T.C.
ÇANAKKALE ONSEKİZ MART ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
YÜKSEK LİSANS TEZİ

WAVELET TABANLI TELİF HAKKI KORUMA YÖNTEMİ

Ramazan GÜRLEK
Bilgisayar Mühendisliği Anabilim Dalı
Tezin Sunulduğu Tarih: **24/10/2011**

Tez Danışmanı:
Yrd.Doç.Dr. İbrahim TÜRKYILMAZ

ÇANAKKALE

YÜKSEK LİSANS TEZİ SINAV SONUÇ FORMU

RAMAZAN GÜRLEK tarafından **YRD. DOÇ. DR. İBRAHİM TÜRKYILMAZ** yönetiminde hazırlanan "**WAVELET TABANLI TELİF HAKKI KORUMA YÖNTEMİ**" başlıklı tez tarafımızdan okunmuş, kapsamı ve niteliği açısından bir Yüksek Lisans tezi olarak kabul edilmiştir.

Yrd. Doç. Dr. İbrahim TÜRKYILMAZ

Danışman

Doç. Dr. İsmail KADAYIF

Jüri Üyesi

Yrd.Doç.Dr. Can AKTAŞ

Jüri Üyesi

Sıra No :

Tez Savunma Tarihi: 24/10/2011

Prof. Dr. İsmet KAYA

Müdür

Fen Bilimleri Enstitüsü

İNTİHAL (AŞIRMA) BEYAN SAYFASI

Bu tezde görsel, işitsel ve yazılı biçimde sunulan tüm bilgi ve sonuçların akademik ve etik kurallara uyularak tarafımdan elde edildiğini, tez içinde yer alan ancak bu çalışmaya özgü olmayan tüm sonuç ve bilgileri tezde kaynak göstererek belirttiğimi beyan ederim.

Ramazan GÜRLEK

TEŞEKKÜR

Bu tezin gerçekleştirilmesinde, çalışmamın her aşamasında benden bir an olsun yardımlarını esirgemeyen, değerli fikir ve katkıları ile çalışmalarıma yön veren danışmanım Yrd. Doç.Dr. İbrahim TÜRKYILMAZ'a, ders aldığım değerli hocalarıma ve desteğini benden esirgemeyen eşim Zuhal ÖLMEZ GÜRLEK'e sonsuz teşekkürlerimi sunarım.

Ramazan GÜRLEK

SİMGELER VE KISALTMALAR

CA	Sertifika Otoritesi (Certification Authority)
DWT	Ayrık Dalgacık Dönüşümü (Discreate Wavelet Transform)
DCT	Ayrık Kosinüs Dönüşümü (Discreate Cosinus Transform)
DFT	Ayrık Fourier Dönüşümü (Discreate Fourier Transform)
PSNR	Doruk Sinyal Gürültü Oranı (Peak Signal-to-Noise Ratio)
LSB	En Az Anlamlı Bit (Least Significant Bit)
LL_t	t'inci Seviye Temel Alt Bant Görüntü
LH_t	t'inci Seviyeden Düsey Alt Bant Görüntü
HL_t	t'inci Seviye Yatay Alt Bant Görüntü
HH_t	t'inci Köşegensel Alt Bant Görüntü
H_X	X Görüntüsünün Yüksekliği
W_X	X Görüntüsünün Genişliği
O	Orijinal görüntü
W	Filigran
K	Anahtar

ÖZET

WAVELET TABANLI TELİF HAKKI KORUMA

Ramazan GÜRLEK

Çanakkale Onsekiz Mart Üniversitesi

Fen Bilimleri Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı Yüksek Lisans Tezi

Danışman: Yrd. Doç.Dr. İbrahim TÜRKYILMAZ

24/10/2011, 67

Telif hakları koruma için sayısal imza yöntemi iyi tanımlanmış bir güvenlik metodudur. Bu sebepten telif hakları koruma için sayısal filigran oluşturmak oldukça dikkat çekmektedir. Maalesef önerilen filigran yöntemleri hala bazı eksiklikler içermektedir. Kriptoğrafik araçların ve sayısal filigranlamanın avantajlarının her ikisinde mümkün olduğu yollarla kriptoğraflama araçlarının filigranlama içirisine yerleştirmeye çalışacaktır. Herkes tarafından doğrulanabilen özelliği ve tolere edilebilir bozulma özelliği bu yüzden mümkün olmaktadır. Bu fikirler temel alınarak, geleneksel filigranlama tekniklerinden farklı olarak, kayıpsız ve sağlam telif hakları koruma yöntemi önerilmektedir.

Yöntemimiz geleneksel görüntü işleme, geometrik bozulmalar ve bazı amaçlı saldırılara koayabilme yeteneğine sahiptir. Ne yazık ki önerilen filigranlama yöntemi hala bazı az sayıda tehdit unsuru için zayıflık göstermektedir.

Sağlamlık özelliğini ispatlamak için bir dizi deneyler gerçekleştirildi. Stirmark saldırıları önerilen yöntemin değerlendirme doğrulaması için kullanılmıştır.

Anahtar sözcükler: Sayısal Filigran, Sayısal İmza, Telif Hakkı, Dalgacık Dönüşümü

ABSTRACT

WAVELET BASED COPYRIGHT PROTECTION

Ramazan GÜRLEK

Çanakkale Onsekiz Mart University

Graduate School of Natural and Applied Sciences

Department of Computer Engineering

Advisor : Assist. Prof. Dr. İbrahim TÜRKYILMAZ

24/10/2011, 67

It is well known that a digital signature scheme is a well-defined security method for copyright protection. For this reason, construction of digital watermarking has received considerable attention for copyright protection. Unfortunately, the proposed watermarking schemes have some deficiencies. Here, cryptographic tools will be introduced into watermarking schemes, in such a way that both the advantages of cryptographic tools and digital watermarking are available. The publicly verifiable and tolerant distortion properties are possible for this case. Based on this idea, apart from the conventional watermarking techniques, a lossless and robust copyright-protection scheme is proposed.

Our scheme is capable of resisting common image processing, geometric distortions and some intentional attacks. Unfortunately, proposed watermarking method still has some weakness for a few numbers of the attacks.

The robustness property has been proved conducting for a series of experiments. As specialy, the StirMark attacks are adopted as benchmark verification of the proposed method.

Keywords: Digital Watermark, Digital Signature, Copyright, Wavelet Transformation

İÇERİK **Sayfa**

BÖLÜM 1
GİRİŞ

Günümüzde hızlı gelişen multimedya ve network ortamlarındaki gelişmeler dikkate alındığında sayısal verilerin eskiye göre daha hızlı ve kolaylıkla dağıtılabilmesi önemli ve üzerinde durulması gereken bir gerçektir. Sayısal verilerin kopyasının kolaylıkla yapılmasından dolayı, sayısal telif hakları korumanın güçlendirilmesi önemli bir konu olarak ortaya çıkmaktadır.

Telif hakları koruma için sayısal imza yöntemi ve sayısal zaman mührü iyi tanımlanmış iki farklı güvenlik metodudur (Schneier, 1996). Bununla beraber, bu teknikler sayısal görüntülerin korunmasında ne yazik ki uygun olmamaktadır. Bunun nedeni, görüntü boyutunun metinden çok daha büyük ve sayısal görüntüyü imzalamanın daha çok zaman gerektirmesidir. Diğer bir neden de imzalanmış veride bozulmalara izin verilmemesidir. Bu gereksinim sayısal görüntü için her zaman gerekli değildir. Küçük bozulmalar içeren imzalanmış görüntü hala kabul görülebilmektedir. Çünkü insanın görsel algılama sistemi küçük seviyedeki bozulmaları algılayabilecek hassaslıkta değildir (Chen ve ark.,1998).

Son 20 yılda sayısal filigranlama, telif hakları koruma alanında kayda değer ilgi çekmiştir. Ticari marka, mühür veya seri numarası gibi imza ve telif hakları mesajı içeren sayısal filigranlama teknikleri kullanılmaktadır. Gömülen filigran ticari değeri yok etmeyecek şekilde bozulmalara karşı dayanıklı olmalıdır. Böylece talep edilen telif hakları koruma başarılmış olmaktadır.

Şekil 1.1 Filigran ve 20 Türk lirası.

Şekil 1.1'de gürüldüğü gibi 20 TL'lik kağıt banknotun Atatürk portresinin olduğu tarafı ışığa tutup bakılırsa, sol tarafta filigran olarak Atatürk portresinin küçüğü ile küpür değerini gösteren "20" sayısının yankılandığı görülmektedir. Bu filigran, kağıt yapımı sürecinde kağıda doğrudan gömülür ve bu nedenle paranın sahtesini yapmak oldukça zorlaştırılmış olur. Bu aynı zamanda kalpazanın 20 TL'lik banknotun mürekkebini temizleyip aynı kağıt üzerine 100 TL'lik banknotu basması şeklinde yapılan yaygın sahtecilik yöntemine de engel olmuş olur.

Günümüzdeki çoğu kağıt filigranlarında olduğu gibi 20TL banknot üzerindeki filigranın, bu tezin konusu ile yakından ilgili iki temel özelliği vardır. Birincisi; filigran sadece özel bir algılama sürecinin bir sonucu olarak görünür hale gelir, normal kullanımı sırasında görünmez (banknotun ışığa tutulduğu durum). İkincisi; filigran, içinde gizlenen nesne hakkında bilgi taşır (bu durumda, filigran banknotun doğruluğunu gösterir).

Filigranlama diğer fiziksel nesnelere ve elektronik sayısal sinyallere de uygulanabilmektedir. Kumaşlar, giysi etiketleri ve ürün paketlemeler, özel görünmez boyalar ve mürekkepler, filigranlanabilir fiziksel nesne örnekleri olarak karşımıza çıkmaktadır. Müzik, fotoğraf ve videonun kullanıldığı elektronik sunumlar yaygın türlerdeki filigranlanabilir sinyallerdir.

Genel olarak, ilgilendiğimiz filigranlama sistemi bir gömücü ve bir algılayıcıdan oluşmaktadır. Gömücü iki girdi almaktadır. Biri, bir filigran olarak kodlamak istenilen mesaj, diğeri içine işaret veya mesajı gömmek istediğiniz korunması amaçlanan nesnesidir. Filigran gömücünün çıktısı genellikle iletilir veya kaydedilir. Daha sonra, bu, filigran algılayıcı için bir girdi olarak kullanılır. Çoğu algılayıcılar filigranın var olup olmadığını belirlemeye çalışır, eğer varsa, kodlanan mesajı çıktı olarak verir.

Yukarıda verilen ana hatlar dikkate alınarak yapmış olduğumuz çalışmayı tez düzenin de genel hatlarıyla şu şekilde sıralayabiliriz: Birinci Bölümde telif hakları ve filigranlamaya kavramına bir giriş yapılmıştır. Filigranlamanın tarihçesi ile giriş yapılan ikinci bölümde, filigranlama sistemleri ve temel ilkeleri anlatıldıktan sonra filigranlama yöntemleri, filigranlama yöntemlerin temel özellikleriyle önerilen yöntemin temel özellikleri açıklanmıştır. Üçüncü bölümde, tez çalışmasında kullanılan materyaller ve önerilen telif hakkı koruma için filigranlama algoritması ayrıntılı bir şekilde açıklanmıştır. Dördüncü bölümde sayısal deney sonuçları ve bu sonuçların değerlendirmeleri yer almaktadır. Beşinci ve son bölümde ise sonuçların yorumlanmasından elde edilen filigranlama yapılırken dikkat edilmesi gereken bazı önemli öneriler bulunmaktadır.

BÖLÜM 2
ÖNCEKİ ÇALIŞMALAR

2.1. Telif Hakkı ve Filigranlamanın tarihçesi

Tarihte bilinen ilk telif hakkı vakası 6. yüzyılda meydana gelmiştir. Cathach veya Clan O'Donnell'in savaş kitabı olarakta bilinen Aziz Columba'nın Zeburu, Zeburun mevcut en eski İrlandaca el yazmasıdır. Aynı zamanda dünyada bilinen telif hakkı ihlalinin ilk örneği olarak kabul edilebilir (El yazması milattan sonra 560 ile 630 tarihleri arasına aittir; geleneksel olarak 567 tarihi verilmektedir). Elde edilen bilgilere göre Columba izni olmadan başrahip Finnian'ın Zeburunu kopyalamıştır. Aziz Finnian bu olayı öğrendiğinde o kopyanın kendisine teslim edilmesini istemiş, ancak Columba reddetmiştir. Bunun üzerine Finnian, Kral Diarmait Mac Cerbhaill'e başvurur. Kral, "Her ineğin buzağısı kendisine aittir, bu nedenle her kitabın kopyası da o kitaba aittir " hükmünü verir ve Columba kopyayı Finnian'a teslim etmesini emreder ama Columba bu olay yüzünden çıkan Culdreimhe savaşına kadar bu karara uymaz (Arnold ve ark., 2003).

Filigrana gelince, kağıt yapımı sanatını daha önceki bin yıllarda Çin'de icat olmasına rağmen, ilk kağıt filigran 1282'li yıllarda İtalya'da ortaya çıkmıştır. Filigranlar kağıt kalıplara ince tel paternleri eklenerek yapılmıştır. Kağıt, telin olduğu yerde biraz daha ince ve saydam olmaktadır (Cox ve Ark.2003).

İlk filigranların anlam ve amacı belirsizdir. Kalıpların hangi kağıt yaprağından yapıldığını tespiti gibi pratik işlevler için veya kağıdı imal edenin tespiti için ticari amaçlı olarak kullanılmış olabileceği tahmin edilmektedir. Öte yandan, filigranlar mistik işaretleri temsil etmek veya sadece dekorasyon amaçlı olarak da kullanılmış olabileceği ifade edilmektedir (Cox ve Ark., 2003).

On sekizinci yüzyılda, Avrupa ve Amerika'da yapılan kağıt üzerinde filigran daha net faydalı olmuştur. Kağıdın imal edildiği tarihi kaydetmek ve orijinal yaprak boyutlarını göstermek için ticari olarak kullanılmışlardır. Ayrıca aynı tarihlerde filigranlar para ve diğer belgeler üzerinde sahteciliğe karşı önlem olarak kullanılmaya başlanmıştır (Seitz, 2005).

Sayısal filigranlamadan ilk ne zaman söz edildiğini belirlemek zordur. Dijital damgalamaya benzeyen ilk örnek 1954 yılında görülmüştür; Muzac şirketinden Emil Hembrooke tarafından hak sahipliğini kanıtlamak için müziğe fark edilemeyen kimlik kodu gömme metodu olarak tanımlanan ve "ses ve benzeri sinyallerin belirlenmesi" ismi verilen patenti kayda geçirmiştir. 1979 yılında ise Szepanski taklitciliğe karşı durmak için

dokümanlara üzerinde yer alabilecek bir makina-algılayabilir patern tanımlamıştır. Dokuz yıl sonra, Holt *ve ark*., bir ses sinyalinin içine kimlik kodu gömmek için bir yöntem tanımlamıştır. Ancak, Komatsu ve Tominaga 1988 yılında, sayısal filigranlama terimini kullanmış ilk kişiler olarak ortaya çıkmaktadır (Cox ve Miller, 2001; Cox ve ark., 2002).

1990'lı yılların sonlarında sayısal sistemlerde çeşitli içerikteki filigranlamaya ilgide patlama olmuştur. Fotoğraf, ses ve video ana odak noktası olmak üzere, ikili görüntü, metin, çizimler, üç boyutlu modeller, animasyon parametreleri, çalıştırılabilir kod ve entegre devreler gibi içerikler filigranlanmıştır.

2.2. Filigranlamanın temel ilkeleri

Bu araştırma alanı hala nispeten yeni olması ve farklı gelenekleri ile çeşitli disiplinlerden katılımcıların araştırmalara katkıda bulunmasından dolayı, terminolojinin kullanımı oldukça çeşitlidir. Bu bölüm filigranlama sistemlerine ve onların tanıtımı için bu kapsamda kullanılan terimler için bir biçimsel giriş niteliği taşımaktadır (Arnold ve ark., 2003).

Geçerli damgalama sistemlerinin temel prensibi olan filigranın şifrelenmesi ve şifresinin çözülmesi için aynı anahtarın kullanılmasından dolayı simetrik şifrelemeyle karşılaştırılabilir (Arnold ve ark., 2003). Her filigranlama sistemi, filigranlama şifreleyicisi ve ilgili şifre çözücüsü olmak üzere iki alt sistemden oluşur. Bir damgalama sistemi tüm orijinal veri kümesi O, tüm filigranlar kümesi W ve tüm anahtarlar K olmak üzere $\langle O, C, W, K, E_K, D_K, C_\tau \rangle$ değişkenler grubuyla tanımlanabilir. Aşağıdaki iki fonksiyon, sırasıyla gömme ve algılama süreçlerini tanımlamaktadır;

$$E_K : O \times W \times K \to O \tag{2.1}$$

$$D_K : O \times K \to W \tag{2.2}$$

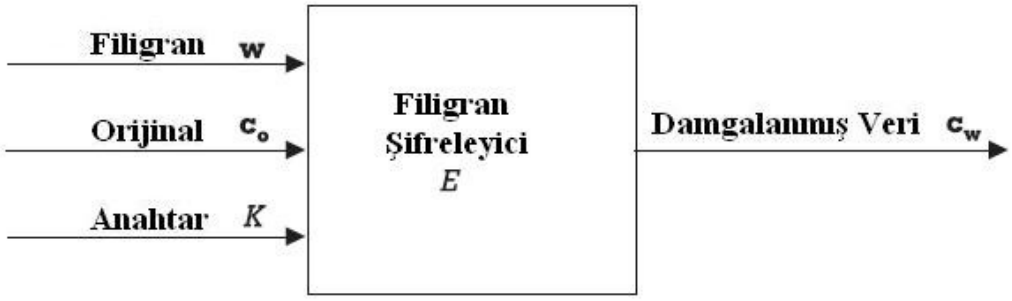
Karşılaştırıcı fonksiyonu

$$C_\tau : W^2 \to \{0,1\} \tag{2.3}$$

karşılaştırma için τ eşiğini kullanarak çıkartılmış ile gerçekten gömülmüş filigranı karşılaştırır. Gömme sürecinin girdi parametreleri, taşıyıcı nesne (veya orijinal c_o), gömülecek w filigranı, ilaveten K gizli veya açık anahtarıdır;

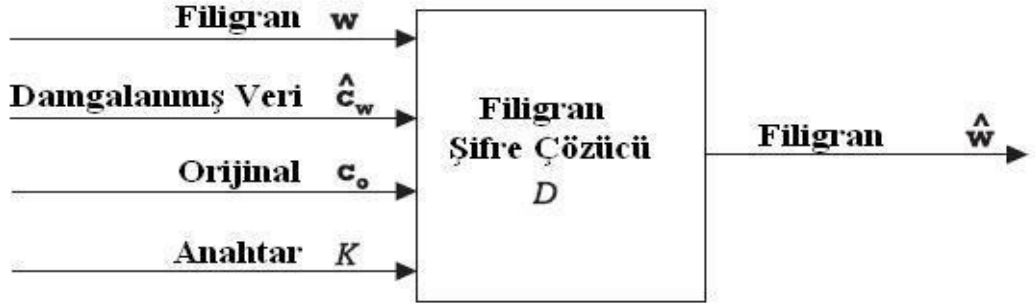
$$E_K(c_o, w) = c_w \tag{2.4}$$

Şifreleyicinin çıkışını işaretlenmiş veri kümesi oluşturur (bakınız, Şekil 2.1).



Şekil 2.1 Genel filigran şifreleyici.

Algılama sürecinde işaretlenmiş ve muhtemelen değiştirilmiş $\hat{c}_w$ veri kümesi, orijinal c_o, filigran w ve gömme işlemi sırasında kullanılan K anahtarı giriş parametrelerinin maksimum kümesini oluşturur (bakınız, Şekil 2.2).



Şekil 2.2 Genel Filigran Şifre Çözücü.

Filigranlama sistemlerinin çeşitli tiplerinde, okuma sürecinde girdi parametrelerinin sayısı farklılık göstermektedir. Çıkarılmış filigran $\hat{w}$, mümkün olan manipülasyonlar nedeniyle gömülmüş filigran w'den genellikle farklılıklar içerir. Her iki Filigranın benzerliğini değerlendirebilmek için, karşılaştırıcı fonksiyonu C_τ, τ eşik değerine dayalı olarak şüpheli filigranı okunan ile karşılaştırılır:

$$C_\tau\left(\hat{w}, w\right) = \begin{cases} 1, & c \geq \tau \\ 0, & c < \tau \end{cases} \tag{2.5}$$

Eşik değeri olarak seçilen τ, algoritmaya bağlıdır ve kusursuz bir sistemde filigranı açıkça tanımlayabilmesi gerekmektedir. Filigranlama sistemlerinin bu biçimsel analizi ayrıca filigranlama algoritmalarının geometrik bir yorumunu geliştirmek için de kullanılabilir.

2.3. Filigranlama sistemleri

Filigranların çeşitli türleri yanı sıra, dört farklı filigranlama sistemi algılama sürecinde giriş ve çıkışa göre sınıflandırılmaktadır. Algılayıcı tarafında daha fazla bilgiyi kullanmak, tüm filigranlama sisteminin güvenilirliğini artırır ama gömücü tarafta filigranlama yaklaşımının uygulanabilirliğini sınırlar.

Algılama sürecinde taraf bilgisi orijinal c_o ve filigran w'nin kendisi olabilir (bakınız, Şekil 2.2). Bu nedenle, taraf bilgi gereksinimlerinin dört permütasyonu mümkündür.

Kör olmayan filigranlama sistemleri, okuma sürecinde en azından orijinal veriyi gerektirir. Bu tür sistemi şifre çözme süreci içinde filigranın gerekli olup olmadığına bağlı olarak ilave alt bölümlere bölebiliriz.

- Tip I sistemlerde potansiyel olarak manipüle edilmiş veri kümesinin filigranı orijinali vasıtasıyla algılanır:

$$D_K\left(\hat{c}_w, c_o\right) = \hat{w} \tag{2.6}$$

- Tip II sistemler ilaveten filigran kullanırlar ve bu nedenle en genel halde betimlenirler:

$$D_K\left(\hat{c}_w, c_o, w\right) = \hat{w} \quad \text{ve} \quad C_\tau\left(\hat{w}, w\right) = \begin{cases} 1, & c \geq \tau \\ 0, & c < \tau \end{cases} \tag{2.7}$$

Bu sistemler filigran *w*, veri kümesi $\hat{c}_w$ içine gömülmüş müdür sorusuna cevap verir. Bu şekilde filigranın bilgi içeriği 1 bittir. Daha fazla bilgi kullanarak, bu filigranlama yöntemlerinde sağlamlık genel olarak artış içindedir.

- Yukarıdaki yöntemden farklı olarak, yarı kör filigranlama algılama için orijinal veri kullanmaz:

$$D_K\left(\hat{c}_w, w\right) = \hat{w} \quad \text{ve} \quad C_\tau\left(\hat{w}, w\right) = \begin{cases} 1, & c \geq \tau \\ 0, & c < \tau \end{cases} \tag{2.8}$$

Bu, orijinale erişimin pratik veya mümkün olmadığı uygulamalarda esastır. Yarı kör filigranlama yöntemleri kopya kontrolü ve telif haklarının korunması için kullanılabilir.

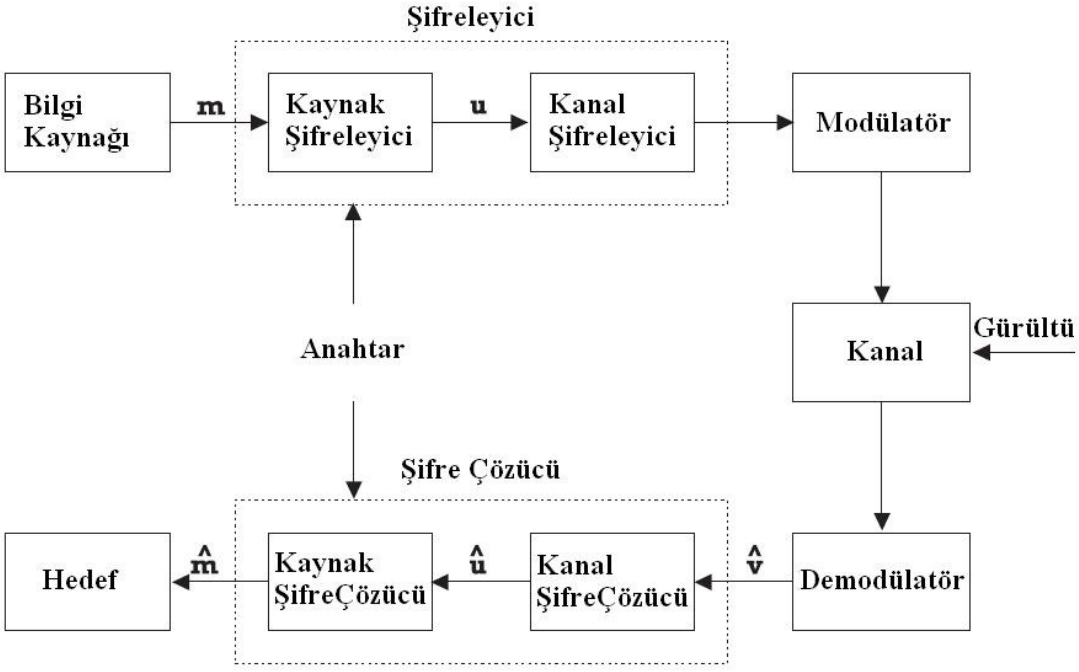
- Kör filigranlama bir filigranlama sisteminin geliştirilmesi için en büyük meydan okumadır. Çözme sürecinde ne orijinal ne de filigran kullanılır:

$$D_K\left(\hat{c}_w\right) = \hat{w} \tag{2.9}$$

Bu örneğin yasadışı dağıtılan kopyaların takibi sırasında olduğu gibi $\hat{c}_w$ işaretlenmiş veri kümesinin n bitlik bilgisinin okunmasının gerektiği uygulamalarda gereklidir.

2.4. Filigranlama Sistem Modelleri

Filigranlama, filigranlanmış orijinal eseri içeren filigranın bir kanal üzerinden haberleşmesi olarak düşünülebilir. Bu nedenle, filigran için kavramsal modellerinin geliştirilmesindeki doğal bir yaklaşım, iletişim modelleri ve ilgili filigranlama algoritmaları arasındaki benzerlikleri incelemektir. Her iki model veriyi bilgi kaynağından (filigran) bir hedefe (kullanıcı veya başka bir sistem) iletir.



Şekil 2.3 Güvenli iletim için haberleşme modeli.

İletişimin tipik modeli (Şekil 2.3'te gösterildiği gibi) çeşitli bloklardan oluşmaktadır. Bu model 1948 yılında Shannon tarafından tanıtıldı (Cox, 2002). Kaynak mesajı m kaynak şifreleyici üzerinden ikili sayı dizisi u'ya dönüştürülerek şifrelenmiş kaynağını bilgi dizisi olarak sunar. Süreç kaynak çıkışını gösteren bitlerin sayısını azaltmak için ve bilgi dizisinden kaynağın yeniden anlaşılır inşasını sağlamak için gerçekleştirilir (Lin ve Costello, 1983).

Kanal şifreleyici kodlanmış bilgi dizisi u'yu kod kelimesi olarak adlandırılan v

şifrelenmiş dizisine dönüştürür.

Bir fiziksel kanal üzerinden ayrık sembolleri iletmek için, bir modülatör şifrelenmiş v dizisinin her bir sembolünü iletim için uygun biçime dönüştürür (Proakis ve Manolakis, 1992). Kanal üzerinden iletimi sırasında, dönüştürülüş dizi gürültü tarafından bozulmuştur. İletimi bozabilen farklı biçimlerdeki gürültü kanal karakteristikleri ile geçirilir. Alıcı tarafında, demodülatör iletilmiş diziyi işletir ve şifrelenmiş dizisinin kopyasını içeren $\hat{v}$ çıkışını üretir. Şifreleyicidekine benzer olarak, kanal şifre çözücüsü iletilmiş doğru diziyi tahmin ederek demodülatörün çıkışını ikili dizi $\hat{u}$'ya dönüştürür. Mükemmel bir kanalda tahmin edilen $\hat{u}$, doğru dizi u'nun bir kopyasıdır. Dikkatli tasarlanmış kaynak şifreleyicileri kanalın gürültüsüyle olan bozulmalardan kaynaklanan kodlama hatalarını azaltabilir (Proakis ve Manolakis, 1992). Son adımda kaynak şifre çözücü çıkış kaynağını tahmin ederek $\hat{u}$ şifresi çözülmüş dizisiye dönüştürerek hedefe gönderir.

İletişim kanallarının farklı türleri iletim sırasında uygulanan gürültünün tipine ve gürültünün sinyale nasıl uygulandığına göre kategorize edilebilir.

Kanal karakteristiklerinin yanı sıra, haberleşmeyi engellemeye çalışan aktif saldırılara ve haberleşmeyi gözetlemeye çalışan pasif saldırılara karşı güvenliği sağlamalarına göre iletim ayrıca sınıflandırılabilir.

Saldırılara karşı savunma aşağıdakilere dayanır:

- Aktif saldırıları engellemeye çalışan genişleme spektrumlu (spread spectrum) teknikler;
- Kriptografi, mesajın gizliliğini garanti etmek için şifreleme.

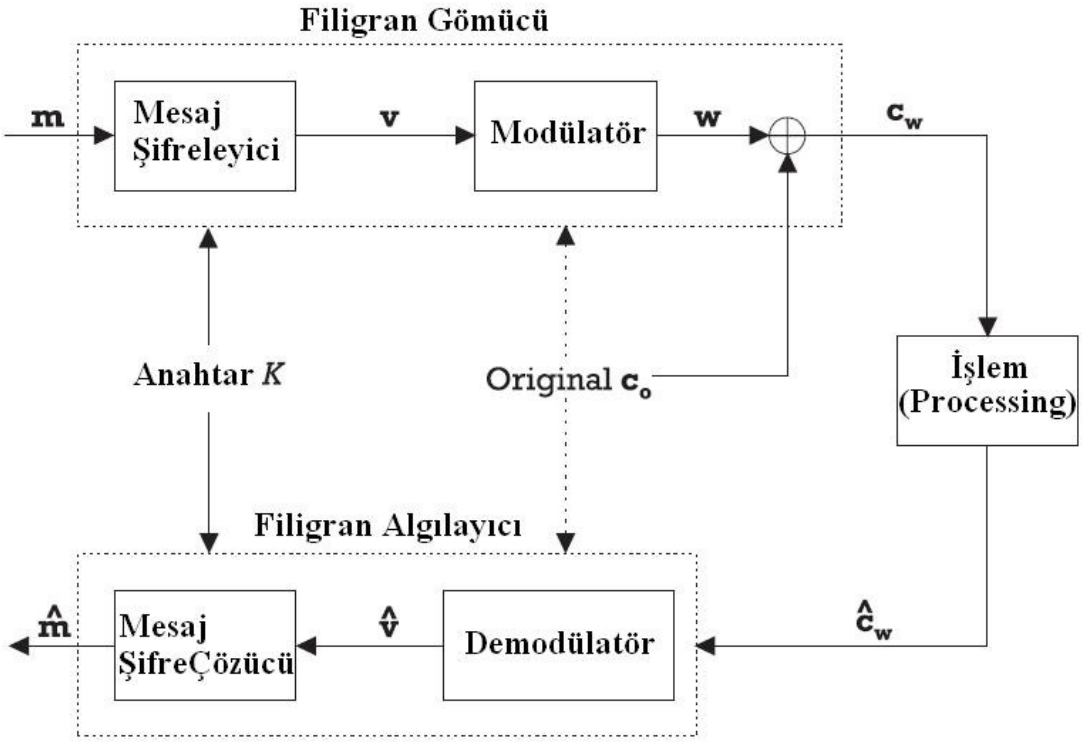
Sayısal filigranlama ve Spread spektrumlu teknikleri farklı haberleşme grupları arasındaki haberleşme frekansını bozma gibi aktif saldırılarını engellemede benzer güvenlik gereksinimlerini yerine getirmeye çalışır. Spread-spectrum teknolojileri şifreleyici ve şifre çözücü kanallarda gizli anahtara göre modülasyonu gerçekleyerek haberleşmenin gizliliğini kurar (bakınız, Şekil 2.3).

Bir filigranlama modeli değişik yorumlamalarla haberleşme modelindeki gibi aynı temel blokları içeren haberleşmeye dayanır. Modülasyon/demodülasyon bloklarını içeren, sırasıyla filigran gömücü/algılayıcı ve kanal şifreleyici/şifre çözücü arasında doğrudan bir benzerlik vardır. İletilen mesaj filigran kendisidir. Kanal üzerideki sinyalin güvenli iletiminin ilave gereksimi şifreleme ve şifre çözme yordamında gizli anahtarın kullanımını gerektirir

Kanal karakteristikleri şu şekilde modellenebilir:

- Filigran taşıyan koruyucu nesne kanalı temsil eder;
- Filigranlanmış nesnenin iletimi sırasında meydana gelebilecek farklı işlem tarafından farklı gürültü oluşur. Bu ilave işlem tahmin edilen manipülasyonlar veya kasıtlı saldırılar olabilir.

Filigran gömücünün şifreleme bloğu m filigran mesajını v şifrelenmiş dizisine şifreler. Modülasyon sırasında, kanal üzerinde iletilebilmesi için v dizisi bir fiziksel sinyale yani w filigran sinyaline dönüştürülür. Filigranlanmış ve orijinal koruyucu nesne arasındaki fark filigranın eklenmesine rağmen orijinal veri kümesindeki gibi temelde aynı sayısal gösterimin olmasıdır. Örneğin, bir ses dosyası için eklenmiş filigran koruma parçasında olduğu gibi aynı örnekleme hızlı ve bit çözünürlüklü sinyal olacaktır. Filigran algılama tarafında, olası bozuk filigranlanmış nesne, v kodlanmış dizisinin bozulmuş hali olan $\hat{v}$'ye demodüle edilir. $\hat{m}$ filigran mesajı, filigran mesaj şifreleyici vasıtası ile $\hat{v}$'den elde edilir (bakınız, Şekil 2.4).



Şekil 2.4 Temel filigran iletişim modeli.

Temel iletişim sistemine benzer olarak, şifreleyici üç adımı gerçekleştirmek zorundadır:

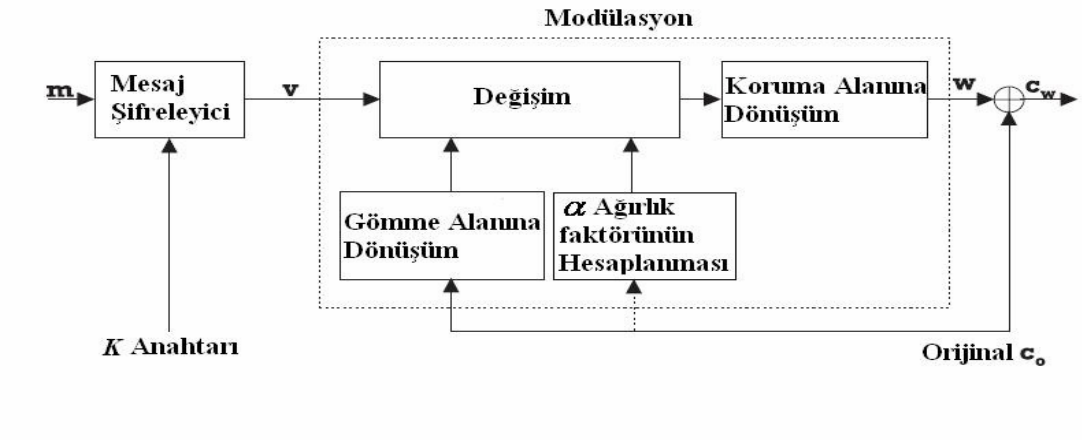
1. Gizli anahtar kullanarak mesajı kodlanmış diziye şifrele

2. Kodlanmış diziyi, koruma nesnesinden ayrı olarak kanala uygun olarak fiziksel tasarıma monte et.

3. Filigranlanmış nesneyi üretmek için modüle edilmiş diziyi koruma nesnesine ekle.

Mevcut sayısal filigranlama sistemlerini sınıflandırmak için, filigran gömücülerin/algılayıcıların temel inşa bloklarını ayrıntılı şekilde incelemek gerekir.

İlk yaklaşımlar Koruma nesnesi c_o'a kanal karakteristiklerini düşünmeden üretilen filigran paternini eklenmesi şeklinde filigran şifreleyicilerine uygulanmıştır. Bu ilk nesilden itibaren yöntemler bazı sezgisel kriterlere dayanarak filigran gömme için gömme alanı içinde önemli bileşenler kümesi tanımlanmıştır (Cox ve ark., 1997). Şekil 2.5'de resmedildiği gibi, bu genellikle önceden seçilmiş taşıyıcı bileşenlerin değişiminin gerçekleştirildiği daha başka sinyal sunumuna dönüşümünü içerir. Yöntemlerin bir kısmı filigranı gömmek için bileşenler olarak zayıftan ortaya kadar frekans aralığını kullanarak fourier domaininde çalışmaktadır (Koch ve Zhao,1995).



Şekil 2.5. Temel filigran gömücü.

Deneyimler sonucunda bilinmelidir ki, gömülmüş filigranın sağlamlığı ile filigranlanmış nesnenin kalitesi arasındaki uzlaşmanın oluşması, algısal önemli bileşenler aracılığıyla olur. İki zıt gereksinim olan algısal görünürlük ve filigran sağlamlık arasında ayarlamayı sağlamak için, ağırlık faktörlerinin α vektörü hesaplanır. En eski algoritmalarda (Cox ve ark., 1997) sırasıyla gömme kuvvetini ve gömülmüş filigranın gücünü kontrol etmek için eşit elemanlı $\alpha = \{\alpha[i]\}_{i=1}^{N}, \alpha[i] = \alpha_{const}, \forall i$ vektörü kullanılmıştır (Şekil 2.6). Koruma nesnesi ve kanalın lokal değişimleri düşünülmeden tüm

ağırlık faktörü kullanılırsa, olası bir aslına uygunluk kaybının oluşacağından, bu tip basit yöntemlerin en belirgin dezavantajı, koruma nesnesi ve gömülmüş filigran arasındaki bağıntıyı kaybetmesidir. Ayrıca, gerçek kapak nesne ile ilgili gömülü filigran sağlamlığının optimizasyonu dikkate alınmaz. Bu açıdan bakıldığında, hem gömme ve hem de algılama yöntemi geliştirmek için özel koruyucu nesneden az bilgi dikkate alınır ya da hiç dikkate alınmaz. Daha gelişmiş algoritmalar algısal eşiklerini ve ilgili α ağırlık vektörünü hesaplamak için koruyucu nesneyi inceleyerek niteliğini optimize ederler (Arnold ve Schilz, 2002). Algısal eşikleri diye adlandırılanlar, farklı medya türleri için algısal modellerden elde edilir (Pan, 1995). Bu bilgi eklenen paterni biçimlendirmek için şifreleyicinin modülasyon bloğunda maksimum kaliteyi sağlamak amacıyla kullanılır. Bu nedenle, eklenen patern koruyucu nesnenin bir fonksiyonudur. Bu yöntemler genelde filigranın sağlamlığı üzerinde etkisini ihmal ederek, kalite amacıyla optimize etmek için algısal eşikleri kullanır.

Kod çözücüleri filigranı elde etmek için iki adım gerçekleştirir:

1. Mesaj paternini elde etmek için, elde edilen sinyal demodule edilir.
2. Gömülü filigranı geri elde etmek amacıyla mesaj paterni kod çözme anahtarı ile kodu çözülür.

Demodülasyon farklı şekillerde yapılabilir. Orijinal nesne dekoder için mevcutsa, alınan gürültülü filigran paternini elde etmek için filigranlanmış nesneyi içeren sinyalden çıkarılabilir.

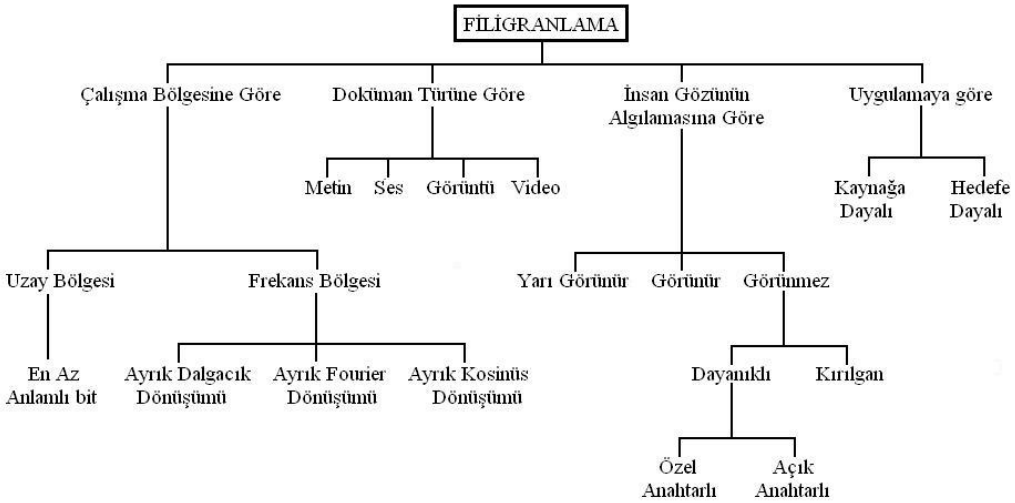
Kör olmayan filigranlama sistemlerinde bu şekilde demodülasyon yapılır. Diğer yaklaşımlar koruyucu nesnenin ilavesinin etkisini dengelemek için veri azaltma fonksiyonlarını kullanırlar. Bu, filigranlanmış nesneden onu çıkarılmadan önce algılama prosedüründe orijinale benzetilmesi ile yapılabilir.

Kod çözme yordamında, filigranın kodlu dizisi $\hat{v}$ dizi çıkarıcı tarafından çıkarılmalıdır; ilk yaklaşımlarda, gömme uzaydaki aynı önceden tanımlanmış taşıyıcı bileşenleri, gömme adımında bunlar gibi dizi okuma için kullanılır. Filigran mesajı $\hat{m}$, filigran mesaj kod çözücüde gizli anahtar vasıtasıyla $\hat{v}$'den çözülür.

2.5.Filigranlama yöntemleri

Günümüze kadar filigranlar ve filigranlama için birçok yöntem geliştirilmiştir. Filigranlar ve filigranlama yöntemleri çalışma bölgesi, doküman türü, insan gözünün algılaması ve uygulamaya göre olmak üzere dört ana kategoride incelenebilir. Her kategori

ayrıca kendi içinde de alt sınıflara ayrılabilmektedir. Buna göre Şekil 2.6.'de sayısal filigranlama kategorileri görülmektedir (Singh, 2011).



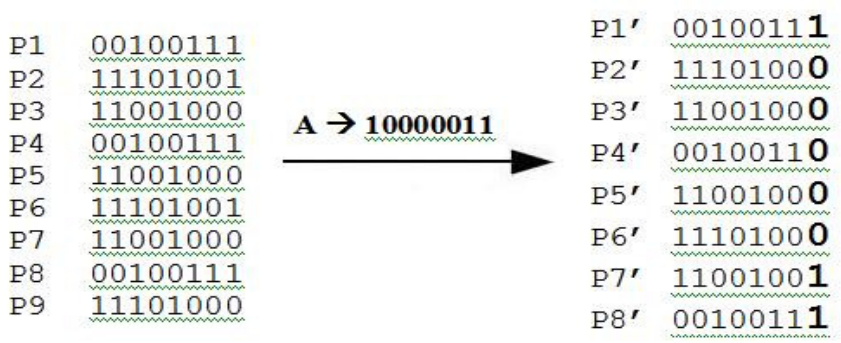
Şekil 2.6. sayısal filigranlama kategorileri.

2.5.1. Çalışma Bölgesine Göre Filigranlama

Filigranın gömülü olduğu bölgeyi dikkate alarak filigranlama yöntemleri iki geniş kategoride sınıflandırılabilir: uzay bölgesi ve frekans bölgesi teknikleri.

2.5.1.1. Uzay Bölgesi Filigranlama

Uzay bölgesi filigranlama teknikleri orijinal görüntünün piksel yoğunluğu değiştirir. En az anlamlı bit (LSB) adı verilen En basit filigranlama tekniği filigranı doğrudan orijinal görüntünün en az öneme sahip bit düzlemine yerleştirilmesidir. En az öneme sahip bitin değiştirilmesi fikri, belirli piksellerin yoğunluğundaki değişim az olduğundan insan görme organı farklılığı algılayamaması prensibine dayalıdır (Şekil 2.7). Uzaysal-bölge tekniklerinin avantajı yüksek algı geçirgenliği ve verimidir. Dezavantajı görüntü işleme ve geometrik dönüşümlere karşı kırılgan olmasıdır.



Şekil 2.7. En az anlamlıbit (LSB) yöntemi ile filigranlama.

2.5.1.1.1. En Az Anlamlı Bit (LSB) Yöntemi

En az anlamlı bit (LSB) şifreleme yöntemi, hemen hemen tüm medya türlerinde, filigranlanma alanında araştırılan ilk tekniklerinden biridir. Bu filigran gürüntüsünden bit paterni ile taşıyıcı sinyalin LSB'sinin yer değişmesine dayanmaktadır. Bitler piksel gibi, belli temsil değerlerine gömülürler. İlgili bitleri gömmek için kullanılan temsil edilen değerlerin bilgisi varsa şifre çözme sırasında filigran tekrar elde edilebilir.

Filigran şifreleyici, tüm c_o taşıyıcı elemanları gizli anahtar tarafından seçilen $c_{oj}[1],...,c_{oj}\left[l\left(c_{oj}\right)\right]^5$ altkümesini kullanır. LSB'lerdeki $c_{oj}[i] \rightleftarrows m[i]$ yer değişme işlemi bu altküme üzerinde gerçekleştirilir. Bu nedenle, şifre çözücü gömme işlemi sırasında kullanılan tüm taşıyıcı elemanlara ihtiyaç duyar. Genellikle $l(c_o) \gg l(m)$ olduğundan, sağlamlık filigranın tekrarlanarak gömülmesiyle geliştirilebilir. LSB'nin gömülmesi için elemanların rastgele seçilmesi ve değiştirilmesi düşük güç ve sabit bir güç yoğunluklu gürültü üretir. Bu gürültünün algılanması orijinal taşıyıcı nesnenin algısal eşiğine ve dolayısıyla içeriğine bağlıdır (Arnold ve ark., 2003).

LSB'lerin rastgele değişiklikleri kodlanmış filigranı yok etmesi nedeniyle ana dezavantaj olarak içerisinde düşük sağlamlık yatıyorsa da bu yöntemin en büyük avantajı, yüksek yük taşımasıdır. Bu, örneğin, son derece LSB kodlanmış filigranı bir dijital-analog ve mütakiben analog-dijital dönüşüm yaşaması pek olası değildir. LSB yöntemlerin karakteristikleri steganografik senaryolara uygulanabilirliğini sınırlar ve tamamen dijital ortam gerektirir.

2.5.2. Frekans Bölgesi Filigranlama

Frekans Bölgesi filigranlama tekniği, ayrık kosinüs dönüşümü (DCT) (Cox ve ark., 1997; Hsu ve Wu, 1999; Niu ve ark., 2000), ayrık dalgacık dönüşümü (DWT) (Hsu ve Wu,1998; Lu ve ark., 2000) veya Ayrık Fourier Dönüşümü (DFT)'nde olduğu gibi dönüşüm bölgesindeki katsayıların genliğini düzenleyerek filigranı gömer. Uzaysal-bölge tekniğinden farklı olarak frekans-bölge tekniğinde farklı görüntü saldırılarına karşı sağlam ve dayanıklıdır ama daha çok hesaplamaya dayalı ek yük kaçınılmazdır. Bu dayanıklılık dikkate alınarak, kabul edilebilir hesaplama karmaşıklığı altında açık anahtar şifreleme ile birlikte çalışan frekans-bölge yöntemi uyarladık.

2.5.3. Doküman Türüne Göre Filigranlama

2.5.3.1. Video Filigranlama

Video filigranlama, normal görüntü filigranlamanın bir üst kümesi olarak düşünülebilir. Bu nedenle, statik görüntülere uygalanabilen teknikler, video görüntülerine uygulanabilir. Ancak, videonun yüksek kare hızı nedeniyle, gömme işlemi canlı yayınlar için hemen hemen gerçek zamanlı olarak gerçekleşmesi gerekir (filigranı gömmek belli bir zaman alacağından bu yayın hızını etkileyebilir). İçerik çevrimdışı oluşturulur ise, bu sınırlama ortadan kalkar. Canlı video filigranlamanın en yaygın biçimi, görünür filigran kullanımıdır. Normalde bir logo veya diğer ayırt edici işareti her bir video çerçevesi üzerinde dikkat çekmeyen bir yere yerleştirilir.

2.5.3.2. Metin Filigranlama

Metin, ham formatlanmamış ASCII metin ve biçimlendirilmiş metin olmak üzere iki kategoriye ayrılır.

Filigran bilgisi satır arası ve kelime arası boşlukların ayarlanmasına dayalı bir yaklaşım kullanılarak biçimlendirilmiş belgeye gömülebilir. Filigran gömmek için başka bir yaklaşım, karakter dizisi bir büyük görüntü olarak kabul edilerek görüntü için kullanılan tipik yaklaşımlar kullanmaktır.

Ham metin, filigran işlemi için büyük bir sorun oluşturur. Şu an için hiçbir başarılı yaklaşımı bilinmemektedir. Tek uygulanabilir yaklaşım her cümleden sonra boşluk karakterlerini ekleyeme dayanmaktadır. Ancak, bu yaklaşım kolayca normal bir metin editörü kullanarak atlanır.

2.5.4. Algılanabilirliğe Göre Sınıflandırma

Filigranlama yöntemleri algılanabilirliğe göre görünür, yarı görünür ve görünmez filigranlama yöntemleri olarak sınıflandırılabilir.

2.5.4.1. Görünür Filigranlama

Görünür Filigranlama, filigranın görülebilir şekilde görüntüye yerleştirilmesidir. Direk olarak uygulandığından dolayı kolay ve hızlı olmasına rağmen, asıl görüntü kalitesini azaltır ve saldırılara karşı kırılabilir. Görünür filigranlar, görüntü veya video filigranlama alanında logo veya kaplama görüntüleri olabilir. Bilginin örtük lokalizasyonu nedeniyle, bu filigran sağlam değildir.

2.5.4.2. Görünmez Filigranlama

Görünmez filigranlama görüntü içerisine gözle algılanamayacak bir şekilde filigranı yerleştirme işlemine denir. İnsan görsel algılama sisteminin özellikleri temel alınarak tasarlandığından asıl görüntü kalitesini azaltmaz. Bu yöntem ile filigranlanan görüntülerde filigran, görüntü içine hak sahibi tarafından bilinen bir algoritma ile gömülerek dağıtılır ve geri elde edilir. Filigranın görüntü içindeki yeri belli olmadığından kırpma saldırılarına karşı dayanıklıdır. Filigranlama algoritmaları sadece hak sahibi tarafından bilindiğinden yetkisi olmayan kişilerin filigrana ulaşmaları zordur. Görünmez filigranlama yöntemleri kendi içinde “dayanıklı” ve “kırılgan” olmak üzere ikiye ayrılır.

2.5.4.2.1. Dayanıklı Filigranlama

Dayanıklı Filigranlama, filigranlanmış görüntünün çeşitli görüntü işleme saldırılarına karşı dayanıklı olduğu ve filigranın tekrar elde edildiğinde tanınabilir olduğu filigranlama yöntemidir. Bu yöntem, filigranlanmış görüntünün heterojen manipülasyonlara karşı dayanması için tasarlanmıştır; filigranlama sistemlerinin güvenlik varsayımından yola çıkan bütün uygulamaları bu tür filigran gerektirir. Dayanıklı filigranlama yöntemleri kullanılan anahtarın bilinip bilinmemesine göre “açık” ve “gizli” filigranlama olarak ikiye ayrılılır.

2.5.4.2.1.1. Açık ve Gizli Anahtarlı Filigranlama

Açık ve gizli anahtarlı filigranlamada filigranlar, filigranı gömmek ve almak amacıyla kullanılan anahtar için gizlilik gereksinimlerine bağlı olarak ayrılmıştır. Filigranlamanın temel prensiplerine göre, kodlama ve kod çözme sürecinde aynı anahtar

kullanılır. Anahtar biliniyorsa, filigranın bu türü açık anahtarlı olarak ve anahtar gizliyse, gizli anahtarlı filigranlar olarak adlandırılırlar. Açık anahtarlı filigranlar güvenlikle ilgili gereksinimlerin olmadığı (örneğin, meta bilgilerini gömmek için) uygulamalarda kullanılabilir.

Geçmiş yıllarda önerilen filigranlama teknikleri gömme ve çıkarma için aynı gizli anahtarı kullanan özel filigranlama yöntemleridir. Ana avantajı ilgili gizli anahtar olmaksızın gömülen filigranın silinmesinin zor olmasıdır. Maalesef ki test görüntüsündeki filigranın varlığı ispat edildiği zaman gizli anahtar ortaya çıkmaktadır. Filigran doğrulandığında gizli anahtar devre dışı bırakılmalıdır çünkü yayınlanan bilgi gizli anahtarı ortaya çıkarmak için yeterlidir. Bu zayıflığı ortadan kaldırmak için hak sahibi farklı gizli anahtarlar kullanarak aynı orijinal görüntüye filigranlar gömmek zorundadır. Birçok filigran ve ilgili gizli anahtarları yönetmek oldukça zordur. Taklit/ortalama saldırıları bu tip sistemler için mümkün olabilmektedir. Bununla beraber bu eksiklikler sayısal filigranlama yöntemi içerisine açık anahtar şifreleme dahil edilerek giderilebilmektedir. Son zamanlarda açık anahtar filigranlama yöntemleri sayısal filigranlama alanında kayda değer ilgi görmektedir. İsminden de anlaşılacağı gibi filigran özel anahtar kullanılarak gömülür ve ardından ilgili açık anahtar kullanılarak çıkartılır. Açık anahtar filigranlama yöntemi oldukça pratiktir herkes hak sahibine danışmadan filigranın varlığını doğrulayabilir ve hiç kimse özel anahtar olmaksızın filigranı silemez.

2.5.4.2.2. Kırılgan Filigranlama

Kırılgan Filigranlama, Filigranlanmış görüntünün çeşitli görüntü işleme saldırılarına karşı dayanıksız olduğu filigranlama yöntemidir. Kırılgan filigranlar çok düşük sağlamlık ile gömülürler. Bu nedenle, bu tip filigranlar ufak manipülasyonlar tarafından bile yok edilebilirler. Bu anlamda o steganografik yöntemler içindeki gizli mesajları karşılaştırabilirler. Nesnelerin bütünlüğünü kontrol etmek için kullanılabilirler.

2.5.4.3. Yarı Görünür Filigranlama

Görünür ya da görünmez filigranlama ile birlikte üçüncü yöntem olan yarı görünür filigranlama, filigranın görüntünün büyük bir bölümü üzerine yarı saydam olarak eklenmesidir. Bu yöntemle eklenen filigranın görüntüden ayrılması, görüntüyü anlamsız kılacağından avantajlıdır. Ancak görüntüyü kullanıcıya bu şekilde sunmak bir dezavantajdır (Oğuz, 2006).

2.5.5. Uygulamaya Göre Filigranlama

2.5.5.1. Kaynak Tabanlı Filigranlama

Kaynak tabanlı filigranlama, haksahipiğini belirleme ve kanıtlamak için belirli bir görüntünün dağıtılan tüm kopyalarına, hak sahibini tanıtan benzersiz filigranın gömülmesiyle elde edilir. Kaynak tabanlı filigran tekrar elde edilen görüntü veya diğer elektronik verinin değiştirilip değiştirilmediği belirleme ve kimlik doğrulama için kullanılabilir.

2.5.5.2.Hedef Tabanlı Filigranlama

Hedef tabanlı filigranlama ise, her dağıtılan kopyaya alıcıyı tanımlayan benzersiz bir filigran eklenerek elde edilen filigranlamadır. Hedef tabanlı filigranlama yasadışı tekrardan satış durumlarına karşı alıyıcıyı izlemek için kullanılabilir.

2.6. Filigranlama Yöntemlerinin Temel Özellikleri

Telif hakları korumanın gerçekleştirilebilmesi için filigranlama yönteminin sahip olması gereken temel özellikler aşağıda özetlenmiştir:

2.6.1 Saydamlık

Filigranlanan görüntü algısal olarak görünmemeli ve görüntüyü bozmamalıdır. Filigranlanmış görüntünün kalitesi çok az kayıp veya hiç kayıpsız olmalıdır. Kayıpsız filigranlama yöntemi özelikle medikal görüntülere uyarlanır. Sanatçılar hiç bozulmama olmasında ısrar edeceklerinden kayıpsız filigranlama yöntemi iyi bir çözümdür.

2.6.2 Sağlamlık

Bulandırma, JPEG sıkıştırma, gürültüleme, keskinleştirme, ölçekleme, kesme ve yazdırma-kopyalama-tarama gibi yaygın sinyal işleme ve geometrik bozulmalar sonrasında filigran tekrar elde edilmelidir. Başka bir değişle, bozulan görüntünün kalitesinin kabul edilebilir varsayımı altında filigran silme saldırılarına karşı dayanıklı olmalıdır. Bunlara ek olarak filigranlama yöntemini değerlendirmek için StirMark ve unZign iki güçlü değerlendirme testidir (Lu ve ark., 2000; Petitcolas ve ark., 1999). Genellikle filigranlama yöntemleri StirMark ve unZign saldırılarına dayanamazsa kolaylıkla kırıldığı kabul edilir.

2.6.3. Güvenlik

Kerckhoff prensibine göre, bir şifre sisteminin güvenliği şifre algoritmasının gizli tutulmasına bağlı olmamalıdır (Schneier, 1996). Güvenlik sadece anahtarın gizli tutulmasına bağlı olmalıdır. Benzer olarak gömülmüş filigran silinemezken filigran algoritması açık olmalıdır.

2.6.4. Körlük

Test görüntüsündeki filigranın varlığının doğrulanması için orijinal görüntünün kullanılmasına gerek yoktur. Yani telif hakları sahibi orijinal görüntüleri korumak için ekstra disk alanı ayırmak zorunluluğunda değildir. Kör filigranlama özelliği pratikte zorunludur.

2.6.5. Çoklu Filigranlama

Bu yöntem, sayısal görüntünün dağıtımının takibi için önemli bir tekniktir. Bununla beraber çoklu filigranlama yönteminde öndeki filigranın üzerine sonraki filigranı geçirmekten kaçınılmalıdır. Gelişmiş filigranlama yöntemi bu zayıflığın üstesinden gelmelidir.

2.6.6. Belirlilik

Filigranlama tekniği görüntünün sahibini doğruca ve açıkça doğrulamalıdır. Claver ve ark. (1997), çoklu hak sahipliği iddiası probleminde (kilitleme problemi, taklit saldırı veya terslenebilir saldırıda) olduğu gibi bir korsanın filigranlanmış görüntüye legal olmayan filigran ekleyerek hak sahipliğini belirsizleştirebileceğini iddia etmiştir.

Günümüzde önerilen yöntemlerin hemen hemen hepsi yukarıdaki gereksinimleri aynı anda karşılayamamaktadır, özelikle döndürmeye, kesmeye ve yazdırma-kopyalama-taramaya dirençlidir. Gerçekte saydamlık ve sağlamlık özellikle çoğu önerilen filigranlama yöntemlerinde birbirine muhalefet eden gereksinimlerdir. Çoklu filigranlama yöntemi ve taklit saldırısı önerilen filigranlama yöntemlerinin hemen hemen hepsi için zorluk oluşturmaktadır.

Cox ve ark. (1997)'da ikili filigran dizisi, en büyük değerdeki DCT katsayılarının içerisine gömülmüştür. Böylece bu yöntem görüntü işleme ve yaygın geometrik dönüşümlere karşı sağlamdır. Hsu ve Wu (1998, 1999) orta-frekans katsayılarını düzenleyerek ikili filigranı gömmek için ayrık kosinüs/parçacık dönüşüm yöntemlerini önermişlerdir. Bu yöntem yaygın görüntü işlemeye karşı dayanıklıdır fakat geometrik

bozulmalara karşı hala zayıftır. Cox ve ark. (1997) ve Hsu ve Wu (1998,1999)'nun ana zayıflıkları filigranı tespit etmek ve çıkarmak için orijinal görüntüye ihtiyaç duymasıdır. Diğer problem çoklu filigranların bu yöntemlere uygun olmamasıdır. Chang ve ark. (1999), durağan görüntünün telif haklarını koruması için özgün yöntemler önermişlerdir. Filigranlamış görüntü orijinal ile aynıdır. Filigranı çıkarmak için orijinal görüntüye ihtiyaç yoktur. Çoklu filigranlama tekniklerinin mümkün olması ve taklit/ortalama saldırılarından sakınılabilmesi bahsedilmesi gereken önemli noktalardır. Maalesef ki, döndürme, yazdırma-kopyalama-tarama gibi bazı geometrik bozulmalar üstesinden gelinmesi gereken zorluklardır.

Lu ve ark. (2000)'da ve Niu ve ark. (2000)'da iki gri düzeyi sayısal filigranlama teknolojisi önermiştir. Niu ve ark. (2000)'da gözle görülür biçimde tanınabilir örnek sekiz ikili bit düzlemine ayrıştırılmıştır. Kalanları gizli anahtar olarak kullanılmak üzere, bazı ikili bit düzlemleri orijinal görüntünün orta DCT bileşenlerinin içerisine gömülmüştür. Bu özel filigranlama yönteminin ana dezavantajları: (1) filigranın varlığını doğrulamak için orijinal görüntü gereklidir; (2) sağlamlık özelliği JPEG sıkıştırmaya ve genel görüntü işlemeye karşı dayanıklıdır, fakat geometrik bozulmalar hala zorluk oluşturmaktadır; (3) çoklu filigranlama için uygun değildir. Lu ve ark. (2000)'da ortak görüntü işleme için verimli dayanıklı olan başka sağlamlık gri düzeyi filigranlama yöntemi önermişlerdir. İlk olarak original görüntü ve gri düzey filigran aynı boyuttadır ve her ikisi eş zamanlı olarak DWT tarafından dönüştürülürler. Sonra filigran daha büyük katsayıların içine gömülür. Filigranı gömmek için değişiklik genliklerine karar vermek için açık bozulma sunulmuştur. Bu filigranlama yönteminde filigranın varlığını doğrulamak için orijinal görüntü gerekli değildir ama gizli görüntüyü korumak için gereklidir. Bu yöntemin Stirmark ve unZign saldırılarında hayatta kalabildiğini belirtmekte fayda vardır. Bununla birlikte bazı zayıflıkları vardır: (1) gizli anahtar örneğin gizli görüntü, gri düzey filigran ile aynı boyuttadır; (2) küçük açılı döndürme, kesme ve yazdırma-kopyalama-tarama gibi geometrik bozulmalardan kolayca zarar görebilir; (3) çoklu filigranlama için uygun değildir.

Gizli anahtar, özel filigranlama yöntemlerinde genel bir zorluk olan doğrulama evresinde açığa çıkar.

Günümüzde, sayısal ortamları telif hakkı koruması için sayısal filigranlama teknolojisi iyi bir adaydır. Ne yazık ki, taklit saldırılar, kopya saldırılar gibi bazı saldırılar önerilen filigranlama yöntemlerinin sağlamlık özelliği için hala zorluk oluşturmaktadır. Şifrelemeyle ilgili araçlar, bozulmalara izin veren veriler için uygun olmamalarına rağmen,

iyi tanımlanmış güvenlik servislerinin sağlanması için en iyi araçlardır (Wei-bin ve ark., 2002).

2.7. Önerilen Yöntemin Özellikleri

Bu tezde önerilen yöntemin özellikleri aşağıdadır:

2.7.1. Gri Seviye Logo Görüntü

Çoğu filigranlama yöntemleri filigran olarak ikili sıra veya görüntüler kullanmaktadır ama çoğu logolar (ticari markalar) pratikte gri düzey kullanmaktadırlar. Çeşitli saldırılara karşı gri düzey filigranın ikili filigrana göre hayatta kalma şansı çok yüksektir (Lu ve ark., 2000). Maalesef iyi bilinmektedir ki, gri seviye filigranı orijinal görüntüye gömmek genellikle daha şiddetli bozulmalar olarak tanıtılmaktadır. Bu yüksek kalitedeki görüntü ve bozulmasız uygulamalar için çok büyük bir sakıncadır.

2.7.2. İnanç

Görmek inanmaktır. Güncel filigran algılama metotları insanların tüm ihtiyaçlarını tamamen karşılayamamaktadır. Filigran pratikte belirli uygulamalarda tanınabilir örnek olarak işlem görmeli ve gözlemci çıkarılmış filigran için açıkça hüküm verebilmelidir.

2.7.3. Genel Doğrulama

Herkes telif hakkı logolarının varlığını kendi kendine doğrulayabilmeli ama silememeli veya bozamamalı. Bu yöntem filigran doğrulama için hak sahiplerinin genel giderlerini azaltabileceğini işaret etmektedir.

2.7.4. Kasti Saldırılar

Sağlamlık gereklidir ama güvenliği garanti etmek için yeterli değildir (Craver ve ark., 1998). Şifreleme sistemlerinde, filigranlamanın çıkarma safhasında herhangi bir saldırgan filigranların varlığına karşı gelebilirse saldırılar başarılı olarak nitelendirilir. Çalışmada kullanılan yöntem taklit saldırısı, taklit/ortalama saldırısı ve kopya saldırısına karşı dayanabilmektedir (Kutter ve ark., 2000).

2.7.5. StirMark Saldırısı Ve UnZign Saldırısı

Stirmark saldırısı saldırıya uğramış filigranlanmış görüntü orijinal filigranlanmış görüntüye algısal olarak çok yakın olduğu rastgele lokal/global geometrik bozulmaları

sunar. Bununla birlikte, saldırıya uğramış görüntü büyük bozulmalara uğrar. UnZign saldırısı lokal piksel sapmasını sunar ve çoğu filigranlama yöntemlerine saldırmada çok verimlidir.

BÖLÜM 3

MATERYAL VE YÖNTEM

3.1. Giriş

Bu bölümde, sayısal gri seviye görüntülerin filigranlanması amacıyla önerilen bir filigranlama yöntemi ayrıntılarıyla anlatılmaktadır. Filigranlama yönteminin geliştirilmesinde kullanılan araçlar 'Materyal' alt baslığı altında yer almaktadır. Görüntünün filigranlanması ve filigranın tekrar elde edilme yönteminin yapısı ile çalışması hakkında ayrıntılı bilgi 'Yöntem' alt başlığı altında ele alınmıştır.

3.2. Materyal

Bu tez çalışmasında bilgisayar ortamına aktarılan sayısal gri seviye görüntülerin filigranlanması ve filigranın çıkarılması amacıyla geliştirilen yöntem için bir bilgisayar yazılımı hazırlanmıştır. Yazılım Windows® XP Service Pack 3 işletim sistemi üzerinde yapılmıştır. Önerilen algoritmanın tasarımında ve kodlamasında, Matlab yüksek seviyeli teknik programlama dili kullanılmıştır. Önerilen algoritma Stirmark Benchmark 4.0.129 proğramı kullanılarak test edilmiştir. Yazılımın hazırlandığı ve testlerin yapıldığı bilgisayar, Intel®Core™ 2 Duo CPU @ 2.20 GHz islemcili, üzerinde 3 GByte RAM ve 256 MB ekran kartı bulunan bir masaüstü bilgisayardır.

Önerilen filigranlama yönteminin testleri için kullanılan filigran, Sekil 4.1.'de görülen 64×64 piksel boyutlarındaki gri seviye logo görüntüsüdür. Bu filigran, 512×512 piksel boyutlarındaki Lena, Baboon, Barbara, Peppers resimlerine gömülmüştür (Sekil 4.2.'de).

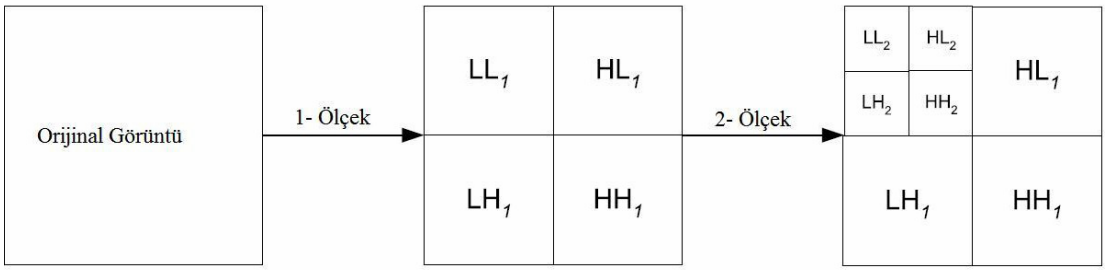
Şekil 3.1. 64×64 Piksel boyutundaki gri seviye logo görüntüsü.

Şekil 3.2. 512×512 piksellik görüntüler: (a) Lena, (b) Barbara, (c) Baboon, (d) Peppers.

3.3 .Ön Hazırlıklar

3.3.1. Dalgacık Dönüşümü

Dalgacık dönüşümü ayrıştırma için matematiksel bir araçtır (Shapiro, 1993; Stollnitz ve ark., 1995; Wang ve Kuo, 1997). 2- ölçek dalgacık dönüşümü Şekil 3.3'de gösterildiği gibi DWT modelini kısaca özetleyebiliriz. Resim ilk olarak LL_1, LH_1, HL_1 ve HH_1 ile gösterilen 4 alt banda ayrıştırılır. LH_1, HL_1 ve HH_1 en detaylı ölçeklenme dalgacık katsayılarını, yani yüksek frekanslı detaylandırılmış bilgiyi içerir. Tüm şeklin kaba bir örneği olan LL_1, resmin içerisindeki en çok enerjinin olduğu düşük frekanslı bileşendir. LL_1 i, LL_2, LH_2, HL_2 ve HH_2 daha kaba parçalarına ayırarak dalgacık dönüşümünü tekrar uygular. Bu işlem t defa tekrarlandığında t-ölçek seviyeli dalgacık dönüşümü olan LL_t alt bandı elde edilebilir.



Şekil 3.3. Görüntünün 2-ölçek dalgacık dönüşümü ile 7 altbanda bölünmesi.

Şekil 3.4. Lena Görüntüsünün 2-ölçek dalgacık dönüşümü ile 7 altbanda bölünmesi.

İnsanın görsel sistemi, yüksek frekans bileşenlerinden ziyade düşük frekans bileşenleri daha hassastır. Makul saldırılar altında düşük frekanslı bileşenler, yaşamına devam edebilir. Sonuç olarak orijinal görüntünün LL_t'si değiştirilmiş görüntüye çok benzerdir (Şekil 3.4).

3.3.2. Vektör Kuantizasyonu

Vektör kuantizasyon gerekli ve güçlü kayıplı görüntü sıkıştırma metodudur. Yıllar boyunca yapılan birçok araştırmada vektör kuantizasyon görüntü taşıması, sıkıştırılması ve işlemesi içerisinde kullanılmıştır (Chan ve Jan, 1998).

Desen tanımanın formu olarak tanımlanan Vektör kuantizasyonda görüntü, bazı eşleştirme kriterleri temel alınarak kod kitabının üyeleri olan girdidir. Kod kitabının bir

üyesi kod kelimesi olarak adlandırılır. Her bir kod kelimesi indekslenir. Vektör kuantizasyon temel yapısı şifreleme ve şifre çözme üyelerini içerir.

Şifreleme aşamasında, her bir girdi görüntü vektörü için kod kitabındaki en uygun eşleşen kod kelimeleri belirlenmelidir. Her bir blok bağımsız olarak şifrelenmeli ve Kod kitabının içindeki ilgili kod kelimelerine karşılıklı gelen indeksler kaydedilir. *I* indeks kümesi elde edilebilir ve şifre çözücüye gönderilebilir.

Şifre çözme aşamasında şifre çözücü, şifreleyiciden elde edilen indeks kümesine göre görüntüyü tekrar inşa etmek için aynı kitap koduna sahip olmalıdır. Her bir indeks ilgili kod kelimeleriyle değiştirilir. Tüm girdi indeksleri değiştirildikten sonra; Vektör kuantizasyon şifre çözücüsü şifrelenmiş görüntüyü tekrar inşa edebilir.

3.3.3. Sayısal İmza Ve Sayısal Zaman Mühürleme

Telif hakkı ve patent içeren bir anlaşmazlıkta eğer 2 kişi hak sahipliği iddiasında bulunursa noter, gerçek hak sahibinin kim olduğunu nasıl doğrulayacaktır? Tabi ki, anlaşmazlık olan işten en erken kopyasını üreten kişi davayı kazanır. Adalet, zaman mühürleme ve sayısal imza gibi iki iyi tanımlanmış güvenlik servisi kullanılarak sağlanabilir.

Zaman mühürleme, sayısal verinin belirli bir zamanda oluşturulduğunun veya imzalandığının doğrulaması amacıyla kullanılan bir tekniktir. Diğer taraftan sayısal imza, imzalanmış veri ve imzalayanın kişisel anahtarını temel alan bilginin bir parçasıdır. Bu yolla herhangi biri imzalayanın açık anahtarına erişerek imzanın doğruluğunu kontrol edebilir (Schneier, 1996).

Kısaca sayısal imza, veri oluşturulduğunda, hak sahibi yazar ve sayısal zaman mührünü tanımlamak için bir çözümdür. Bundan dolayı patent almak istediğiniz bir şeyi korumak için sayısal imza ve sayısal zaman mührünün kombinasyonu etkili bir çözüm sağlar. Çünkü bilgisayarda gün ve saat kolaylıkla değiştirilebildiğinden, zaman mührü teknolojisi güvenilir sertifika otoritesi (CA) tarafından yapılmıştır. Ancak görüntü, ses ve video gibi çoğu sayısal veri, kolay kopyalama ve makul bozulmaya izin verme karakteristiklerine sahiptir. Bir korsan orijinal sayısal veriyi tek başına insan duygularıyla algılamanın imkansız olacağı şekilde değiştirmek için bu karakteristikleri kullanabilir ve o sayısal verinin hak sahipliği iddiasında bulunabilir. Makul bozulmalar insan gözüyle fark edilmez ama güvenlik servis doğrulama araçlarında başarısız olur. Bu servisler içerikten ziyade bit katarına hassas olduklarından bir sayısal filigranlama şeması içindeki şifreleme araçlarına sokmak büyük zorluk oluşturur.

3.3.4. StirMark Benchmark

StirMark saldırı yöntemi Cambridge Üniversitesi'nde bir araştırma grubu tarafından tasarlanmış, filigranlama algoritmalarının sağlamlığını test etmek için kullanılan güçlü bir yöntemdir (Petitcolas ve ark., 1999). Bu yöntem Sinyal arttırma, sıkıştırma, ölçekleme, kırpma, döndürme, kıvrım filtrelemesi, geometrik dönüştürme ve görüntüyü geometrik olarak rastgele bozma işlemlerinden oluşmaktadır. İlk versiyonu Kasım1997 yılında yayınlanmıştır.

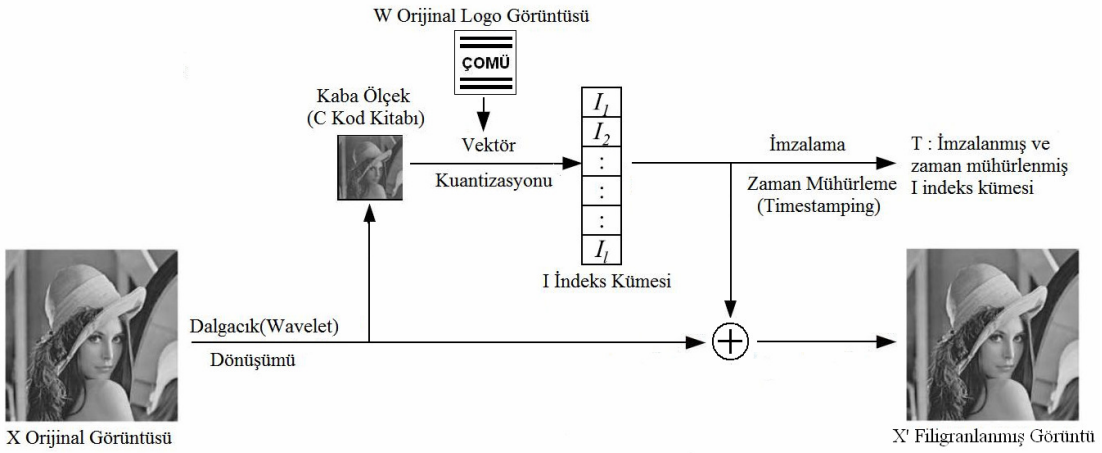
3.4. Yöntem

Her ne kadar alçak frekans bileşenleri makul saldırılardan sonra hayatta kalabilseler de insan gözüyle algılanmaktadırlar. Bu sebepten çoğu frekans-bölge filigranlama yöntemleri, filigranı orta-seviye frekans içine yerleştirmeye çalışır. Ancak, daha alçak frekans bileşenlerinin önemli saldırılar altında hayatta kalması filigran güvenliği için iyi bir özelliktir. Bu yüzden alçak frekans bileşen özellik katsayılarına uygulandı.

Önerilen yeri sağlam telif hakları koruma yöntemi kayıpsız bozulma ve sağlamlık avantajlarına sahiptir. Bu yöntem için safhalar, gömme safhası ve açma safhası olarak gruplandırılabilir.

3.4.1. Sertifika Üretme Algoritması

Gömme aşaması Şekil 3.5'de gösterilmektedir. Algoritmayı ayrıntılı olarak aşağıda açıklayacağız.



Şekil 3.5. Haksahibi ve CA tarafından sertifika ve filigranlanmış görüntü üretilmesi.

Orijinal görüntü ve logo görüntüsünü her pikselde 8 bit olacak şekilde gri-seviye görüntü olarak kabul edelim. *X* orijinal görüntüsü ve *W* logo görüntüsü aşağıda tanımlanmıştır:

$$X = \{x_{i,j} \mid 0 \le x_{i,j} \le 255, \quad 0 \le i < W_X, \quad 0 \le j < H_X\}, \tag{3.1}$$

W_x ve H_x sırayla *X*'in genişliği ve yüksekliğidir.

$$W = \{w_{m,n} \mid 0 \le w_{m,n} \le 255, \quad 0 \le m < W_W, \quad 0 \le n < H_W\}, \tag{3.2}$$

W_w ve H_w sırayla *W*'in genişliği ve yüksekliğidir. Genellemeyi bozmadan, çalışmamızda W_x, H_x, W_w ve H_w için sayısal değerler 2'nin kuvvetleri olarak alınacaktır.

3.4.1.1. Adım 1. Orijinal Görüntünün Dalgacık Dönüşümü

Dalgacık dönüşüm safhasında, orijinal giri-seviye görüntünün *t*-ölçek ayrıştığını ve LL_t'nin elde edildiğini kabul edelim. Burada *t* önceden belirlenmiş bir sabittir. Hak sahibi verimlilik ve sağlamlık arasında bir seçim yapmasına bağlı olarak *t* değerini belirleyebilir. Kaba bütün şeklin boyutu örneğin LL_t (kısaca *L*) altbandı için W_L ve H_L değerleri,

$$W_L = \frac{W_X}{2^t} \quad \text{ve} \quad H_L = \frac{H_X}{2^t} \text{ ' dir.} \tag{3.3}$$

Burada *L* aşağıdaki gibi tanımlanmıştır

$$L = \{l_{i,j} \mid 0 \le l_{i,j} \le 255, \quad 0 \le i < W_L, \quad 0 \le j < H_L\} \tag{3.4}$$

3.4.1.2. Adım 2. Vektör Kuantizasyonu Yoluyla İndeksleri Elde Etme

Vektör kuantizasyon şifreleme safhasında, *L*'yi kod kitabı *C* ve c_q'nin *q*'nuncu kod kelimesi olarak alalım. Böylece $C = \{c_q, q = 1,2,..,k\}$ olur. Burada kod kelimesinin boyutu n pikseldir ve kod kitabındaki kod kelime sayısı *k* aşağıdaki gibi tanımlanır.

$$k = \frac{W_L \times H_L}{n} \tag{3.5}$$

Logo görüntüsü *n* piksellik aynı kod kelimesi boyutuyla *l* adet birbiriyle örtüşmeyen alt-kare bloklarına(vektörlerine) parçalanır. m_p, *p*'ninci vektörü ifade ettiği kabul edilirse,

$$W = \{m_p, \quad p = 1,2,...,l\} \tag{3.6}$$

Şifreleme işlemi sırasında, her bir $m_p = (m_{p1}, m_{p2}, ..., m_{pn})$ vektörü için, *i* indeksini bulmak

için $1 \le i \le k$ aralığında $c_i = (c_{i1}, c_{i2}, ..., c_{in})$ olmak üzere, minimum

$$D(m_p, c_i) = \sum_{r=1}^{n} (m_{pr} - c_{ir})^2 \tag{3.7}$$

değeri hesaplanır. Sonuç olarak, *i* indeksini I_p olarak kaydedersek indeks kümesi $I=\{I_p, p=1,2,3...,l\}$ elde edilir.

3.4.1.3. Adım 3. İndeks Kümesinin Sayısal İmzalanması ve Zaman Mühürlenmesi

I indeks kümesi hak sahibi tarafından sayısal imzalama tekniğiyle imzalanır ve $Sign_{OprivateK}()$'nin hak sahibinin özel anahtarı OprivateK'yi kullanan sayısal imzalama şemasını ifade etmesi suretiyle, $S = Sign_{OprivateK}(I)$ elde edilir. Hak sahibi *S*'yi güvenli CA'ya iletir. CA kendisine iletilene tarih ve zamanı ekleyerek sayısal olarak zaman mühürler ve $TSign_{CAprivateK}()$ 'nın CA tarafından özel anahtar *CAprivateK* ile kullanılan zaman mühürleme teknolojisini ifade etmesi suretiyle $T = TSign_{CAprivateK}(S)$ elde edilir(Wei-Bin ve ark., 2002). Bu yöntem indeks kümesini değişimden korur ve herkes test görüntüsüne ilişkin telif hakkı logosunu doğrulamak için bunu kullanabilir.

CA tarafından zaman mühürlenmesi ücrete tabi olduğundan, Algoritmanın zaman mühürlenmesi kısmı isteğe bağlı daha sonradan eklenebilir. Ancak istenildiği takdirde zaman mühürlenmesi CA'ya ücret ödenerek yapılabildiğini unutmayalım. İndeks kümesi *X* orijinal görüntüsüne gömülerek filigranlama işlemi yapılmıştır.

3.4.1.3. Adım 4. İndeks Kümesinin Filigranlanması

İndeks kümesinin filigranlaması, *X* orijinal görüntüsünün *y*-ölçek alt bandına dalgacık dönüşümüyle ayrılarak elde edilen LL_y'ye ağırlıklandırılmış İndeks kümesi kümesi eklenerek gerçekleştirilir (Pan ve Ark., 2004; Seitz, 2005). İndeks kümesinin filigranlaması işleminin matematiksel gösterimi denklem 3.8'de görülmektedir.

$$LL_y = LL_y + k * I \tag{3.8}$$

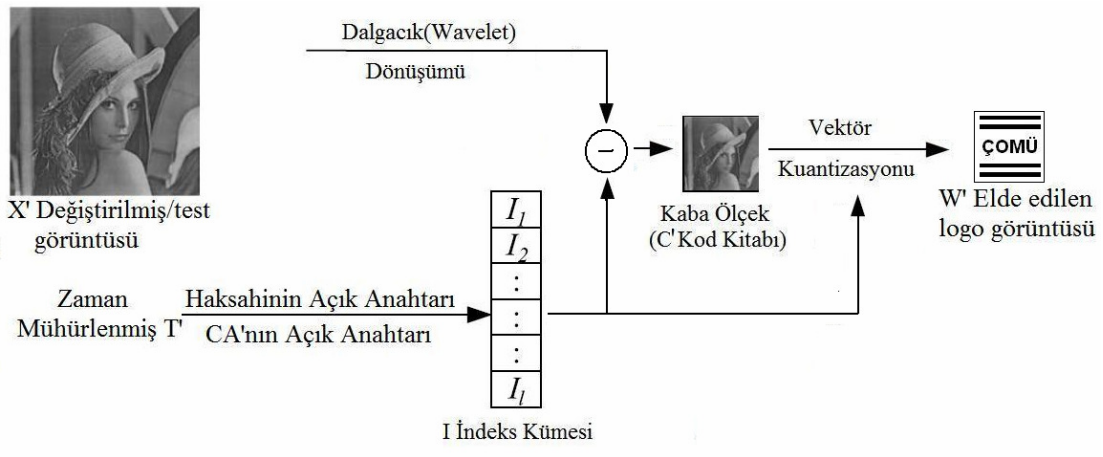
k ağırlıklandırma katsayısının bilinmesi koşuluyla değiştirilmiş görüntüden Orijinal görüntü elde edilebilir.

3.4.2. Doğrulama Algoritması

Bundan sonra doğrulama aşamasında alıcı logo görüntüsünün ne zaman elde

edildiğini doğrulamak için CA'nın açık anahtarını kullanabilir ve hak sahibinin açık anahtarını kullanarak *I* indeks kümesinin bütünlüğünü doğrular. Şekil 3.6'da logo görüntüsünün elde edilmesi için algoritmayı tanımlamaktadır.

X' test görüntüsünün yeni kaba şeklinden indek kümesi filigranı çıkartılarak elde edilen *C'*, sertifika oluşturma algoritmasının verildiği 1. adımdaki gibi hesaplanır. Sonra önceki görüntü tekrar inşa etmek için, şifre çözücü şifreleyicide olduğu gibi aynı kod kitabını kullanmalıdır. Bununla beraber önerilen yöntemde orijinal kod kitabı doğrulama işlemi için gerekmez çünkü doğrulama algoritmasında *C'* yeni kod kitabı gibi kullanılır. Vektör kuantizasyon şifre çözme sürecinde, alıcı imza ve zaman mührünü ve yeni *C'* kod kitabını koruyan indeks kümesini temel alarak telif hakkı logosunu tekrar inşa edebilir. Böylece herhangi birisi test edilmiş/bozulmuş görüntünün dalgacık dönüşümünden sonra kaba ölçekli görüntüden elde edilen açık indeks kümesi ve yeni kod kitabını kullanarak logo görüntüsü elde edilir.



Şekil 3.6. Logo görüntüsünün tekrar elde edilmesi.

BÖLÜM 4

ARAŞTIRMA BULGULARI VE TARTIŞMA

4.1. Giriş

Geliştirilen telif hakkı koruma yönteminin uygulanabilirliğini kanıtlamak için yapılan deneyler bu bölümde açıklanacaktır. Bu deneylerde logo görüntüsü *W* olarak Şekil 4.1 (e)'daki 64×64 piksellik COMU'yu, orijinal görüntü *X* olarakta Şekil 4.1 (a), (b), (c) ve (d)'deki 512×512 piksellik Lena, Peppers, Baboon, Barbara kullanıldı. Deneylerimizdeki tüm görüntüler 2×2 piksellik bloklara bölündü. Logonun blok sayısı $(64/2)\times(64/2)=1024$ 'dir. Orijinal görüntüye 4-ölçek seviye dalgacık dönüşümü uygulanmıştır. Kod kitabı kaba ölçekten elde edilir ve 32×32 pikselliktir. Kod kitabındaki kod kelimeleri bu yüzden 256'dır. Tüm gerekli parametreler aşağıda verilmiştir:

$$W_X = H_X = 512, W_W = H_W = 64, W_L = H_L = 32,$$
$$n = 2\times 2 = 4, l = 1024, t = 4, k = 256$$

Bu süreçte sağlamlık ile logo görüntüsünün kalitesi arasında ve sağlamlık ile sertifika üretim/doğrulama aşamasının etkiliği arasında tercihe bağlı olarak t-ölçek seviyesi belirlenir.

Test görüntüsü ile original görüntü arasında kaliteyi hesaplamak için denklem 4.1'da matematiksel ifadesi verilen peak signal-to-noise ratio (PSNR) kullanıldı. Bir mühendislik terimi olan tepe sinyal-gürültü oranı (PSNR), sinyalin mümkün olan maksimum gücü ile gösteriminin aslına uygunluğunu etkileyen gürültü bozulmasının gücü arasındaki orandır. Sinyallerin çok geniş dinamik alanları olması nedeniyle, PSNR genellikle logaritmik desibel ölçeği türünden ifade edilir (Wikipedia).

$$PSNR = 10\log\frac{E_{MAX}^2 \times W_X \times H_X}{\sum\left(X_{i,j} - X_{i,j}^{'}\right)^2} \tag{4.1}$$

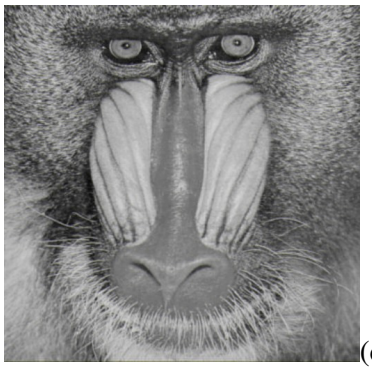
Formüldeki W_x ve H_x sırayla *X*'in genişliği ve yüksekliğini ifade etmektedir. $X_{i,j}$, *(i,j)* kordinatinin original değerini, $X_{i,j}^{'}$ *(i,j)* kordinatinin değiştirilmiş değerini, E_{MAX}^2 görüntü piksellerinin en büyük enerjisini ifade etmektedir.

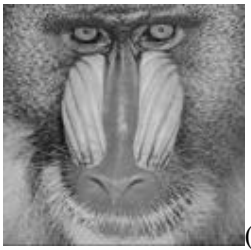
Deneysel sonuçlar saldırılar karşısında görüntü ciddi şekilde bozulsa bile geri elde edilen filigranların tanınabilir olduğunu göstermektedir. Elde edilen logo görüntüsü insan gözüyle algılanabilmektedir.

Ayrıca yöntemimizin natürel görüntüye uyarlanabilirliğini göstermek için ikinci logo görüntüsü olarak Şekil 4.1 (f)'de 128×128 piksellik baboon görüntüsünü kulladık


(a)

(b)


(e)

(c)

(d)

(f)

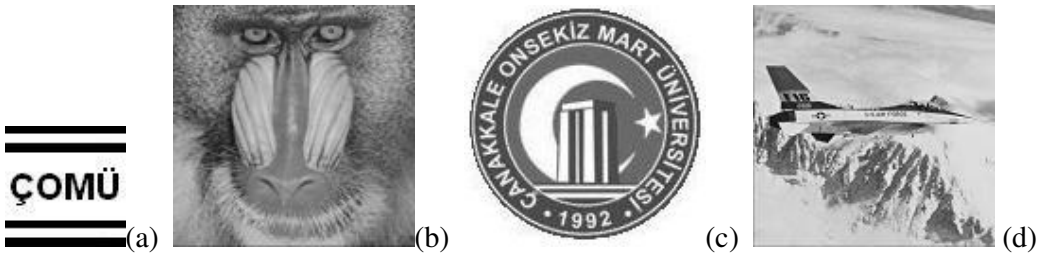
Şekil 4.1. Orijial görüntüler: (a) Lena, (b) Peppers, (c) Baboon, (d) Barbara, (e) COMU logosu, (e) 128×128 piksellik Baboon görüntüsü.

4.2. İndeks Kümesinin Filigranlanması

İndeks kümesinin filigranlaması işleminde k ağırlıklandırma katsayısının değerinin belirlenmesinde kullanılan kriter; saydamlık yani filigranlanmış görüntünün orijinal görüntüden gözle görülür şekilde fark veya bozulma olup olmamasıdır. Bunun sağlanması için araştırma kapsamında yapılan deneylerde her farklı orijinal görüntü ve logo için en uygun k ağırlıklandırma katsayısının değerinin farklı olduğu gözlemlenmiştir. COMU logosu için Lena'da $k > 0.024$, Baboon'da $k > 0.071$, Barbara'da $k > 0.022$, Peppers'da $k > 0.031$, Airplane'de $k > 0.051$ olduğunda bozulmalar gözle gürülür olmaktadır. Aynı şekilde Baboon logosu için Lena'da $k > 0.04$, Barbara'da $k>0.06$, Peppers'da $k > 0.07$, Airplane'de $k > 0{,}093$ değerini geçince bozulmalar gözle gürülür olmakla birlikte Baboon için $k>0{,}170$ değeri için ancak bozulmalar algılanabilecek boyutta olmaktadır. Yukarıda belirtilen sonuçlara dayanarak, deneylerimizde tüm indekslerin filigranlanması aşamasında ağırlıklandırma katsayı değeri $k = 0.02$ kullanılmıştır.

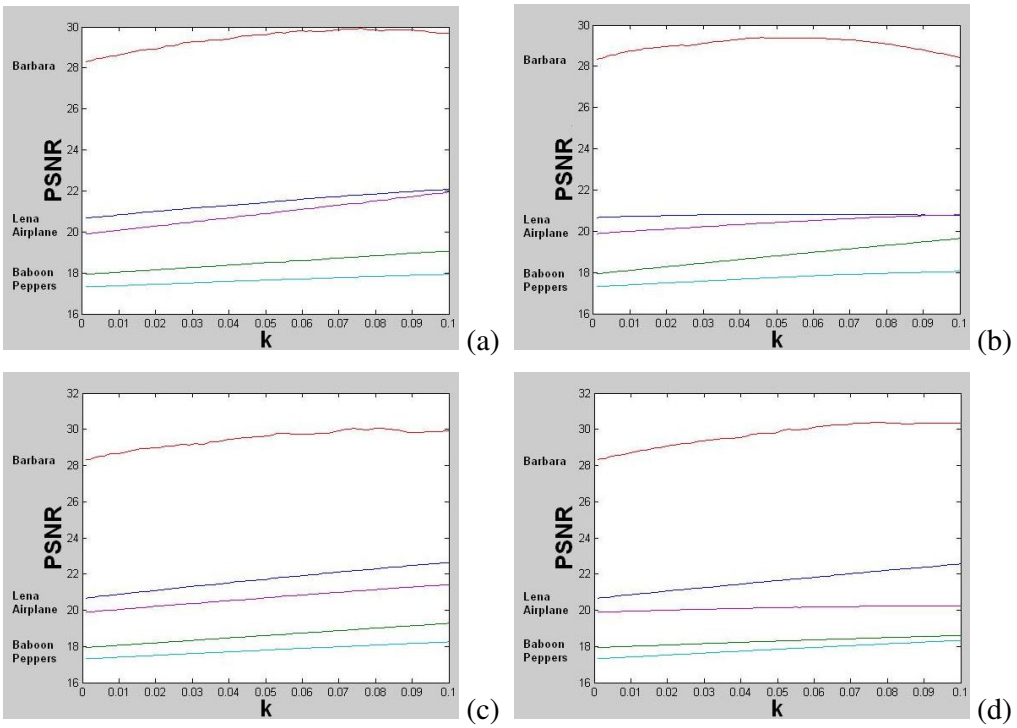
Lena, Baboon, Barbara, Peppers, Airplane görüntülerine Şekil 4.2. (a), (b), (c) ve (d)'de gösterilen COMU, Baboon, COMU amblemi, airplane logolarının $k \in [0,\ 0{,}1]$ aralığında 0.001 artırımlarla gömülmesiyle elde edilen PSNR değerlerine ait grafik Şekil

4.3'de verilmiştir.



(a) (b) (c) (d)

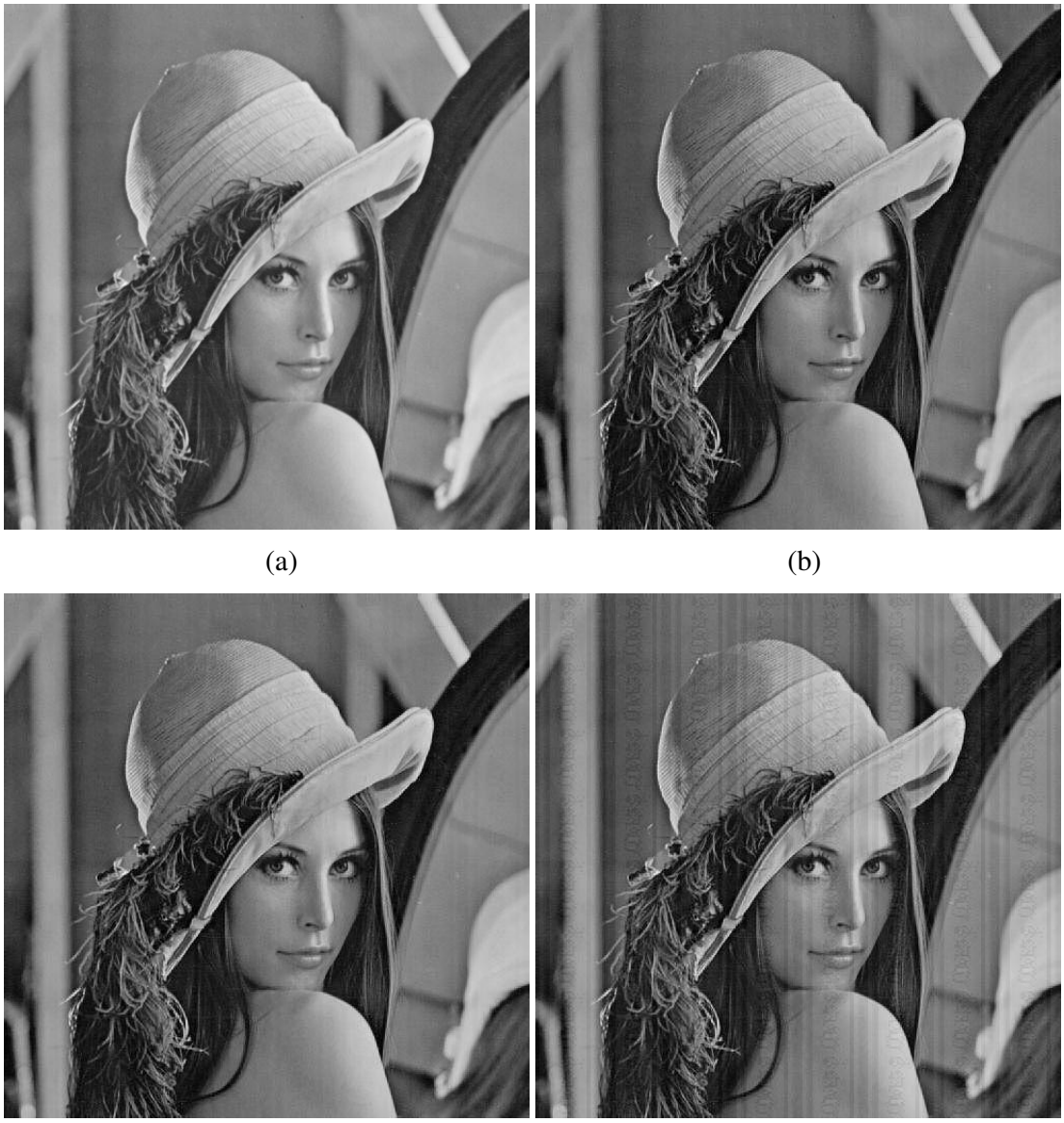
Şekil 4.2.(a) 64×64 piksel COMU logusu, (b) 128×128 piksel Baboon logosu, (c) 128×128 piksel COMU amblemi logosu, (d) 128×128 piksel airplane logosu.



(a) (b) (c) (d)

Şekil 4.3. (a) Lena, Baboon, Barbara, Peppers, Airplane görüntülerine COMU logosunun $k \in [0, 0,1]$ aralığında 0,001 artırımlarla gömülmesiyle elde edilen PSNR değerlerine ait grafik, (b) Lena, Baboon, Barbara, Peppers, Airplane görüntülerine Baboon logosunun $k \in [0, 0,1]$ aralığında 0,001 artırımlarla gömülmesiyle elde edilen PSNR değerlerine ait grafik, (c) Lena, Baboon, Barbara, Peppers, Airplane görüntülerine COMU amblemi logosunun $k \in [0, 0.1]$ aralığında 0,001 artırımlarla gömülmesiyle elde edilen PSNR değerlerine ait grafik, (d) Lena, Baboon, Barbara, Peppers, Airplane görüntülerine Airplane logosunun $k \in [0, 0,1]$ aralığında 0,001 artırımlarla gömülmesiyle elde edilen PSNR değerlerine ait grafik.

Şekil 4.4(a)'daki orijinal Lena görüntüsüne farklı ağırlıklandırma katsayılarıyla COMU logosunun gömülmesi sonucunda elde edilen filigranlanmış görüntüler incelendiğinde $k \geq 0.024$ değerleri için bozulmalar algılanmaya başlamakta, $k=0.10$ değerinde görüntü bozulması dikkat çekici olmaktadır (Şekil 4.4 (b), (c) ve (d)).

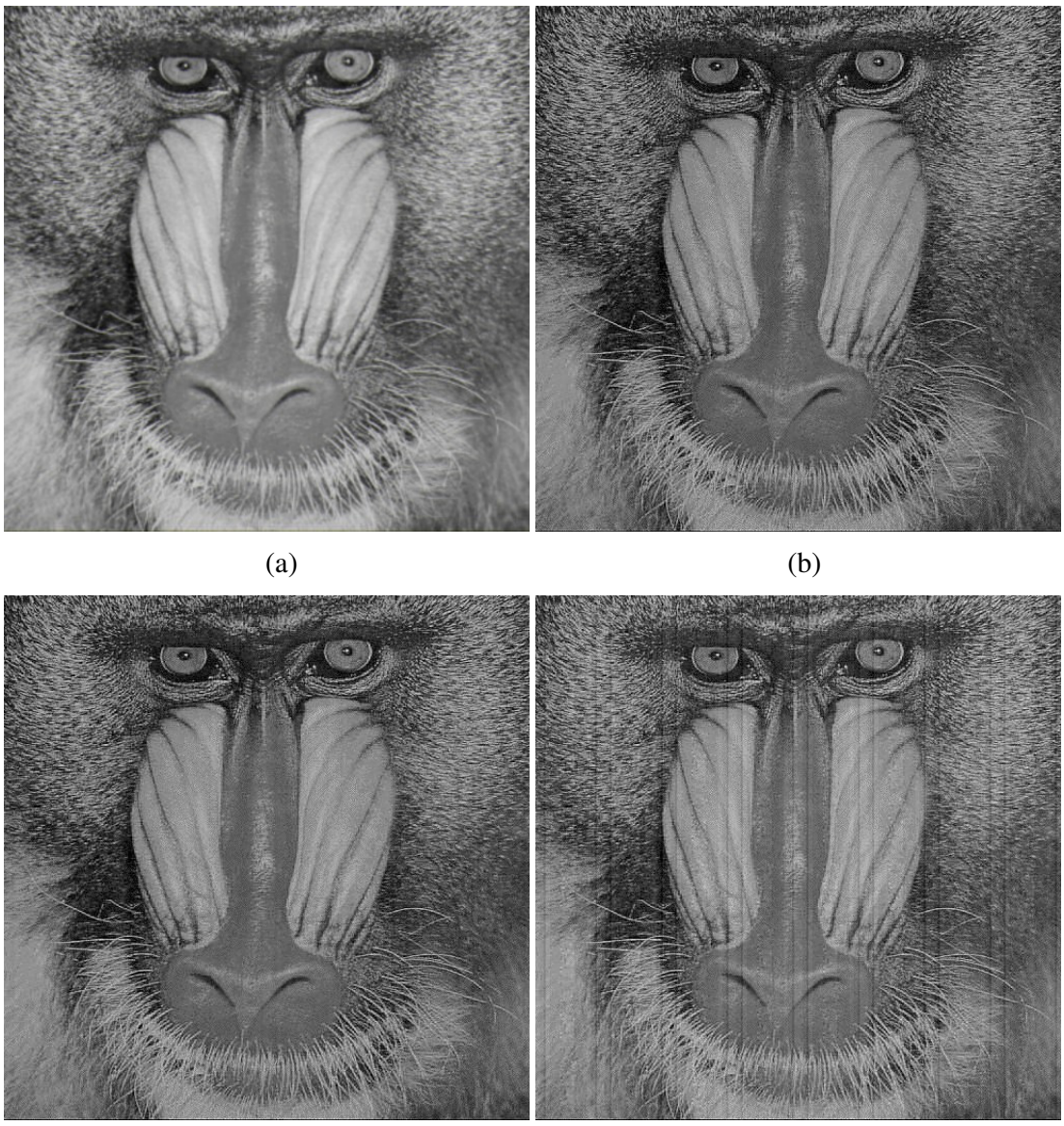


(a) (b)

(c) (d)

Şekil 4.4. (a) Orijinal Lena görüntüsü, (b) $k=0.02$ ağırlıklandırma katsayısıyla COMU logosunun Lena görüntüsüne gömülmüş görüntüsü, (c) $k=0.024$ ağırlıklandırma katsayısıyla COMU logosunun Lena görüntüsüne gömülmüş görüntüsü, (d) $k=0.10$ ağırlıklandırma katsayısıyla COMU logosunun Lena görüntüsüne gömülmüş görüntüsü.

Şekil 4.5(a)'daki orijinal Baboon görüntüsüne farklı ağırlıklandırma katsayılarıyla COMU logosunun gömülmesi sonucunda elde edilen filigranlanmış görüntüler incelendiğinde k=0.071 değeri için gri ton değerlerin birbirine yakın olduğu bölgelerde bozulmalar algılanmakta, $k \geq 0.30$ olduğunda ancak görüntünün genelinde bozulmalar görülebilir olmaktadır (Şekil 4.5 (b), (c) ve (d)).

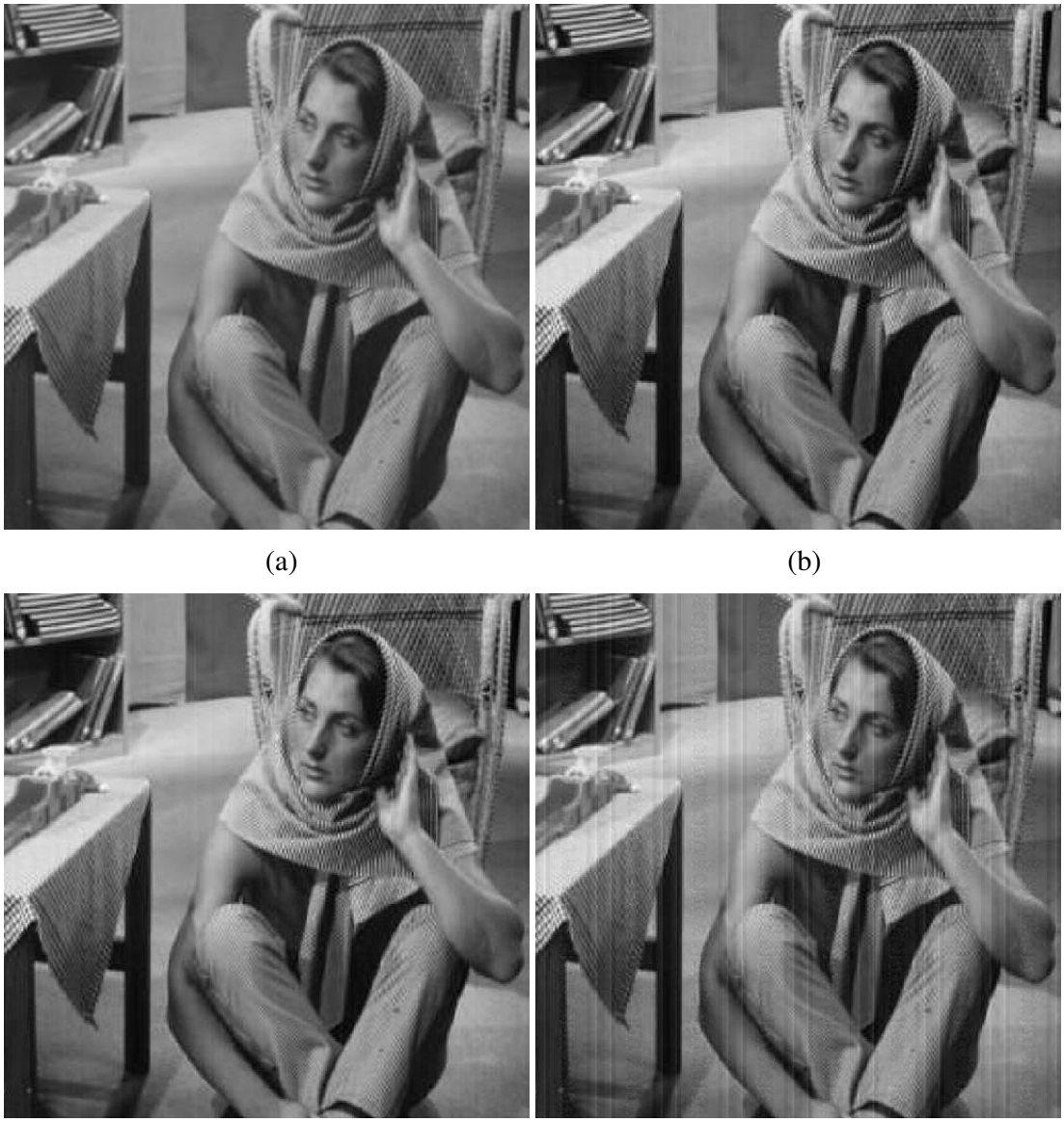


(a) (b)

(c) (d)

Şekil 4.5. (a) Orijinal Baboon görüntüsü, (b) k=0.02 ağırlıklandırma katsayısıyla COMU logosunun Baboon görüntüsüne gömülmüş görüntüsü, (c) k=0.071 ağırlıklandırma katsayısıyla COMU logosunun Baboon görüntüsüne gömülmüş görüntüsü, (d) k=0.30 ağırlıklandırma katsayısıyla COMU logosunun Baboon görüntüsüne gömülmüş görüntüsü.

Şekil 4.6(a)'daki orijinal Barbara görüntüsüne farklı ağırlıklandırma katsayılarıyla COMU logosunun gömüldüğünde, Lena görüntüsünde olduğu gibi *k*'nın küçük değerlerinden itibaren (*k*=0.022) görüntünün bozulmaya başladığı görülmektedir (Şekil 4.6 (b), (c) ve (d)).

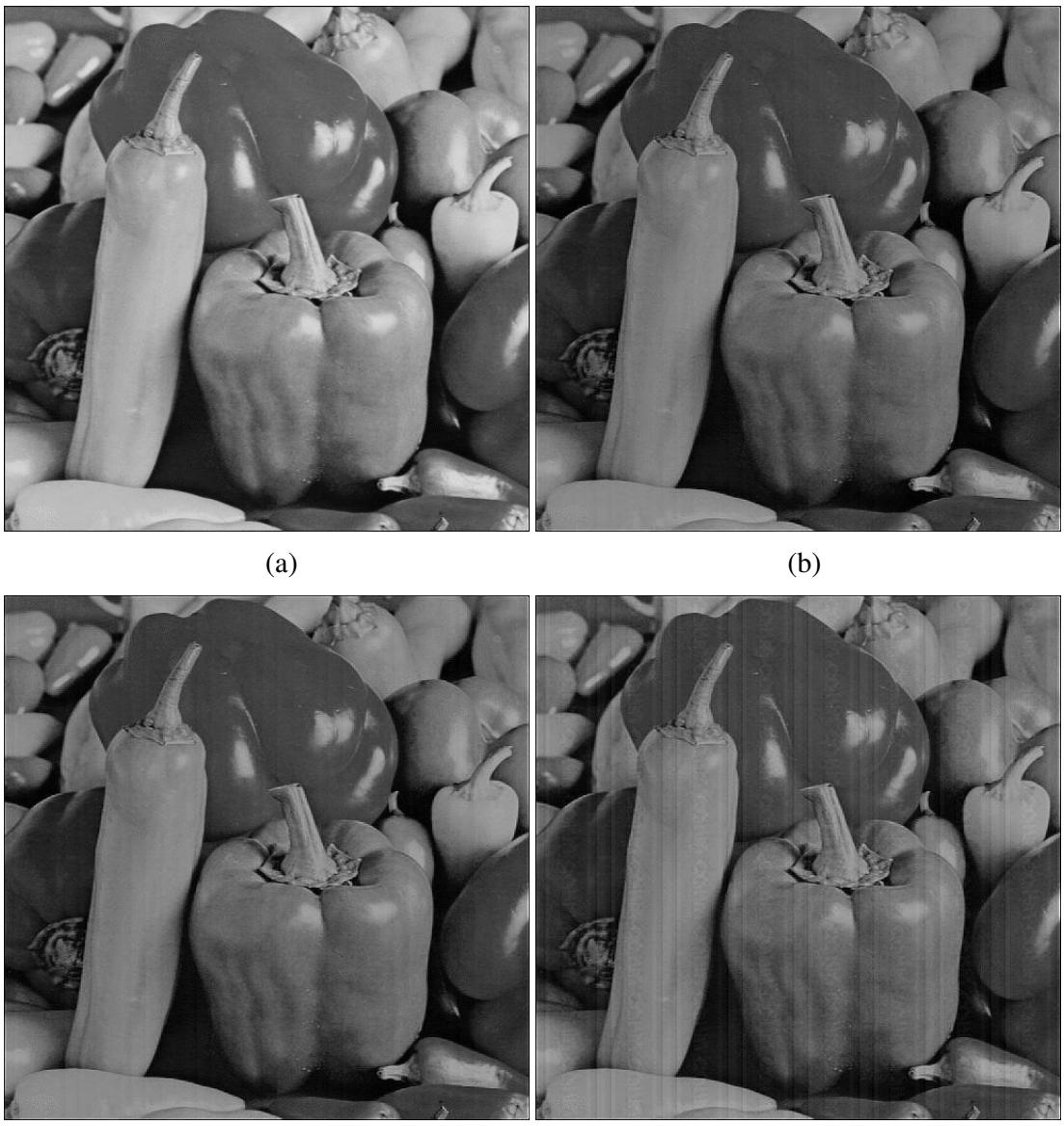


(a) (b)

(c) (d)

Şekil 4.6. (a) Orijinal Barbara görüntüsü, (b) *k*=0.02 ağırlıklandırma katsayısıyla COMU logosunun Barbara görüntüsüne gömülmüş görüntüsü, (c) *k*=0.022 ağırlıklandırma katsayısıyla COMU logosunun Barbara görüntüsüne gömülmüş görüntüsü, (d) *k*=0.10 ağırlıklandırma katsayısıyla COMU logosunun Barbara görüntüsüne gömülmüş görüntüsü.

Şekil 4.7(a)'daki orijinal Peppers görüntüsüne farklı ağırlıklandırma katsayılarıyla COMU logosunun gömülmesi sonucunda elde edilen filigranlanmış görüntüler incelendiğinde birbirine yakın renk tonlarının bulunduğu büyük alanların bulunmasında dolayı Lena ve Barbara görüntülerinde olduğu gibi k'nın küçük değerlerinden itibaren ($k \geq 0.031$) filigranlamış görüntüdeki bozulmalar algılanmaktadır (Şekil 4.7 (b), (c) ve (d)).

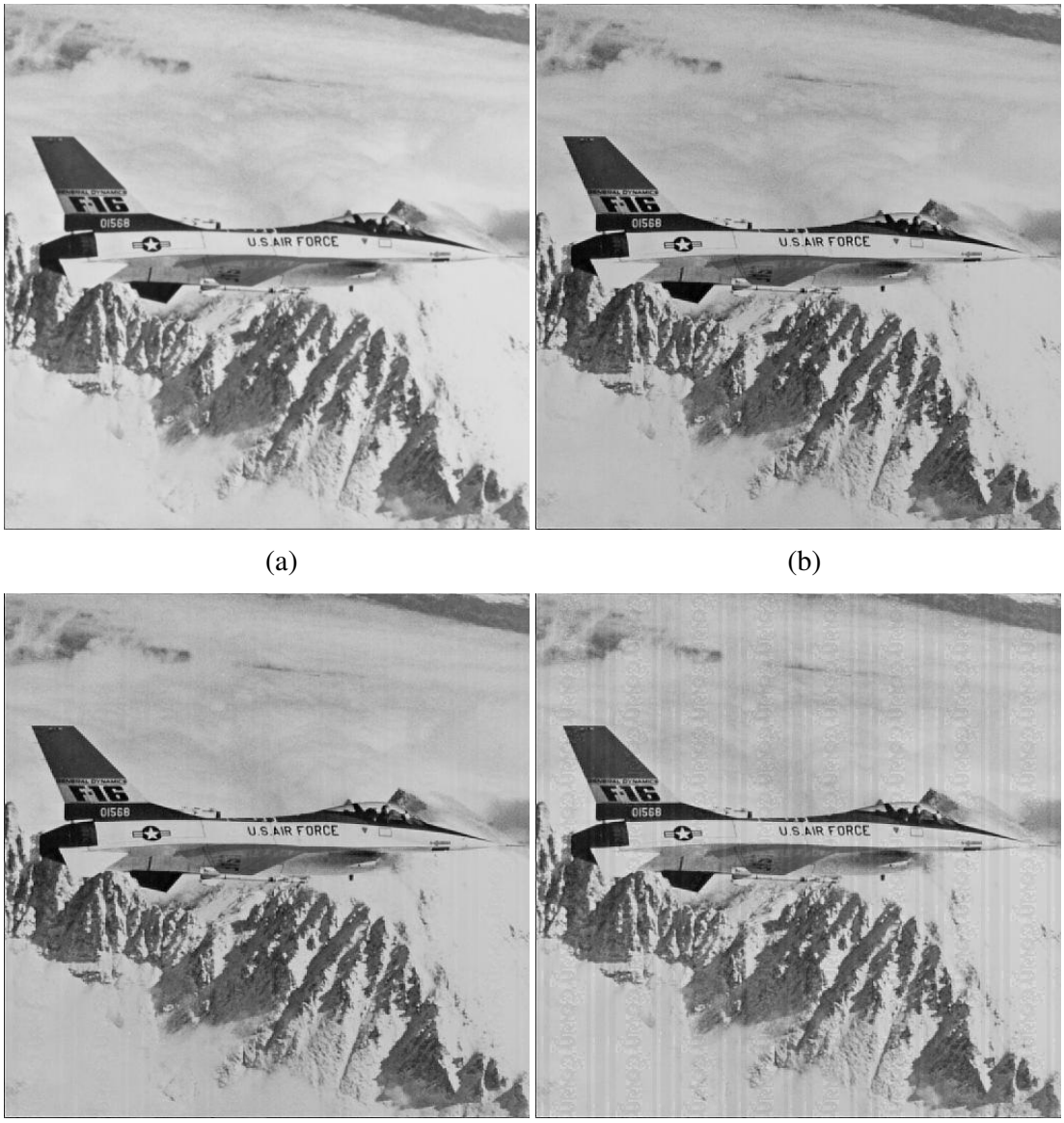


(a) (b)

(c) (d)

Şekil 4.7. (a) Orijinal Peppers görüntüsü, (b) k=0.02 ağırlıklandırma katsayısıyla COMU logosunun Peppers görüntüsüne gömülmüş görüntüsü, (c) k=0.031 ağırlıklandırma katsayısıyla COMU logosunun Peppers görüntüsüne gömülmüş görüntüsü, (d) k=0.10 ağırlıklandırma katsayısıyla COMU logosunun Peppers görüntüsüne gömülmüş görüntüsü.

Şekil 4.8(a)'daki orijinal Airplane görüntüsüne farklı ağırlıklandırma katsayılarıyla COMU logosunun gömüldüğünde, Baboon görüntüsünde olduğu gibi gri ton geçişlerinin sık olmasından dolayı $k \geq 0.056$ değerinde ancak bozulmalar gözle görülür olmaktadır (Şekil 4.8 (b), (c) ve (d)).

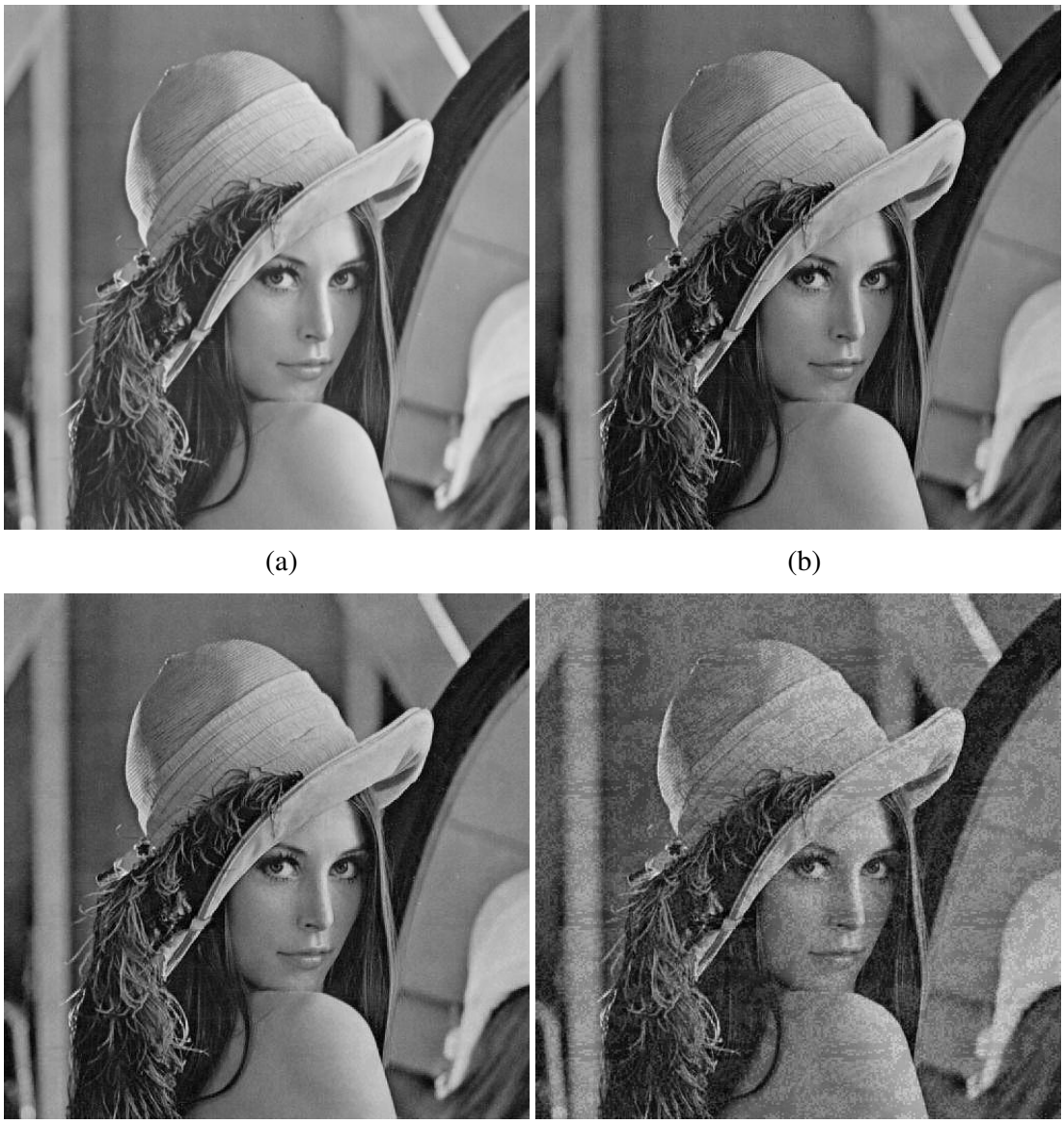


(a) (b)

(c) (d)

Şekil 4.8. (a) Orijinal Airplane görüntüsü, (b) k=0.02 ağırlıklandırma katsayısıyla COMU logosunun Airplane görüntüsüne gömülmüş görüntüsü, (c) k=0.056 ağırlıklandırma katsayısıyla COMU logosunun Airplane görüntüsüne gömülmüş görüntüsü, (d) k=0.20 ağırlıklandırma katsayısıyla COMU logosunun Airplane görüntüsüne gömülmüş görüntüsü.

Şekil 4.9(a)'daki orijinal Lena görüntüsüne $k \in \{0.02, 0.04, 0.20\}$ ağırlıklandırma katsayılarıyla Baboon logosunun gömülmesiyle elde edilen filigranlanmış görüntüler Şekil 4.9 (b), (c) ve (d)'de gösterilmektedir. COMU logosunun gömüldüğü Lena görüntüsünde k=0.024 iken bozulma algılabiliyorken Baboon logosunun gömüldüğü Lena görüntüsünde k=0.04 değerinden itibaren bozulmalar algılanabilmektedir.

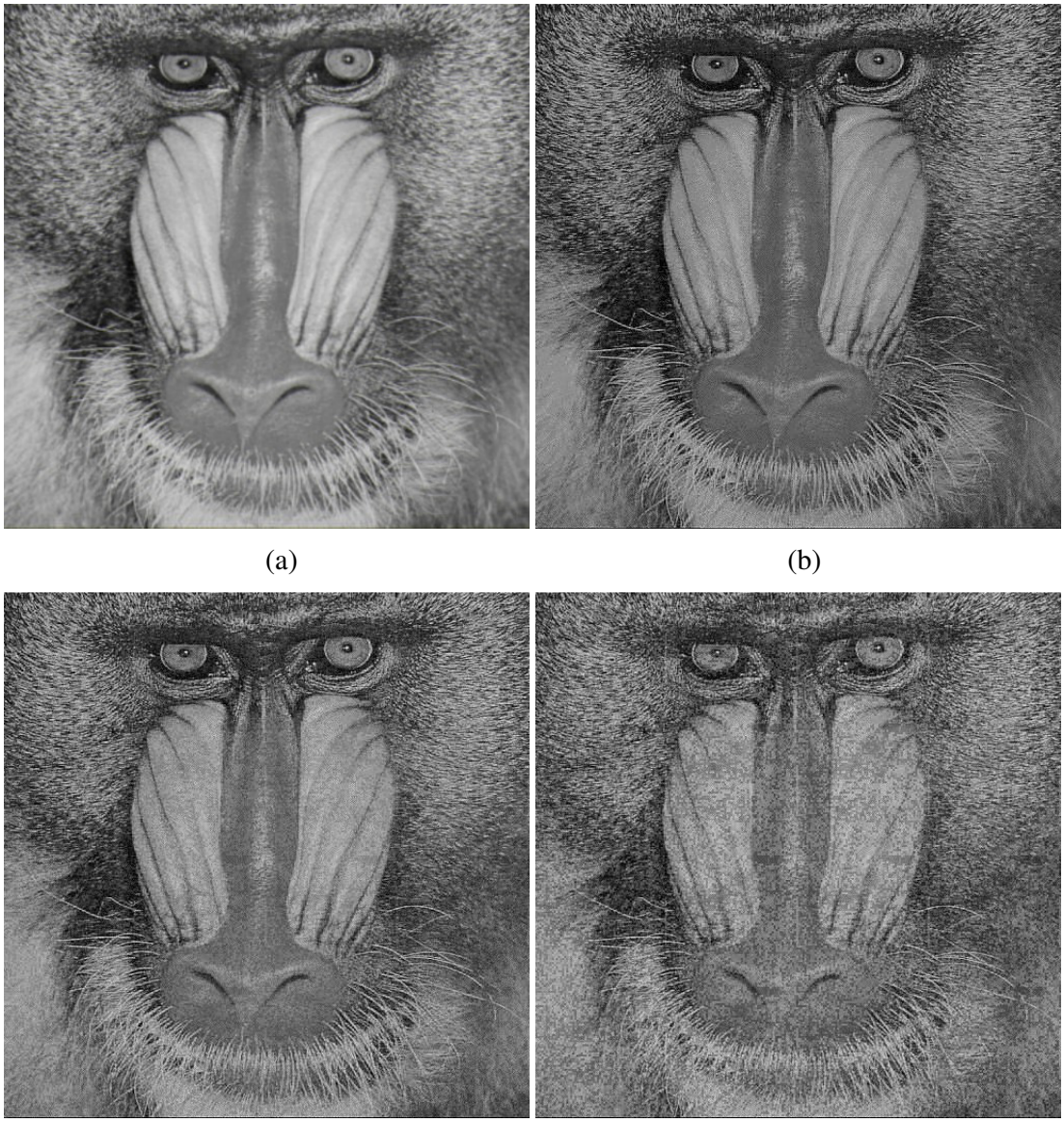


(a) (b)

(c) (d)

Şekil 4.9. (a) Orijinal Lena görüntüsü, (b) k=0.02 ağırlıklandırma katsayısıyla Baboon logosunun Lena görüntüsüne gömülmüş görüntüsü, (c) k=0.04 ağırlıklandırma katsayısıyla Baboon logosunun Lena görüntüsüne gömülmüş görüntüsü, (d) k=0.20 ağırlıklandırma katsayısıyla Baboon logosunun Lena görüntüsüne gömülmüş görüntüsü.

Şekil 4.10 (a)'daki orijinal Baboon görüntüsüne $k \in \{0.02, 0.171, 0.40\}$ ağırlıklandırma katsayılarıyla Baboon logosunun gömülmesiyle elde edilen filigranlanmış görüntüler Şekil 4.10 (b), (c) ve (d)'de gösterilmektedir.

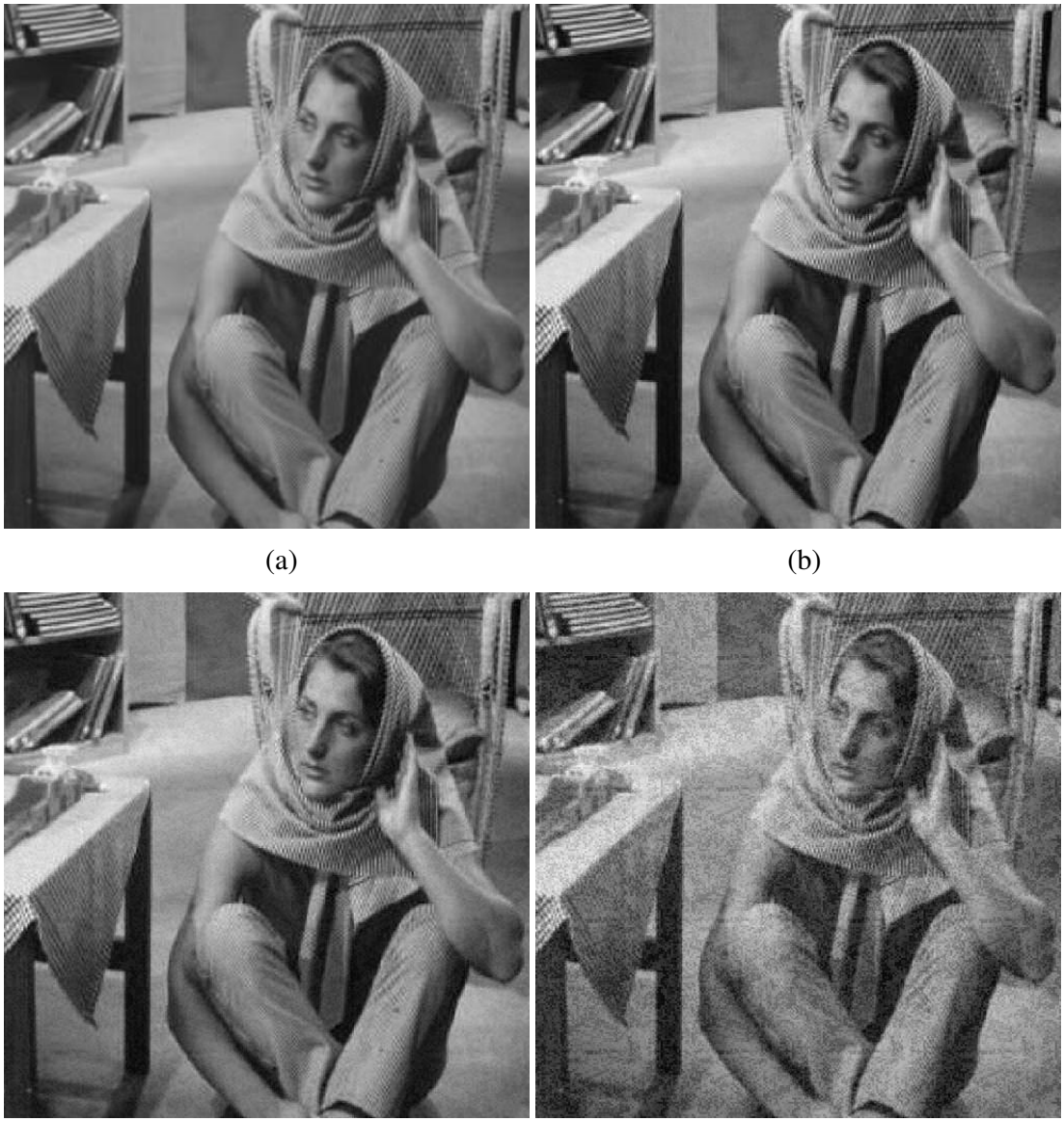


(a) (b)

(c) (d)

Şekil 4.10. (a) Orijinal Baboon görüntüsü, (b) k=0.02 ağırlıklandırma katsayısıyla Baboon logosunun Baboon görüntüsüne gömülmüş görüntüsü, (c) k=0.171 ağırlıklandırma katsayısıyla Baboon logosunun Baboon görüntüsüne gömülmüş görüntüsü, (d) k=0.40 ağırlıklandırma katsayısıyla Baboon logosunun Baboon görüntüsüne gömülmüş görüntüsü.

Şekil 4.11 (a)'daki orijinal Barbara görüntüsüne $k \in \{0.02, 0.06, 0.20\}$ ağırlıklandırma katsayılarıyla Baboon logosunun gömülmesiyle elde edilen filigranlanmış görüntüler Şekil 4.11 (b), (c) ve (d)'de gösterilmektedir.

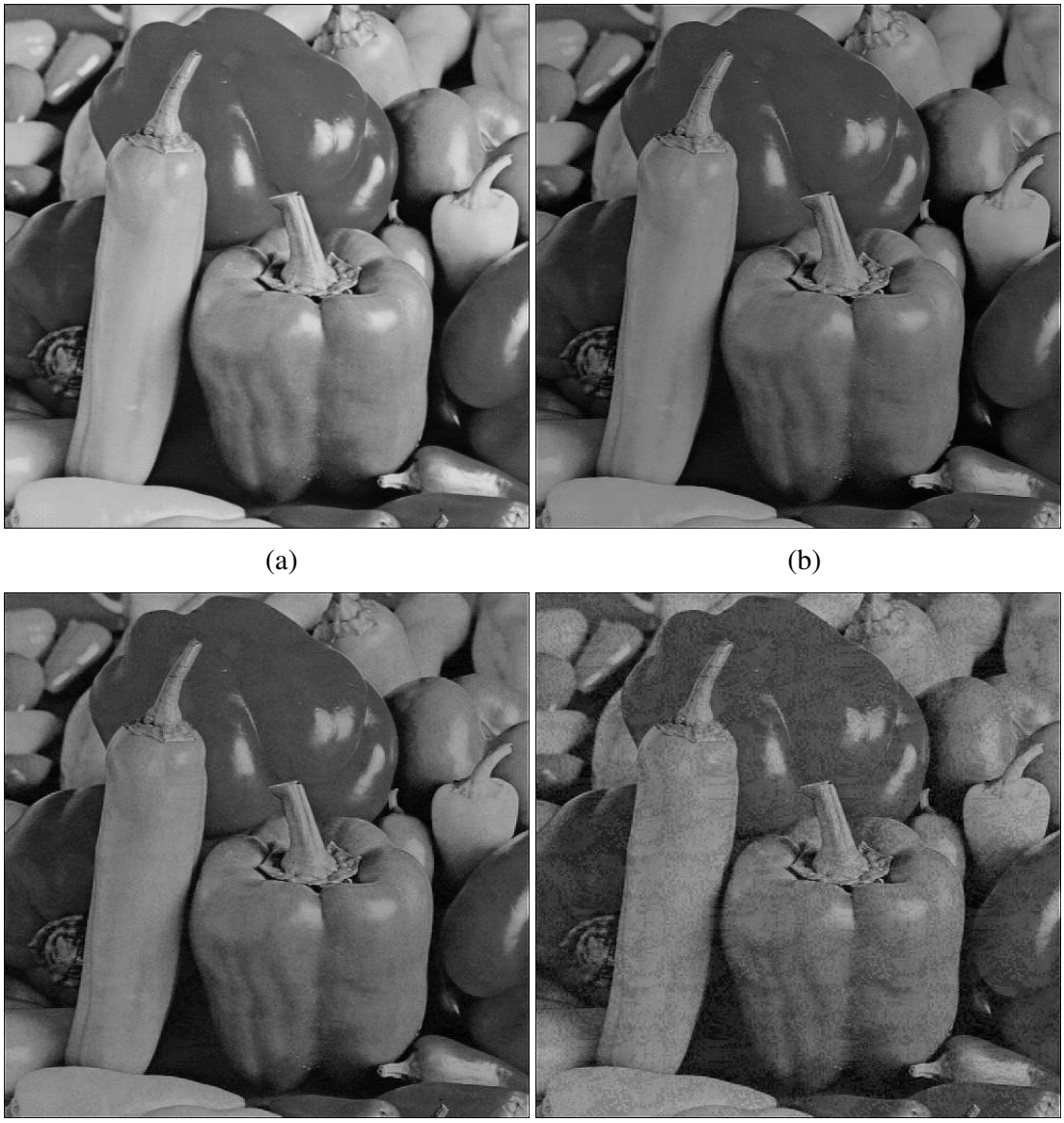


(a) (b)

(c) (d)

Şekil 4.11. (a) Orijinal Barbara görüntüsü, (b) k=0.02 ağırlıklandırma katsayısıyla Baboon logosunun Barbara görüntüsüne gömülmüş görüntüsü, (c) k=0.06 ağırlıklandırma katsayısıyla Baboon logosunun Barbara görüntüsüne gömülmüş görüntüsü, (d) k=0.20 ağırlıklandırma katsayısıyla Baboon logosunun Barbara görüntüsüne gömülmüş görüntüsü.

Şekil 4.12 (a)'daki orijinal Peppers görüntüsüne $k \in \{0.02, 0.07, 0.20\}$ ağırlıklandırma katsayılarıyla Baboon logosunun gömülmesiyle elde edilen filigranlanmış görüntüler Şekil 4.12 (b), (c) ve (d)'de gösterilmektedir.

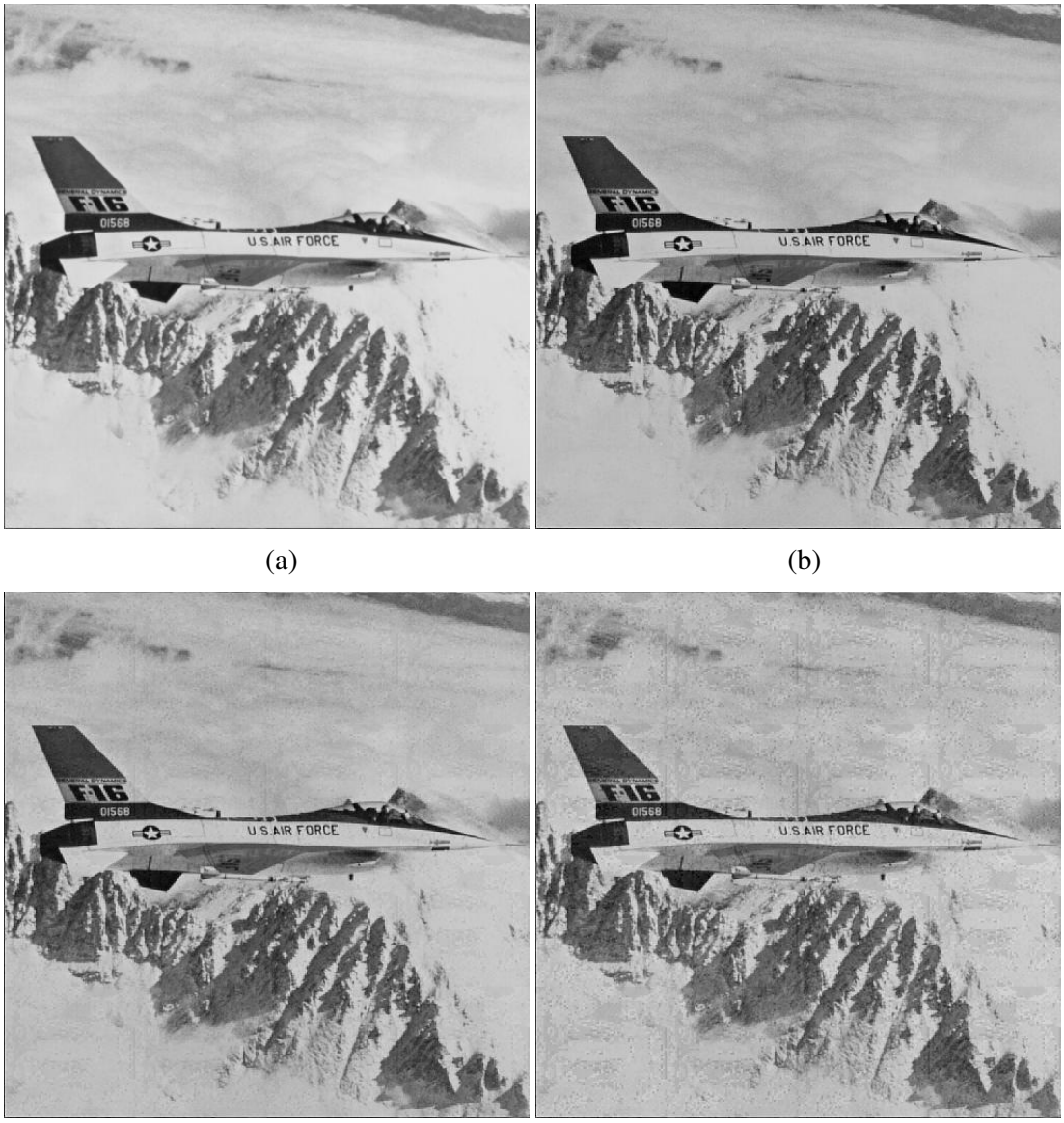


(a) (b)

(c) (d)

Şekil 4.12. (a) Orijinal Peppers görüntüsü, (b) k=0.02 ağırlıklandırma katsayısıyla Baboon logosunun Peppers görüntüsüne gömülmüş görüntüsü, (c) k=0.07 ağırlıklandırma katsayısıyla Baboon logosunun Peppers görüntüsüne gömülmüş görüntüsü, (d) k=0.20 ağırlıklandırma katsayısıyla Baboon logosunun Peppers görüntüsüne gömülmüş görüntüsü.

Şekil 4.13 (a)'daki orijinal Airplane görüntüsüne $k \in \{0.02, 0.093, 0.20\}$ ağırlıklandırma katsayılarıyla Baboon logosunun gömülmesiyle elde edilen filigranlanmış görüntüler Şekil 4.13 (b), (c) ve (d)'de gösterilmektedir.



(a) (b)

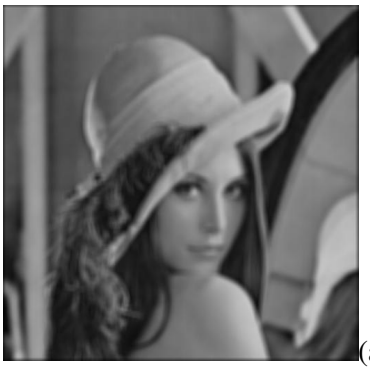
(c) (d)

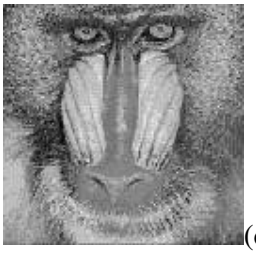
Şekil 4.13. (a) Orijinal Airplane görüntüsü, (b) k=0.02 ağırlıklandırma katsayısıyla Baboon logosunun Airplane görüntüsüne gömülmüş görüntüsü, (c) k=0.093 ağırlıklandırma katsayısıyla Baboon logosunun Airplane görüntüsüne gömülmüş görüntüsü, (d) k=0.20 ağırlıklandırma katsayısıyla Baboon logosunun Airplane görüntüsüne gömülmüş görüntüsü.

4.3. Deneyler

4.3.1. Görüntü Bulanıklaştırma

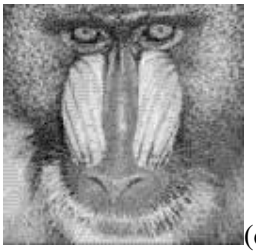
İlk olarak, filigranlanmış Lena görüntüsü Şekil 4.14 (a)'da görüldüğü gibi bulanıklaştırıldı ve PSNR değerini 19dB elde edildi (Çizelge 1'de PSNR değerleri verilmiştir). Buna rağmen elde edilen logo görüntülerinin algılanabildiği görülmektedir (Şekil 4.14 (b) ve (c)). Benzer işlemler Şekil 4.15, 4.16, 4.17 'de Baboon, Barbara ve Peppers görüntülerine uygulanmıştır.


(a)


(b)

(c)

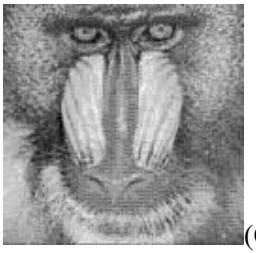
Şekil 4.14. (a) Bulanıklaştırılmış Lena görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.


(a)


(b)

(c)

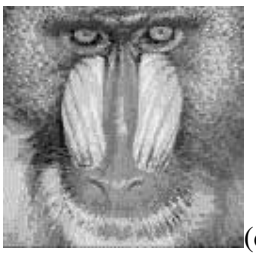
Şekil 4.15. (a) Bulanıklaştırılmış Baboon görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.

 (a) 

(b)  (C)

Şekil 4.16. (a) Bulanıklaştırılmış Barbara görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.

 (a) 

(b)  (c)

Şekil 4.17. (a) Bulanıklaştırılmış Peppers görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.

Çizelge 1.Bulanıklaştırmada Elde Edilen PSNR Değerleri (dB)

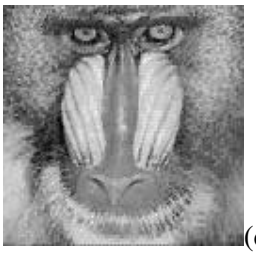
Orijinal Görüntü	**Logo Görüntüsü**	
	Lena	**Baboon**
Lena	19.1197	18.9987
Baboon	15.5150	15.5930
Barbara	12.6428	24.4313
Peppers	16.3024	16.3427

4.3.2. Görüntü JPEG Sıkıştırma

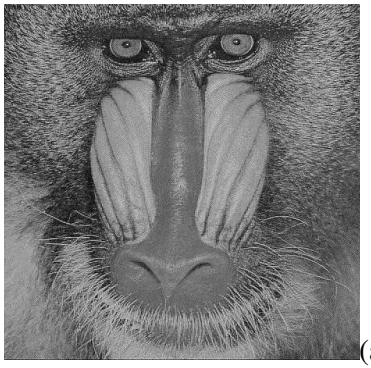
Şekil 4.18 (a)'da filigranmış Lena'nın StirMark Benchmark ile %50 JPEG sıkıştırılmış, Şekil 4.18 (b) ve (c) geri elde edilen logo görüntüsü gösterilmektedir. Benzer

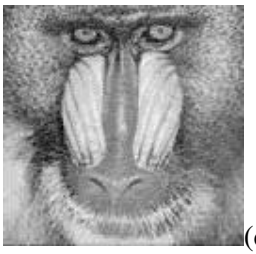
işlemler Şekil 4.19, 4.20, 4.21'de Baboon, Barbara ve Peppers resimlerine uygulanmıştır. Çizelge 2'de PSNR değerleri verilmiştir.


(a)


(b)

(c)

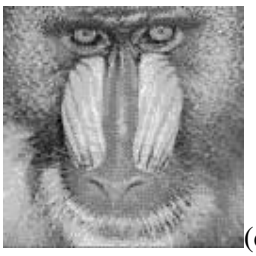
Şekil 4.18. (a) %50 JPEG sıkıştırılmış Lena görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon Logosu.


(a)


(b)

(c)

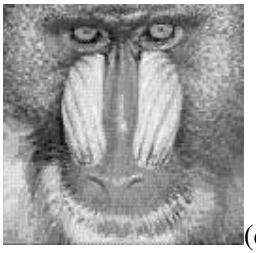
Şekil 4.19. (a) %50 JPEG sıkıştırılmış Baboon görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.


(a)


(b)

(c)

Şekil 4.20. (a) %50 JPEG sıkıştırılmış Barbara görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.

 (a) 

(b)  (c)

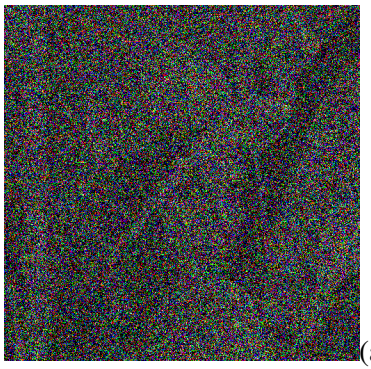
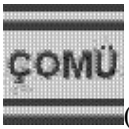
Şekil 4.21. (a) %50 JPEG sıkıştırılmış Peppers görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.

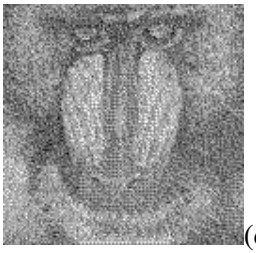
Çizelge 2. %50 JPEG Sıkıştırılmada Elde Edilen PSNR Değerleri(dB)

Orijinal Görüntü	**Logo Görüntüsü**	
	Lena	**Baboon**
Lena	27.0165	26.7212
Baboon	21.0267	21.1655
Barbara	24.7828	20.7079
Peppers	20.6434	20.7079

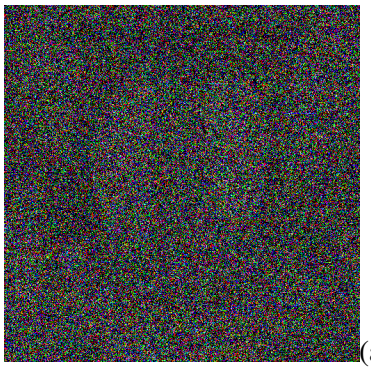
4.3.3. Görüntüye Gürültü Ekleme

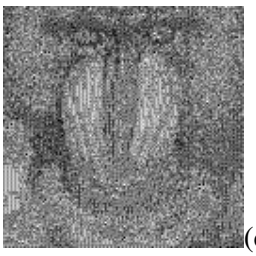
StirMark Benchmark tarafından %80 gürültü eklenen filigranlanmış görüntü Şekil4.22.(a)'da ve geri elde edilen logo görüntüleri Şekil 4.22.(b) ve (c) gösterilmiştir. Benzer işlemler Şekil 4.23, 4.24, 4.25'de Babon, Barbara ve Peppers resimlerine uygulanmıştır. Çizelge 3'de PSNR değerleri verilmiştir.

 (a) 

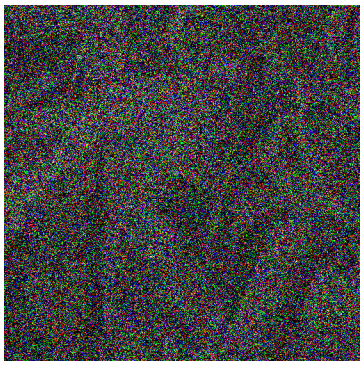
(b)  (c)

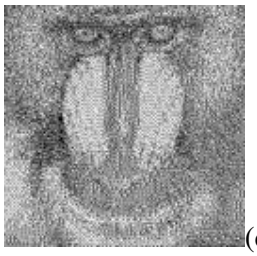
Şekil 4.22. (a) %80 Gürültü eklenmiş Lena görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.

 (a) 

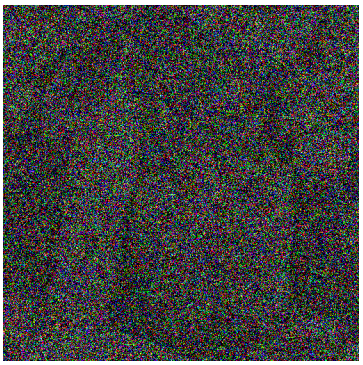
(b)  (c)

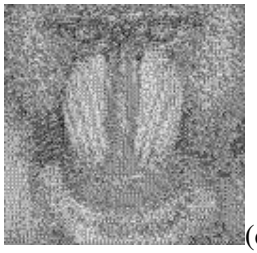
Şekil 4.23. (a) %80 Gürültü eklenmiş Baboon görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.

 (a) 

(b)  (c)

Şekil 4.24. (a) %80 Gürültü eklenmiş Barbara görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.


(a)


(b)

(c)

Şekil 4.25. (a) %80 Gürültü eklenmiş Peppers görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.

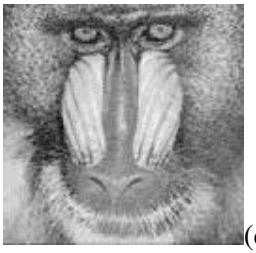
Çizelge 3. %80 Gürültü Eklemede Elde Edilen PSNR Değerleri (dB)

Orijinal Görüntü	**Logo Görüntüsü**	
	Lena	**Baboon**
Lena	8.0679	8.0758
Baboon	7.6837	7.6680
Barbara	8.1954	8.2104
Peppers	8.1529	8.1473

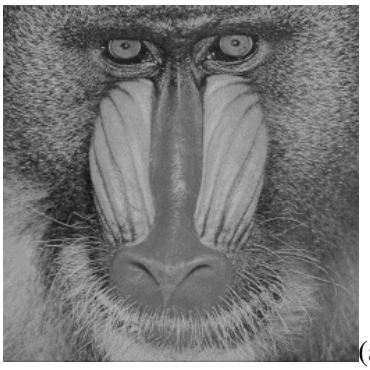
4.3.4. Görüntü Ölçekleme

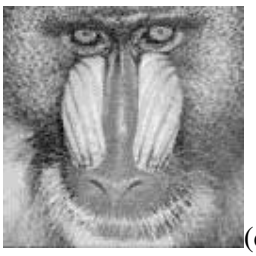
Stirmark benchmark ile 512×512 piksellik görüntü 256×256 piksele ölçeklendirmiştir. Ölçeklenen 256×256 piksellik görüntü tekrar 512×512 piksele ölceklendi (Şekil 4.26.(a)). Ölçekleme işleminde bazı ayrıntılar kaybolsa da logo görüntüsünü tekrar elde edildi (Şekil 4.26.(b), (c)). Aynı işlemler şekil 4.27, 4.28, 4.29'de Babon, Barbara ve Peppers resimlerine uygulanmıştır. Çizelge 4'de PSNR değerleri verilmiştir.


(a)


(b)

(c)

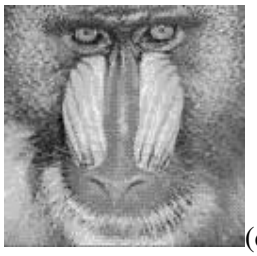
Şekil 4.26. (a) Ölçeklenmiş Lena görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.


(a)


(b)

(c)

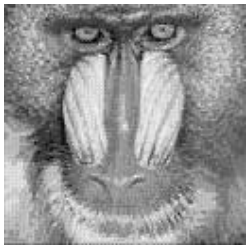
Şekil 4.27. (a) Ölçeklenmiş Baboon görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.


(a)


(b)

(c)

Şekil 4.28. (a) Ölçeklenmiş Barbara görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.


(a)


(b)

(c)

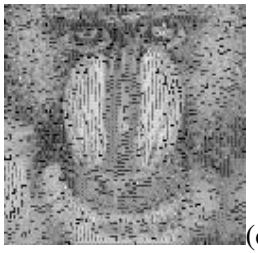
Şekil 4.29. (a) Ölçeklenmiş Peppers görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.

Çizelge 4. %50 Ölçeklemede Elde Edilen PSNR Değerleri (dB)

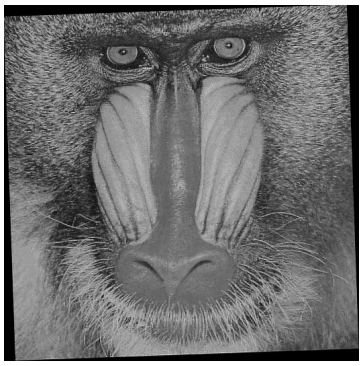
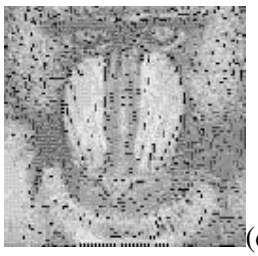
Orijinal Görüntü	**Logo Görüntüsü**	
	Lena	**Baboon**
Lena	27.9895	27.6309
Baboon	19.7707	19.8799
Barbara	25.6347	24.6399
Peppers	20.2863	20.3418

4.3.5. Görüntü Döndürme

Çoğu filigranlama yöntemi döndürme işlemi uygulandıktan sonra hayatta kalamamaktadır. StirMark Benchmark ile 2° döndürülen görüntü 512×512 piksele ölçeklenmiştir (Şekil 4.30.(a)) ve tekrar elde edilen logo görüntüleri Şekil 4.30.(b) ve (c) de gösterilmiştir. Benzer işlemler şekil 4.31, 4.32, 4.33'de Babon, Barbara ve Peppers resimlerine uygulanmıştır. Çizelge 5'de PSNR değerleri verilmiştir.

 (a)  (b)  (c)

Şekil 4.30. (a) 2° Döndürmüş Lena görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.

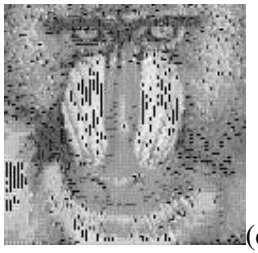
 (a)  (b)  (c)

Şekil 4.31. (a) 2° Döndürmüş Baboon görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.

 (a)  (b)  (c)

Şekil 4.32. (a) 2° Döndürmüş Barbara görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.


(a)


(b)

(c)

Şekil 4.33. (a) 2° Döndürmüş Peppers görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.

Çizelge 5. 2° Döndürmede Elde Edilen PSNR Değerleri (dB)

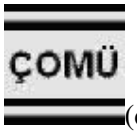
Orijinal Görüntü	**Logo Görüntüsü**	
	Lena	**Baboon**
Lena	14.5033	14.4948
Baboon	13.4440	13.4667
Barbara	14.2152	14.1251
Peppers	13.9265	13.9369

4.3.6. Görüntü Kırpma

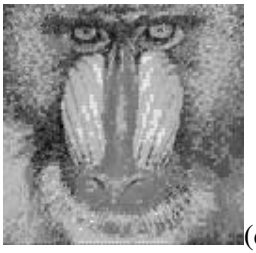
Şekil4.34.(a)'da Stirmark benchmark ile filigranmış lena görüntüsünün orta kısımlarından kıpılmış hali görülmektedir. Logo görüntüsünü doğrulamak için kırpılmış görüntüyü legal olarak dağıtılan filigranlamış lena görüntüsü üzerine yapıştırıldı Şekil4.34.(a). Yapılan bu saldırıya karşı yinede logo görüntüleri geri elde edebilmektedir. Benzer işlemler Şekil 4.35, 4.36, 4.37'de Baboon, Barbara ve Peppers resimlerine uygulanmıştır. Çizelge 6' de PSNR değerleri verilmiştir.

(a)

(b)

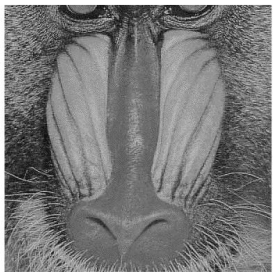


(c)

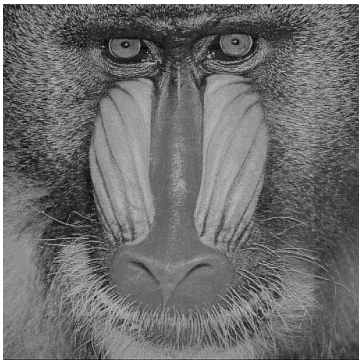


(d)

Şekil 4.34. (a) Kırpılmış Lena görüntüsü, (b) kırpılmış Lena görüntüsünün filigranlamış Lena görüntüsü üzerine yapıştırılmış görüntüsü, (c) COMU logosu, (d) elde edilen Baboon logosu.



(a)



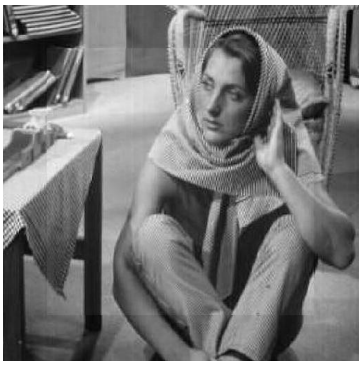
(b)

(c)

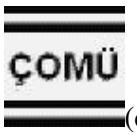
(d)

Şekil 4.35. (a) Kırpılmış Baboon görüntüsü, (b) kırpılmış Baboon görüntüsünün filigranlamış Baboon görüntüsü üzerine yapıştırılmış görüntüsü, (c) COMU logosu, (d) elde edilen Baboon logosu.

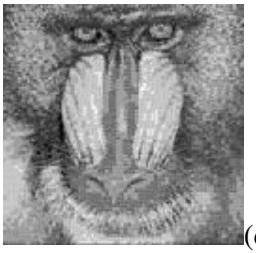
(a)



(b)



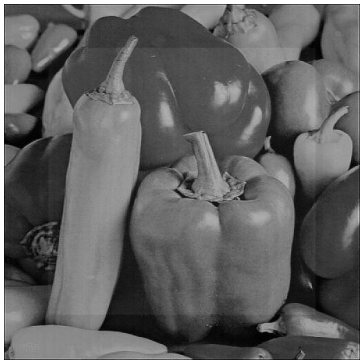
(c)



(d)

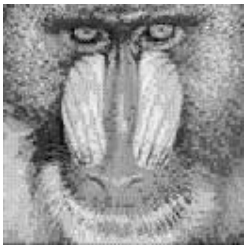
Şekil 4.36. (a) Kırpılmış Barbara görüntüsü, (b) kırpılmış Barbara görüntüsünün filigranlamış Barbara görüntüsü üzerine yapıştırılmış görüntüsü, (c) COMU logosu, (d) elde edilen Baboon logosu.

(a)



(b)

(c)



(d)

Şekil 4.37. (a) Kırpılmış Peppers görüntüsü, (b) kırpılmış Peppers görüntüsünün filigranlamış Peppers görüntüsü üzerine yapıştırılmış görüntüsü, (c) COMU logosu, (d) elde edilen Baboon logosu.

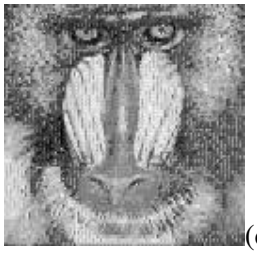
Çizelge 6. Kırpma Sonucu Elde Edilen PSNR Değerleri (dB)

Orijinal Görüntü	Logo Görüntüsü	
	Lena	Baboon
Lena	8.3205	8.3216
Baboon	17.2508	17.3318
Barbara	23.4495	24.9494
Peppers	18.9603	18.9626

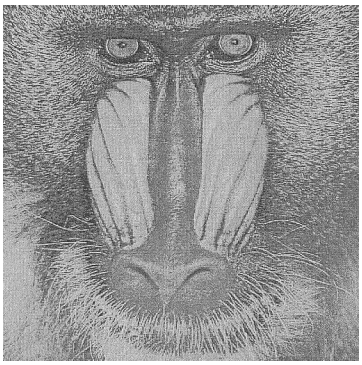
4.3.7. Görüntüyü Yazdırma-Kopyalama-Tarama

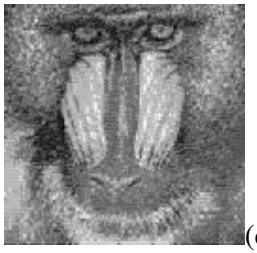
Şekil 4.38(a)'da değiştirilmiş Lena görülmektedir. İlk olarak filigranlanmış Lena standart kağıt üzerine 600dpi çözünürlükle yazdırıldı. Yazdırınlan görüntünün fotokopisi çekildi ve 200dpi, 256 gri seviye ayarlarla tarayıcıda tarandı. Görüntünün fotokopisi çekilirken ve taranırken kağıt tam düzgün olarak yerleştirilemediğinden görüntü az da olsa döndürülmüş olarak elde edilebildi Son olarak taranan görüntü 512×512 piksele ölçeklendi. Yazdırma, kopyalama, tarama, döndürme, ölçekleme olmak üzere Beş bozulma safhasından geçen filigranlanmış görüntünün her ne kadar hasarlanmış olsa da Şekil 4.38.(b) ve (c) de logo görüntüleri elde edildi. Benzer işlemler şekil 4.39, 4.40, 4.41'da babon Barbara ve Peppers resimlerine uygulanmıştır. Çizelge 7'de PSNR değerleri verilmiştir.


(a)

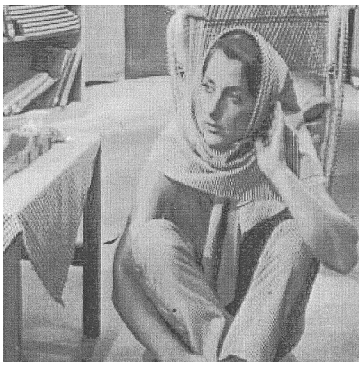

(b)

(c)

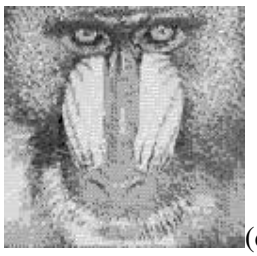
Şekil 4.38. (a) Yazdırma-kopyalama-tarama yapılmış Lena görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.


(a)

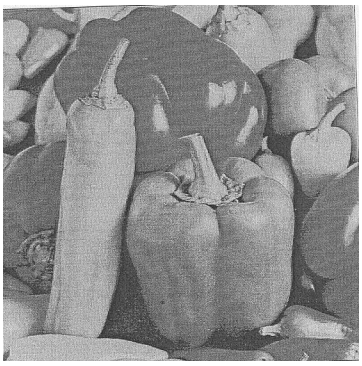

(b)

(c)

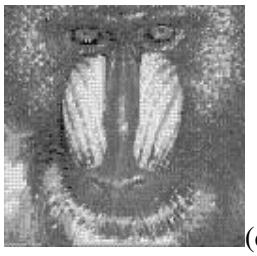
Şekil 4.39. (a) Yazdırma-kopyalama-tarama yapılmış Baboon görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.


(a)


(b)

(c)

Şekil 4.40. (a) Yazdırma-kopyalama-tarama yapılmış Barbara görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.


(a)


(b)

(c)

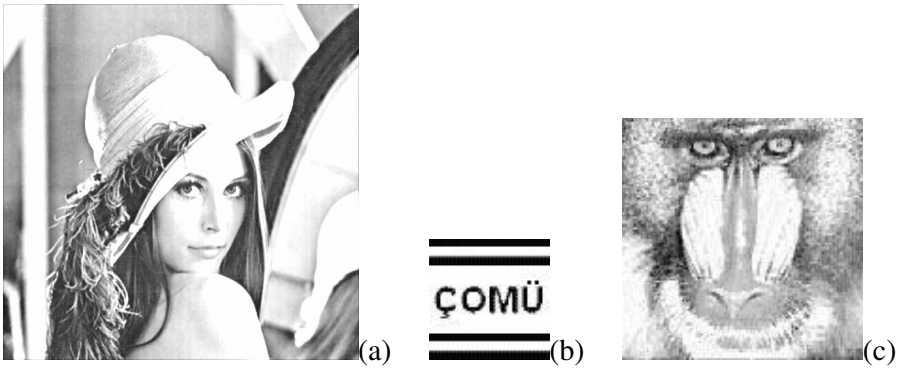
Şekil 4.41. (a) Yazdırma-kopyalama-tarama yapılmış Peppers görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.

Çizelge 7. Yazdırma-Kopyalama-Tarama Sonucu Elde Edilen PSNR Değerleri(dB)

Orijinal Görüntü	Logo Görüntüsü	
	Lena	Baboon
Lena	14.4626	14.9508
Baboon	12.5499	12.7055
Barbara	12.5494	12.3324
Peppers	6.5775	6.7224

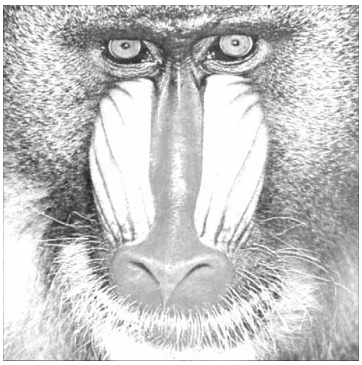
4.3.8. Görüntüyü Kıvrım filtreleme (ConvFilter)

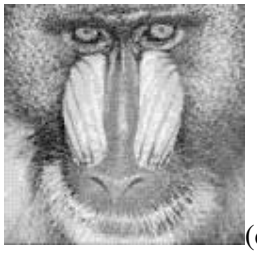
StirMark Benchmark ile filigranmış lena görüntüsünün Kıvrım filtrelenmiş (Gaussian filtreleme ve keskinleştirme yapılmış) hali Şekil 4.42.(a) 'da ve geri elde edilen logo görüntüleri Şekil 4.42.(b) ve (c) görülmektedir. Benzer işlemler Şekil 4.43, 4.44, 4.45'de Baboon, Barbara ve Peppers resimlerine uygulanmıştır. Çizelge 8'de PSNR değerleri verilmiştir.



(a) (b) (c)

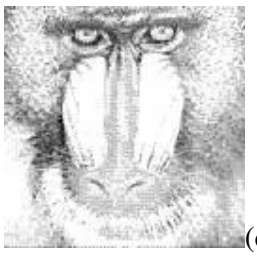
Şekil 4.42. (a) Kıvrım filtrelenmiş Lena görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen baboon logosu.


(a)

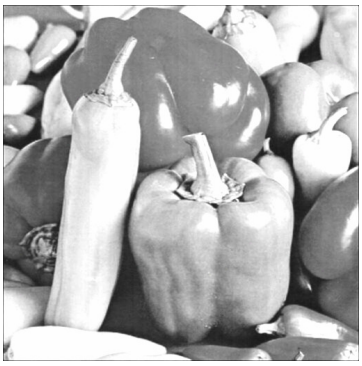

(b)

(c)

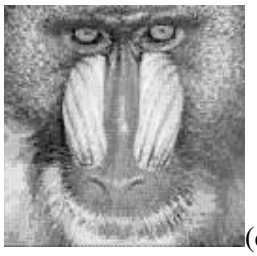
Şekil 4.43. (a) Kıvrım filtrelenmiş Baboon görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.


(a)


(b)

(c)

Şekil 4.44. (a) Kıvrım filtrelenmiş Barbara görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.


(a)


(b)

(c)

Şekil 4.45. (a) Kıvrım filtrelenmiş Peppers görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.

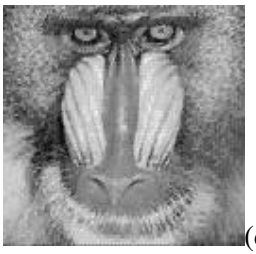
Çizelge 8. Kıvrım Filtreleme Sonucu Elde Edilen PSNR Değerleri (dB)

Orijinal Görüntü	Logo Görüntüsü	
	Lena	Baboon
Lena	11.0649	11.1231
Baboon	11.0544	10.9694
Barbara	8.4926	8.3554
Peppers	12.9059	12.8664

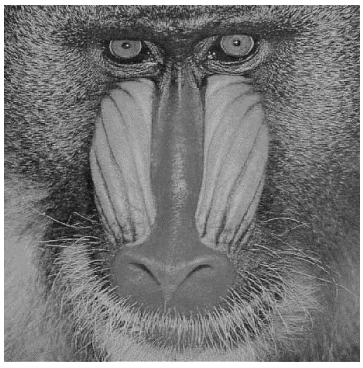
4.3.9. Görüntüden Satır Silme

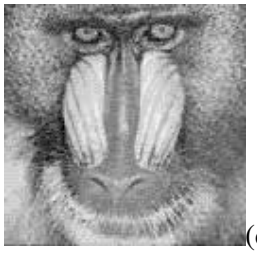
StirMark Benchmark ile filigranmış Lena görüntüsüne %10 satır silme uygulanmış görüntüsü Şekil 4.46(a) ve değiştirilmiş görüntü 512×512 piksele ölçeklenerek geri elde edilen logo görüntüleri Şekil 4.46(b) ve (c) de görülmektedir. Benzer işlemler Şekil 4.47, 4.48, 4.49'de Baboon, Barbara ve Peppers resimlerine uygulanmıştır. Çizelge 9'de PSNR değerleri verilmiştir.

 (a) 

(b)  (c)

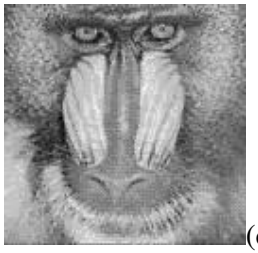
Şekil 4.46. (a) Satır silinmiş Lena görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.


(a)

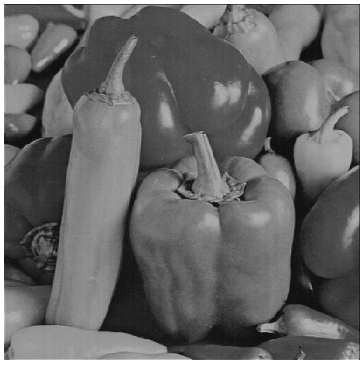

(b)

(c)

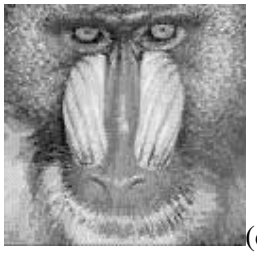
Şekil 4.47. (a) Satır silinmiş Baboon görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.


(a)


(b)

(c)

Şekil 4.48. (a) Satır silinmiş Barbara görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.


(a)


(b)

(c)

Şekil 4.49. (a) Satır silinmiş Peppers görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.

Çizelge 9. %10 Satır Silme Sonucu Elde Edilen PSNR Değerleri (dB)

Orijinal Görüntü	**Logo Görüntüsü**	
	Lena	**Baboon**
Lena	26.9819	26.7004
Baboon	19.8792	19.9876
Barbara	24.8795	24.0036
Peppers	20.1454	20.2066

Tekrar elde edilen logo resmi doğrulayıcı için anlamlıysa tam hak sahipliği doğrulanır. Lena görüntüsü yerine Şekil 4.50'daki airplane görüntüsünü kullandığımızda, filigranlarımız bazı saldırılara karşı hayatta kalsa da bir kısım saldırılara karşı başarısız olmaktadır. Şekil 4.51(a) gibi StirMark Benchmark ile Kıvrım filtrelenmiş (Gaussian filtreleme ve keskinleştirme yapılmış) görüntüden Şekil 4.51.(b) ve (c) görülen logolar geri elde edilip algılanabilirken, Şekil 4.52.(a)'deki gibi kırpma saldırısından sonra elde edilen Şekil 4.52.(b) ve (c)'deki logolar anlamsız olduğundan hak sahipliği doğrulanamamaktadır

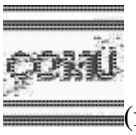
Şekil 4.50.Original Airplane görüntüsü.

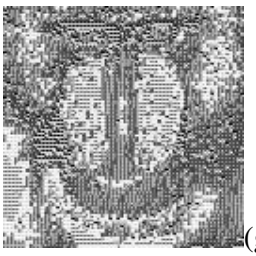
(b)


(c)

(d)

Şekil 4.51. (a) Kıvrım filtrelenmiş Airplane görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.

(e)


(f)

(g)

Şekil 4.52. (a) Kırpılmış Airplane görüntüsü, (b) geri elde edilen COMU logosu, (c) elde edilen Baboon logosu.

BÖLÜM 5
SONUÇ VE ÖNERİLER

Tüm yaptığımız deneyler sonucunda, telif hakkı koruma yöntemimizin sahip olduğu özellikleri aşağıda sıralayabiliriz:

Sağlamlık: Standart saldırılar altında, telif hakkı koruma yöntemi, JPEG sıkıştırma, bulanıklaştırma, gürültü ekleme, keskinleştirme, ölçekleme, döndürme, kırpma, kıvrım filtreleme, satır silme ve baskı-fotokopi-tarama saldırıları gibi çeşitli görüntü işleme ve geometrik döndürmelere karşı dayanıklıdır.

Saydamlık: Filigranlanan görüntü algısal olarak görünmemekle birlikte görüntüyü bozmamıştır. Filigranlanmış görüntünün kalitesi çok az kayıplıdır.

Güvenlik: Bu telif hakkı koruma tekniği güvenliği dijital imza ve dijital zaman damgasına dayanmaktadır. İmza ve zaman mührü için ticari teknolojiler mevcuttur.

Körlük: Çıkarma aşaması logo görüntüsünü elde etmek için orijinal görüntüye gerek duymaz. Pratikte, bu telif hakkı koruma programının önemli bir özelliğidir.

Çoklu filigranlama. Çoklu filigralama yönteminde, sondaki telif hakkı logosu öndeki telif hakkı logosunu engellememelidir. Bu yöntem farklı logo görüntüleri için sertifikalı indeks kümelerini ekleyerek çoklu logo görüntülerini destekleyebilir.

Belirlilik: İndeks kümesi sayısal imza teknolojisiyle korunduğundan, indeks kümesinin değişikliğine izin verilmez. Sayısal zaman mührü filigranlanmış görüntüye bir korsanın herhangi bir yasadışı telif hakkı logosu eklemesini önleyebilir. Yöntemimiz, telif hakkı logosunun gömülü olduğunu ayırt ederek çoklu sahiplik iddiaları problemini çözebilir.

Gri-seviye logo görüntüler: Sadece bir ikili patern değil, aynı zamanda gri seviye logo yöntemimizde bir filigran olarak işlenebilir. Gri-seviye görüntüsü ikili görüntüden daha uygundur ve birçok logo görüntüleri (ticari) pratikte gri seviye görüntü olduklarından geniş uygulama alanı vardır.

İnanç: İnsanlar algılama sonucundan ziyade tekrar elde edilen görsel tanınabilir telif hakkı logosunu üzerinden hüküm vermeye daha çok inanırlar.

Genel Doğrulama: Yöntemimizde hak sahibi açık anahtarlı altyapıya dayanan kişisel özel anahtar dışında herhangi bir gizli anahtar korumaya gerek duymaz. Bir kimse görüntünün hak sahipliğini doğrulamak istiyorsa, sadece hak sahibi ve CA'nın açık anahtarlarına ihtiyaç duyar.

StirMark Saldırıları: Deneylerimizdeki kullanılan değiştirilmiş görüntülerin çoğu

StirMark saldırılarına uğramış görüntüler olduğundan, önerilen yöntemin StirMark saldırılarına karşı başarıyla hayatta kaldığını söyleyebiliriz

Yöntemimizdede kayda değer başka avantajlarda vardır. İlk olarak, orijinal görüntüden daha büyük bir logo görüntüsü seçmek mümkündür. İkincisi, sağlamlık ile logo görüntüsünün kalitesi arasında, ve sağlamlık ile sertifika üretim/doğrulama aşamasının etkiliği arasında tercihe bağlı olarak ölçek seviyesini belirlenebilir.

Buna ek olarak, bir saldırganın zaman mührüyle birlikte bütün olası indeks kümelerini kaydetmesi ve daha sonra bu bahsedilen zaman mührüyle daha sonra kaydedilen herhangi bir görüntünün hak sahipliği iddiasında bulunması teorik olarak mümkündür. Ancak, pratikte bu gibi durumla karşılaşma olasılığı oldukça düşüktür. Kod kitabı boyutu k olsa da, k^l mümkün indeks kümeleri vardır. Deneylerimizde k=256 (512×512 piksellik orijinal görüntü) ve l=1024 (64×64 piksellik logo görüntüsü) olduğundan, $(256)^{1024}$ mümkün indeks kümesi oluşmaktadır. Dolayısıyla, bir saldırganın bir zaman mührüyle bu k^l olası indeks kümelerini kaydetmesi mümkün görünmemektedir. Önerilen yöntemde, algısal benzer iki farklı görüntü, aynı indeks kümesiyle birbirine çok benzeyen iki logo görüntüsü çıkarabilir. Bu zayıflığı önlemek için, LL_t alt bandı kod kelimelerine ayrılmadan önce sözde rastlantısal (pseudo-random) olarak değiştirilmelidir.

Telif hakkı korumanın güvenlik ve güvenilirliliği, şifreleme ve filigranlama tekniklerinin birlikte kullanılmasıyla yüksek düzeyde sağlanacaktır ve artacaktır. Bu fikre dayanarak, telif hakkı koruma yöntemizde, dalgacık dönüşümü, vektör kuantizasyonu, sayısal imza uygulaması gerçekleştrilmiştir.

Sonuç olarak, bu yöntem genel görüntü işleme ve kırpma, döndürme ve baskı-fotokopi-tarama gibi basit geometrik saldırıları karşı dayanıklı olmaktadır. Yukarıdaki tüm özellikler dikkate alındığında tez kapsamında önerilen yöntemin, klasik yöntemlere göre başarımının oldukça yüksek olduğu sonucu ortaya çıkmaktadır.

KAYNAKLAR

Arnold M., Schilz K.,2002. Quality Evaluation of Watermarked Audio Tracks. *Proceedings of Electronic Imaging, Security and Watermarking of Multimedia Contents IV*, Vol. 4675, San Jose, CA:SPIE : 91–101.

Arnold M., Schmucker M., Wolthusen S.D., 2003. *Digital Watermarking Techniques and applications of digital watermarking and content protection*. Boston, Artech House. 15-32.

Chang C.C., Hwang K.F., Hwang M.S., 1999. A block based digital watermarks for copy protection of images. Fifth Asia-Pacific Conference On Communications/Fourth Optoelectronics And Communications Conference, Beijing, China.

Chang C.C., Jau J.C., 1998. A fast reconstruction method for transmitting images progressively. IEEE Transactions on Consumer Electronics 44 (4), 1225–1233.

Chen T.S., Chang C.C., Hwang M.S., 1998. A virtual image cryptosystem based upon vector quantization. IEEE Transactions on Image Processing 7 (10).

Cox I.J., Kilian J., Leighton F.T., Shamoon T., 1997. Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing 6 (12), 1673–1687.

Cox I.J., Miller M.L., 2001. Electronic Watermarking: The First 50 Years. Published in the Proceedings of The IEEE 2001 Int. Workshop on MultiMedia Signal Processing.

Cox I.J., Miller M.L., Bloom J.A., 2002. *Models of Watermarking*: *Digital Watermarking*: 41-55.

Cox I.J., Miller M.L., Bloom J.A., Fridrich J., Kalker T., 2003. *Introduction to Digital Watermarking and Steganography* (2): 1-12.

Craver S., Memon N., Yeo B.L, Yeung M., 1997. Can invisible watermarks resolve rightful ownership. In: Proceedings of the SPIE Storage and Retrieval for Still Image and Video Databases V, vol. SPIE 3022, pp. 310–321.

Craver S., Yeo B.L., Yeung M., 1998. Technical trials and legal tribulations. Communications of the ACM 41 (7).

Holt L., Maufe B.G., Wiener A., 1988. Encoded Marking of a Recording Signal.*U.K. Patent* GB 2196167A,

Hsu C.T., Wu J.L., 1998. Multiresolution watermarking for digital images. *IEEE Transactions on Circuits and SystemII: Analog and Digital Signal Processing* 45 (8).

Hsu C.T., Wu J.L., 1999. Hidden Digital Watermarks in Images. *IEEE Transactions on Image Processing* 8 (1).

Koch E., Zhao J., 1995. Towards Robust and Hidden Image Copyright Labeling. *Proceedings of 1995 IEEE Workshop on Nonlinear Signal and Image Processing*, Neos Marmaras, Greece: 452–455.

Komatsu N., Tominaga H., 1988. Authentication System Using Concealed Images in Telematics. *Memoirs of the School of Science and Engineering, Waseda University,* 52: 45–60.

Kutter M., Voloshynovskiy S., Herrigel A., 2000. The watermark copy attack. *Proceedings of SPIE: Security and Watermarking of Multimedia Contents* II San Jose, CA, 3971.

Lin S., Costello D. J., (1983, *Error Control Coding: Fundamentals and Applications*, Prentice-Hall Series in Computer Applications in Electrical Engineering, Englewood Cliffs, NJ: Prentice Hall.

Lu C.S., Huang S.K., Sze C.J., Liao H.Y., 2000. A new watermarking technique for multimedia protection.*Multimedia Image and Video Processing.* CRC Press, Boca Raton.

Niu X.M., Lu Z.M., Sun S.H., 2000. Digital watermarking of stil images with gray-level digital watermarks. IEEE Transactions onConsumer Electronics 46 (1).

Pan D.,1995. A Tutorial on MPEG / Audio Compression. *IEEE Multimedia* 2 (2): 60–74.

Pan J.S., Huang H.C, Jain L.C., 2004. Watermarking Based on Spatial Domain. *Intelligent Watermarking Techniques* : 135-147.

Petitcolas F.A., Anderson R.J., Kuhn M.G., 1999. Inforamtion hiding a survey. Proceedings of the IEEE special issue on protection of multimedia contents.

Proakis J. G., Manolakis D. M., 1992. *Digital Signal Processing: Principles, Algorithms and Applications(2*), Basingstoke, U.K.: Macmillan Publishing Company.

Oğuz C., 2006. Görüntü İşrateleri İçin Yeni Bir Sayısal Damgalama Yöntemi (Yüksek Lisans Tezi), İstanbul Üniversitesi, İstanbul, Türkiye.

Schneier B., 1996.Foundations. *Applied Cryptography*(2). Wiley, New York.: 15-32

Seitz J., 2005, Digital Watermarking: An Introduction. *Digital Watermarking For Digital Media* : 1-29.

Shapiro J.M., 1993. Embedded image coding using zerotrees of wavelet coefficients. Signal Processing IEEE Transactions on Signal Processing 41 (12), 3445–3462.

Singh V., 2011. Digital Watermarking: A Tutorial. *Cyber Journals: Multidisciplinary*

Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), January Edition.

Stollnitz E.J., DeRose T.D., Salesin D.H., 1995. Wavelets for computer graphics: a primer. IEEE Computer Graphics and Applications.

Wang H.J., Kuo C.C., 1997. A multi-threshold wavelet coder for high fidelity image compression. Proceedings International Conference on Image Processing 1, 652–655.

Wei-Bin L., Tung-Her C., 2002. A Public Verifiable Copy Protection Technique for Still Images. *The Journal of Systems and Software 62* (3): 195-204.

Wikipedia *Peak signal-to-noise ratio.* (b.t.). Retrieved May 8, 2011, from http://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio

ÇİZELGELER **Sayfa No**

ŞEKİLLER **Sayfa No**

ÖZGEÇMİŞ

1978 yılında Kahramanmaraş'ın Elbistan ilçesinde doğdu. 1996 yılında Elbistan Analolu Lisesinden mezun oldu ve aynı yıl Karadeniz Teknik Üniverisitesi Biligisayar Mühendisliği bölümünü kazandı. 2001 yılında üniveriteden mezun olduktan sonra 2004 yılına kadar çeşitli özel şirketlerde Bilgisayar Mühendisi olarak çalıştı. 2004-2005 yıllarında yedek subay olarak vatani görevini tamamladıktan sonra Eskişehir Büyükşehir Belediyesinde işe başladı ve 1,5 sene kadar Bilgisayar Mühendisi olarak çalıştıktıktan sonra ayrıldı. 2007 sonbaharında Kıyı Emniyeti Genel Müdürlüğünde Bilgisayar Mühendisi olarak işe başladı ve halen bu Kurumda çalışmaktadır.

Kişisel Bilgiler:

Adres: TOKİ 960 Konutları
C13 Blok D:17
Kepez/ÇANAKKALE

Tel :0544 717 93 39

E-posta: gurlekr@hotmail.com