



T.C.
KONYA TEKNİK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ



NFT'LERİN VIDEO FİLİGRANLAMADA KULLANIMI

Ibrahima Sory CAMARA

YÜKSEK LİSANS TEZİ

Bilgisayar Mühendisliği Anabilim Dalı

Temmuz-2023
KONYA
Her Hakkı Saklıdır

TEZ KABUL VE ONAYI

Ibrahima Sory CAMARA tarafından hazırlanan “Nft’lerin Video Filigranlamada Kullanımı” adlı tez çalışması 05/07/2023 tarihinde aşağıdaki jüri tarafından oy birliği ile Konya Teknik Üniversitesi Lisansüstü Eğitim Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı’nda YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Jüri Üyeleri**İmza****Başkan**

Doç. Dr. Mehmet Akif ŞAHMAN

.....

Danışman

Prof. Dr. İsmail BABAOĞLU

.....

Üye

Dr. Öğr. Üyesi Alper KILIÇ

.....

Yukarıdaki sonucu onaylarım.

Prof. Dr. Mevlüt UYAN
Enstitü Müdürü

TEZ BİLDİRİMİ

Bu tezdeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edildiğini ve tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

DECLARATION PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Ibrahima Sory CAMARA

Tarih: 05.07.2023

ÖZET**YÜKSEK LİSANS TEZİ****NFT'LERİN VIDEO FİLİGRANLAMADA KULLANIMI****Ibrahima Sory CAMARA**

**Konya Teknik Üniversitesi
Lisansüstü Eğitim Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı**

Danışman: Prof. Dr. İsmail BABAOĞLU**2023, 124 Sayfa****Jüri**

**Prof. Dr. İsmail BABAOĞLU
Dr. Öğr. Üyesi Alper KILIÇ
Doç. Dr. Mehmet Akif ŞAHMAN**

Bu çalışmada, NFT uygulamaları için özel olarak tasarlanmış yeni bir video filigran algoritması sunulmaktadır. Önerilen algoritma, video içeriğine filigran yerleştirmek amacıyla tasarlanmış ve ardından filigranın bütünlüğünü ve direncini değerlendirmek için çeşitli saldırılara karşı test edilmiştir.

Önerilen algoritmanın performansı, sıkıştırma, geometrik, zamanlı, filtreleme, gürültü ekleme ve kuantizasyon saldırıları gibi kapsamlı bir saldırı setine karşı değerlendirilmiştir. Sonuçlar, algoritmanın farklı saldırılara karşı değişen direnç seviyeleri gösterdiğini ve filigranın sağlamlığını etkileyen bazı zayıf noktaların olduğunu göstermektedir. Özellikle, H.264 (aynı ayarlarla) ve Huffvuv gibi kayıplı ve kayıpsız sıkıştırma yöntemlerine ve Wiener filtresi gibi frekans alanı filtreleme saldırılarına karşı başarılıdır.

Bu çalışmanın bulguları, NFT uygulamaları için daha sağlam video filigran tekniklerinin geliştirilmesi için değerli içgörüler sunmaktadır. Önerilen algoritma, özellikle NFT'ler bağlamında dijital dünyada video içeriğini güvence altına almak için umut verici bir potansiyele sahiptir. NFT önce oluşturulur, ardından meta verileri eklenir, benzersiz jeton URI'si belirlenir ve NFT OpenSea platformuna yüklenir. Daha sonra belirli bir NFT'nin URL (Tekdüzen Kaynak Bulucu)'si seçilen bir videonun karelerinin içine gömülür. Video sahibini belirlemek için, kareler videodan çıkarılır ve URL'ler karelerden çıkarılır, ardından birbiriyle karşılaştırılarak mükemmel bozulmamış URL elde edilir. Bu URL bizi OpenSea'deki NFT'ye yönlendirir ve orada tüm bilgiler saklanır.

Anahtar Kelimeler: Blok zinciri, Takas Olmayan Jetonlar (NFT), Dijital varlık koruması, Fikri mülkiyet hakları, Multimedya güvenliği, Video filigranlama.

ABSTRACT**MS THESIS****APPLICATION OF NFTS IN VIDEO WATERMARKING****Ibrahima Sory CAMARA****Konya Technical University
Institute of Graduate Studies
Department of Computer Engineering****Advisor: Prof. Dr. İsmail BABAOĞLU****2023, 124 Pages****Jury****Prof. Dr. İsmail BABAOĞLU
Dr. Öğr. Üyesi Alper KILIÇ
Doç. Dr. Mehmet Akif ŞAHMAN**

In this study, we present a novel video watermarking algorithm specifically designed for NFT applications. The proposed algorithm was designed with the intent to embed watermarks in video content and was subsequently tested against various attacks to evaluate the integrity and resilience of the watermark.

The performance of the proposed algorithm was evaluated against a comprehensive set of attacks, including compression, geometric, temporal, filtering, noise addition, and quantization attacks. The results indicate that the algorithm demonstrates varying levels of resilience to different attacks, with some areas of vulnerability that impact the robustness of the watermark. Notably, it is successful against lossy and lossless compression methods, such as H.264 (with the same settings) and Huffvuv, and frequency-domain filtering attacks, such as the Wiener filter.

The findings of this study provide valuable insights for the development of more robust video watermarking techniques for NFT applications. The proposed algorithm demonstrates promising potential for securing video content in the digital world, particularly in the context of NFTs. The NFT is first created, then its metadata is added, its unique token uri is set and then the NFT is deployed on the OpenSea platform. The URL of the specific NFT is then embedded inside the frames of a selected video. To know the owner of the video, the frames are extracted from the video and the URLs are extracted from the frames and compared with each other in order to get the perfect uncorrupted URL which will lead us to the NFT on OpenSea where all the information is stored.

Keywords: Blockchain, Digital asset protection, Intellectual property rights, Multimedia security, Non-fungible token (NFT), Video watermarking.

ÖNSÖZ

Tez arařtırmam süresince verdiđi destek ve rehberlik için danıřmanım Doç. Dr. İsmail Babaođlu'na en derin řükranlarımı sunuyorum. Ayrıca Konya Teknik Üniversitesi Mühendislik ve Dođa Bilimleri Fakültesi Bilgisayar Mühendisliđi Bölümü öğretim üyelerine deđerli görüşleri için teşekkür ederim.

Anneme sürekli sevgisi ve benim yeteneklerime olan inancı için minnettarım, aynı zamanda bu yolculuk boyunca arkadaşlarıma ve akranlarıma arkadaşlık için teşekkür ederim. Bu kişiler, akademik ve kişisel gelişimimde önemli bir rol oynamışlardır ve desteđe olan takdirim daima sürecektir.

Ibrahima Sory CAMARA
KONYA-2023



İÇİNDEKİLER

ÖZET	3
ABSTRACT.....	4
ÖNSÖZ	5
SİMGELER VE KISALTMALAR	8
1. GİRİŞ.....	1
2. KAYNAK ARAŞTIRMASI	6
2.1. Takas Olmayan Jetonlar (NFT'ler): Evrim ve Uygulamalar.....	6
2.1.1. Nft'lerin ortaya çıkışı	6
2.1.2. Nft'lerin dijital sanatlarda ve ötesindeki kullanımı	7
2.2. Dijital Filigranlama Teknikleri ve Video İçeriğinde Görünmez Filigranlama	8
2.2.1. Spatial alanında video filigranlama	8
2.2.2. Dönüşüm alanında video filigranlama.....	11
3. MATERYAL VE YÖNTEM.....	15
3.1 Blok Zinciri (Blockchain).....	15
3.1.1 Blok zinciri yapısı	16
3.1.2 Konsensüs algoritmaları	19
3.1.3 Zorluklar ve son gelişmeler	25
3.2. Takas Olmayan Jetonlar.....	28
3.2.1. Protokoller	31
3.2.2. Jeton standartları	33
3.2.3. NFT'lerde istenen özellikler.....	35
3.2.4. Güvenlik değerlendirmesi	36
3.2.5. Güvenlik ve gizlilik sorunları	38
3.2.6. Genişletilebilirlik sorunları	39
3.3. Video ve Dijital Filigranlama	40
3.3.1 Filigranlamanın gerekliliği	40
3.3.2. Filigranlama gereksinimleri.....	42
3.3.3. Korelasyon temelli filigranlama teknikleri: mekansal alan temel tekniği	46
3.3.4. Bir görüntüye birden fazla bit veya logo gömme uzantıları	50
3.3.5. Dönüşüm alanları için teknikler.....	55
3.3.6. Geometrik dönüşümleri önceden tahmin etme	64
3.3.7. Korelasyon tabanlı filigranlama.....	68
3.3.8. Korelasyon tabanlı olmayan filigranlama teknikleri	71
3.3.9. Parite bit değiştirme ile mpeg video filigranlama.....	72
3.3.10. DCT katsayısı sıralaması	73
3.3.11. DEW algoritması kullanarak MPEG video filigranlama.....	74
3.3.12. Belirgin nokta modifikasyonu	77
3.3.13. Fraktal tabanlı filigranlama.....	78
3.4. NFT Oluşturma	78
3.4.1. NFT sözleşmesini kullanıma sunma:	80
3.4.2. Rastgele sayı üretici entegrasyonu:	80

3.4.3. Koleksiyon parçaları oluşturma:	80
3.4.4. Meta veri üretme:	80
3.4.5. Meta verileri ve görselleri IPFS'ye yükleme (isteğe bağlı):	80
3.4.6. Jeton URI'sini ayarlama:	81
3.4.7. NFT'yi bir pazarda gösterme:	81
3.5. Video ve Ses İşleme.....	81
3.5.1 Video işleme	81
3.5.2. Ses işleme	83
3.6. Tüm Video Karelerine NFT Gömme:.....	84
3.7. Karelere ve Ses Dosyasına Videoyu Yeniden Birleştirme:	86

4. ARAŞTIRMA SONUÇLARI VE TARTIŞMA..... 88

4.1 Sonuçların Genel Bakışı	89
4.2. Her Saldırının Detaylı Analizi	91
4.2.1. Orjinal filigranlı saldırısız.....	92
4.2.2. Renk nicemleme saldırıları	92
4.2.3. Palet tabanlı nicemleme gif (256 renk).....	94
4.2.4. Alt örnekleme saldırıları	94
4.2:0 alt örnekleme saldırısı.....	94
4.2.5. Sıkıştırma saldırıları.....	96
4.2.6. Kopyalama saldırısı	96
4.2.7. Sıkıştırma saldırıları CRF30 ve CRF50.....	97
4.2.8. Kayıpsız sıkıştırma saldırısı ffv1	98
4.2.9. Kare ortalama saldırısı	99
4.2.10. Kare ekleme saldırısı	100
4.2.11. Kare hızı değiştirme saldırıları (FPS 15, FPS 20, FPS 25).....	100
4.2.12. Whatsapp sıkıştırma saldırısı	101
4.2.13. Mekansal filtre saldırısı: Gaussian bulanıklık	102
4.2.14. Gürültü eklenmesi saldırısı: Gaussian gürültü.....	103
4.2.15. Frekans alanı filtreleme saldırısı: yüksek geçiren filtre.....	103
4.2.16. Kayıpsız sıkıştırma saldırısı Huffvuv	104
4.2.17. Zamansal saldırılar: kare ekleme (30)	104
4.2.18. Sıkıştırma saldırısı libx265 CRF28.....	105
4.2.19. Sıkıştırma saldırısı libx265 CRF28 yuv420p.....	105
4.2.20. Sıkıştırma saldırısı libx265	105
4.2.21. Frekans alanı filtreleme saldırısı: düşük geçiren filtre.....	105
4.2.22. Frekans alanı filtreleme saldırısı: medyan filtresi.....	106
4.2.23. Örnek en-boy oranı saldırısı: 2*SAR.....	106
4.2.24. Ters oynatma saldırısı	106
4.2.25. Wiener filtre saldırısı	106

5. SONUÇLAR VE ÖNERİLER..... 108

KAYNAKLAR 110

SİMGELER VE KISALTMALAR

Kısaltmalar

3B-DWT	: Üç Boyutlu Ayrık Dalgacık Dönüşümü
ABD	: Amerika Birleşik Devletleri
AAC	: Gelişmiş Ses Kodlaması
AVI	: Ses Video Ara Bölmesi
BGR	: Mavi Yeşil Kırmızı (bir renk formatı)
BER	: Bit hata oranı
CD	: Kompakt Disk
CDMA	: Kod Bölmeli Çoklu Erişim
CRF	: Sabit Oran Faktörü
dBFT	: Yetkilendirilmiş Bizans Hata Toleransı
DCT	: Ayrık Kosinüs Dönüşümü
DCT-AC	: Ayrık Kosinüs Dönüşümü - Gelişmiş Video Kodlama
DEW	: Diferansiyel Enerji Filigranı
DFT	: Ayrık Fourier Dönüşümü
DS-CDMA	: Doğrudan Sıralı Kod Bölmeli Çoklu Erişim
DPOS	: Delege Edilmiş Hisse Kanıtı
DVD	: Dijital Çok Yönlü Disk
DWT	: Ayrık Dalgacık Dönüşümü
EIP-721	: Ethereum İyileştirme Önerileri No. 721
EIP-1155	: Ethereum İyileştirme Önerileri No. 1155
FFT	: Hızlı Fourier Dönüşümü
FPS	: Saniye Başına Kare Sayısı
GHOST	: Açgözlü En Ağır Gözlenen Alt-Ağacı
HEVC	: Yüksek Verimli Video Kodlama (H.265)
HH	: DWT'nin yüksek-yüksek bandı
HL	: DWT'nin yüksek-düşük bandı
HVS	: İnsan Görsel Sistemi
IFPI	: Uluslararası Fonografik Endüstrisi Federasyonu
IP	: Fikri Mülkiyet
IPFS	: Gezegenlerarası Dosya Sistemi
ISBN	: Uluslararası Standart Kitap Numarası
ISRC	: Uluslararası Standart Kayıt Kodu
JSON	: JavaScript Nesne Gösterimi
JPEG	: Ortak Fotoğraf Uzmanları Grubu
libx264	: Bir H.264 video kodlayıcı kütüphanesi
libx265	: Bir H.265/HEVC video kodlayıcı kütüphanesi
LH	: DWT'nin düşük-yüksek bandı
LL	: DWT'nin düşük-düşük bandı
LPM	: Log Polar Map
LSB	: En Az Anlamlı Bit
MKV	: Matroska Video
MPEG	: Hareketli Görüntü Uzmanları Grubu
MP4	: MPEG-4 Bölüm 14
MSE	: Ortalama Kare Hatası
NFT	: Takas Olmayan Jetonlar (Non Fungible Token)
PBFT	: Pratik Bizans Hata Toleransı
PCM	: Darbe Kodu Modülasyonu

PNG	: Taşınabilir Ağ Grafikleri
PoS	: Hisse Kanıtı
PoW	: İş Kanıtı
PSNR	: En yüksek Sinyal-Gürültü Oranı
SAR	: Örnek En Boy Oranı
SCP	: Stellar Mutabakat Protokolü
SVD	: Tekil Değer Ayrışımı
SURF	: Hızlandırılmış Güçlü Özellikler
UNL	: Benzersiz Düğüm Listesi
URI	: Tekdüzen Kaynak Tanımlayıcı
URL	: Tekdüzen Kaynak Bulucu
VLC	: Değişken Uzunluk Kodlaması
VP9	: Google tarafından sunulan WebM video formatı
VRF	: Doğrulanabilir Rastgele Fonksiyonu
YUV	: Renk temsil model
Yuv420p	: 4:2:0 kroma alt örnekleme YUV renk uzayı



1. GİRİŞ

Dijital çağ, dijital içerik üretimi ve tüketiminde eşi benzeri görülmemiş bir patlamaya neden olmuş, ayrıca iletişim, öğrenme ve eğlence biçimimizi değiştirmiştir. İnternetin gelişmeye devam etmesiyle birlikte, görüntüler, müzik ve video içerik gibi dijital varlıklar giderek değerli hale gelmiş, doğrulama ve fikri mülkiyet hakları konusunda sorular ortaya çıkarmıştır. Bu yüzden de dijital varlıklara değer ve sahiplik durumunda şeklimizi değiştirebilecek sanat, müzik, oyunlar ve video içerik gibi çeşitli alanları kapsayan devrim niteliğinde bir yenilik olan takas olmayan jetonlar (NFT'ler) dünyası devreye girmektedir. NFT piyasasının hızla genişlemesi, güvenli ve verimli bir şekilde NFT'leri video içeriklerini entegre edebilmek, görsel kaliteyi veya kullanıcı deneyimine zarar vermeden kullanılabilir.

Bu çalışma, görünmez filigranlama tekniklerinin video içerikte takas olmayan jetonlarını örtmek için cezbedici alanına derinlemesine inerek dijital varlıkların korunması, sahiplik atfı ve blok zinciri teknolojisinin çoklu ortam platformlarıyla sorunsuz entegrasyonunun kapılarını açmaktadır. Amaç, yaratıcıları güçlendirmek, fikri mülkiyetlerini korumak ve hızla değişen dijital ortamda para kazanma ve tanınma için yeni fırsatlar yaratmaktır.

Takas olmayan jetonlar (NFT'ler), genellikle bir sanat eseri, müzik parçası, koleksiyon eşyası veya satın alma kanıtından nadir posta pulları, gayrimenkul ve fiziksel sanat eserleri gibi çeşitli varlıklar değerli öğelerin benzersizliğini sertifikalandıran blok zincirinde depolanan veri parçalarıdır (Cornelius, 2021; Wang ve ark., 2021). NFT'ler, dijital varlık olarak işlem yapılabilirliği nedeniyle son yıllarda büyük ilgi görmektedir. Ethereum gibi bir jeton standardı blok zinciri olan akıllı sözleşmeler, kullanılarak ödeme ve varlık transferi otomatikleştirilerek, karşılıklı birbirine güvenmeyen taraflar arasında tek bir işlemde takas edilebilirler (Khati ve ark., 2022).

Ethereum bağlamında, hesaplar arasında değer ve bilgi transferi, blok zinciri defterinin küresel durumuna kaydedilen bir işleme yol açar. Tipik olarak standart değiştirilebilir para birimi olarak Ether (ETH) gibi yerel bir jeton kullanılır. Ethereum topluluğu tarafından tanıtılan ERC-721 standardı, NFT'ler oluşturmak için en yaygın kullanılan standartlardan biridir ve piyasayı hâlâ domine etmektedir (Khati ve ark., 2022).

NFT'lerin bilinebilirliği, dijital sanatların tanıtılmasından sonra artmıştır. CryptoKitties ve CryptoPunks gibi koleksiyonlar ilk olarak dijital sanat NFT'leri olarak tanınmışlardır (Khati ve ark., 2022). 2021 yılında Ethereum ağı, sadece NFT'ler için

günlük olarak bir milyondan fazla işlem kaydetmiştir. OpenSea gibi NFT pazarları, toplamda 20 milyar doları aşan satış hacmi elde etmiştir ve NFT koleksiyonlarının toplam piyasa değeri Nisan 2022'de yaklaşık olarak 13.492.390.000 doları bulmuştur (Khati ve ark., 2022).

Dijital sanatlar dışında, çeşitli NFT türlerine olan ilgi artmış olup, Hyperledger, Solana ve Multichain gibi diğer blok zinciri platformları NFT uyumlu yükseltmeler geliştirmiş ve bu mevcut merkezi olmayan pazarları etkileyerek gelecekteki uygulama fırsatlarını artırmıştır. Ancak, NFT piyasasının hızla büyümesine rağmen, bu alanda akademik araştırma geri planda kalmıştır (Khati ve ark., 2022).

Dijital çağ, bilgisayar teknolojilerindeki ilerlemeler, ağlar ve Moore'un yasası sayesinde görüntü, ses ve video dosyaları gibi multimedya içeriklerin oluşturulması, depolanması ve yayılmasında önemli bir artışa yol açmıştır (Eldering ve ark., 1999). İnternet aynı zamanda multimedya bilgilerinin kolayca değiş tokuş edilmesine olanak sağlamış, insanların istedikleri gibi video kopyalamasını, işlemesini ve iletmesini mümkün kılmıştır (Yu ve ark., 2018). Bununla birlikte, bu kolaylık aynı zamanda korsanlık, ihlal ve hırsızlık gibi zorluklara da yol açmıştır. Bu durum yalnızca fikri mülkiyet haklarını ihlal etmekle kalmamış, aynı zamanda video endüstrisinin sağlıklı gelişimini de tehlikeye atmıştır (Wolfgang ve ark., 1999).

Kriptografi gibi geleneksel telif hakkı koruma teknolojileri, şifrelenmiş veriler çözüldüğünde fikri mülkiyet haklarını etkin bir şekilde izlemekte ve onaylamada sınırlamaları olduğu için dijital ürünleri korumada yetersiz kalmaktadır. Bu soruna bir yanıt olarak, steganografi, dijital filigranlama ve gizli iletişim gibi bilgi gizleme teknolojileri, geçerli bir alternatif olarak ortaya çıkmıştır (Jung, 2016).

Bilgi gizleme teknolojisinin önemli bir dalı olan dijital filigranlama, dijital ürünler için telif hakkı koruma sorunlarını çözebilecek potansiyele. Telif hakkı veya kimlik doğrulama bilgisi gibi görünmez işaretlerin dijital içeriklere gömülmesiyle yetkisiz kullanıcılar gizli bilgiyi algılayamazlar, böylece telif hakkı koruması sağlanır. Dijital filigranlama teknolojisi zaman içinde evrim geçirmiş ve uygulamaları hâlihazırda statik dijital görüntülerden video, ses ve belgelere kadar genişlemiştir. Video içeriğinin İnternet üzerinde bilgi aktarımının baskın formu haline gelmesiyle birlikte, video filigranlama teknolojisi önemli bir araştırma alanı haline gelmiştir (Yu ve ark., 2018).

Filigranlar, dayanıklı, kırılabilir ve yarı kırılabilir olmak üzere üç kategoriye ayrılmaktadır (Verma ve Jha, 2015). Dayanıklı filigranlar çeşitli saldırılara karşı dirençlidir ve genellikle telif hakkı koruması için kullanılır. Öte yandan, kırılabilir

filigranlar müdahale saldırılarına karşı hassastır ve içerik doğrulama ve müdahale tespiti için kullanılmaktadır. Yarı kırılğan filigranlar ise dayanıklı ve kırılğan filigranların avantajlarını bir araya getirerek, yaygın sinyal işleme operasyonlarını kötü niyetli saldırılardan ayırabilir.

Dijital filigranlama teknikleri, görüntü, ses ve belgeler gibi çeşitli multimedya içeriği telif hakkı koruması için kapsamlı bir şekilde araştırılmış olsa da, takas olmayan jetonların (NFT'ler) doğrudan video içeriğine gömülmesi konusunda sınırlı araştırma yapılmıştır. Benzersiz ve bölünemez dijital varlıklar olarak NFT'ler, yaratıcı endüstride önemli bir ivme kazanmış ve sahiplik ve değer atfetme şeklini değiştirecek potansiyele sahiptir. Ancak, video içeriğine görünmez bir filigran olarak NFT koyulması konusunda mevcut araştırma eksikliği açıkça ortadadır. Bu boşluk, video içeriğinin görsel kalitesini korurken sahiplik atfını güvenli ve verimli bir şekilde sağlamak için yeni yöntemlerin geliştirilmesini gerektirmektedir. Bu araştırma boşluğuna cevap vermek, içerik oluşturuculara, NFT pazar yerlerine ve diğer paydaşlara dijital varlıklarını genişletmek ve dijital ekosistemde daha iyi koruma ile yönetim imkanı sunacaktır.

Bu tez, NFT'yi video içeriğine yerleştirmek için mevcut yöntemlerin eksikliğini gidermeyi ve hızla büyüyen NFT pazarında dijital varlıkları koruyan ve dijital video içeriğinin orijinalliğini sağlayan yenilikçi çözümlerin geliştirilmesine katkıda bulunmayı amaçlamaktadır.

Araştırma sorusunu etkili bir şekilde ele almak için özel hedefler aşağıda belirtilmiştir.

- Önerilen NFT filigranlama algoritmasının bir prototipini uygulamak ve bunu video içeriğine NFT ekleme ve çıkartma için bir sisteme entegre etmek.

- Önerilen NFT filigranlama algoritmasının performansını çeşitli koşullar altında ve saldırı senaryolarında deneyler yaparak değerlendirmek, dayanıklılığını, algılanamazlığını ve çıkartma doğruluğunu değerlendirmek.

- Değerlendirme süreci sırasında belirlenen herhangi bir sınırlamayı ele almak için önerilen NFT filigranlama algoritmasına yönelik ileriye dönük araştırma önerileri ve potansiyel iyileştirmeler sunmak.

Bu hedefler, araştırma sorusuyla uyumlu olup, NFT'lerin video içeriğine filigranlama alanında yenilikçi çözümlerin geliştirilmesine katkıda bulunmayı amaçlamaktadır.

Bu çalışmamızda yürütülen araştırma, görünmez filigranlama tekniklerini kullanarak NFT'leri video içeriğine gömmek için yenilikçi bir çözüm geliştirerek dijital ekosisteme etki etmektedir. Bu araştırmanın önemi aşağıda açıkça belirtilmiştir:

Fikri Mülkiyet Haklarının Korunması: Dayanıklı ve algılanamaz bir NFT filigranlama algoritması geliştirerek, bu araştırma içerik oluşturucuların fikri mülkiyet haklarının korunmasına katkıda bulunacak, çalışmalarının doğru atıf ve tazminatını almalarını sağlayacaktır.

Dijital Korsanlıkla Mücadele: Önerilen NFT filigranlama tekniği, içerik sahiplerinin korsan kopyaların kökenini izlemesini ve doğrulamasını sağlayarak dijital korsanlığı ve yetkisiz video içeriği dağıtımını engellemeye yardımcı olur, böylece dijital video pazarının genel güvenliğini güçlendirir.

NFT Piyasasında Güven ve Otantiklik Oluşturma: Video içeriğine güvenli ve verimli bir şekilde NFT gömmenin bir yöntemi, hızla büyüyen NFT piyasasında güven ve otantiklik oluşturmaya yardımcı olmak, böylece çeşitli endüstrilerde benimsenmesini teşvik etmektedir.

Yeni uygulamaların ve hizmetlerin geliştirilmesini teşvik etme: Önerilen NFT filigranlama algoritması, NFT'ler, dijital içerik yönetimi ve telif hakkı korumasıyla ilgili yeni uygulamaların ve hizmetlerin geliştirilmesinin yolunu açabilir, böylece dijital ekosistemde yenilik ve ekonomik büyümeyi teşvik eder.

Dijital filigran alanını geliştirme: Bu araştırma konusu, NFT'lerin video içeriğine filigranlama alanındaki araştırma boşluğunu ele alarak, daha geniş bir dijital filigranlama alanına katkıda bulunacak ve bu alanda gelecekteki araştırmaları ve teknolojik ilerlemeleri bilgilendirebilecek değerli bilgiler ve bulgular sunacaktır.

Genel olarak, bu araştırmanın önemi dijital varlıkların daha etkili bir şekilde korunmasına ve yönetilmesine, NFT piyasasının büyümesine katkıda bulunmasına ve dijital ekosistemde yenilikleri teşvik etmesine dayanmaktadır.

Okuyucuyu yönlendirmek ve tez için net bir yapı sağlamak amacıyla aşağıdaki taslak, ana bölümleri ve bölümleri sunmaktadır:

Giriş: Araştırma konusunu tanıtır, arka plan bilgisi sağlar, araştırma boşluğunu belirler, araştırma sorusunu ve hedeflerini belirtir, metodolojiyi açıklar, araştırmanın önemini vurgular ve tezin bir taslağını sunar.

Literatür İncelemesi: Dijital filigranlama teknikleri, NFT'ler ve telif hakkı korumasında uygulamaları hakkındaki mevcut literatürü gözden geçirir, özellikle multimedya içerikte filigranlama tekniklerine odaklanır.

NFT Filigranlama Algoritması Tasarımı: Önerilen görünmez NFT filigranlama algoritmasının tasarımını ve geliştirilmesini, ana bileşenlerini, prensiplerini ve video içeriğine NFT'lerin gömülmesi ve çıkarılması için kullanılan teknikleri açıklar.

Uygulama Sistemi: Önerilen NFT filigranlama algoritmasının uygulanmasını, video içeriğine NFT'lerin gömülmesi ve çıkarılması için bir sisteminin geliştirilmesini sunmaktadır.

Performans Değerlendirmesi ve Analizi: Önerilen NFT filigranlama algoritmasının performansını değerlendirmek için çeşitli koşullar ve saldırı senaryoları altında deneyler yapar, dayanıklılığını, algılanamazlığını ve çıkarım doğruluğunu değerlendirir.

Öneriler ve Gelecek Araştırmalar: Önerilen NFT filigranlama algoritmasının potansiyel sınırlamalarını belirler ve bu sınırlamaları ele almak için gelecek araştırmalar ve iyileştirmeler için öneriler sunmaktadır.

Sonuç: Araştırmanın temel bulgularını özetler, araştırmanın önemini tekrar vurgular ve tezi sonlandırır.

Bu tezin yapısı, giriş, literatür taraması, önerilen NFT filigranlama algoritması tasarımı, uygulama sistemi, performans değerlendirme, öneriler ve telif hakkı koruması için multimedya içeriğinde görünmez NFT filigranlama araştırması için sonucu içerir.

Bu taslak, araştırmanın düzenli, tutarlı ve anlaşılabilir bir şekilde organize edilmesini sağlayarak tez için bir yol haritası görevi görmektedir.

2. KAYNAK ARAŞTIRMASI

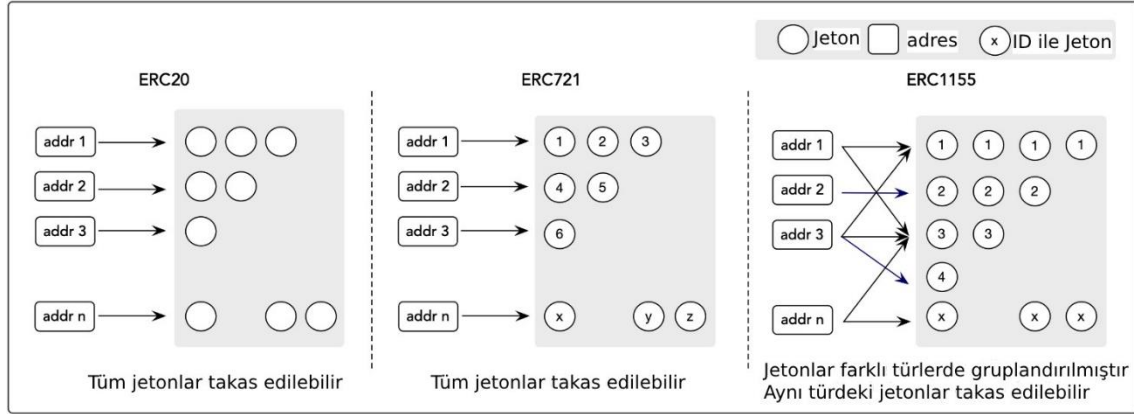
Bu literatür taramasında, Takas Olmayan Jetonlar (NFT'ler), dijital filigranlama teknikleri ve video içeriği bağlamında görünmez filigranlama alanındaki mevcut ve eski araştırmalar ve gelişmeler tartışılacaktır. Araştırma, NFT'lerin temel programlarına, gelişimlerine ve sundukları zorluklara odaklanacak ve ardından dijital filigranlama tekniklerini ve uygulamalarını analiz edecektir.

2.1. Takas Olmayan Jetonlar (NFT'ler): Evrim ve Uygulamalar

2.1.1. Nft'lerin ortaya çıkışı

NFT kavramı, Kevin McCoy ve Anil Dash'in 2014 Mayıs'ında ilk NFT'yi geliştirdiği zaman ortaya çıkmıştır. Ayrıca, NFT, Ethereum blok zinciri konsorsiyumu tarafından Ethereum ERC-721 standardının önerilmesiyle 2017 yılında daha geniş araştırma yapılarak netlik kazanmıştır. NFT'lerin dijital sanatlarda ilk başarılı uygulamalarından biri olan CryptoKitties, önemli bir yer edinmiştir. Bu dönemde NFT'lerin hızlı gelişimi, çeşitli bloglar, YouTube videoları ve web makaleleri aracılığıyla belgelenmiştir. (Khati ve ark., 2022).

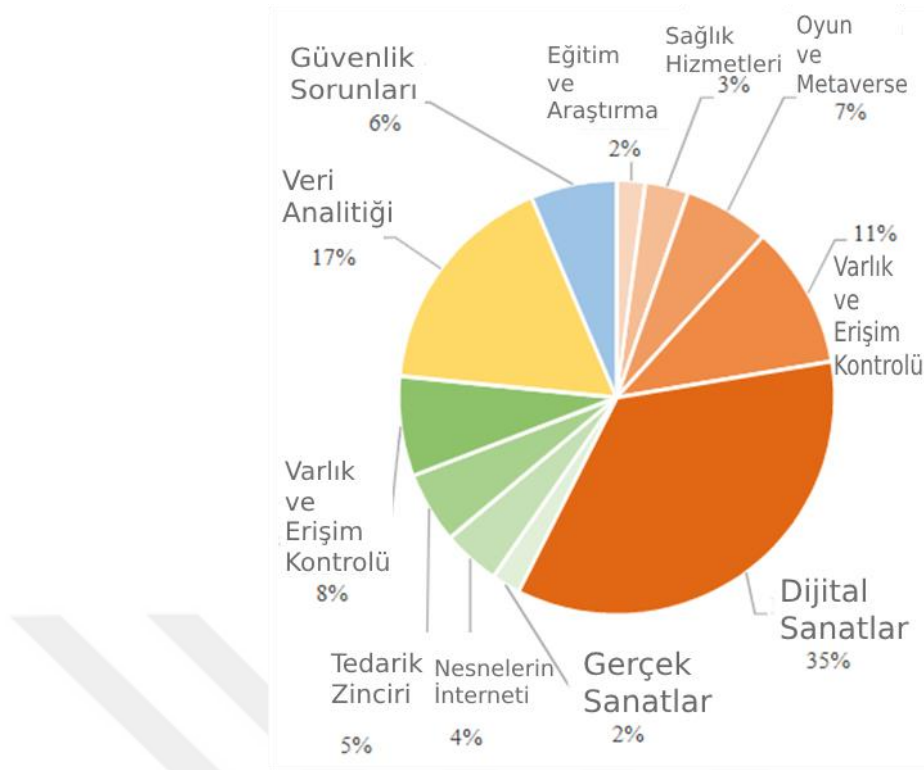
2019'un başlarında, NFT'leri tanıtan ilk akademik makaleler ortaya çıkmaya başlamış ve bunlar yaratıcı sanat toplulukları ve diğer endüstriler için potansiyel faydalarını açıklamıştır. Ethereum ERC-721 standardını takiben, Hyperledger gibi diğer blok zinciri çerçeveleri NFT'leri uygulamaya başlamış ve NFT'leri kullanarak gerçek dünya tedarik zincirlerindeki mevcut uygulama zorluklarına yönelik araştırma önerileri sunmuştur. (Khati ve ark., 2022). NFT'lerle ilgili jeton standartları Şekil 2.1'de gösterilmiştir.



Şekil 2.1. NFT'lerle ilgili jeton standartları (Wang ve ark., 2021)

2.1.2. Nft'lerin dijital sanatlarda ve ötesindeki kullanımı

2020'nin sonları ve 2021'in başlarında, sanat topluluğunun NFT'lerle deney yapmaya başlaması ve yaratıcı çalışmalarını NFT'ye dönüştürmesiyle birlikte NFT'lerle ilgili literatürde muazzam bir artışa tanıklık etmiştir. (Rehman ve ark., 2021; Wang ve ark., 2021) gibi birkaç makale, mevcut ekosistemde NFT'lerle denemenin zorluklarını ve faydalarını, tedarik zincirlerini, Nesnelerin İnternetini, fon toplama süreçlerini ve erişim kontrolünü ele almıştır. (Chalmers ve ark., 2022; Ito ve ark., 2022) gibi pazar çalışması makaleleri, NFT ekonomisinin hızlı büyümesini ve kısa sürede oluşan potansiyel balonu anlamayı amaçlamıştır. Diğer makaleler, tüccarların sosyal davranışlarını ve Twitter gibi sosyal platformlardaki etkilerini incelemiştir (Kapoor ve ark., 2022) ve NFT ticaretindeki riskleri değerlendirmek, sonuçları tahmin etmek ve güvenlik sorunlarını belirlemek için sosyal medya verilerini kullanmıştır. Her kategorideki bilimsel makalelerin yüzdesi Şekil 2.2'de gösterilmiştir.

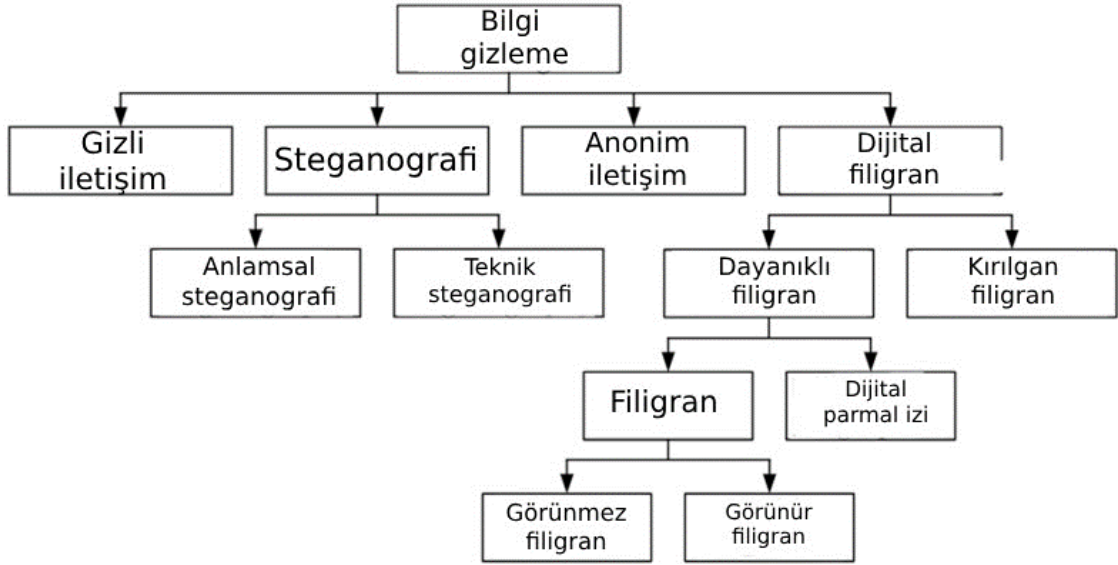


Şekil 2.2. Her kategorideki bilimsel makalelerin yüzdesi (Khati ve ark., 2022)

2.2. Dijital Filigranlama Teknikleri ve Video İçeriğinde Görünmez Filigranlama

2.2.1. Spatial alanında video filigranlama

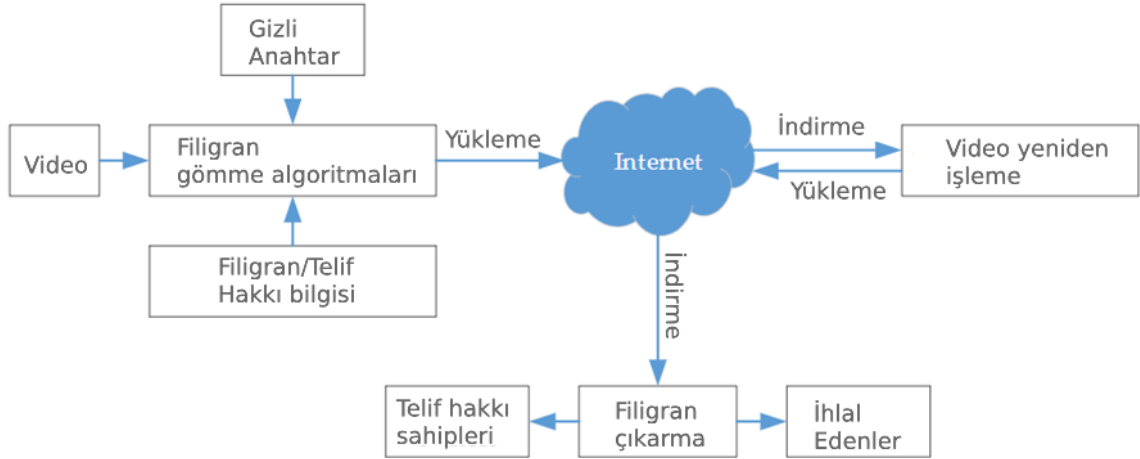
Spatiyal alan filigranlama teknikleri genellikle düşük karmaşıklığa ve yüksek taşıma kapasitesine sahip olan orijinal videonun parlaklık veya renkli bileşenlerine filigranı doğrudan etkiler. Öne çıkan spatial alan yöntemleri arasında en az anlamlı bit (LSB) değiştirme (Jindal ve ark., 2016), spektrum yayılma modülasyonu (Cox ve ark., 1997) ve diğerleri bulunur. Bilgi gizleme alanının ana dalları aşağıda şekil 2.3'te anlatılmak istenmiştir.



Şekil 2.3. Bilgi gizleme alanının ana dalları (Yu ve ark., 2018)

2.2.1.1. En az anlamlı bit (lsb) değiştirme

LSB yöntemi, filigranı bileşenin en az anlamlı bitine gömen klasik bir gömme tekniğidir. H. Kaur ve E. Kaur (2016), optimize edilmiş bir LSB tekniği kullanarak görünmez bir video filigranlama algoritması önermiştir. Bu yaklaşım, güvenliği artırmak için farklı sayı belirtici ve gizli anahtar kullanmaktadır. Ancak, LSB değiştirme yöntemi basitliğine rağmen düşük dayanıklılık sorunuyla karşı karşıya gelmiştir. Bu sorunu ele almak için, Bayoudh ve ark. (2017), hızlandırılmış güçlü özellikler (SURF) temelli çoklu-karakter dinamik video filigranlama algoritması önermiştir. Filigran bilgisi, orta anlamlı bit (MIDSB) ve LSB değiştirilerek üç YUV renk uzayı bileşenine gömülür, bu da dayanıklılığı ve görünmezliği artırır. Ayrıca, iş birliği ve kod dönüştürme saldırılarına karşı etkili bir şekilde direnir. Telif hakkı korumasında video filigran uygulaması Şekil 2.4'te belirtilmiştir.



Şekil 2.4. Telif hakkı korumasında video filigran uygulaması (Yu ve ark., 2018)

2.2.1.2. Yayılma spektrumu modülasyonu

Yayılma spektrumu temelli filigranlama algoritmaları etkili bir spatial alan tekniğidir. Orijinal video kareleri belirli bir sıra ile taranarak bir boyutlu sinyal elde edilir ve filigran bilgisi, yayılma spektrumu teknolojisi kullanılarak sözde rasgele dizilimlere modüle edilir ve video sinyaline gömülür (Masoumi ve ark., 2015). Önceki bir çalışmada (Tokar ve ark., 2009), filigran video karesiyle aynı boyuta genişletilmiş ve ardından kare şeklinde gömülmüştür. Bu yöntem, farklı karelerdeki aynı filigranlar, ortalama sürecinde birbirini güçlendirerek kare ortalama saldırılarına karşı direnir. Çeşitli saldırılara karşı dayanıklılığı artırmak için, Preda ve Vizireanu (2011), filigran bit hatalarını telafi etmek için döngüsel hata düzeltme kodlarını tanıtmıştır. Yayılma spektrumu, filigranın güç spektrumunu yaymak için kullanılmış ve yayılan filigran, parlaklık piksellerinde spatial ve temporal tekrarlarını kullanarak gömülmüştür.

2.2.1.3. Diğer güçlü spatial alan filigranlama teknikleri

Spatial alanda çeşitli güçlü video filigranlama algoritmaları bulunmaktadır. Venugopala ve ark. (2014), gri tonlamalı filigran görüntüsünü sekiz bit düzleme ile ayıştırmış ve bunları orijinal videonun farklı sahnelerine koymuştur. Bahrami ve Tab (2018), SURF ve blok sınıflandırmasına dayanan yarı-kör video filigranlama algoritması önermişlerdir. Li ve ark. (2016), ölçeklenebilir tekrar sıkıştırma ve kod dönüştürme saldırılarına karşı dirençli bir video filigranlama algoritması için bir spatial uniform mapping modeline dayanan bir yöntem önermişlerdir. Spatial alan filigranlama

algoritmaları, düşük karmaşıklıkları nedeniyle erken dönemde yaygın olarak kullanılmış olsa da sınırlı dayanıklılıkları, ilerleyen video kodlama teknolojisi karşısında uygulama alanlarının kısıtlanmasına yol açmıştır.

2.2.2. Dönüşüm alanında video filigranlama

Dönüşüm alanı filigranlama algoritmaları öncelikle video karelerini frekans alanına dönüştürerek filigranı koymak için frekans alanındaki katsayıları değiştirir. Yaygın kullanılan frekans alanı dönüşümleri arasında ayrık kosinüs dönüşümü (DCT), ayrık dalgacık dönüşümü (DWT) ve tekil değer ayrışımı (SVD) bulunmaktadır. Birçok dönüşüm alanı filigranlama algoritması, farklı dönüşümlerin avantajlarını kullanarak performansı artırmak için iki veya daha fazla dönüşümü birleştirir.

2.2.2.1. DCT temelli filigranlama algoritmaları

DCT temelli filigranlama algoritmaları, DCT'nin enerji sıkıştırma özelliğini kullanıp, bu özellik video karelerinin enerjisini DC katsayıları ve düşük frekanslı alt bantta yoğunlaştırır (Li ve Sui, 2012). Liu ve ark. (2010), yüksek frekans katsayıları korelasyon algoritması temelinde DCT alanında sağlam bir video filigranlama algoritması önermiştir. Cheng ve ark. (2013), kod bölmeli çoklu erişim (CDMA) modülasyonunu kullanarak DCT alanında kurtarılabılır bir video filigranlama algoritması sunmuştur. Nguyen ve Duan (2015), bir gri tonlamalı filigran görüntüsünden ayrıştırılan sekiz bit düzleme görüntüyü sağlam bir şekilde DCT katsayılarına koymuştur. Thanh ve ark. (2014), video filigranlama algoritmasında filigran koyma ve çıkarma bölgeleri arasında senkronizasyon sağlamak için KAZE özelliğini benimsemiştir.

Birçok DCT temelli filigranlama algoritması ayrıca kuantizasyon indeksi modülasyonu (QIM) şemasını kullanmıştır (Chen ve Wornell, 2001). Önceki bir makalede (Yang ve ark., 2008), hesaplama süresini azaltmak için sözde 3B DCT dönüşümü tanıtılmıştır. Huang ve ark. (2010), QIM'i sözde 3B DCT ile birleştirerek kör video filigranlama algoritması önermiştir. Campisi ve Neri (2007), QIM ve rasyonel dither modülasyonu (RDM) temelli bir filigran gömme tekniği önermiştir. Cedillo-Hernandez ve ark. (2018), bir video filigranlama algoritmasına mekansal ve zamansal fark edilebilir bozulma (JND) profili uygulamıştır.

Spatial alan filigranlama algoritmalarına kıyasla, DCT temelli filigranlama algoritmaları daha dayanıklıdır. Ancak, güçlü geometrik saldırılara karşı direnç göstermekte hala zorluk çekmektedir.

2.2.2.2. DWT temelli filigranlama algoritmaları

DWT temelli filigranlama algoritmaları mükemmel mekansal yerleştirme, frekans yayılımı ve çoklu çözünürlük özellikleri nedeniyle popülerdir. Abdulfetah ve ark. (2010), görsel modellere dayanan adaptif bir video filigranlama algoritması önermişlerdir. Bu algoritma, parlaklık maskeleme, doku maskeleme ve entropi maskeleme kullanarak JND maskelemesini elde etmek için koyma pozisyonlarını adaptif olarak ayarlamaktadır. El'Arbi ve ark. (2011), bir video dizisinin farklı sahnelerine farklı parçaları filigran olarak koymuşlar ve koyma pozisyonlarını HVS'ye dayanarak adaptif olarak ayarlamışlardır. Başka bir makalede (Singh, 2018), videoya ait önemli kareler ve hareketli kareler elde etmek için sahne tespiti kullanılmış ve filigran bitleri rastgele olarak birinci seviye DWT'nin iki yüksek frekans katsayısına koyulmuştur. Gao ve ark. (2017), tam sayı dalgalet dönüşümü ve SIFT kullanarak geometrik saldırılara karşı dirençli bir video çift filigranlama algoritması önermişlerdir.

Bir önceki makalede (Preda ve Vizireanu, 2010), gizli bir anahtar ve kuantizasyon yöntemi kullanılarak orta-yüksek frekanslı dalgalet katsayılarının ikinci seviyesine filigran eklenmiştir. Preda ve Vizireanu (2011), kuantizasyon ve yayılma spektrumu teknolojisini kullanarak sağlam bir filigranlama algoritması önermişlerdir. Gupta ve ark. (2018), çerçeveleri yeniden boyutlandırmak için DWT'yi kullanmış ve LL ve HL bantlarının maksimum ortalaması kullanılarak filigran pozisyonları seçmişlerdir. Başka bir makalede (Masoumi ve Amiri, 2013), sahne değişiklik analizi uygulanmış ve hareketli kısmı belirlemek için 3B-DWT (Üç Boyutlu Ayırık Dalgacık Dönüşümü) kullanılmış ve dalgalet katsayıları elde edilmiştir. Bhardwaj ve ark. (2018), kaldırma dalgalet dönüşümü (LWT) katsayı farkına dayanan önemli kare seçimi (SFS) kullanarak sağlam bir video filigranlama algoritması önermişlerdir. HVS ile birleştirildiğinde DWT temelli filigranlama algoritmalarının avantajlarına rağmen, çeviri ve ölçekleme saldırılarına karşı dayanıklılıkları hala zayıftır.

2.2.2.3. SVD temelli filigranlama algoritmaları

SVD (Tekil Değer Ayrışımı), mükemmel kararlılığa ve içsel özelliklere sahip benzersiz bir matris dönüşümüdür. Sağlam video filigranlamada yaygın olarak kullanılmaktadır. Filigran bilgisi genellikle tekil değerler matrisine eklenerek iyi fark edilemezlik sağlanır (Kerbiche ve ark., 2017). SVD genellikle DWT ile birleştirilerek sağlam video filigranlama için kullanılır (Agilandeewari ve Ganesan, 2016; Panda ve Garg, 2016; Adul ve Mwangi, 2017; Ponnisathya ve ark., 2017; Himeur ve Boukabou, 2018; Sathya ve Ramakrishnan, 2018; Shanmugam ve Chokkalingam, 2018). Bir önceki makalede (Himeur ve Boukabou, 2018), hızlı gradyan magnitud benzerlik sapması (GMSD) algoritmasının sahne sınırlarını tespit etmek için kullanıldığı ve DWT ve SVD'nin çıkarılan ana karelerin içine filigran bilgisi eklendiği belirtilmiştir. Adul ve Mwangi (2017), tekil değerler matrislerine filigran bilgisi eklemek için hibrit SVD/DWT tekniklerine dayanan bir kör video filigranlama algoritması önermişlerdir.

Başka bir makalede (Panda ve Garg, 2016), düşük payload ile yüksek dayanıklılık elde etmek için dört farklı ekleme yöntemi önermiş ve karşılaştırma yapmıştır. Sathya ve Ramakrishnan (2018), sahne değişiklik tespiti ve Fibonacci dizisi kullanarak ana kareler çıkarmış, DWT ve SVD'ye dayanarak seçilen ana karelere şifrelenmiş filigranı eklemişlerdir. Agilandeewari ve Ganesan (2016), renkli filigran görüntüsünü 24 bit düzleme ayırmış, daha güzel çoklu çözünürlük alt bantları elde etmek için contourlet dönüşümü (CT) ve DWT kullanmıştır. Filigran eklemek için DWT alt bantlarını oluşturarak SVD kullanmışlardır. Bir önceki makalede (Ponnisathya ve ark., 2017), anahtar kare seçimi için kaotik harita kullanılmış ve dönüştürülmüş kareler ile filigran görüntüsü üzerinde SVD gerçekleştirilerek filigran ekleme yapılmıştır. Shanmugam ve Chokkalingam (2018), tüm video karelerini işlemiş, parlaklık bileşenlerinde DWT uygulamış ve LH alt bantları üzerinde 2 seviye DWT kullanmış ayrıca filigran ekleme için SVD kullanmışlardır.

2.2.2.4. Hibrit dönüşüm tabanlı filigranlama algoritmaları

Farklı dönüşüm yöntemlerinin avantajlarını birleştirmek ve performansı iyileştirmek için birçok hibrit alan filigranlama algoritması ortaya çıkmıştır. Bir makalede (Kerbiche ve ark., 2018), sahne tanımlama ve sahne özetleme yöntemleri kullanılarak video özetleri oluşturulmuş ve kalabalık kaynaklarından elde edilen hareketli nesneler ve orijinal videodan oluşturulan mozaik karelerden iki tür özellik bölgesi tespit edilmiştir.

Bu özellik bölgeleri birleştirilerek nihai mozaik oluşturulmuş ve filigran DCT, DWT ve SVD yöntemleri kullanılarak ekleme yapılmıştır.

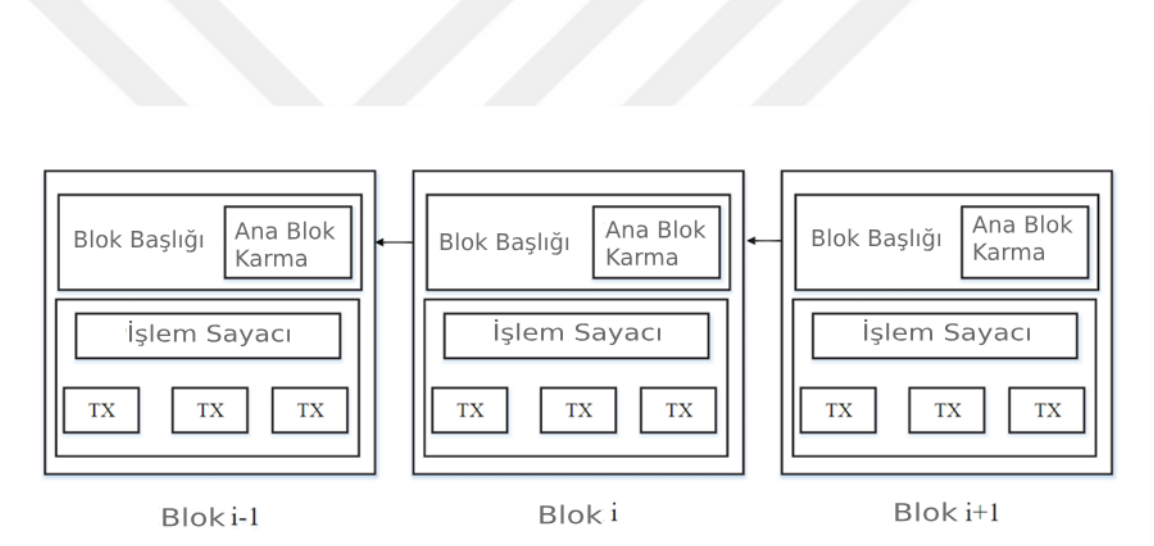
Gaj ve ark. (2017), filigranı gömmek için DCT ve 3B-DWT'yi birleştirmişlerdir. Bu durumda çerçeve karıştırma ve projeksiyon saldırılarına karşı direnç sağlanmaktadır. Bazı hibrit DWT/DCT tabanlı video filigranlama algoritmaları, DCT'nin enerji sıkıştırma özelliği ve DWT'nin çoklu çözünürlük özelliğini kullanmaktadır (Joshi ve ark., 2016; Kunhu ve ark., 2016). Bir makalede (Jiang ve ark., 2015), 2B-DWT ve sözde-3B DCT tabanlı bir sıfır-video filigran algoritması önerilmiştir. Log-polar dönüşümünün tanıtılması, döndürme işlemlerine karşı dayanıklılığı artırmıştır. Filigran, yayılma spektrumu teknolojisi aracılığıyla kod bölme çoklu erişim filigranına kodlanmış ve filigran gömmek için SVD ile birleştirilmiştir.



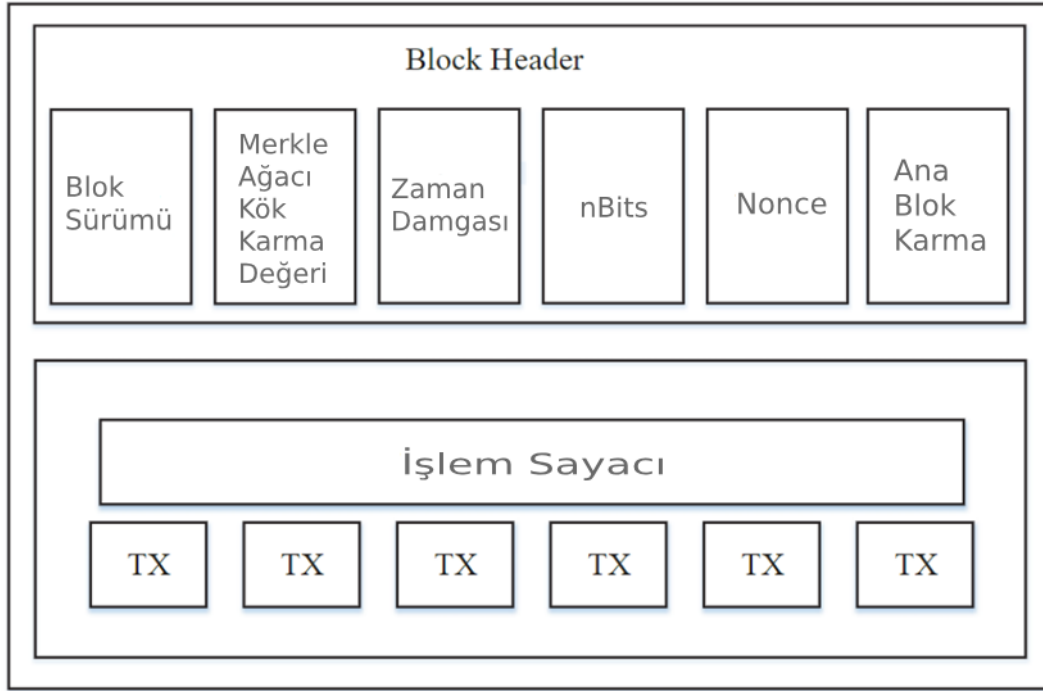
3. MATERYAL VE YÖNTEM

3.1. Blok Zinciri (Blockchain)

Blok zinciri, geleneksel halka açık defterler gibi, işlem kayıt listesini içeren bloklardan oluşan bir dizi olarak tanımlanabilir (Chuen, 2015). Bir bloğun başlık kısmında bulunan önceki blok karmasıyla, bir bloğun sadece bir üst bloğu bulunmaktadır. Ayrıca, Ethereum blok zincirinde, bloğun atalarının çocukları olan "amca" bloklarının da karmaları saklanır (Buterin, 2014). Blok zincirinin ilk bloğuna "genesis blok" denmektedir ve hiçbir üst bloğa sahip değildir. Blok zincirinin, sürekli bir blok dizisinden oluşan bir örneği ve Blok yapısı Şekil 3.1 ve Şekil 3.2’ da belirtilmiştir.



Şekil 3.1. Blok zincirinin, sürekli bir blok dizisinden oluşan bir örneği (Zheng ve ark., 2017)



Şekil 3.2. Blok yapısı (Zheng ve ark., 2017)

3.1.1. Blok zinciri yapısı

3.1.1.1. Blok

Blok başlığı kısımları:

- (i) Blok sürümü: hangi blok doğrulama kurallarının izleneceğini belirtir.
- (ii) Merkle ağacı kök karması: bloktaki tüm işlemlerin karması.
- (iii) Zaman damgası: 1 Ocak 1970'den bu yana evrensel saat dilimindeki saniye cinsinden geçerli zaman.
- (iv) nBits: geçerli bir blok karması için hedef eşik değeri.
- (v) Nonce: genellikle 0 ile başlayan ve her karması hesaplaması için artan 4 baytlık bir alan.
- (vi) Üst blok karması: önceki bloğa işaret eden 256 bitlik bir karması.

Blok gövdesi, bir sayaç ve işlemlerden oluşur. Bir bloğun içerebileceği işlem sayısı, blok boyutuna ve her bir işlemin boyutuna bağlıdır. Blok zinciri, işlemlerin kimlik doğrulamasını sağlamak için asimetrik bir kriptografi mekanizması kullanılır (Zheng ve ark., 2017). Ayrıca güvenilmeyen bir ortamda asimetrik kriptografiye dayalı dijital imza kullanılır.

3.1.1.2. Dijital imza

Her kullanıcının bir çift gizli anahtar ve açık anahtarı bulunmaktadır. Gizli olarak saklanması gereken anahtar, işlemleri imzalamak için kullanılır. Dijital olarak imzalanmış işlemler tüm ağ üzerinde yayınlanır. Tipik bir dijital imza, imzalama aşaması ve doğrulama aşaması olmak üzere iki bölümden oluşur. Örneğin, bir kullanıcı Alice, başka bir kullanıcı Bob'a bir mesaj göndermek istiyor.

(1) İmzalama aşamasında, Alice verilerini gizli anahtarıyla şifreler ve Bob'a şifrelenmiş sonucu ve orijinal veriyi gönderir.

(2) Doğrulama aşamasında, Bob, değeri Alice'in açık anahtarıyla doğrular. Bu şekilde, Bob verinin değiştirilip değiştirilmediğini kolayca kontrol edebilir. Blok zincirlerinde kullanılan tipik dijital imza algoritması eliptik eğri dijital imza algoritmasıdır (ECDSA) (Johnson ve ark., 2001).

3.1.1.3. Blok zincirinin temel özellikleri

Blok zinciri, aşağıdaki temel özelliklere sahiptir (Zheng ve ark., 2017):

- Merkezi olmama: Geleneksel merkezi işlem sistemlerinde, her işlem merkezi güvenilir bir kuruluş (örneğin, merkez bankası) tarafından doğrulanmak zorundadır, bu da merkezi sunucularda maliyet ve performans darboğazlarına yol açar. Merkezi modun aksine, blok zincirinde üçüncü bir taraf artık gereksizdir. Blok zincirindeki konsensüs algoritmaları, dağıtım yapan bir ağda veri tutarlılığını sağlamak için kullanılır.

- Süreklilik: İşlemler hızlı bir şekilde doğrulanabilir ve geçersiz işlemler dürüst madenciler tarafından kabul edilmez. Bir kez blok zincirine dahil edildiğinde, işlemlerin silinmesi veya geri alınması neredeyse imkansızdır. Geçersiz işlemler içeren bloklar hemen tespit edilebilir.

- Anonimlik: Her kullanıcı, gerçek kimliğini açığa çıkarmayan bir farklı adresle blok zinciri ile etkileşime geçebilir. Blok zinciri, içsel kısıtlamalar nedeniyle mükemmel gizlilik korumasını garanti edemez.

- Denetlenebilirlik: Bitcoin blok zinciri, kullanıcı bakiyeleri hakkında Harcanmamış İşlem Çıktısı (UTXO) modeline dayalı olarak veri depolamaktadır (Nakamoto, 2008): Herhangi bir işlem, önceki harcanmamış işlemlere dayanmaktadır. Mevcut işlem blok zincirine kaydedildiğinde, başvuru harcanmamış işlemlerin

durumu harcanmış durumuna geçer. Bu nedenle işlemler kolayca doğrulanabilir ve takip edilebilir.

3.1.1.4. Blok zinciri sistemlerinin sınıflandırılması

Mevcut blok zinciri sistemleri genellikle üç bölümden oluşur: halka açık blok zinciri, özel blok zinciri ve konsorsiyum blok zinciri (Buterin, 2015). Halka açık blok zincirinde tüm kayıtlar herkese görünür ve herkes konsensüs sürecine katılabilir. Konsorsiyum blok zincirinde ise yalnızca önceden seçilmiş bir grup düğüm konsensüs sürecine katılır. Özel blok zincirinde ise yalnızca belirli bir kuruluştan gelen düğümler konsensüs sürecine katılabilir.

Bir özel blok zinciri, tamamen bir kuruluş tarafından kontrol edilen merkezi bir ağ olarak kabul edilir. Birden fazla kuruluş tarafından oluşturulan konsorsiyum blok zinciri, yalnızca düğümlerin küçük bir kısmının konsensüsü belirlemek için yapıldığı kısmi merkezi olabilmektedir. Üç blok zinciri türü arasındaki karşılaştırma Çizelge 3.1'de listelenmiştir.

Çizelge 3.1. Halka açık blok zinciri, konsorsiyum blok zinciri ve özel blok zinciri arasındaki karşılaştırmalar (Zheng ve ark., 2017).

Mülkiyet	Halka açık blok zinciri	Konsorsiyum blok zinciri	Özel blok zinciri
Konsorsiyum belirleme	Tüm madenciler	Seçilmiş düğüm seti	Bir organizasyon
Okuma izni	Halka açık	Hem halka açık hem de sınırlı olabilir	Hem halka açık hem de sınırlı olabilir
Değiştirilemezlik	Neredeyse müdahale edilemez	Değiştirilebilir	Değiştirilebilir
Verimlilik	Düşük	Yüksek	Yüksek
Merkezi	Hayır	Kısmi	Evet
Konsorsiyum süreci	İzin gerektirmeyen	İzin gerektiren	İzin gerektiren

- **Konsensüs belirleme:** Halka açık blok zincirinde, her düğüm konsensüs sürecine katılabilmektedir. Konsorsiyum blok zincirinde, yalnızca belirli bir düğüm kümesi bloğun doğrulamasından sorumludur. Özel bir zincirde ise tamamen bir kuruluş tarafından kontrol edilir ve kuruluş nihai konsensüsü belirleyebilmektedir.

- **Okuma izni.** Halka açık blok zincirindeki işlemler herkese görünürken, özel blok zinciri veya konsorsiyum blok zinciri duruma bağlıdır.

- **Değişmezlik.** Halka açık blok zincirinde kayıtlar birçok katılımcıda depolandığından, işlemlere müdahale etmek neredeyse imkansızdır. Öte yandan, özel bir

blok zinciri veya konsorsiyum blok zincirinde işlemler sınırlı sayıda katılımcı olduğu için kolaylıkla değiştirilebilir.

- Verimlilik. Halka açık blok zinciri ağındaki birçok düğüm nedeniyle işlemlerin ve blokların yayılması oldukça zaman alır. Sonuç olarak, işlem verimliliği sınırlıdır ve gecikme süresi yüksektir. Daha az doğrulayıcıya sahip olan konsorsiyum blok zinciri ve özel blok zinciri daha verimli olabilmektedir.

- Merkeziyet. Üç blok zinciri türü arasındaki temel fark, halka açık blok zincirinin, merkezi olmayan konsorsiyum blok zincirinin kısmen merkezi ve özel blok zincirinin tamamının merkezi olmasıdır, çünkü tek bir grup tarafından kontrol edilmektedir.

- Konsensüs süreci. Halka açık blok zincirinde herkes konsensüs sürecine izin almadan katılabilirken, konsorsiyum blok zinciri ve özel blok zinciri izin alarak katılabilmektedir.

Halka açık bir blok zinciri dünyaya açıktır ve birçok kullanıcı aktif olarak kullanabilmektedir. Daha çok halka açık blok zinciri gün geçtikçe ortaya çıkmaktadır. Konsorsiyum blok zinciri birçok iş uygulamasında kullanılabilir.

3.1.2. Konsensüs algoritmaları

Blok zincirinde, güvensiz düğümler arasında nasıl bir konsensüs sağlanacağı, (Lamport ve ark., 1982) ile ilgili olarak, Bizans Generalleri (BG) Probleminin bir dönüşümü haline gelmiştir. BG probleminde, bir grup general, bir kısmı Bizans ordusuna komuta eder ve şehri çevreler. Bazı generaller saldırmayı tercih ederken, diğer generaller geri çekilmeyi tercih eder. Ancak, yalnızca generallerin bir kısmı şehre saldırırsa saldırı başarısız olur. Bu nedenle, saldırmak veya geri çekilmek konusunda bir anlaşmaya varmaları gerekmektedir. Dağıtılmış bir ortamda konsensüse nasıl ulaşılabileceği konusunda zorluk yaşanmaktadır. Blok zinciri içinde bir zorluktur çünkü blok zinciri ağı dağıtılmıştır. Blok zincirinde, dağıtılmış düğümlerdeki defterlerin hepsinin aynı olduğunu sağlayan merkezi bir düğüm yoktur. Farklı düğümlerdeki defterlerin tutarlı olmasını sağlamak için bazı protokoller gereklidir.

Blok zincirinde konsensüse ulaşmak için yaygın olarak kullanılan bazı yöntemler aşağıda verilmiştir.

3.1.2.1. Konsensüs yöntemleri

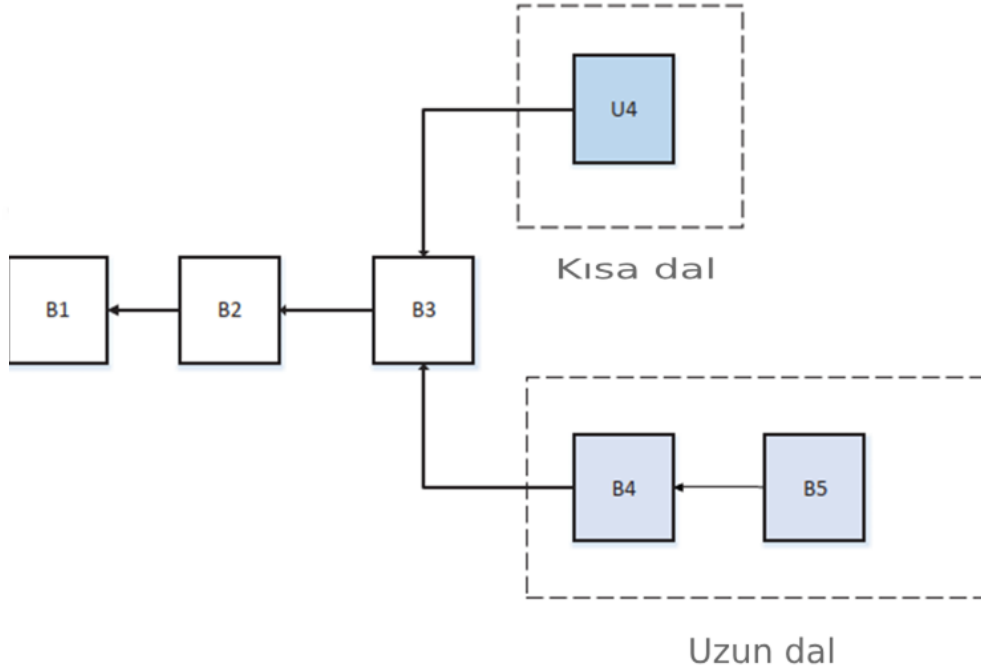
PoW (İş Kanıtı), Bitcoin ağında kullanılan bir konsensüs stratejisidir (Nakamoto, 2008). Merkezi olmayan bir ağda, işlemleri kaydetmek için bir düğümün seçilmesi gerekmektedir. En kolay yol rastgele seçimdir. Ancak, rastgele seçim saldırılara açıktır. Bu nedenle, bir düğümün bir blok işlemi yayınlamak istemesi durumunda, düğümün ağa saldırmayacağını kanıtlamak için çok çalışması gerekmektedir. Genellikle bu çalışma, bilgisayar hesaplamalarını içerir. Tipik Konsensüs Algoritmalarının Karşılaştırılması Çizelge 3.2'e gösterilmiştir.

Çizelge 3.2. Tipik Konsensüs Algoritmalarının Karşılaştırılması (Zheng ve ark., 2017)

Mülkiyet	PoW	PoS	PBFT	DPOS	Ripple	Tendermint
Düğüm kimlik yönetimi	Açık	Açık	izin gerektiren	Açık	Açık	izin gerektiren
Enerji tasarrufu	Hayır	Kısmi	Evet	Kısmi	Evet	Evet
Düşmanın tolere edilebilir gücü	<25% Hesaplama gücü	<51% Pay	<33.3% Hatalı kopyalar	<51% Doğrulayıcılar	<20% UNL'deki hatalı düğümler	<33.3% Bizans oy gücü
Örnek	Bitcoin	Peercoin	Hyperledger Fabric	Bitshares	Ripple	Tendermint

PoW'da, ağın her bir düğümü blok başlığının bir karma değerini hesaplamaktadır. Blok başlığı bir nonce içerir ve madenciler nonce'yu sık sık değiştirerek farklı karma değerleri elde etmeye çalışırlar. Konsensüs, hesaplanan değer belirlen bir verilen değere eşit veya daha küçük olması gerektiğini belirtmektedir. Bir düğüm hedef değere

ulaştığında, bloğu diğer düğümlere yayınlarken, diğer düğümler karma değerinin doğruluğunu karşılıklı olarak gerçekleştirmektedir. Blok doğrulandığında, diğer madenciler bu yeni bloğu kendi blok zincirlerine eklemektedir. Karma değerlerini hesaplayan düğümlere madenci denir ve PoW işlemi Bitcoin'de madencilik olarak adlandırılır. Blok zinciri dallarının senaryosu Şekil 3.3'te gösterilmiştir. Daha uzun dal ana zincir olarak kabul edilirken, daha kısa olanı reddedilecektir.



Şekil 3.3. Blok zinciri dallarının senaryosu (Zheng ve ark., 2017)

Merkezi olmayan ağda, birden çok düğüm uygun Nonce'yu neredeyse aynı anda bulduğunda, geçerli bloklar eş zamanlı olarak oluşturulabilir. Sonuç olarak, Şekil 3.3'te gösterildiği gibi dallar oluşabilir. Ancak, iki rekabet eden Fork'un aynı anda bir sonraki bloğu oluşturması olası değildir. PoW protokolünde, bundan sonra daha uzun olan bir zincir doğru olarak kabul edilir. Aynı anda doğrulanan U4 ve B4 bloklarıyla oluşturulan iki çatalı düşünelim. Madenciler, daha uzun bir dal bulunana kadar bloklarını madencilığe devam ettirirler. B4, B5 daha uzun bir zincir oluşturduğu için, U4 üzerindeki madenciler daha uzun dala geçiş yapar.

PoW protokolünde madenciler, birçok bilgisayar hesaplaması yapmak zorundadır, ancak bu işler çok fazla kaynak tüketir. Kaybı azaltmak için, çalışmaların bazı yan uygulamaları olan PoW protokolleri tasarlanmıştır. Örneğin, Primecoin (King, 2013), matematiksel araştırmalar için kullanılabilecek özel asal sayı zincirlerini aramaktadır.

PoS (Hisse Kanıtı), PoW'a göre enerji tasarruflu bir alternatiftir. PoS'da madenciler, sahip oldukları miktarı kanıtlamak zorundadır. Daha fazla miktara sahip olan kişilerin ağa saldırma olasılıklarının daha düşük olduğu düşünülmektedir. Hesap bakiyesine dayalı seçim oldukça adildir ve en zengin kişi ağda baskın olmaktadır. Sonuç olarak, bir sonraki bloğu kimin oluşturacağını belirlemek için stake büyüklüğü ile birleşen çözümler önerilmiştir. Özellikle, Blackcoin (Vasin, 2014), bir sonraki üreticiyi tahmin etmek için rastgel eleştirme kullanmaktadır. Stake büyüklüğü ile birlikte en düşük karma değerini arayan bir formül kullanır. Peercoin (King ve Nadal, 2012), coin yaşına dayalı seçimi tercih etmektedir. Peercoin'de, daha eski ve daha büyük coin setleri bir sonraki bloğu oluşturma olasılığı daha yüksektir. PoW'a göre PoS daha fazla enerji tasarrufu sağlar ve daha etkilidir. Ne yazık ki, madencilik maliyetinin neredeyse sıfır olması, saldırıların bir sonucu olarak ortaya çıkabilmektedir. Birçok blok zinciri, başlangıçta PoW kullanır ve daha sonra PoS'a geçiş yapar. Örneğin, Ethereum yakın zamanda PoW'dan PoS'a geçmiştir.

PBFT (Pratik Bizans Hata Toleransı), Bizans hatalarına dayanıklı bir çoğaltma algoritmasıdır (Miguel ve Barbara, 1999). Hyperledger Fabric (Zheng ve ark., 2017), PBFT'yi konsensüs algoritması olarak kullanır, çünkü PBFT, en fazla 1/3 hatalı Bizans replika ile başa çıkabilmektedir. Yeni bir blok bir turda belirlenir. Her turda, bazı kurallara göre birincil bir düğme seçilir ve işlem sırasını belirler. Tüm süreç üç aşamaya ayrılır: ön hazırlık, hazırlık ve onaylama. Her aşamada, bir düğme, tüm düğümlerin 2/3'ünden fazlasının oylarını aldıysa bir sonraki aşamaya gitmektedir. Bu nedenle, PBFT, her düğümün ağ tarafından bilinmesini gerektirir. PBFT gibi, Stellar Mutabakat Protokolü (SCP) (Mazieres, 2015) de bir Bizans anlaşma protokolüdür.

PBFT'de her bir düğüm diğer düğümleri sorgulamak zorundadır, ayrıca SCP katılımcılara, diğer katılımcıların hangi setine inanacaklarını seçme hakkı vermektedir. PBFT'ye dayanarak, Antshares (Ago, 2016) dBFT (Yetkilendirilmiş Bizans Hata Toleransı) uygulanmıştır. dBFT'de bazı profesyonel düğümler, işlemleri kaydetmek için oy verilir.

DPOS (Delege Edilmiş Hisse Kanıtı). PoS ve DPOS arasındaki temel fark, PoS'un doğrudan demokratik olması, DPOS'un ise temsilci demokratik olmasıdır. Sahipler, blok oluşturmak ve doğrulamak için delegelerini seçerler. Bloğu doğrulamak için çok daha az düğüm olduğundan, blok hızlı bir şekilde onaylanabilir ve bu da işlemlerin hızlı bir şekilde onaylanmasına yol açar. Aynı zamanda, blok boyutu ve blok aralıkları gibi ağın parametreleri delegeler tarafından ayarlanabilir. Ayrıca, kullanıcılar dürüst olmayan

delegeler hakkında endişelenmek zorunda kalmazlar ve onlara kolayca oy verebilirler. DPOS, Bitshares (Zheng ve ark., 2017)'in temelidir. Ripple (Schwartz ve ark., 2014), daha büyük ağ içinde ortaklaşa güvenilen alt ağları kullanan bir konsensüs algoritmasıdır. Ağda, düğümler sunucu (konsensüs sürecine katılan) ve müşteri (sadece fon transferi yapan) olarak iki tipe ayrılır. Her sunucunun Benzersiz Düğüm Listesi (UNL) vardır. UNL, sunucu için önemlidir. Bir işlemi deftere ekleyip eklemeyeceğini belirlerken, sunucu UNL'deki düğümleri sorgular ve alınan onaylar %80'e ulaştığında işlem deftere eklenir. Bir düğüm için UNL'deki hatalı düğümler %20'den az olduğu sürece defter doğru kalır.

Tendermint (Kwon, 2014), bir Bizans konsensüs algoritmasıdır. Bir turda yeni bir blok belirlenir. Bu turda, bir önerici, onaylanmamış bir blok yayınlamak üzere seçilir. Tendermint Üç adımdan oluşur: 1) Ön oylama adımı. Doğrulayıcılar, önerilen blok için bir ön oylama yayınlamayı seçerler. 2) Ön taahhüt adımı. Eğer düğme önerilen blok üzerindeki ön oylamaların 2/3'ünden fazlasını almışsa, o blok için bir ön taahhüt yayınlamalıdır. Eğer düğme ön taahhütlerin 2/3'ünden fazlasını almışsa, taahhüt adımına girer. 3) Taahhüt adımı. Düğme, bloğu doğrular ve o blok için bir taahhüt yayınlamalıdır. Düğme, taahhütlerin 2/3'ünü aldığı anda, bloğu kabul eder. PBFT'ye kıyasla, düğmelerin geçerli olabilmesi için jetonların kilitlemeleri gerekir. Bir doğrulayıcının adil olmadığı tespit edilirse, ona ceza verilir.

3.1.2.2. Konsensüs algoritmalarının karşılaştırması

Farklı konsensüs algoritmalarının avantajları ve dezavantajları vardır. Çizelge 3.2'de, farklı konsensüs algoritmaları arasında bir karşılaştırma yapılmıştır (Zheng ve ark., 2017).

- Düğme kimlik yönetimi. PBFT, her turda birinciliği seçmek için her madencinin kimliğini bilmesi gerektiğini belirtirken, Tendermint her turda bir önerici seçmek için doğrulayıcıları bilmesini gerektirir. PoW, PoS, DPOS ve Ripple için düğmeler ağa serbestçe katılabilir.

- Enerji tasarrufu. PoW'da, madenciler hedef değere ulaşmak için sürekli olarak blok başlığını karma işlemi yaparlar. Sonuç olarak, işlemin gerektirdiği elektrik miktarı muazzam bir ölçüye ulaşmıştır. PoS ve DPOS için madenciler blok başlığını karma işlemi yapmak zorundadır, ancak arama alanı sınırlı olacak şekilde tasarlandığından iş büyük

ölçüde azalacaktır. PBFT, Ripple ve Tendermint için konsensüs sürecinde madencilik yoktur. Bu nedenle enerji büyük ölçüde tasarruf edilir.

- Hasımların tolere edilebilir gücü. Genel olarak, hash gücünün %51'i, ağı kontrolünü ele geçirmek için bir eşik olarak kabul edilir. Ancak PoW sistemlerindeki bencil madencilik stratejisi (Eyal ve Sirer, 2014), madencilerin gelirini elde etmelerine yardımcı olmak için sadece %25 karma gücüne sahip olmalarını sağlar. PBFT ve Tendermint, en fazla 1/3 hatalı düğümü işleyecek şekilde tasarlanmıştır. Ripple, UNL'deki hatalı düğümlerin %20'den az olduğu kanıtlanmıştır.

- Örnek olarak Bitcoin, PoW'a dayanırken, Peercoin yeni bir eşler arası PoS kripto para birimidir. Ayrıca, Hyperledger Fabric konsensüs sağlamak için PBFT'yi kullanır. Akıllı sözleşme platformu Bitshares, konsensüs algoritması olarak DPOS'u benimser. Ripple, Ripple protokolünü uygularken, Tendermint Tendermint protokolünü tasarlar.

PBFT ve Tendermint, izin verilen protokollerdir. Düğme kimliklerinin tüm ağ tarafından bilinmesi gerektiğini savunur, bu yüzden genellikle kamu yerine ticari modda kullanılabilirler. PoW ve PoS, halka açık blok zincirleri için uygundur. Konsorsiyum veya özel blok zincirleri, PBFT, Tendermint, DPOS ve Ripple'a tercih gösterebilir.

3.1.2.3. Konsensüs algoritmalarındaki gelişmeler

İyi bir konsensüs algoritması, verimlilik, kolaylık ve güvenlik anlamına gelir. Son zamanlarda, blockchain mutabakat algoritmalarını geliştirmek için birçok çalışma yapılmıştır. Yeni konsensüs algoritmaları, blok zincirinin belirli sorunlarını çözmeyi amaçlayarak tasarlanmıştır. PeerCensus (Decker ve ark., 2016)'un temel fikri, blok oluşturmayı ve işlem onayını birbirinden ayırmaktır, böylece konsensüs hızı önemli ölçüde artırılabilir. Ayrıca, Kraft (2016), bir bloğun görelisi olarak istikrarlı bir hızda oluşturulmasını sağlamak için yeni bir konsensüs yöntemi önermiştir. Yüksek blok oluşturma hızı, Bitcoin'in güvenliğini tehlikeye atmaktadır. Bu nedenle, Ağgözlü En Ağır Gözlenen Alt-Ağacı (GHOST) zincir seçim kuralı (Sompolinsky ve Zohar, 2013), bu sorunu çözmek için tasarlanmıştır. Bu durumda en uzun dal yerine, GHOST dallara ağırlık verir ve madencilere daha iyisini sunmak için en iyi dalı seçebilir. Chepurnoy ve ark. (2016), blok oluşturmak için geçmiş durum anlık fotoğraflarının etkileşimsiz kanıtlarını sunan herhangi birine katılmak konusunda anlaşmaya varan eşler arası blok zinciri sistemleri için yeni bir konsensüs algoritması sunmuştur. Buna benzer bir

protokolde madenciler, tam blokların yerine sadece eski blok başlıklarını depolamak zorunda kalır.

3.1.3 Zorluklar ve son gelişmeler

3.1.3.1. Ölçeklenebilirlik

Blockchain'in gün geçtikçe artan işlem miktarıyla karşı karşıya kalması, Blockchain'in hacimli hale gelmesine neden olmaktadır. Her bir düğüm, geçerli işlemleri doğrulamak için tüm işlemleri depolamak zorunda kalır çünkü mevcut işlemin kaynağının harcanıp harcanmadığını kontrol etmek zorundadır. Ayrıca, blok boyutu ve yeni bir blok oluşturmak için kullanılan zaman aralığının orijinal sınırlamaları nedeniyle Bitcoin blok zinciri yalnızca saniyede yaklaşık 7 işlemi kaydedebilir, bu da gerçek zamanlı olarak milyonlarca işlemi kaydetme gereksinimini karşılayamaz. Bunun yanı sıra, blok kapasitesi çok küçük olduğundan, yüksek işlem ücretine sahip işlemler tercih edildiği için birçok küçük işlem gecikmeli olabilmektedir.

Blockchain'in ölçeklenebilirlik sorununu ele almak için önerilen nedenler bulunmaktadır ve bunlar aşağıda sırasıyla açıklanmıştır:

- Blockchain depolamasının optimize edilmesi. Bir düğümün tam bir kopyasını işletmesi daha zor olduğundan, Bruce, ağ tarafından eski işlem kayıtlarının kaldırıldığı (veya unutulduğu) yeni bir kripto para birimi planı önermiştir (Bruce, 2014). Tüm boş olmayan adreslerin bakiyesini tutmak için hesap ağacı adında bir veri tabanı kullanılmaktadır. Bunun yanı sıra, hafif istemci de bu sorunu çözmeye yardımcı olmaktadır. Hafif bir istemcilere izin vermek için VerSum adında yeni bir yöntem önerilmiştir (van den Hooff ve ark., 2014). VerSum, hafif istemcilerin pahalı hesaplamaları büyük girişler üzerinde dış kaynaklı hale getirmesine izin vermektedir. Birden fazla sunucudan gelen sonuçları karşılaştırarak hesaplama sonucunun doğruluğunu sağlar.

- Blok zincirinin yeniden tasarlanması. (Eyal ve ark., 2016) çalışmasında, Bitcoin-NG önermiştir. Bitcoin-NG'nin temel fikri, geleneksel bloğu iki bölüme ayırmaktır: Lider seçimi için bir anahtar blok ve işlemleri depolamak için mikro bloklar oluşturulmuştur. Protokol, zamanı dönemlere ayırır. Her dönemde, madenciler anahtar blok oluşturmak için karma yapmak zorundadır. Anahtar blok oluşturulduğunda, düğüm mikro blokları oluşturmakla sorumlu lider haline gelir. Bitcoin-NG ayrıca, mikro blokların ağırlığını

taşımayan en ağır (en uzun) zincir stratejisini genişletmiştir. Bu şekilde, blok zinciri yeniden tasarlanmış ve blok boyutu ile ağ güvenliği arasındaki denge sağlanmıştır.

3.1.3.2. Gizlilik sızıntısı

Blockchain, her bir kullanıcının gizlilik miktarını genel anahtar ve özel anahtar aracılığıyla koruyabilir. Kullanıcılar gerçek kimliklerini ifşa etmeden özel anahtar ve genel anahtarlarıyla işlem yapmaktadırlar. Ancak, Blockchain'in işlem gizliliğini garanti edemediği (Meiklejohn ve ark., 2013), (Kosba ve ark., 2016) çalışmalarında belirtmektedir. Çünkü her genel anahtar için tüm işlemler ve bakiyelerin değerleri kamuoyunca görülebilir. Bunun yanı sıra, son çalışmalar (Barceló, 2014), Bitcoin işlemlerinin bir kullanıcının bilgilerini ortaya çıkarmak için bağlantılandırılabilirliğini göstermiştir. Ayrıca, Biryukov ve ark. (2014), kullanıcı takma adlarını IP adresleriyle ilişkilendirmek için bir yöntem sunmuştur. Kullanıcılar Network Address Translation (NAT) veya güvenlik duvarları arkasında olsalar bile, her istemci bir set tarafından benzersiz şekilde tanımlanabilir, bu set öğrenilebilir ve bir işlemin kaynağını bulmak için kullanılabilir (Biryukov ve ark., 2014). Blockchain'in anonimliğini artırmak için birçok yöntem önerilmiştir ve bunlardan en çok kullanılan ikisi ele alınmıştır:

1. Karıştırma (Möser, 2013). Blockchain'de, kullanıcı adresleri takma adlardır. Ancak, birçok kullanıcı sık sık aynı adresle işlem yapar, bu nedenle adreslerin gerçek kimlikle ilişkilendirilmesi mümkündür. Karıştırma hizmeti, birden fazla giriş adresinden birden fazla çıkış adresine fon transferi yaparak anonimlik sağlayan bir hizmet türüdür. Örneğin, adresi A olan kullanıcı Alice, adresi B olan Bob'a bazı fonlar göndermek istiyor. Alice doğrudan giriş adresi A ve çıkış adresi B ile bir işlem yaparsa, Alice ve Bob arasındaki ilişki ortaya çıkabilir. Bu nedenle, Alice güvendiği bir aracı olan Carol'e fon gönderebilir. Ardından, Carol, çıkış adresleri c1, c2, c3 vb. ile Bob'a fonları transfer eder ve çoklu çıkışlar d1, d2, B, d3 vb. Bob'un adresi B de çıkış adreslerinde bulunur. Bu şekilde, Alice ve Bob arasındaki ilişkinin ortaya çıkması daha zor hale gelir. Ancak, aracı kötü niyetli olabilir. Alice ve Bob'un özel bilgilerini kasıtlı olarak açıklayabilir. Ayrıca, Carol'ün Alice'in fonlarını Bob'un adresine değil kendi adresine transfer etmesi de mümkündür. Mixcoin (Bonneau ve ark., 2014), hileli davranışları önlemek için basit bir yöntem sağlamaktadır. Aracı, fon miktarı ve transfer tarihi dahil olmak üzere kullanıcıların taleplerini kendi özel anahtarıyla şifreler. Ardından, aracı para transfer etmezse, herhangi biri aracının hile yaptığını doğrulayabilir. Bu durumda hırsızlık tespit

edilir, ancak engellenmez. Coinjoin'e ilham verilen CoinShuffle (Ruffing ve ark., 2014), çalınmayı önlemek için çıkış adreslerini karıştırmak için merkezi bir karıştırma sunucusuna dayanabilir.

2. Anonimlik. Zerocoin'de sıfır bilgi ispatı kullanılır (Miers ve ark., 2013). Madenciler bir işlemi dijital imza ile doğrulamak zorunda değildir, ancak geçerli jetonların listesine ait jetonları doğrulamak zorundadır. Ödemelerin kökeni, işlemlerden bağımsız olarak işlem grafiği analizlerini önlemek için bağlantısını keser. Bu sorunu çözmek için Zerocash (Sasson ve ark., 2014) önerilmiştir. Zerocash'te, sıfır bilgi Kısa Olarak Etkin Olmayan İspatlar (zk-SNARKs) kullanılır. İşlem miktarları ve kullanıcıların elindeki jetonların değerleri gizlenir.

3.1.3.3. Bencil madencilik

Blok zinciri, iş birliği yapan bencil madencilerin saldırılarına karşı hassastır. Özellikle, Eyal ve Sirer (2014), ağın hile yapmak için yalnızca küçük bir bölümünün hash gücünü kullanması durumunda bile savunmasız olduğunu göstermiştir. Bencil madencilik stratejisinde, bencil madenciler çıkarılan bloklarını yayınlamadan saklarlar ve özel dal yalnızca belirli koşullar sağlandığında halka açıklanır. Özel dal, mevcut genel zincirden daha uzun olduğundan tüm madenciler tarafından kabul edilir. Özel blok zinciri yayınlanmadan önce, dürüst madenciler kaynaklarını boşa harcarken bencil madenciler rekabetsiz bir şekilde özel zincirlerini madencilik yaparlar. Bu nedenle, bencil madenciler daha fazla gelir elde etme yönündedirler. Bencil madencilğe dayanan birçok saldırı önerilmiştir ve bunlar Blockchain'in güvenli olmadığını göstermektedir. Stubborn mining (Nayak ve ark., 2016) çalışmasında, madenciler ağ düzeyi karanlık saldırılarıyla madencilik saldırılarını karmaşık bir şekilde birleştirerek kazancı artırabilir. “Trail-stubbornness” (iz inatçılığı), madencilerin özel zincir geride kalsa bile blokları madencilğe devam ettiği inatçı stratejilerden biridir. Ancak, bazı durumlarda, basit inatçı madencilikle karşılaştırıldığında %13 daha fazla kazanç sağlayabilir. (Sapirshtein ve ark., 2015), küçük madenciler için basit bencil madencilikten daha fazla para kazanan bencil madencilik stratejileri olduğunu göstermektedir.

Bencil madencilik sorununu çözmeye yardımcı olmak için Heilman (Heilman, 2014), dürüst madencilerin hangi dalı takip edeceğini seçmek için yeni bir yaklaşım sunmuştur. Rasgele radyo sinyali ve zaman damgalarıyla, dürüst madenciler daha yeni blokları seçer. Bununla birlikte, (Heilman, 2014), sahteciliğe açık zamanaşımı

damgalarına karşı savunmasızdır. ZeroBlock (Solat ve Potop-Butucaru, 2017), basit bir düzen üzerine kurulmuştur: Her blok, ağ tarafından belirlenen bir maksimum süre içinde üretilmeli ve kabul edilmelidir. ZeroBlock içinde bencil madenciler beklenen ödülün daha fazlasını elde edemezler.

3.2. Takas Olmayan Jetonlar

Takas olmayan jetonlar (NFT), Ethereum'un akıllı sözleşmelerinden türetilen bir kripto para birimidir (Fairfield, 2021). NFT ilk olarak Ethereum İyileştirme (EIP)-721 (Entriken ve ark., 2018)'de önerildi ve daha sonra EIP-1155 (Entriken ve ark., 2018)'de geliştirildi. NFT, Bitcoin (Nakamoto, 2008) gibi klasik kripto paralardan farklıdır çünkü özgül özelliklere sahiptir (Shirole ve ark., 2020). Bitcoin (Nakamoto, 2008), tüm jetonların eşdeğer ve ayırt edilemez olduğu standart bir coindir. Buna karşılık, NFT hiçbir şekilde değiştirilemez bu da onu bir şeyi veya birini benzersiz bir şekilde tanımlamak için uygun hale getirir. Daha spesifik olmak gerekirse, Ethereum'daki akıllı sözleşmeler üzerinde NFT'leri kullanarak bir yaratıcı, videolar, resimler, sanatlar (Franceschet ve ark., 2020), etkinlik biletleri (Regner ve ark., 2019) gibi dijital varlıkların varlığını ve sahipliğini kolayca kanıtlayabilir. Ayrıca, yaratıcı her bir NFT piyasasında veya kişiden kişiye takas yaparken her başarılı işlemde telif ücreti kazanabilir. Tüm geçmiş takas edilebilirliği, derin likidite ve uyumlu işlem yetenekleri NFT'yi umut verici bir fikri mülkiyet (IP) koruma çözümü haline getirir. Gerçekte NFT'lerin sadece kodlardan ibaret olduğunu söylemek yanlış olmasına rağmen, bir alıcı için, dijital bir nesne olarak göreceli nadirliği dikkate alındığında, kodlara belirli bir değer atfeder. Bu, düşünülemez görünen bu IP ile ilgili ürünlerin satış fiyatlarını sağlam bir şekilde korur.

Son yıllarda, NFT'ler endüstriyel ve bilimsel topluluklar tarafından kayda değer bir ilgiyle karşılaşmıştır. 2021 yılında, NFT piyasasının ortalama 24 saatlik işlem hacmi 4.592.146.914 USD iken, tüm kripto para piyasasının 24 saatlik işlem hacmi 341.017.001.809 USD olmuştur (Wang ve ark., 2021). NFT ile ilgili çözümlerin likiditesi, bu kısa sürede (5 ay) tüm kripto para piyasasının %1.3'ünü oluşturmuştur. Erken yatırımcılar, benzersiz dijital koleksiyonları satarak binlerce kat getiri elde etmişlerdir. Mayıs 2021'de NFT ile ilgili piyasa, Ocak 2020'ye göre önemli ölçüde artmıştır (Wang ve ark., 2021). Özellikle, toplam satış sayısı 25,729'dur ve tamamlanan satışlarda harcanan toplam miktar 34,530,649.86 USD'ye ulaşmıştır. Özellikle, birincil pazar satışlarının toplam sayısı 17.140'ı işgal ederken, ikincil satışların (kullanıcıdan kullanıcıya) sayısı

8.589'du. Buna karşılık, birincil piyasa satışlarında kullanılan toplam USD miktarı 8.816.531,10'dur (Wang ve ark., 2021).

Ayrıca, aktif pazar cüzdanları 12,836'ya ulaşmış ve zaman geçtikçe hızla artmıştır. Şaşırtıcı bir şekilde, NFT satışları 12 milyon olarak tahmin edilirken (Aralık 2020), sadece iki ay içinde 340 milyona çıkmıştır (Şubat 2021). Bu patlama, NFT'yi bir çılgınlık haline getirmiş ve hatta bazıları tarafından dijital varlıkların geleceği olarak tanımlanmıştır. Yukarıdaki verilere ek olarak, insanlar çeşitli türdeki NFT'lere ilgi göstermektedir. NFT'li oyunlara veya takaslara heyecanla katılmaktadırlar. Ethereum'daki ilk NFT'lerden biri olan CryptoPunks, 10.000'den fazla koleksiyonluk punk (6039 erkek ve 3840 kadın) oluşturmuş ve ERC-721 standardının popüler hale gelmesini sağlamıştır (Wang ve ark., 2021). CryptoKitties, NFT'leri resmi olarak duyuran ve üreme mekânının oyunlaştırılmasıyla 2017'de piyasaya sürülen bir başka örnektir. Katılımcılar, nadir kedileri açık artırmada yüksek fiyatlarla mücadeleyle satın almak için çetin bir rekabet içine girmiş ve en yüksek fiyat 999 ETH'den fazla olmuştur (eşdeğer olarak 3M USD) (Wang ve ark., 2021). Diğer önemli bir örnek ise NBA Top Shot'tur, bu platform NBA anlarının dijital kısa videolarını satın almak/satmak için kullanılan bir NFT ticaret platformudur. Dünya genelinden binlerce NBA hayranı, 7.6 milyonun üzerinde top shot anı toplamış ve yeni yeteneklerin, veteranların ve yükselen yıldız oyuncuların kadrosunu oluşturmuştur. Picasso Punks, Hashmasks, 3DPunks, unofficial punks, Polkamon, Chubbies, Bullrun Babes, Aavegotchi, CryptoCats, MoonCats Rescue, NFT box gibi diğer projeler de büyük başarı elde etmektedir (Wang ve ark., 2021). NFT'lerin etrafında bir heves döngüsü olduğu şüphesizdir, çoğu ürün yüksek fiyatlarla satılabilmektedir, hatta bazıları yüzler veya binlerce ETH'ye (kripto para birimi) denk gelebilmektedir. Oyunlar ve koleksiyonlar dışında NFT'ler aynı zamanda sanat (Trautman, 2021), bilet etkinlikleri (Regner ve ark., 2019), değer (Chevet, 2018; Chohan, 2021), IoT (Omar ve Basir, 2020) ve finans (Dowling, 2021; Musan ve ark., 2020) gibi alanların gelişimine de katkıda bulunmaktadır.

NFT'lerle ilgili diğer pazar türleri de, istatistiksel web siteleri NonFungible.Com, DappRadar, NFT bank, DefiPulse, Coingecko, ticaret platformlar, OpenSea, SuperRare, Nifty Gateway, Rarible, Zora ve sözde NFT ekosistemleri (Dego) gibi anında bilgi sağlayan ve güvenli ortamlar sağlayan önemli roller oynamaktadır (Wang ve ark., 2021). NFT'lerin mevcut merkeziyetsiz pazarlar ve gelecekteki iş fırsatları üzerinde muazzam bir etkisi olmasına rağmen, NFT teknolojileri hala çok erken aşamadır. Bazı potansiyel zorluklar dikkatlice ele alınmalı, aynı zamanda umut verici fırsatlar da vurgulanmalıdır.

Dahası, NFT'ler hakkında çok sayıda kaynak mevcut olmasına rağmen (bloglar, wikiler, forum gönderileri, kodlar vb.), sistematik bir çalışma henüz mevcut değildir (Wang ve ark., 2021).

Bu bölümde, NFT'nin faaliyetleriyle ilgili teknik bileşenleri ele alınmıştır. Bu bileşenler, tamamen işlevsel bir NFT şemasının temelini oluşturur.

Blockchain: Nakamoto tarafından önerilmiş olup Bitcoin, dağıtık ağda işlem verileri üzerinde anlaşmaya varmak için proof of work (PoW) (Gervais ve ark., 2016) algoritmasını kullanmıştır. Blockchain, şifreleme protokolleri kullanılarak bağlantılı ve korunan bir veri kaydı listesini koruyan dağıtılmış ve sadece eklemeye izin veren bir veritabanı olarak tanımlanır (Garay ve ark., 2017). Blockchain, büyük bir güvensiz katılımcı ağıyla üzerinde anlaşılan uzun süredir süregelen Bizans sorununa (Lamport ve ark., 2019) bir çözüm sunmuştur. Paylaşılan veriler blockchain'deki dağıtılmış düğümlerin çoğu onaylandığında, depolanan verilerde yapılan herhangi bir değişiklik tüm verileri geçersiz kılar ve değişmez hale getirmektedir. NFT şemalarında yaygın olarak kullanılan en yaygın blockchain platformu Ethereum'dur (Wood, 2014) ve akıllı sözleşmelerin yürütülmesi için güvenli bir ortam sağlar. Ayrıca, bazı çözümler özelleştirilmiş zincir motorlarını veya blockchain platformlarını bırakarak uzmanlaşmış uygulamalarını desteklemek için kendi platformlarını oluşturur, bunlardan bazıları Flow, EOS, Hyperledger (Bal ve Ner, 2019; Hong ve ark., 2019) ve Fast Box (Wang ve Li, 2021)'tur.

Akıllı Sözleşme. Szabo tarafından çıkarılmış ve dijital müzakereleri hızlandırmayı, doğrulamayı veya yürütmeyi amaçlayan araçlardır. Ethereum (Wood, 2014), akıllı sözleşmeleri blockchain sistemini (Bano ve ark., 2017) (Garay ve Kiayias, 2020) daha da geliştirmiştir. Blockchain tabanlı akıllı sözleşmeler karmaşık işlevsellikleri gerçekleştirmek ve nihai tutarlılığı sağlamak için Turing-kapsamlı bir betik dili kullanmıştır. Akıllı sözleşmeler, güvenilir bir üçüncü taraf olmadan bilinmeyen tarafların ve merkezi olmayan katılımcıların adil takaslar yapmasına olanak tanır ve çeşitli endüstrilerde uygulamalar oluşturmanın birleşik bir yöntemini sunmaktadır. Akıllı sözleşmelere dayalı uygulamalar, durum geçiş mekanizmalarına dayanır. Talimatları ve parametreleri içeren durumlar, tüm katılımcılar tarafından paylaşılır ve bu talimatların yürütülmesinin şeffaflığını garanti etmektedir. Ayrıca, durumlar arasındaki konumlar dağıtılmış düğümler arasında aynı kalması gerekmektedir, bu da tutarlılığı sağlamak için önemlidir. Çoğu NFT çözümü CryptoPunks, CryptoKitties, NBA Top Shot, Picasso

Punks, Hashmasks, duyarlı yürütme için akıllı sözleşmelerden oluşan blockchain tabanlı platformlara dayanmaktadır.

Adres ve İşlem: Blockchain adresi ve işlem, kripto paralardaki temel kavramlardır. Bir blockchain adresi, kullanıcının varlıkları gönderip alması için benzersiz bir tanımlayıcıdır ve bankadaki varlıkları harcarken bir banka hesabına benzer. Bir çift genel anahtar ve özel anahtar tarafından oluşturulan belirli bir sayıda alfasayısal karakterden oluşur. NFT'leri transfer etmek için özel anahtara sahip olduğunu kanıtlaması ve doğru dijital imza ile varlıkları başka bir adrese(adreslere) göndermesi gerekmektedir. Bu basit işlem genellikle bir kripto para cüzdanı kullanılarak gerçekleştirilir ve ERC-777 (Dafflon ve ark., 2017) standardında akıllı sözleşmeleri devreye sokmak için bir işlem gönderme şeklinde temsil edilmektedir.

Veri Kodlama: Veriyi bir biçimden başka bir biçime dönüştürme işlemidir. Normalde, birçok dosya, disk alanı tasarrufu için etkili, sıkıştırılmış formatlara veya yüksek kalite/çözünürlüğe sahip bir sıkıştırılmamış formata kodlanır. Bitcoin ve Ethereum gibi yaygın blockchain sistemlerinde, işlem elemanlarını (fonksiyon adları, parametreler ve dönüş değerleri gibi) kodlamak için onaltılı değerler kullanılır. Bu, ham NFT verisinin bu kuralları izlemesi gerektiği anlamına gelir. Bir kişi, NFT tabanlı fikri mülkiyetin sahibi olduğunu iddia ederse, aslında yaratıcı tarafından imzalanan orijinal onaltılı değer parçasını sahiplendirir. Diğer kişiler ham veriyi serbestçe kopyalayabilir, ancak mülkiyetin sahibi olamazlar. Bunun temelinde, NFT ile ilgili faaliyetlerin (örneğin, satın alma/satma/takas/ihale) akıllı sözleşmelerin temel işlem prosedürüne benzer şekilde bu dört aşamada işlenmesi gerektiği gözlemlenebilir.

3.2.1. Protokoller

NFT'nin kurulması, kayıtlar için altta yatan dağıtılmış defterin yanı sıra eşler arası ağda ticaret için değiştirilebilir işlemlere ihtiyaç duyan kurumlardır. Bu bölüm, dağıtılmış defteri, NFT verilerini depolamak için özel bir veri tabanı türü olarak ele almaktadır. Bu temel alınarak, NFT paradigması için iki tasarım modeli belirlenmiştir (Wang ve ark.,2021). İlk protokol, NFT'leri başlatıcının oluşturmasını ve ardından alıcıya satmasını içeren basit ve klasik bir yaklaşımla yukarıdan aşağıya doğru kurulur. Buna karşılık, ikinci yol (örneğin, Loot), bu süreci tersine çevirir: bir NFT şablonu belirlenir ve her kullanıcı kendi benzersiz NFT'lerini oluşturabilir. Aşağıda bu iki tasarım modelinin ayrıntılı protokolleri sunulmuştur. Her ikisi için de blok zinciri sistemlerinde

yürütüldüklerinde çok benzer bir iş akışını takip ederler (bkz. Şekil 3.4). Sonuç olarak farklı tasarımlar temel işleyiş mekanizmasını değiştirmez (Wang ve ark.,2021).

Yukarıdan Aşağıya: İlk tasarım için (örneğin, CryptoPunks), bir NFT protokolü farklı iki rol içerir: NFT sahibi ve NFT alıcısı.

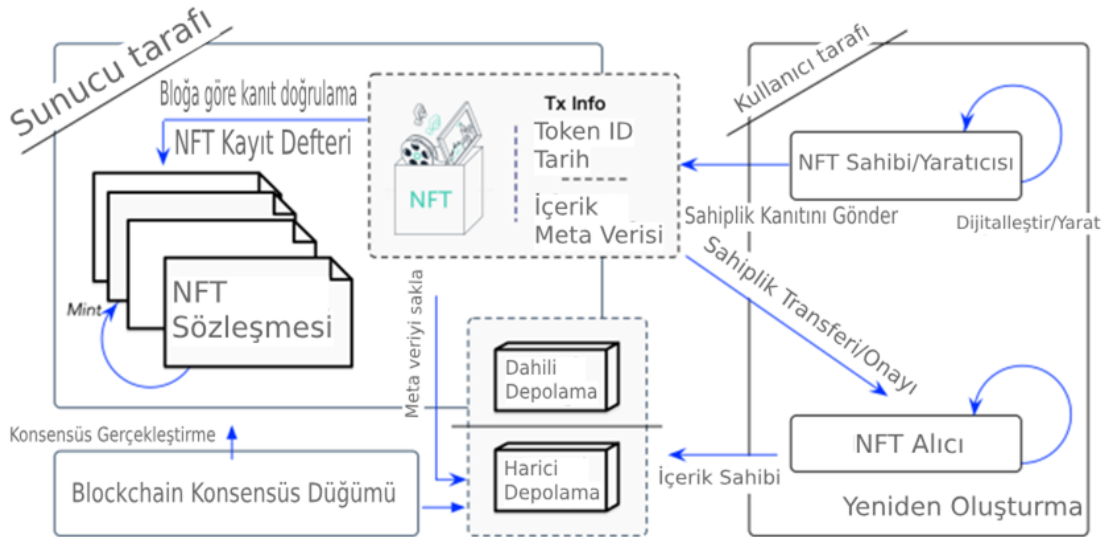
NFT Dijitalleştirme: Bir NFT sahibi, dosyanın, başlığın ve açıklamanın tamamen doğru olduğunu kontrol eder. Ardından, ham veriyi uygun bir formata dönüştürür.

NFT Depolama: Bir NFT sahibi, ham veriyi blok zinciri dışında bir harici veri tabanına kaydeder. Bu işlem gaz tüketen bir işlemidir, bu yüzden ham veriyi blok zinciri içinde depolama seçeneği de mevcuttur.

NFT İmzalama: NFT sahibi, NFT verisinin karma değerini içeren bir işlemi imzalar ve ardından akıllı bir sözleşmeye işlemi gönderir.

NFT Oluşturma ve Ticaret: Akıllı sözleşme, NFT verisiyle işlemi aldığı anda oluşturma ve ticaret süreci başlar.

NFT Onaylama: İşlem onaylandığında, oluşturma süreci tamamlanır. Bu yaklaşımla, NFT'ler benzersiz bir blok zinciri adresine sürekli olarak bağlanır ve süreklilik kanıtı olarak kullanılır. NFT Sistemlerinin İş Akışı Şekil 3.4'te belirtilmiştir.



Şekil 3.4. NFT Sistemlerinin İş Akışı

Yukarıdan Aşağıya: Bu tasarım için (örneğin, Loot), protokol iki rol içerir: NFT oluşturucu ve NFT alıcı. Çoğu durumda, bir alıcı aynı zamanda bir oluşturucu olarak hareket edebilir çünkü bir alıcı bir NFT ürününe teklif verdiğinde rastgele tohumlara dayalı olarak oluşturulur. Bu, kullanıcı özelleştirmesi açısından fonksiyonları genişletir.

Burada, öncekiyle karşılaştırıldığında farklılıkları vurgulamak için üst simge kullanılmıştır.

-Şablon Oluştur: Proje kurucusu, farklı özelliklerin (karakter tarzı, silahlar veya aksesuarlar) oyundaki temel kurallarını belirlemek için akıllı sözleşme aracılığıyla bir şablon başlatmaktadır.

-NFT Rasgeleleştirme: Bir alıcı bir NFT'ye teklif verdiğinde, temel çizgilerin üzerine ek özellikler kümesiyle NFT ürününü özelleştirebilir. Bu ek özellikler, başlangıç aşamasında önceden tanımlanmış bir veri tabanından rastgele seçilmektedir.

-NFT Oluşturma ve Ticaret. İlgili akıllı sözleşme tetiklendiğinde, oluşturma ve ticaret süreci başlar.

-NFT Onaylama. Tüm işlemler akıllı sözleşmeler aracılığıyla gerçekleştirilir. Oluşturulan NFT, uzlaşma işlemi tamamlandığında sürekli olarak blok zincirinde depolanır. Bir blok zinciri sisteminde her bloğun sınırlı bir kapasitesi vardır. Bir bloktaki kapasite dolunca, diğer işlemler orijinal veri bloğuna bağlı gelecekteki bir bloğa girer. Sonunda, tüm bağlantılı bloklar uzun vadeli bir geçmiş oluşturur ve kalıcı olarak yerini korur. NFT sistemi, esas olarak blok zinciri tabanlı bir uygulamadır. Bir NFT oluşturulduğunda veya satıldığında, akıllı bir sözleşmeyi tetiklemek için yeni bir işlem göndermek gereklidir. İşlem onaylandıktan sonra, NFT'nin meta verileri ve sahiplik bilgileri yeni bir bloğa eklenir ve bu şekilde NFT'nin geçmişi değiştirilmeden kalır ve sahiplik korunur.

3.2.2. Jeton standartları

Bu bölümde, NFT'lerle ilgili jeton standartları olan ERC-20 (Vogelsteller ve Buterin, 2015), ERC-721 (Etriken ve ark., 2018) ve ERC-1155 (Radomski ve ark., 2018) açıklanmaktadır. Bu standartlar, mevcut NFT sistemleri üzerinde büyük bir etkiye sahiptir. Aşağıda bu yöntem detaylı bir şekilde ele alınmıştır. NFT Standart Arayüzleri Şekil 3.5'te belirtilmiştir.

Algorithm 1: NFT Standard Interfaces (with selected functions)

```

interface ERC721 {
    function ownerOf(uint256 tokenId) external view returns (address);
    function transferFrom(address from, address to, uint256 tokenId)
    external payable; ...
}
interface ERC1155 {
    function balanceOf(address owner, uint256 id) external view returns
    (uint256);
    function balanceOfBatch(address[] owners, uint256[] ids) external view returns (uint256[]);
    function transferFrom(address from, address to, uint256 id, uint256
    quantity) external payable; ...
}

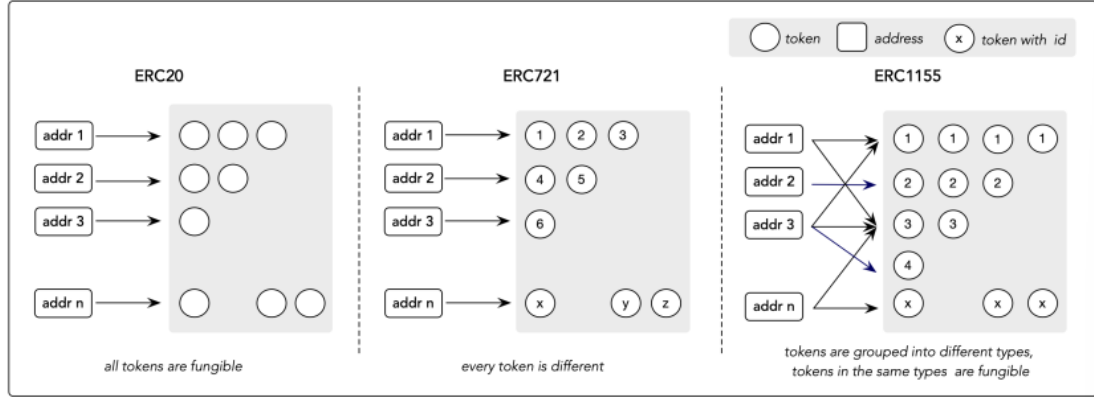
```

Şekil 3.5. NFT Standart Arayüzleri (seçilen fonksiyonlarla birlikte) (Wang ve ark., 2021)

En yaygın jeton standardı ERC-20'den (Vogelsteller ve Buterin, 2015) gelmektedir. Bu, gereklilikleri karşılayan Ethereum üzerinde çıkarılabilen değiştirilebilir jeton kavramını tanıtmaktadır. Bu standart, jetonları birbirine eşit hale getirir (hem tür hem de değer açısından). Herhangi bir jeton her zaman diğer tüm jetonlara eşittir. Bu, 2015'ten bu yana Başlangıçta Para Teklifi (ICO) çılgınlığını tetiklemiştir. Birçok genel zincir ve çeşitli blockchain tabanlı DApp'ler (Raval, 2016; Cai ve ark., 2018), bu şekilde yeterli başlangıç fonlarını elde etmektedir. Buna karşılık, ERC-721 (Etriken ve ark., 2018), değiştirilebilir jetonlardan farklı olan benzersiz bir jeton standardı tanıtır. Bu tür bir jeton benzersizdir ve başka bir jeton ile ayırt edilebilir durumdadır. Özellikle, her NFT'nin tokenId adında bir uint256 değişkeni vardır ve sözleşme adresi ve uint256 tokenId çifti küresel olarak benzersizdir. Ayrıca, tokenId, zombiler veya çizgi film karakterleri gibi özel tanımlamaların görüntüsünü oluşturmak için bir giriş olarak kullanılabilir (Wang ve ark., 2021).

Başka bir standard olan ERC-1155 (Çoklu Jeton Standardı) (Radomski ve ark., 2018), hem değiştirilebilir hem de takas olmayan jetonların temsiline olanak sağlamaktadır. Herhangi bir sayıda jetonu temsil edebilen bir arayüz geliştirmiştir. Önceki standartlarda, her sözleşmedeki her tokenId yalnızca tek bir jeton türünü içerir. Örneğin, ERC-20 her jeton türünü ayrı sözleşmelerde dağıtır. Aynı şekilde, ERC-721 benzer yapılandırmalara sahip değiştirilemez jeton grubunu tek bir sözleşmede dağıtır. Buna karşılık, ERC-1155 tokenId'in işlevselliğini genişletir, böylece her biri farklı yapılandırılabilir jeton türlerini bağımsız olarak temsil edebilir. Alanı, özel olarak

belirlenmiş bilgileri (metadata), kilitleme süresi, tarih, arz veya diğer özellikleri gibi özelleştirilmiş bilgileri içerebilir. NFT ile İlgili Jeton Standartları Şekil 3.6'da anlatılmıştır.



Şekil 3.6: NFT ile İlgili Jeton Standartları (Wang ve ark., 2021)

3.2.3. NFT'lerde istenen özellikler

NFT şemaları temelde merkezi olmayan uygulamalardır (Buterin, 2014) ve dolayısıyla altta yatan genel hesap defterinden kaynaklanan faydalar/özelliklerden yararlanırlar. Özellikleri aşağıda maddeler halinde belirtilmiştir.

- Doğrulanabilirlik. NFT, jeton meta verileri ve sahipliği halka açık olarak doğrulanabilir.
- Şeffaf İşleyiş. NFT'lerin minting (yaratma), satış ve satın alma gibi faaliyetleri halka açıktır.
- Uygunluk. NFT sistemi asla çökmemezlik özelliğine sahiptir. Alternatif olarak, tüm jetonlar ve ihraç edilen NFT'ler her zaman satışa sunulur ve alınabilir.
- Değişikliklere Karşı Dayanıklılık. NFT meta verileri ve ticaret kayıtları kalıcı olarak depolanır ve işlemler onaylandıktan sonra manipüle edilemez.
- Kullanılabilirlik. Her NFT, en güncel bilgilere sahiptir ve kullanıcı dostudur ayrıca bilgiler açık bir şekilde sunulur.
- Atomiklik. NFT'lerin ticareti, bir atomik, tutarlı, izole edilmiş ve kalıcı (ACID) işlemde tamamlanabilir. NFT'ler aynı paylaşılan yürütme durumunda çalışabilir.
- Ticaret yapılabilirlik. Her NFT ve ilgili ürünler keyfi olarak ticaret edilebilir ve takas edilebilir.

3.2.4. Güvenlik deęerlendirmesi

Bir NFT sistemi, blok zinciri, depolama ve web uygulaması gibi bileşenlerden oluşan birleşik bir teknoloji kombinasyonudur. NFT sisteminde güvenlik deęerlendirmesi zorlu bir süreçtir çünkü her bileşen bütün sistemi saldırganlara karşı savunmasız hale getirebilecek bir saldırı arayüzü haline gelmektedir. Bu nedenle, STRIDE tehdit ve risk deęerlendirmesi benimsenmiştir (Shostack ve ark., 2008). Bu deęerlendirme, bir sistemin tüm güvenlik yönlerini kapsamaktadır: kimlik doęrulama, bütünlük, inkar edilemezlik, kullanılabilirlik ve erişim kontrolü. Potansiyel güvenlik sorunları araştırılmış ve bu sorunları çözmek için bazı savunma mekanizmaları önerilmiştir (bkz. Çizelge 3.3) (Wang ve ark., 2021).

Sahtekarlık. Sistemde başka bir varlık (örneğin başka bir kişi veya bilgisayar) taklit etme yeteneğidir ve kimlik doęrulama ile ilgilidir. Bir kullanıcı NFT'lerin yaratılması veya satılması için etkileşimde bulunduğunda, kötü niyetli bir saldırgan kimlik doęrulama zafiyetlerinden yararlanabilir veya kullanıcının özel anahtarını çalabilir, ayrıca NFT'lerin sahipliğini yasa dışı olarak transfer edebilir. Bu nedenle özel anahtar sızıntılarını önlemek için NFT akıllı sözleşmesinin resmi olarak doęrulanmasını ve soğuk cüzdan kullanılmasını önerir.

Deęiştirme. NFT verilerinin kötü niyetli bir şekilde deęiştirilmesini ifade eder ve bütünlüğe aykırıdır. Blok zinciri sağlam bir genel işlem defteri olduğunu varsayalım (Garay ve ark., 2015; Garay ve ark., 2017) ve bir karma algoritması ön resim direncine ve ikinci resim direncine sahip olsun (Rogaway ve Shrimpton, 2004). NFT'lerin meta verileri ve sahiplięi, işlemin onaylandıktan sonra kötü niyetli olarak deęiştirilemez. Ancak, blok zinciri dışında depolanan veriler manipüle edilebilir. Bu nedenle kullanıcıların NFT ile ilgili özelliklerle ilgili ticaret/takas sırasında hem hash verilerini hem de orijinal verileri NFT alıcısına göndermelerini önerir.

İnkar edilemezlik. Bir ifadenin sahibinin inkar edememesi durumunu ifade eder ve güvenlik özellięi ile ilgilidir (Menezes ve ark., 2018). Özellikle, bir kullanıcının başka bir kullanıcıya NFT gönderdięi gerçeęi inkar edilemez. Bu, blok zinciri güvenlięi ve bir imza şemasının sahtecilięi önleme özellięi tarafından garanti altına alınır. Ancak, karma veriler kötü niyetli bir saldırgan tarafından manipüle edilebilir veya karma veriler bir saldırganın adresiyle bağlanabilir. Bu nedenle, çoklu imza sözleşmesi kullanmanın bu sorunu kısmen çözebileceęine inanmaktadır çünkü her bağlam birden fazla katılımcı tarafından onaylanmalıdır.

Bilgi Açıklanması. Bilgi sızıntısı, bilginin yetkisiz kullanıcılara maruz kalması durumunda ortaya çıkar ve gizlilik ihlalidir (Menezes ve ark., 2018). NFT sisteminde, akıllı sözleşmelerdeki durum bilgileri ve talimat kodu tamamen şeffaftır ve herhangi bir gözlemci tarafından herhangi bir durum ve değişiklikleri kamuoyunda erişilebilir durumdadır. Kullanıcı sadece NFT karmasını blok zincirine koyarsa, kötü niyetli saldırganlar kolayca karmayı ve işlemi birbirine bağlayabilir. bu nedenle, NFT geliştiricisinin kullanıcı gizliliğini korumak için düz akıllı sözleşmeler yerine gizliliği koruyan akıllı sözleşmeler (Li ve ark., 2019; Li ve ark., 2020) kullanmasını önermektedir. NFT'lerin Potansiyel Güvenlik Sorunları ve Karşılık Gelen Çözümler Çizelge 3.3'te belirtilmiştir.

Çizelge 3.3. NFT'lerin Potansiyel Güvenlik Sorunları ve Karşılık Gelen Çözümler (Wang ve ark., 2021).

	Güvenlik Sorunları	Sonuçlar
Sahtecilik (Kimlik Doğruluğu)	Bir saldırgan kimlik doğrulama açıklarını sömürebilir. Bir saldırgan bir kullanıcının özel anahtarını çalabilir.	Akıllı sözleşmede formel doğrulama Özel anahtar sızıntısını önlemek için soğuk cüzdan kullanmak
Manipülasyon (Bütünlük)	Blok zinciri dışında depolanan veriler manipüle edilebilir.	NFT'leri ticaret yaparken hem orijinal veriyi hem de karma veriyi NFT alıcısına gönderme
Reddetme (İnkâr Edilemezlik)	Karması aldatıcının adresiyle bağlantı kurabilir.	Kısmen çok imzalı bir sözleşme kullanma
Bilgi Açıklaması (Gizlilik)	Bir saldırgan kolaylıkla karma ve işlemi kullanarak belirli bir NFT alıcısını veya satıcısını bağlayabilir.	Kullanıcının gizliliğini korumak için akıllı sözleşmeler yerine gizlilik koruyucu akıllı sözleşmeler kullanma

Hizmet Reddi (Erişilebilirlik)	NFT verileri, varlık blok zinciri dışında depolanıyorsa kullanılamaz hale gelebilir.	Zayıf bir konsensüs algoritmasıyla hibrit blok zinciri mimarisi kullanma
Yetki Yükseltme (Yetkilendirme)	Kötü tasarlanmış bir akıllı sözleşme, nft'lerin böyle özelliklerini kaybetmesine neden olabilir	Akıllı sözleşmelerde formel doğrulama

Hizmet Reddi (DoS). DoS saldırısı (Moore ve ark., 2006), kötü niyetli bir saldırganın normal işlevlerini kesintiye uğratarak bir sunucuyu kullanıcılarına erişilemez hale getirmeyi hedeflediği bir tür ağ saldırısıdır. DoS, kullanılması izinsiz olanlar tarafından gerçekten kullanılabilen NFT hizmetinin kullanılamaz hale gelmesine ve çökmesine neden olur. Neyse ki, blok zinciri kullanıcının işlemlerinin yüksek kullanılabilirliğini garanti etmektedir.

Yetki Yükseltme. Yetki Yükseltme (Shostack ve ark., 2019), yetkilendirme ile ilgili bir özelliktir. Bu tür bir tehditte, saldırgan başlangıçta verilen izinlerin ötesinde izinler elde edebilir. NFT sisteminde, satma izinleri bir akıllı sözleşme tarafından yönetilir. Yine de kötü tasarlanmış bir akıllı sözleşme NFT'lerin bu tür özelliklerini kaybetmesine neden olabilir.

3.2.5. Güvenlik ve gizlilik sorunları

Kullanıcı verilerinin güvenliği sistemlerin birinci önceliğidir. Bununla birlikte, (blok zincirine bağlı zincirin dışında depolanan) veriler, bağlantıyı kaybetme veya kötü niyetli taraflarca kötüye kullanılma riski taşır. Bunlar aşağıda ayrıntılı olarak açıklanmaktadır.

- NFT Veri Erişilemezliği. Ana akım NFT projelerinde (Flow , Sandbox Decentraland), bir dosyanın kopyası yerine belirteçle etiketlenen ve ardından gaz tüketimini azaltmak için blok zincirinde kaydedilen bir kriptografik "hash" tanımlayıcı olarak kullanılır. Bu, kullanıcının NFT'ye olan güvenini kaybetmesine neden olabilir çünkü orijinal dosya kaybolabilir veya zarar görebilir. Birkaç NFT projesi, IPFS (Gezegenlerarası Dosya Sistemi)(Benet, 2014) gibi özel bir dosya depolama sistemiyle entegre edilmiştir. IPFS adresleri, birisinin IPFS ağındaki herhangi bir yerde

barındırıyorsa bir içeriği bulmanıza olanak sağlar. Bu tür sistemler çok fazla hatalara sahiptir. Kullanıcılar NFT meta verilerini IPFS düğümlerine "yüklerken", verilerinin tüm düğümler arasında replike edileceğinin garantisi yoktur. Eğer varlık IPFS üzerinde depolanıyorsa ve bunu depolayan tek düğüm ağdan ayrılmışsa, veri erişilemez hale gelebilir (Benson, 2021). Bu sorun DECRYPT.IO (Benson, 2021) tarafından rapor edilmiştir. Ayrıca, bir NFT yanlış bir dosya adresine işaret edebilir. Bu durumda, bir kullanıcı NFT'ye gerçekten sahip olduğunu kanıtlayamaz. Kısacası, NFT sistemi için dış sistemlere (depolama) dayanmak zayıflıktır.

-Anonimlik/Gizlilik. Mevcut aşamada, NFT'lerin anonimliği ve gizliliği hala yeterince çalışılmamıştır. Çoğu NFT işlemi, sadece takma ad olarak pseudo-anonimlik sağlayan temel Ethereum platformuna dayanır. Kullanıcılar gerçek kimlikleriyle ilgili bağlantılar halka açık değilse kısmen kimliklerini gizleyebilirler. Aksi takdirde, açığa çıkan adres altında kullanıcıların tüm faaliyetleri gözlemlenebilir. Mevcut gizlilik koruma çözümleri (örneğin, homomorfik şifreleme (Wang ve ark., 2020), sıfır bilgi ispatı (Wang ve Kogan, 2018), halka imza (Noether, 2015), çok taraflı hesaplama (Raman ve ark., 2018)) karmaşık şifreleme öğeleri ve güvenlik varsayımları nedeniyle henüz NFT ile ilgili düzenlemelere uygulanmamıştır (Wang ve ark., 2021). Diğer blok zinciri tabanlı sistemler gibi, hesaplama maliyetlerini azaltmak, gizlilik vadeden düzenlemelerin uygulanmasında anahtar olmaktadır.

3.2.6. Genişletilebilirlik sorunları

NFT sistemlerinin genişletilebilirliği iki yönlüdür. İlk olarak, bir sistemin diğer ekosistemlerle etkileşime geçebilme yeteneği üzerinde durulur. İkincisi, mevcut sürüm geride kaldığında NFT sistemlerinin güncellemeler alıp alamayacağına odaklanır.

- NFT Uyumluluğu (çapraz zincir). Mevcut NFT ekosistemleri birbirinden izole edilmiştir. Kullanıcılar bir tür ürün seçtiğinde, yalnızca aynı ekosistem/ağ içinde bunları satın alabilir/satabilir/takas edebilir. Bunun nedeni temelindeki blok zinciri platformudur. Uyumluluk ve çapraz zincir iletişimi, DApp'lerin geniş çapta benimsenmesi için her zaman engeller olmuştur. (Zamyatin ve ark., 2019) gözlemlerine dayanarak, çapraz zincir iletişimlerini dış güvenilir tarafların yardımıyla uygulanabilir. Bu şekilde, merkeziyetçilik özelliği kısmen kaybedilmiştir. Neyse ki, NFT ile ilgili projelerin çoğu temel olarak Ethereum'u kullanmaktadır. Bu, benzer bir veri yapısına sahip olduklarını ve aynı kurallar altında değiş tokuş yapabileceklerini göstermektedir.

- Güncellenebilir NFT'ler. Geçiş dönemi blok zincirleri protokollerini yumuşak çatal (geleceğe yönelik uyumlu küçük değişiklikler) ve sert çatal (önceki protokollerle çelişebilecek önemli değişiklikler) aracılığıyla günceller. Var olan bir blok zincirine güncellemelerin uygulanmasıyla ilgili zorluklar ve takaslar (Ciampi ve ark., 2020) belirtilmiştir. Genel modele rağmen, yeni bir sürüm hala belirli düşmanca davranışları tolere etme ve güncelleme sürecinde çevrimiçi kalma gibi sıkı gereksinimlerle karşı karşıyadır. NFT sistemleri temel platformlarına sıkı sıkıya bağlıdır. Veriler genellikle ayrı bileşenlerde (IPFS dosya sistemi gibi) depolanırken, en önemli mantık ve jeton zinciride kaydedilir. İyileştirmelerle sistemin düzgün bir şekilde güncellenmesi bir gereklilik olacaktır.

3.3. Video ve Dijital Filigranlama

3.3.1 Filigranlamanın gerekliliği

Dijital verilerin analog verilere göre birçok avantajı olmasına rağmen, hizmet sağlayıcılar, telif hakkı korumalarının olmaması ve telif hakkıyla korunan materyalin sınırsız kopyalanması ve dağıtılması korkusu nedeniyle hizmetleri dijital biçimde sunmakta tereddüt ediyorlardı. Telif hakkı sorunlarından dolayı, dijital olarak kaydedilmiş materyalin fikri mülkiyeti korunmalıdır (Samuelson, 1991). Telifli içerik için yeterli koruma sistemlerinin bulunmaması, dijital versatile disk (DVD) (Taylor, 1997) tanıtımının gecikmesinin nedeni olabilir. Bazı medya şirketleri, kopya koruma sorunu çözülene kadar DVD materyali sunmayı reddetmiştir (Rupley, 1996; Renaud, 1996). Tüketici elektroniği endüstrisi ve film endüstrisinin temsilcileri dijital video kayıt cihazlarıyla ilgili yasal düzenlemeler aramaya başlamışlardır. Fikri mülkiyeti ve tüketicilerin haklarını koruyan yolları tanımlayan öneriler, ABD (Amerika Birleşik Devletleri) Kongresine sunulmuştur (Renaud, 1996) ve 28 Ekim 1998 tarihinde Başkan Clinton tarafından imzalanan Digital Millennium Copyright Act yasasına yol açmıştır. Avrupa Birliği, CD (Kompakt Disk)'ler veya DVD'ler de dahil olmak üzere dijital multimedya ürünleri için böyle bir fikri mülkiyet hakları koruması hazırlamaktadır (Langelaar ve ark., 2000).

Dijital ses ve video verilerinin kopya koruması ve telif hakkı koruması sağlamak için iki tamamlayıcı teknik geliştirilmiştir: şifreleme ve filigranlama (Cox ve Miller, 1997). Şifreleme teknikleri, verilerin göndericiden alıcıya iletilmesi sırasında dijital

verileri korumak için kullanılabilir (Langelaar, 1999). Ancak, alıcı verileri aldıktan ve şifre çözüldükten sonra, veri orijinal veriyle aynı hale gelir ve koruma kalkar. Filigranlama teknikleri, bir filigran adı verilen gizli algılanamaz bir sinyali doğrudan orijinal veriye gömerek şifrelemeyi tamamlayabilir. Bu tür bir filigran, aşağıdaki amaçlar için kullanılabilir:

- Telif Hakkı Koruması: Fikri mülkiyetin korunması için veri sahibi, verisine telif hakkı bilgisini temsil eden bir filigran gömebilir. Bu filigran, telif haklarının ihlal edildiği durumlarda mahkemede sahipliğini kanıtlayabilir.

- Parmak İzi (Fingerprinting): Yasadışı kopyaların kaynağını takip etmek için, sahip, parmak izi tekniklerini kullanabilir. Bu durumda, sahip, farklı müşterilere sağlanan verilerin kopyalarına farklı filigranlar gömebilir. Parmak izi, veriyle ilişkili müşteri kimliğiyle ilişkilendirilen bir seri numarasının veriye gömülmesine benzetilebilir. Bu, fikri mülkiyet sahibinin, verileri üçüncü taraflara sağlayarak lisans sözleşmesini ihlal eden müşterileri belirlemesini sağlamaktadır.

- Kopya Koruma: Bir filigranda saklanan bilgiler, kopya koruma amacıyla doğrudan dijital kayıt cihazlarını kontrol edebilir (Langelaar ve ark., 1998). Bu durumda, filigran bir kopya yasağı biti temsil eder ve kaydediciye yönelik filigran tespit cihazları, kaydediciye sunulan verilerin depolanıp depolanamayacağını belirler.

- Yayın İzleme: Ticari reklamlara filigranlar gömülerek, otomatik bir izleme sistemi reklamların sözleşmeye uygun bir şekilde yayınlanıp yayınlanmadığını doğrulamaktadır (Anderson ve Petitcolas, 1998). Yalnızca reklamlar değil, değerli televizyon ürünleri de yayın izlemesiyle korunabilir (Kalker ve ark., 1999). Haber öğeleri, saatte 100.000 dolardan daha yüksek bir değere sahip olabilir, bu da onları fikri mülkiyet hakları ihlaline karşı çok savunmasız hale getirir. Bir yayın gözetleme sistemi, tüm yayın kanallarını kontrol edebilir ve televizyon istasyonlarına farklı ücretlendirme yapabilir.

- Veri Doğrulama: Kırılgan filigranlar (Wolfgang ve Delp, 1999), verinin orijinalliğini kontrol etmek için kullanılabilir. Kırılgan filigran, verinin değiştirilip değiştirilmediğini belirtir ve verinin hangi noktalarda değiştirildiğine ilişkin yerel bilgi sağlar. Filigranlama teknikleri, sadece koruma amaçları için değil, diğer uygulamalar için de kullanılır.

- İndeksleme: Video posta için indeksleme, yorumların video içine gömülebileceği; film ve haber öğeleri için indeksleme, arama motorları tarafından kullanılacak işaretçi ve yorumların eklenmesi olarak bilinir.

- Tıbbi Güvenlik: Tarih ve hastanın adının tıbbi görüntülere gömülmesi, faydalı bir güvenlik önlemi olabilmektedir (Anderson ve Petitcolas, 1998).

- Veri Gizleme: Filigranlama teknikleri, gizli özel mesajların iletilmesinde kullanılmaktadır. Çeşitli hükümetler şifreleme hizmetlerinin kullanımını kısıtladığından, insanlar mesajlarını başka verilerin içine gizlemektedirler.

Bazı yazarlar, örneğin (Bender ve ark., 1996) çalışmasında, filigranlama tekniğinden yalnızca birkaç bit (bir bit kadar az) verinin telif hakkı bildirimine/koruma uygulamalarına gömüldüğü durumda bahseder. Diğer uygulamaların ise veri gömme kategorisine girdiği düşünülmektedir. Ancak (Langelaar ve ark., 2000) makalelerinde tüm bu uygulamalar için damgalama terimini kullanmayı tercih etmektedir. Onların görüşüne göre filigran, günümüzde kopya koruma/doğrulama sınırlarının ötesindeki uygulamalar için kullanılmaktadır, örneğin Digimarc'ın Akıllı Görüntüleri (Alattar, 2000).

3.3.2. Filigranlama gereksinimleri

Her filigranlama uygulamasının kendine özgü gereksinimleri vardır. Bu nedenle, tüm filigranlama teknikleri için karşılanması gereken bir gereksinim seti yoktur. Bununla birlikte, yukarıda bahsedilen çoğu uygulama için genel yönergeler verilebilir:

Algısal Şeffaflık: Çoğu uygulamada, filigranlama algoritması, gömülü filigranın altta yatan ana verinin kalitesini etkilemeden gömülmesi gerekmektedir. Bir filigran gömme işlemi, insanların orijinal veriyi filigranlı veriden ayırt edememesi durumunda gerçekten algılanamaz kabul edilmektedir (Swanson ve ark., 1998). Bununla birlikte, orijinal veri doğrudan filigranlı veriyle karşılaştırıldığında, en küçük değişiklik bile fark edilebilir hale gelebilmektedir. Filigranlı veri kullanıcıları genellikle orijinal veriye erişimleri olmadığı için bu karşılaştırmayı yapamazlar. Bu nedenle, filigranlı verideki değişiklikler, veriler orijinal veriyle karşılaştırılmadığı sürece fark edilmez olabilmektedir (Voyatzis ve ark., 1998).

Filigranın Taşıdığı Veri Yüğü: Bir filigranda depolanabilecek bilgi miktarı uygulamaya bağlıdır. Kopya koruma amaçları için genellikle bir bitlik veri yükü yeterlidir.

Uluslararası Fonografik Endüstrisi Federasyonu'ndan (IFPI) gelen bir ses filigranlama teknolojisi önerisine göre, bir ses filigranının minimum veri yükü, sinyal seviyesi ve müzik türünden bağımsız olarak saniyede 20 bit olmalıdır (Langelaar ve ark.,

2000). Bununla birlikte, (Petitcolas ve ark., 1998) çalışmasına göre, bu minimum değer çok iddialıdır ve sadece birkaç bitlik bir değere düşürülmelidir.

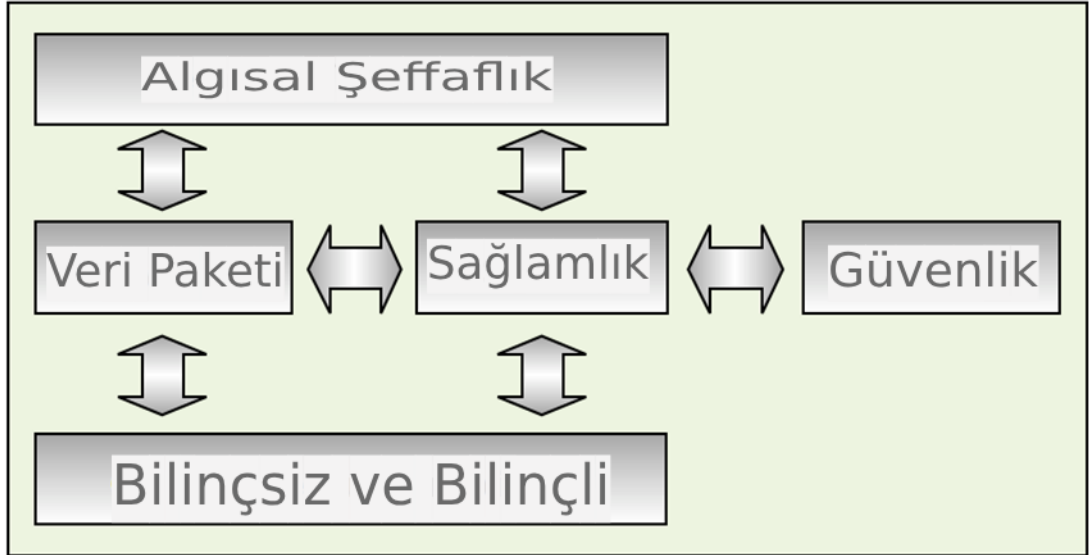
Fikri mülkiyet haklarının korunması için ISBN (Uluslararası Standart Kitap Numarası) veya daha iyisi ISRC (Uluslararası Standart Kayıt Kodu) gibi bir miktar bilginin gömülmesinin istendiğini varsaymak mümkün görünmektedir. Buna ek olarak, telif hakkı yılı, eserde verilen izinler ve derecelendirme gibi bilgiler de eklenmelidir (Kutter ve Petitcolas, 1999). Bu, yaklaşık olarak 60 bit (Fridrich ve Goljan, 1999) veya 70 bit (Kutter ve Petitcolas, 1999) bilginin ana veriye, görüntüye, video karesine veya ses parçasına eklenmesi gerektiği anlamına gelir.

Dijital ses ve video için filigran yüküyle ilgili başka bir önemli kavram, filigran ayrıntısıdır. Filigran ayrıntısı, bir birim filigran bilgisi gömmek için ne kadar veriye ihtiyaç duyulduğunu temsil eder. Yukarıdaki örneği kullanarak, bir birim filigran bilgisi 60 veya 70 bitlik bir bilgiyi içerir. Bu, tek bir video karesine eklenebilir veya 100 video karesi üzerine yayılabilir (veya aynı şekilde ses için, filigran 1 saniyelik bir parçada gömülebilir. Örneğin 5 saniyelik ses verisine yayılabilir). Filigranın bu şekilde yayılması istenmeyebilir çünkü birisi sadece filigranlı videodan 80 kare alırsa, filigran bilgisi artık geri alınamaz hale gelir. Dijital videolar için, 1 saniye video en küçük telif hakkına sahip birim olarak kabul edilir. Bu nedenle, filigran bilgisi, 1 saniyeden daha kısa bir video parçasına (yaklaşık olarak 25 kare) gömülmelidir. Yine yukarıdaki örneği kullanarak, filigran bit hızı 70 bit/s'den fazla olmalıdır (Langelaar ve ark., 2000).

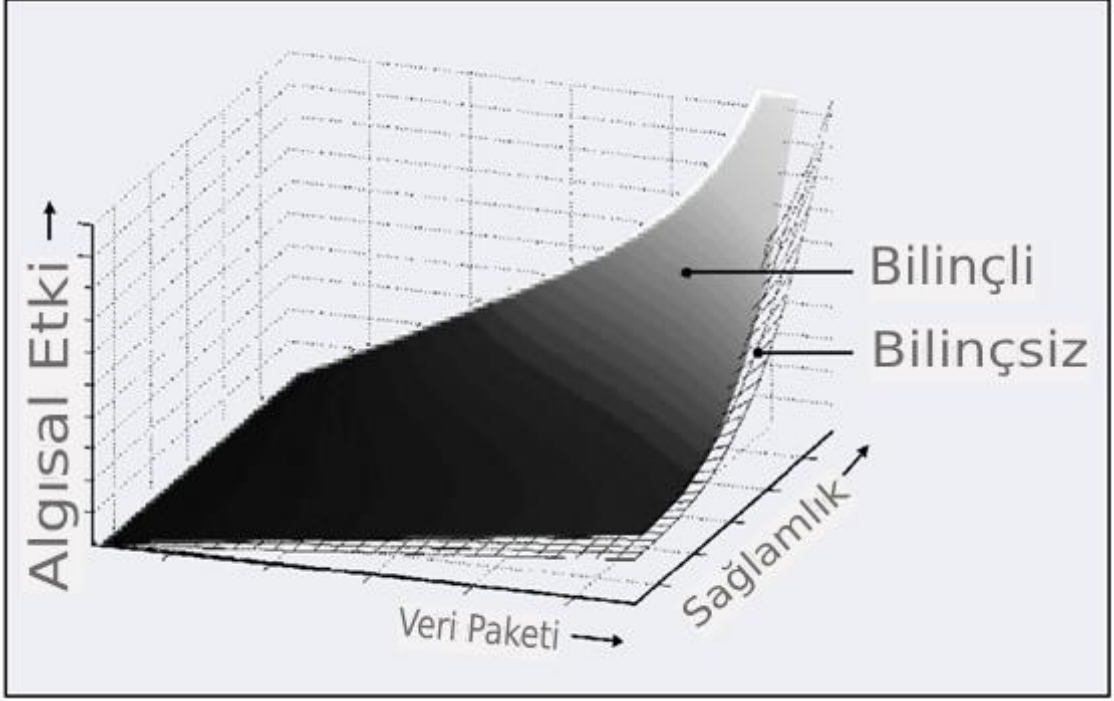
Dayanıklılık: Ana verinin otantik olup olmadığını kanıtlamak için hassas bir filigranın, ana verinin işleme tekniklerine veya kasıtlı değişikliklerine karşı dayanıklı olması gerekmez, çünkü filigranın algılanamaması, ana verinin değiştirildiğini ve artık otantik olmadığını kanıtlamaktadır. Bununla birlikte, başka bir uygulama için filigran kullanılıyorsa, filigranın kalitesi kasıtlı veya kasıtsız şekilde bozursa bile her zaman ana veride kalması istenmektedir. Kasıtsız kalite bozucu işlemler arasında veri depolama veya iletimi içeren uygulamalar bulunur, bu durumda veriye kayıplı sıkıştırma teknikleri uygulanır. Diğer kasıtsız kalite bozucu işlemler ise filtreleme, yeniden örnekleme, dijital-analog (D/A) ve analog-dijital (A/D) dönüşümüdür. Öte yandan, bir filigran sadece filigranı kaldırmak için yapılan işlemlere tabi tutulabilir (I. Cox ve Miller, 1997). Ayrıca, aynı içeriğin farklı filigranlarla çok sayıda kopyası varsa, parmak izleme için durumun ortaya çıkması nedeniyle filigranın kaldırılması mümkündür. Genel olarak, filigranın kullanılmadan veya değiştirilmeden çıkarılabilmesi için ana verinin algısal kalitesinin

yeterince bozulması gerekmektedir, böylece kullanılamaz hale gelir (Langelaar ve ark., 2000).

Güvenlik: Filigranlama tekniklerinin güvenliği, şifreleme tekniklerinin güvenliğiyle aynı şekilde yorumlanabilir. Kerckhoff'un varsayımı, verileri şifrelemek için kullanılan yöntemin yetkisiz bir tarafa bilindiğini ve güvenliğin bir anahtarın seçiminde toplandığı belirtilir (Massey, 1992). Bu nedenle, bir filigranlama tekniği, filigranı gömmek ve çıkarmak için kullanılan tam algoritmaların bilinmesinin yetkisiz bir tarafa filigranın varlığını tespit etmede veya kaldırmada yardımcı olmaması durumunda çok daha güvenlidir (Swanson ve ark., 1998). Temel gereksinimler arasındaki karşılıklı bağımlılıklar ve Güvenli bir filigran için temel gereksinimler arasındaki ilişkinin gösterimi şekil 3.7 ve 3.8'de gösterilmiştir.



Şekil 3.7. Temel gereksinimler arasındaki karşılıklı bağımlılıklar (Langelaar ve ark., 2000)



Şekil 3.8. Güvenli bir filigran için temel gereksinimler arasındaki ilişkinin gösterimi. (Langelaar ve ark., 2000)

Bilinçli ve bilinçsiz filigranlama: Telif hakkı koruması ve veri izleme gibi bazı uygulamalarda, filigran çıkarma algoritmaları orijinal filigranlı olmayan veriyi kullanarak filigranı bulabilmektedir. Buna bilinçsiz filigranlama denir (Kutter ve Peticolas, 1999). Diğer birçok uygulamada, örneğin kopya koruma ve indeksleme gibi uygulamalarda, filigran çıkarma algoritmaları orijinal filigranlı olmayan veriye erişemez. Bu, filigran çıkarımını daha zor hale getirmektedir. Bu tür filigranlama algoritmalarına genel, kör veya Bilinçli filigranlama algoritmaları denir.

Yukarıda listelenen gereksinimler birbirleriyle ilişkilidir. Örneğin, her bir filigran biti için ana veriye çok sayıda büyük değişiklikler yaparak çok sağlam bir filigran elde edilebilir. Ancak, ana verideki büyük değişiklikler fark edilebilir ve her filigran biti için çok fazla değişiklik, bir veri nesnesinde depolanabilecek maksimum filigran bit miktarını sınırlar. Bu nedenle, farklı gereksinimler arasında bir denge göz önünde bulundurulmalıdır, böylece her uygulama için optimal bir filigran geliştirilebilir. Temel gereksinimler arasındaki karşılıklı bağımlılıklar Şekil 3.7'de gösterilmiştir.

İyi tasarlanmış güvenli bir filigran için temel gereksinimler arasındaki ilişki Şekil 3.8'de temsil edilir. Algısal etki eksenleri, filigranlama nedeniyle verinin kalite bozulmasını temsil eder. Algısal etki ne kadar yüksekse, kalite bozulması o kadar kötü

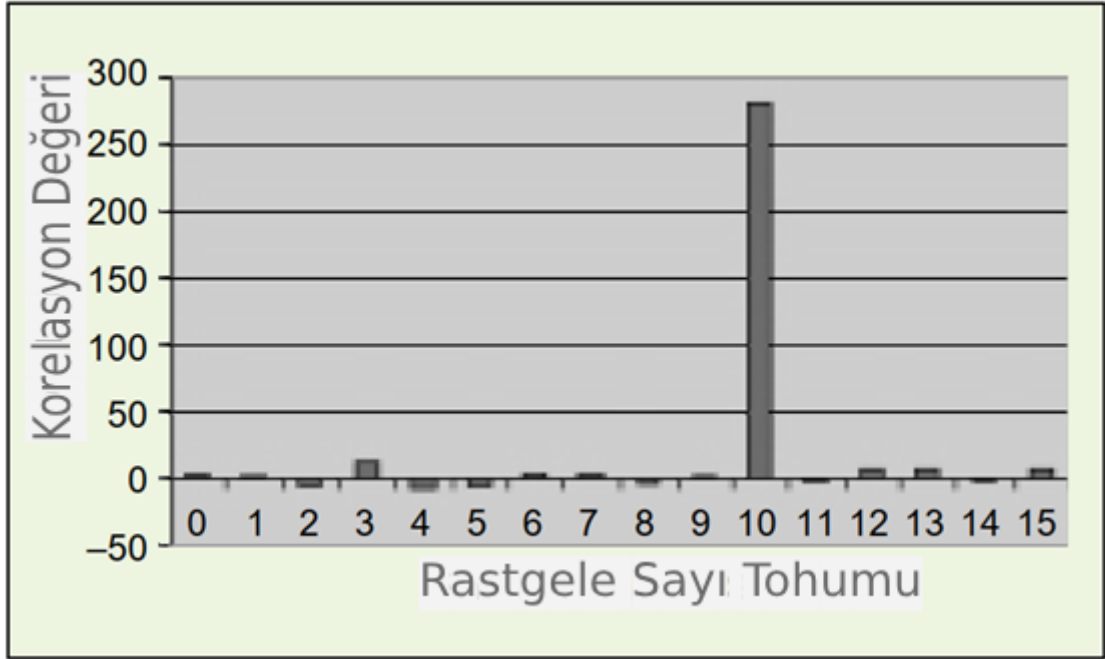
olur. Yük eksenleri, veriye gömülebilecek veri miktarını temsil eder. Dayanıklılık eksenleri, filigranlama sisteminin saldırılara karşı direnme yeteneğini temsil eder. Bir filigranın güvenliği, dayanıklılığı büyük ölçüde etkilemektedir. Eğer bir filigran güvenli değilse, dayanıklı değildir.

3.3.3. Korelasyon temelli filigranlama teknikleri: mekansal alan temel tekniği

Mekansal alanda bir görüntüye filigran eklemenin en basit yolu, piksellerin parlaklık değerlerine bir sözde rastgele gürültü deseni eklemektir. Bu prensibe dayanan birçok yöntem bulunmaktadır (Schyndel ve ark., 1994; Bender ve ark., 1995; Caronni, 1995; Pitas ve Kaskalis, 1995; Hartung ve Girod, 1996; Pitas, 1996; Smith ve Comiskey, 1996; Wolfgang ve Delp, 1996; Langelaar ve ark., 1997; Wolfgang ve Delp, 30 Haziran - 3 Temmuz 1997; Wolfgang ve Delp, Kasım 1997; Zeng ve Liu, 1997; Fridrich, 1999), (Kalker ve ark., 1999; Wolfgang ve Delp, 1999; Hanjalic ve ark., 2000). Genel olarak, sözde rastgele gürültü deseni özellikle $\{-1,0,1\}$ gibi tamsayılarla temsil edilir, ancak ondalık sayılar da kullanılabilir. Desen, tohumlar, doğrusal kaydırma kayıtları veya rastgele karıştırılmış ikili görüntüler gibi bir anahtar kullanılarak oluşturulur. Tek kısıtlamalar, desendeki enerjinin daha az homojen dağıtılmış olması ve desenin ana görüntü içeriğiyle ilişkili olmamasıdır. Filigranlı görüntüyü oluşturmak için $I_w(x, y)$, sözde rastgele desen $W(x, y)$ küçük bir kazanç faktörü k ile çarpılır ve ana görüntü $I(x, y)$ üzerine eklenir.

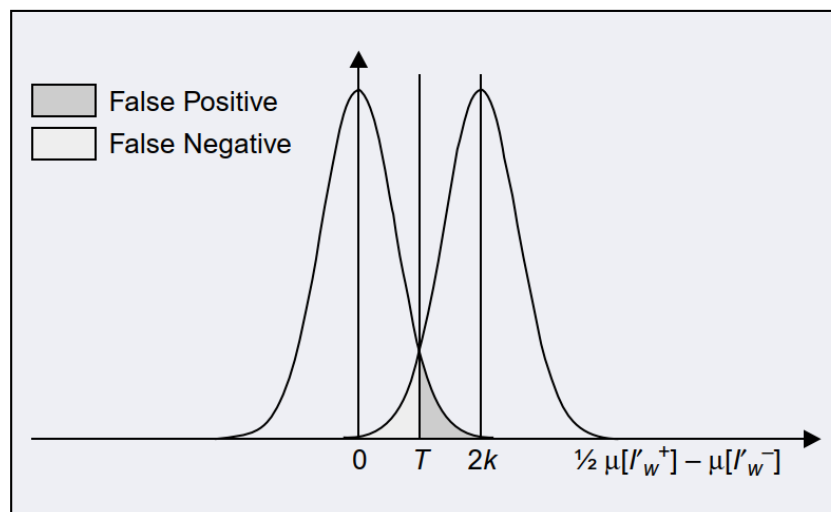
$$I_w(x,y)=I(x,y)+k.W(x,y). \quad (3.1)$$

Bir potansiyel olarak filigranlı bir görüntüde $I'_w(x,y)$ filigranı tespit etmek için, görüntü (x, y) ile sözde rastgele gürültü deseni $W(x, y)$ arasındaki korelasyonu hesaplanır. Genel olarak, $W(x, y)$ korelasyondan önce sıfır ortalama değerine normalize edilir. Farklı anahtarlar kullanılarak oluşturulan sözde rastgele desenler arasındaki korelasyon çok düşüktür. Bu nedenle, tespit sürecinde doğru anahtarla oluşturulan sözde rastgele bir desen için korelasyon değeri çok yüksek olacak ve aksi durumda da çok düşük olacaktır. Tohum=10 ile oluşturulan bir pseudo-random örüntü için diğer tohumlarla oluşturulan rasgele örüntüler arasındaki korelasyon değerleri Şekil 3.9'da verilmiştir.



Şekil 3.9. Tohum=10 ile oluşturulan sözde rastgele model için diğer tohumlarla oluşturulan sözde rastgele modeller arasındaki korelasyon değerleri. (Langelaar ve ark., 2000)

Şekil 3.9, 0 ile 15 arasında değişen tohumlar kullanılarak oluşturulan bazı pseudo-rastgele desenlerin filigranlı görüntüye olan korelasyon değerlerini göstermektedir. Doğru tohum (10) kullanıldığında korelasyonun çok yüksek olduğu, yanlış tohumlar kullanıldığında ise korelasyonun çok düşük olduğu görülmektedir. Filigran Tespit İşlemi Şekil 3.10’da gösterilmiştir.



Şekil 3.10. Filigran Tespit İşlemi. (Langelaar ve ark., 2000)

Tespit sürecinde genellikle bir eşik değeri T ile belirlenir ve filigranın tespit edilip edilmediğine karar verilir. Eğer korelasyon belirli bir eşik değeri T 'yi aşarsa, filigran dedektörü görüntünün $I'_w(x,y)$ filigranı $W(x,y)$ içerdiğini belirler.

$$\begin{aligned} R_{I'_w(x,y)W(x,y)} > T &\rightarrow W(x,y) \text{ tespit edildi.} \\ < T &\rightarrow W(x,y) \text{ tespit edilmedi.} \end{aligned} \quad (3.2)$$

$W(x,y)$ yalnızca $\{-1, 1\}$ tam sayılarından oluşuyorsa ve -1 'lerin sayısı 1 'lerin sayısına eşitse, korelasyon aşağıdaki gibi tahmin edilebilir:

$$R_{I'_w(x,y)W(x,y)} = 1/N \sum_{i=1}^N I'_w(x,y) W_i(x,y) = 1/2 \{ \mu[I_w^+(x,y)] - \mu[I_w^-(x,y)] \} \quad (3.3)$$

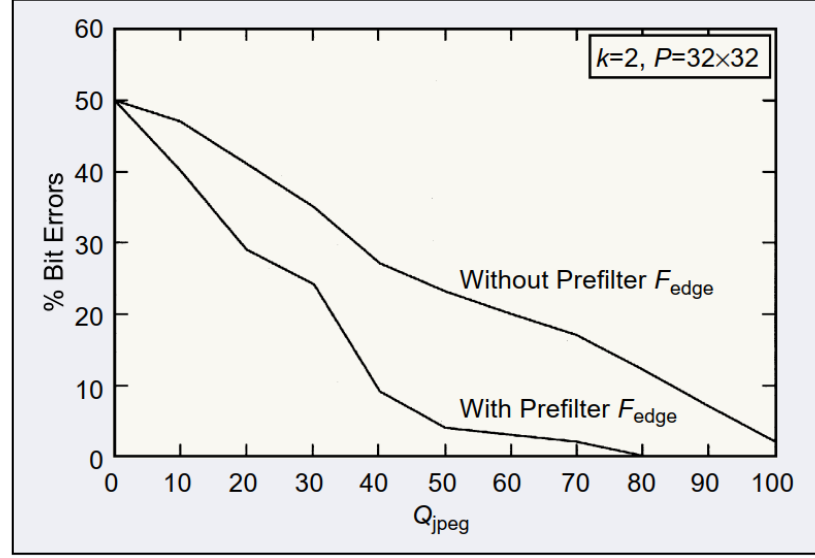
Burada N , I'_w resmindeki piksellerin sayısını temsil eder ve aynı zamanda karşılık gelen gürültü deseninin pozitif veya negatif olduğu piksellerin kümesini ifade eder. $\mu[I_w^+(x,y)]$ ise $I_w^+(x,y)$ içindeki piksellerin ortalama değerini gösterir. (3.3)'den anlaşılacağı üzere, filigranın tespit sorunu, filigranlı bir görüntüde rastgele seçilmiş iki piksel kümesinin aynı ortalamaya sahip olup olmadığı hipotezini test etmekle ilgilidir.

Tespit süreci sırasında, filigranı algılayıcısı iki tür hata yapabilir. İlk olarak, hiç filigranı olmamasına rağmen bir filigranı varmış gibi algılama yapabilir. Buna yanlış pozitif denir. İkinci olarak, filigranı olduğu halde algılayıcı filigranın varlığını reddedebilir. Buna da yanlış negatif denir. Algılama sürecinin olasılık fonksiyonu Figür 3.14'da sunulmaktadır. (Kalker ve ark., 1998) de bu iki hata türünün olasılıkları, birinci dereceden otoregresif bir görüntü modeline dayanılarak türetilmiştir.

$$\begin{aligned} P_{fp} &= 1/2 \operatorname{erfc} \left(\frac{(T\sqrt{N})}{(\sigma_w \sigma_I \sqrt{2})} \right) \text{ ve } P_{fn} = 1/2 \operatorname{erfc} \left(\frac{(\sigma_w^2 - T\sqrt{N})}{(\sigma_w \sigma_I \sqrt{2})} \right) \\ \operatorname{erfc}(x) &= 1/(\sqrt{2\pi}) \int_a^b e^{(-t^2/2)} dt \end{aligned} \quad (3.4)$$

Burada, P_{fp} yanlış pozitif olasılığını, P_{fn} yanlış negatif olasılığını, σ^2 filigranı piksellerinin varyansını ve σ_I^2 ise görüntü piksellerinin varyansını temsil eder. Eğer filigranı deseni $W(x,y)$ sadece $\{-1,1\}$ tamsayılarından oluşuyorsa ve -1 sayısı 1 sayısına eşitse, filigranın varyansı σ_w^2 , k^2 'ye eşittir. Hatalar P_{fp} ve P_{fn} , kazanç faktörü k

artırılarak en aza indirgenebilir. Ön filtreleme ile filigran tespiti ve ön filtreleme olmadan filigran Şekil tespiti Şekil 3.11’de gösterilmiştir.



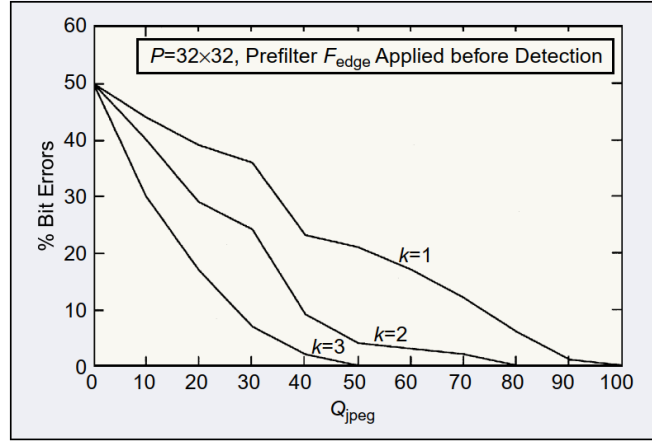
Şekil 3.11. Ön filtreleme ile filigran tespiti ve ön filtreleme olmadan filigran tespiti. (Langelaar ve ark., 2000)

Bağlantı faktörü için daha büyük değerler kullanmak, ancak filigranının görsel kalitesini azaltır. Görsel içerik, özellikle düşük frekans bileşenlerinde filigraniyle karışabilir, bu nedenle detektörün güvenilirliği, korelasyondan önce eşleşen filtreleme uygulanarak artırılabilir (Schyndel ve ark., 1994; Depovere ve ark., 1998; Hanjalic ve ark., 2000). Bu, orijinal görüntünün korelasyona olan katkısını azaltır. Örneğin, basit bir kenar vurgulama sonlu impuls tepki (FIR) filtresi F kullanılabilir, burada F_{edge} aşağıdaki konvolüsyon çekirdeği ile verilir:

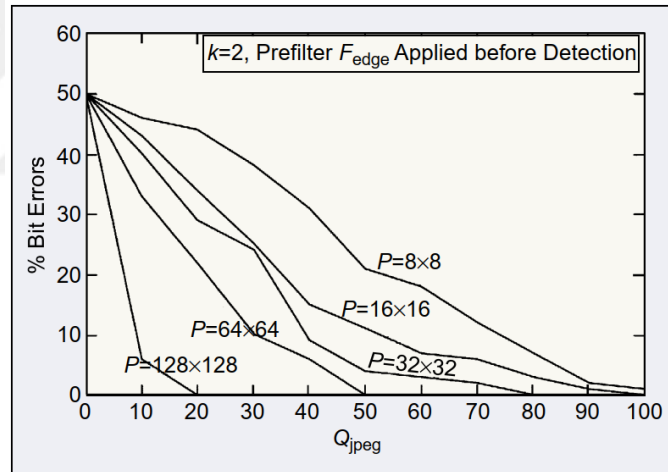
$$F_{edge} = \begin{bmatrix} -1 & -1 & -1 \\ -1 & -10 & -1/2 \\ -1 & -1 & -1 \end{bmatrix} \quad (3.5)$$

Sonraki bölümde sunulan deneysel sonuçlar, bu filtrelemeyi korelasyondan önce uygulamanın hata olasılığını önemli ölçüde azalttığını göstermektedir. Hatta filigranının görsel kalitesi korelasyondan önce ciddi şekilde etkilense bile bu ölçü görünmektedir (Langelaar ve ark., 1997; Hanjalic ve ark., 2000). (Liang ve Rodriguez, 2000) çalışmasında, filigranının dayanıklılığını artırmak için spektrum eşitleme yapma yöntemini önermiştir. Kazanç faktörü K 'nın bir filigranının dayanıklılığı üzerindeki etkisi

ve Bir filigranın dayanıklılığı üzerinde piksel başına filigran bit sayısı etkisi Şekil 3.12, Şekil 3.13'te gösterilmiştir.



Şekil 3.12. Kazanç faktörü K'nın bir filigranın dayanıklılığı üzerindeki etkisi.(Langelaar ve ark., 2000)



Şekil 3.13. Bir filigranın dayanıklılığı üzerinde piksel başına filigran bit sayısının etkisi. (Langelaar ve ark., 2000)

3.3.4. Bir görüntüye birden fazla bit veya logo gömme uzantıları

Filigranı algılayıcısının bakış açısından bir görüntü I , filigran bilgisini bozan Gauss gürültüsü olarak değerlendirilebilir. Dahası, filigranlı görüntü I_w , filigranı bilgisinin iletimi sırasında Gauss gürültüsüne tabi olan bir iletişim kanalının çıktısı olarak görülebilir. Bu durumda, filigranın güvenilir iletimi teorik olarak mümkündür, ancak bilgi hızı iletim kanalının kapasitesini aşmaması gerekmektedir. Kanal kapasitesi aşağıdaki şekilde verilmiştir (Shannon ve Weaver, 1949):

$$C = W_b \log_2 \left(1 + \frac{(\sigma^{2w})}{\sigma_I^2} \right) \text{ bit/pixel} \quad (3.6)$$

Burada, C , filigran bilgisi bitleri başına görüntü pikseli biriminde verilmiş ve mevcut bant genişliği W_b , piksel başına bir çevirmeyle eşitlenmiştir. Ancak pratik sistemler için, daha sıkı bir deneysel alt sınır belirlenebilmektedir (Smith ve Comiskey, 1996).

$$C = W_b \log_2 \left(1 + \frac{(\sigma^{2w})}{(\alpha \cdot \sigma_I^2)} \right) \text{ bit/pixel} \quad (3.7)$$

Burada, α küçük bir marj faktörüdür, bir birimden daha büyük ve genellikle yaklaşık üçtür. Sinyal-gürültü oranı $\frac{(\sigma^{2w})}{\sigma_I^2}$ bir birimden önemli ölçüde daha küçük olduğundan, (3.7) yaklaşık olarak aşağıdaki gibi ifade edilebilir:

$$C \approx 1/\ln 2 \left(\frac{(\sigma^{2w})}{(\alpha \cdot \sigma_I^2)} \right) \text{ bit/pixel} \quad (3.8)$$

Bu denklem doğrultusunda, önceki bölümde açıklanan temel teknik kullanılarak bir resimde sadece 1 bit bilgi depolamak mümkün olmalıdır. 7 bit $b_0b_1 \dots b_7$ için bir CDMA filigran oluşturma örneği ve Filigranın çıkarılması örneği Şekil 3.14, Şekil 3.15'de gösterilmiştir

RP_0	: -1	1	1	-1	-1	1	-1	-1	1	1	-1	b_0	: 0	→	$+RP_0$	: -1	1	1	-1	-1	1	-1	-1	1	1	-1	
RP_1	: 1	1	-1	-1	1	-1	-1	1	1	-1	1	b_1	: 0	→	$+RP_1$	: 1	1	-1	-1	1	-1	-1	1	1	-1	1	
RP_2	: 1	-1	-1	1	-1	-1	1	1	-1	1	-1	b_2	: 1	→	$-RP_2$	: -1	1	1	-1	1	1	-1	-1	1	-1	1	
RP_3	: -1	-1	1	-1	-1	1	1	-1	1	-1	-1	b_3	: 1	→	$-RP_3$	: 1	1	-1	1	1	-1	-1	1	-1	1	1	
RP_4	: -1	1	-1	-1	1	1	-1	1	-1	-1	1	b_4	: 0	→	$+RP_4$	: -1	1	-1	-1	1	1	-1	1	-1	-1	1	
RP_5	: 1	-1	-1	1	1	-1	1	-1	-1	1	1	b_5	: 1	→	$-RP_5$	: -1	1	1	-1	-1	1	-1	1	1	-1	-1	
RP_6	: -1	-1	1	1	-1	1	-1	-1	1	1	1	b_6	: 0	→	$+RP_6$	: <u>-1</u>	<u>-1</u>	<u>1</u>	<u>1</u>	<u>-1</u>	<u>1</u>	<u>-1</u>	<u>-1</u>	<u>1</u>	<u>1</u>	<u>1</u>	+
															W	: -3	5	1	-3	1	3	-7	1	3	-1	3	

Şekil 3.14. 7 bit $b_0b_1 \dots b_7$ için bir CDMA filigran oluşturma örneği. (Langelaar ve ark., 2000)

W	:	-3	5	1	-3	1	3	-7	1	3	-1	3	
I	:	98	98	97	98	97	96	97	96	95	94	94	+
I_W	:	95	103	98	95	98	99	90	97	98	93	97	

$$E[(RP_0 - E[RP_0]) \cdot (I_W - E[I_W])] = +15.6 \rightarrow b_0 = 0$$

$$E[(RP_1 - E[RP_1]) \cdot (I_W - E[I_W])] = +16.4 \rightarrow b_1 = 0$$

$$E[(RP_2 - E[RP_2]) \cdot (I_W - E[I_W])] = -26.4 \rightarrow b_2 = 1$$

$$E[(RP_3 - E[RP_3]) \cdot (I_W - E[I_W])] = -3.1 \rightarrow b_3 = 1$$

$$E[(RP_4 - E[RP_4]) \cdot (I_W - E[I_W])] = +21.6 \rightarrow b_4 = 0$$

$$E[(RP_5 - E[RP_5]) \cdot (I_W - E[I_W])] = -23.6 \rightarrow b_5 = 1$$

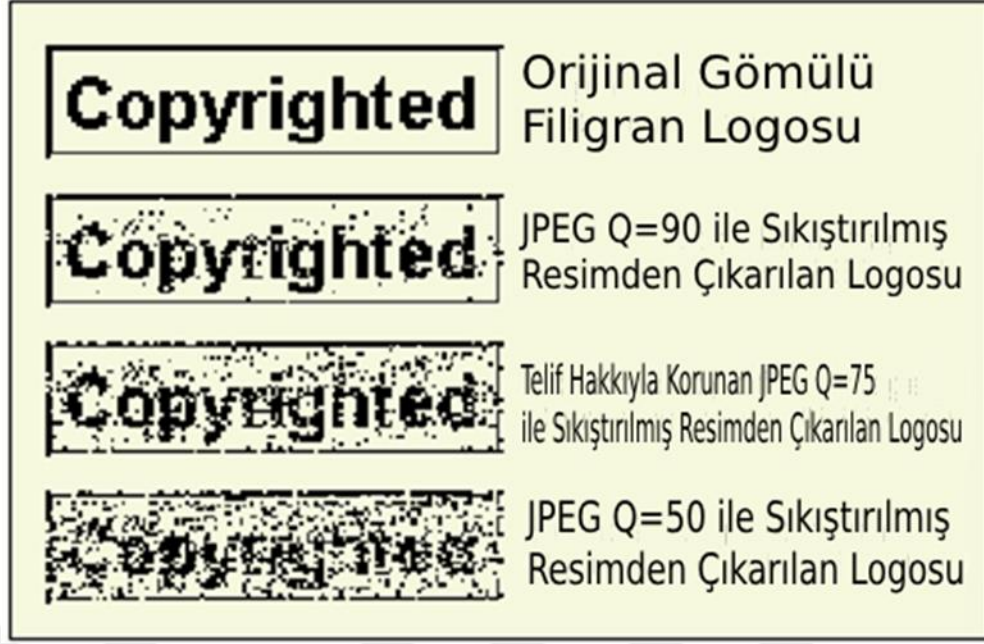
$$E[(RP_6 - E[RP_6]) \cdot (I_W - E[I_W])] = +0.4 \rightarrow b_6 = 0$$

Şekil 3.15. Filigranın çıkarılması örneği. (Langelaar ve ark., 2000)

Temel filigranlama tekniğinin taşıma kapasitesini artırmak için birkaç yöntem bulunmaktadır. Bir resme bir dizi filigranı biti $b_0 b_1 \dots b_{l-1}$ gömmenin en basit yolu, resmi I alt resimlere $I_0 I_1 \dots I_{l-1}$ bölmek ve her alt resme bir filigran eklemektir, burada her filigran dizeye bir biti temsil eder (Smith ve Comiskey, 1996; Langelaar ve ark., 1997; Hanjalic ve ark., 2000). (3.8) kullanılarak, bir alt resimde bir biti algılamak için gereken piksel sayısı güvenilir bir şekilde hesaplanabilir.

$$P \approx \frac{(\alpha \sigma_I^2 \ln 2)}{\sigma_W^2}. \quad (3.9)$$

Filigran bitleri birkaç farklı şekilde temsil edilmektedir. Filigran biti bir'e eşitse, bir sahte rastgele desen eklenir ve alt görüntü etkilenmez. Bu durumda, algılayıcı alt görüntü ile sahte rastgele desen arasındaki korelasyonu hesaplar ve korelasyon belirli bir eşik değerini aşarsa filigran bitine 1 değerini atar; aksi takdirde filigran bitinin sıfır olduğu varsayılır. Bir JPEG (Ortak Fotoğraf Uzmanları Grubu) bozulmuş görüntüden çıkarılan filigran logoları Şekil 3.16'de gösterilmiştir.



Şekil 3.16. Bir JPEG bozulmuş görüntüden çıkarılan filigran logoları. (Langelaar ve ark., 2000)

Bir eşik kullanımı, watermark biti 0 için RP_0 ve 1 için RP_1 olarak iki farklı sahte rastgele desen ekleyerek engellenebilir. Algılayıcı şimdi alt görüntü ile bu iki desen arasındaki korelasyonu hesaplar. En yüksek korelasyonu sağlayan desene karşılık gelen bit değeri filigran bitine atanır. (Smith ve Comiskey, 1996) çalışmasında, bu iki desen $RP_0 = -RP_1$ işaretinde farklılık gösteren şekilde seçilir. Bu durumda, algılayıcının alt görüntü ile sadece bir desen arasındaki korelasyonu hesaplaması yeterlidir; korelasyonun işareti filigran bit değerini belirler.

Filigran detektöründe ön filtrelemenin, kazanç faktörü k 'nin ve filigranın P biti başına piksel sayısının filigranın sağlamlığı üzerindeki etkisini incelemek için aşağıdaki deneyler yapılmıştır (Langelaar ve ark., 2000). İlk olarak (Smith ve Comiskey, 1996) yöntemi kullanılarak bir görüntüye filigran eklenir. Daha sonra filigranlı görüntü JPEG algoritması (Pennebaker ve Mitchell, 1993) ile sıkıştırılır, burada sıkıştırma algoritması Q_{jpeg} 'in kalite faktörü değişken yapılır. Son olarak, filigran sıkıştırılmış görüntüden çıkarılır ve orijinal olarak yerleştirilmiş filigran bitleriyle karşılaştırılır. Bu deneyden, JPEG kalite faktörüne bağlı olarak JPEG sıkıştırmasından kaynaklanan filigran bit hatalarının yüzdesi bulunmuştur (Langelaar ve ark., 2000).

İlk deney, $k=2$ kazanç faktörüyle $P=32 \times 32$ piksel filigran bit başına yerleştirilen bir filigranın algılanmasından önce (3.5) ile verilen ön filtrelemenin etkisini göstermektedir. Şekil 3.11'de, bu ön filtrelemeyi kullanan bir algılayıcı ve düz bir algılayıcı için JPEG sıkıştırması nedeniyle oluşan filigran bit hatalarının yüzdesi

çizilmiştir. Açıkça görülebilir ki, ön filtreleme filigranın sağlamlığını önemli ölçüde artırır.

İkinci deney, $P=32 \times 32$ piksel filigran bit başına yerleştirilen bir filigranın algılanmasında kullanılan bir ön filtreleme ile k kazanç faktörünün artırılmasının etkisini göstermektedir. Şekil 3.12'den, kazanç faktörünün artmasıyla filigranın sağlamlığının önemli ölçüde iyileştirilebileceği sonucu çıkmaktadır.

Üçüncü deney, $k=2$ kazanç faktörüyle bir ön filtreleme kullanılarak algılanan bir filigranın filigran bit başına düşen piksel sayısı P 'nin sağlamlığı üzerindeki etkisini göstermektedir. Şekil 3.13'dan, P 'nin artmasıyla filigranın taşıma kapasitesinin azalması, sağlamlığın önemli ölçüde arttığını gösterir.

Temel filigranlama tekniğinin taşıma kapasitesini artırmak için bir diğer yöntem, Doğrudan Sıralı Kod Bölmeli Çoklu Erişim (DS-CDMA) yayılı spektrumlu iletişimi kullanmaktır (Ruanaidh ve Pereira, 1998; Ruanaidh ve Pun, 1998). Burada, her bir filigran biti $b_0 b_1 \dots b_{(l-1)}$ dizisinden b_j için aynı boyutta stokastik olarak bağımsız bir sahte rastgele desen RP_i oluşturulur. Bu desen, bit değeri b_j 'ye bağlıdır. Burada, b_j değeri 0'ı temsil ediyorsa $+RP_i$ deseni kullanılır ve b_j değeri 1'i temsil ediyorsa RP_i deseni kullanılır. Tüm l rastgele desenlerin $\pm RP_i$ toplamı filigranı oluşturur. Bir görüntüye filigran eklemekten önce, kazanç faktörü olan veya onu belirli bir küçük aralıkla sınırlayan filigran ölçeklendirilebilir. Bir boyutlu filigran oluşturma örneği Figür 3.14'da sunulmuştur. Bu örnek, yedi farklı sahte rastgele deseni kullanarak yedi filigran biti 0011010 gömmektedir. Filigran bit dizisi $b_0 b_1 \dots b_{(l-1)}$ 'nin her bir biti b_j için, normalleştirilmiş görüntü I'_w ile ilgili sahte rastgele desen RP_i arasındaki korelasyon hesaplanarak çıkarılabilir. Eğer korelasyon pozitif ise, filigran bitine değer 0 atanır, aksi takdirde filigran biti 1 olarak kabul edilir.

Yukarıda açıklanan filigran yükünü genişletme yöntemleri, yani her bir filigran biti için ayrı görüntü bölmeleri kullanma ve CDMA kullanma yöntemleri avantajları ve dezavantajları vardır. Her bir filigran biti kendi görüntü bölmesine sahipse, bitler arasında karışma olmaz ve korelasyonları hesaplamak için sadece birkaç çarpma işlemi gereklidir. Ancak, görüntü kırıldığında, kenarda bulunan filigran bitleri kaybolur. CDMA teknikleri kullanıldığında ise, görüntü kırıldıktan sonra tüm bitlerin kurtarılma olasılığı yüksektir. Ancak, filigran bitleri birbirleriyle karışabilir ve korelasyonları hesaplamak için birçok çarpma işlemi gereklidir, çünkü her bir bit görüntünün tamamına yayılmıştır.

Yukarıda bahsedilen yöntemlerle gömülen filigran bitleri herhangi bir şeyi temsil edebilir: telif hakkı mesajları, seri numaralar, düz metin, kontrol sinyalleri vb. Bu bitlerle temsil edilen içerik sıkıştırılabilir, şifrelenebilir ve hata düzeltme kodlarıyla korunabilir. Bazı durumlarda, bir filigran olarak bir bit dizisi yerine küçük bir logo gömmek daha kullanışlı olabilir. Eğer filigranlı görüntü bozulursa, filigran logosu da etkilenecektir. Ancak bu durumda, insan görsel sisteminin sofistike desen tanıma yetenekleri logonun tespit edilmesi için kullanılabilir. Örneğin, bu bölümde açıklanan teknikler kullanılarak, 512 x 512 pikseli bir görüntüye 128 x 32 piksellik ikili bir filigran logosu gömülebilir. Her bir logo pikseli, siyah veya beyaz bir logo pikseli için görüntü bölmesine sahte rastgele desen +RP veya -RP eklenerek 8 x 8 piksellik bir görüntü bölmesine yerleştirilir. Figür 3.15'de bir örnek olarak, kayıplı JPEG (Pennebaker ve Mitchell, 1993) sıkıştırma algoritması kullanılarak filigranlı görüntü bozulduktan sonra çıkarılan logoların sonuçları gösterilmektedir. Figür 3.16'den, ağır şekilde bozulmuş olsa bile, logonun hala tanınabilir olduğu görülebilir.

3.3.5. Dönüşüm alanları için teknikler

Önceki bölümde açıklanan teknikler, dönüşüm alanı verilerine de uygulanabilir. Her dönüşüm alanının kendi avantajları ve dezavantajları vardır. (Ruanaidh ve ark., 1996) çalışmasında, ayrık Fourier dönüşümünün (DFT) fazı bir filigran gömmek için kullanılır, çünkü görüntünün anlaşılabilirliği için DFT değerlerinin fazı, genlikten daha önemlidir. Görüntünün en önemli bileşenlerine filigran yerleştirmek, filigranın sağlamlığını artırır, çünkü filigranı kaldırmak için bu önemli görüntü bileşenlerini değiştirmek, görüntünün kalitesini ciddi şekilde bozmaktadır. DFT değerlerinin fazını kullanma ikinci neden, iletişim teorisinden iyi bilinen bir gerçektir ki faz modülasyonu, genlik modülasyonuna kıyasla daha üstün gürültü dayanıklılığına sahiptir (Ruanaidh ve ark., 1996).

Birçok filigranlama tekniği, DFT genlik modülasyonunu kullanır, çünkü bu modülasyonun çevirme veya kaydırma invaryan özelliği bulunmaktadır (Ruanaidh ve ark., 1996; Ruanaidh ve Pun, 1997; Herrigel, Petersen ve ark., 1998; Herrigel, Ruanaidh ve ark., 1998; Ruanaidh ve Pereira, 1998; Ruanaidh ve Pun, 1998; S. Pereira ve ark., 1999). Uzaysal alanda görüntünün döngüsel kaydırılması DFT genliğini etkilemediği için, bu etki alanına gömülü filigran, çeviri değişmez olacaktır. Bir CDMA filigran kullanılıyorsa biraz kesilme direncine sahiptir. Ayrıca, filigran doğrudan en önemli orta bant frekanslarına yerleştirilebilir, çünkü en düşük frekans katsayılarının modülasyonu

görünür hatalara yol açarken, en yüksek frekans katsayıları gürültüye, filtreleme ve kayıplı sıkıştırmaya karşı çok hassastır. Son olarak, filigran DFT genlik katsayılarını $|I(u,v)|$ aşağıdaki şekilde modüle ederek görüntü içeriğine bağımlı hale getirebilir (Cox ve ark., 1995):

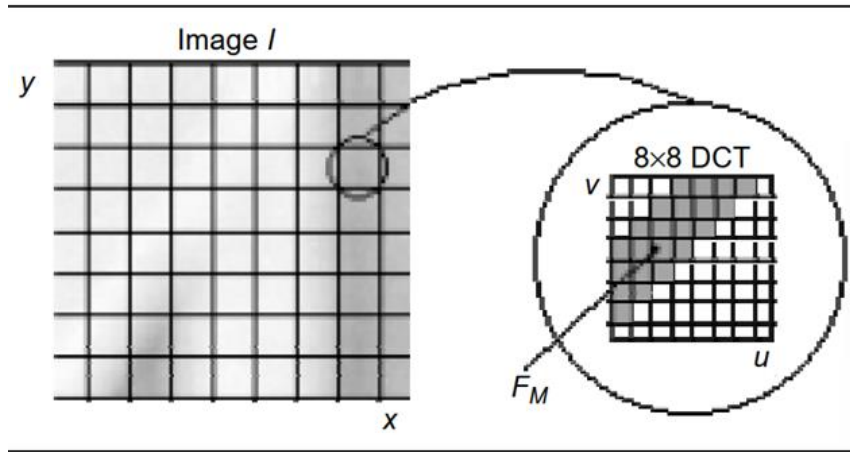
$$|I_w(u,v)| = |I(u,v)| \cdot (1 + k \cdot W(u,v)). \quad (3.10)$$

Burada, $W(u,v)$ bir CDMA filigranını, iki boyutlu (2-B) bir sahte rastgele deseni temsil eder ve α , kazanç faktörünü ifade eder. Bir DFT katsayısının değişimi sabit değil, DFT katsayısının genliğine orantılıdır. Küçük DFT katsayıları neredeyse etkilenmezken, daha büyük DFT katsayıları daha şiddetli bir şekilde etkilenir. Bu Weber'in kanununa (Jain, 1981) uygunluk gösterir. İnsan görsel sistemi, görüntülerde değişiklikleri eşit şekilde algılamaz, ancak görsel hassasiyet bir görüntüdeki görelî değişikliklere karşı neredeyse sabittir. Eğer ΔI algılanabilir bir fark ise, o zaman $\Delta I / I = \text{sabit}$ olur. (3.10) yeniden yazılarak aşağıdaki şekilde ifade edilir:

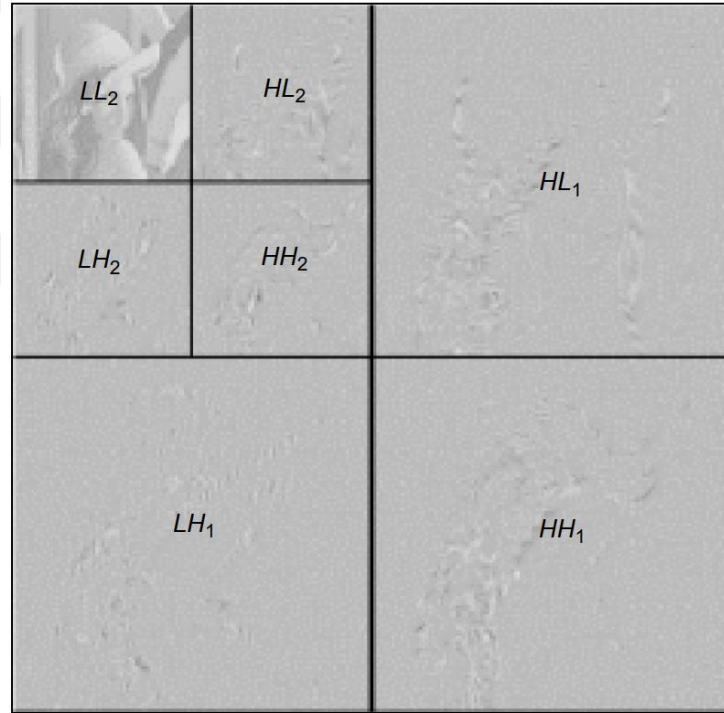
$$\frac{|I_w(u,v)| - |I(u,v)|}{|I(u,v)|} = \Delta I \frac{(u,v)}{|I(u,v)|} = k \cdot W(u,v) \cong \text{sabit} \quad (3.11)$$

Burada filigran çoğunlukla daha büyük DFT katsayılarına, yani görsel olarak en önemli bileşenlere eklenir. Bu şekilde filigranın dayanıklılığı artar.

Dikkat edilmesi gereken nokta, Fourier katsayılarının simetrisinin korunmasıdır. Böylece, ters dönüşümle mekansal alana geri dönüldüğünde görüntü verileri hala gerçel değerlidir. $N \times M$ pikseli bir görüntüdeki $|I(u,v)|$ katsayısı (3.10) formülüne göre değiştirilirse, ona karşılık gelen değeri hesaplanır. Bir DCT bloğunda orta bant frekanslarının tanımı ve bir görüntünün iki seviyeli DWT ayrıştırması Şekil 3.17, Şekil 3.18'de gösterilmiştir.



Şekil 3.17. Bir DCT bloğunda orta bant frekanslarının tanımı. (Langelaar ve ark., 2000)



Şekil 3.18. Bir görüntünün iki seviyeli DWT ayrıştırması. (Langelaar ve ark., 2000)

$|I(N - u, M - v)|$ Aynı şekilde değiştirilmelidir.

Filigran gömme için yaygın olarak kullanılan bir başka alan ise ayrık kosinüs dönüşümü (DCT) alanıdır (Boland ve ark., 1995; Cox ve ark., 1995; Cox ve ark., 1996; Hsu ve Wu, 1996; Ruanaidh ve ark., 1996; Piva ve ark., 1997; Podilchuk ve Zeng, 1997; Tao ve Dickinson, 1997; Wolfgang ve ark., 1999). DCT kullanılarak bir görüntü

kolaylıkla sahte frekans bantlarına ayrılabilir, böylece filigran en önemli orta bant frekanslarına kolaylıkla gömülebilir. Ayrıca, HVS'nin DCT baz görüntülere olan hassasiyeti kapsamlı bir şekilde incelenmiş ve önerilen JPEG nicelleme tablosuna yol açmıştır (Pennebaker ve Mitchell, 1993). Bu sonuçlar, filigranın neden olduğu bozulmanın görsel etkisini tahmin etmek ve minimize etmek için kullanılabilir. Son olarak, blok tabanlı DCT, görüntü ve video sıkıştırma için yaygın olarak kullanılmaktadır. Bir görüntüyü işlemek için kullanılan sıkıştırma düzeniyle aynı alana (bu durumda DCT alanına) bir filigran gömerek, kayıplı sıkıştırma tahmin edilebilir, çünkü sıkıştırma şeması tarafından hangi DCT katsayılarının atılacağı tahmin edilebilir. Gerçek zamanlı filigran uygulamaları için DCT ayrışımının avantajı da alınabilir.

8 x 8 DCT katsayıları $F(u,v)$ aşağıdaki gibi modüle edilir:

$$I_{(w_{(x,y)})} = \begin{matrix} I_{(x,y)}(u,v) \cdot (k \cdot W_{(x,y)}(u,v)), u,v \in F_M \\ I_{(x,y)}(u,v), u,v \notin F_M \end{matrix} \quad x,y=1,8,16 \quad (3.12)$$

Burada, F_M , orta bant frekanslarını temsil eder, k kazanç faktörünü, (x, y) görüntü I 'deki bir 8 x 8 piksel bloğunun mekansal konumunu ve (u, v) ise karşılık gelen 8 x 8 DCT bloğundaki DCT katsayısını temsil eder.

Filigran, modülasyon fonksiyonunu aşağıdaki gibi değiştirerek görüntüye bağımlı hale getirilebilir.

$$I_{(w_{(x,y)})} = \begin{matrix} I_{(x,y)}(u,v) \cdot (1+k \cdot W_{(x,y)}(u,v)), u,v \in F_M \\ I_{(x,y)}(u,v), u,v \notin F_M \end{matrix} \quad x,y=1,8,16 \quad (3.13)$$

DCT alanı temelli filigranlama sistemlerinin performansında daha fazla iyileştirme, yaygın olarak kullanılan saf Gauss varsayımı yerine genelleştirilmiş Gauss modeline dayanan filigran tespitçilerinin kullanılmasıyla elde edilebilir (Hernández ve ark., 2000). (Hernández ve ark., 2000) çalışmasında, görüntüler için DCT alanı filigranlama yöntemlerine yönelik teorik bir analiz gerçekleştirilerek, belirli bir görüntü için beklenen performansın önceden ölçülebileceği ve görüntü özellikleri ile sistem parametrelerinin (örneğin, filigran uzunluğu) son performans üzerindeki etkisinin analiz edilebileceği analitik ifadeler sunulmuştur. Ayrıca, bu analizin sonucu, belirli bir yanlış pozitif oran elde etmek için uygun tespit eşiği T 'nin belirlenmesine yardımcı olabilir.

(Hernández ve ark., 2000) çalışmasında, saf Gauss gürültü varsayımından vazgeçilerek önemli performans iyileştirmelerinin elde edilebileceği iddia edilmektedir.

Eğer filigranlama teknikleri HVS'nin özelliklerinden faydalanabiliyorsa, daha fazla enerjiye sahip filigranlar görüntüde daha iyi gizlenebilir, bu da filigranların daha sağlam hale gelmesini sağlar. Bu açıdan bakıldığında, ayrık dalgacık dönüşümü (DWT), HVS için frekans modellerinin hesaplama açısından verimli bir versiyonu olarak çok çekici bir dönüşümdür (Barni ve ark., 1999). Örneğin, insan gözünün yüksek çözünürlüklü DWT bantlarında ve 45°'lik bir yönelime sahip DWT bantlarında gürültüye daha az duyarlı olduğu ortaya çıkmıştır. Ayrıca, gömülü sıfır-ağaç dalgaletti (EZW) kodlaması gibi DWT tabanlı görüntü ve video kodlaması, JPEG2000 (Xia ve ark., 1997) gibi gelecek görüntü ve video sıkıştırma standartlarına dahil edilecektir. Aynı alana (DWT alanı) bir filigran gömmek, sıkıştırma yönteminden hangi DWT bantlarının etkileneceği tahmin edilebildiğinden, kayıplı EZW sıkıştırmalarını tahmin etmemizi sağlar. Ayrıca, gerçek zamanlı filigran uygulamaları için DWT bölme kullanılabilir (Langelaar ve ark., 2000). Birçok yaklaşım, bu bölümde tanımlanan temel teknikleri yüksek çözünürlüklü DWT bantları LH_1 (DWT'nin düşük- yüksek bandı), HH_1 (DWT'nin yüksek-yüksek bandı) ve HL_1 (DWT'nin yüksek-düşük bandı) (Şekil 3.18) üzerinde uygular (Boland ve ark., 1995; Ruanaidh ve ark., 1996; Kundur ve Hatzinakos, 1997; Xia ve ark., 1997; Barni ve ark., 1999).

Her üç DWT bandındaki DWT katsayıları aşağıdaki gibi modüle edilir:

$$I_w(u,v)=I(u,v)+k.W(u,v). \quad (3.14)$$

DWT filigranı, her üç DWT bandındaki DWT katsayılarını aşağıdaki gibi modüle ederek görüntüye bağımlı hale getirilebilir:

$$I_w(u,v)=I(u,v).(1+k.W(u,v)) \quad (3.15)$$

HVS'ye Dayalı Filigran Enerji Uyarlaması Filigranın sağlamlığı, filigranın enerjisini artırarak iyileştirilebilir. Ancak enerjiyi artırmak görüntü kalitesini düşürür. HVS'nin özelliklerinden faydalanarak enerji, insan gözünün fark etmeyeceği yerlerde yerel olarak artırılabilir. Sonuç olarak, HVS'yi kullanarak, eğer bu enerji görüntü üzerinde

eşit olarak dağıtılmış olsaydı, algısal olarak görünmez filigranlar gömmek mümkün olacaktı ve bu filigranların enerjisi daha yüksek olabilirdi.

Bir görsel sinyalin algılanması için, belirli bir kontrasta sahip olması gerekmektedir. Bu kontrast, ortalama parlaklık ve frekansa bağlıdır. Ayrıca, benzer bir frekansta rahatsız edici bir sinyali maskeleyebilen bir sinyal vardır (Wandell, 1995), (Bartolini ve ark., 1998). Bu maskeleme etkisi, önceki bölümde tanımlanan görüntüye bağımlı DCT filigranlama yönteminde zaten kullanılmaktadır, burada DCT katsayıları (3.13) kullanılarak modüle edilir. Burada, görüntüde bulunan her bir sinüsoidal (maskeleme sinyali), maskeleme sinyaline orantılı bir amplitüde sahip başka bir sinüsoidal (filigran) eklenir. Eğer kazanç faktörü 'k' doğru şekilde ayarlanmışsa, frekans maskesi gerçekleşir.

HVS, yüksek parlaklık bölgelerindeki değişikliklere daha az duyarlıdır. Bu durum, filigran kazanç faktörünün parlaklığa bağlı olarak değiştirilebileceği şekilde kullanılabilir (Kutter ve ark., 1997). Ayrıca, insan gözünün mavi kanala karşı daha az hassas olduğu düşünüldüğünde, bir renkli görüntünün parlaklık kanalına gömülmüş algısal olarak görünmez bir filigrandan daha fazla enerji içerebilir (Kutter ve ark., 1997).

Görüntünün kenarları etrafında ve dokulu alanlarda, HVS düz bölgelere göre bozulmalara daha az duyarlıdır. Bu etki, filigran enerjisini yerel olarak bu maskeleme bölgelerinde artırarak filigranlamada da kullanılabilir (Macq ve Quisquater, 1995). Bu bölümün ilk iki alt bölümünde tanımlanan temel mekansal filigranlama teknikleri, mekansal maskeleme telafisi ile genişletilebilir. Örneğin, aşağıdaki modülasyon fonksiyonunun kullanılmasıyla:

$$I_w(x, y) = I(x, y) + Msk(x, y) \cdot k \cdot W(x, y) \quad (3.16)$$

Burada $W(x, y)$ filigranın 2-B boyutsuz rastgele desenini temsil eder, 'fark' sabit bir kazanç faktörünü gösterir ve $Msk(x, y)$ bir maskeleme görüntüsünü temsil eder. Maskeleme görüntüsünün değerleri 0 ile k'_{max} arasında değişir ve orijinal görüntü $I(x, y)$ 'deki her bir karşılık gelen noktadaki bozulmalara karşı duyarsızlık ölçüsünü verir. (Kalker ve ark., 1999) Msk maskeleme görüntüsü, orijinal görüntüyü bir Laplacian yüksek geçiren filtre ile elde edilen filtrelenmiş görüntünün mutlak değerlerini alarak oluşturulur.

Şekil 3.19(a)'da basit bir Prewitt kenar belirleyici kullanılarak oluşturulan bir maske gösterilmektedir. Şekil 3.19(b), bu maske ile modüle edilmiş güçlenen filigranı

göstermektedir. (Ng ve Cheng, 1999) 'de 8 x 8 DCT AC-katsayılarının karesel toplamı, bir maskeleme görüntüsü oluşturmak için kullanılır. Şekil 3.20(a), bu DCT-AC (Ayrık Kosinüs Dönüşümü - Gelişmiş Video Kodlama) enerjisi kullanılarak oluşturulan bir maske göstermektedir. Şekil 3.20(b), bu maske ile modüle edilmiş güçlendirilmiş filigranı sunmaktadır.

Deneyler, HVS'ye uyumlu lokal olarak adapte edilmiş bir maskeye modüle edilmiş algısal olarak görünmez bir filigranın, sabit bir kazanç faktörü ile modüle edilmiş algısal olarak görünmez bir filigrandan iki kat daha fazla enerji içerebileceğini göstermiştir.

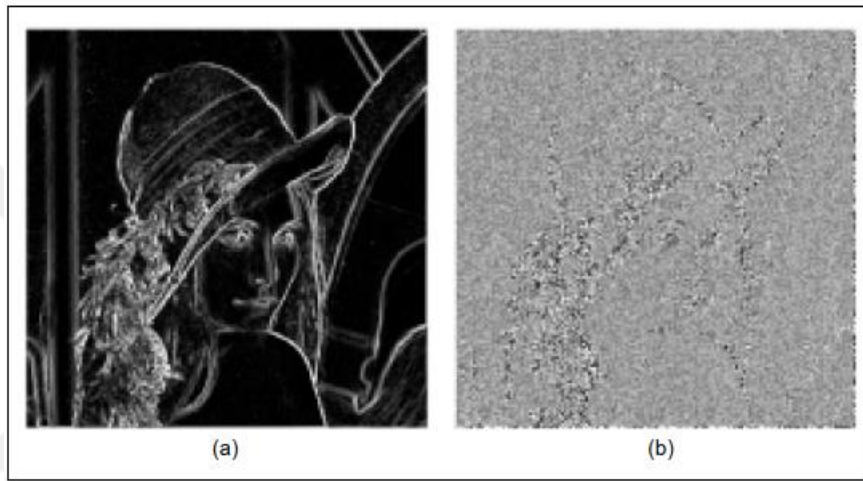
Bu enerji artışının filigranın sağlamlığı üzerindeki etkisini incelemek için aşağıdaki deney yapılmıştır. Görünür bir suistimal oluşturan bir sabit kazanç faktörü $k=2$ kullanarak (Smith ve Comiskey, 1996)'de tanımlanan "döşemeli" yayma spektrumu filigranlama yöntemiyle bir filigran $W_{\text{fixed}}(x,y)$ eklenmektedir. Bu sabit kazanç faktörünü artırmak, sonuçta elde edilen filigranlı görüntüde görünür eserlere neden olur. Ardından, başka bir görüntüsüne aynı yöntemi kullanarak ancak bu kez lokal olarak adapte edilmiş değişken bir kazanç faktörü kullanarak bir filigran $W_{\text{var}}(x,y)$ eklenmektedir. $W_{\text{var}}(x,y)$ filigranının $W_{\text{fixed}}(x,y)$ filigranına göre yaklaşık olarak iki kat daha fazla enerji içerdiği halde, elde edilen filigranlı görüntüde filigran fark edilemez.

Ardından, JPEG algoritmasına (Pennebaker ve Mitchell, 1993) sahip filigranlı her iki görüntü de sıkıştırılır, burada sıkıştırma algoritmasının kalite faktörü Q_{jpeg} değişkenine ayarlanır. Son olarak, filigranlar sıkıştırılmış görüntüden çıkarılır ve önceden yerleştirilmiş filigran bitleriyle bit bit karşılaştırılır. Bu deneyden, JPEG kalite faktörüne bağlı olarak JPEG sıkıştırmasından kaynaklanan filigran bit hatalarının yüzdesi bulunur. Esnek bir kazanç faktörü uygulayarak HVS'ye uyumlu bir şekilde ayarlanabilen bir kazanç faktörü ile biraz daha sağlam bir hale getirilebileceği görülebilir.

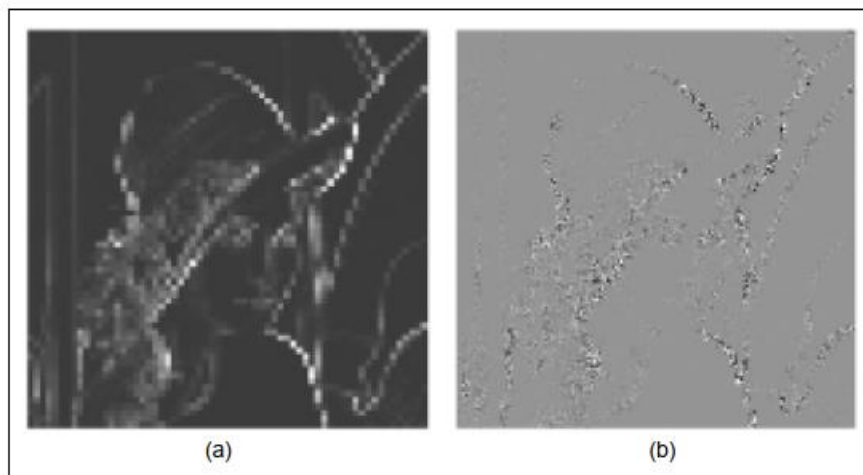
Mekansal maskeleme, filigranın başka bir alanda, örneğin DFT, DCT veya DWT'de gömülü olduğunda da uygulanabilir. Bu durumda, mekansal olmayan filigran önce bir görüntüye 1 gömülür ve geçici bir görüntü I_{wt} ile sonuçlanır. Filigranlı görüntü I_w şimdi orijinal görüntü I ile bu geçici görüntü I_{wt} 'yi yukarıda açıklandığı gibi bir maskeleme görüntüsü Msk aracılığıyla karıştırarak oluşturulur. (Piva ve ark., 1997; Bartolini ve ark., 1998) :

$$I_w(x,y) = (1 - Msk(x,y))I(x,y) + Msk(x,y) \cdot I_{wt}(x,y) \quad (3.17)$$

Burada, maskeleme görüntüsü sıfır ile bir arasındaki değerlere ölçeklendirilmelidir. HVS'ye dayalı daha sofistike modellere dayanan filigranlama yöntemleri (Swanson ve ark., 1996; Fleet ve Heeger, 1997; Goffin ve ark., 1997; Kundur ve Hatzinakos, 1997; Piva ve ark., 1997; Podilchuk ve Zeng, 1997; Bartolini ve ark., 1998; Barni ve ark., 1999; Wolfgang ve ark., 1999) makalelerinde bulunabilir. Prewitt operatörüne dayalı maskeleme görüntüsü kullanılarak filigranlama Şekil 3.19'de ve DCT-AC enerjisine dayalı maskeleme görüntüsü kullanılarak filigranlama Şekil 3.20'de belirtilmiştir.



Şekil 3.19. Prewitt operatörüne dayalı maskeleme görüntüsü kullanılarak filigranlama. (a) Maskeleme görüntüsü ve (b) fark $W(x, y) = I(x, y) - I_w(x, y)$. (Langelaar ve ark., 2000)



Şekil 3.20. DCT-AC enerjisine dayalı maskeleme görüntüsü kullanılarak filigranlama. (a) Maskeleme görüntüsü ve (b) fark $W(x, y) = I(x, y) - I_w(x, y)$. (Langelaar ve ark., 2000)

Kayıplı sıkıştırma ile güçlü bir şekilde sıkıştırılmış bir filigranın, daha önceki mekânsal filigran lama teknikleriyle bir görüntüye eklenen bir filigranı, güvenilir bir şekilde tespit edilemez. Bu durum, bu tür filigranlarının temelde düşük güçlü, yüksek frekanslı gürültüden oluşmasından kaynaklanır. JPEG, yüksek frekans bileşenlere daha az bit tahsis ettiğinden, bu tür filigranları kolayca bozulabilir. Ayrıca, bu filigranları doğrusal veya ortanca filtreler gibi düşük geçiren işlemlerden de ciddi şekilde etkilenebilir.

JPEG sıkıştırmasına karşı dayanıklılık çeşitli şekillerde iyileştirilebilir. (Smith ve Comiskey, 1996) makalesinde, sözde rasgele desen W , JPEG algoritması kullanılarak önce sıkıştırılır ve ardından sıkıştırılmış hali açılır. Ortaya çıkan model W 'nin enerjisi, sıkıştırma yoluyla kaybedilen enerjiyi telafi etmek için artırılır. Buradaki fikir, aksi halde sıkıştırma işlemi sırasında daha sonra kaybolacak olan tüm enerjiyi önceden filtrelemek için sıkıştırma algoritmasını kullanmaktır. Bu şekilde oluşturulan bir filigranın, küçük sayısal eserler dışında, aynı kalite faktörünü kullanan daha fazla JPEG sıkıştırmasında değişmez olduğu varsayılır. Filtreleme gibi filigran deseninin diğer ön bozulması, filigranlı görüntünün diğer beklenen bozulmasını önlemek için uygulanabilir.

(Nikolaidis ve Pitas, 1996) makalesinde, filigran modelinin enerjisi, tüm pikseller için aynı gain faktörü k yerine her piksel için ayrı bir gain faktörü $k_{x,y}$ hesaplanarak daha düşük frekanslara kaydırılır. İlk olarak, 0 ve k sayılarını içeren bir sözde rasgele model $W(x, y)$ oluşturulur. Sonra, model 8×8 bloklara bölünür ve her 8×8 blok için DCT dönüşümü $W(u, v)$ hesaplanır. 8×8 bloklarındaki sıfır olmayan elemanlar artık kazanç faktörleri $k_{x,y}$ olarak kabul edilir ve hassas yüksek frekanslı DCT bantlarındaki FH enerjisi Φ en aza indirilecek şekilde uyarlanır.

$$\Phi = \sum \sum_{u,v \in F_H} W(u, v)^2 F_H = \{u, v \mid 5 < u \leq 8, 5 < v \leq 8\} \quad (3.18)$$

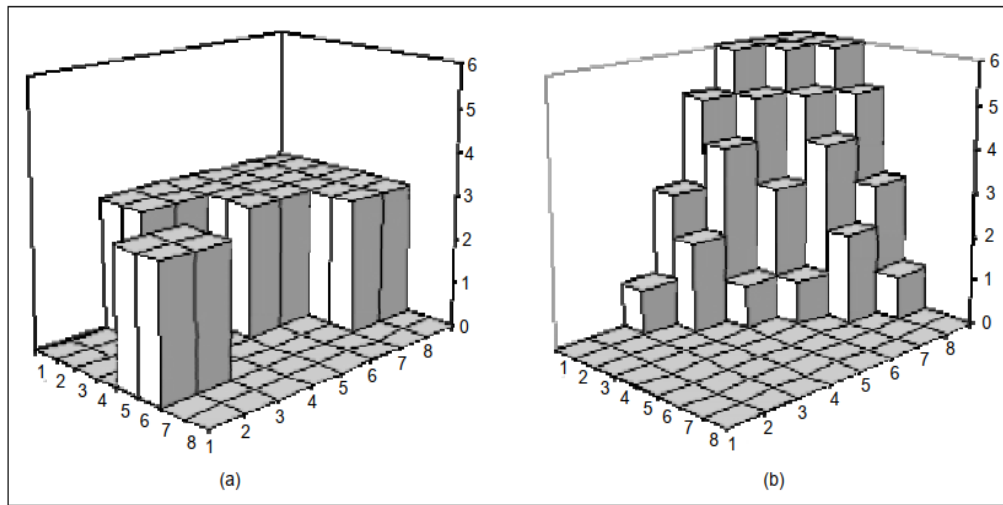
Enerji Φ aşağıdaki kısıtlamalar altında minimuma indirilir:

$$\sum_{x=1}^8 \sum_{y=1}^8 W(x, y) \cdot k = \sum_{x=1}^8 \sum_{y=1}^8 W(x, y) \cdot k_{x,y}, k_{min} \leq k_{x,y} \leq k_{max}. \quad (3.19)$$

Bu yüksek enerji minimumunun filigran modeli üzerindeki etkisi Şekil 3.21'de gösterilmiştir. Şekil 3.21(a) sabit bir $k=3$ gain faktörü kullanılan 8×8 bir blok içinde filigran modelini gösterir. $k_{min} = 0$ ve $k_{max} = 6$ ile yapılan Yüksek enerji

minimizasyonundan sonra, filigran modeli düzgün bir şekilde sıfıra yaklaşır [Şekil 3.21(b)], ancak sıfırdan farklı piksellerin toplamı hala orijinal modeldeki sıfırdan farklı piksellerin toplamına eşittir.

(Langelaar ve ark., 1997; Hanjalic ve ark., 2000) makalelerinde, her biri 32×32 piksel bloğu için farklı bir gain faktörü k türetilerek JPEG sıkıştırması bağışıklığı elde edilir. Bir filigran bitini temsil eden 32×32 bir sözde rasgele model, bir 32×32 görüntü bloğuna eklenir. Bu filigranlı görüntü bloğunun bir kopyası, nispeten düşük bir kalite faktörü kullanılarak JPEG standardına göre bozulur. Bu bozulmuş kopyadan filigran biti doğru bir şekilde çıkarılamazsa, filigran modeli daha yüksek bir gain faktörü ile görüntüye eklenir ve biti kontrol etmek için yeni bir bozulmuş kopya oluşturulur. Bu işlem her bir bit için tekrarlanır ve bozulmuş kopyalardan güvenilir bir şekilde tüm bitler çıkarılabilir. Bu şekilde oluşturulan bir filigran, kopyaların bozulduğu kalite faktörüne eşit veya daha büyük bir kalite faktörü kullanılarak yapılan JPEG sıkıştırmaya karşı dirençlidir. Şekil 3.21’de bu tür bir filigran örneği, görünürlük amaçlı büyütülmüş olarak gösterilmektedir.



Şekil 3.21. (a) Orijinal filigran bloğu ve (b) düşük frekanslı filigran bloğu. (Langelaar ve ark., 2000)

3.3.6. Geometrik dönüşümleri önceden tahmin etme

Bir filigran sadece kayıplı sıkıştırma tekniklerine karşı dayanıklı olmamalı, aynı zamanda kaydırma, ölçeklendirme, kırpma, döndürme gibi geometrik dönüşümlere karşı da dayanıklı olmalıdır. Geometrik dönüşümler genellikle görüntü kalitesini etkilemez,

ancak önceki bölümlerde açıklanan tekniklerle eklenen çoğu filigran tespit edicileri için algılanamaz hale gelir. Geometrik dönüşümler genellikle filigranın sözde rasgele modeli ile filigranlı görüntü arasındaki senkronizasyonu etkilediğinden, tespit edicinin hesaplamaları yapmadan önce senkronizasyonun yeniden elde edilmesi gerekmektedir.

Kaydırma dayanıklılığını elde etmenin en açık yolu, DFT genliği modülasyon tekniğini kullanmaktır. Herhangi bir nedenle başka bir filigranlama gömme alanı tercih ediliyorsa ve kaydırma dayanıklılığı gerekiyorsa, bir işaretçi ekleyerek çevresel alanda çevirme belirlenebilir. Bu işaretçi, filigranın kendisi gibi sözde rasgele bir model olabilir. Tespit edici, işaretçiyi görüntüdeki tüm olası konumlara kaydırarak ve işaretçi ile ilgili görüntü parçası arasındaki korelasyonu hesaplayarak işaretçinin mekansal konumunu belirler. Son olarak, görüntü orijinal konumuna geri kaydırılır ve normal filigranı tespit işlemi uygulanır.

Bir işaretçi için kapsamlı bir arama heslemsel olarak oldukça derindir. Bu nedenle (Kalker ve ark., 1999) makalesinde farklı bir yaklaşım önerilmiştir: sözde rasgele bir model, görüntüde farklı konumlara iki kez eklenir. filigranı içeriği, yani filigranı bitleri, burada iki filigranı modelinin göreceli konumlarında gömülür. filigranı tespit edici, hızlı Fourier dönüşümü (FFT) kullanarak görüntü ile filigranı modeli arasındaki faz korelasyonunu hesaplar ve iki modelin korelasyon zirvelerini tespit eder. filigranı içeriği, zirvelerin göreceli konumundan elde edilir. Eğer tüm görüntü tespit edilmeden önce kaydırılırsa, korelasyon zirvelerinin mutlak konumları değişecek ve göreceli konumlar değişmeden kalıp tespit edici için filigranı bitleri okunabilir olacaktır.

(Fleet ve Heeger, 1997) makalesinde, bir görüntüye ölçeklendirme, döndürme ve kaydırma yapılabilmesi için kullanılabilecek bir ızgara eklemek için bir yöntem önermektedir. İzgara, FFT frekans alanında zirveler olarak görünen sinüzoidal sinyallerin toplamıyla temsil edilir. Bu zirveler geometrik bozulmayı belirlemek için kullanılır. Her blok için yerel kazanç faktörünün daha düşük bir kaliteye sahip bir görüntüye dayandığı filigranı Şekil 3.22 ve Dönme, ölçekleme ve kaydırma bağımsız filigran yöntemi Şekil 3.23' de gösterilmiştir.

Sonrasında, tahmini filigranı W'n otokorelasyon fonksiyonu hesaplanır. Bu fonksiyon, merkezde ve birden çok gömülü filigranı konumunda zirve değerlerine sahip olacaktır. Eğer görüntü bir geometrik dönüşüm geçirmişse, otokorelasyon fonksiyonundaki zirveler aynı dönüşümü yansıtacak ve böylece görüntüyü orijinal boyut ve yönelimine dönüştürmek için kullanılabilecek bir ızgara sağlayacaktır.

(Ruanaidh ve Pun, 1997; Herrigel, Petersen ve ark., 1998; Herrigel, Ruanaidh ve ark., 1998; Ruanaidh ve Pereira, 1998; Ruanaidh ve Pun, 1998; Pereira ve ark., 1999) makalelerinde ise, DFT ve log polar map (LPM) birleşimi kullanarak dönme, ölçekleme ve kaydırmaya dayanıklı bir alan kullanılarak filigranının gömülmesini öneren bir yöntem geliştirmiştir. Şekil 3.22, bu filigranlama yönteminin bir şemasını sunmaktadır.

İlk olarak bir ölçeklenme, bağımsız alan elde etmek için DFT genliği hesaplanmaktadır. Sonrasında, DFT genliğinin her bir noktası (u,v) için LPM'deki karşılık gelen bir nokta (u,8) belirlenir:

$$U = \ell^\mu \cos((\theta)P = \ell^\mu \sin(\theta) \quad (3.21)$$

Bu LPM'nin koordinat sistemi, dönme ve ölçeklemeyi yatay ve dikey eksen boyunca kaydırmaya dönüştürür. Bu LPM'nin DFT genliğini alarak, dönme, ölçekleme ve kaydırmaya dayanıklı bir alan elde edilir. Bu alanda bir CDMA filigranı eklenir, örneğin katsayıları (3.10) kullanarak modüle edilir.

Uygulamada, HVS'ye uyarlanmış bir değişken kazanç faktörünün filigranla ilgili bir yöntemin sağlamlığı üzerindeki etkisinin uygulanmasının zor olduğu kanıtlanmıştır. Bu nedenle, yazarlar biraz farklı bir yaklaşım önermektedir. Bu yaklaşımda, ölçeklendirmeden bağımsız genlik DFT alanına CDMA'nın bir filigranı, ölçek ve dönüş bağımsızlığı sağlamak için şablon adı verilen ikinci bir filigranla birlikte gömülür. Filigranı kaldırmak için, önce aşağıdakini kullanarak filigranlı görüntünün ölçeğini ve yönünü belirlerler: filigranlı görüntünün DFT'si hesaplanır.

DFT genliklerinin ve şablon deseninin LPM'si hesaplanır.

İki LPM arasındaki yatay ve dikey ofsetler, tüm arama ve çapraz-korelasyon tekniklerini kullanarak hesaplanır ve ölçek ve dönme faktörü bulunur.

Sonraki adımda, görüntü orijinal boyut ve yönelimine geri dönüştürülür ve bilgi taşıyan filigranı çıkarılır.

3.3.7. Korelasyon tabanlı filigranlama

MPEG (Hareketli Görüntü Uzmanları Grubu) için Teknikler Gerçek zamanlı filigranlama uygulamalarında, dayanıklılık önemli bir faktör olmanın yanı sıra, hesaplama karmaşıklığı da önemli bir yer tutmaktadır. Genel olarak, görüntü veya video verileri JPEG veya MPEG sıkıştırılmış biçimde iletilir. Gerçek zamanlı filigranlama, bu sıkıştırılmış biçimi dikkate almalıdır, çünkü verilerin tamamen açılması, filigran eklenmesi ve tekrar sıkıştırılması hesaplama açısından çok zahmetlidir.

Bu nedenle, sıkıştırılmış bit akışı, kod sözcükleri veya DCT dönüşüm katsayıları üzerinde doğrudan çalışabilen filigranlama teknikleri geliştirmek arzu edilir, çünkü verilerin tamamen açılması ve tekrar sıkıştırılması gerekmez. Bu bölümde, MPEG video akışları için iki yöntem ele alınmıştır. Kod sözcükleri ve DCT katsayıları üzerinde çalışan diğer yöntemler ilerleyen bölümlerde ele alınmıştır.

(Wu ve Wu, 1997) makalesinde, bir MPEG sıkıştırılmış video akışının DC-DCT katsayılarına doğrudan DCT dönüşümlü bir sözde rasgele model eklenmektedir. filigranlama işlemi yalnızca I-karelerin parlaklık değerlerini dikkate alır. Bir filigranını gömmek için aşağıdaki prosedür uygulanır: İlk olarak, gizli bir anahtara dayanan $\{-1,1\}$ aralığında tamsayılardan oluşan bir sözde rasgele model üretilir. Bu model, I-karelerin boyutlarına sahiptir. Ardından, model, bir filigran bit dizisi ile modüle edilir ve bir kazanç faktörü ile çarpılır. Son olarak, 8×8 blok DCT dönüşümü, modüle edilmiş model üzerine uygulanır ve elde edilen DC katsayıları, her I-karenin ilgili DC değerlerine eklenir. Filigranın, önceki bölümlerde açıklandığı gibi DCT alanında veya mekansal alanda korelasyon teknikleri kullanılarak algılanabilir.

Yazarlar, algoritmanın video akışının görsel kalitesini önemli ölçüde azalttığını bildirmektedir. Bu nedenle, filigranın kazanç faktörü çok düşük (<1) seçilmeli ve her bir filigran biti için piksel sayısı son derece yüksek ($>> 100.000$) seçilmelidir. Bu durumun temel nedeni, filigran modelinin yalnızca 64 DCT katsayısından biri olan DC bileşeni içine gömülmesidir. Ayrıca, model yalnızca insan gözünün oldukça hassas olduğu düşük frekans bileşenlerinden oluşmaktadır. Karşılaştırma yapmak için, önceki bölümde açıklanan korelasyon tekniğini kullanarak çoklu bitleri gömmek için kullanılan algoritma, bir kazanç faktörü olarak iki ve her bir filigran biti için yaklaşık 1000 piksel kullanır.

(Hartung ve Girod, 1996; Hartung ve Girod, 1997; Hartung ve Girod, 1998) makalelerinde daha sofistike bir filigranlama algoritması önerilmiştir. Bu algoritma, DC-katsayıları yanı sıra her bir I-, P- ve B-karenin AC-katsayılarına da bir filigran

gömülmesini sağlar. filigranı burada, bir gizli anahtara dayanan $\{-1,1\}$ aralığında tamsayılardan oluşan bir sözde rasgele modeldir. Bu model, video karelerinin boyutlarına sahiptir. Model, bir filigranı bit dizisiyle modüle edilir ve bir kazanç faktörü k ile çarpılır.

Filigranını gömmek için, filigranı modeli $W(x, y)$ 8×8 bloğa bölünür. Bu bloklar DCT alanına dönüştürülür ve $W_{x,y}(u, v)$ olarak adlandırılır, burada $x, y=0,8,16,\dots$ ve $u,v=0,\dots,7$. Sonraki adımda, 2-B bloklar $W_{x,y}(u, v)$ zigzag tarama düzenine göre yeniden düzenlenir ve $W_{x,y}(i)$ dizilerine dönüşür, burada $i=0,\dots,63$. $W_{x,y}(0)$ DC-katsayısını temsil eder ve $W_{x,y}(63)$ 8×8 filigranı bloğunun en yüksek frekanslı AC-katsayısını belirtir. İlgili MPEG kodlu 8×8 video içerik blokları $I_{x,y}(i)$ ile aynı şekilde kodlandığından, bu diziler doğrudan filigranını eklemek için kullanılabilir. Her bir I-, P- veya B-karenin video bloğu $I_{x,y}(i)$ için aşağıdaki adımlar uygulanır:

1. DC-katsayısı aşağıdaki şekilde modüle edilir:

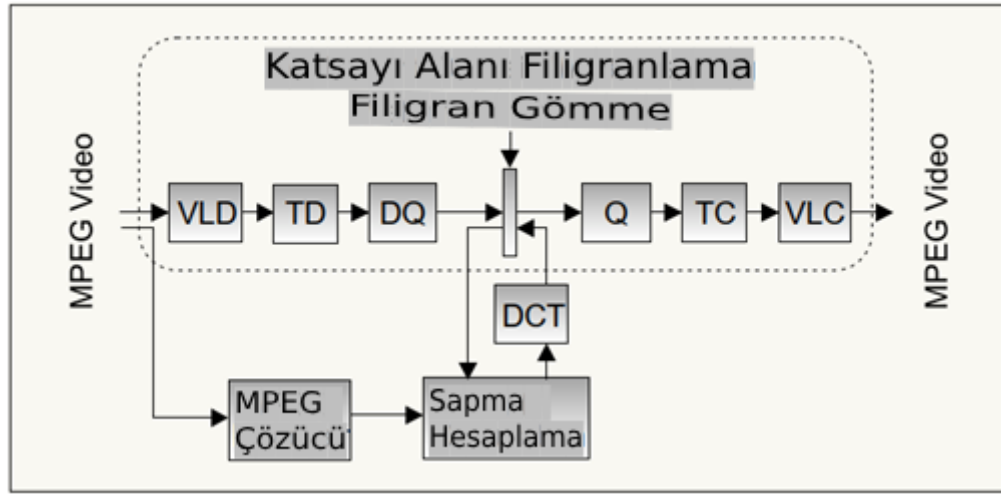
$$I_{W_{x,y}}(0) = I_{\bar{x},y}(0) + W_{\bar{x},y}(0) \quad (3.22)$$

Bu, filigran bloğunun ortalama değerinin video bloğunun ortalama değerine eklenmesi anlamına gelir.

2. AC-katsayılarını modüle etmek için, kodlanmış video bloğunun bit akışı VLC (Değişken Uzunluklu Kodlaması) koduna göre taranır ve bir sonraki sıfırdan farklı DCT katsayısını temsil eden sonraki VLC kod kelimesi bulunur. Bu kod kelimesinin çalışma ve seviyesi, konumunu zigzag tarama üzerindeki i pozisyonunu ve büyüklüğünü $I_{x,y}(i)$ belirlemek için çözümlenir. Filigranlı video bloğu için aday bir DCT katsayısı üretilir ve aşağıdaki şekilde tanımlanır:

$$I_{W_{x,y}}(i) = I_{x,y}(i) + W_{x,y}(i), i \neq 0 \quad (3.23)$$

Şimdi, video bit hızının artırılmaması kısıtı devreye girer. $I_{x,y}(i)$ 'i kodlamak için gereken VLC'nin S_{z_l} boyutu ve $I_{W_{x,y}}(i)$ 'yi kodlamak için gereken VLC'nin boyutu $S_{z_{lw}}$, MPEG-2 standardının VLC-Tabloları B.14 ve B.15 kullanılarak belirlenir (Langelaar ve ark., 2000). Aday DCT katsayısını kodlayan VLC'nin boyutu mevcut VLC'nin boyutuna eşit veya daha küçükse, mevcut VLC değiştirilir. Aksi takdirde, VLC etkilenmez. Kayma telafisi nedeniyle karmaşıklık artışı Şekil 3.24'da gösterilmiştir.



Şekil 3.24. Kayma telafisi nedeniyle karmaşıklık artışı. (Langelaar ve ark., 2000)

DCT katsayısı $I_{x,y}(i)$ aşağıdaki şekilde modüle edilir:

$$\text{If } Sz_{I_w} \leq Sz_I \text{ o zaman } I_{w_{x,y}}(i) = I_{x,y}(i) + W_{x,y}(i) \text{ aksi taktirde } I_{w_{x,y}}(i) = I_{x,y}(i) \quad (3.24)$$

Bu işlem, kodlanmış video bloğunun tüm AC-katsayıları işlenene kadar tekrarlanır. Filigran bilgisini çıkarmak için, MPEG kodlu video akışının ilk olarak kodu tamamen çözülür ve filigran bitleri, kodu çözülmüş çerçevelerin standart teknikler kullanılarak uzamsal alanda filigran modeli $W(x,y)$ ile ilişkilendirilmesiyle elde edilir.

MPEG kodlu bir video akışında DCT katsayılarını doğrudan değiştirmenin büyük bir sorunu, kayma veya hata birikimidir. Bir MPEG kodlu video akışında, önceki çerçevelerden gelen tahminler, gerçek çerçeveyi yeniden oluşturmak için kullanılır ve bu da gelecekteki tahminler için bir referans olarak hizmet edebilir. filigranlama işleminden kaynaklanan bozulma zamanla yayılabilir. Tüm video kareleri filigran basarken, önceki çerçevelerden ve mevcut çerçeveden gelen filigranları birikebilir ve görsel hatalara yol açabilmektedir.

$$I_{w_{x,y}}(i) = I_{x,y}(i) + W_{x,y}(i) + Dr_{x,y}(i) \quad (3.25)$$

Bu nedenle, kayma telafisi sinyali Dr eklenmelidir. Bu sinyal, filigranlanmamış bit akışının (hareketle telafi edilen) tahminleri ile filigranlı bit akışı arasındaki farka eşit

olmalıdır. Denklem (3.23), bir kayma telafili filigranlama düzeninde değişir. Kayma telafisi sinyalinin bir dezavantajı, filigranlaması algoritmasının karmaşıklığının önemli ölçüde artmasıdır, çünkü kayma telafisi sinyalini hesaplamak için ek bir DCT işlemi ve tam bir MPEG çözme adımı gerekmektedir.

Bit hızı kısıtı nedeniyle, DCT katsayılarının sadece yaklaşık olarak %10-20'si, video içeriği ve MPEG nicemleyicinin hassaslığına bağlı olarak filigranlama işlemiyle değiştirilir. Bazı durumlarda, özellikle çok düşük bit hızına sahip videolarda, yalnızca DC-katsayıları değiştirilir. Bu, yalnızca filigranı deseni $W(x, y)$ 'nin bir kısmının gömülebileceği anlamına gelir, genellikle yaklaşık olarak %0.5... 3% arasında (Hartung ve Girod, 1998). Sadece mevcut (sıfırdan farklı) DCT katsayıları filigranlı olduğu için, gömülü filigranı video içeriğine bağımlıdır. Sadece düşük frekanslı içeriğe sahip bölgelerde, filigranı otomatik olarak yalnızca düşük frekans bileşenlerinden oluşur. Bu, HVS ile uyumludur. filigranı enerjisi, çoğunlukla çok miktarda video içeriği enerjisi içeren bölgelere gömülür.

(Hartung ve Girod, 1998) makalesindeki yazarlar, filigranın yerleştirme sürecinin karmaşıklığının, mekansal alanda filigranı ekleme ve yeniden kodlama sürecini takip eden bir çözme işlemi karmaşıklığından çok daha düşük olduğunu bildirir. Karmaşıklık, tam bir MPEG çözme işlemi karmaşıklığından biraz daha yüksektir. Gömme için tipik parametre ayarları, filigranı kazanç faktörü için $k=1, \dots, 5$ ve filigranı biti başına piksel sayısı için $P=500,000, \dots, 1,000,000$ olup, bu da filigranı etiket bit hızlarının saniyede sadece birkaç bayt olduğunu verir. Yazarlar, filigranın görünmez olduğunu, sadece filigranlanmamış videoyla doğrudan karşılaştırmada görülebildiğini ve filigranın mekansal veya frekans alanında filtreleme, gürültü ekleme ve nicemleme gibi doğrusal ve doğrusal olmayan işlemlere karşı sağlam olduğunu ifade etmektedir.

3.3.8. Korelasyon tabanlı olmayan filigranlama teknikleri

En Az Anlamlı Bit Değiştirme Korelasyona dayanmayan mekansal alan filigranlama tekniklerinin en basit örneği, LSB değiştirme yöntemidir. Bir gri seviye görüntüde her piksel 8 bit değeriyle temsil ediliyorsa, görüntü sekiz bit düzlemine ayrılabilir.

En az anlamlı bit düzlemi görsel olarak anlamlı bilgi içermediğinden, büyük bir miktarda filigranı bitiyle kolayca değiştirilebilir. LSB değişikliklerini kullanan daha karmaşık filigranlama algoritmaları (Schyndel ve ark., 1994; Aura, 1995; Aura, 1996;

Hirotsugu, 1996; Fridrich ve Goljan, 1999) gibi kaynaklarda bulunabilir. Bu filigranlama teknikleri çok güvenli değildir ve işleme tekniklerine karşı dayanıklı değildir, çünkü LSB düzlemi kolayca rastgele bitlerle değiştirilebilir ve böylece filigranı bitleri kaldırılabilir.

3.3.9. Parite bit değiştirme ile mpeg video filigranlama

Sıkıştırılmış bir bit akışında, sıkıştırma algoritmasında kullanılan kod kelimelerine doğrudan erişim sağlanmaktadır. Yukarıda açıklanan LSB tekniğine benzer şekilde, bu kod sözcükleri değiştirilerek, yüksek yükleme kapasiteli, hesaplama açısından verimli bir filigranlama yöntemi elde edilebilir (Langelaar ve ark., 1998; Hanjalic ve ark., 2000).

Teknik aşağıdaki gibi açıklanmaktadır.

1 etiket biti b_j 'den ($j = 0, 1, 2, \dots, l - 1$) oluşan bir filigran, uygun VLC'ler seçilerek ve nicelenmiş seviyelerinin LSB'sini b_j değerine zorlayarak MPEG akışına gömülür. Kodlama sonrasında VLC'deki değişikliğin çözme sonrası algılanabilir ve MPEG bit akışının orijinal boyutunu koruduğundan emin olmak için, yalnızca başka bir VLC'nin birlikte bulunduğu VLC'ler seçilir.

- Aynı çalışma uzunluğuna sahip,
- Bir birimlik kantize seviye farkına sahip,
- Aynı kod kelimesi uzunluğuna sahip.

Bu gerekliliği karşılayan bir VLC, bir etiket-bit taşıyan VLC (lc-VLC) olarak adlandırılır. MPEG-2 standardının B.14 ve B.15 tablolarına göre (Langelaar ve ark., 2000), böyle birçok lc-VLC mevcuttur. Ayrıca, Kaçış-kodundan (Escape-code) takip eden tüm sabit uzunluklu kodlanmış DCT katsayıları da bu gerekliliği karşılar.

İntra ve inter kodlu makroblokardaki VLC'ler filigranlama işleminde kullanılabilir. DC katsayıları kullanılmaz, çünkü diğer DC katsayılarından tahmin edilir ve farklı bir set VLC ve Kaçış kodu ile kodlanır. Ayrıca, intra ve inter kodlu karelerdeki her bir DC katsayısının değiştirilmesi, kayma nedeniyle görünür eserlere yol açabilir. Sadece AC katsayılarını dikkate alarak, filigran video içeriğine daha iyi uyum sağlayacak ve kayma sınırlı olacaktır.

MPEG-video bit akışına etiket bit akışı L'yi eklemek için, her makro bloktaki VLC'ler test edilir. Eğer bir lc-VLC bulunursa ve seviyesinin LSB'si etiket biti b_j ($j=0,1,2,\dots,l-1$) ile eşit değilse, bu VLC başka bir VLC ile değiştirilir ve yeni VLC'nin

LSB seviyesi etiket bitini temsil eder. Eğer seviyenin LSB'si etiket biti b_j ile eşitse, VLC değiştirilmez. Bu işlem, tüm etiket bitleri gömülünceye kadar tekrarlanır.

Etiket bit akışı L 'yi çıkarmak için, her makro bloktaki VLC'ler test edilir. Bir lc-VLC bulunursa, seviyesinin LSB tarafından temsil edilen değer etiket biti b_j olarak atılır. Bu işlem, $j=0,1,2,...,l-1$ için tekrarlanır ve artık lc-VLC bulunamayana kadar devam eder.

Bu teknik, anlamlı bir kalite bozulması olmaksızın yüksek bir yükleme kapasitesi (en fazla 29 kbit/s) sağlar (Langelaar, 2000). Bu yöntemle gömülen filigranı, video akışının çözülüp yeniden kodlanması veya başka bir rastgele üretilen filigranı deseni kullanılarak akışın yeniden etiketlenmesiyle kolayca kaldırılabilir. Bu teknik, yeniden etiketlemeye dirençli hale getirmek için aşağıdaki gibi genişletilebilir (Langelaar, 2000). Artık etiket bitleri b , VLC'lerin LSB'lerine doğrudan depolanmaz, bunun yerine gizli bir anahtara dayalı $\{-1,1\}$ tam sayılardan oluşan bir boyutlu bir sözde rasgele filigranı deseni $W(x)$ üretilir ve bu desen b_i etiket bitleriyle modüle edilir. Bu modüle deseni video akışına eklemek için kullanılan işlem yukarıda açıklanan işleme benzerdir.

Aynı çalıştırma uzunluğuna ve aynı kod sözcüğü uzunluğuna sahip başka iki VLC'nin olduğu VLC'ler de yalnızca seçilir. Bir VLC'nin seviye farkı $+\delta$ ve diğer VLC'nin seviye farkı $-\delta$ olmalıdır. Birçok lc-VLC, göreceli olarak küçük bir 8 için (örn. $\delta=1,2,3$) bu gereklilikleri karşılar. bu modeli taşıyan VLC'ler basitlik için (pc-VLC'ler) olarak adlandırılır.

Filigranı bir video akışına eklemek için, modüle edilmiş filigran deseni pc-VLC'lerin seviyelerine eklenir. Filigranı kaldırmak için pc-VLC'ler bir dizide toplanır. filigranı etiket bitleri şimdi bu pc-VLC'lerin dizisi ile gizli filigranı deseni $W(x)$ arasındaki korelasyon hesaplanarak alınabilir. Bir filigranı etiket biti b_i kodlamak için 1.000 ile 10.000 arasında pc-VLC gereklidir ve böylece filigranı yükünü önemli ölçüde azaltır. Bununla birlikte, bağımsız farklı desenlerin temel deseni $W(x)$ oluşturmak için kullanılması durumunda, birbirleriyle etkileşmeden birden fazla filigranı etiket biti dizisi ekleyebilir.

3.3.10. DCT katsayısı sıralaması

(Koch ve Zhao, 1994; Koch ve Zhao, 1995; Zhao ve Koch, 1995; Burgett ve ark., 1998) çalışmalarında, bir filigranı bit dizisi 8×8 blok DCT alanında ekleyen bir filigranlama yöntemi önerilmiştir. Bir resme filigranı eklemek için, resim 8×8 bloklara

bölünür. Bu 8×8 bloklardan DCT dönüşümü hesaplanır ve her blokta orta bant frekanslarında F_M seçilen iki veya üç DCT katsayısı belirlenir. Seçilen katsayılar, varsayılan JPEG kuantizasyon tablosu (Pennebaker ve Mitchell, 1993) ve nispeten düşük bir JPEG kalite faktörü kullanılarak kantize edilir. Seçilen katsayılar, büyüklükleri belirli bir ilişki oluşturacak şekilde uyarlanır. Seçilen katsayılar arasındaki ilişkiler, sekiz deseni (kombinasyonu) oluşturur ve üç gruba ayrılır.

İki grup "1" veya "0" filigranı bitlerini temsil etmek için kullanılırken, üçüncü grup geçersiz desenleri temsil eder. Bir bloğun istenen deseni korumak için yapılan değişiklikler çok büyük hale gelirse, blok geçersiz olarak işaretlenir. Örneğin, bir bloğa değeri 1 olan bir filigranı biti gömülmesi gerekiyorsa, üçüncü katsayının diğer iki katsayıdan daha düşük bir değere sahip olması gerekmektedir.

3.3.11. DEW algoritması kullanarak MPEG video filigranlama

DEW yöntemi, sıkıştırılmış veri akışındaki yüksek frekanslı DCT katsayılarını seçici olarak atma temeline dayanır. Veri tanımlayıcısının (etiket) bilgi bitleri, yüksek frekanslı DCT katsayıları çıkarılan DCT bloklarının bir deseninde, yani DCT blokları arasındaki enerji farkı deseninde kodlanır. Bu nedenle, teknik diferansiyel enerji filigranı (DEW) olarak adlandırılır.

Yöntem şu şekilde açıklanır. (Langelaar ve ark., 2000)'in gömülmek istediği bilgi etiket bit dizisi L_j ($j = 0, 2, \dots, l - 1$) olarak temsil edilir. Bu etiket biti dizisi, bir JPEG sıkıştırılmış sabit resimden veya bir MPEG sıkıştırılmış video akışının I-kareden alınan n adet 8×8 DCT bloğuna bit bit gömülür. Tartışmanın basitliği için, durağan görüntüler ve MPEG I-kareni "görüntüler" olarak anılacaktır.

Yeterli dayanıklılık elde etmek için n genellikle 16 ile 64 arasında değerler alır, bu da tek bir etiket bitinin bir görüntü bölgesine gömüldüğü anlamına gelir. Ancak, etiket bitleri gömülmeden önce, 8×8 DCT bloklarının görüntü içindeki konumları rastgele karıştırılır. Bu karıştırma işlemi, bir yandan etiketleme algoritmasının gizli anahtarı oluştururken, diğer yandan DCT bloklarının istatistiklerini mekansal olarak rastgele hale getirir.

Etiket biti dizisinin her bir biti, karışık bir görüntüdeki özel etiket biti taşıyan bölgesi veya kısaca lc-bölgesinde gömülür.

"Yüksek frekanslı" enerjinin JPEG veya MPEG sıkıştırılmış görüntüler veya video kareleri için kolayca belirlenmesi için, $S(c)$ tarafından gösterilen zigzag taranmış DCT katsayılarının bir alt kümesi üzerinde enerji hesapları yapılır.

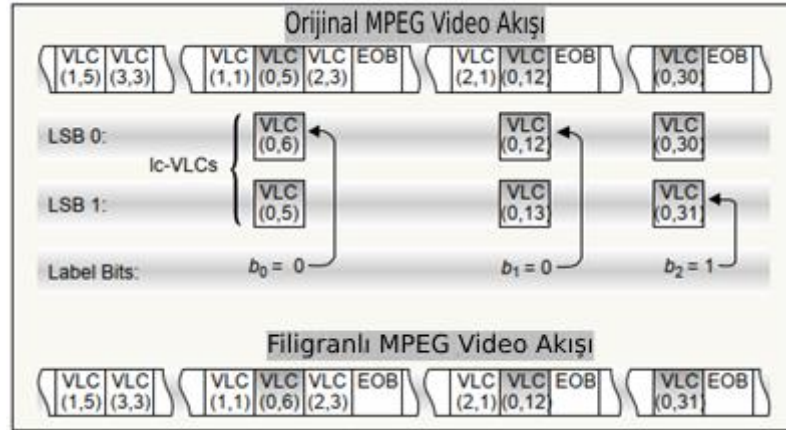
$$S(c) = \{i \in \{0,63\} | (i > c)\} \quad (3.26)$$

Zigzag taranmış DCT katsayıları (3.26) ile yüksek frekanslı DCT katsayılarının taşıdığı enerjinin hesaplanmasına göre numaralandırılmıştır. $i=0$ indeksi bir DCT bloğunun DC-katsayısına karşılık gelir. Enerjilerin hesaplandığı DCT katsayıları alt kümesi $S(c)$, kesim indeksi c tarafından tanımlanır. Bir lc-bölgesi için uygun bir kesim indeksi seçimi, etiket dayanıklılığı ve görünürlüğü açısından önemlidir. Kesim indeksi ne kadar büyükse, etiket gömme işlemi tarafından girilen bozulma o kadar az olur. Burada her lc-bölgesi için uygun bir kesim indeksi olduğu varsayılmıştır (Langelaar ve ark., 2000). Unutulmamalıdır ki farklı lc bölgeleri, mekansal içeriklerine bağlı olarak farklı kesim indekslerine sahip olabilir.

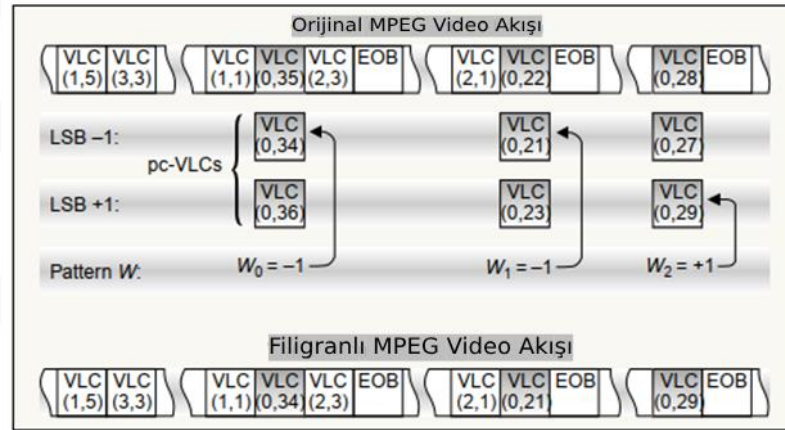
Enerji E_A , lc-altbölgesi A'daki (DCT yüksek frekanslı) enerji, aşağıdaki şekilde tanımlanır:

$$E_A(c, \eta, Q_{jpeg} = \sum_{b=0}^{\frac{n}{2}-1} \sum_{i \in S(c)} ([\theta_{i,b}]_{Q_{jpeg}})^2 \quad (3.27)$$

Burada $\theta_{i,b}$, incelenmekte olan lc-alt bölgesi A'nın b'nci DCT bloğundaki i indeksi ile ağırlıklandırılmamış DCT katsayısını gösterir. E_A 'nın hesaplanmasından önce $[\]_{Q_{jpeg}}$ notasyonu, bizim durumumuzda Q_{jpeg} kalite faktörü ile standart JPEG niceleme prosedürü (Pennebakker ve Mitchell, 1993) kullanılarak DCT katsayılarının yeniden veya önceden nicelleştirildiğini belirtir. Etiket bitlerini MPEG sıkıştırılmış I-karelerine gömmek için benzer bir yaklaşım izlenebilir. Ön kantilenme işlemi, yalnızca kesme indekslerinin belirlenmesi ve (3.26) formülünün hesaplanması için kullanılır, ancak etiket gömülmesi sırasında gerçek görüntü verilerine uygulanmaz. LSB filigran örneği Şekil 3.25a 'da ve Yeniden etiketlemeye dayanıklı filigranlama yönteminin örneği Şekil 3.25b'de verilmiştir.



Şekil 3.25a. LSB filigran örneği. (x, y) çiftleri, MPEG VLC kodlamasında kullanılan (sıfır çalıştırma, düzey) çiftlerini temsil eder. (Langelaar ve ark., 2000)



Şekil 3.25b. Yeniden etiketlemeye dayanlı filigranlama yönteminin örneği. (Langelaar ve ark., 2000)

lc alt bölgesi B'deki enerji, E_B ile benzer şekilde tanımlanır.

lc alt bölgesi A ve lc alt bölgesi B arasındaki enerji farkı D şu şekilde tanımlanır:

$$D(c, n, Q_{jpeg}) = E_A(c, n, Q_{jpeg}) - E_B(c, n, Q_{jpeg}) \quad (3.28)$$

Bir etiket bitinin değeri, enerji farkı D'nin işareti olarak kodlanır. Etiket biti 0, $D > 0$ olarak tanımlanırken, etiket biti 1, $D < 0$ olarak tanımlanır. Bu nedenle etiket yerleştirme prosedürü, enerji farkını D manipüle etmek için E_A ve E_B 'yi uyarlanmalıdır. Etiket biti 0'ın gömülmesi gerekiyorsa, lc-alt bölge B'nin DCT bloklarında kesme indeksi c'den sonraki tüm enerji karşılık gelen DCT katsayılarını sıfıra ayarlayarak sona ulaşmaktadır.

Bu nedenle, etiket gömme işlemi E_A ve E_B yi D enerji farkını manipüle etmek için uyarlamamız gerekmektedir. Etiket biti 0 gömülmeliyse, lc alt bölgesi B'nin DCT bloklarındaki kesim noktası c'den sonraki tüm enerji, ilgili DCT katsayıları sıfıra ayarlanarak ortadan kaldırılır. Bu durumda

$$D = E_A - E_B = E_A - 0 = +E_A \quad (3.29)$$

Eğer etiket biti 1 gömülmeliyse, lc alt bölgesi A'nın DCT bloklarındaki kesim noktası c'den sonraki tüm enerji, $D = -E_B$ elde edilerek ortadan kaldırılır. Filigranı sıkıştırılmış bit akışına gömüldüğü için, DCT katsayıları bit akışını yeniden kodlamadan kolayca sıfıra zorlanabilir, seçilen kesim noktasına kadar 8 x 8 DCT bloklarının bitiş işareti (EOB) bir lc alt bölgesi'den DC-katsayısına doğru kaydırılarak yapılabilir.

3.3.12. Belirgin nokta modifikasyonu

(Rongen ve ark., 1999)'de, bir görüntünün belirgin noktalarının değiştirilmesine dayanan bir filigranlama yöntemi önerilmektedir. Belirgin noktalar, bir görüntüdeki belirli bir belirginlik fonksiyonunun maksimum olduğu izole noktalar olarak tanımlanır. Bu noktalar, örneğin bir görüntüdeki köşeler veya yüksek enerji bölgeleri olabilir.

Bir filigranı gömmek için görüntüden en yüksek belirginliğe sahip piksellerin kümesi S çıkarılır. Daha sonra, aynı boyutta bir ikili rasgele desen $W(x, y)$ oluşturulur. Üç katsayı arasındaki ilişkinin uyarlanması temelinde filigranlama Şekil 3.26 ve DCT katsayıları arasındaki ilişkileri uyarlayarak oluşturulan filigranlama Şekil 3.27'de gösterilmiştir.

Bu bir çizgi veya blok deseni olabilir. Eğer bu desen yeterince rasgele ve tüm piksellerin %50'sini kaplıyorsa, küme S'teki tüm belirgin noktaların %50'si desen üzerinde (yani desendeki siyah piksellerde), %50'si desen dışında yer alır. Son olarak, küme S'teki belirgin noktalar, istatistiksel olarak anlamlı bir yüksek yüzdeye sahip olacak şekilde uyarlanır, yani büyük bir kısmı filigranı deseninin üzerinde bulunur. Belirgin noktaları uyarlamak için iki yol vardır:

- Belirgin noktaların konumu, noktaları filigranı desenine doğru bükerek değiştirilebilir. Bu durumda, görüntüye küçük, yerel geometrik değişiklikler eklenir.
- Noktaların belirginliği, bir belirgin noktanın çevresine iyi seçilmiş piksel desenlerinin eklenmesiyle azaltılabilir veya artırılabilir.

Filigranını algılamak için görüntüden en yüksek belirginliğe sahip piksellerin kümesi S çıkarılır ve belirgin noktaların desen üzerindeki ve desen dışındaki yüzdeliklerini karşılaştırılır. Eğer her iki desende de yaklaşık olarak %50 ise filigranı algılanmaz. Eğer belirgin noktaların yüksek bir yüzdesi desen üzerinde bulunuyorsa, filigranı algılanır. Bu doğrultuda filigranının taşıma kapasitesi 1 bittir.

3.3.13. Fraktal tabanlı filigranlama

Fraktal sıkıştırma tekniklerine dayanan birçok filigranı gömmesi algoritması önerilmiştir (Davern ve Scott, 1996; Puate ve Jordan, 1996; Bas ve ark., 1998; Bas ve ark., 1999). Bunlar genellikle blok tabanlı yerel iterasyon fonksiyon sistemi kodlaması (Jacquin, 1992) kullanır. Burada ilk olarak fraktal sıkıştırma algoritmasının temel ilkeleri kısaca açıklanmıştır. Bir görüntü, iki farklı çözünürlük seviyesinde bölünür. İlk seviyede, görüntü $n \times n$ boyutundaki aralık bloklarına bölünür. İkinci seviyede, görüntü $2n \times 2n$ boyutundaki alan bloklarına bölünür. Her aralık bloğu için, iki blok arasındaki ortalama kare hatanın en küçük olduğu dönüştürülmüş bir alan bloku aranır. Aralık blokları, alan bloklarıyla eşleştirilmeden önce, aşağıdaki dönüşümler alan blokları üzerinde uygulanır.

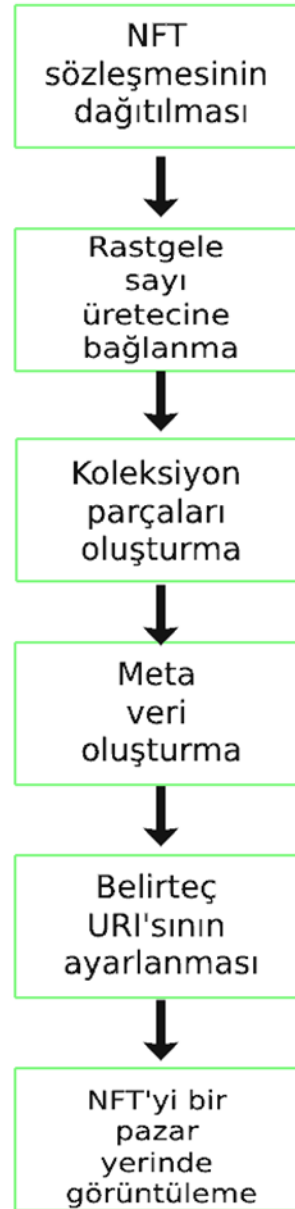
İlk olarak, alan blokları, boyutlarının aralık bloklarıyla aynı olması için iki kat azaltılır. Ardından, alan bloklarının sekiz izometrisi belirlenir (orijinal blok ve onun aynalı versiyonu 0, 90, 180 ve 270° döndürülmüş olarak). Son olarak, ışıklılık değerleri için ölçek faktörü ve ofset uyarlanır. Görüntü artık, her aralık bloğu için uygun geometrik ve ışıklılık dönüşümlerini kullanarak ilişkiler kümesi tarafından tamamen tanımlanır: en iyi uyan alan bloğunun dizin numarası, yönelimi, ışıklılık ölçeklendirme ve ışıklılık ofseti. Bu ilişkiler kümesini kullanarak, bir görüntü kodlayıcısı, her bir aralık bloğunun ilgili alan bloğundan ilişkili geometrik ve ışıklılık dönüşümlerini kullanarak içeriğini hesaplayarak görüntüyü yeniden oluşturabilir. Sonuç olarak elde edilen görüntüyü başlangıç görüntüsü olarak alarak bu süreci tekrarlayarak orijinal görüntü içeriği yeterince yakın bir şekilde yaklaşıncaya kadar devam edilir.

3.4. NFT Oluşturma

NFT oluşturma süreci, benzersiz ve doğrulanabilir dijital varlıkların üretimi, depolanması ve dağıtımını sağlamak için birkaç adım içerir. Bu adımlar, NFT sözleşmesini kullanıma sunma, rastgele sayı üretici entegrasyonu, koleksiyon parçaları

oluřturma, meta veri üretme, isteęe baęlı olarak meta verileri ve görselleri IPFS'ye yükleme, jeton URI'sini ayarlama ve NFT'yi bir pazarda gösterme işlemlerini kapsar.

Bu çalışma büyük ölçüde (Patrick, 2021) ve (Qingquan Wang, 2021)'dan esinlenmiştir. NFT'lerin oluřturma ve dağıtma adımları ařaęıdaki řekil 3.26'da gösterilmektedir.



Şekil 3.26. NFT'lerin oluřturulması ve devreye alınması süreçleri

3.4.1. NFT sözleşmesini kullanıma sunma:

Proje, Takas Olmayan Jetonlar (NFT'ler) oluşturan bir akıllı sözleşmenin kullanıma sunulmasıyla başlar. Sözleşme, Ethereum blockchain üzerinde benzersiz jetonların oluşturulmasına olanak tanıyan yaygın olarak kabul gören ERC721 standardına dayanmaktadır.

3.4.2. Rastgele sayı üretici entegrasyonu:

Koleksiyonlara rastgele bir öğe eklemek için sözleşme, Chainlink'in Doğrulanabilir Rastgele Fonksiyonu (VRF) ile entegre olur. Bu, her koleksiyon parçasının türünün oluşturma sonrası rastgele atanmasını sağlar.

3.4.3. Koleksiyon parçaları oluşturma:

Kullanıcılar yeni bir koleksiyon öğesi oluşturmak istediklerinde akıllı sözleşmeye bir istekte bulunurlar. Sözleşme daha sonra Chainlink VRF kullanarak bir rastgele sayı üretir ve bu sayede yeni koleksiyona bir tür atar. Tür, önceden tanımlanmış üç türden biri olarak seçilir. Tür atanır atanmaz, koleksiyon parçası basılır ve sahiplik istekte bulunan kullanıcıya devredilir.

3.4.4. Meta veri üretme:

Oluşturulan her koleksiyon öğesi için ek bilgiler sağlayan meta veriler üretilir, örneğin ad, açıklama ve resim. Meta veriler JSON (JavaScript Nesne Gösterimi) dosyası olarak oluşturulur ve zincir dışında saklanır. Her tür için görseller, önceden tanımlanmış bir görsel URL dizisinden alınır.

3.4.5. Meta verileri ve görselleri IPFS'ye yükleme (isteğe bağlı):

Proje, meta verilerin ve görsellerin İçerik Adresli Dosya Sistemi (IPFS) olarak bilinen ve dağıtık bir dosya sistemi olan IPFS'ye isteğe bağlı olarak yüklenmesine olanak tanır. Bu adım, meta verilerin ve görsellerin, orijinal barındırma sunucusunda bir arıza olsa bile erişilebilir ve değiştirilemez kalmasını sağlar.

3.4.6. Jeton URI'sini ayarlama:

Meta verileri ve görselleri IPFS'ye yükledikten sonra (ayarlandıysa), her koleksiyon için jeton URI ayarlanır. Jeton URI, ilgili koleksiyon için meta veri dosyasına işaret eden benzersiz bir URL'dir. Bu, akıllı sözleşmedeki bir işlevi çağırarak ve tokenId ile birlikte meta veri URL'sini sağlayarak gerçekleştirilir.

3.4.7. NFT'yi bir pazarda gösterme:

Jeton URI ayarlandıktan sonra kullanıcılar, NFT'lerini OpenSea gibi pazarlarda sergileyebilirler; burada meta veriler ve görseller sergilenir. Bu, kullanıcıların benzersiz koleksiyonlarını sergilemelerine, takas etmelerine veya satmalarına olanak tanır.

Özetle, NFT oluşturma süreci, Ethereum blockchain üzerinde rastgele atanmış türlerle benzersiz koleksiyonlar oluşturma, her koleksiyon için meta veri üretme, isteğe bağlı olarak meta verileri ve görselleri IPFS'ye yükleme, meta verilere işaret eden jeton URI'sini ayarlama ve kullanıcıların NFT'lerini bir pazarda sergilemelerine olanak tanıma işlemlerini içerir.

3.5.Video ve Ses İşleme

Video ve ses işleme, video için ayrıştırma, demultipleksleme, kod çözme, kare çıkarma, görüntü kodlama ve çıktı ile ses için giriş dosyasını analiz etme, ses akışını kod çözme, işleme ayarları, ses kalitesini yapılandırma, ses akışını kodlama ve ses çıktısını yazma gibi birçok adımları içermektedir.

3.5.1 Video işleme

Kontrol Etme: Program, giriş video dosyasını okur ve video, ses, meta veri akışlarını kapatmaktan sorumlu konteyner formatını belirler (ör. MP4, AVI, MKV vb.). Konteyner formatı, dosya içindeki bireysel akışların nasıl düzenlendiğini belirler.

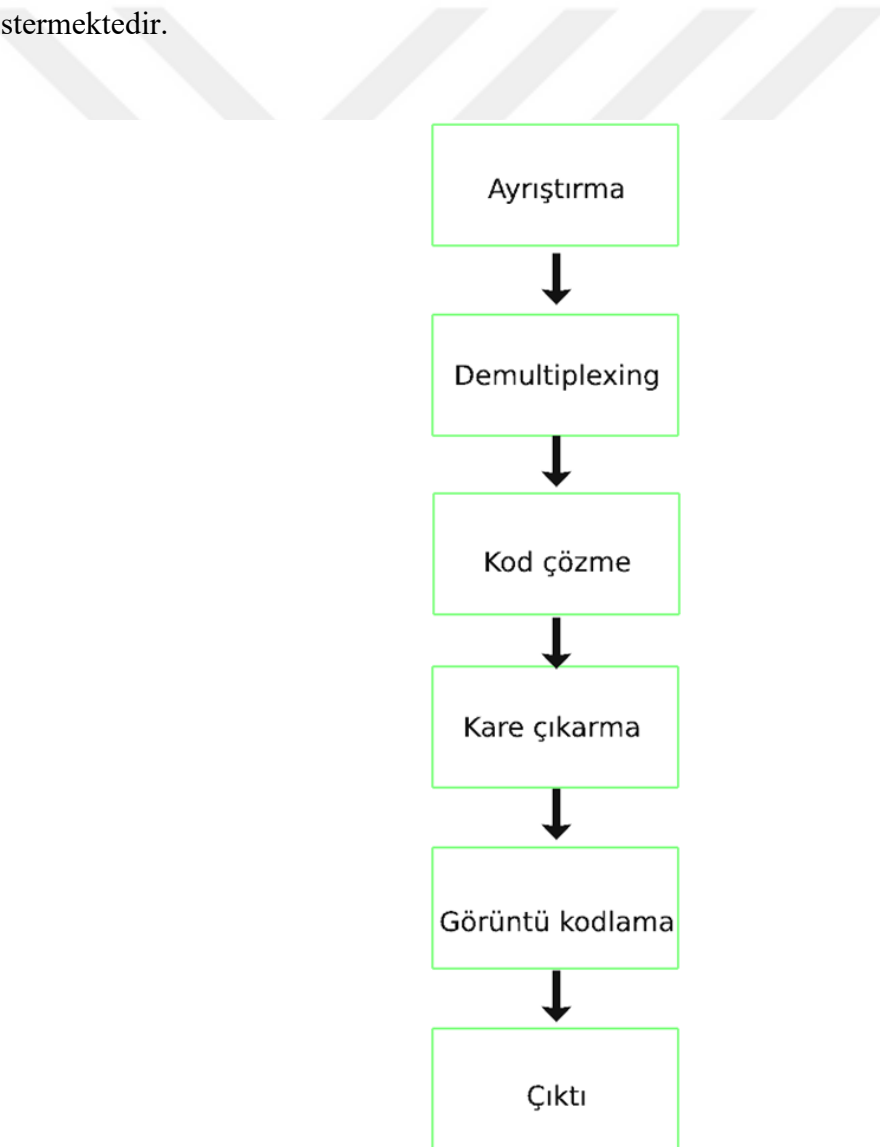
Ayrırma İşlemi: Konteyner formatı belirlendikten sonra program, video, ses ve varsa altyazıları içeren farklı akışları ayırmaktadır. Kare çıkarma durumunda, program öncelikle video akışına odaklanır.

Kod çözme: Video akışı genellikle belirli bir algoritma kullanılarak sıkıştırılır (ör. H.264, VP9, HEVC vb.). Program, sıkıştırılmış video akışını kod çözer ve bunu ham, sıkıştırılmamış kareler dizisine dönüştürür. Kod çözme, kodeğe bağlı olarak sıkıştırmanın açılması, hareket telafisi ve ters dönüşüm gibi diğer işleme adımlarını içerir.

Kare çıkarma: Video akışı artık bireysel karelere kod çözüldüğüne göre, program her kareyi ayrı ayrı çıkarır.

Görüntü kodlama: Program, her çıkarılan kareyi istenen görüntü formatına dönüştürür (bu durumda PNG). Bu, ham kare verilerini belirli bir görüntü formatına kodlamayı, gerekli sıkıştırmayı ve görüntü dosyasını yazmayı içerir.

Çıktı: Son olarak, program her kodlanmış görüntüyü belirtilen dizine, verilen adlandırma düzeni ile kaydeder. Şekil 3.27, videodan kareleri çıkarma işlemlerini aşağıda göstermektedir.



Şekil 3.27. Videodan kareleri çıkarma işlemleri

3.5.2. Ses işleme

Giriş dosyasını analiz etme: Program, giriş dosyasını okur ve video ve ses algortimaları, bit hızları ve akış süreleri gibi özelliklerini analiz eder.

Ses akışını kod çözme: Program, giriş ses akışını kod çözer ve orijinal kodekten (ör. AAC(Gelişmiş Ses Kodlaması)) sıkıştırılmamış bir formata (ör. PCM) dönüştürür. İşleme ayarları: Verilen komut, ses çıktısı için libmp3lame algoritma bileşenini belirtir. Program, bu algoritma bileşenini çıktı ses akışını kodlamak için kullanacaktır.

Ses kalitesini yapılandırma: Program, libmp3lame algoritması için en yüksek kaliteyi ve minimum sıkıştırmayı sağlayacak şekilde yapılandırır.

Ses akışını kodlama: Program, ses akışını belirtilen kalite ayarları ile libmp3lame algoritma bileşeni kullanarak MP3 formatına kodlar.

Ses çıktısını yazma: Program, kodlanmış MP3 ses akışını "audio.mp3" çıktı dosyasına yazar.

Özetle, video ve ses işleme, video ve ses akışlarının işlenmesi ve dönüştürülmesi için çeşitli adımlar içerir. Video işleme, giriş dosyasının ayrıştırılmasından çıktı görüntülerin oluşturulmasına kadar uzanırken, ses işleme, ses dosyasının analizinden ve kod çözülmesinden ses akışının yeniden kodlanması ve çıktı dosyasına yazılmasına kadar uzanır. Bu süreçler, videoların ve ses dosyalarının düzenlenmesi, dönüştürülmesi ve işlenmesi için önemli adımlardır. Şekil 3.28, videodan ses çıkarma işlemlerini aşağıda göstermektedir.



Şekil 3.28. Videodan ses çıkarma işlemleri

3.6. Tüm Video Karelerine NFT Gömme:

DWT, SVD ve DCT yöntemlerini kullanarak filigran gömme işlemi aşağıdaki adımları içerir:

Giriş görüntüsü BGR(Mavi Yeşil Kırmızı) renk uzayında verilir ve ardından YUV renk uzayına dönüştürülür. Bunun nedeni, insan gözünün Y kanalına (ışık şiddeti) U ve V kanallarından (krominans) daha duyarlı olmasıdır. YUV renk uzayında çalışmak, filigranın insan gözü için daha az algılanabilir bir şekilde yerleştirilmesine olanak tanır.

Görüntünün Y ve U kanallarına Ayırık Dalgacık Dönüşümü (DWT) uygulanır. Bu adım, görüntüyü farklı frekans alt bantlarına ayırarak, filigranın insan gözü için daha az hassas olan yüksek frekans bileşenlerine gömülmesine olanak tanır.

Görüntü bloklara ayrılır ve filigran bitleri bu bloklara kodlanır. İşlem, DWT'den elde edilen yaklaşım katsayıları matrisindeki her blok için gerçekleştirilir.

Her blok için Ayırık Kosinüs Dönüşümü (DCT) uygulanır. Bu, bloğu mekansal alandan frekans alanına dönüştürür ve bloğun enerjisini birkaç katsayıda yoğunlaştırır. Bu adım, filigranın görsel etkisi en aza indirgenmiş şekilde gömülebileceği blok alanlarını belirlemeye yardımcı olur.

DCT katsayılarına Tekil Değer Ayırıştırması (SVD) uygulanır. SVD, bir matrisi diğer üç matrisin çarpımı olarak ifade eden bir matris faktörizasyon tekniğidir. Bu durumda, DCT katsayıları üç matrise ayrılır: U, S (tekil değerleri içeren bir köşegen matris) ve V.

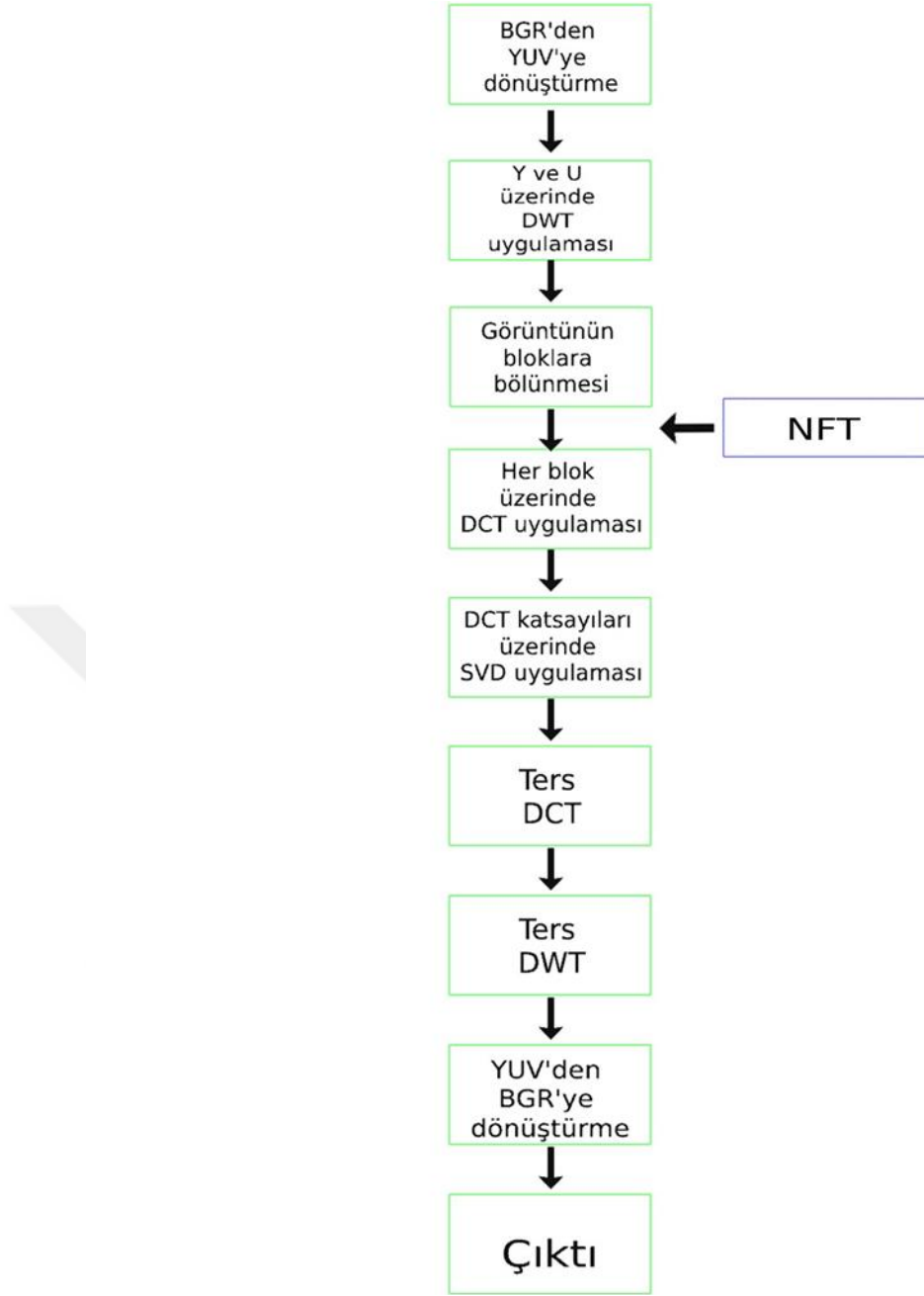
Filigran biti, tekil değerler matrisine (S) ilk tekil değeri hafifçe değiştirerek gömülür. Değişiklik, filigran bitinin daha sonra kod çözme işlemi sırasında algılanabilmesi için yapılır, ancak blokta önemli görsel değişikliklere neden olmayacak kadar incedir.

U, modifiye edilmiş S ve V matrislerini çarparak modifiye edilmiş DCT katsayıları elde edilir. Ardından, modifiye edilmiş katsayılar ters DCT uygulanır ve blok mekansal alana geri dönüştürülür.

Filigranlı bloklar, filigranlı yaklaşım katsayıları matrisini oluşturmak için birleştirilmiştir. Filigranlı yaklaşım katsayılarına ve diğer alt bantlara ters DWT uygulanarak filigranlı Y ve U kanalları elde edilir.

Filigranlı YUV görüntüsü, son filigranlı görüntüyü elde etmek için BGR renk uzayına geri dönüştürülür.

Filigran kod çözme işlemi, benzer adımları izler ancak filigranlı görüntüden filigran bitlerini çıkarmak için ters sırada gerçekleştirilir. Şekil 3.29, NFT'yi tüm çerçevelere yerleştiren işlemleri gösterir.



Şekil 3.29. NFT'yi tüm çerçevelere gömme işlemleri

3.7. Karelere ve Ses Dosyasına Videoyu Yeniden Birleştirme:

Program, kareleri ve ses dosyasını tek bir video dosyasına birleştirmek için birkaç adım izler. Çeşitli algoritmalar, formatlar ve optimizasyonlar nedeniyle, tam süreç oldukça karmaşık olabilir, ancak işlem adımlarına genel bir bakış:

Giriş dosyalarını çözme: Program, giriş dosyalarını (görüntü dizisi ve ses dosyası) açar ve uygun algoritmalarla çözer. Görüntü dizisi için program, dosya adındaki deseni

tanır ve görüntü dosyalarını doğru sırayla okur. Ses dosyası için program, uygun algoritma bileşenini kullanarak ses örneklerini çözer.

Senkronizasyon ve yeniden örnekleme: Gerekirse, program video ve ses akışlarını senkronize eder ve zaman içinde doğru şekilde hizalanmış olduklarını sağlar. Bu, sesin yeniden örneklendirilmesi veya belirtilen kare hızına uyacak şekilde video karelerinin zaman damgalarının ayarlanmasını içerebilir.

Video ve ses kodlama: Program, belirtilen algoritmaları kullanarak video ve ses akışlarını yeniden kodlar (video için libx264 ve ses için libmp3lame). Video algoritması, görüntü karelerini sürekli bir video akışına sıkıştırır ve ses algoritması, ses örneklerini sürekli bir ses akışına sıkıştırır.

Birleştirme İşlemi: Program, kodlanmış video ve ses akışlarını tek bir kap içerisine birleştirme (bu durumda MP4). Kap formatı, video ve ses akışlarını, düzgün oynatmayı sağlamak için akış bilgileri ve zamanlama verileri gibi gerekli metaverilerle birleştirir.

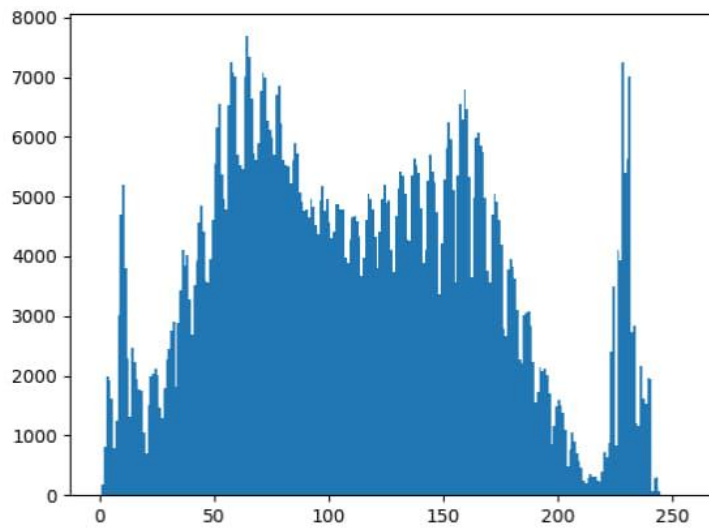
Çıktı dosyasını yazma: Program, verileri belirtilen çıktı dosyasına yazar. Bu dosya şimdi birleştirilmiş video ve ses akışlarını içerir ve oynatma veya daha fazla işlem için hazırdır.

4. ARAŞTIRMA SONUÇLARI VE TARTIŞMA

Bu Tez çalışması, önerilen Görünmez NFT Filigranlama algoritmasının filigranının bütünlüğünü tehlikeye atabilecek çeşitli saldırılara karşı dayanıklılığını ve verimliliğini test etmiştir. Algoritmanın performansı, Hamming Mesafesi, Bit Hata Oranı (BER), Ortalama Kare Hatası (MSE), En yüksek Gürültü Oranı (PSNR), Korelasyon Katsayısı ve başarıyla geri alınan filigranlarının yüzdesi gibi birkaç temel parametre kullanılarak değerlendirilmiştir. Aşağıdaki Şekil 4.1, Şekil 4.2, Şekil 4.3 ve Şekil 4.4'te orijinal kare, orijinal karenin histogramı, filigran kare ve filigran karenin histogramı belirtilmiştir.



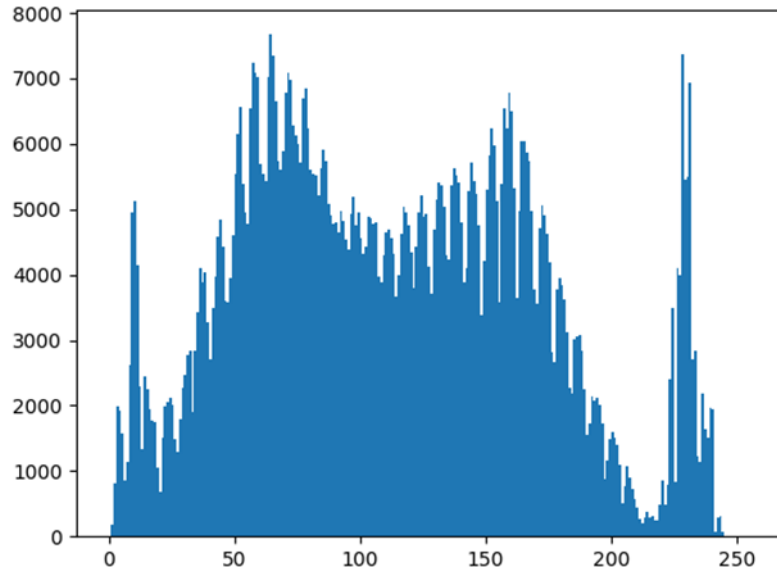
Şekil 4.1. Orijinal kare



Şekil 4.2. Orijinal karenin histogramı



Şekil 4.3. Orijinal filigranlı karen



Şekil 4.4. Orijinal filigranlı karenin histogramı

4.1 Sonuçların Genel Bakışı

Bu çalışmada önerilen, görünmez NFT filigranlama teknik üzerinde gerçekleştirilen çeşitli saldırılardan elde edilen sonuçlar ele alınmıştır. Bu saldırılar, filigranının dayanıklılığını değerlendirmek ve gömülü takas olmayan jetonun hangi özel durumlarda tehlikeye girebileceğini anlamak için araştırma yapılmıştır. Filigran eklenmiş videodaki Saldırılar çizelge 4.1’de listelenmiştir.

Orijinal video 25 fps, 1120 kb/s bit hızına sahiptir ve H.264 algoritması kullanılarak sıkıştırılmıştır.

Çizelge 4.1. Filigran eklenmiş videodaki Saldırılar

	Hamming Distance	BER	MSE	PSNR	Correlation Coefficient	Elde Edilen Filigran %
Orijinal filigran, saldırı olmadan	14807	0,016	11,510	37,519	0,999	100
Renk nicemleme saldırısı 8-bit	19235	0,020	21,674	34,771	0,998	96,202
Renk nicemleme saldırısı 16-bit	19282	0,0209	21,638	34,778	0,998	100
Palet tabanlı nicemleme GIF (256 renk)	24679	0,026	34,851	32,7085	0,988	35,820
Alt örnekleme 4:2:0 saldırısı	19235	0,0208	21,674	34,771	0,998	96,202
Alt örnekleme 4:2:2 saldırısı	19282	0,020	21,638	34,778	0,998	100
Sıkıştırma saldırısı bit hızı 1000k	18271	0,019	19,721	35,181	0,998	26
Kopyalama saldırısı	15558	0,016	13,471	36,836	0,999	100
Sıkıştırma saldırısı crf30	19217	0,020	21,770	34,752	0,997	35,66
Sıkıştırma saldırısı crf50	58902	0,063	65,060	29,997	0,973	6,56
Kayıpsız sıkıştırma saldırısı ffv1	15558	0,0168	13,471	36,836	0,999	100
Kare ortalaması saldırısı	26563	0,0288	28,662	33,557	0,980	2,5
Kare ekleme saldırısı	17211	0,018	16,259	36,019	0,997	6,477
Kare Hızı Değiştirme saldırısı fps 15	15765	0,017	14,320	36,571	0,998	19,9
Kare Hızı Değiştirme saldırısı fps 20	15762	0,017	14,245	36,593	0,998	82,278
Kare Hızı Değiştirme saldırısı fps 25	15807	0,017	14,129	36,629	0,998	94,936
Whatsapp Sıkıştırma saldırısı	15525	0,016	13,474	36,835	0,999	53,932
Mekansal	70308	0,076	68,132	29,797	0,964	5,98

filtreleme saldırısı GaussianBlur						
Gürültü ekleme saldırısı Gaussian Noise	30723	0,033	44,340	31,662	0,993	7,812
Frekans alanı filtreleme saldırısı Yüksek geçiren filtre	25136	0,027	26,918	33,830	0,996	7,142
Kayıpsız sıkıştırma saldırısı Huffiyuv	19243	0,020	21,096	34,888	0,998	100
Zamansal Saldırılar Kare ekleme 30	15970	0,017	14,382	36,552	0,998	94,936
Sıkıştırma Saldırısı Libx265 Crf28	17354	0,018	18,268	35,513	0,998	7,407
Sıkıştırma Saldırısı Libx265 Crf28 Yuv420p	20401	0,022	25,658	34,038	0,998	5,172
Sıkıştırma Libx265	17354	0,018	18,268	35,513	0,998	7,407
Frekans alanı filtreleme saldırısı Alçak geçiren filtre	19790	0,0214	23,963	34,335	0,998	11,904
Frekans alanı filtreleme saldırısı Medyan filtresi	35524	0,038	37,856	32,349	0,989	18,681
Örnek en-boy oranı saldırısı 2SAR	15665	0,0169	14,182	36,613	0,998	63,291
Ters oynatma saldırısı	18230	0,0197	19,067	35,327	0,998	31,868
Wiener filtre saldırısı	15516	0,0168	14,131	36,628	0,998	100

4.2. Her Saldırının Detaylı Analizi

Aşağıda birkaç belirli saldırı detaylı olarak ele alınmıştır:

4.2.1. Orjinal filigranlı saldırısız

Bu senaryo, kontrol veya temel durumumuzu temsil eder, yani orijinal filigranına hiçbir saldırı uygulanmaz. Herhangi bir değişiklik olmaksızın filigran lama sistemimizin doğal ölçütlerini anlamak için temel bir kavramdır. Bu durumda Hamming mesafesi 14807 ve Bit Hata Oranı (BER) 0,016'dur. Bu değerler düşüktür, çünkü orijinal video ile kendisi arasında minimal fark veya hata olması beklenir.

Ortalama Kare Hatası (MSE) ise 11,510'dur. Bu ölçüm, orijinal ve 'saldırıya uğramış' video (bu durumda orijinal kendisi) arasındaki ortalama kare farklarını temsil eder. Düşük MSE, teoride orijinal ve kendisi arasında hiçbir fark olmaması gerektiği beklentimizle uyumludur.

En yüksek Sinyal-Gürültü Oranı (PSNR) 37,519 dB'dir. PSNR, orijinal sinyalin maksimum olası gücü ile gürültü (bozulma) gücü arasındaki oranı ölçer. Bizim durumumuzda bozulma olmadığı için PSNR yüksektir, bu da mükemmel bir yeniden yapılandırma kalitesini işaret eder.

Korelasyon katsayısı 0,999'dir ve 1'e çok yakındır, bu da orijinal video ile kendisi arasında çok yüksek bir benzerlik olduğunu gösterir. Son olarak, filigranı kurtarma oranı %100'dür, bu da beklentilerimize uyumludur. Herhangi bir saldırı olmadığı için filigranı tamamen kurtarılabilir olmalıdır.

Bu temel senaryo, filigranlaması sistemimizin normal koşullarda doğru çalıştığını gösterir. Bu durumdan türetilen ölçütler, çeşitli saldırıların etkisini değerlendirmek için bir referans olarak kullanılacaktır.

4.2.2. Renk nicemleme saldırıları

Renk nicemleme, bir görüntüde kullanılan farklı renklerin sayısını azaltır. Bu, görüntü temsiliyetini basitleştirir ve filigranının bütünlüğünü bozabilmektedir.

4.2.2.1. 8-bit renk nicemleme saldırısı:

8-bit renk nicemleme saldırısında, videoda kullanılan renklerin sayısı önemli ölçüde azaltılır. Bu saldırı şekli, videodaki renk bilgisini basitleştirir ve potansiyel olarak filigranının bütünlüğünü bozabilir. Bu saldırıda Hamming mesafesi, renk nicemleme işlemi nedeniyle benzerlik azalmasıyla artan 19235'tir.

Bit Hata Oranı (BER), orijinal videodan biraz daha yüksek olan 0,020'dur, bu da saldırı nedeniyle biraz daha yüksek bir hata seviyesini işaret eder. Bu saldırı için Ortalama Kare Hatası (MSE) 21,674'tür ve neredeyse orijinal MSE'nin iki katıdır. Bu artış, renk nicemleme işlemi nedeniyle oluşan bozulmayı gösterir.

En yüksek Sinyal-Gürültü Oranı (PSNR) bu senaryoda 34,771 dB'ye düşer. Orijinal videoya göre bu düşüş, saldırıdan sonra filigranlı videonun kalitesinde bir azalmayı işaret eder. Korelasyon katsayısı biraz azalarak 0,998 olur, ancak hala yüksektir. Bu değer, bazı bozulmaların meydana gelmesine rağmen, genel olarak video yapısının büyük ölçüde korunduğunu gösterir. Saldırıya rağmen, filigranı kurtarma oranı %96,202 olarak nispeten yüksek kalmıştır. Bu değer, filigranla ması yöntemimizin renk nicemleme saldırılarına karşı direnç gösterdiğini savunmaktadır, çünkü filigranının büyük bir kısmı hala kurtarılabilmektedir.

Sonuç olarak, 8-bit renk nicemleme saldırısı videoya bazı hatalar ve bozulmalar katmış olsa da filigranı kurtarma üzerindeki etkisi nispeten küçüktür. Bu sonuç, kullanılan filigran lama tekniğinin bu seviyedeki renk nicemleme saldırılarına karşı direncini göstermektedir.

4.2.2.2. 16-bit renk nicemleme saldırısı:

Bu saldırıda Hamming mesafesi 19282'dir, bu da orijinal videoya göre bir artışı gösterir. Bu artış, renk bit derinliğinin 16 bit olarak azaltılmasıyla ortaya çıkan benzerlik azalmasını yansıtır.

Bit Hata Oranı (BER) biraz artarak 0,020'e yükselir, bu da saldırının ek hatalar eklediğini gösterir.

Ortalama Kare Hatası (MSE) 21,638'e yükselir ve neredeyse orijinal videonun iki katıdır, 8-bit renk nicemleme saldırısıyla benzerdir. Bu artış, 16-bit renk nicemleme işleminin önemli ölçüde bozulmalara yol açtığını gösterir. En yüksek Sinyal-Gürültü Oranı (PSNR) 34,778 dB'ye düşer. Bu düşüş, filigranlı videonun genel kalitesinin saldırıdan etkilendiğini göstermektedir.

Bu bozulmalara rağmen, korelasyon katsayısı hala yüksek olan 0,998'dir, bu da videonun büyük ölçüde orijinal yapısını koruduğunu gösterir. İlginç bir şekilde, bu saldırıdan sonra bile filigranı kurtarma oranı %100'dür. Bu sonuç, renk nicemleme saldırılarına karşı filigranlaması yönteminin dirençli olduğunu ve renk derinliğindeki azalmaya rağmen filigranının tamamen kurtarılabildiğini göstermektedir.

Sonuç olarak, 16-bit renk nicemleme saldırısı filigranlı videoda bir miktar bozulma ve hata getirmiş olsa da, filigranlama tekniği dirençli olduğunu kanıtlamış ve saldırı sonrası filigranının tamamen kurtarılabilir olduğunu göstermiştir. Bu saldırı biçimi altında filigranlaması yönteminin filigranı bilgisini koruma konusundaki sağlamlığı takdir edilebilir.

4.2.3. Palet tabanlı nicemleme gif (256 renk)

Palet tabanlı nicemleme GIF saldırısı, videonun 256 renkle sınırlı bir palet içinde GIF formatına dönüştürülmesini sağlar. Bu saldırı biçimi video kalitesini ve dolayısıyla filigranlamanın etkinliğini önemli ölçüde değiştirebilir.

Bu saldırıda Hamming mesafesi 24679'dur ve orijinal filigranından bir artış gösterir, bu da bu saldırının filigranını önemli ölçüde bozar. Bit Hata Oranı (BER) 0,026'e yükselmiştir, bu da saldırıdan sonra bit hatalarının sayısının arttığını gösterir. Bunun sebebi, 256 renkli paletle sınırlı olan GIF formatının, videoda ve sonuç olarak filigraninde bozulmaya neden olması olabilir.

Ortalama Kare Hatası (MSE) 34,851'ye yükselmiştir ve orijinal videodan önemli ölçüde artmıştır, bu da 256 renkli bir paletle nicemlemenin videonun verilerinde önemli değişikliklere neden olduğunu gösterir.

En yüksek Sinyal-Gürültü Oranı (PSNR) 32,708 dB'ye düşmüştür, bu da orijinal videoya göre genel video kalitesinin, bozulma ve gürültü açısından kötüleştiğini gösterir. Korelasyon katsayısı, orijinal videoya göre azalmış olsa da hala yüksek olan 0,988'dur, bu da orijinal ve saldırıya uğramış videolar arasında makul bir benzerlik düzeyi olduğunu gösterir. Bu bozulmalara rağmen, filigranı kurtarma oranı %35,82 gibi nispeten yüksek kalmıştır. Bu, filigranının üçte birinden fazlasının saldırı sonrası hala çıkarılabilir olduğunu gösterir.

Sonuç olarak, palet tabanlı GIF nicemleme saldırısı önemli bozulmalar ve artan hata oranları getirmiş olsa da filigranlama yöntemi yine de filigranının önemli bir kısmını korumayı başarmıştır. Bu direnç, bu tür saldırılara karşı kullanılan filigranlaması yönteminin sağlamlığını vurgular.

4.2.4. Alt örnekleme saldırıları

4.2.4.1. 4:2:0 alt örnekleme saldırısı

4:2:0 alt örnekleme saldırısında, videodaki renk bilgisi daha düşük bir çözünürlükte alt örneklendirilir, bu da filigranı bozabilmektedir. Hamming mesafesi burada 19235 olarak ortaya çıkar, 8-bit renk nicemleme saldırısının etkisiyle benzerdir.

Bit Hata Oranı (BER) 0,020 olarak artmıştır, bu da saldırıdan sonra daha fazla bit hataları olduğunu gösterir. Bit hatalarının artması, renk bilgi çözünürlüğünü azaltan alt örnekleme tekniğiyle uyumludur ve bu da filigranını bozabilmektedir. Ortalama Kare Hatası (MSE) değeri 21,674'e yükselir, bu da saldırının orijinal ve saldırıya uğramış videoların piksel değerleri arasındaki ortalama kare farkının belirgin bir şekilde arttığını gösterir.

En yüksek Sinyal-Gürültü Oranı (PSNR) 34,771 dB'dir ve bu, orijinal videoya göre video kalitesinin düştüğünü gösterir. Alt örnekleme, videoya gürültü ve bozulma getirerek PSNR değerini azaltır. Korelasyon Katsayısı hala yüksek olup 0,998 olarak kalmıştır, bu da orijinal ve saldırıya uğramış videolar arasında önemli bir benzerlik olduğunu gösterir. Ancak, filigranı kurtarma oranı hala %96,20 gibi yüksektir, bu da olumlu bir işarettir. Saldırı tarafından getirilen bozulmalara rağmen, neredeyse tüm filigranı kurtarılabilmektedir.

Sonuç olarak, 4:2:0 alt örnekleme tarafından getirilen bozulmalara rağmen, filigranlama yöntemi yüksek bir direnç göstermiştir. Bu saldırıya karşı filigranının kurtarma oranı, filigranlamanın etkinliği ve direnci konusunda ikna edici kanıtlar sunmaktadır.

4.2.4.2. 4:2:2 alt örnekleme saldırısı

Alt örnekleme 4:2:2 saldırısı, renk bilgisinin yatay çözünürlüğünün azaltılmasıyla gerçekleşirken, dikey çözünürlüğün tam olarak korunması anlamına gelir. Bu durum filigranının bütünlüğünü etkileyebilir. Sonuçlara göre, Hamming mesafesi 19282 olarak ortaya çıkar.

Bit Hata Oranı (BER) 0,020'e yükselir, bu da saldırı sırasında daha fazla bit hataları tanıtıldığını ve filigranının bütünlüğünü olumsuz etkileyebileceğini gösterir. Ortalama Kare Hatası (MSE) değeri 21,638'e yükselir, bu da saldırının orijinal ve saldırıya uğramış videoların piksel değerleri arasındaki ortalama kare farkının önemli ölçüde arttığını gösterir.

En yüksek Sinyal-Gürültü Oranı (PSNR) 34,778 dB olarak ölçülür ve bu, alt örnekleme saldırısı nedeniyle video kalitesinin azaldığını gösterir. Saldırıya rağmen, Korelasyon Katsayısı hala 0,998 düzeyinde oldukça yüksektir ve orijinal ile saldırıya uğramış videolar arasında yüksek bir benzerlik olduğunu gösterir. İlginç bir şekilde, filigranı kurtarma oranı hala %100'dür, bu da saldırı tarafından getirilen bozulmalara rağmen tüm filigranının başarıyla kurtarılabildiğini gösterir.

Sonuç olarak, Alt örnekleme 4:2:2 saldırısı filigranında bazı bozulmalar getirmiş olsa da bu bozulmalar filigranının kurtarılmasını engelleyecek düzeyde değildir. Bu durum, filigranlamanın teknik gücünü ve video içeriğini koruma yeteneğini vurgular.

4.2.5. Sıkıştırma saldırıları

Sıkıştırma saldırıları, video dosyasının boyutunu azaltmayı amaçlar ve bu da filigranını etkileyebilir.

4.2.5.1. 1000k bit oranlı sıkıştırma saldırısı

Bu saldırı yöntemi, video içeriğini 1000 kilo bit/saniye bit oranında sıkıştırmayı içerir.

En yüksek Sinyal-Gürültü Oranı (PSNR), 35,181 dB'dir. Korelasyon Katsayısı, 0,998 olarak belirlenmiştir ve orijinal ve saldırıya uğramış videolar arasında yüksek bir benzerlik derecesini göstermektedir. Bununla birlikte, filigran kurtarma oranı %26 ile oldukça düşüktür. Bu, daha düşük bit hızıyla sıkıştırmanın filigranın önemli bir bölümünü bozduğunu gösterir.

Sonuç olarak, 1000k Bit Hızı Sıkıştırma Saldırısı çok tatmin edici olmayan iyileşme oranı. Filigranlama yönteminin bu tür saldırılara karşı dirençli olabilmesi için daha fazla geliştirilmesi gerektiği görülmektedir.

4.2.6. Kopyalama saldırısı

Kopyalama saldırısı, filigranlı videonun doğrudan bir kopyasını oluşturmayı içerir. Bu tür bir saldırı, filigranını değiştirmeden başka bir içeriğe kopyalamayı amaçlar.

Sonuçların değerlendirilmesinde: Hamming mesafesi, orijinal filigranından biraz daha yüksek olan 15558'dir, ancak bu küçük fark, filigranın büyük ölçüde korunduğunu

göstermektedir. Bit Hata Oranı (BER), 0,0168'dir. Bu, orijinalden daha yüksek olsa da hala oldukça düşük bir değerdir ve düşük sayıda bit hatası olduğunu göstermektedir.

Ortalama Kare Hatası (MSE), 13,471'dir. Bu, orijinal ve kopyalanmış videolar arasında düşük bir bozulma olduğunu göstermektedir. En yüksek Sinyal-Gürültü Oranı (PSNR), 36,836 dB'dir. Bu yüksek değer, video içeriğinin kalitesinin kopyada iyi bir şekilde korunduğunu göstermektedir. Korelasyon Katsayısı, 0,999 olarak belirlenmiştir ve orijinal ve kopyalanmış videolar arasında çok yüksek bir benzerlik derecesini göstermektedir. Filigranı kurtarma oranı %100'dür. Bu, filigranın kopyalanan videoda mükemmel bir şekilde sonuçlandığını göstermektedir.

Sonuç olarak, filigranlama yöntemi, kopyalama saldırılarına karşı son derece etkilidir, çünkü filigranı tam olarak kurtarılmıştır. Bu, filigranlamanın bütünlüğü ve tanıma yeteneğini doğrudan kopyalama durumunda bile koruyabilen bir filigranlama yöntemi olduğunu göstermektedir. Bu, video içeriğinin izinsiz kopyalanmasına karşı mükemmel bir koruma sağlamaktadır.

4.2.7. Sıkıştırma saldırıları CRF30 ve CRF50

Video sıkıştırmasındaki CRF (Sabit Oran Faktörü) parametresi, dosya boyutu ile video kalitesi arasındaki dengeyi etkiler. CRF30 ve CRF50, daha yüksek sıkıştırma seviyelerine karşılık vermektedir.

4.2.7.1. Sıkıştırma saldırısı CRF30:

CRF değeri 30 kullanılarak gerçekleştirilen bir sıkıştırma saldırısıdır. Bu, filigranının yeterince sağlam olmadığı durumlarda filigranını bozabilir veya kaldırabilir.

Sonuç olarak, Hamming mesafesi 19217'dir ve filigrandaki bazı bitlerin sıkıştırma işlemi sırasında değiştirildiği görülebilir. Bit Hata Oranı (BER) 0,0208'dur. Bu, orijinal videodan daha yüksektir ve sıkıştırma sonrasında bit hatalarında bir artış olduğunu gösterir.

Ortalama Kare Hatası (MSE) 21,770'dir ve orijinal ile sıkıştırılmış video arasında önemli bir bozulma olduğunu temsil eder. En yüksek Sinyal-Gürültü Oranı (PSNR) 34,752 dB'dir. PSNR, orijinal videoya kıyasla azalmıştır, bu da sıkıştırma nedeniyle video kalitesinin bozulduğunu gösterir. Korelasyon Katsayısı 0,997'tür ve orijinal ile sıkıştırılmış videolar arasındaki korelasyonu biraz etkilediğini gösterir. Filigranı kurtarma

oranı %35,66'dır ve CRF 30 sıkıştırma sonrasında sadece orijinal filigranının bir kısmı kurtarılabilir durumdadır.

Sonuç olarak, filigranlama yöntemi CRF 30 sıkıştırma saldırısına karşı bir miktar hassasiyet göstermiştir. Sıkıştırma süreci, filigranının kurtarıla bilirliğini önemli ölçüde etkileyen bozulmalara neden olmuştur. Bu nedenle, bu tür saldırılara karşı filigranlamanın direncini artırmak için daha fazla araştırma ve geliştirmeler önerilmektedir.

4.2.7.2. Sıkıştırma saldırıları CRF50:

Hamming mesafesi 58902'dir ve orijinal videodan önemli ölçüde daha yüksektir. Bu, sıkıştırma süreci sırasında filigranında önemli sayıda bitin değiştirildiğini görmekteyiz. Bit Hata Oranı (BER) 0,063'dir. BER, orijinal videodan önemli ölçüde daha yüksektir ve sıkıştırma sonrasında bit hatalarında büyük bir artış olduğunu gösterir.

Ortalama Kare Hatası (MSE) 65,060'dır. Bu, orijinal ile sıkıştırılmış video arasında büyük bir bozulma olduğunu gösterir. En yüksek Sinyal-Gürültü Oranı (PSNR) 29,997 dB'dir. PSNR, orijinal videoya kıyasla belirgin bir şekilde azalmıştır ve sert sıkıştırma nedeniyle video kalitesinde ciddi bir bozulma olduğunu gösterir.

Korelasyon Katsayısı 0,973'dir ve bu değer orijinal videodan önemli ölçüde daha düşüktür. Bu, sert sıkıştırmanın orijinal ile sıkıştırılmış videolar arasındaki korelasyonu büyük ölçüde etkilediğini gösterir. Filigranı kurtarma oranı yalnızca %6,56'dır ve CRF 50 sıkıştırma sonrasında orijinal filigranının küçük bir kısmı kurtarılabilir durumdadır.

Sonuç olarak, filigranlamanın CRF 50 sıkıştırma saldırısına karşı önemli bir hassasiyeti olduğu görülmektedir. Sert sıkıştırma, filigranının kurtarıla bilirliğini önemli ölçüde etkileyen önemli bozulmalara neden olmuştur. Bu nedenle, bu tür saldırılara karşı filigranlamanın dayanıklılığını sağlamak için önemli geliştirmeler yapılması gerekmektedir.

4.2.8. Kayıpsız sıkıştırma saldırısı ffv1

FFV1 ile gerçekleştirilen Kayıpsız Sıkıştırma Saldırısı, FFV1 kod ekini kullanarak video içeriğinin dosya boyutunu bilgi kaybı olmadan azaltma sürecini ifade etmektedir. Bu yöntem teorik olarak filigranının bütünlüğünü koruması gerektiğinden, hiçbir video verisi kaybolmaz.

Sonuç olarak; Hamming Mesafesi 15,558 ve Bit Hata Oranı (BER) 0,016 olarak belirlenmiştir. Bu değerler nispeten düşüktür ve filigranının bit yapısının iyi korunduğunu gösterir. Ortalama Kare Hatası (MSE) 13,471 ve En yüksek Sinyal-Gürültü Oranı (PSNR) 36,836 olarak raporlanmıştır. Bu metrikler, orijinal ve saldırıya uğramış videolar arasında yüksek bir benzerlik olduğunu gösterir ve bu da bu sıkıştırma yönteminin kayıpsız doğasını yansıtır.

Korelasyon Katsayısı 0,999, hemen hemen maksimum değer olan 1'e çok yakındır. Bu, orijinal ve saldırıya uğramış videolar arasında neredeyse mükemmel bir korelasyon olduğunu göstermektedir. Filigranının geri alım oranı %100'dür, bu en yüksek olası orandır. Bu, kayıpsız sıkıştırma sürecinde filigranının tamamen korunduğunu doğrulamaktadır.

Sonuç olarak, bu çalışmada önerilen filigranlama yöntemi için FFV1 kullanılarak gerçekleştirilen Kayıpsız Sıkıştırma Saldırısı önemli bir tehdit söz konusu değildir. Dosya boyutunun azaltılmasına rağmen, filigranı tamamen korunmuştur ve bu da kayıpsız bir sıkıştırma yönteminden beklenen bir sonuç olmuştur. Bu kayıpsız sıkıştırmaya karşı gösterilen direnç, filigranlama şemasının olumlu bir özelliğidir ve böyle bir sıkıştırmanın rutin olarak uygulandığı gerçek dünya uygulamalarında kullanılabilirliğini göstermektedir.

4.2.9. Kare ortalama saldırısı

Kare ortalama saldırısı, bir videonun her bir karesinin bitişik kareleriyle ortalaması alınarak içeriğin hafifçe bulanıklaştırılması ve gömülü filigranının bozulması potansiyelini taşıyan bir manipülasyon tekniğidir.

Sonuç olarak, Hamming Mesafesi 26,563 ve Bit Hata Oranı (BER) 0,028 olarak ölçülmüştür. Bu değerler, orijinal değerlere kıyasla artmış ve filigranın bit yapısında önemli bir bozulma olduğunu göstermektedir. Ortalama Kare Hatası (MSE) 28,662 ve Piksel Sinyal-Gürültü Oranı (PSNR) 33,557 olarak hesaplanmıştır. Bu değerler, kare ortalamasıyla oluşan bulanıklık etkisi nedeniyle video içeriğinde bir miktar bozulma olduğunu göstermektedir.

Korelasyon Katsayısı 0,980 olarak ölçülmüştür. Bu değer, diğer saldırılara kıyasla yüksek olsa da video yapısının saldırıdan önemli ölçüde etkilendiğini göstermektedir. Filigran kurtarma oranı yalnızca %2,5'tir, bu zamana kadarki en düşük orandır. Bu, filigranın büyük bir kısmının saldırıdan etkilendiğini ve tespit edilemediğini

göstermektedir. Sonuç olarak; kare ortalama saldırısı, bu çalışmada önerilen filigranlama yöntemi için ciddi bir tehdit oluşturmaktadır. Filigranın önemli ölçüde bozulması, filigranlama şemasının kare ortalama tarafından tanımlanan bulanıklığın üstesinden gelmekte zorlandığını göstermektedir. Filigranlama yönteminin daha ileri geliştirilmesinde, böyle temporal değişim tekniklerine karşı ek dayanıklılığın dikkate alınması önerilmektedir.

4.2.10. Kare ekleme saldırısı

Kare ekleme saldırısı, ek karelerin video içeriğine eklenmesiyle gerçekleştirilen bir yöntemdir ve amacı filigranlama dizisini bozmaktır. Hedef, filigranı bozacak kadar düzensizlikleri videoda oluşturmaktır.

Sonuç olarak; Hamming Mesafesi 17,211 ve Bit Hata Oranı (BER) 0,018 olarak ölçülmüştür. Bu değerler, filigranda fark edilebilir düzeyde bozulma olduğunu göstermektedir ve kare ekleme saldırısının filigranı önemli ölçüde etkilediğini göstermektedir.

Ortalama Kare Hatası (MSE) 16,259 ve Piksel Sinyal-Gürültü Oranı (PSNR) 36,019 olarak hesaplanmıştır. Bu değerler, saldırı sonrası video kalitesinin oldukça iyi olduğunu göstermektedir, ancak yüksek MSE değeri bazı bir miktar kalite kaybının olduğunu göstermektedir.

Korelasyon Katsayısı 0,997 olarak ölçülmüştür. Bu oldukça yüksek değer, kare ekleme saldırılarına rağmen video içeriğinin genel yapısının korunduğunu göstermektedir. Filigran kurtarma oranı oldukça düşük, yani %6,48'dir. Bu, saldırı sonrası filigranın önemli bir kısmının algılanamaz hale geldiğini göstermektedir.

Sonuç olarak, kare ekleme saldırısı, test edilen filigranlama sistemi üzerinde oldukça etkili olmuş ve gömülü filigranda önemli düzeyde bozulmaya neden olmuştur. Filigranlama sisteminin gelecek iterasyonları, bu zayıflığı azaltmak için zamansal tekrarlama ve geliştirilmiş tespit mekanizmalarını dikkate alabilir.

4.2.11. Kare hızı değiştirme saldırıları (FPS 15, FPS 20, FPS 25)

Hamming Mesafesi: Hamming Mesafesi değerleri, tüm fps değerlerinde tutarlı görünmektedir; bu, saldırının orijinal ve değiştirilmiş kareler arasındaki farklı konumların sayısını önemli ölçüde etkilemediğini gösterir.

BER (Bit Hata Oranı): BER değerleri tüm fps değerleri için çok düşüktür (yaklaşık 0,017), bu da saldırının orijinal karelerdeki toplam bit sayısına kıyasla yalnızca az sayıda bit hatası ortaya çıkardığını düşündürür. Bu, çerçeve hızı değiştirme saldırısına karşı filigran sisteminin nispeten sağlam bir performansını gösterir.

MSE (Mean Squared Error): MSE değerleri, farklı fps değerleri için nispeten birbirine yakındır ve bu, değiştirilen karelerin kalitesinin kare hızındaki değişiklikten önemli ölçüde etkilenmediğini gösterir. Bu aynı zamanda damgalama algoritmasının kare hızı değişikliklerine karşı dayanıklı olabileceğini düşündürür.

PSNR (Peak Signal-to-Noise Ratio): PSNR değerleri nispeten yüksektir ve bu, değiştirilen çerçevelerin kalitesinin orijinal çerçevelere oldukça yakın olduğunu gösterir. Daha yüksek PSNR değerleri, daha iyi kalite anlamına gelir ve sonuçlar, saldırıdan sonra bile karelerin görsel olarak hala benzer olduğunu gösterir.

Korelasyon Katsayısı: Yüksek korelasyon katsayısı değerleri (0,998 civarında), orijinal ve değiştirilmiş çerçeveler arasında güçlü bir benzerliği gösterir. Bu, kare hızı değiştirme saldırısının getirdiği değişikliklerin minimum olduğunu ve karelerin yüksek oranda ilişkili kaldığını gösterir.

Elde Edilen Filigran: Elde edilen filigranın yüzdesi, kullanılan fps'ye görelidir (%19,9 ila %94,936 aralığında). Bu, filigranın kare hızı değişikliğinden etkilenebileceğini ve filigranın elde edilmesinde değişen başarı ile sonuçlanabileceğini gösterir.

Genel olarak sonuçlar, sistemde kullanılan filigranlama algoritmasının farklı fps değerlerinde "Kare Hızı Değiştirme Saldırısı"na karşı direnç gösterdiğini göstermektedir. Düşük BER ve MSE değerleri, yüksek PSNR ve korelasyon katsayısı değerleri ile birlikte, değiştirilen çerçevelerin orijinal çerçevelere yüksek derecede benzerlik gösterdiğini gösterir. Bununla birlikte, filigranı elde etmede değişen başarı oranları, filigran çıkarma işleminin çerçeve hızı değişikliklerinden etkilenebileceği anlamına gelir. Farklı çerçeve hızı koşullarında filigran çıkarma performansını artırmak için daha fazla analiz ve iyileştirme gerekebilir.

4.2.12. Whatsapp sıkıştırma saldırısı

WhatsApp sıkıştırması, bir video WhatsApp mesajlaşma servisi aracılığıyla gönderildiğinde uygulanan bir sıkıştırma biçimidir. Dosya boyutunu azaltarak daha kolay transfer sağlamaya odaklandığından, bu tür bir sıkıştırma video kalitesi üzerinde ve dolayısıyla gömülü filigran üzerinde önemli bir etkiye sahiptir.

Hamming Mesafesi 15,525 ve Bit Hata Oranı (BER) 0,016, filigran üzerinde orta düzeyde bir bozulma olduğunu gösterir ve WhatsApp sıkıştırmasının filigranın bütünlüğünün etkilendiğini gösterir. Ortalama Kare Hatası (MSE) 13,474 ve Piksel Sinyal-Gürültü Oranı (PSNR) 36,835, sıkıştırma sonrasında video kalitesinin görece yüksek kaldığını gösterir. Bununla birlikte, sıkıştırmadan dolayı video kalitesinde bir miktar bozulmalar meydana gelmektedir.

Korelasyon Katsayısı 0,999, sıkıştırma sonucunda genel olarak video içeriğinin yapısının büyük ölçüde korunduğunu gösterir. Bu durum, WhatsApp'ın sıkıştırma algoritmasının görsel kaliteyi korumaya çalışırken boyutu azaltmaya odaklanmasından kaynaklanabilmektedir. Ancak, filigran kurtarma oranı yalnızca %53,93 olduğundan, filigranın önemli bir kısmının sıkıştırma sürecinde bozulduğu veya kaybolduğu anlaşılmıştır.

4.2.13. Mekansal filtre saldırısı: Gaussian bulanıklık

Mekansal filtre saldırısı, bir filtre uygulanarak video içindeki piksellerin değiştirildiği bir video manipülasyonu türüdür. Gaussian bulanıklık, Gaussian fonksiyonuna dayanan bir mekansal filtre türüdür ve video içindeki pikselleri bulanıklaştırır. Bu durum, videodaki keskinlik ve detayları azaltabilir ve gömülü filigranı belirsizleştirebilmektedir. Hamming Mesafesi 70,308 ve Bit Hata Oranı (BER) 0,0762 oldukça yüksek değerlerdir, bu da Gaussian bulanıklık saldırısının gömülü filigranı önemli ölçüde bozduğunu gösterir.

Ortalama Kare Hatası (MSE) 68,132 ve Piksel Sinyal-Gürültü Oranı (PSNR) 29,797, videonun bulanık etkisi nedeniyle önemli bir kalite düşüşüne uğradığını gösterir. Gaussian bulanıklığın amacı, bir videonun keskinliğini ve netliğini azaltmaktır, bu nedenle kalitede bozulma beklenmektedir. Korelasyon Katsayısı 0,964, video içeriğinin genel yapısının bir dereceye kadar korunduğunu gösterir, ancak Gaussian bulanıklık etkisi gömülü filigranın tespiti üzerinde önemli değişikliklere neden olmaktadır.

Filigran kurtarma oranı %5,98 olarak düşüktür, bu da filigranın büyük bir kısmının Gaussian bulanıklık nedeniyle kaybolduğunu veya bozulduğunu gösterir.

Sonuç olarak, Gaussian bulanıklık saldırısı, filigranlama sistemi için önemli bir zorluk oluşturmaktadır. Filigranın Gaussian bulanıklık gibi mekansal filtre saldırılarına karşı sağlamlığı korunabilirlik ve tespit edilebilirlik açısından yeniden gözden

geçirilmelidir. Bunun için daha dirençli filigranlama tekniklerinin kullanılması veya mekansal filtrelerin etkilerini dengelemek için ek yöntemlerin kullanılması düşünülebilir.

4.2.14. Gürültü eklenmesi saldırısı: Gaussian gürültü

Gürültü eklenmesi, rastgele gürültünün video piksellerine eklenerek yapılan bir video manipülasyon saldırısıdır. Bu gürültü, gömülü filigranı belirsizleştirebilen bir etkiye sahiptir. Özellikle Gaussian gürültüsü, normal dağılıma uyan ve istatistiksel gürültü için yaygın olarak kullanılan bir modeldir.

Hamming Mesafesi 30,723 ve Bit Hata Oranı (BER) 0,033, Gaussian gürültü saldırısının gömülü filigranın bütünlüğünü önemli ölçüde etkilediğini gösterir. Bu değerler, gürültü eklemenin filigranın bitlerine birçok değişiklik getirdiğini göstererek filigrana büyük ölçüde zarar verdiğini gösterir.

Ortalama Kare Hatası (MSE) 44,340 ve En yüksek Sinyal-Gürültü Oranı (PSNR) 31,662, gürültü eklenmesi nedeniyle video kalitesinde belirgin bir düşüş olduğunu gösterir. Düşük PSNR değeri, videoda daha fazla gürültü olduğunu ve netliği etkilediğini göstermektedir.

Korelasyon Katsayısı 0,993, oldukça yüksek olmasına rağmen Gaussian gürültüsünün video içeriğine önemli değişiklikler getirdiğini ve gömülü filigranın tespit edilebilirliğini etkilemektedir. Filigran kurtarma oranı %7,8125 olarak oldukça düşüktür, bu da filigranın büyük bir kısmının Gaussian gürültü nedeniyle kaybolduğunu veya bozulduğunu gösterir.

Sonuç olarak, Gaussian gürültü saldırısı, filigranlama sistemi için önemli bir zorluk oluşturmaktadır. Gürültü eklenmesi saldırılarına karşı filigranlama sisteminin sağlamlığının artırılması düşünülmelidir. Olası çözümler, daha dirençli filigranlama tekniklerinin uygulanması veya Gaussian gürültüsünün etkilerini dengelemek için gürültü azaltma yöntemlerinin kullanılması gerekebilir.

4.2.15. Frekans alanı filtreleme saldırısı: yüksek geçiren filtre

Frekans alanı filtreleme, bir görüntünün veya videonun frekans bileşenlerini değiştirir. Yüksek geçiren filtre durumunda, düşük frekans bileşenleri bastırılırken, yüksek frekans bileşenlerine vurgu yapılır. Bu, özellikle filigranın düşük frekans alanına gömülü olduğu durumlarda filigranı önemli ölçüde etkileyebilir.

Hamming Mesafesi 25,136 ve Bit Hata Oranı (BER) 0,027 ile yüksek geçiren filtre, filigran üzerinde belirgin bir etkiye sahiptir. Bu, filigran bitlerinde önemli bir değişiklik olduğunu yansıtır ve yüksek frekansların vurgusu ile filigran üzerindeki etkisini gösterir.

Ortalama Kare Hatası (MSE) 26,918 ve Piksel Sinyal-Gürültü Oranı (PSNR) 33,830, yüksek geçiren filtrenin video içeriğini önemli ölçüde değiştirdiğini gösterir. Görece yüksek MSE, orijinal ve saldırıya uğramış video içeriği arasında önemli bir fark olduğunu gösterir. Ancak, PSNR değeri yüksek geçiren filtre uygulamasına rağmen video kalitesinin makul olduğunu ifade etmektedir.

0,996 Korelasyon Katsayısı, orijinal ve saldırıya uğramış filigran arasında güçlü bir pozitif korelasyon olduğunu gösterir. Frekans değişikliklerine rağmen, orijinal ve saldırıya uğramış filigran bitleri arasında belirgin bir benzerlik vardır, bu da filigranın tespitinde yardımcı olmaktadır. %7,142 filigran kurtarma oranı oldukça düşüktür. Bu, filigranın çoğunluğunun kaybolduğunu veya tespit edilemez olduğunu gösterir ve yüksek geçiren filtrenin neden olduğu önemli frekans değişikliği ile uyumludur.

Sonuç olarak, yüksek geçiren filtre saldırısı, filigranlama yöntemi için önemli bir zorluk oluşturmaktadır. Yüksek geçiren filtreleme gibi frekans alanı saldırılarına karşı filigranlama yönteminin dayanıklılığı artırılmalıdır. Bu, filigranın orta frekans bölgesine gömülmesiyle sağlanabilir, bu da frekans alanı saldırılara karşı dayanıklılık ve algısal görünmezlik arasında bir denge sunabilir.

4.2.16. Kayıpsız sıkıştırma saldırısı Huffuyv

Huffuyv kayıpsız sıkıştırma saldırısı etkileyici sonuçlar vermiştir. Gömülü filigranın %100 oranında mükemmel bir şekilde tespit edildiğini gösteren bir filigran çıkarma doğruluğu elde edilmiştir. Bit hızı hafifçe yükselmiş olup 21,096 olarak gerçekleşmiştir, ancak PSNR değeri 34,888 ile görüntü kalitesinin yüksek olduğunu göstermiştir. Korelasyon katsayısı neredeyse 1'e yakın (0,998), bu da orijinal filigranla çok yüksek bir benzerlik olduğunu göstermektedir.

4.2.17. Zamansal saldırılar: kare ekleme (30)

Frame ekleme zamansal saldırısında saniyede 30 ekstra kare eklenmiştir. Bu, filigran çıkarma doğruluğunda hafif bir azalmaya (94,936%) yol açmış, bu da çerçeveye

manipülasyonuna karşı bir dereceye kadar direnç olduğunu göstermektedir. PSNR ve MSE değerleri sırasıyla 36,552 ve 14,382 olarak kaydedilmiştir. Yüksek bir korelasyon katsayısı olan 0,998, orijinal ve saldırıya uğramış filigran arasında güçlü bir benzerlik olduğunu göstermektedir.

4.2.18. Sıkıştırma saldırısı libx265 CRF28

Libx265 sıkıştırma saldırısı sırasında sabit bir hız faktörü (CRF) olan 28 kullanıldığında, filigran çıkarma doğruluğu önemli ölçüde düşerek %7,407 oldu. PSNR hala görece yüksek bir seviyede olan 35,513 olarak kaydedildi, bu da iyi bir görüntü kalitesini göstermektedir. MSE ise 18,268 idi. Korelasyon katsayısı 0,998'ya düşmüş olup, bu da saldırıdan sonra filigranın kalitesinin biraz düştüğünü göstermektedir.

4.2.19. Sıkıştırma saldırısı libx265 CRF28 yuv420p

Libx265 codec kullanılarak yapılan bu saldırıda, CRF değeri 28 ve YUV420p renk uzayı kullanılmış ve filigran çıkarma doğruluğu %5,172 olmuştur. PSNR ve MSE değerleri sırasıyla 34,038 ve 25,658 idi. Daha düşük çıkarma doğruluğuna rağmen, 0,998 olan korelasyon katsayısı, filigranlı kare ile orijinal arasında hala yüksek bir benzerlik olduğunu göstermektedir.

4.2.20. Sıkıştırma saldırısı libx265

Libx265 codec kullanılan bu genel sıkıştırma saldırısı sonucunda filigran çıkarma doğruluğu %7,407 olmuş, özel CRF28 saldırısıyla benzer bir sonuç meydana gelmiştir. PSNR değeri 35,513 olarak sabit kaldı ve MSE 18,268 idi. Korelasyon katsayısı ise biraz daha düşük olarak 0,998 idi.

4.2.21. Frekans alanı filtreleme saldırısı: düşük geçiren filtre

Düşük geçiren filtre saldırısında filigran çıkarma doğruluğu %11,904 olarak gerçekleşti. PSNR ve MSE değerleri sırasıyla 34,335 ve 23,963 idi. 0,998 olan korelasyon katsayısı, orijinal ve saldırıya uğramış filigran arasında yüksek bir benzerlik olduğunu

göstermektedir, ancak daha düşük çıkarma doğruluğu saldırının belirgin bir etkisi olduğunu savunmaktadır.

4.2.22. Frekans alanı filtreleme saldırısı: medyan filtresi

Medyan filtresi saldırısı, filigran çıkarma doğruluğunu %18,681'e düşürdü, bu da filigran tespitinde önemli bir bozulmaya işaret etmektedir. PSNR ve MSE sırasıyla 32,349 ve 37,856 idi, bu da video kalitesinde önemli bir değişiklik olduğunu göstermektedir. Korelasyon katsayısı ise 0,989'e göre nispeten düşüktür, bu da orijinal filigrandan sapma olduğunu göstermektedir.

4.2.23. Örnek en-boy oranı saldırısı: 2*SAR

2*SAR saldırısı sırasında filigran çıkarma doğruluğu oldukça yüksek olarak %63,291 oldu. PSNR ve MSE değerleri sırasıyla 36,613 ve 14,182 idi. 0,998 olan korelasyon katsayısı, orijinal filigranla güçlü bir benzerlik olduğunu göstermektedir.

4.2.24. Ters oynatma saldırısı

Ters oynatma saldırısında filigran çıkarma doğruluğu %31,868 olarak gerçekleşti, bu da filigranın manipülasyondan orta düzeyde etkilendiğini göstermektedir. PSNR ve MSE değerleri sırasıyla 35,327 ve 19,067 idi. 0,998 olan korelasyon katsayısı, orta düzeyde çıkarma doğruluğu etkisine rağmen, orijinal ve saldırıya uğramış filigran arasında güçlü bir benzerlik olduğunu göstermektedir.

4.2.25. Wiener filtre saldırısı

Wiener filtre saldırısı filigran çıkarma doğruluğu üzerinde önemli bir etkisi olmamış ve yüksek bir değer olan %100'ü korumuştur. Bu da Filigranın bu özel saldırı türüne karşı yüksek bir dirence sahip olduğunu göstermektedir. 0,998 olan yüksek korelasyon katsayısı da bunu desteklemekte olup, orijinal ve saldırıya uğramış filigran arasında güçlü bir benzerlik olduğunu göstermektedir.

Bu bulgular, görünmez NFT filigranlama yöntemimizin, yapılan saldırı türüne ve yoğunluğuna bağlı olarak çeşitli düzeylerde dayanıklı olduğunu göstermektedir.

Gelecekteki arařtırmalar yöntemi daha da geliřtirebilir ve bu saldırılara karřı önlemler alınarak görünmez filigranlama tekniklerinin video içeriklerindeki dayanıklılıđını artırabilir.

Sonuç olarak, önerilen Görünmez NFT Filigranlama algoritması, dijital içerik sahiplerinin haklarını koruma konusunda oldukça iyi potansiyel göstermektedir. Bununla birlikte, daha fazla arařtırma ve geliřtirme yapılması gerekmektedir, böylece daha geniş bir saldırı yelpazesine karřı dayanıklılıđı artırılabilir.



5. SONUÇLAR VE ÖNERİLER

Görünmez filigran kullanımının video içerisinde oluşturulan Takas olmayan jetonlar (NFT'ler) için incelenmesi, önemli bilgiler ve sonuçlar ortaya koymuştur. Amacımız, bu konseptin geçerliliğini sağlamak ve çeşitli saldırılara karşı dayanıklılığını değerlendirmektir. Bulgularımız, bu alanda keşfedilecek önemli potansiyele sahip olduğunu doğrulamaktadır ve büyüyen dijital ekonomide önemli bir yere sahiptir.

Araştırmamız, NFT filigranlamasının video içerisine etkili bir şekilde yerleştirilebileceğini ve çeşitli saldırılara karşı büyük ölçüde dayanıklı olduğunu göstermektedir. Birçok saldırı, yüksek filigran kaldırma hassasiyeti ve güçlü korelasyon katsayıları sağladı. Orijinal ve filigranlı kareler arasında yüksek bir benzerlik olduğunu göstermiştir.

Ancak, bazı saldırılar filigranı önemli ölçüde bozmuştur. Bu saldırıların daha fazla araştırılması gerekiyor ve bunlara yönelik çözümler potansiyel olarak daha sonraki araştırmalarda belirlenebilir.

Bu bulgular doğrultusunda aşağıdaki öneriler verilmiştir.

Geometrik dayanıklılığın daha fazla araştırılması: Geometrik saldırılar filigran için en büyük zorlukları oluşturduğundan, gelecek araştırmalar NFT filigranlamasının bu tür manipülasyonlara karşı dayanıklılığını artırmaya odaklanmalıdır. Geometrik dönüşümler ve değişmez anlar gibi, uzay alanında filigranlama için gelişmiş tekniklerin keşfedilmesi önemlidir.

Yükselen video formatları ve teknolojilerine uyum sağlanması: Video teknolojisi geliştikçe, saldırı yöntemleri de değişecektir. Gelecek araştırmaların, sanal gerçeklik ve 360 derece videolar gibi yükselen video formatları ve teknolojilerini dikkate alması ve filigranlama tekniklerini buna göre adapte etmesi önemlidir.

Blockchain tabanlı doğrulama sistemlerinin keşfi: NFT'lerin doğası gereği blockchain teknolojisiyle ilişkilendirilmesi, filigranlı videolar için blockchain tabanlı doğrulama sistemlerinin keşfedilmesinde büyük bir potansiyel vardır. Bu, video içeriğinin otantikliğini ve sahipliğini sağlamaya yardımcı olabilir ve NFT filigranlamasının faydalarını daha da artırabilir.

Sonuç olarak, video içeriğindeki görünmez NFT filigranlama, dijital içerikte güçlü bir alanı temsil eder ve büyük bir potansiyele sahiptir. Zorluklar olmasına rağmen, sürekli araştırma ve geliştirme ile bu zorlukların etkili bir şekilde çözülebileceğine

inıyoruz. Daha fazla araştırma ile daha güvenli ve doğrulanabilir bir dijital içerik alanı d şenebilir.



KAYNAKLAR

- Cornelius K., 2021 “Betraying Blockchain: Accountability, Transparency and Document Standards for Non-Fungible Tokens (NFTs),” *Information*, vol. 12, no. 9.
- Khati, P., Shrestha, A.K., Vassileva, J., 2022, Non-Fungible Tokens Applications: A Systematic Mapping Review of Academic Research, in: *2022 IEEE 13th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pp. 0323–0330. <https://doi.org/10.1109/IEMCON56893.2022.9946500>
- Eisenach, J.A.; Eldering, C.A.; Sylla, M.L., 1999, Is there a Moore’s law for bandwidth? *IEEE Commun. Magazine*, vol. 37, no. 10, pp. 117–121.
- Wang, C., Yu, X., Zhou, X., 2018. A Survey on Robust Video Watermarking Algorithms for Copyright Protection. *Applied Sciences* 8, no. 10: 1891.. <https://doi.org/10.3390/app8101891>
- Delp, E.J., Podilchuk, C.I., Wolfgang, R.B., 1999, Perceptual watermarks for digital images and video. *Proceedings of the IEEE*, , vol. 87, no. 7, pp. 1108-1126.
- Jung, K.H., 2016, A survey of reversible data hiding methods in dual images *IETE Technical Review*, 33, 441–452.
- Jha, R.K., Verma, V.S., 2015, An overview of robust digital image watermarking. *IETE Technical Review*, 32, 479–496.
- Bawany, N.Z.; Imran, J.; Rehman, W.; Zainab, H.E., 2021, “NFTS: Applications and challenges” *22nd International Arab Conference on Information Technology (ACIT)*, Muscat, Oman, 2021, pp. 1-7.
- Chalmers, D.; Fisch, C.; Matthews, R.; Quinn, W.; Recker, J., 2022, “Beyond the bubble: Will NFTs and digital proof of ownership empower creative industry entrepreneurs?” *Journal of Business Venturing Insights*, vol. 17, doi: 10.1016/j.jbvi. 2022.e00309.
- Guhathakurta, D.; Gupta, M.; Kapoor, A.; Kumaraguru, P.; Mathur, M.; Yadav, R., 2022, “TweetBoost: Influence of Social Media on NFT Valuation,” [Online], arXiv. Web adresi: https://www.engineeringvillage.com/share/document.url?mid=cpx_M17190e9517f8af96247M6f821017816328&database=cpx [Ziyaret Tarihi: 1 Ağustos 2023].
- Bhardwaj, A.; Goel, S.; Jindal, S.; Mahant, I.; Puri, T.; Singh, S.; Sood, D., 2016, Performance analysis of LSB based watermarking for optimization of PSNR and MSE. *International Journal of Security and Its Applications*, 10, 345–350.
- Cox, I.J.; Kilian, J.; Leighton, F.T.; Shamoon, T., 1997, Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673-1687.
- Kaur, H.; Kaur, E.V., 2016, Invisible video multiple watermarking using optimized techniques. *In Proceedings of the Online International Conference on Green Engineering and Technologies*, Coimbatore, India, pp. 1-9.

- Bayoudh, I.; Jabra, S.B.; Zagrouba, E., 2017, Online multi-sprites based video watermarking robust to collusion and transcoding attacks for emerging applications. *Multimedia Tools Appl.* 77, 14361–14379.
- Hamza, A.B.; Masoumi, M.; Rezaei, M., 2015, A blind spatio-temporal data hiding for video ownership verification in frequency domain. *AEU-Int. J. Electron. Commun.*, 69, 1868–1879.
- Kanocz, T.; Levicky, D.; Tokar, T., 2009, Digital watermarking of uncompressed video in spatial domain. *In Proceedings of the 19th International Conference Radioelektronika*, Bratislava, Slovakia, pp. 319-322,.
- Preda, R.O.; Vizireanu, N., 2011, New robust watermarking scheme for video copyright protection in the spatial domain. *UPB Scientific Bulletin, Series C: Electrical Engineering*, 73(1), 93–104.
- Chiplunkar, N.N.; Sarojadevi, H.; Venugopala, P.S.; Bhat, V., 2014, Video watermarking by adjusting the pixel values and using scene change detection. *In Proceedings of the 5th International Conference on Signal and Image Processing*, Bangalore, India, pp. 259-264.
- Bahrami, Z.; Tab, F.A., 2018, A new robust video watermarking algorithm based on SURF features and block classification. *Multimedia Tools Appl.* 77, 327–345.
- Li, X.; Wang, X.; Wang, X.J.; Yang, W.M., 2016, A robust video watermarking scheme to scalable recompression and transcoding. *In 6th Proceedings of the International Conference on Electronics Information and Emergency Communication*, Beijing, China, pp. 257-260.
- Li, J.F.; Sui, A.N., 2012, A digital video watermarking algorithm based on DCT domain. *In Proceedings of the 5th International Joint Conference on Computational Sciences and Optimization*, Harbin, China, pp. 557-560.
- Li, N.; Liu, G.Q.; Zhao, Y.L.; Zheng, X.S, 2010, A robust digital video watermark algorithm based on DCT domain. *In Proceedings of the International Conference on Computer Application and System Modeling*, Taiyuan, China, pp. V2-202-V2-205.
- Cheng, M.Z.; Lei, M.; Wu, C.H.; Xi, M.C.; Yuan, K.G., 2013, Recoverable video watermark in DCT domain. *Journal of Computers*, 8(2), 533–538.
- Duan, D.N.; Nguyen, T.T., 2015, A robust blind video watermarking in DCT domain using even-odd quantization technique. *In Proceedings of the International Conference on Advanced Technologies for Communications*, Ho Chi Minh City, Vietnam, pp. 439-444.
- Hiep, P.T.; Tam, T.M.; Tanaka, K.; Thanh, T.M., 2014, Robust semi-blind video watermarking based on frame-patch matching. *AEU-Int. J. Electron. Commun.*, 68, 1007–1015.

- Chen, B.; Wornell, G.W. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. *IEEE Trans. Inf. Theory* 2001, 47, 1423–1443.
- Hsu, W.H.; Huang, H.Y.; Yang, C.H., 2008 An adaptive video watermarking technique based on DCT domain. *In Proceedings of the 8th International Conference on Computer and Information Technology*, Sydney, Australia, pp. 589-594.
- Huang, H.Y.; Hsu, W.H.; Yang, C.H., 2010, A video watermarking technique based on pseudo-3D DCT and quantization index modulation. *IEEE Trans. Inf. Forensics Secur.*, 5, 625–637.
- Campisi, P.; Neri, A., 2007 3D-DCT video watermarking using quantization-based methods. *In Proceedings of the 15th European Signal Processing Conference*, Poznan, Poland, pp. 2544-2548.
- Cedillo-Hernandez, A.; Cedillo-Hernandez, M.; Miyatake, M.N.; Meana, H.P., 2018, A spatiotemporal saliency-modulated JND profile applied to video watermarking. *J. Vis. Commun. Image Represent.* 52, 106–117.
- Abdulfetah, A.A.; Sun, X.; Yang, H., 2010, Robust adaptive video watermarking scheme using visual models in DWT domain. *Inf. Technol. J.*, 9, 1409–1414.
- Amar, C.B.; Charfeddine, M.; El'Arbi, M.; Koubaa, M., 2011, A dynamic video watermarking algorithm in fast motion areas in the wavelet domain. *Multimedia Tools Appl.*, 55, 579–600.
- Singh, K.M., 2018, A robust rotation resilient video watermarking scheme based on the SIFT. *Multimedia Tools Appl.*, 77, 16419–16444.
- Chen, S.Q.; Gao, Q.; Li, Z., 2017, A video dual watermarking algorithm against geometric attack based on integer wavelet and SIFT. *In Proceedings of the International Conference on Cryptography, Security and Privacy*, Wuhan, China, Pages 33–37.
- Preda, R.O.; Vizireanu, D.N., 2010, A robust digital watermarking scheme for video copyright protection in the wavelet domain. *Measurement*, 43(10), 1720–1726.
- Preda, R.O.; Vizireanu, D.N., 2011, Robust wavelet-based video watermarking scheme for copyright protection using the human visual system. *J. Electron. Imaging*, 20, 146–152.
- Chandra, M.; Gupta, G.; Gupta, V.K., 2018, An efficient video watermarking based security model. *Microsyst. Technol.*, 24, 2539–2548.
- Amiri, S.; Masoumi, M., 2013, A blind scene-based watermarking for video copyright protection. *AEU-Int. J. Electron. Commun.*, 67, 528–535.
- Bhardwaj, A.; Jha, R.K.; Verma, V.S., 2018, Robust video watermarking using significant frame selection based on coefficient difference of lifting wavelet transform. *Multimedia Tools Appl.*, 77, 19659–19678.

- Jabra, S.B.; Kerbiche, A.; Zagrouba, E.; Charvillat, V., 2017, Robust video watermarking approach based on crowdsourcing and hybrid insertion. *In Proceedings of the International Conference on Digital Image Computing: Techniques and Applications*, Sydney, Australia, pp. 1-8.
- Boukabou, A.; Himeur, Y., 2018, A robust and secure key-frames based video watermarking system using chaotic encryption. *Multimedia Tools Appl.*, 77, 8603–8627.
- Adul, V.; Mwangi, E. A robust video watermarking approach based on a hybrid SVD/DWT technique. *In Proceedings of the IEEE AFRICON: Science, Technology and Innovation for Africa*, Cape Town, South Africa, pp. 309-313.
- Garg, P.; Panda, J., 2016 An efficient video watermarking approach using scene change detection. *In Proceedings of the India International Conference on Information Processing*, Delhi, India, pp. 1-5.
- Ramakrishnan, S. and Sathya, S.P.A., 2018, Fibonacci based key frame selection and scrambling for video watermarking in DWT-SVD domain. *Wirel. Pers. Commun.*, 102, 2011–2031.
- Agilandeewari, L.; Ganesan, K., 2016, A robust color video watermarking scheme based on hybrid embedding techniques. *Multimedia Tools Appl.*, 75, 8745–8780.
- Dhinakaran, S.; Ponnisathya, S.; Ramakrishnan, S.; Sabari, A.P.; Dhamodharan, P., 2017, Chaotic map based video watermarking using DWT and SVD. *In Proceedings of the International Conference on Inventive Communication and Computational Technologies*, Coimbatore, India, pp. 45-49.
- Chokkalingam, A.; Shanmugam, M., 2018, Performance analysis of 2 level DWT-SVD based non blind and blind video watermarking using range conversion method. *Microsyst. Technol.*, 24, pp.4757-4765.
- Charvillat, V.; Jabra, S.B.; Kerbiche, A.; Zagrouba, E., 2018, A robust video watermarking based on feature regions and crowdsourcing. *Multimedia Tools Appl.*, 77, 26769–26791.
- Bora, P.K.; Gaj, S.; Rathore, A.K.; Sur, A., 2017, A robust watermarking scheme against frame blending and projection attacks. *Multimedia Tools Appl.*, 76, 20755–20779.
- Agarwal, P.; Girdhar, M.; Gupta, S.; Joshi, A.M.; Sarker, R., 2016, Combined DWT-DCT-based video watermarking algorithm using Arnold transform technique. *In Proceedings of the International Conference on Data Engineering and Communication Technology*, Lavasa City, India, pp. 455-463.
- Jiang, D.Y.; Kim, J.W.; Li, D., 2015, A spread spectrum zero video watermarking scheme based on dual transform domains and log-polar transformation. *Int. J. Multimedia Ubiquitous Eng.*, 10(4), 367–378.
- Chuen, D.L.K., 2015, *Handbook of Digital Currency*, 1st ed. Elsevier.

- Buterin, V., 2014, A next-generation smart contract and decentralized application platform, white paper, 3(37), 2-1..
- Chen, X.; Dai, H.; Wang, H.; Xie, S.; Zheng, Z., 2017. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, in: *2017 IEEE International Congress on Big Data (BigData Congress)*, pp. 557–564. <https://doi.org/10.1109/BigDataCongress.2017.85>
- Johnson, D.; Menezes, A.; Vanstone, S., 2001 , “The elliptic curve digital signature algorithm (ecdsa),” *International Journal of Information Security*, vol. 1, no. 1, pp. 36–63.
- Nakamoto, S., 2008, “Bitcoin: A peer-to-peer electronic cash system”, [Online], Web Adresi: <https://bitcoin.org/bitcoin.pdf>
- Buterin, V., 2015, “On public and private blockchains”, [Online], Web Adresi: <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>
- Lamport, L.; Pease, M.; Shostak, R., 1982, “The byzantine generals problem,” *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 4, no. 3, pp. 382–401, 1982.
- King, S., 2013, “Primecoin: Cryptocurrency with prime number proof-of-work”, 1(6).
- Vasin, P., 2014, “Blackcoins proof-of-stake protocol v2”, [Online]. Web Adresi: <https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf>, 71.
- King, S. and Nadal, S., 2012, “Ppcoin: Peer-to-peer crypto-currency with proof-of-stake” Kendinden Yayınlanmış Kağıt, vol. 19(1).
- Castro, M. and Liskov, B., 1999, Practical byzantine fault tolerance. In *OsDI*, Vol. 99, No. 1999, pp. 173-186).
- Mazieres, D., 2015. The stellar consensus protocol: A federated model for internet-level consensus. Stellar Development Foundation, 32, pp. 1-45.
- Britto, A.; Schwartz, D.; Youngs, N., “The ripple protocol consensus algorithm,” *Ripple Labs Inc White Paper*, vol. 5(8), p. 151.
- Kwon, J., 2014. Tendermint: Consensus without mining. Draft v. 0.6, fall, 1(11), pp.1-11.
- Eyal, I. and Sirer, E.G., 2018. *Majority is not enough: Bitcoin mining is vulnerable. Communications of the ACM*, 61(7), pp. 95-102.
- Decker, C., Seidel, J. and Wattenhofer, R., 2016, January. Bitcoin meets strong consistency. In *Proceedings of the 17th International Conference on Distributed Computing and Networking*, pp. 1-10.
- Kraft, D., 2016. Difficulty control for blockchain-based consensus systems. *Peer-to-peer Networking and Applications*, 9, pp.397-413.

- Sompolinsky, Y. and Zohar, A., 2013. Accelerating bitcoin's transaction processing. fast money grows on trees, not chains. *Cryptology ePrint Archive*.
- Chepurnoy, A., Larangeira, M. and Ojiganov, A., 2016. A prunable blockchain consensus protocol based on non-interactive proofs of past states retrievability. arXiv preprint arXiv:1603.07926.
- Bruce, J.D., 2014. The mini-blockchain scheme. White paper, 1, pp.1-10.
- van den Hooff, J., Kaashoek, M.F. and Zeldovich, N., 2014. Versum: Verifiable computations over large public logs. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1304-1316).
- Eyal, I., Gencer, A.E., Sirer, E.G. and Van Renesse, R., 2016. {Bitcoin-NG}: A scalable blockchain protocol. In *13th USENIX symposium on networked systems design and implementation (NSDI 16)* (pp. 45-59).
- Jordan, G.; Levchenko, K.; McCoy, D.; Meiklejohn, S.; Pomarole, M.; Savage, S.; Voelker, G. M., 2013, "A fistful of bitcoins: Characterizing payments among men with no names," in *Proceedings of the 2013 Conference on Internet Measurement Conference (IMC'13)*, New York, NY, USA, pp. 127-140.
- Barcelo, J., 2014. User privacy in the public bitcoin blockchain. Web adresi: <http://www.dtic.upf.edu/jbarcelo/papers/20140704>.
- Biryukov, A., Khovratovich, D. and Pustogarov, I., 2014, November. Deanonimisation of clients in bitcoin p2p network. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security* (pp. 15-29).
- Möser M., 2013, "Anonymity of bitcoin transactions: An analysis of mixing services" in *Proceedings of Münster Bitcoin Conference*, Münster, Germany, pp. 17–18.
- Bonneau, J.; Clark, J.; Felten, E. W.; Kroll, J. A.; Miller, A.; Narayanan, A., 2014, "Mixcoin: Anonymity for bitcoin with accountable mixes," in *Proceedings of International Conference on Financial Cryptography and Data Security*, Berlin, Heidelberg, pp. 486–504.
- Kate, A.; Moreno-Sanchez, P.; Ruffing, T., 2014, "Coinshuffle: Practical decentralized coin mixing for bitcoin," in *Proceedings of European Symposium on Research in Computer Security*, Cham, pp. 345-364.
- Garman, C.; Green, M.; Miers, I.; Rubin, A. D., 2013, "Zerocoin: Anonymous distributed e-cash from bitcoin," in *Proceedings of IEEE Symposium Security and Privacy (SP)*, Berkeley, CA, USA, pp. 397–411.
- Chiesa, A.; Garman, C.; Green, M.; Miers, I.; Sasson, E. B.; Tromer, E.; Virza, M., 2014, "Zerocash: Decentralized anonymous payments from bitcoin," in *Proceedings of 2014 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA, pp. 459–474.

- Kumar, S.; Miller, A.; Nayak, K.; Shi, E., 2016, “Stubborn mining: Generalizing selfish mining and combining with an eclipse attack,” in *Proceedings of 2016 IEEE European Symposium on Security and Privacy (EuroS&P)*, Saarbrücken, Germany, pp. 305–320.
- Sapirshtein, A., Sompolinsky, Y., Zohar, A., 2015, “Optimal selfish mining strategies in bitcoin,” arXiv preprint arXiv:1507.06183.
- Heilman, E., 2014, One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner. In *Financial Cryptography and Data Security: FC 2014 Workshops, BITCOIN and WAHC 2014*, Barbados, March 7, Gözden Geçirilmiş Seçilmiş Bildiriler 18 (pp. 161-162).
- Potop-Butucaru, M.; Solat, S., 2016, “ZeroBlock: Timestamp-Free Prevention of Block-Withholding Attack in Bitcoin,” *Sorbonne Universites, UPMC University of Paris 6*, [Online], Web Adresi: <https://hal.archives-ouvertes.fr/hal-01310088>
- Fairfield, J.A., 2022, Tokenized: The law of non-fungible tokens and unique digital property. *Ind. LJ*, 97, p. 1261.
- Entriiken, W., Evans, J., Sachs, N., Shirley, D., 2018, Eip-721: Erc-721 non-fungible token standard. [online], Web Adresi: <https://eips.ethereum.org/EIPS/eip-721> [Ziyaret Tarihi: 1 Ağustos 2023].
- Bhirud, S.; Darisi, M.; Shirole, M., 2020: Cryptocurrency token: An overview. *IC-BCT 2019: Proceedings of the International Conference on Blockchain Technology*, pp. 133–140.
- Colavizza, G.; Franceschet, M.; Smith, T., ve ark., 2020, Crypto art: A decentralized view. *Leonardo*, 54(4), pp.402-405.
- Regner, F.; Schweizer, N.; Urbach, N., A., 2019, Nfts in practice–non-fungible tokens as core component of a blockchain-based event ticketing application
- Chen, S.; Li, R.; Wang, Qi; Wang, Qin., 2021, Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges, arXiv preprint arXiv:2105.07447, <https://doi.org/10.48550/arXiv.2105.07447>
- Trautman, L.J., 2021. Virtual art and non-fungible tokens. *Hofstra L. Rev.*, 50, p.361.
- Chevet, S., 2018, Blockchain technology and non-fungible tokens: Reshaping value chains in creative industries. *SSRN* 3212662.
- Chohan, U.W., 2021, Non-fungible tokens: Blockchains, scarcity, and value. *Critical Blockchain Research Initiative (CBRI) Working Papers*.
- Basir, O.; Omar, A.S., 2020 Capability-based non-fungible tokens approach for a decentralized aaa framework in iot. In: *Blockchain Cybersecurity, Trust and Privacy*, Springer, pp. 7–31.
- Dowling, M., 2022, Fertile LAND: Pricing non-fungible tokens. *Finance Research Letters*, 44, p. 102096.

- Gervais, A.; Musan, D.I.; William, J., 2020, Nft. finance leveraging non-fungible tokens. *Imperial College London, Department of Computing*.
- Gervais, A., ve ark., 2016, On the security and performance of proof of work blockchains. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. pp. 3–16.
- Garay, J., Kiayias, A., Leonardos, N., 2017, The bitcoin backbone protocol with chains of variable difficulty. In: *Annual International Cryptology Conference*, Springer pp. 291–323.
- Lamport, L., Shostak, R., Pease, M.: The byzantine generals problem. In: *Concurrency: the Works of Leslie Lamport*, pp. 203–226 (2019)
- Wood, G., ve ark., 2014, Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper* 151, 1–32
- Bal, M., Ner, C., 2019, Nftracer: a non-fungible token tracking proof-of-concept using hyperledger fabric. *arXiv preprint arXiv:1905.04795*
- Li, R.; Wang, Q., 2021, A weak consensus algorithm and its application to highperformance blockchain. In: *IEEE INFOCOM 2021-IEEE Conference on Computer Communications (INFOCOM)*.
- Al-Bassam, M.; Azouvi, S.; Bano, S.; Danezis, G.; McCorry, P.; Meiklejohn, S.; Sonnino, A. 2019, Sok: Consensus in the age of blockchains. In: *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*. pp. 183–198
- Garay, J. and Kiayias, A., 2020, Sok: A consensus taxonomy in the blockchain era. In *Topics in Cryptology–CT-RSA 2020: The Cryptographers’ Track at the RSA Conference 2020*, Springer International Publishing. San Francisco, CA, USA, pp. 284–318.
- Baylina, J.; Dafflon, J.; Shababi, T., 2017, Eip-777: Erc-777 token standard, [online], Web Adresi: <https://eips.ethereum.org/EIPS/eip-777> [Ziyaret Tarihi: 1 Ağustos 2023]
- Buterin, V.; Vogelsteller, F., 2015, Eip-20: Erc-20 token standard, [online], Web Adresi: <https://eips.ethereum.org/EIPS/eip-20>, [Ziyaret Tarihi: 1 Ağustos 2023]
- Binet, E.; Castonguay, P.; Cooke, A.; Radomski, W.; Sandford, R.; Therien, J., 2018, Eip-1155: Erc-1155 multi token standard. Ethereum Improvement Protocol, EIP-1155, [online], Web Adresi: <https://eips.ethereum.org/EIPS/eip-1155>. [Ziyaret Tarihi: 1 Ağustos 2023]
- Raval, S., 2016, Decentralized applications: harnessing Bitcoin’s blockchain technology. *O’Reilly Media, Inc*.
- Garay, J., Kiayias, A., Leonardos, N., 2015, The bitcoin backbone protocol: Analysis and applications. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, Springer, pp. 281–310.

- Rogaway, P., Shrimpton, T.: Cryptographic hash-function basics, 2004, Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance,. In: *FSE*, Springer, pp. 371–388.
- Menezes, A.J., Van Oorschot, P.C., Vanstone, S.A., 2018, Handbook of applied cryptography. *CRC press*.
- Galindo, D.; Li, R.; Wang, Q., 2019, Auditable credential anonymity revocation based on privacy-preserving smart contracts. In: *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, Springer, pp. 355–371.
- Li, R., ve ark., 2020, An accountable decryption system based on privacy-preserving smart contracts. In: *International Conference on Information Security*, Springer, pp. 372390.
- Moore, D.; Savage, S.; Voelker, G., 2006, Inferring internet denial-of-service activity. *ACM Trans. Comput. Syst.* 24, 115–139
- Shostack, A., 2008, Experiences threat modeling at microsoft. *MODSEC@ MoDELS*, p.35.
- Benson, J., 2021, Your nfts can go missing—here’s what you can do about it. [online], Web adresi: <https://decrypt.co/62037/missing-or-stolen-nfts-how-to-protect> , [Ziyaret Tarihi: 1 Ağustos 2023]
- Hu, J.; Qin, B.; Wang, Q.; Xiao, F., 2020. Preserving transaction privacy in bitcoin. *Future Generation Computer Systems*, 107, pp.793-804.
- Kogan, A.; Wang, Y., 2018. Designing confidentiality-preserving Blockchain-based transaction processing systems. *International Journal of Accounting Information Systems*, 30, pp.1-18.
- Noether, S., 2015 Ring signature confidential transactions for monero. *IACR Cryptol. ePrint Arch.*, 1098.
- Raman, R.K., ve ark. , 2018. Trusted multi-party computation and verifiable simulations: A scalable blockchain approach. *arXiv preprint arXiv:1809.08438*.
- Zamyatin, A., ve ark. , 2021. Sok: Communication across distributed ledgers. In *Financial Cryptography and Data Security: 25th International Conference, FC 2021, Virtual Event, March 1–5, 2021, Revised Selected Papers, Part II* 25 (pp. 3-36).
- Ciampi, M., ve ark. , 2020. Updatable blockchains. In *Computer Security–ESORICS 2020: 25th European Symposium on Research in Computer Security, ESORICS 2020, Proceedings, Part II* 25, pp. 590-609.
- Samuelson, P., 1991. Digital media and the law. *Communications of the ACM*, 34(10), pp.23-28.
- Taylor, J., 1997, DVD Demistified: The Guidebook for DVD-Video and DVD-ROM. *New York, NY: BIBLIOGRAPY CHAPTERS*, pp.1-4.

- Rupley, S., 1996. What's holding up DVD?. *PC Magazine*, 15(20), p.34.
- Renaud, J.-L., 1996, PC industry could delay DVD, *Advanced Television Markets*, 47.
- Langelaar, G.C.; Lagendijk, R.L.; Setyawan, I. , 2000. Watermarking digital image and video data. A state-of-the-art overview. *IEEE Signal processing magazine*, 17(5), pp.20-46.
- Cox, I.J. and Miller, M.L., 1997, June. Review of watermarking and the importance of perceptual modeling. In *Human Vision and Electronic Imaging II* (Vol. 3016, pp. 92-99).
- Langelaar, G.C., 1999. Conditional access to television service. In *Wireless communication. Chapter: network concepts and standards. Section: Broadcast systems, digital video broadcasting (DVB). 3rd ed.[CD-ROM]*, pp. 1-3.
- Biemond, J.; Lagendijk, R.L.; Langelaar, G.C. , 1998. Real-time labeling of MPEG-2 compressed video. *Journal of Visual Communication and Image Representation*, 9(4), pp.256-270.
- Anderson, R.J. and Petitcolas, F.A., 1998. On the limits of steganography. *IEEE Journal on selected areas in communications*, 16(4), pp.474-481.
- Depovere, G.; Haitsma, J.; Kalker, T. , 1999, Video watermarking system for broadcast monitoring. In *Security and Watermarking of Multimedia contents*, Vol. 3657, pp. 103-112.
- Delp, E.J.; Wolfgang, R.B. , 1999, April. Fragile watermarking using the VW2D watermark. In *Security and Watermarking of Multimedia Contents* (Vol. 3657, pp. 204-213).
- Bender, W.; Gruhl, D.; Lu, A.; Morimoto, N. , 1996. Techniques for data hiding. *IBM systems journal*, 35(3.4), pp.313-336.
- Kobayashi, M.; Swanson, M.D.; Tewfik, A.H. , 1998. Multimedia data-embedding and watermarking technologies. *Proceedings of the IEEE*, 86(6), pp.1064-1087.
- Nikolaides, N.; Pitas, I.; Voyatzis, G. , 1998, September. Digital watermarking: An overview. In *9Th European signal processing conference (EUSIPCO 1998)* (pp. 1-4).
- Anderson, R.J.; Petitcolas, F.A.P. , 1998, September. Weaknesses of copyright marking systems. In *Multimedia and security workshop at ACM Multimedia*, Vol. 98, pp. 55-61.
- Kutter, M., Petitcolas, F.A.P., 1999, Fair benchmark for image watermarking systems. In *Security and watermarking of multimedia contents*, Vol. 3657, pp. 226-239.
- Fridrich, J. and Goljan, M., 1999, Comparing robustness of watermarking techniques. In *Security and watermarking of multimedia contents*, Vol. 3657, pp. 214-225.
- Massey, J.L., 1992, "Contemporary cryptology: An introduction" in *Contemporary Cryptology: The Science of Information Integrity*, pp. 3-39.

- Osborne, C.F.; Tirkel, A.Z.; van Schyndel, R.G., 1994, "A digital watermark," in *Proc. IEEE Int. Conf. Image Processing*, vol. 2, pp. 86-90.
- Bender, W.; Gruhl, D.; Morimoto, N., 1995, "Techniques for data hiding," in *Proc. SPIE, Storage and Retrieval for Image and Video Databases III*, vol. 2420, pp. 165-173.
- Caronni, G., 1995, "Assuring ownership rights for digital images," in *Proc. Reliable IT Systems, VIS '95*, Germany, pp. 251-263.
- Girod, B.; Hartung, F., 1996, "Digital watermarking of raw and compressed video," in *Proc. SPIE 2952: Digital Compression Technologies and Systems for Video Communication*, pp. 205-213.
- Pitas, I., 1996, "A method for signature casting on digital images," in *Proc. ICIP-96, IEEE Int. Conf. Image Processing*, vol. III, Switzerland, pp. 215-218.
- Kaskalis, T.H.; Pitas, I., 1995, "Applying signatures on digital images," in *Proc. IEEE Workshop on Nonlinear Signal and Image Processing*, Neos Marmaras, Thessaloniki, Greece, pp. 460-463.
- Comiskey, B.O.; Smith, J.R., 1996, "Modulation and information hiding in images. In *International Workshop on Information Hiding*, pp. 207-226.
- Delp, E.J.; Wolfgang, R.B., 1996, "A watermark for digital images," in *Proc. IEEE Int. Conf. Image Processing*, vol. III, Lausanne, Switzerland, pp. 219-222.
- Langelaar, G.C.; Lagendijk, R.L.; van der Lubbe, J.C.A., 1997, "Robust labeling methods for copy protection of images," in *Proc. SPIE Electronic Imaging '97, Storage and Retrieval for Image and Video Databases V*, San Jose, CA, pp. 298-309.
- Delp, E.J.; Wolfgang, R.B., 1997, "A watermarking technique for digital imagery: Further studies," in *Proc. Int. Conf. Imaging Science, Systems, and Technology*, Las Vegas, NV, pp. 279-287.
- Delp, E.J.; Wolfgang, R.B., 1997, "Overview of image security techniques with applications in multimedia systems," in *Proc. SPIE Conf. Multimedia Networks: Security, Displays, Terminals, and Gateways*, vol. 3228, Dallas, TX, pp. 297-308.
- Liu, B.; Zeng, W., 1997, "On resolving rightful ownerships of digital images by invisible watermarks," in *Proc. ICIP 97, IEEE Int. Conf. Image Processing*, Santa Barbara, CA, pp. 552-555.
- Fridrich, J., 1999, June. Robust bit extraction from images. In *Proceedings IEEE International Conference on Multimedia Computing and Systems*, Vol. 2, pp. 536-540.
- Biemond, J.; Hanjalic, A.; Langelaar, G.C.; Lagendijk, R.L.; van Roosmalen, P.M.B., 2000, *Image and Video Databases: Restoration, Watermarking and Retrieval, Advances in Image Communications*, vol. 8, New York, Elsevier Science.

- Depovere, G.; Kalker, T.; Linnartz, J-P.; Maes, M., 1998, "On the reliability of detecting electronic watermarks in digital images," in *Proc. IX European Signal Processing Conf.*, vol. 1, Island of Rhodes, Greece, pp. 13-16.
- Liang, T.; Rodriguez, J., 2000, "Improved watermarking robustness via spectrum equalization," in *Proc. IEEE ICASSP 2000*, Istanbul, Turkey, pp. 5-9.
- Shannon, C.E.; Weaver, W.W., 1949, *The Mathematical Theory of Communications*, [online], Urbana, IL: Univ. of Illinois Press, https://pure.mpg.de/rest/items/item_2383164/component/file_2383163/content [Ziyaret Tarihi: 1 Ağustos 2023].
- Mitchell, J.L.; Pennebaker, W.B., 1993, *The JPEG Still Image Data Compression Standard*.
- O'Ruanaidh, J.J. and Pereira, S., 1998, September. Secure robust digital image watermark. In *Electronic Imaging: Processing, Printing, and Publishing in Color*, Vol. 3409, pp. 150-163.
- O'Ruanaidh, J.J. and Pun, T., 1997, October. Rotation, scale and translation invariant digital image watermarking. In *Proceedings of International Conference on Image Processing*, Vol. 1, pp. 536-539.
- Boland, F.M.; Dowling, W.J.; Ó Ruanaidh, J.J.K., 1996, "Phase watermarking of digital images," in *Proc. IEEE Int. Conf. Image Processing*, vol. III, Lausanne, Switzerland, pp. 239-242.
- Boland, F.M.; Ó Ruanaidh, J.J.K.; Sinnen, O., 1996. Watermarking digital images for copyright protection. *IEE PROCEEDINGS VISION IMAGE AND SIGNAL PROCESSING*, 143, pp.250-256.
- Herrigel, A.; Ó Ruanaidh, J.; Petersen, H.; Pun, T.; Shelby, P., 1998, "Copyright techniques for digital images based on asymmetric cryptographic techniques," presented at *Workshop on Information Hiding*, Portland, Oregon, USA.
- Herrigel, A.; Ó Ruanaidh, J.J.K.; Pereira, S.; Petersen, H.; Pun, T., 1998, "Secure copyright protection techniques for digital images," in *Information Hiding (Lecture Notes in Computer Science*, vol. 1525), D. Aucsmith, Ed. Berlin, Germany, pp. 169-190.
- Csurka, G.; Deguillaume, F.; Ó Ruanaidh, J.J.K.; Pereira, S.; Pun, T., 1999. Template based recovery of Fourier-based watermarks using log-polar and log-log maps. In *Proceedings IEEE international conference on multimedia computing and systems*, Vol. 1, pp. 870-874.
- Cox, I.J.; Kilian, J.; Leighton, T.; Shamoon, T., 1995, "Secure spread spectrum watermarking for multimedia," *NEC Res. Insti., Princeton, NJ, Tech. Rep.* 95-10.
- Jain, A.K., 1981, "Image data compression: A review," *Proc. IEEE*, vol. 69, pp. 349-389.

- Boland, F.M.; Dautzenberg, C.; Ó Ruanaidh, J.J.K., 1995, "Watermarking digital images for copyright protection," in *Proc. IEE Int. Conf. on Image Processing and Its Applications*, pp. 326-330.
- Barni, M.; Bartolini, F.; Cappellini, V.; Lippi, A.; Piva, A., 1999, "A DWT-based technique for spatio-frequency masking of digital signatures," in *Proc. SPIE/IS&T Int. Conf. Security and Watermarking of Multimedia Contents*, vol. 3657, San Jose, CA, pp. 31-39.
- Arce, G.R.; Boncelet, C.G.; Xia, X.-G., 1997, "A multiresolution watermark for digital images," in *Proc. ICIP 97, IEEE Int. Conf. Image Processing*, Santa Barbara, CA, pp. 548-551.
- Boland, F.M.; Dowling, W.J.; Ó Ruanaidh, J.J.K., 1996, "Watermarking digital images for copyright protection," *Proc. Inst. Elec. Eng. Vision, Image, and Signal Processing*, vol. 143, no. 4, pp. 250-256.
- Hatzinakos, D.; Kundur, D., 1997, "A robust digital image watermarking scheme using wavelet-based fusion," in *Proc. ICIP 97, IEEE Int. Conf. Image Processing*, Santa Barbara, CA, pp. 544-547.
- Wandell, B. A., 1995, "Foundations of vision," Sinauer Associates, Inc., Sunderland, MA.
- Barni, M.; Bartolini, F.; Cappellini, V.; Piva, A., 1998, "Mask building for perceptually hiding frequency embedded watermarks," in *Proc. 5th IEEE Int. Conf. Image Processing ICIP '98*, vol. I, Chicago, IL, pp. 450-454.
- Bossen, F.; Jordan, F.; Kutter, M., 1997, "Digital signature of color images using amplitude modulation," in *Proc. SPIE Electronic Imaging '97, Storage and Retrieval for Image and Video Databases V*, San Jose, CA, pp. 518-526.
- Macq, B.M.; Quisquater, J.-J., 1995, "Cryptology for digital TV broadcasting," *Proc. IEEE*, vol. 83, pp. 944-957.
- Cheng, L.M.; Ng, K.S., 1999, "Selective block assignment approach for robust digital image watermarking," in *Proc. SPIE/IS&T Int. Conf. Security and Watermarking of Multimedia Contents*, vol. 3657, San Jose, CA, pp. 14-17.
- Barni, M.; Bartolini, F.; Cappellini, V.; Piva, A., 1997, "DCT-based watermark recovering without resorting to the uncorrupted original image," in *Proc. ICIP 97, IEEE Int. Conf. Image Processing*, Santa Barbara, CA, pp. 520-527.
- Swanson, M.D.; Tewfik, A.H.; Zhu, B., 1996, "Transparent robust image watermarking," in *Proc. IEEE Int. Conf. Image Processing*, vol. III, Lausanne, Switzerland, pp. 211-214.
- Fleet, D.J.; Heeger, D.J., 1997, "Embedding invisible information in color images," in *Proc. ICIP 97, IEEE Int. Conf. Image Processing*, Santa Barbara, CA, Vol. 1, pp. 532-535.
- Delaigle, J.-F.; De Vleeschouwer, C.; Goffin, F.; Macq, B.; Quisquater, J.-J., 1997, "A low cost perceptive digital picture watermarking method," in *Proc. SPIE Electronic Imaging '97, Storage and Retrieval for Image and Video Databases V*, San Jose, CA, pp. 264-277.

- Podilchuk, C., Zeng, W., 1997, "Perceptual watermarking of still images," in *Proc. 1997 IEEE 1st Workshop Multimedia Signal Processing*, Princeton, NJ, pp. 363-368.
- Nikolaidis, N.; Pitas, I., 1996, "Copyright protection of images using robust digital signatures," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing (ICASSP-96)*, vol. 4, Atlanta, GA, pp. 2168-2171.
- Wu, S.F., Wu, T.L., 1997, "Selective encryption and watermarking of MPEG video," in *Proc. Int. Conf. Image Science, Systems, and Technology, CISST'97*, pp. 0-9.
- Girod, B.; Hartung, F. , 1997, January. Watermarking of MPEG-2 encoded video without decoding and reencoding. In *Multimedia Computing and Networking 1997*, Vol. 3020, pp. 264-274.
- Girod, B.; Hartung, F. , 1998. Watermarking of uncompressed and compressed video. *Signal processing*, 66(3), pp.283-301.
- Langelaar, G.C., 2000, "Real-time watermarking techniques for compressed video data," Ph.D. dissertation, *Delft University of Technology*.
- Aura, T., 1995, "Invisible communication," in *Proc. HUT Seminar on Network Security '95*, Espoo, Finland.
- Aura, T., 1996, Practical invisibility in digital communication. In *Information Hiding: First International Workshop Cambridge, UK, May 30–June 1, 1996 Proceedings 1*, pp. 265-278.
- Hirotsugu, K., 1996, "An image digital signature system with ZKIP for the graph isomorphism," in *Proc. ICIP-96, IEEE Int. Conf. Image Processing*, vol. III, Lausanne, Switzerland, pp. 247-250.
- Fridrich, J.; Goljan, M., , 1999, "Protection of digital images using self embedding," in *Proc. Symp. Content Security and Data Hiding in Digital Media*, New Jersey Institute of Technology.
- Koch, E.; Rindfrey, J.; Zhao, J., 1994 , "Copyright protection for multimedia data," in *Proc. Int. Conf. Digital Media and Electronic Publishing*, Leeds, U.K.
- Koch, E.; Zhao, J., 1995, "Towards robust and hidden image copyright labeling," in *Proc. IEEE Workshop Non-Linear Signal and Image Processing*, Neos Marmaras, Thessaloniki, Greece, pp. 452-455.
- Koch, E.; Zhao, J., 1995, "Embedding robust labels into images for copyright protection," *Proc. Int. Congr. Intellectual Property Rights for Specialized Information, Knowledge and New Technologies*, Vienna, Austria.
- Burgett, S.; Koch, E.; Zhao, J. , 1998, Copyright labeling of digitized image data. *IEEE Communications Magazine*, 36(3), pp.94-100.

- Maes, M.J.J.J.B.; Rongen, P.M.J.; van Overveld, C.W.A.M., 1999, "Digital image watermarking by salient point modification," in *Proc. SPIE Electronic Imaging '99, Security and Watermarking of Multimedia Contents*, San Jose, CA, pp. 273-282.
- Davern, P.; Scott, M., 1996, "Fractal-based image steganography," in *PreProc. Information Hiding, Univ. of Cambridge, U.K.*, pp. 245-256.
- Jordan, F.; Puate, J., 1996, "Using fractal compression scheme to embed a digital signature into an image," in *Proc. SPIE Photonics East Symp.*, Boston, MA.
- Bas, P.; Chassery, J-M.; Davoine, F., 1998, "Self-similarity based image watermarking," in *Proc. IX European Signal Processing Conf., Island of Rhodes, Greece*, pp. 2277-2280.
- Bas, P.; Chassery, J-M.; Davoine, F., 1999, "A geometrical and frequential watermarking scheme using similarities," in *Proc. SPIE Electronic Imaging '99, Security and Watermarking of Multimedia Contents*, San Jose, CA, pp. 264-272.
- Jacquin, A.E., 1992, "Image coding based on a fractal theory of iterated contractive image transformations," *IEEE Trans. Image Processing*, vol. 2, pp. 18-30.
- Collins P., 2021, full-blockchain-solidity-course-py [online], <https://github.com/smartcontractkit/full-blockchain-solidity-course-py>, [Ziyaret Tarihi: 1 Ağustos 2023]
- Wang Q., 2021, invisible-watermark [online], <https://github.com/ShieldMnt/invisible-watermark>, [Ziyaret Tarihi: 1 Ağustos 2023].