptolojik yöntemlerde sayısal veriye uygulanan şifre bir kez çözüldükten sonra artık bu veri için herhangi bir koruma söz konusu değildir (Yıldırım, 2017). Günümüzde en fazla kullanılan kriptoloji yöntemi olan RSA, 100 basamaklıdan büyük asal sayılar (Karpinskyy ve Kinakh, 2003) kullanarak şifreleme yapan bir asimetrik şifreleme yöntemidir (Tunçer ve Karakuzu, 2016). Kriptolojik yöntemde, iletim ortamında taşınan verinin güvenliği şifreleme yönteminin başarısına bağlıdır. Yöntemi ve anahtarı ele geçiren üçüncü şahıs, iletilen tüm şifreli verileri çözebilir. Ancak bazı durumlarda, veriyi şifresiz olarak göndermek kriptolojiden daha güvenli olmaktadır. Bu durumda steganografik

yöntemler kullanılmaktadır. Bu yöntemler; iletilecek veriyi şifrelemek yerine, şüphe çekmeyecek başka bir verinin içine gizleyerek, ortada gizli bir verinin var olduğundan şüphelenilmemesi esasına dayanır. Steganografi, kriptografi kullanımının yasadışı olduğu veya yetersiz olduğu durumlarda iyi bir alternatif olmaktadır (Farid, 2001). Steganografi kelimesi ilk olarak el yazması şeklinde basılan Trithemius' un kitabında geçmiştir (Arnold vd., 2003). Kökleri antik Yunan'a kadar uzanan steganografi; adını Yunanca gizlemek, örtmek manasında gelen στεγανοζ (steganos) ve yazma anlamına gelen γραφειυ (graphein) sözcüklerinden alır (Boyacı, 2017; Tunçer ve Karakuzu, 2016). Steganografik mesajları göndermek için kullanıldığı bilinen ilk yazılı kanıt, kölelerle ilgili Herodot öyküsüdür (Çev:S´elincourt, 1996). Yunan tarihçisi Heredot' un bir çalışmasında anlattığı gizli mesaj yollama tekniğinde; Histiaus, Pers işgali altındaki İyonya şehri Milet'e yolladığı kölesinin kafa derisine bir mesaj dövmelettirmiştir. Zamanla kölenin saçı uzamış ve mesaj saçın altında görünmez hale gelmiştir. Daha sonra, Köle Milet valisi Aristogoras' a yollanmıştır. Aristogoras, kölenin saçını kazıtmış ve "Persler'e karşı ayaklanma başlatın" gizli mesajını alarak bir ayaklanma çıkartmıştır. Burada gizli veriyi taşıyan köle bile taşıdığı verinin içeriğinden habersizdir (Petitcolas vd., 1999). Bir başka örnekte Taktikçi Aeneas, yaşadığı zamanda "son teknoloji" olarak nitelendirildiği güvercinlerin taşıdığı mesajları gizlemek gibi birçok steganografi tekniği önermiştir. Bunlardan en çok kullanılanları; harf vuruşlarının şiddetini değiştirerek veya yazım ortamında küçük delikler açılarak bir metindeki harfleri işaretlemektir (Çev:Whitehead, 2002). Steganografinin bilinen en etkili ve ustaca kullanımlarından biri, Komutan Jeremiah Denton' ın Kuzey Vietnam' da esir olarak kaldığı dönemde, yanı başında yapılan bir basın açıklamasında, gözlerini kırparak Mors kodunda T-O-R-T-U-R-E (işkence) yazmasıdır. 11 Eylül 2001' de Amerika' nın New York eyaletindeki ikiz kulelere yapılan terörist saldırılardan sonra, iletişimin gizlenmesi yollarının çeşitli suç faaliyetleri için kullanabileceği ortaya çıkmış ve steganografiye olan ilgi önemli ölçüde artmıştır.

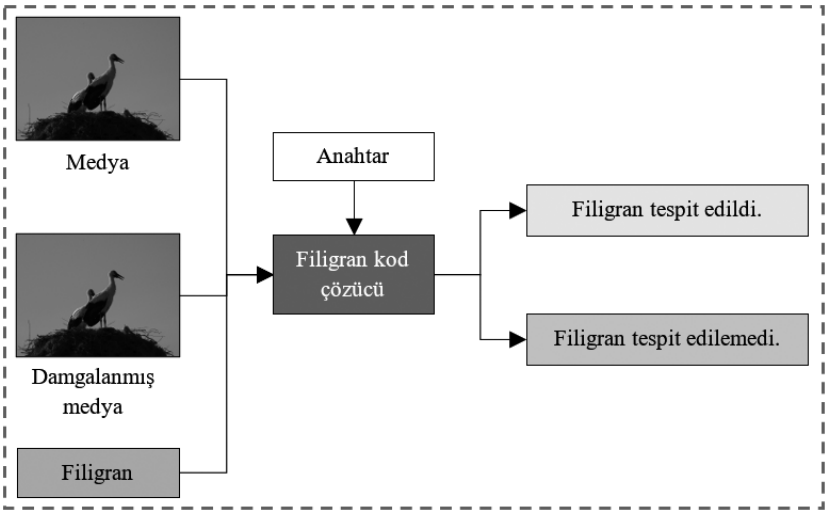
Steganografi; gizli veri, gizleme fonksiyonu ve kapak verisi olmak üzere üç temel elemandan oluşmaktadır. Gizli veri, gönderici tarafından alıcıya güvenli bir şekilde aktarılmak istenilen veriyi içerir. Gizleme fonksiyonu, gönderici tarafından gizli verinin gizlenme yöntemi ve anahtarını içerir. Kapak verisi ise gizli verinin gömüleceği, iletim ortamında şüphe çekmeyecek herhangi bir veriyi içerir (Kutucu vd., 2015). Steganografik yöntem, ilk önce gizli veriyi doğru yerleştirmek için kapak verisinde yeterli veri alanı bulmayı hedefler (Liu vd, 2011). Kapak verisi uygun değilse veri gizleme işlemi gerçekleştirilemez. Steganografi; askeri, biyometri ve sağlık alanı başta olmak üzere, birçok alanda ve

çeşitli amaçlar için kullanılmaktadır. Özellikle askeri iletişimin şifrelenmesi her zaman yeterli olmamaktadır. Şifrelenmiş bir bilginin iletimi, düşman tarafından fark edilebilir. Ayrıca biyometrik uygulamalarda, parmak izleri, el izleri, retina görüntüsü gibi veriler saklanırken veya taşınırken bu verilerin güvenliği son derece önemlidir. (Chaum, 1981). Bir steganografik sistemin performansı çeşitli özelliklere dayanarak değerlendirilebilir. Bunlardan en önemlisi, algılanamazlıktır. Algılanamazlık; gizli verinin ne kadar iyi kamufle edildiğini ifade eder. Bir diğer ölçü steganografik veri yüküdür. Veri yükü; kapak verisinin ne kadar gizli veri taşıyabileceğini ifade eder. Taşınacak veri boyutu azaldıkça ve kapak verisi boyutu arttıkça steganografik yöntemin başarısı da artacaktır. Steganografide yapılan çalışmalar, genelde daha küçük boyutlu kapak veride daha büyük boyutlu gizli veriyi başarılı bir şekilde fark edilmeden taşıyabilecek algoritmalar geliştirme üzerine odaklanmıştır. Bunun dışında bir iletim ortamında transfer edilen veri sayısı arttıkça, stego verilerin tespit edilme ihtimali de aynı orantıda azalacaktır (Eggers vd., 2002). Steganografi, gizli veriyi korumak için kapak verisini kullanır, ancak telif hakkı koruması gibi durumlarda, kapak verisini korumak için gizli bir veri kullanmak gerekmektedir. Bu durumlarda; steganografiden evirilmiş olan damgalama teknikleri kullanılmaktadır (Hamza, 2008). Damgalama tekniği, filigran olarak adlandırılan bir gizli veri ya da imgeyi, multimedya nesnesi gibi bir sayısal nesneye gömen, daha sonra da aynı işlemin tersini uygulayarak gömdüğü veriyi geri çıkarabilen tekniktir (Alasafi, 2016). Sayısal sinyal; metin, ses, resim veya video olabilir (Patel vd.,2013). Sayısal damgalama teknolojisi, bilgisayar bilimleri, kriptografi, işaret işleme ve haberleşme disiplinlerinden araştırmacıların üzerinde çalıştığı, bu disiplinlerin her birinden parçalar içeren bir alandır (Öztürk, 2009). Şekil 1' de görüldüğü gibi, damgalama sistemi genel olarak; filigran kodlayıcı, filigran kod çözücü, filigran ve anahtar bileşenlerinden oluşur (Kahalkar, 2012).



**Şekil 1.** Damgalama Sistemi

Bazı damgalama yöntemlerinde filigran çıkartılıp okunabilir. Bu işleme filigran çıkarma denir. Bazı durumlarda ise, sadece medyada bir filigran olup olmadığının tespit edilmesi amaçlanmaktadır. Bu işleme de filigran tespiti denir (Şekil 2). Filigranın çıkartılması genelde sahipliği ispat ederken, tespit edilmesi sadece sahipliğin doğrulamaktadır (Öztürk, 2009). Standart bir damgalama sürecinde, orijinal medya da filigran da birbirlerinden bağımsız olarak ses, metin, resim veya video olabilir (Rachid, 2014).




**Şekil 2.** Filigran Tespiti İşlemi (Pan vd., 2004)

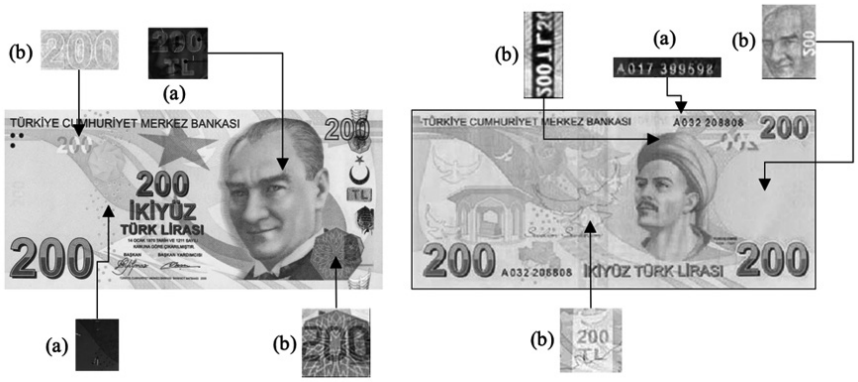
Bir sayısal damgalama yönteminde, damgalama neticesinde orijinal medyada değişimler olmaktadır. Filigran çıkartma veya tespiti esnasında orijinal medya hatasız olarak geri elde edilemeyebilir. Orijinal medyada oluşan değişimler, bazı uygulamalarda kabul edilemez. Örneğin, askeri bir uygulamada kullanılan sayısal bir görüntü üzerinde oluşacak bozulmalar, vurulacak hedefin haritadaki yerini değiştirip telafisi mümkün olmayan sonuçlara neden olabilir. Benzer şekilde, hastalık teşhisi için kullanılan tıbbi bir görüntüde oluşacak bir hata, doktorun yanlış teşhis koymasına ve ölümcül sonuçlara yol açabilir. Hassas verilerin kullanıldığı bu tür uygulama alanları için geliştirilmiş ve damgalanmış sinyalden orijinal sinyalin hatasız olarak geri elde edilebildiği yöntemler genel olarak tersinir (kayıpsız) damgalama olarak adlandırılmaktadır (Baraklı, 2014; Yıldırım,

2017; Feng vd., 2006). Damgalama ve steganografinin kullanım alanları oldukça farklı olsa da her ikisi de belirli yöntemleri ortak kullanmaktadır. Her ikisinin de kullanımı, internetin yaygınlaşması ile zirveye çıkmıştır. Ayrıca damgalama, kriptolojinin eksikliklerini gidermek amacıyla ortaya atılan tamamlayıcı bir teknoloji olarak düşünülebilir (Yıldırım, 2017; Podilchuk ve Delp, 2001). Örneğin, kullanıcı şifrelenmiş bir sayısal medyayı izleme, dinleme veya medya üzerinde değişiklik yapma şansına sahip değildir. Bu işlemlerin her biri için şifre çözme işlemi gerekmektedir. Damgalanmış bir medyada ise içeriğe herhangi bir ön işleme gerek duyulmaksızın erişilebilmekte ve yalnızca yetkili alıcılar tarafından filigrana erişim sağlanabilmektedir.

## 2. TARİHTE FİLİGRAN

Bilinen örnekleri olsa da damgalamanın ilk kez ne zaman kullanıldığını belirlemek zordur. Damgalama tekniklerinin kullanımı eski uygarlıklara kadar gitmektedir. Birçok filigranın varlığının yıllarca farkına varılamamıştır. Bilinen ilk damgalama uygulamaları kâğıtlar üzerinde görülmüştür. Kâğıt yapımı sanatı bin yıl önce Çin' de icat edilmiş olsa da bilinen ilk kâğıt filigranları, 1282 yılında İtalya' da yapılmıştır. Filigranlar, kâğıt kalıplarına ince tel kalıpları eklenerek yapılmıştır ancak bu filigranların anlamı ve amacı kesin olarak tespit edilememiştir. Tahminlere göre kâğıdın markasını ve kâğıdı üreten fabrikayı bildirmek için kullanılmış olabilirler (Shih, 2005). 18.yüzyılda Avrupa ve Amerika'da kâğıtlar üzerindeki filigranların yaygın şekilde kullanılmaya başlandığı bilinmektedir. Bu filigranlarda kâğıdın üretildiği tarih, kâğıt boyutu ve telif hakkı bilgileri yer almaktadır. Filigranların ilk defa para ve diğer belgelerde sahteciliğe karşı tedbir olarak kullanılmaya başlanması da bu sıralarda gerçekleşmiştir (Shih, 2005). "Watermark" (damgalama) teriminin 18. yüzyılın sonlarına doğru ortaya çıktığı bilinmektedir ve ilk olarak Almanca "wassermarke" olarak kullanıldığı tahmin edilmektedir. (Simpson ve Weiner, 1989) Watermark kelimesi anlam olarak "suyu işaretleme" gibi algılansa da bu kelimenin işaretlerin suyun kâğıda yansımasına benzediğinden kullanıldığı tahmin edilmektedir. I. Dünya Savaşı'nda Alman casusları, Britanya savaş gemilerini ve destroyerlerini değişik miktarda sigara olarak kodlamıştır. Örneğin; "Portsmouth' ta 5000 sigara ihtiyacı var" denildiğinde Portsmouth' ta 5 tane kruvazör var demek istenmiştir (Monathy, 1999). 1954' te Muzak Corporation'dan Emil Hembrooke, müzik eserlerinde damgalama için patent başvurusunda bulunmuştur. Bu yöntem, 1 kHz'lik bir filtreyi aralıklarla uygulayarak müziğe Mors kodu ile hazırlanmış bir tanımlama kodu eklenmesi şeklindedir (United States Patent, 1961). Yöntem, Muzak tarafından 1984'e kadar kullanılmıştır. Daha sonra bu yöntemle Muzak'ın

bilinçaltı reklam mesajlarını dinleyicilerine sunduğuna dair söylentiler çıkmıştır. 1979'da Szepanski, sahtecilikten korunma amaçlı, belgeler üzerine yerleştirilebilen ve makineyle bulunabilir bir damgalama modeli tanımlamıştır (Szepanski, 1979). Dokuz yıl sonra Holt ve arkadaşları, ses sinyallerine bir tanımlama kodu gömmek için bir yöntem geliştirmiştir (UK Patent, 1988). İlk defa "sayısal damgalama" (digital watermark) terimini kullanan, 1988'de yaptıkları çalışma ile Komatsu ve Tominaga olmuştur (Komatsu ve Tominaga, 1988). 1990'lı yılların başından sonra sayısal damgalama terimi sıklıkla kullanılmaya başlanmıştır. Sayısal damgalama konularında yapılan ilk çalıştay "Information Hiding Workshop" 1996' da gerçekleştirilmiştir (Anderson, 1996). Damgalama çalışmalarındaki artış, telif hakkı koruması çalışmalarındaki artış ile paralel olarak ilerlemiştir. Kasım 1993'te Marc Andreessen'in ilk popüler web tarayıcısı olan Mosaic Web Browser'ı kullanıma sürmesiyle, kullanıcılar internet üzerinden müzik, resim ve video gibi medya dosyalarını indirmeye başlamışlardır (Abbate, 1999). 1990'ların sonunda içeriklerin damgalanması için sayısal sistemlere olan ilgi artmıştır. Temel odağı fotoğraf, ses ve video olmakla beraber, metin, üç boyutlu modeller, animasyon parametreleri, yürütülebilir kod ve bütünleşmiş devreler gibi diğer içeriklerin de damgalanması üzerinde çalışmalar yapılmıştır. Genellikle amaçlanan; telif hakkı sahibi ile ilgili bilginin gömülmesi, kayıt donanımı bilgilerinin gömülmesi, taşıyıcı verinin içeriğinin değişip değişmediğinin doğrulanması, multimedya nesnesi ile ilgili izinlerin oynatma ortamı yazılımı tarafından görülmesi olarak özetlenebilir. Son yıllarda, sayısal damgalamada gelişmiş sinyal işleme tekniklerini kullanan uygulamalar geliştirilerek güncel problemlere yeni çözümler üretilmeye çalışılmaktadır (Hua vd., 2016). İkibinli yıllarda damgalamaya karşı artan ilgi, ticari damgalama ve kayıt altına alma çözümlerini de gündeme getirmiştir. Digimarc firması tarafından geliştirilen ve Adobe Photoshop yazılımı içinde de gömülü olarak bulunan yöntem bunun en önemli örneklerden birisidir (Yavuz, 2008). Damgalama tekniklerinin tarih boyunca bilinen en yaygın kullanımı, günümüzde de olduğu gibi para, çek, bono gibi kıymetli kâğıtlarda gerçekleşmiştir (Abdülkhaev, 2016). Para ışığa tutulduğunda, kâğıdın içine gizlenmiş filigranlar görülür. Bu filigranlar sahte para basılmasını zorlaştırmak ve orijinal ile sahte parayı ayırt etmek için geliştirilmiştir. En çok kullanılan sahte para basma yöntemlerinden biri, düşük değerli paranın yıkanıp ortaya çıkan filigranlı boş kâğıda yüksek değerli paranın basılmasıdır. Ancak paranın içindeki filigranlar (Şekil 3) sayesinde bu sahtecilik tespit edilebilmektedir.




**Şekil 3.** 200 TL Banknot Üzerindeki Algılanabilir ve Algılanamaz Filigranlar (a) Yalnızca Ultraviyole Işıkta Görünenler, (b) Güneş Işığında Görünenler

## 3. FİLİGRANIN ÖZELLLİKLERİ

Bir damgalama yönteminin başarımı, özelliklerindeki başarımı ile ölçülebilir. Örneğin filigran yerleştirilmiş medya çeşitli sinyal işleme yöntemlerine maruz bırakıldığında filigranın sağlam kalabilmesi, medya analog bir yayın üzerinden alınıp dijital formda kaydedildiğinde veya tam tersi işlemde filigranın sağlam kalabilmesi damgalamanın başarımı ile ilgilidir. Tamamlanmış damgalama işleminin başarımı, filigranı algılayan bir detektörün algılaması sonucunda ölçülebilir. Basitçe filigran tam olarak okunabilmişse damgalama işi başarılıdır denilebilir. Bir başka deyişle, filigranın algılanma olasılığı damgalama işleminin başarısını gösterir. Damgalama işlemi maliyet gerektiren bir işlemdir. Medyayı okuyacak tüm cihazların ve yazılımların filigranı algılayabilecek teknolojiye sahip olması gerekmektedir. Burada eser üreticisi damgalama maliyetini karşılamak veya eserini kopya korumasına karşı savunmasız bırakmanın maliyeti arasında seçim yapmak zorundadır. Sayısal damgalamanın etkinliği, birçok farklı performans ölçütü ile değerlendirir. Her uygulama için farklı ölçüt öncelikli olabilir, hatta bazı ölçütler tamamen görmezden gelinebilir (Spanias vd., 2007). Sayısal damgalama başarım ölçütleri olarak algılanamazlık, güvenlik, veri yükü, maliyet, Yanlış Pozitif Oran (YPO), etkinlik, çoklu damgalama, doğruluk, şifreleme ve damgalama anahtarı ve karmaşıklık sayılabilir.

### 3.1. Algılanamazlık

Steganografinin de en önemli özelliklerinden biri olan algılanamazlık, gönderilen tüm verilerin istatistiki dağılımı hakkında kesin bilgiye sahip olmakla ilgilidir.

İletişim kanalında istatistiki anormaliye sahip bir medya transfer ediliyorsa, bu medya doğrudan stego-kapak verisi olarak nitelendirilebilir. Ancak görüntüler üzerinde bu tarz bir algılama yöntemi kullanmak ve istatistik oluşturmak oldukça zordur. Genelde kullanılan yöntem, sayısal görüntülerdeki piksellerin belli bir olasılık geçiş matrisi olan bir Markov değişkeninin gerçeklenmesi olarak modellenmesidir. Algılanamazlık; kısaca orijinal veri ile damgalanmış veri arasındaki benzerliğin maksimum düzeyde olması olarak tanımlanabilir (Rachid, 2014).

### 3.2. Güvenlik

Bir filigranın güvenliği, düşman saldırılara karşı direnme kabiliyetini ifade eder. Düşman bir saldırı filigranı tamamen yok etmek, okunamaz hale getirmek veya amacını engellemek için özel olarak tasarlanmış bir algoritmadır. Damgalama saldırıları, yetkisiz kaldırma, yetkisiz yerleştirme ve yetkisiz algılama olmak üzere üç aşamada incelenebilir. Yetkisiz kaldırma ve yerleştirme aktif saldırılar olarak sınıflandırılır. Çünkü bu saldırılar orijinal medyayı değiştirmektedirler. Yetkisiz algılama orijinal medyada değişiklik yapmaz ve bu nedenle pasif bir saldırı olarak adlandırılır. Damgalanmış her medyanın saldırılara karşı korunmasına gerek yoktur. Örneğin, tüketici bilgilendirmesi için ürün bilgisine yerleştirilmiş bir filigranın güvenliğe ihtiyacı yoktur çünkü bu filigrana saldırı yapacak kişinin herhangi bir kazanım elde etmesi mümkün değildir. Yani bu damgalanmış medyanın saldırıya uğrama ihtimali yok denecek kadar azdır. Yetkisiz kaldırma, bir filigranın algılanmasını engelleyen saldırıdır. Dolayısıyla filigran ortadan kalkmaz ama karmaşık bir detektörle bile algılanamayacak duruma getirilmeye çalışılır. Damgalamayı ortadan kaldırmak demek, orijinal medyayı damgalamadan önceki ham haline getirmek demektir ki bu yalnızca bir saldırıyla mümkün olacak bir durum değildir. Birçok filigran detektörü, döndürülmüş bir resmin içindeki filigranı algılamakta zorluk çeker. En basit saldırılardan biri, resmi algılanmayacak derecede hafifçe bir tarafa döndürmektir. Bu saldırıda filigran yok edilmez, ancak detektörün algılamayacağı bir duruma getirilmeye çalışılır. Karmaşık bir detektör, resmin döndürülmüş olduğunu tahmin edebilir ve bu saldırıdan etkilenmeden filigranı tespit edebilir. Sahtecilik olarak da adlandırılan yetkisiz yerleştirme; yasadışı bir filigran ile filigran içermeyen bir veriyi damgalamak anlamına gelir. Örneğin bir kimlik doğrulama uygulamasında yetkisiz yerleştirme yapan bir yazılım, detektörün hatalı bir kimlik algılamasına sebep olabilir. Damgalamada güvenlik, orijinal medyanın düşman saldırılarına maruz kaldığında filigranın kendisini koruması yeteneğini ifade eder.

### 3.3. Veri yükü

Orijinal medyaya gömülebilecek filigranın bit sayısı değerine, damgalamanın veri yükü veya kapasitesi denir (Abbasfard, 2009). Örneğin bir görüntü dosyası damgalanırken veri yükü o dosyaya kodlanabilecek filigran biti sayısı iken, ses dosyası için saniye başına gömülü bitlerin sayısını gösterir. Damgalanmış medyanın veri yükü ne kadar fazlaysa, filigran algılayıcının da o aynı oranda hızlı çalışabiliyor olması gerekmektedir. Veri yükü ne kadar az ise damgalanmış medya saldırılara karşı o kadar güçlü ve güvenli olur (Brassil vd., 1995).

### 3.4. Maliyet

Filigran kodlayıcı ve çözücü geliştirilmesi veya gerçekleştirilmesinin maliyet hesabı oldukça karmaşıktır ve gerçekleştirilecek iş modeline göre değişiklik gösterir (Decker, 2001). Maliyete büyük ölçüde etki eden bir diğer konu da damgalama ve algılama sürecinde beklenen hızdır (Alsalami ve Al-Akaidi, 2003). Örneğin yayın izlemede (broadcasting), hem damgalayıcı hem de algılayıcı gerçek zamanlı çalışmalıdır ama filigran güvenliği çok dikkate alınmaz. Burada yüksek hız gerektiği için, yalnız bir algılayıcı çoğu zaman yeterli olmamaktadır. Ancak bir kimlik doğrulama uygulamasında damgalamanın ve algılamanın ne kadar zaman aldığının önemi yoktur. Önemli olan filigranın güvenliğidir.

### 3.5. Yanlış Pozitif Oranı

Bir filigran detektör yazılımı veya donanımı, filigran içermeyen bir kapak veriyi, verilerin dizilimi ile ilgili bir benzerlik nedeniyle filigran içeriyor gibi algılayabilir. Bu hatalı algılamanın meydana gelme olasılığına Yanlış Pozitif Oranı (YPO) denir. Bir yöntemde YPO'nun artması yöntemin güvenilirliğini ve hızını düşürür, sonuç olarak maliyetini arttırır. Steganografide buna benzer bir durum olan Yanlış Alarm Oranı (YAO) söz konusudur. YAO, bir steganaliz algoritmasının, iletilen medyada gizli bir veri olmadığı halde, gizli bir veri bulunduğunu bildirmesi ihtimalidir. YPO'ya benzer şekilde YAO yükseldikçe, sistemin maliyeti artar, kullanılabilirliği ve güvenilirliği düşer.

### 3.6. Etkinlik

Bir damgalama yönteminin gömme etkinliği, filigran yerleştirildikten hemen sonra medyaya detektörün uygulanması ile ölçülebilir. Steganografide etkinliğin ölçüsü, gizli verinin algılanamaz olmasıdır. Damgalama sistemlerinde filigranın kodlanma etkinliği; filigran ekleme için kullanılan yöntemlerin sayısal medyaların içerisine filigran ekleme başarısıdır. Filigran ekleme işlemi bittikten hemen

sonra filigran bulucu tarafından o sayısal medya üzerinde filigran taraması yapılır ve filigran eklenme etkinliğinin genelde %100 olması beklenir. Ancak bazı damgalama uygulamalarında damgalanmış medya ile orijinal medyanın birbirlerine benzerliği daha önemli olduğu için yöntemde %100 etkinlik beklentisi olmaz. (Cox vd., 2007; Ertürkler, 2007; Fındık, 2010).

### 3.7. Çoklu Damgalama

Damgalama işlemi yapıldıktan sonra, yetkili filigran algılayıcı tarafından filigranın bir veya birkaç defa değiştirilmesi gerekebilir. Örneğin satın alınan bir Çok Amaçlı Sayısal Diskin (Digital Versatile Disc - DVD) bir kopyasının, tüketici tarafından yedekleme amacıyla elinde tutmasına izin verilebilir. Bu durumda kopya koruması için kullanılan filigranın kolaylıkla değiştirilebilir olması gerekir ki bu da bu filigranın güvensiz olduğunu gösterir. Burada en iyi çözüm çoklu filigran kullanımıdır. Örneğin yalnızca bir kez kopyalanmasına izin verilen bir DVD kopyalandığında, orijinal kopyasındaki filigran kopyaya aktarılır ve bunun bir kopya olduğunu belirten ikinci bir filigran eklenir. Her iki filigranın varlığı artık bu DVD'nin kopyalanamayacağı anlamını göstermektedir. Ancak mevcut medyayı bozmadan ikinci kez damgalamak bir takım teknik zorlukları beraberinde getirmektedir (Qiao ve Nahrstedt, 1999). Çoklu damgalama, orijinal medyada daha fazla bozulma demektir. Örneğin bir müzik yapım şirketi, ürettiği bir şarkı için bir damgalama yapabilir. Fakat bu şarkıyı çevrimiçi satan farklı firmalar, kendi sattıkları şarkılara kendi firmalarını belirten bir filigran eklemek isteyebilirler. Bu durumda bir şarkı üzerinde birden fazla kez damgalama işlemi yapılmış olur. Amaç müziğin üreticisi ve tedarikçisinin görülmesi olsa da eklenen her filigran orijinal veriyi değiştirdiği için müzik kalitesine küçük de olsa değişiklikler olması kaçınılmazdır.

### 3.8. Doğruluk

Damgalama yapılacak olan medya ile damgalanmış medya bit düzeyinde karşılaştırıldığında, yerleştirilen filigrandan kaynaklı küçük bir fark ortaya çıkacaktır. Damgalamanın doğruluk değeri, ham medya ile damgalanmış medyanın algısal benzerlik yüzdesi olarak ifade edilir. Örneğin bir Frekans Modülasyonü (FM) radyo sinyali veya Ulusal Televizyyon Sistemleri Komitesi (National Television System Committee - NTSC) yayın standartları ile aktarılacak bir ses sinyali, bu yayın standartları gereği düşük kalite olacağı için orijinal medya ile damgalanmış medya arasındaki benzerlik oranı yüksek olacaktır. Ayrıca bu standartlarda taşınan medyada filigran olup olmadığını alınan verinin kalitesi

veya netliği ölçü alınarak tahmin etmek imkânsız gibidir. Bazı durumlarda da medya iletim sürecinde bozulmaya uğrayabilir. Bu nedenle doğruluk kavramını; kapak medya ile filigran kodlayıcıdan üretilip iletim kanalından gönderildikten sonra alıcı tarafta elde edilen damgalanmış medyanın algısal benzerliği olarak ifade etmek daha doğrudur (Alsalami ve Al-Akaidi, 2003).

### 3.9. Anahtar

Geleneksel kriptografi yöntemlerinin en büyük zaafı sistemin güvenliği açısından algoritmanın sadece geliştiriciler tarafından bilinmesidir. Bu yüzden de bazı güvenlik açıkları ancak algoritma kullanıma sunulduktan sonra tespit edilebilmektedir. Bu durumda eğer algoritmada ciddi bir güvenlik açığı tespit edilmişse, artık yeni bir algoritma geliştirmekten başka çare yoktur. Bu sorunu aşmanın en kolay yolu anahtarlamalı şifreleme algoritmaları olmuştur. Bu algoritmalarda güvenlik genellikle gizli anahtarlar kullanılarak sağlanmaktadır. Bu anahtarlar basitçe, mesajların nasıl şifreleneceğini belirleyen az sayıdaki bit sekansıdır. Burada algoritmanın nasıl çalıştığı bilinse bile, doğru anahtar ele geçirilmeden şifrelenmiş veriyi çözmek oldukça zordur. Ayrıca anahtar boyutu büyüdükçe veri güvenliği de buna paralel olarak artmaktadır. Kısaca belirli bir anahtarla şifrelenmiş bir veri, yalnızca aynı anahtarla çözülebilir. Damgalama sistemlerinde de aynı yöntem kullanılabilmektedir. Filigran bir şekilde yetkisiz olarak algılansa bile çözülememesi için bir anahtarla şifrelenebilir. Böylece yalnızca yetkili algılayıcı geçerli anahtara sahip olduğu için filigranı tam olarak çözebilir. Damgalamada basit bir anahtar kullanımına örnek olarak bir görüntüye sahte bir gürültü uygulanması gösterilebilir. Bu gürültü örüntüsü aslında damgalanacak veriyi içerir ancak bu örüntünün spektrumu anahtar veride gizlidir. Algılayıcı bu anahtar ile örüntü içindeki veriyi okur, birleştirir ve filigranı oluşturur. Burada algoritma saldırgan tarafından bilinse bile, örüntü bilgisi yani anahtara sahip olmayan saldırgan, filigranı çözemeyecektir. Burada bir üst seviye güvenlik yöntemi, filigranın örüntüye dönüştürülmeden önce bir başka anahtarla şifrelenmesidir. Dolayısıyla algılayıcının önce örüntüyü okumak, sonra onu çözmek için iki farklı anahtara ihtiyacı olacaktır ki bu yöntem filigran algılama saldırılarına karşı oldukça güvenlidir.

### 3.10. İşlem Karmaşıklığı

Damgalama ve filigran çıkarma, prensip olarak düşük işlem karmaşıklığına sahip olmalıdır (Hartung ve Girod, 1997b). Genelde damgalama işleminin işlem karmaşıklığı, filigranı çıkarma işleminin karmaşıklığı kadar önemli değildir. Telif

hakkı koruması gibi, bir defa ve çevrimdışı olarak yapılan damgalama işleminin işlem karmaşıklığı yüksek olabildiği gibi (Abbasfard, 2009) gerçek zamanlı filigran çıkarma gerektiren uygulamalarda işlem karmaşıklığı, işlemin yapılacağı donanımın gücü de hesaplanarak oldukça düşük tutulmak durumundadır (Rachid, 2014).

## 4. FİLİGRAN UYGULAMA ALANLARI

Sayısal damgalama tekniklerinin en yaygın uygulama alanları; telif hakkı koruması, aidiyet kanıtlama, işlem izleme, doğrulama, kopyalama denetimi, aygıt denetimi, miras geliştirmeleri, içerik arşivleme, sayısal parmak izi, yayın izleme ve meta-veri yerleştirmedir.

### 4.1. Telif hakkı koruması

5846 sayılı Fikir ve Sanat Eserleri Kanununun 22. Maddesinde, eser sahibinin hakları açıkça belirtilmektedir. 21 Şubat 2001 tarihinde bu kanunda değişiklikler yapılmış ve son halini almıştır; "Bir eserin aslını veya kopyalarını, herhangi bir şekil veya yöntemle, tamamen veya kısmen, doğrudan veya dolaylı, geçici veya sürekli olarak çoğaltma hakkı münhasıran eser sahibine aittir. Eserlerin aslından ikinci bir kopyasının çıkarılması ya da eserin işaret, ses ve görüntü nakil ve tekrarına yarayan, bilinen ya da ileride geliştirilecek olan her türlü araca kayıt edilmesi, her türlü ses ve müzik kayıtları ile mimarlık eserlerine ait plan, proje ve krokilerin uygulanması da çoğaltma sayılır. Aynı kural, kabartma ve delikli kalıplar hakkında da geçerlidir. Çoğaltma hakkı, bilgisayar programının geçici çoğaltılmasını gerektirdiği ölçüde programın yüklenmesi, görüntülenmesi, çalıştırılması, iletilmesi ve depolanması fiillerini de kapsar." Benzer olarak Amerika Birleşik Devletleri yasalarına göre bir hikâyenin, resmin, şarkının veya herhangi bir başka orijinal eserin geliştiricisi, bu eserin fiziksel biçimde kaydedildiği andan itibaren otomatik olarak telif hakkına sahiptir. Fakat eser sahipleri eserlerini bir şekilde dağıtmak isterlerse, oluşturulan her kopyaya bir telif hakkı bildirimi eklemeleri gerekmektedir. Ancak 1988 yılından sonra, telif hakkı bildiriminin artık zorunlu olmayacağı hususu kanun maddesine eklenmiştir. Ayrıca telif hakkı bildirimi olmayan bir eserin eser sahibinin izni olmadan dağıtılması durumunda, dağıtıcıya uygulanacak yaptırımlarda kısıtlamaya gidileceği de belirtilmiştir. Buradaki en büyük risk, izinsiz kopyalamayı yapan kişinin telif hakkı bildirimi olan bölümünü kırpmasıdır. Bu durumda, kopya eseri satın alan kişiler, telif hakkı bildirimini görmediği için, yasa dışı kopyayı kullandığının farkında olmayacaktır. Özellikle bir kenarına eser sahibinin telif hakkı bildiriminin eklenmiş olduğu

durağan görüntü türündeki eserlerin, o bölgenin kırpılıp izinsiz dağıtılması oldukça kolaydır. Bunun en bilinen örneği, damgalama alanında literatüre geçmiş olan Lena Soderberg adlı İsveçli bir mankendir. 1972 yılında Lena'nın bazı fotoğraflarını yayınlayan ünlü bir magazin dergisi, fotoğraflara telif hakkı eklemek amacıyla bir görünür filigran eklemiştir (Şekil 4). Ancak bu fotoğraf kırpılarak filigran kolayca yok edilmiş filigransız kopyası dağıtılmıştır (Po, 2001).


**Şekil 4.** Lena İmgesinin Çoğaltılan Kopyası (a) ve Uygulanan Filigran (b)

Sayısal damgalama uygulanmış bir görüntüde eğer filigran gizlenmişse, eser kopyalandıkça otomatik olarak filigran da eserle beraber kopyalanmaktadır. Ayrıca filigran yalnızca çözücü yazılım tarafından görülebildiği için, eserin içinden çıkarılması kolay bir işlem değildir. Bu konuda dünya çapında adını en fazla duyurmuş şirket, merkezi Amerika Oregon Eyaleti' nde bulunan olan Digimarc Corporation'dır ve halen dijital filigran ürün ve teknolojileri için uygulamalar geliştirmektedir. Üçyüzelliden fazla patente sahip olan Digimarc, askeri, finansal ve ticari alanlarda telif hakkı koruması için damgalama hizmetleri vermektedir. Bunun yanında Digimarc ve Adobe firmalarının birlikte geliştirdiği bir eklenti ile Photoshop yazılımı üzerinde çizim yapan herhangi bir kullanıcı, eserine algılanamaz filigran ekleyerek damgalayabilir. Bu yazılımda oluşturulan filigranlar internet erişimine açık bir veri tabanında tutularak kontrolü de buradan sağlanmaktadır. Ancak bu yöntemle yapılan damgalamanın ülkemizde kanun önünde geçerliliği bilinmemektedir.

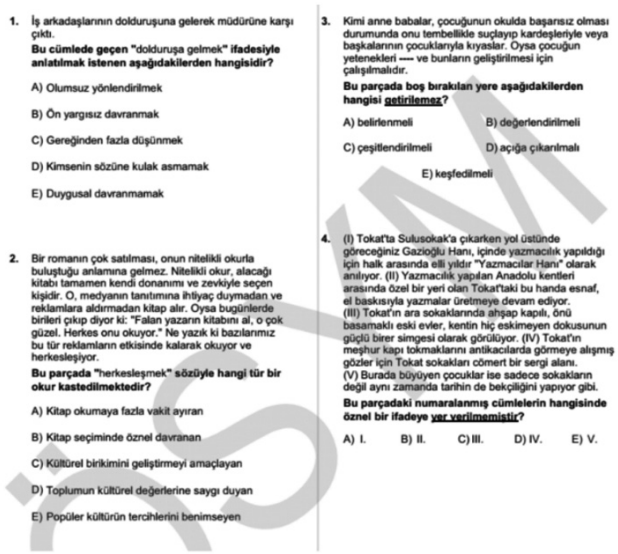
### 4.2. Aidiyet kanıtlama

Damgalama sadece telif hakkı sahipliğini tanımlamak için değil, eser sahipliğini kanıtlamak için de uygulanmaktadır. Örneğin bir metnin içindeki eser sahibini bildiren bir filigran elde edilip, bu metin farklı bir kişi bilgisi ile yeniden damgalanırsa, gerçekte eser sahibinin kim olduğuna dair soru işareti oluşacaktır.

Bu problemin çözümü için bugüne kadar geliştirilmiş en iyi yöntem, filigranlar için merkezi bir veri tabanı oluşturmaktır. Medya sahibi eserini oluşturduktan sonra filigranı kodlar ve bu halini bir telif hakkı bürosuna göndererek eseri kaydettirebilir. Böylece filigran değişikliği durumunda gerçek eser sahibinin kim olduğu kolayca ortaya çıkacaktır. Ancak bu yöntem, ekstra maliyet gibi bazı zorlukları beraberinde getirmektedir.

### 4.3. İşlem izleme

Bir medyanın kimin tarafından korsan olarak çoğaltıldığını tespit etmek amacıyla işlem izleme yaklaşımı kullanılır. Örneğin medyanın yetkili dağıtıcılarının her birisi için ayrı filigranlar üretilir ve medya bu dağıtıcılara verilirken dağıtıcının filigranı ile damgalanır. Daha sonra medyanın korsan dağıtımı tespit edilirse, bir korsan kopya ele geçirilir ve ele geçirilen korsan kopyadaki filigran çözülerek hangi dağıtıcı tarafından korsan dağıtım yapıldığı tespit edilir. Ancak bu yöntemin farkında olan bir dağıtıcı, medyanın korsan kopyasını üretmeden önce, filigranı ortadan kaldırmak veya filigrana hasar vermek için medya üzerinde çeşitli saldırı yöntemleri uygulayabilir. İşlem izleme için damgalama tanımına girmeyen birkaç teknoloji vardır. Bunlardan en yaygını görünür işaretler kullanmaktır. Örneğin, resmi evrak, banka evrakı gibi önemli bilgiler taşıyan bir evrakta, gerçek metnin arka planında ve metnin okunmasına engel teşkil etmeyecek şekilde büyük karakterler içeren bir görünür damgalama yapılır (Şekil 5).



1. İş arkadaşlarının dolduruşuna gelerek müdürüne karşı çıktı.
**Bu cümlede geçen "dolduruşa gelmek" ifadesiyle anlatılmak istenen aşağıdakilerden hangisidir?**
A) Olumsuz yönlendirilmek
B) Ön yargısız davranmak
C) Gereğinden fazla düşünmek
D) Kimsenin sözüne kulak asmamak
E) Duygusal davranmamak

2. Bir romanın çok satılması, onun nitelikli okurla buluştuğu anlamına gelmez. Nitelikli okur, alacağı kitabı tamamen kendi donanımı ve zevkiyle seçen kişidir. O, medyanın tanıtımına ihtiyaç duymadan ve reklamlara aldırmadan kitap alır. Oysa bugünlerde birileri çıkıp diyor ki: "Falan yazarın kitabını al, o çok güzel. Herkes onu okuyor." Ne yazık ki bazılarımız bu tür reklamların etkisinde kalarak okuyor ve herkesleşiyor.
**Bu parçada "herkesleşmek" sözüyle hangi tür bir okur kastedilmektedir?**
A) Kitap okumaya fazla vakit ayıran
B) Kitap seçiminde öznel davranan
C) Kültürel birikimini geliştirmeyi amaçlayan
D) Toplumun kültürel değerlerine saygı duyan
E) Popüler kültürün tercihlerini benimseyen

3. Kimi anne babalar, çocuğunun okulda başarısız olması durumunda onu tembellikle suçlayıp kardeşleriyle veya başkalarının çocuklarıyla kıyaslar. Oysa çocuğun yetenekleri ---- ve bunların geliştirilmesi için çalışılmalıdır.
**Bu parçada boş bırakılan yere aşağıdakilerden hangisi getirilemez?**
A) belirlenmeli B) değerlendirilmeli
C) çeşitlendirilmeli D) açığa çıkarılmalı
E) keşfedilmeli

4. (I) Tokat'ta Sulusokak'a çıkarken yol üstünde göreceğiniz Gazioğlu Hanı, içinde yazmacılık yapıldığı için halk arasında elli yıldır "Yazmacılar Hanı" olarak anılıyor. (II) Yazmacılık yapılan Anadolu kentleri arasında özel bir yeri olan Tokat'taki bu handa esnaf, el baskısıyla yazmalar üretmeye devam ediyor. (III) Tokat'ın ara sokaklarında ahşap kapılı, dönü basamaklı eski evler, kentin hiç eskimeyen dokusunun güçlü birer simgesi olarak görülüyor. (IV) Tokat'ın meşhur kapı tokmaklarını antikacılarda görmeye alışmış gözler için Tokat sokakları cömert bir sergi alanı. (V) Burada büyüyen çocuklar ise sadece sokakların değil aynı zamanda tarihin de bekçiliğini yapıyor gibi.
**Bu parçadaki numaralanmış cümlelerin hangisinde öznel bir ifadeye yer verilmemiştir?**
A) I. B) II. C) III. D) IV. E) V.

**Şekil 5.** ÖSYM Soru Kitapçığında Kullanılmış Bir Filigran Örneği

### Doğrulama

Sayısal teknolojiler geliştikçe, bir eserin gerçek olup olmadığını ayırt etmek de zorlaşmaktadır. Örneğin bir dijital görüntü, görüntü işleme yazılımı kullanarak kolayca tahrif edilebilir. Tahrif edilmiş görüntü bir hukuki sürece dâhil olursa, buradaki değişiklik ciddi bir sorun teşkil edebilir. Benzer problemler ile ses ve video türünde medyalarda da karşılaşılmaktadır. Burada en yaygın doğrulama yöntemlerinden birisi damgalamadır. Bir içeriğin orijinaline, içerisindeki veriler ve bir anahtar kullanarak bir sayısal imza eklenir. İçerik üzerinde değişiklik yapıldı ise, aynı imzalama yöntemi ile yeniden imza üretilir ve içerikteki imza ile karşılaştırılır. İçeriğin bir biti bile değişmiş olsa, imzalar arası farklılık sebebiyle medyada yapılmış olan değişiklik böylece fark edilebilir.

### 4.4. Kopya denetimi

Kopya denetimi, diğer damgalama tekniklerinden farklı olarak kopyalama yapıldıktan sonra yasadışı kopya üreteni takip amaçlı değil, kopyalama yapılmadan önce eser sahibinin haklarını korumayı amaçlamaktadır. Yasadışı bir eylemi yapan kişiyi yakalayıp cezalandırmaktansa, eylem yapılmadan önce ona engel olmak çok daha iyidir. Bu yüzden, kopyalama denetiminde orijinal ürünü satın alan kişiye bile ürün şifrelenmiş olarak teslim edilir. Hatta çoğunlukla ürün şifreli olarak zaten piyasada rahatça gezinebilmektedir. Ancak şifreyi çözecek anahtar sadece ürünün orijinal kopyasını satın alan kişiye verilir (Cox vd., 2007). Bu yöntemin en yaygın kullanılan örneği şifreli Televizyon (TV) yayınlarıdır. Yayını satan alan kişinin elinde bir kripto anahtar içeren akıllı kart vardır ve halka açık durumdaki şifreli yayın bu anahtar ile çözebilmektedir. Bu tarz şifrelemede, şifreleme sistemini yasadışı olarak aşmaya çalışmanın üç temel yolu vardır. Birincisi ve en zoru, milyonlarca deneme yaparak doğru anahtara ulaşmaya çalışmaktır. Ancak anahtar ne kadar fazla sayıda bitten oluşmuşsa, bu yöntemle bulunma olasılığı da o kadar düşüktür. İkinci bir yöntem, ters mühendisliktir. Yani yapılmış olan şifreleme algoritmasının tersini bulmaya çalışmaktır. Üçüncü ve en kolay yöntem ise şifreli veriyi çözmek için gereken anahtarı yasal olarak elde edip şifreyi çözdükten sonra elde edilen şifresiz veriyi korsan olarak çoğaltmaktır. Örneğin şifreli bir TV yayınını çözecek akıllı kartı satın alan bir kullanıcı, çözülen yayını başka bir kanaldan daha ucuza dağıtabilir. Sonuçta içerik kullanılmadan önce çözülmelidir ve bir kez çözüldüğünde, tüm koruma kaybolmuştur.

### 4.5. Aygıt denetimi

Temel olarak bir aygıtın işlediği medya ile ilgili özel bir bilginin, aygıtın çözebileceği bir yöntem ile medyanın içine gömülmesidir. Doğası gereği, damgalama ile aygıt denetimi, çoğu zaman güvenlik gereksinimlerine ihtiyaç duymamaktadır (Cox ve Miller, 2002). Damgalama yöntemi kullanarak aygıt denetimi fikri ilk olarak 1981 yılında Ray Dolby tarafından ortaya atılmıştır. O dönemde birçok radyo istasyonu stereo ses yayınlarını aynı yöntemle yayınlarken, bazı radyo istasyonları Ray Dolby tarafından geliştirilmiş gürültü azaltma tekniği kullanarak yayın yapmaktaydı. Bu yayınların ses kalitesi çok daha yüksek olsa da tüm radyo alıcıları bu Dolby sinyalleri çözebilecek çözücü donanım ve yazılıma sahip değildi. Sahip olanlarda ise seçilen radyo istasyonunun Dolby mi yoksa normal yayın mı yaptığını kullanıcının radyo cihazı üzerindeki bir düğme ile açıp kapatması gerekiyordu. Ray Dolby; ses spektrumu içine insan kulağının algılayamayacağı frekansta bir filigran yerleştirerek radyo alıcı cihazın gelen sinyalin Dolby olup olmadığını anlamasını sağlamıştır. Bu teknikle analog radyo yayınlarında ilk defa damgalama tekniği kullanıldığı gibi, aynı zamanda ilk defa aygıt denetimi yapılmıştır (United States Patent, 1981).

### 4.6. Miras geliştirmeleri

Dünya çapında standart haline gelmiş bir sistemin yenilenmesi esnasındaki en büyük problem, sistemi kullanan cihazların hepsinin aynı anda değiştirilememesi nedeniyle yeni geliştirilen cihazların, eski cihazların kullanmakta olduğu standartları çalıştırmak zorunda olmasıdır. Bunun en iyi örneği uluslararası hava trafik kontrol sinyallerinin birçoğunun hâlen analog sinyalleri kullanıyor olmasıdır (Vassiliadis vd., 2004). Bu sistemde pilotlar birbirleriyle veya havaalanı ile haberleşmeden önce kimlik bildirimi yapmak zorundadır. Örneğin bir Türk Hava Yolları (THY) pilotu ile hava trafik kontrolörü arasında geçmiş örnek bir konuşma aşağıdaki gibidir:

- **Pilot:** THY420 Antalya tower iyi akşamlar. Rwy 36R full establish 12 mil.
- **Kule:** THY420 iyi akşamlar yaklaşmaya devam edin 4 nm' de ikaz edin. Rüzgâr 350/8 kt.
- **Pilot:** THY420 Rüzgâr 350/8 kt. 4nm ikaz edilecek.
- **Pilot:** THY420 4nm
- **Kule:** THY420 Rwy36R'ye iniş serbest. Rüzgâr 350/8 kt.
- **Pilot:** THY420 Rüzgâr alındı. Rwy36R' ye iniş serbest.
- **Kule:** THY420 Pisti terk edince ikaz edin.
- **Pilot:** THY420 Pist terk edildi.

- **Kule:** THY420 121.9' dan Ground ile temasa geçin.
- **Pilot:** THY420 121.9' dan Ground ile temasa geçiliyor. İyi akşamlar.

Konuşmada görüldüğü üzere hem pilot hem de kule her konuşmanın başında uçağın kimliğini belirten bir çağrı işareti kullanmaktadır. Sayısal bir sinyalizasyon kullanıldığımda bu çağrı işareti sinyal başlığı olarak gönderilebilmektedir. Ancak analog sinyalde çağrı sinyalinden kurtulabilmek için hem alıcı hem de verici telsiz cihazları kimlik bilgilerini içeren bir filigran oluşturup analog sinyale damgalayabilmektedir. Avrupa Hava Seyrüsefer Güvenliği Organizasyonu olan Eurocontrol, bu damgalama yönteminin kullanılabilirliği ve güvenliği üzerine çalışmalar yapmıştır (Hering vd., 2003). Bir başka örnek, Tektronix' in ses ve video sinyallerinin senkronize edilmesi için geliştirdiği sayısal damgalayıcıdır. Bu damgalayıcıdaki zorluk, video ve ses yayınlarını çözme işleminin farklı sürelerde gerçekleşmesidir. Bir yayını çözme işlemi yapan bir TV, iki verinin farklı zamanlarda çözülmesinden dolayı sesin ve görüntünün örtüşmemesi yani senkron kayması denilen sorunla karşılaşılabilir. Ses ve görüntüyü senkronize etmek için Tektronix firması, video sinyalinin içine ses verisinin çok düşük kalitede ve sıkıştırılmış olarak eklenmesi ve çözülen asıl ses verisi ile zaman çizelgesi üzerinde üst üste bindirilmesi yöntemini önermiştir (Cox vd., 2007).

### 4.7. İçerik arşivleme

İçerik arşivleme için kullanılan damgalama teknikleri, medyaların aidiyetinin veya özelliklerinin birbirleriyle karıştırılmaması için kullanılmaktadır. Bu tip damgalamanın en çok kullanıldığı alan tıp alanıdır. Bir hastanın medikal görüntüleri veya benzer sayısal medyalar başka bir hastanınki ile karıştığında sonuçlar ölümcül olabilmektedir. Bu nedenle her medya üretildiğinde, hastanın, doktorunun, teşhis ve tedavi gibi bilgilerin medikal medyaya görünmez bir filigran ile damgalanması iyi bir çözüm olmaktadır. Veri tabanlarına kaydedilen bu verilerin isimlerinin karışması, silinmesi veya veri tabanının çökmesi durumunda bu sayısal medyaların içerisine eklenen filigranlar yardımıyla medya hakkında bilgiye ulaşılabilmektedir (Ertürkler, 2007).

### 4.8. Sayısal parmak izi

Parmak izi, kişisel filigran olarak kabul edilir. Sayısal içeriği yasadışı kopyalayan kaynağın tespit edilmesi için kullanılabilir. Medyayı satın alan bir müşteri, bu medyanın bir kopyasını oluşturmak isterse, medyayı kopyalayan yazılım kişiye özel sayısal parmak izi adında bir filigran ekler. Ortamda yasal olmayan kopya tespit edilirse, bu kopyanın hangi müşteri tarafından dağıtımının yapıldığı,

kopyanın içerdiği filigran ile tespit edilebilir. Sayısal parmak izi, müşterinin kimlik bilgilerinin bir kısmını içerecek şekilde yerleştirilebilir. Bu yöntem, fikri mülkiyet sahibinin verileri üçüncü tarafa sağlayarak lisans sözleşmelerini ihlal eden müşterileri belirlemesini sağlar. Böylece sayısal içeriğin yasadışı dağıtımından sorumlu kişi kolayca bulunabilir (Gupta, 2012).

### 4.9. Yayın izleme

Özellikle TV ve radyo istasyonlarında kullanılan bir sayısal damgalama uygulamasıdır. Yayınlanmaya başlayacak medya içerisine sayısal filigran eklenir ve izlendiği veya dinlendiği cihazda bu sinyaller alınarak doğru yayının izleyicilere ulaşıp ulaşmadığı kontrol edilir (Fındık, 2010). Her medya yayınlandığı zaman yeniden filigran tanımlaması yapılır (Cox vd, 2000). Bu yöntemin geliştirilmesi 1997 yılında Japonya' da ortaya çıkan bir skandala dayanır. TV kanalları, reklam için ayırdıkları sürenin aynı zaman dilimini birden fazla şirkete satarak yayınlamadıkları reklamlar için ödeme almıştır (Ertürkler, 2007). Reklam yayınlarını gözlemleyecek bir sistem olmamasından dolayı, bu uygulama 20 yıldan daha uzun bir süre hiç fark edilmeden devam etmiştir (Cox vd., 2007). Reklam veren firmaların dikkati ile bu durum ortaya çıkmış ve büyük tazminatlar ödenmiştir. Daha sonra bu sorunların üstesinden gelebilmek amacıyla çeşitli teknikler ortaya çıkmıştır. Bunlardan birisi insan kaynaklı çözümlerdir. Yayınları izleyen kişiler gördükleri ya da dinledikleri şeyleri bildirerek bir yayın kontrolü yapabilirler. Fakat bu yöntem hem insan faktörünün yapabileceği yanlışlıklar sebebiyle hem de çok maliyetli bir yöntem olması sebebiyle tercih edilmemiştir. Bu durum otomatik yayın izleme yöntemlerine geçiş için önemli bir sebep olmuştur.

### 4.10. Meta-veri yerleştirme

Meta veri, orijinal medyayı tanımlayan verileri içerir. Meta veri damgalama yönteminde, filigran mutlaka orijinal medya ile ilintili olmalıdır. Örneğin bir ses dosyası için şarkı sözleri, bir sayısal imge dosyası için fotoğrafı çeken veya resmi çizen sanatçının bilgileri ile filigran oluşturulup medya damgalanır (Mahajan ve Gogate, 2016).

### 4.11. Veri bütünlüğü

Verinin bütünlüğünün bozulmasına neden olan şey veride yapılan yetkisiz değişikliklerdir. Bu değişiklikler zararlı veya masum değişiklikler olabilir. Masum değişiklik verinin içeriğini değiştirmez ancak kalitesini değiştirir. Zararlı değişiklikler verinin içeriğine müdahale eder. Verinin içeriği değişmişse artık bu veri sahte olarak ele alınmalıdır. Verinin sahteciliğini tespit etmek için doğrulama

işlemi gerçekleştirilir. Özellikle kıymetli evrak görüntülerinde doğrulama yöntemleri sayısal görüntünün bütünlüğünü doğrular. Hem kimlik doğrulama hem de bütünlük konularını ele almak için son yıllarda farklı uygulamalar için çok çeşitli şemalar önerilmiştir. Kimlik doğrulama verilerini aktarma yöntemlerine bağlı olarak bu programlar kabaca iki kategoriye ayrılabilir: etiketleme tabanlı şemalar ve filigran tabanlı şemalar. Etiketlemeye dayalı kimlik doğrulama şemaları, kimlik doğrulama verilerini ayrı bir dosyada saklar. Bu tür şemalar korumalı bir görüntünün değiştirilip değiştirilmediğini belirleyebilir ancak veri bütünlüğünün bozulduğu mekânsal yerleşimleri belirleyemez. Ek olarak, kimlik doğrulama verilerinin ayrı bir dosyada saklanması yalnızca önemli bakım giderleri sağlamakla kalmaz, aynı zamanda iletim ve depolama için ek bant genişliği ve bellek gerektirir. Filigran temelli şemalar, kimlik doğrulama verileri olarak sayısal filigranlar kullanır ve bunları doğrudan bu sorunlara açık bir çözüm sağlayan orijinal medyaya gömer.

## 5. MEDYANIN TÜRÜNE GÖRE FİLİGRAN

Filigran yerleştirilecek medya türleri genellikle metin, resim, ses ve video medyalarıdır. Metin damgalama genellikle metnin sahibinin telif hakkını korumaya ve dağıtmaya yönelik uygulamalarda kullanılır. Metin verisini değiştirmeden filigran yerleştirmek kolay bir işlem olmadığı için metnin algılanamayan bölümleri seçilmektedir. Metin damgalama diğer medya türleri ile karşılaştırıldığında, verinin daha az fazlalık içermesi ve insanların anormal görünümdeki bir metne karşı oldukça duyarlı olmaları sebebiyle algılanamazlık özelliği bakımından dezavantajlıdır (Samphaiboon, 2009). Doğal olarak tüm diller için tek bir yöntemi uygulayabilmek imkânsızdır (Alla ve Prasad, 2009). Faklı dillerin farklı karakteristik özellikleri vardır. Metin damgalamada filigran metnin içine gömüldüğünden, yöntem, kullanılan yazım dili ve onun kurallarına oldukça bağımlı olmaktadır (Al-Nazer ve Gutub, 2009). Metin damgalama için önerilmiş farklı yöntemler bulunmaktadır. Doğal dilde oluşturulmuş bir metindeki cümlelerin sentaktik, semantik ve sözcük yapısında değişiklik yaparak filigran ekleyen sisteme sözbilimsel damgalama denir. Format tabanlı yöntemler genelde metin üzerinde İGS ile algılanamayacak değişiklikler yaparak damgalamayı amaçlar. Kelimeler arasında fazladan boşluk bırakmak, yazı tipini, yazı büyüklüğünü, sayfa boyutunu ve girintileri değiştirmek temel yöntemlerdir (Petitcolas, 2000; Boyacı, 2017). Sözcük tabanlı yöntemler cümlenin sentaktik ve semantik yapısını bozmadan metine filigranı yerleştirmeye çalışır (Bennett,

2004). Sentaktik dilbilimsel damgalama ise cümledeki kelimelerin diziliminde yapılan değişikliklerle filigran gömme tekniğidir. Semantik dilbilimsel yöntemde ise Tablo 1' de gösterildiği şekilde metnin anlamı aynı olacak şekilde kelimelerin kendisi veya dizilimi değiştirilir (Boyacı, 2017).

| **Tablo 1. Metin Tabanlı Damgalama Örnekleri** | |
|---|---|
| **Orijinal cümle** | **Ali ata bak.** |
| **Format tabanlı** | Ali ata bak. |
| **Sözcük tabanlı** | Ali baksın. |
| **Sentaktik** | Ali bak ata. |
| **Semantik** | Bak ata Ali. |

Görüntü damgalama yöntemleri analog veya sayısal olarak işlenme durumuna göre iki sınıfta incelenir. Sayısal ortamda uygulanan damgalama yöntemleri genelde piksel veya örnek tabanlı çalışır ve bu yöntemlere uzamsal alanda veya uzamsal uzayda damgalama yöntemleri denir. Bu yaklaşımda filigran, görüntülerin piksellerine yerleştirilir. Filigran, kırpma, gürültü ekleme gibi saldırılara karşı dayanıklıdır, öyle ki bu saldırılardan sonra filigranın bir kısmı kurtarılabilir (Patel vd., 2013). Damgalanacak görüntü bir sinyal olarak algılanıyor yani frekans düzleminde inceleniyor ve damgalama burada uygulanıyorsa bu tür yöntemlere de frekans alanında veya frekans uzayında damgalama denir (Boreiry ve Keyvanpor, 2017). Bunun için hem görüntü hem de filigranın önce frekans alanı dönüşümleri alınır ve elde edilen katsayılar ile istenen frekans düzeyine filigran yerleştirilir (Mahmoud vd., 2005). Görüntü frekans alanından tekrar uzamsal alana dönüştürüldüğünde, filigran görüntünün tamamına yayılmış olduğu için saldırganlar tarafından algılanması ve çözülmesi zorlaşmıştır. Filigran, görüntü sinyalinin frekans alanının orta frekansları gibi en az dikkat çekici alanlarına gömülebilir. Böylece damgalamanın sağlamlığı ve algılanamazlığı sağlanmış olur. Ana verinin kırpılması durumunda, filigranın bir kısmı halen kurtarılabilir (Abdülkhaev, 2016). Damgalama araştırmalarının önemli bir bölümünü frekans düzleminde yapılan araştırmalar oluşturmaktadır (Oğuz, 2006). Uzamsal alanda damgalama yöntemlerinde, filigranın bir bitinin yeri ile bir sonrakinin yeri arasında istatistiksel bağlılık bulunduğu için bu yöntemler saldırılara karşı frekans alanında damgalama yöntemlerine göre daha dayanıksızdır. Ancak frekans dönüşümü gibi karmaşık işlemler gerektirmediği için daha hızlı çalışır (Dar, 2014). Frekans uzayında yapılan görüntü damgalama uygulamalarında ise

her bir frekans bileşenine filigran verisi yerleştirilemediği için piksel uzayında yapılan görüntü damgalamaya göre daha az veri yükü elde edilir (Uçar, 2014).

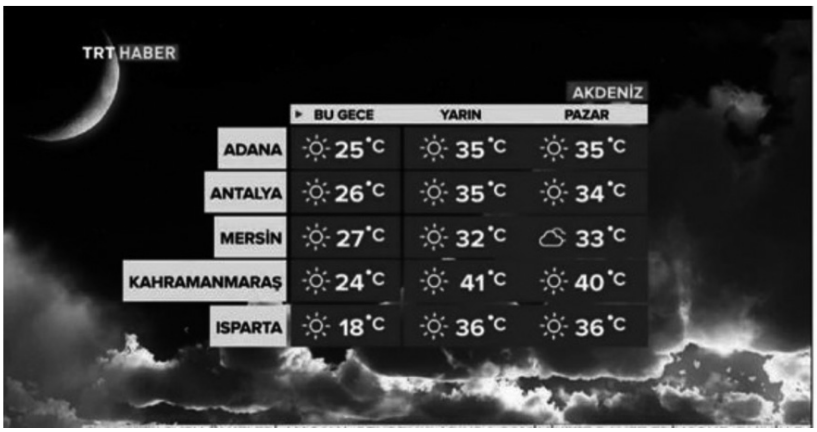
Taşınabilir müzik cihazları ve akıllı telefonlardaki müzik uygulamalarının yaygınlaşmasının sonucunda, telif haklarının korunması ve sayısal müziklerin güvenliğinin sağlanması ve izinsiz çoğaltılmasının engellenmesi için çeşitli ses damgalama yöntemleri geliştirilmiştir. Ses damgalamada en önemli ölçüt İİS'dir. Ses medyası damgalandıktan sonra İİS tarafından kapak verisindeki değişim algılanamayacak kadar az olmalıdır. Ses damgalama işlemi tıpkı video ve görüntü damgalamada olduğu gibi sıkıştırma ve filtreleme gibi pek çok saldırılara karşı dayanıklılık göstermelidir (Doğan, 2011). Ses verisinde kopya koruması için sıklıkla kullanılan damgalama yöntemlerinin en büyük problemi orijinal ses verisinde gerçekleşebilecek kalite kayıplarıdır (Rachid, 2014). Buna rağmen algılanamazlık yönünden ses damgalama, görüntü damgalamaya göre daha başarılı yöntemler sunar (Zhang ve Xie, 2014). Ses damgalamada ideal veri yükü miktarı, her 1kHz için 1kbps dir (Bhattacharyya vd., 2011). Telefon görüşmeleri 8 kHz, ses DVD'leri 96 kHz ve 192 kHz örnekleme sıklığına sahiptir. Örnekleme sıklığı, sesin frekans spektrumuna bir üst sınır koyarak veri gizlemeyi etkilemektedir. Örneklenen ses sinyali kuantalama ile sayısal ikili veri dizisine dönüştürülür. (Koyun ve Macit, 2018). Ses sinyali önce ses örneklerine bölünür. Ses medyasının veri yükü filigranın boyutunun çok üzerinde ise ilk örnekten itibaren filigran damgalanacak, sondaki örnekler boş kalacaktır. Gerçek hayatta duyulan sesler, sesin ortamdaki duvar ve nesnelerden defalarca yansıması nedeniyle doğal olarak çok sayıda yankı içerir (Ko vd., 2005). Ses sinyalindeki yankı bilgisine filigran gizlemek, damgalamada kullanılan yöntemlerden birisidir. Yankı gizleme, orijinal ses verisine, İİS tarafından algılanamayacak düzeyde bir yankı eklenmesi esasına dayanır ve insan kulağının zamansal maskeleme etkisinden yararlanır. Ses damgalamada kullanılan bir diğer yöntem kuantalamadır. Bu yöntemde orijinal ses örneği, modifiye edilmiş ses örneği ile değiştirilir. Ses sinyalinin her bir örneğine yalnız bir bit veri gömülebilir. Kuantalama yöntemi, uygulamada basit, filigranın algılanabilirliği bakımından güçlü ancak veri yükü bakımından zayıf bir yöntemdir (Khatri ve Chaudhari, 2013). Ses damgalamada, SS yöntemi de kullanılır. Bu yöntemde filigran, orijinal ses sinyalinin farklı frekans bantlarına yayılarak damgalanır. Yama tekniği de ses damgalamada kullanılan yöntemlerden biridir. Bu teknik, ilk olarak görüntü damgalama için rasgele istatistiksel bir yöntem olarak geliştirilmiştir (Bender, 1996). Temel olarak ses verisinin alt kümelerine filigranı gömmeyi amaçlar (Khatri ve Chaudhari, 2013). Parite kodlama yönteminde ise orijinal sinyali tüm örneklerine ayırmak yerine sinyal

örnek bölgelerine bölünür ve filigranın sıradaki bit değeri o bölgenin parite kodu ile karşılaştırılarak gömülür. Eğer parite biti ile filigranın sıradaki biti uyuşmazsa, yöntem filigranın sıradaki bitini örnek bölgesindeki örneklerin bir kısmının en önemsiz bitlerine gömer (Aigal ve Vasambekar, 2012).

Videolar, arka arkaya gösterilen görüntülerin birleşimi olarak düşünülebilir. Bu nedenle video damgalama yöntemlerinin çoğu görüntü damgalama tekniklerine dayanır ve doğrudan ham videoya veya sıkıştırılmış videoya uygulanır (Kashyap ve Singh, 2014). Video, görüntülerin dışında aynı zamanda ses verisi de içerir. Video damgalama yöntemlerinin çoğu yalnızca videoyu durağan görüntü çerçeveleri şeklinde ele alarak çalışsa da nadiren video içerisindeki ses verisine filigran yerleştiren yöntemler de kullanılmıştır.

## 6. ALGIYA GÖRE FİLİGRAN

İnsan algısı, damgalamanın önemli konularından biridir. Damgalama yöntemleri filigranların insan tarafından kolayca algılanıp algılanamamasına göre; algılanabilir, algılanamaz ve yarı saydam olarak üç sınıfta incelenir. Elbette, algılanamaz olanı daha çok tercih edilir, ancak bazı durumlarda filigranın algılanabilir olması gerekebilir. Filigranın algılanabilir olup olmaması uygulamaya göre değişmektedir (Abdülkhaev, 2016). Algılanabilir damgalama; filigranın İGS veya İSS ile kolayca algılanabildiği damgalama şeklidir. Örneğin bir TV kanalı, görüntünün bir köşesine kendi logosunu koyabilir (Şekil 6) veya bir müzik satış şirketi, sattığı müziklerin herhangi bir yerinde kendi firmasının reklamını sesli olarak yapabilir (Abdülkhaev, 2016).




**Şekil 6.** Algılanabilir Damgalama Örneği: Filigran Olarak TRT Haber Logosu

Algılanabilir damgalamanın önemli problemi, damgalama esnasında orijinal verinin bozulması ihtimalidir. Ayrıca algılanabilir filigran orijinal veriden kolaylıkla çıkarılamamalıdır. Çıkarma yapılabilse bile orijinal sinyalde veri kaybı yaşanmalı veya kullanılmaz hale gelmelidir. Filigran genellikle logo veya tescil şeklinde olduğu için filigranın yetkisiz çıkarımı sonucunda medyanın illegal çoğaltılması ve aidiyetinin belirsizliği sorunları ortaya çıkar (Doğan, 2011). Bu yüzden kırpma işlemine karşı filigranı korumak için filigran görüntüde geniş bir alana yayılmalı veya görüntünün önemli bir bölümü üzerine yerleştirilmelidir. (Oğuz, 2006). Yarı saydam damgalama, orijinal medya üzerinde İGS veya İİS tarafından sınırlı algılanabilecek değişimlere izin verilir. Genellikle bir görüntünün arka planına, görüntünün orijinali ile benzerliğini azaltmadan bir logonun yerleştirilmesi gibi uygulamalarda kullanılır. Algılanamaz damgalama, filigranın İGS veya İSS tarafından tespit edilemediği damgalama tipidir (Oğuz, 2006). Amaç filigranın varlığından alıcının haberdar olmaması, hatta şüphelenmemesidir. Algılanamazlık ve sağlamlık arasındaki ters orantıdan dolayı, algılanabilir damgalamaya göre daha az sağlamdır. Algılanabilir damgalama ile en büyük farkı, orijinal medyada daha az değişiklik yapmasıdır (Doğan, 2011).

## 7. SONUÇ

Sayısal damgalama; gelişen mobil teknolojiler, medya üretiminin kolaylaşması ve kişisel verilerin gizliliği problemlerindeki artış ile günden güne daha önemli bir araştırma alanı olarak karşımıza çıkmaktadır. Sayısal damgalama çalışmaları telif hakkı koruması için filigranlar gibi sağlam damgalama yöntemleri üzerinde yoğunlaşmış olsa da, pratikte veri güvenliği için kırılgan damgalama yöntemleri çok fazla kullanılmaktadır. Özellikle bir dijital görüntü üzerinde izinsiz değişiklik yapılma riski söz konusu ise, damgalama yönteminin kırılganlık ölçüsü, aynı zamanda yöntemin başarısını göstermektedir.

Yakın gelecekte müzik üreticilerinin telif hakları, müzik ve söyleşi paylaşım platformlarının daha da yaygınlaşması ile tamamen ikinci plana atılacaktır. Ayrıca çevrimiçi TV ve film izleme platformlarına ucuz ve kolay erişim ile sinema endüstrisi kan kaybetmiş, korsan video dağıtımı da oldukça azalmıştır. Önümüzdeki yıllarda müzik ve film dosyalarındaki telif hakkı sorunlarının da büyük ölçüde azalacağı söylenebilir. Ancak bireylerin mobil cihazları ile kolayca üretebildiği içerikler için telif hakkı sorunları artarak devam edecektir. Multimedya teknolojileri için sayısal damgalama teknolojilerinin uzun yıllar geliştirilmeye devam edecektir.

## KAYNAKÇA

Abbasfard, M., 2009. Digital Image Watermarking Robustness: A Comparative Study, Bilgisayar Mühendisliği A.B.D., Yüksek Lisans Tezi, 74s, Delft University of Technology, Hollanda.

Abbate, J., 1999. Inventing the Web, Proceedings of the IEEE, 87(11), 1999–2002.

Abdülkhaev, A., 2016. A New Approach for Video Watermarking, Gaziantep Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 66s.

Aigal, P., Vasambekar, P., 2012. Hiding Data in Wave Files, International Conference in Recent Trends in Information Technology and Computer Science, 20-24.

Al-Nazer, A., Gutub, A., 2009. Exploit Kashida Adding to Arabic e-Text for High Capacity Steganography, International Workshop on Frontiers of Information Assurance & Security (FIAS 2009) - IEEE 3rd International Conference on Network & System Security (NSS 2009), Gold Coast, Queensland, Avusturalya, 447-451.

Alasafi, L., 2016. Copyright Protection By Robust Digital Image Watermarking in Unsecured Communication Channels, Süleyman Demirel Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 62s, Isparta.

Alla, K., Prasad, R. S. R., 2009. An Evolution of Hindi Text Steganography, Sixth International Conference on Information Technology: New Generations, ITNG 2009, Las Vegas, Nevada, 1577 – 1578.

Alsalami, M.A.T., Al-Akaidi, M.M., 2003. Digital Audio Watermarking - A Survey, Proceedings of 17th European Simulation Conference, 25s.

Anderson, R. (Ed), 1996. Information Hiding - Vol 1174 of Lecture Notes in Computer Science, 350s, Springer-Verlag.

Arnold, M., Schmucker, M., Wolthusen, S.D., 2003. Techniques and Applications of Digital Watermarking and Content Protection, Artech House, 273s, Londra.

Baraklı, B., 2014. Tersinir Video Damgalama, Sakarya Üniversitesi, Fen Bilimleri Enstitüsü, Doktora Tezi, 101s.

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

Bennett, K., 2004. Linguistic steganography: Survey, analysis, and robustness concerns for hiding information in text, CERIAS Tech Report 2004-13, Center for Education and Research in Information Assurance and Security, Purdue University, West Lafayette, Indiana, USA.

Bhattacharyya, S., Kundu, A., Sanyal, G., 2011. A Novel Audio Steganography Technique by M16MA, International Journal of Computer Applications, (30)8, 26-34.

Boyacı, O., 2017. Doğal Dilde Steganografi, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 73s.

Boreiry, M., Keyvanpour, M.R., 2017. Classification of Watermarking Methods Based on Watermarking Approaches, Artificial Intelligence and Robotics (IRANOPEN) ,Tahran, İran, 73-76.

Brassil, J., Low, S., Maxemchuk, N., O'Gorman, L. 1995. Hiding Information in Document Images, Proceedings of the 29th Annual Conference on Information Sciences and Systems, 482-489.

Chaum D., 1981. Untraceable Electronic Mail, Return DWTresses and Digital Pseudonyms, Communications of the ACM, 24(2), 84-88.

Chore, A.M., Tiwari, N., 2017. Survey on Different Methods of Digital Audio Watermarking, Int. Journal of Engineering Research and Application, (7)6, 113-116.

Cox, I.J., Miller, M.L., 2002. The First 50 Years of Electronic Watermarking, EURASIP Journal on Applied Signal Processing (2), 126-132.

Cox, I., Miller, M., Bloom, J., Fridrich, J., Kalker, T., 2007. Digital Watermarking and Steganography 2nd Edition, Morgan Kaufmann Publishers, 624s, U.S.A.

Cox, I., Miller, M., Bloom, J., 2000. Watermarking Applications and Their Properties, International Conference on Information Technology 2000, Las Vegas, 1-5.

Dar, A.B., 2014. Watermarking in Frequency Domain A Review, International Journal Of Engineering And Computer Science, (3)11, 9215-9218.

Decker, S., 2001. Engineering considerations in Commercial Watermarking, IEEE Communications Magazine, 39(8), 128-133.

Doğan, Ş., 2011. Yeni bir sayısal damgalama tekniği ile biyometrik uygulamalar, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Doktora Tezi, 128s, Elazığ.

Eggers, J.J., Bauml, R., Girod, B., 2002. A Communications Approach to Image Steganography, Proceedings of SPIE (4675) Security and Watermarking of Multimedia Contents IV San Jose, California, USA.

Ertürkler, M., 2007. Sayısal filigranlar ile kripto imzalarının birlikte kullanılması ve çoklu ortam verisi üzerindeki uygulamaları, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Doktora Tezi, 220s.

Farid, H., 2001. Detecting Steganographic Message in Digital Images, Technical Report TR2001-412, Dartmouth College, 1-9.

Feng, J.B., Lin, I.C., Tsai, C.S., Chu Y.P., 2006. Reversible watermarking: Current status and key issues, International Journal of Network Security, 2(3), 161-171.

Fındık, O., 2010. Yapay Zeka Teknikleri Kullanarak Sabit Görüntüler İçin Sayısal Damgalama, Selçuk Üniversitesi, Fen Bilimleri Enstitüsü, Doktora Tezi, 120s.

Fridrich, J., 2006. Minimizing The Embedding Impact in Steganography, Proceeding of the 8th Workshop on Multimedia and Security, Geneva- İsviçre, 2-10.

Gupta, M.D. (Ed), 2012. Watermarking - Volume 2, INTECH, 276s, Slavka Krautzeka, Hırvatistan.

Hamza, Y.A., 2008. Blok Kırpma Kodlamasına ve Ayrık Dalgacık Dönüşümüne Dayalı, Dayanıklı Dijital Renkli Resim Damgalama Sistemi, Anadolu Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 92s.

Hartung, F., Girod, B., 1997. Watermarking of uncompressed and compressed video, Signal Processing, (66), 283-301.

Hering, H.,Hagmüller, M., Kubin, G., 2003. Safety and security increase for air traffic management through unnoticeable watermark aircraft identification tag transmitted with the VHF voice communication, Proceedings of the 22'nd Digital Avionics Systems Conference, 4(2), 1–10.

Herodotus, 1996. The Histories, Çev. S´elincourt, A., Penguin Books, 688s, Londra.

Hua, G., Huang, J., Shi, Y.Q., Goh, J., Thing, V.L.L., 2016. Twenty years of digital audio watermarking - a comprehensive review, Signal Processing, (128), 222–242.

Kahalkar, C., 2012. Digital Audio Watermarking for Copyright Protection, International Journal of Computer Science and Information Technologies, (3), 4185-4188.

Karpinskyy M., Kinakh Y., 2003. Reliability of RSA Algorithm and its Computational Complexity, IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Lviv, Ukrayna, 494-496.

Kashyap, N., Singh, S.N., 2014. Analysis of Multimedia Watermarking Techniques, International Journal of Emerging Technology and Advanced Engineering, (4)2, 517-521.

Khatri, G.B., Chaudhari, D.S., 2013. Digital Audio Watermarking Applications and Techniques, International Journal of Electronics and Communication Engineering & Technology (IJECET), (4)2, 109-115

Ko, B.S., Nishimura, R., Suzuki, Y., 2005. Time-spread echo method for digital audio watermarking, IEEE Trans. Multimedia, (7)2, 212–221.

Komatsu, N ve Tominaga, H., 1988. Authentication system using concealed image in telematics, Memoirs of the School of Science and Engineering, Waseda University, 52:45–60.

Koyun, A., Macit, H. B., 2018. Generating a stego-audio data using LSB technique and robustness test, Journal of Engineering Sciences and Design, 6(1), 87-92.

Kutucu, H., Dişli, A., Akça, M., 2015. Çok Katmanlı Steganografi Tekniği Kullanılarak Mobil Cihazlara Haberleşme Uygulaması, Akademik Bilişim Konferansı, Eskişehir.

Liu, B., Xu, E., Wang, J., Wei, Z., Xu, L., Zhao, B., Su, J., 2011. Thwarting Audio Steganography Attacks in Cloud Storage Systems, International Conference on Cloud and Service Computing, 259-265.

Mahajan, D.L., Gogate, S.A., 2016. Overview of Digital Watermarking and its Techniques, MIT- SOM PGRC KJIMRP National Research Conference (Special Issue), 197-204.

Mahmoud, K., Datta, S., Flint J., 2005. Frequency Domain Watermarking: An Overview, The International Arab Journal of Infotmation Technology, (2)1, 33-47.

Monathy, S.P., 1999. Digital Watermarking: A Tutorial Review, Report, Dept. Of Electrical Engineering, Indian Institute of Science, 24s.

Oğuz, C., 2006. Görüntü İşaretleri için Yeni Bir Sayısal Damgalama Yöntemi, İstanbul Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 100s, İstanbul.

Öztürk, M., 2009. Zaman-Frekans Analizi Kullanarak Görüntü Damgalama, İstanbul Üniversitesi, Fen Bilimleri Enstitüsü, Doktora Tezi, 110s.

Pan J.S., Huang H.C., Jain L.C., 2004. Intelligent Watermarking Techniques, World Scientific Publishing Co. Pte. Ltd., 680 p.

Patel, M., Sajja, P.S., Sheth, R., 2013. Analysis and Survey of Digital Watermarking Techniques, International Journal of Advanced Research in Computer Science and Software Engineering, (3)10, 203-210.

Petitcolas, F.A.P., Anderson, R.J. Kuhn, M.G., 1999. Information Hiding: A Survey, Proceedings of the IEEE, 87 (7), 1062-1078.

Po, L.M., 2001. Lenna 97: A Complete Story of Lenna. Erişim tarihi: 06.09.2018, http://www.ee.cityu.edu.hk/~lmpo/lenna/Lenna97.html.

Podilchuk, C.I., Delp, E.J., 2001. Digital watermarking: algorithms and applications, IEEE Signal Processing Magazine, 18(4), 33-46.

Qiao, L., Nahrstedt, K., 1999. Non-invertible watermarking methods for MPEG encoded audio. Proceedings of SPIE Conference on Security and Watermarking of Multimedia Data, (3657), 194–203.

Rachid, R.S.,2014. Binary Image Watermarking on Audio Signal Using Wavelet Transform, Çankaya Üniversitesi, Matematik-Bilgisayar Bilimleri Bölümü, Yüksek Lisans Tezi, 42s, Ankara.

Samphaiboon, N., 2009. Steganography via running short text messages, Multimedia Tool Applications, 52(2–3), 569–596.

Shih, F. Y., 2005. Digital Watermarking and Steganography Fundamentals and Techniques, CRC Press, 200s, London

Simpson, J., ve Weiner, E, 1989. Oxford English Dictionary, Oxford University Press, 22000s, Oxford, England.

Spainas, A., Painter, T., Atti, V., 2007. Audio Signal Processing and Coding, Wiley Interscience, 459s, New Jersey, A.B.D.

Szepanski, W., 1979. A signal theoretic method for creating forgery-proof documents for automatic verification, Carnahan Conference on Crime Counter measures, Proceedings May 16-18, 101–109.

Şatır, E., 2013. Bilgi Güvenliği İçin Metin Steganografisinde Yeni Bir Yaklaşım, Selçuk Üniversitesi, Fen Bilimleri Enstitüsü, 82s.

Şen, Ş., 2006. İndirgenmiş SPN (Substitution Permutatin Network) Algoritması için Lineer Kriptanaliz Uygulaması, Yüksek Lisans Tezi, Trakya Üniversitesi, Fen Bilimleri Enstitüsü, 113s, Edirne.

Tacticius, A. 2002. How to Survive Under Siege, Clarendon ancient history series, Çev. Whitehead, D., Bristol Classical Press, 236s, Bristol, U.K.

Tunçer, S., Karakuzu, C., 2016. Veri Güvenliğini Artırmak Amacıyla Bilgiyi Şifreleme ve Steganografik Yöntemlerle Görüntüye Gizleme, Elektrik-Elektronik ve Bilgisayar Sempozyumu, Tokat, Türkiye, 183-87.

Uçar, A., 2014. Gezgin Ortamda Görüntü Damgalama Uygulaması, Kocaeli Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 34s.

UK Patent, GB 2196167A,1988. Holt, L., Maufe, B. G., ve Wiener, A., Encoded marking of a recording signal.

United States Patent, 3,004,104, 1961. Hembrooke, E.F., Identification of soundandlikesignals.

United States Patent, 4,281,217, 1981. Dolby, R., Apparatus and method for the identification of specially encoded FM stereophonic broadcasts.

Ülker, E., Fındık, O., İşcan, H., 2006. Selçuk Üniversitesinde Sayısal İmza Uygulaması, Ulusal Elektronik İmza Sempozyumu, Ankara, 123-129.

Vassiliadis, S., Wong, S., Gaydadjiev, G., Bertels, K., Kuzmanov, G., Panainte, E.M., 2004. The Molen Polymorphic Processor, IEEE Transactions on Computers, (190), 1363–1375.

Yalman, Y., Ertürk, İ., 2009. Gerçek Zamanlı Video Kayıtlarına Veri Gizleme Uygulaması, XI. Akademik Bilişim Konferansı Bildirileri, Harran Üniversitesi, Şanlıurfa, 545-552.

Yavuz, E., 2008. Duruk İmgelerde Damgalama ve Veri Saklama, Ankara Üniversitesi, Fen Bilimleri Enstitüsü, Doktora Tezi, 167s.

Yıldırım, İ., 2017. Şifreli ve Şifresiz Videolar İçin Yinelemeli Histogram Değiştirme Tabanlı Tersinir Video Damgalama, Sakarya Üniversitesi, Fen Bilimleri Enstitüsü, Doktora Tezi, 86s, Sakarya.

Zhang, X., Xie, X., 2014. Audio Watermarking Based on Multiple Echoes Hiding for FM Radio, Interspeech 2014 Singapore, 1386-1390.