T.C.
MİLLÎ SAVUNMA ÜNİVERSİTESİ
ALPARSLAN SAVUNMA BİLİMLERİ VE MİLLÎ GÜVENLİK ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANA BİLİM DALI
SİBER GÜVENLİK PROGRAMI

DİJİTAL SUÇLULARIN KİMLİKLERİNİ AÇIĞA ÇIKARMADA KULLANILAN YENİ BİR EKRAN FİLİGRANLAMA YÖNTEMİ GELİŞTİRİLMESİ

YÜKSEK LİSANS TEZİ

ÖMER FARUK KERMAN
2281806

TEZ DANIŞMANI: DR.ÖĞR.ÜYESİ AYBİKE ŞİMŞEK

ANKARA
EKİM 2024

T.C.
MİLLÎ SAVUNMA ÜNİVERSİTESİ
ALPARSLAN SAVUNMA BİLİMLERİ VE MİLLÎ GÜVENLİK ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANA BİLİM DALI
SİBER GÜVENLİK PROGRAMI

DİJİTAL SUÇLULARIN KİMLİKLERİNİ AÇIĞA ÇIKARMADA KULLANILAN YENİ BİR EKRAN FİLİGRANLAMA YÖNTEMİ GELİŞTİRİLMESİ

YÜKSEK LİSANS TEZİ

ÖMER FARUK KERMAN
2281806

TEZ DANIŞMANI: DR.ÖĞR.ÜYESİ AYBİKE ŞİMŞEK

ANKARA
EKİM 2024

ÖZGÜNLÜK RAPORU

Tez çalışmamın a) Kapak sayfası, b) Giriş, c) Ana bölümler ve ç) Sonuç kısımlarından oluşan toplam 73 sayfalık kısmına ilişkin, 07/08/2024 tarihinde şahsım tarafından Turnitin adlı intihal tespit programından aşağıda belirtilen filtremeler uygulanarak alınmış olan özgünlük raporuna göre, tezimin benzerlik oranı %1'dir.

Uygulanan filtremeler:

1- Kaynakça hariç
2- Alıntılar hariç/dahil
3- 5 kelimeden daha az örtüşme içeren metin kısımları hariç

Millî Savunma Üniversitesi Alparslan Savunma Bilimleri ve Millî Güvenlik Enstitüsü Lisansüstü Tez Çalışması Özgünlük Raporu Alınması ve Kullanılması Uygulama Usul ve Esasları'nı inceledim ve bu Uygulama Esasları'nda belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğruluğu beyan ederim.

Ömer Faruk KERMAN

07/08/2024

ETİK BEYAN

Milli Savunma Üniversitesi Enstitüleri Lisansüstü Tez Hazırlama Kılavuzu'nda yer alan kurallarına uygun olarak hazırladığım bu tez çalışmasında; tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi, tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu, tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi, kullanılan verilerde herhangi bir değişiklik yapmadığımı, bu tezde sunduğum çalışmanın özgün olduğunu, bildirir; aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Bu tezdeki düşünce, görüş, varsayım, sav veya tezler bana aittir; Millî Savunma Üniversitesi ve Alparslan Savunma Bilimleri ve Millî Güvenlik Enstitüsü sorumlu tutulamaz.

Ömer Faruk KERMAN

07/08/2024

ÖNSÖZ ve TEŞEKKÜR

Dijital çağın hızla gelişen dünyasında, kuruluşlar, bilgi güvenliği konusunda sürekli olarak yeni zorluklarla karşı karşıya kalmaktadır. Artan siber tehditler ve veri güvenliği endişeleri, işletmeleri daha da savunmasız hale getirirken, geleneksel güvenlik çözümlerinin sınırlamaları da giderek daha belirgin hale gelmektedir. Bu minvalde, Veri Kaybını Önleme (Data Lost Prevention, DLP) sistemleri gibi yaygın olarak kullanılan güvenlik çözümleri önemli bir rol oynamaktadır. Bu sistemlerin sadece iç ve dış tehditlere karşı koruma sağladığı düşünüldüğünde, içeriden gelen potansiyel tehditlerin dijital iz bırakmadan sızıntıları gerçekleştirebileceği gerçeği göz ardı edilmemelidir. Bu tez çalışmasında, ekran görüntüsü alarak veri sızıntısı yapan kişiyi tespit etmeyi amaçlayan bir çalışma yapılmıştır. Önerilen yöntem sayesinde, ekran çekimi yoluyla veri sızıntısı yapılan resimlerden, dijital suçlunun kimliğinin belirlemesi ve bu kişinin gerçekleştirdiği olayla ilişkilendirmesi amaçlanmıştır.

Bu tez çalışmasının hazırlanmasında ihtiyacım olan her konuda gösterdiği ilgi ve özveriden dolayı danışmanım Dr.Öğr.Üyesi Aybike ŞİMŞEK hocama, bana bu eğitim ve vizyon seviyesini kazandıran Milli Savunma Üniversitesinde görevli başta hocalarım olmak üzere ilgili tüm personele, tez konusu seçmemde ve bilgi ve tecrübeleri ile bana yol gösteren Türk Silahlı Kuvvetleri'nde görev alan komutan ve arkadaşlarıma ve bilhassa yüksek lisans eğitimime başladığım andan itibaren bana maddi ve manevi olarak büyük destek sağlayan aileme teşekkürü borç bilirim.

ANKARA; Ekim 2024 Ömer Faruk KERMAN

İÇİNDEKİLER

TABLO LİSTESİ

ŞEKİL LİSTESİ

KISALTMALAR

BRIEF : Binary Robust Independent Elementary Features
CNN : Convolutional Neural Network
DCT : Discrete Cosine Transform
DLP : Data Lost Prevention
DRM : Digital Rights Management
DT : Discrete Transform
DWT : Discrete Wavelet Transform
EMD : Exploiting Modification Direction
FAST : Features from Accelerated Segment Test
FFT : Fast Fourier Transform
FRFS : Feature Region Filtering System
GRV : Gaussian Random Vector
HVS : Human Visual System
I-SIFT : Improved-Scale-Invariant Feature Transform
JND : Just Noticeable Difference
JPEG : Joint photographic Experts Group
LSB : Least Significant Bit
MSE : Mean Squared Error
ORB : Oriented FAST and Rotated BRIEF
PSNR : Peak Signal-to-Noise Ratio
PVD : Pixel Value Differencing
QDFT : Quantized Discrete Fourier Transform
SSDeN : Structural Similarity for Digital Evidence in Noise
SSIM : Structural Similarity Index Measure
SSRIW : Secreen Shooting Resilience Image Watermarking
SVD : Singular Value Decomposition
TD : Tensor Decomposition
WYSIWYG : What You See Is What You Get

TÜRKÇE ÖZ

Dijital Suçluların Kimliklerini Açığa Çıkarmada Kullanılan Yeni Bir Ekran Filigranlama Yöntemi Geliştirilmesi

Ömer Faruk KERMAN

Millî Savunma Üniversitesi, Alparslan Savunma Bilimleri ve Millî Güvenlik Enstitüsü

Ankara, Ekim, 2024

Kuruluşların bilgi sistemlerini yalnızca harici siber saldırganlara karşı değil, aynı zamanda kişisel çıkar sağlamak amacıyla hassas bilgileri çalmak için erişimlerini istismar edebilecek kendi bünyelerindeki kötü niyetli kişilere karşı da korumaları gerekir. Özellikle içerideki bu kötü niyetli kişiler, dijital kameralar kullanarak bilgisayar ekranlarında görüntülenen belgeleri gizlice izleyebilir ve yakalayabilir. Failler, kurumda kullanılan bilişim sistemleri ve/veya e-posta gibi daha geleneksel iletişim yöntemleri yerine dijital kameraları tercih ederek dijital izlerden kaçabilir ve böylece kimliklerinin tespit edilmesini ve belirlenmesini zorlaştırabilirler. Kurumlar kamera donanımlı cihazların kullanımını yasaklayan bir politika uygulasa bile, küçük kameraların her yerde bulunması bu tehdidin devam etmesine olanak tanır. Bu tezde, bahsedilen tehdide karşı, kullanılan uygulamadan bağımsız olarak ekrana gizli bilgiler içeren görünmeyen filigranlar yerleştiren yeni bir teknik önerilmiştir. Normal kullanım sırasında fark edilemeyen bu görünmez filigranlar, yakalanan görüntülerden çıkarılabilir ve veri sızıntılarının yerini zamanını ve kim tarafından gerçekleştirildiğini belirlemeye yardımcı olur.

Anahtar Sözcükler: Ekran Filigranı, Steganografi, Veri Hırsızlığı, Kötü Niyetli Çalışanlar, Soruşturma ve İlişkilendirme

Bilim Kodu : 92438

Sayfa Sayısı : 64

Tez Danışmanı : Dr.Öğr.Üyesi Aybike ŞİMŞEK

ABSTRACT

Development of a Novel Screen Watermarking Method Used to Reveal the Identity of Digital Criminals

Ömer Faruk KERMAN
Turkish National Defense University
Alparslan Defence Sciences and National Security Institute
Ankara, Oct, 2024

Organizations have to protect their information systems not only against external cyber attackers, but also against malicious insiders who may exploit their access to steal sensitive information for personal gain. In particular, these malicious insiders can use digital cameras to surreptitiously monitor and capture documents displayed on computer screens. By using digital cameras instead of more traditional communication methods such as IT systems and/or email, perpetrators can evade digital traces, making them harder to identify and identify. Even if organizations implement a policy prohibiting the use of camera-equipped devices, the ubiquity of small cameras allows this threat to persist. In this thesis, to counter this threat, a new technique has been proposed that places invisible watermarks containing confidential information on the screen, regardless of the application used. Unnoticeable during normal use, these invisible watermarks can be extracted from captured images and help identify the location of data leaks, when they occurred and by whom.

Keywords: Screen Watermarking, Steganography, Data Theft, Malicious Insiders, Investigation and Attribution

Science Code : 92438
Pages : 64
Supervisor : Asst.Prof.Dr. Aybike ŞİMŞEK

1. GİRİŞ

Kuruluşlar hassas bilgilerini yalnızca dış saldırganlardan değil, aynı zamanda içeriye sızan kişiler veya kötü niyetli çalışanlar gibi iç tehditlerden de korumalıdır. Bu endişeyi gidermek için Veri Kaybını Önleme (DLP) sistemleri gibi çözümler giderek daha fazla kullanılmaktadır. Ancak DLP yazılımı internet erişimi, e-posta gönderme, yazıcıdan döküm alma, ekran görüntüsü alma veya harici medyaya erişim gibi eylemleri günlüğe kaydedecek veya engelleyecek şekilde yapılandırılabilir. Bu durumda DLP yazılımının etkinliği bazı koşullarda sınırlı kalabilir.

Harici medyaya yazdırma veya kurumun e-posta hizmetini kullanma gibi geleneksel iletişim kanalları yoluyla gerçekleşen veri sızıntıları ya önlenebilir ya da en azından failin eylemlerinin dijital izinden sızıntının kaynağı tespit edilebilir. Ancak, DLP sistemleri gibi çözümler, içeriden birinin dijital kamera kullanarak bir bilgisayar ekranının görüntüsünü yakalamasını engelleyemez. Bu durum, bir çalışanın belirli bir belgeyi görüntüleme yetkisine sahip olmasının, bu belgenin görüntüsünü yetkisiz taraflara sızdırabilmesi olasılığının olması anlamına da gelir. DLP yazılımı bir belgenin görüntüsünün çekilip çekilmediğini tespit edemediğinden, kamera kullanmak failin dijital izlerden kolayca kaçmasını sağlar. Bu da sızdırılan bir görüntüye dayanarak failin kimliğini belirleme ve kanıtlama sürecini zorlaştırır. Kamera donanımlı akıllı telefonların yaygınlaşması ve dijital gözlük ya da lens gibi yeni teknolojilerin ortaya çıkması, veri sızıntısı tehdidinin kontrolünü daha da zorlaştırmaktadır.

Veri sızıntısı tehditleriyle başa çıkabilmek için bilgi güvenliği alanında ekran filigranlama, steganografi ve kriptografi gibi teknikler önemli faydalar sağlamaktadır. Ekran filigranlama, fotoğraf veya videolar aracılığıyla sızdırılan içeriğin kaynağının tespit edilmesini kolaylaştırmak amacıyla kullanılan bir yöntemdir. Şeffaf bir filigranın bilgisayar ekranına yerleştirilmesi, sızdırılan görüntülerin kaynağını belirlemede önemli bir izleme ve doğrulama aracı olabilir. Steganografi ise bir veri gizleme tekniğidir ve görüntü, ses veya video gibi medya dosyalarının içine gizlenmiş verileri ifade eder. Bu yöntemle, bir belge veya dosya içindeki gizli verileri tespit

etmek oldukça zorlaşır. Dolaysıyla steganografi teknikleri ekran filigranlama aşamasında sıklıkla kullanılır. Ekran görüntüsü alarak bilgi sızdıran kişi gizlenmiş olan verinin varlığını algılayamaz ve bu sayede veri sızıntısı kaynağı tespiti oldukça kolay hale gelir.

Kriptografi konusu ise şifreleme yöntemlerini kapsar ve veri korumada çok önemli bir rol oynar. Kriptografi, verileri şifreleyip güvenli bir şekilde ileterek yetkisiz erişimi önler ve böylece veri sızıntısı riskini azaltır. Aynı şekilde ekran filigranlama sürecinde veri gizlenmeden önce kriptografi teknikleri kullanarak veriyi şifrelemek, filigranın kötü niyetli kişiler tarafından tespit edilmesi durumunda, verinin doğrudan açık bir şekilde okunabilmesi engellenir. Ayrıca doğrulama kapsamında kriptografik karma (hash) kullanılması sayesinde verinin değiştirilip değiştirilmediği de tespit edilmiş olur.

Bu bağlamda, ekran filigranlama yöntemi ile steganografi ve kriptografinin birleştirilmesi, veri güvenliği açısından oldukça kapsamlı ve entegre bir yaklaşım sunmaktadır. Yüksek güvenlikli bir ekran filigranlama sistemi, sızdırılan verilerin kaynağını belirlemede ve izlemede kritik bir araç olma potansiyeline sahiptir. Bu sistem, hassas bilgilerin izinsiz paylaşımını tespit edebilir ve sorumluları belirleyebilir. Steganografi ve kriptografinin bu sisteme entegrasyonu, verilerin gizliliği ve bütünlüğünü koruma konusunda ek güvenlik katmanları sağlar. Steganografi, bilgilerin gizli bir şekilde iletilmesini sağlarken, kriptografi verilerin şifrelenerek yetkisiz erişimlere karşı korunmasını mümkün kılar. Böylelikle, verilerin hem gizliliği hem de bütünlüğü bozulmadan iletilmesi sağlanmış olur.

Sızıntı kaynağının tespiti noktasında, ekran filigranlama yöntemi ile elde edilen bulgular, kurum ağlarında kullanılan diğer güvenlik sistemlerinin log kayıtları ile çapraz doğrulamaya tabi tutulabilir. Şüphelinin hangi gün ve saatte, hangi IP üzerinden, hangi makine üzerinde oturum açtığı rahatlıkla tespit edilebilir. Bu sayede, sızıntının kesin kaynağı daha net ve güvenilir bir şekilde belirlenebilir. Örneğin, ağ trafiği izleme sistemleri, kullanıcı etkinlik kayıtları ve erişim logları gibi farklı veri kaynakları bir araya getirilerek kapsamlı bir analiz yapılabilir. Bu da güvenlik ihlallerinin hızlı ve etkili bir şekilde tespit edilip, gerekli önlemlerin alınmasını sağlar.

Sonuç olarak, ekran filigranlama yöntemi ile steganografi ve kriptografinin bir araya getirilmesi, veri güvenliği stratejilerinde proaktif ve bütünsel bir çözüm sunmaktadır.

Bu yöntem, verilerin korunması ve sızıntıların önlenmesi konularında kurumlara önemli avantajlar sağlayarak, güvenlik açıklarının minimize edilmesine yardımcı olur.

1.1. Tezin Temeli

Kuruluşlar, dijital dünyadaki hızlı değişimler ve artan siber tehditlerle mücadele etmek için sürekli olarak yeni stratejiler geliştirmekte ve teknolojik çözümler aramaktadır. Özellikle, hassas bilgilerin sızdırılmasını önlemek, dış ve iç tehditlerle başa çıkmak için Veri Kaybını Önleme (DLP) sistemleri gibi birçok güvenlik çözümleri yaygın olarak kullanılmaktadır.

Ancak, geleneksel güvenlik sistemlerinin, sadece içeriden ve dışarıdan, sistem üzerinden gelebilecek siber tehditlere yönelik önlemler alabilmesi, içeriden birinin dijital kamera kullanarak bir bilgisayar ekranının görüntüsünü yakalamasını engelleme konusundaki yetersizliği giderek daha fazla dikkat çekmektedir. Bu durum, veri sızıntılarını önlemek için daha yenilikçi ve etkili yaklaşımların geliştirilmesi gerekliliğini ortaya koymaktadır.

Bu sebeple, kurum içinden veri sızıntısı yapan kötü niyetli kişilerin veya çalışanların tespiti ile idari ve/veya adli soruşturmaya konu olacak sızıntının ilgili kişi ile ilişkilendirilmesi kapsamında bir çalışma gerçekleştirilmiştir.

1.2. Tezin Kapsamı ve Önemi

Bu tezin temel amacı, iç tehditlere karşı daha etkili bir koruma sağlama potansiyeline sahip mevcut ekran filigranlama yöntemlerini incelemek ve bu yöntemlerin eksik kaldığı hususlardan biri olan harici bir kamera ile ekran görüntüsünün yakalanması vesilesiyle oluşabilecek sızıntının kim aracılığıyla gerçekleştiğinin tespit edilebildiği yeni bir ekran filigranlama yöntemi ortaya koyarak dijital suçluların belirlenmesidir.

Günümüzde, kuruluşlar dijital suçluların gelişen taktikleri ve gerçekleşebilecek iç tehditler karşısında sürekli olarak güvenliklerini güçlendirmeye çalışmaktadır. Özellikle, kötü niyetli çalışanlar veya içeriye sızmış kişiler vasıtasıyla gerçekleşebilecek veri sızıntısı kaynağının tespiti büyük önem taşımaktadır. Bu sebeple, önerilen ekran filigranlama yöntemi ile kurumlarda kullanılan geleneksel siber güvenlik çözümlerinin entegrasyonu güvenlik açısından sağladığı avantajlarla beraber, kuruluşlara veri sızıntısının hızlı tespiti, azalan ihlal sayısı, kolay entegrasyon,

daha az veri ihlali maliyeti, azalan hukuki masraflar ve verimli kaynak kullanımı gibi hem operasyonel hem de mali konular bakımından da faydalar sağlamaktadır.

Sonuç olarak, önerilen ekran filigranlama yöntemi ile kurumlar daha etkili bir iç tehdit ve veri sızıntısının kaynağını tespit etme yeteneği kazanırlar. Aynı zamanda önerilen yöntemin kullanıldığının bilinmesi potansiyel suçlulara karşı caydırıcı bir etki yaratır. Yöntemin kurumların siber güvenlik stratejilerine entegrasyonu, kurumların operasyonel verimliliğini arttırılabilir. Bu nedenle, kuruluşların önerilen yöntemi kullanmaları, veri sızıntısına dayalı dijital suçlarla mücadelede önemli bir adım olabilir.

1.3. Tezin Yapısı

Bu tez, altı ana bölümden oluşmaktadır. İlk bölüm olan Giriş bölümünde, tezin temeli, kapsamı ve önemi açıklanmaktadır. Bu bölüm, okuyuculara çalışmanın genel bir çerçevesini sunar. İkinci bölümde, teorik temeller ve literatür incelemesi yapılmaktadır. Bu bölümde, bilgi gizleme teknikleri, filigran ve steganografi yöntemleri detaylı bir şekilde incelenmekte ve karşılaştırılmaktadır.

Üçüncü bölüm, ekran filigranlama yöntemlerinin incelenmesi ve bu yöntemlerin karşılaştırılmasını içermektedir. Dördüncü bölümde ise önerilen yaklaşım tanıtılarak kullanılan materyaller ve metodoloji detaylandırılmaktadır. Beşinci bölümde yapılan çalışmaların değerlendirmesi sunulmakta ve altıncı bölümde sonuçlar ile gelecekteki çalışmalar tartışılmaktadır.

2. TEORİK TEMELLER ve LİTERATÜR İNCELEMESİ

Bu bölüm, bilgi gizleme tekniklerini ve steganografi ile filigranlama arasındaki farkları inceleyerek, bilgi güvenliği ve gizliliği konularında genel bir anlayış sağlamayı amaçlamaktadır. Bilgi gizleme, iletişim süreçlerinde hassas bilgilerin güvenli bir şekilde iletilmesini sağlayan bir dizi teknik ve yöntemi içerir. Bu teknikler, bilgiyi farklı medya türlerine gömerek veya değiştirerek gizlemeyi amaçlar.

Bilgi gizleme teknikleri, genellikle kriptografi ile birlikte kullanılarak daha güçlü bir güvenlik sağlar. Kriptografi, bilginin şifrelenmesi ve şifrelenmiş bilginin çözülmesi süreçlerini içeren matematiksel bir alandır. Kriptografi, bilgiyi korumak için şifreleme algoritmalarını kullanarak verilerin gizliliğini sağlar. Ancak, şifrelenmiş verilerin varlığı, göndericinin veya alıcının dikkatini çekebilir ve bu da güvenlik riski oluşturabilir. Şifrelemenin en büyük dezavantajı, verinin varlığının gizlenmemesidir. Şifrelenmiş veri, okunamaz olmasına rağmen, hala veri olarak mevcuttur. Yeterli zaman verilirse, birisi eninde sonunda verinin şifresini çözebilir. Bu soruna bir çözüm steganografidir.

Steganografi, veriyi veri içinde göze çarpmayacak şekilde gizleme sanatıdır. Steganografinin genel olarak amacı, istenmeyen alıcıların steganografik ortamın gizli veri içerdiğinden şüphelenmeyeceği kadar iyi veri gizlemektir. Steganografi, bilginin varlığını gizlemek için çeşitli medya türlerini kullanır. Bu teknik, bilgiyi taşıyan dosyaları veya iletişim araçlarını seçerken, bilginin fark edilmesini zorlaştırır. Steganografi, gizli bilgiyi taşıyan medyanın, normal veya açık bir mesajı temsil etmesini sağlar. Bu da bilgiyi kötü niyetli kişilerin dikkatinden kaçırabilir ve güvenli bir iletişim sağlayabilir.

Filigranlama ise, dijital içeriklere gizli işaretlerin eklenmesini sağlayan bir tekniktir. Bu işaretler, içeriğin sahipliğini veya bütünlüğünü doğrulamak için kullanılabilir. Filigranlama, dijital medyanın korsan kopyalarının tespit edilmesi ve orijinalliğinin korunması için yaygın olarak kullanılmaktadır. Bu alt başlıklar altında incelenen konular, bilgi güvenliği ve iletişim teknolojileri alanında önemli bir role sahiptir. Bu

tekniklerin anlaşılması, bilgi güvenliği stratejilerinin geliştirilmesinde ve uygulanmasında kritik bir öneme sahiptir.

2.1. Bilgi Gizleme Teknikleri

Sosyal medyanın da gelişmesiyle beraber, insanlar vakitlerinin hatırı sayılır bir kısmını bu ortamlarda geçirmeye başlamışlardır. Çevrimiçi ortamda, kullanıcılar paylaştıkları bilgilerin güvenliğinden, başka kimselerin eline geçirilmediğinden emin olmak isterler. Gönderilen bir mesajın sadece gerçekten ilgili kişi tarafından alındığından, mesajdaki diğer çoklu ortam verilerinin de yine üçüncü şahıslar tarafından ele geçirilmediğini bilmek isterler. Günümüzde hem daha pratik olduğundan hem de kişi kendini daha konforlu hissettiğinden iletişim daha çok elektronik ortamlarda gerçekleşmeye başlamıştır. Bu da beraberinde güvenlik, güvenilirlik gibi yeni ihtiyaçlar getirmiştir. Bu ihtiyaçlardan birisi de dijital medyanın bilgisayar ağları üzerinden kolaylıkla ve güven içerisinde iletilmesidir. Bununla birlikte, bir ağ üzerinden iletişim kurarken karşılaşılan önemli bir sorun hem pasif hem de aktif olabilecek üçüncü şahısların, gözetleyicilerin ağ üzerindeki varlığıdır. Pasif bir gözetleyici sadece ağı dinleyebilirken, aktif bir gözetleyici bir mesajı hem dinleyebilir hem de değiştirebilir. İletişimin güven içinde sağlanması için, yalnızca mesajı gönderen kişinin hedeflediği alıcının iletişimin içeriğini deşifre edebilmesini sağlamak ve aynı zamanda iletilen mesajı gizli tutmayı başarmak gerekir. Bu sorunu ele almak için iki temel çözüm ortaya çıkmıştır: bilgi gizleme ve kriptografi (Chugh & Student, 2013).

Güvenli ve gizli bir iletişim yöntemi arayışı standart kullanımın yanı sıra, sadece askeri amaçlar için değil, aynı zamanda ticari strateji ve telif hakkı ile ilgili pazar hedefleri açısından da çok önemlidir. Kriptografi, düz metnin gizli bir anahtar kullanılarak şifreli metne dönüştürülmesini içerir. Ancak, şifreli metinlerin iletilmesi saldırganlar arasında kolayca şüphe uyandırabilir ve potansiyel olarak şifreli metnin ele geçirilmesine, tehlikeye atılmasına veya şifresinin çözülmesine yol açabilir. Kriptografik tekniklerin sınırlamalarının üstesinden gelmek için bilgi gizleme stratejisi benimsenmiştir.

Bilgi gizleme, gizli verilerin dijital bir taşıyıcı kaynak içinde gizlenmesini sağlayan çok disiplinli bir alandır. İletişimlerini başkaları tarafından fark edilmeden sürdürmek isteyen iki taraf gönderici ve alıcıdır. Gönderici, iletişimin varlığını maskeleyen bir

görüntü kullanabilir. Bu görüntü daha sonra herkesin erişimine açık bir kanalda kullanıma sunulur, ancak yalnızca hedeflenen alıcı gizli bilginin farkındadır ve onu çıkarma yeteneğine sahiptir. Bilgi gizleme teknikleri, Şekil 2.1'de gösterildiği gibi, dört ana türe ayrılır: steganografi, filigranlama, parmak izi ve kriptografi.

Şekil 2.1: Bilgi Gizleme Teknikleri.

(Chugh & Student, 2013)' den uyarlanmıştır.

2.1.1. Steganografi

Steganografi, Yunanca "örtülü veya korunan" anlamına gelen 'steganos' ve 'yazı' anlamına gelen 'graphie' kelimelerinden türetilmiştir (Petitcolas ve diğ., 1999). Bu nedenle, steganografi sadece sanat değil, aynı zamanda iletişimin asıl içeriğiyle birlikte gerçekleşen iletişim gerçeğini gizleme bilimidir (Orebaugh, 2004). Gizlilik, steganografi için tek motivasyon değildir. Tek bir varlık oluşturmak için bir veri parçası diğerinin içine gömülebilir, böylece ikisini birlikte tutma ihtiyacı ya da birbirinden ayrılma riski ortadan kalkar. Tıbbi görüntülerin içine hasta bilgilerinin gömülmesi ve iki bilgi parçası arasında kalıcı bir ilişki kurulması bu avantajı vurgulayan bir uygulamadır.

Steganografinin amacı, gizli mesajların şüphe uyandırmadan iletilmesini sağlamaktır. "Ne Görüyorsan Onu Alırsın (What You See is What You Get, WYSIWYG)" konsepti görüntülerin veya diğer materyallerin yazıcıdan çıktısını alırken bazen karşımıza çıksa da her zaman doğru olmayabilir. Görüntüler, İnsan Görsel Sisteminin (Human Visual System, HVS) algıladığından daha fazlasını içerebilir ve binlerce kelimeden daha fazlasına sahip olabilir. Tarih boyunca insanlar gizli iletişim yöntemleri yaratmaya çalışmışlardır. Antik bir Yunan kaydında, mesaj yazmak için kullanılan balmumu tabletlerin balmumunun eritilmesi ve sonrasında alttaki ahşaba bir mesajın yazılması

uygulaması anlatılmaktadır. Balmumu daha sonra tekrar ahşaba uygulanarak yeni, kullanılmamış bir tablet görüntüsü verilmiştir. Sonuçta üretilen tabletler ile, balmumunun altında bir mesaj olduğu halde kimse şüphelenmeden masum bir şekilde taşınabilmiştir. Bu tarihi olaydan çıkarılabilecek önemli bir ders, gizli iletişimin her zaman herkesin bildiği ve kullandığı standart yollarla yapılmasının gerekmediğidir. Başka bir deyişle, bilgi iletmek için görünüşte sıradan ve masum görünen yöntemler kullanılarak gizli mesajlar aktarılabilir. Örneğin, antik Yunan'da mesajlar, balmumu tabletlerin altındaki ahşaba yazılarak gizlenmiştir. Balmumu tekrar tabletin üzerine yerleştirildiğinde, tablet kullanılmamış gibi görünmüş ve kimse içinde gizli bir mesaj olduğundan şüphelenmemiştir.

Başka bir basit örnek olarak, bir kitap şifresi düşünülebilir. Bu yöntemde, gizli mesaj bir kitabın belirli sayfa, satır ve kelimelerinden oluşturulur. Örneğin, mesaj göndermek isteyen kişi, alıcıya belirli bir kitabın adını ve mesajın bulunduğu sayfa ve satır numaralarını verir. Alıcı, bu bilgileri kullanarak kitaptan gizli mesajı çıkarabilir. Bu yöntem, iletişimin görünürde masum bir kitap üzerinden yapılmasını sağlar ve kimse mesajın gizli olduğunu fark etmez. Bu tür yenilikçi ve dikkat çekmeyen yöntemler, gizli mesajların iletilmesinde etkili olabilir.

Bir steganografik sistem iki temel unsuru içermektedir: steganografik kapasite ve algılanamazlık. Steganografik kapasite, gizli bilginin gizli veri taşıyıcısına (örneğin, görüntü, ses dosyası veya metin) ne kadar etkili ve verimli bir şekilde yerleştirilebileceğini ifade eder. Bu kapasite ne kadar yüksek olursa, o kadar fazla bilgi gizlenebilir. Ancak, kapasitenin artırılması, genellikle gizli bilginin taşıyıcı üzerinde daha belirgin değişikliklere neden olabilir.

Algılanamazlık ise, steganografik mesajın varlığının üçüncü taraflarca fark edilmemesini ifade eder. Bu durum, gizli mesajın yerleştirildiği taşıyıcı üzerinde yapılan değişikliklerin, orijinalinden ayırt edilemeyecek kadar küçük ve belirsiz olmasını gerektirir. Taşıyıcı dosyanın görünümü veya yapısı, gizli mesaj içerdiğine dair herhangi bir ipucu vermemelidir.

Ancak, bu iki özellik genellikle birbiriyle çelişir ve bir steganografik sistemin kapasitesi artırılırken aynı zamanda algılanamazlığın korunması oldukça zordur. Başka bir deyişle, daha fazla bilgi gizlemek için yapılan değişiklikler, taşıyıcı dosyanın yapısını ve görünümünü daha fazla etkileyebilir ve bu da gizli mesajın tespit edilme

olasılığını artırabilir. Bu nedenle, etkili bir steganografik sistem tasarlarken, kapasite ve algılanamazlık arasında dikkatli bir denge kurmak gerekmektedir.

2.1.2. Filigranlama

'Filigran', kâğıt yapım sürecinde oluşturulan tanımlayıcı işaretleri ifade eder. En eski filigranlar 13. yüzyıl İtalya'sında ortaya çıkmış ve yetenekli kâğıt üreticilerini veya ticaret loncalarını tanımlamak için hızla tüm Avrupa'ya yayılmıştır. Günümüzde filigranlar hala orijinallik işaretleri olarak ve sahteciliği önlemek için kullanılmaktadır. Filigran, bir 'kapak kaynağına' gömülü 'gizli bir mesajdır'. Kapak kaynağı, gizli mesajın içine gömüldüğü veya üzerine yerleştirildiği açık ve görünür bir öğeyi ifade eder. Örneğin, bir resim dosyası, ses dosyası veya metin belgesi gibi. Kapak kaynağı, dışarıdan bakıldığında normal ve doğal bir şekilde görünen bir nesnedir. Ancak içine gizlenmiş olan filigran, bu normal görünüşün altında yer alır ve genellikle sadece belirli bir anahtar veya yöntemle ortaya çıkarılabilir (Petitcolas ve diğ., 1999). Filigranın varlığı, genellikle görünür filigranlama yöntemiyle belirgin bir şekilde ifade edilir. Bu, belirli bir nesnenin yüzeyine açıkça yerleştirilen ve genellikle gözle görülebilir olan filigran veya işaretlerdir. Örneğin, bir kâğıt üzerinde üretici veya marka adını belirten işaretler bu tür bir görünür filigran olabilir. Bu tür filigranlar, belirli bir kimlik veya orijinallik işareti olarak kullanılır ve sahteciliği önlemek amacıyla geniş çapta benimsenmiştir. Filigranlama tekniklerinin etkinliği filigranın sağlamlığına ve güvenliğine bağlıdır. Belirli bir nesnede bir filigranın varlığı bilinse bile (görünür filigranlama), orijinal (filigranlı) nesneyi değiştirmeden veya yok etmeden filigranı nesneden çıkarmak imkânsız olmalıdır. Bu özellik, filigranların güvenilirliğini sağlamak için kritik bir öneme sahiptir ve steganografik sistemlerde de benzer bir prensip geçerlidir.

Dijital filigranlama, belirli bir algoritma ile görüntülere, videolara, seslere ve diğer çoklu ortam verilerine fikri mülkiyet haklarına sahip damga gömme teknolojisidir. Bu tür bir filigran, sahibinin logosu, seri numarası veya kontrol bilgileri gibi yazar ve kullanıcı bilgilerini içerebilir. Aslında, verilerdeki her yerde bulunan fazlalık ve rastgelelikten yararlanır ve ürün telif hakkını ve veri bütünlüğünü korumak için tespit edilmesi zor ancak ayırt edilebilen bilgiler eklenir. Dijital filigranlama ile kriptografi, steganografi ve parmak izi gibi diğer teknolojiler arasında üç temel fark vardır. Bunlardan birincisi, şifrelemenin aksine, filigranın algılanamamasıdır. Böylelikle

görüntü estetik anlamda bozulmaz. İkinci fark, filigranların ve içine gömüldükleri belgelerin birbirinden ayrılamamasıdır. Belgeler görüntülense veya başka dosya formatlarına dönüştürülse bile filigranlar ortadan kalkmaz. Üçüncü fark ise, filigranların belgelerle tamamen aynı dönüşüm deneyimine sahip olmasıdır. Yani filigranlara bakarak dönüşümün bilgisini alabilirsiniz (Zhang, 2009).

2.1.3. Parmak İzi

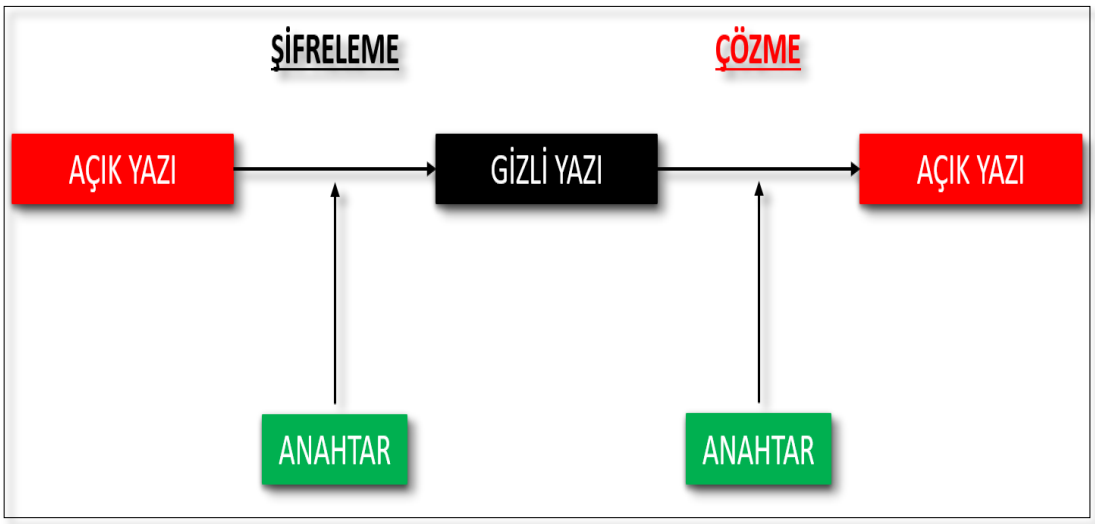
Parmak izi, tespit edilen yasadışı bir veri kopyasının kaynağını izlemek için verileri benzersiz bir şekilde işaretleme işlemidir. Parmak izinin temel amacı, her kullanıcının ilgili veri dosyasının veya içeriğin benzersiz bir işaret içeren bir kopyasını elde etmesidir. Bu işaret, belirli bir veri parçasını veya belgeyi tanımlamak için kullanılabilir. Parmak izi içeren kopyalar yalnızca kimlikleri doğrulanmış kullanıcılara dağıtılabilir ve böylece kopyaları alanların doğru kişiler olması sağlanabilir. Örneğin bir kurum, içerisinde hassas bilgiler (resimler, videolar, vb.) bulunan belgeleri sadece belirli yetkili çalışanlara dağıtmaktadır. Ancak, bir çalışan bu belgelerden birini izinsiz olarak kopyalayıp sızdırdığında, parmak izi sayesinde sızdırılan bilginin kaynağı tespit edilebilir. Parmak izleri, bu belgelerin her bir kopyasına algılanamaz bir şekilde yerleştirilmiş olup, bu sayede belgelerin hangi kişi veya kullanıcı tarafından sızdırıldığı doğrulanabilir. Bu işaretler algılanamaz olmalı ve dağıtılan her karede veya görüntüde bulunmalıdır. Aynı zamanda, birden fazla kopyalama veya düzenleme işlemi ile kaldırılamayacak kadar güvenilir bir şekilde yerleştirilmelidir (Petitcolas ve diğ., 1999).

Dijital içeriğin fikri mülkiyetinin korunmasına yönelik talep, bu alandaki suç artışındaki yükseliş nedeniyle artmaktadır. Bu artış, bilgi teknolojisinin ve organizasyonunun hızlı bir şekilde genişlemesiyle bağlantılıdır. Filigran tekniğini kullanan dijital parmak izi, içerik değişimine karşı etkili bir savunma yöntemidir. Bu teknik, dijital içeriğin orijinalliğini ve bütünlüğünü korumak için kullanılır. İçerik üzerinde herhangi bir değişiklik yapıldığında, filigran içeriğin izinsiz kullanımını tespit etmek ve yasadışı manipülatörleri belirlemek için bir sistem sağlar (Mehan ve diğ., 2013). Bu yöntemde, teslimattan önce içeriğe benzersiz bir kimlik numarası eklenir. Bu kimlik numarasına parmak izi denir. İçeriğin şüpheli bir kopyası oluşturulduğunda, içerik sahibi parmak izi üzerinden yasadışı kullanıcıyı tespit edebilir. Dijital parmak izi, içeriğin sahipliğini doğrulamak ve izinsiz kullanımı

önlemek için önemli bir araçtır. Dijital filigranlama ise genellikle sahipliğin tespit edilmesi için filigranlarının sağlamlığını korur. Bu teknik, içeriğin üzerine gizli olarak yerleştirilen bilgiler aracılığıyla orijinalliği ve bütünlüğü sağlamak amacıyla kullanılır. Filigranlar, içeriğin herhangi bir versiyonunda yer alabilir ve genellikle algılanması zor olduğu için sahteciliği önlemede etkili bir rol oynar. Dijital parmak izi modeli, şeffaflık, algılanamazlık ve güvenilirlik özelliklerini içermelidir. Bu özellikler, dijital içeriğin sahipliğini korumak ve izinsiz kullanımı engellemek için önemlidir.

2.1.4. Kriptografi

Kriptografi, verilerin güvenliği ve gizliliği için temel bir araçtır. Bilgiyi gizlemek ve korumak için sıklıkla kullanılan bir tekniktir. Esas olarak "gizli yazı" anlamına gelen kriptografinin amacı, iletilen veya saklanan verilerin üç temel özelliğini korumaktır: gizlilik, bütünlük ve kimlik doğrulama. Bu özellikler, verilerin sadece yetkili kişiler tarafından erişilebilmesini, verilerin değiştirilmediğini ve verilerin doğruluğunu sağlar. Kriptografinin temel amacı, internet gibi herkese açık bir ortam üzerinden aktarılan verilerin gizliliğini sağlamak ve yetkisiz bir kişi tarafından erişilmesi halinde bu verilerin hiçbir anlam ifade etmemesini garanti altına almaktır. Kriptografi, iletişim sırasında verilerin korunmasını ve güvenliğini sağlamanın yanı sıra, verilerin güvenilirliğini ve doğruluğunu da koruyarak bütünlüğünü sağlar. Veriler şifrelenirken, karmaşık matematiksel işlemler ve algoritmalar kullanılarak şifrelenir. Bu sayede, veriler yetkisiz kişilerden korunur ve iletişimin güvenliği sağlanır. Kriptografi metodolojisi Şekil 2.2'de gösterilmiştir.



Şekil 2.2: Kriptografi Metodolojisi.

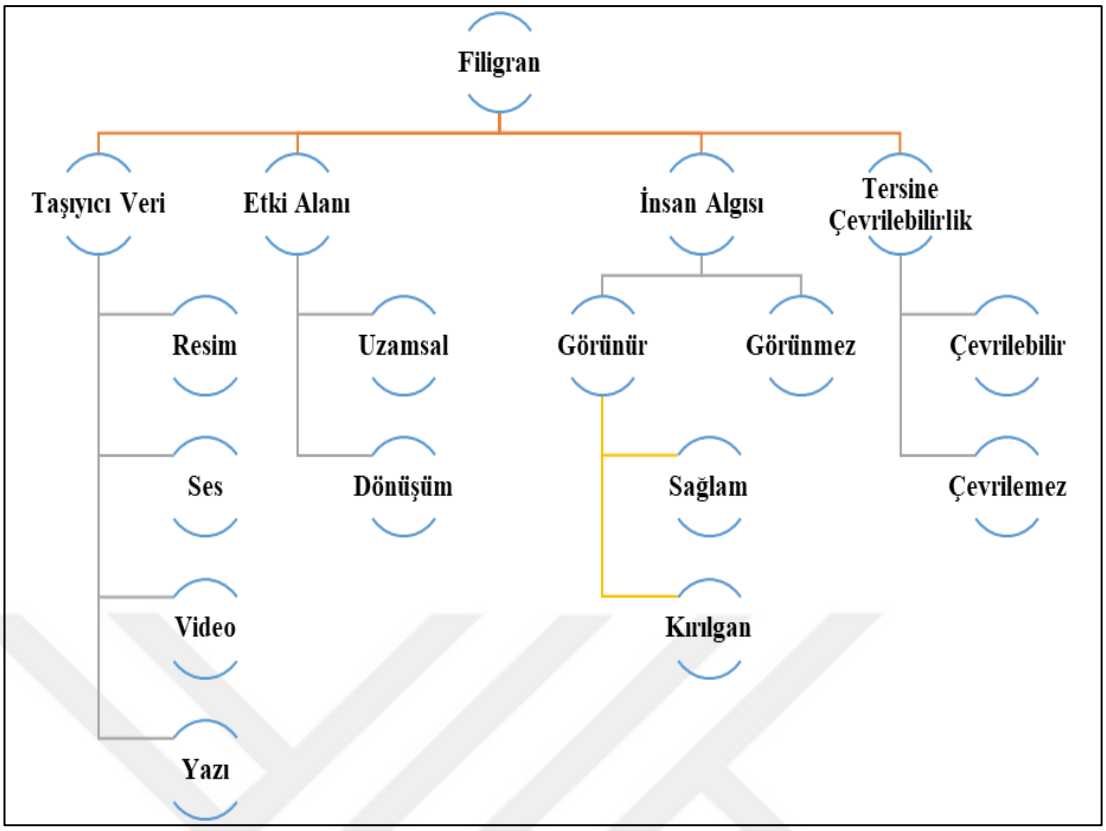
(Singh ve diğ., 2024)'den uyarlanmıştır.

Şekil 2.2.'de gösterildiği gibi, gönderilecek veriler genellikle düz metin olarak adlandırılır ve bir tür karışıklığa veya anlamsız forma dönüştürülür. Bu işlem, verilerin güvenliğini sağlamak için kullanılan şifreleme olarak bilinir. Kriptografi süreci, verilerin güvenliğini sağlamak için kritik bir yöntemdir. İlk adımda, gönderilecek veriler düz metin olarak hazırlanır. Şifreleme sürecinde, uygun bir şifreleme algoritması seçilir ve bir şifreleme anahtarı belirlenir. Seçilen algoritma ve anahtar kullanılarak veriler şifrelenir ve anlamsız bir form kazanır. Şifrelenmiş veri güvenli bir iletişim kanalı üzerinden gönderilir. Alıcı taraf, şifreli metni alır ve doğru şifre çözme algoritması ile doğru şifre çözme anahtarı kullanarak şifreyi çözer. Bu süreçte, şifrelenmiş veri orijinal düz metin haline dönüştürülür ve kullanılabilir hale gelir. Kriptografi, bu adımlarla verilerin gizliliğini, bütünlüğünü ve doğruluğunu koruyarak bilgi güvenliğini sağlar. Kriptografi genellikle Simetrik ve Asimetrik şifreleme olmak üzere iki ana kategoride gruplandırılır (Simmons, 1979). Simetrik şifreleme, aynı anahtarın hem şifreleme hem de deşifreleme işlemlerinde kullanıldığı bir sistemdir. Asimetrik şifreleme ise farklı bir yaklaşımdır. Burada, şifreleme ve deşifreleme için farklı anahtarlar kullanılır. Bu durumda, gönderen taraf bir genel (public) anahtarla metni şifreler ve şifrelenen metin yalnızca sahip olunan özel (private) anahtarla çözülebilir (singh ve diğ., 2024). Bu iki kategori ile beraber hibrit kriptografi de kullanılmaktadır (Priyadharsini & Thamizhmaran, 2023). Bu kriptografi türü, simetrik anahtarın hızı ile asimetrik anahtarın güvenliğini birleştirir. Kriptografik karma (hash) fonksiyonları ise veri bütünlüğünü sağlamak için kullanılır. Bu fonksiyonlar, verinin değiştirilmediğini ve bütünlüğünü koruduğunu doğrular.

Verinin güvenliğini sağlamak için geliştirilen teknolojilerin birincil amacı verinin gizliliğini sağlamak, bütünlüğünü korumak, kullanılabilirlik ve inkâr edilemezlik şartlarını yerine getirmektir. Kriptografi bu ilkelere ulaşmaya yardımcı olur. Kriptografik algoritmalar, iki varlık arasında veri ve bilgi aktarımı için güvenli bir kanal ve bağlantı kurulmasına yardımcı olur. Kriptografi, bilişim teknolojileri dünyasında sürekli gelişen bir alandır. Dijital teknolojinin kullanım alanlarının artması ve her şeyin dijitalleşmesiyle birlikte, veri güvenliği ve dolayısıyla kriptografi her zamankinden daha önemli hale gelmiştir.

2.2. Filigran Teknikleri

Filigran teknikleri; fotoğraf, video, ses ve belgeler gibi dijital varlıklara filigran işareti gizlemek için kullanılır. Filigran, dijital medyanın kendisi hakkında bilgi taşır ve genellikle medya sahibinin haklarını korumak veya medyanın kaynağını doğrulamak için kullanılır. Örneğin, bir fotoğrafın sahibi, fotoğrafın üzerine kendi adını veya bir logo şeklinde filigran ekleyerek mülkiyetini iddia edebilir. Bu teknik, dijital varlıkların izinsiz kopyalanmasını veya değiştirilmesini önlemeye yardımcı olur. Filigranlama, çeşitli kriterlere göre dört ana başlık altında sınıflandırılabilir. Birincisi, taşıyıcı veriye göre filigranlama olup, bu kategori, filigranın uygulandığı dijital medya türüne bağlı olarak sınıflandırılır; resim, ses, video ve yazı filigranlaması gibi. İkincisi, etki alanına göre filigranlama olup, filigranın uygulandığı veri alanına göre sınıflandırılır; uzamsal alan filigranlaması ve dönüşüm alanı filigranlaması gibi. Uzamsal alan filigranlaması, filigranın doğrudan medya verisinin uzamsal özelliklerine eklenmesi sürecidir, örneğin bir resmin piksellerine doğrudan filigran eklemek. Dönüşüm alanı filigranlaması ise, filigranın medya verisinin frekans veya başka bir dönüşüm alanında eklenmesi işlemidir ve genellikle daha sağlam ve gizli filigranlar oluşturur. Üçüncüsü, insan algısına göre filigranlama olup, filigranın insan tarafından algılanabilirliğine göre sınıflandırılır; görünür filigranlama ve görünmez filigranlama gibi. Görünür filigranlama, filigranın açıkça görülebildiği yöntemdir, örneğin bir fotoğrafın üzerine şeffaf bir logo eklemek. Görünmez filigranlama ise, filigranın insan gözüyle algılanamayacak şekilde eklenmesi işlemidir ve genellikle dijital veri analiz araçları ile tespit edilebilir. Son olarak, tersine çevrilebilirliğine göre filigranlama olup, filigranın medyadan geri çıkarılabilirliğine göre sınıflandırılır; tersine çevrilebilir filigranlama ve tersine çevrilemez filigranlama gibi. Tersine çevrilebilir filigranlama, filigranın orijinal medya verisini tamamen geri yüklemek mümkün olacak şekilde eklenmesi sürecidir ve özellikle tıbbi görüntüler veya hassas belgeler gibi orijinal verinin bozulmaması gereken durumlarda kullanılır. Tersine çevrilemez filigranlama ise, filigranın çıkarılamaz ve kalıcı olarak medyaya yerleştirildiği yöntemdir ve orijinal verinin filigran eklendikten sonra geri yüklenemeyeceği anlamına gelir. Şekil 2.3'de Filigran sınıflandırılması gösterilmiştir.



Şekil 2.3: Filigran Sınıflandırması.

(Kadian ve diğ., 2021)'den uyarlanmıştır.

Görünür filigranlama ayrıca sağlam ve kırılgan filigranlama olarak alt bölümlere ayrılabilir. Filigran, filigranlı içerik üzerinde yapılan herhangi bir yasadışı değişiklikten etkilenmediğinde, sağlam filigran olarak bilinir. Ancak, kırılgan bir filigran, birisi filigranlı veriyi yasadışı olarak değiştirmeye veya kurcalamaya çalışırsa yok olur. Yarı kırılgan filigranlar JPEG sıkıştırma gibi belirli görüntü işleme saldırılarına karşı toleranslıdır, ancak görüntü kırpma gibi diğer içerik değişikliklerine karşı hassastır. Görünür filigranlar, görünmez filigranların aksine bir insan gözü tarafından görülebilecek şekildedir ve algılanamaz ve sadece içeriğe bakılarak tespit edilemez.

Kırılgan filigranların varlığı, özellikle dijital varlıkların bütünlüğünün korunması gerektiği durumlarda önemlidir. Kırılgan filigranlar, bir dosyada herhangi bir değişiklik yapıldığında bu değişiklikleri tespit etmeye olanak tanır. Bu nedenle, kırılgan filigranlar, dijital verinin orijinalliğini ve bütünlüğünü korumak için kullanılır. Örneğin, resmî belgeler, tıbbi kayıtlar veya hassas bilgi içeren dosyalar gibi orijinal haliyle kalması gereken verilerde kırılgan filigranlar kullanılır. Bu tür filigranlar,

veride herhangi bir değişiklik yapılması durumunda hemen tespit edilerek veri bütünlüğünün bozulduğunu gösterir.

Sağlam filigranlar ise, dijital medyanın yetkisiz kullanımını ve dağıtımını önlemek için kullanılır. Sağlam filigranlar, çeşitli saldırılara ve manipülasyonlara karşı dayanıklıdır. Örneğin, ticari fotoğraflar, videolar ve müzik dosyaları gibi telif hakkına tabi olan dijital varlıklarda sağlam filigranlar tercih edilir. Bu filigranlar, medya dosyası üzerinde yapılan değişikliklere rağmen varlıklarını korur ve orijinal sahibinin haklarını savunur.

Bir örnek senaryo ile açıklamak gerekirse, bir şirket, önemli bir konferans sırasında tanıtım amaçlı olarak kullanılacak bir dizi dijital broşür hazırlamaktadır. Bu broşürlerin orijinal haliyle kalması ve herhangi bir değişikliğe uğramaması gerektiğinden, kırılgan filigranlar kullanılarak broşürlerin bütünlüğü korunur. Böylece, broşürler üzerinde yapılan herhangi bir değişiklik anında tespit edilerek orijinal belgelerin bozulmaması garanti altına alınır.

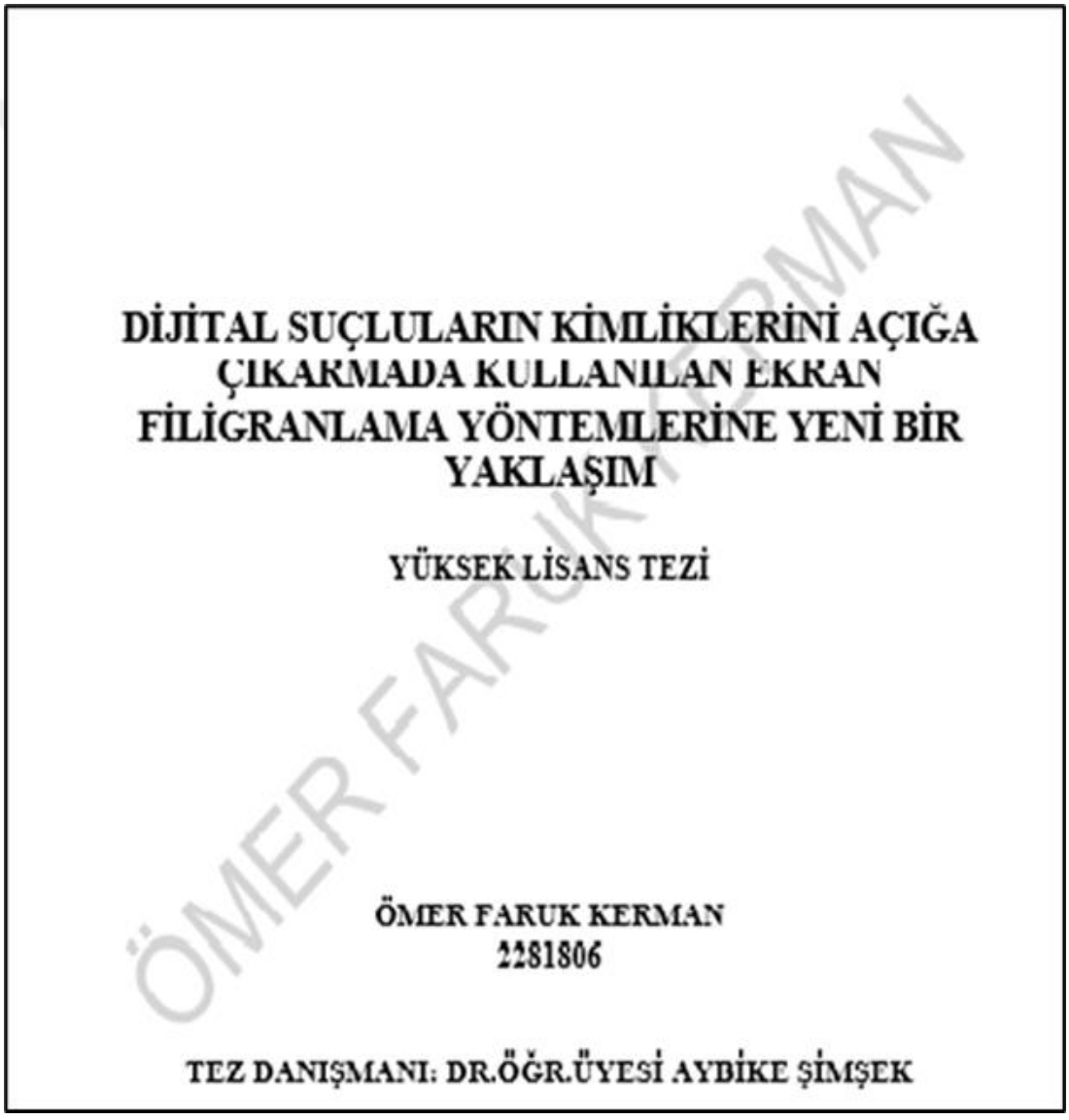
Öte yandan, bir fotoğrafçı, yüksek kaliteli fotoğraflarını çevrimiçi bir portföyde sergilemektedir. Bu fotoğrafların izinsiz kopyalanmasını ve dağıtılmasını önlemek için sağlam filigranlar kullanır. Sağlam filigranlar, fotoğraflar üzerinde yapılan değişikliklere rağmen varlıklarını korur ve fotoğrafçının haklarını savunur. Ayrıca, sağlam filigranlar sayesinde fotoğrafların kaynağı her zaman doğrulanabilir.

Sonuç olarak, hangi filigran türünün kullanılacağı, dijital varlıkların korunması gereken durumlara bağlıdır. Kırılgan filigranlar, veri bütünlüğünün korunması gerektiği durumlarda tercih edilirken, sağlam filigranlar, dijital varlıkların yetkisiz kullanımını ve dağıtımını önlemek için kullanılır. Her iki filigran türü de dijital medyanın güvenliğini sağlamak için önemli bir rol oynamaktadır.

Geliştirilen filigranlama sistemlerinde dikkat edilmesi gereken konulardan bazıları filigranlı görüntünün kalitesi, kasıtlı/kasıtsız saldırılara karşı sağlamlık, filigranın kapasitesi ve güvenliğidir. Filigranın sağlamlığını ve algılanamazlığını artırmak için, dijital filigranlama sistemlerinde dönüşüm alanı (Transform Domain, TD) tekniklerinin yanı sıra makine öğrenimi algoritmaları da kullanılmaktadır (Kadian ve diğ., 2021).

Temel olarak görünür filigran, orijinal görüntünün korunması için orjinal görüntüye uygulanan ikincil bir görüntüdür. Bu ikincil görüntü bir logo, metin veya desenler

olabilir. Orijinal görüntü üzerine eklenen bu ikincil görüntüler başkaları tarafından görülebilir. Filigranın opaklığı ayarlanabilir, daha az veya daha fazla görünür hale getirilebilir. Şekil 2.4'de gösterildiği gibi, "Ömer Faruk Kerman" şeklinde görünür bir filigran eklenmiştir. Bu filigran, şeklin merkezine yerleştirilmiş olup net bir şekilde okunabilmektedir. Görünür filigran, şeklin üzerine eklenerek görsel olarak dikkat çeker ve şeklin sahibini veya kaynağını belirlemek için kullanılır. Böylece, şeklin izinsiz kullanımı veya değiştirilmesi durumunda, orijinal sahibinin hakları korunur. Görünür filigran, genellikle şeffaf veya yarı şeffaf bir şekilde uygulanarak şeklin detaylarını tamamen örtmez, ancak kolayca fark edilebilir.



Şekil 2.4: Görünür Filigran Örneği.

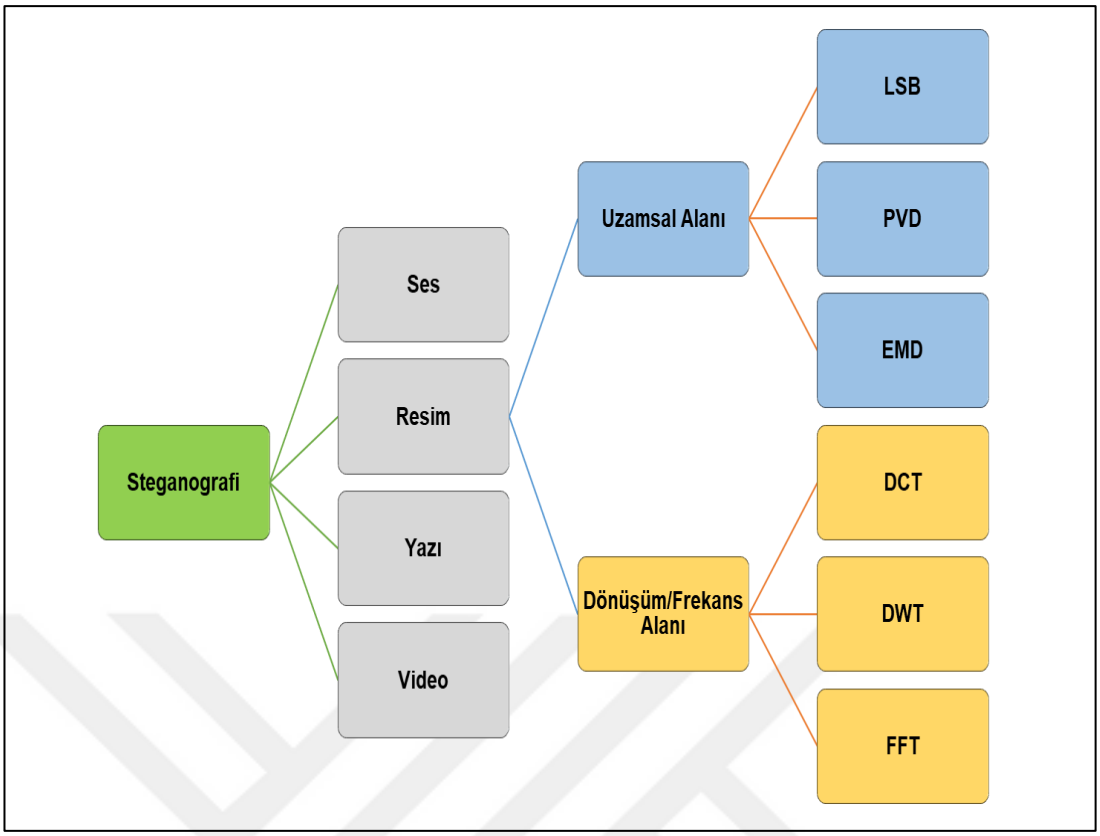
Öte yandan, görünmez filigranlamada filigran medyanın içinde gizlidir ve insan gözüyle algılanamaz, yalnızca özel algoritmalar veya yazılımlar kullanılarak tespit

edilebilir. Bu tür filigranlar, medya dosyasının kalitesini veya görünümünü etkilemeden bilgiyi gizlice saklamayı amaçlar. Filigranı gizlemek için steganografi teknikleri kullanılabilir. Bu teknikler, bir görüntünün, videonun veya ses dosyasının belirli bitlerine küçük değişiklikler yaparak filigranı saklar. Bu değişiklikler, medyanın orijinal kalitesini bozmadan bilgiyi gizler. Bu tür filigranlar, estetik, güvenlik, telif hakkı koruması ve izlenebilirlik gibi nedenlerle tercih edilir. Örneğin, sanat eserleri veya yüksek kaliteli videolar gibi estetik açıdan değerli medyalarda görünmez filigranlar kullanılır, çünkü bunlar medyanın görünümünü bozmaz. Ayrıca, medyanın izinsiz kopyalanmasını ve dağıtılmasını tespit etmek için kullanılırlar, çünkü filigran gizli olduğu için yetkisiz kişiler tarafından fark edilip çıkarılması zordur. Telif hakkı sahipleri, dijital medyanın yasal sahipliğini kanıtlamak için görünmez filigranlar kullanabilir ve bu filigranlar, medya dosyasının herhangi bir yerinde bulunabilir ve medya üzerinde yapılan değişikliklere rağmen varlıklarını korur. Dijital yayıncılık ve dağıtım platformlarında, medyanın hangi kullanıcılar tarafından indirildiği veya görüntülendiği takip edilebilir. Örneğin, bir film stüdyosu, yeni bir filmin ön gösterim kopyalarını dağıtırken her kopyaya görünmez bir filigran ekleyebilir. Bu filigranlar, filmin izinsiz olarak internete sızması durumunda hangi kopyanın sızdırıldığını belirlemeye yardımcı olur. Benzer şekilde, bir müzik yapımcısı, dijital müzik dosyalarına görünmez filigranlar ekleyerek, dosyaların izinsiz paylaşılması durumunda telif hakkı ihlallerini takip edebilir. Görünmez filigranlar, medya sahiplerine ek güvenlik ve izlenebilirlik sağlar.

Filigran teknikleri, dijital medyanın güvenliğini sağlamak, mülkiyet haklarını korumak ve izinsiz kullanımını önlemek için kritik öneme sahiptir ve bu teknikler, dijital dünyada güvenliği artırmak için sürekli olarak geliştirilmektedir.

2.3. Steganografi Teknikleri

Steganografi teknikleri, seçilen kaplama nesnesinin türüne, alan türüne (uzamsal veya dönüşüm/frekans alanı), kullanılan dosya formatının veya sıkıştırmanın türüne ve kaplama nesnesini değiştirmek için kullanılan gömme yönteminin türüne bağlı olarak birbirlerinden farklılık gösterebilir (Hoda ve diğ., 2014). Şekil 2.5'de görüntü steganografi tekniklerinin sınıflandırılması gösterilmektedir.



Şekil 2.5: Görüntü Steganografi Tekniklerinin Sınıflandırılması.

(Hoda ve diğ., 2014)'den uyarlanmıştır.

Bunlardan veri gizleme teknikleri içerisinde uzamsal ve dönüşüm/frekans alanı teknikleri en yaygın kullanılan yöntemlerdir. Uzamsal alan teknikleri, piksellerin yoğunluğunun bit düzeyinde manipülasyonunu ve gürültü manipülasyonunu içerir. Uzamsal alanda veri gömme için çeşitli yaklaşımlar mevcuttur. Bu yaklaşımlardan en küçük anlamlı bit (Least Significant Bit, LSB) değiştirme, piksel değeri farklılaştırma (Pixel Value Differencing, PVD), değişiklik yönlerinden yararlanma (Exploiting Modification Direction, EMD) gibi teknikler uzamsal alanda en çok tercih edilen yöntemlerdir.

En sık kullanılan ve en basit tekniklerden biri olan LSB yöntemi, kapak nesnesinin en az anlamlı bitlerini gizli mesajla değiştirme esasına dayanır. Bu yöntem, özellikle görüntüler üzerinde çalışırken sıklıkla kullanılır. Bunun nedeni insan gözü tarafından fark edilmesi zor olan küçük değişiklikler yapmasıdır. LSB'nin yüksek algısal şeffaflığı, bu yöntemin avantajlarından biridir. Ancak, teknik kayıplı sıkıştırma ve görüntü manipülasyonlarına (ölçekleme, döndürme, kırpma vb.) karşı hassastır. Bu nedenle, güvenlik ve dayanıklılık açısından dikkatli bir şekilde uygulanmalıdır.

Dönüşüm/frekans alanı teknikleri ise sıklık alanı teknikleri (Frequency Domain Techniques, FDT) olarak da bilinir ve görüntüyü uzamsal alandan frekans alanına dönüştürerek çalışır. Bu teknikler, veriyi matematiksel fonksiyonlar kullanarak gizler. Ayrık kosinüs dönüşümü (Discrete Cosine Transform, DCT), ayrık dalgacık dönüşümü (Discrete Wavelet Transform, DWT) ve hızlı Fourier dönüşümü (Fast Fourier Transform, FFT) gibi farklı frekans alanı yöntemleri, dönüşüm kullanılarak gizli veri gömme işlemlerinde yaygın olarak tercih edilir.

DCT (Discrete Cosine Transform) yöntemi, özellikle JPEG sıkıştırma algoritmasında kullanıldığı için yaygındır. Verinin sıkıştırılmış görüntülere gömülmesini sağlar. DWT (Discrete Wavelet Transform), görüntüyü farklı çözünürlük seviyelerine ayırarak veri gömme imkânı tanır ve sıkıştırma sonrası dayanıklılığı artırır. FFT (Fast Fourier Transform), frekans bileşenlerini analiz ederek veri gömme işlemi yapar ve genellikle ses ve görüntü verilerinde kullanılır.

Bu teknikler, veri gizleme konusunda sağlam ve güvenli çözümler sunar çünkü frekans alanında yapılan değişiklikler, uzamsal alandaki değişikliklere göre daha az fark edilebilir ve sıkıştırma, döndürme gibi işlemlere karşı daha dirençlidir. Ancak, bu yöntemlerin uygulanması daha karmaşıktır, bu nedenle de daha fazla hesaplama gücü gerektirir.

Sonuç olarak, uzamsal ve frekans alanı tekniklerinin birleşik kullanımı, veri gizleme süreçlerinde sağladığı basitlik ve dayanıklılık sayesinde geniş bir uygulama yelpazesi sunar. Uzamsal alan teknikleri, veriyi doğrudan medya içerisine ekleyerek basitlik sağlarken, frekans alanı teknikleri (örneğin, DCT veya DWT gibi) veriyi medyanın frekans bileşenleri aracılığıyla gizler. Bu kombinasyon hem veriyi gizlemeyi kolaylaştırır hem de medya üzerinde yapılan çeşitli saldırılara karşı dayanıklılığı artırır. Doğru ve dikkatli bir şekilde uygulandığında, bu teknikler veri güvenliği ve gizliliği açısından önemli bir katkı sağlar, çünkü filigranın algılanması zor olur ve verinin güvenliği korunmuş olur. Ancak, diğer filigranlama yöntemlerinin varlığı da önemlidir çünkü her biri belirli avantajlar sunar. Yöntem seçiminde esneklik sağlarlar; örneğin, belirli bir uygulama veya medya türü için daha uygun olan yöntemler tercih edilebilir. Güvenlik ve algılanabilirlik düzeyleri farklılık gösterir; görünür filigranlar medyanın üzerinde açıkça görülebilirken, görünmez filigranlar genellikle daha az algılanabilir olup daha güçlü bir koruma sağlayabilir. Ayrıca, uygulama senaryolarına göre değişen gereksinimlere göre optimize edilmiş avantajları ve dezavantajları vardır.

Bu çeşitlilik, filigranlama tekniklerinin uygulama alanlarını genişletir ve her birinin belirli koşullarda en iyi performansı göstermesini sağlar. Dolayısıyla, doğru yöntemin seçilmesi, veri güvenliği ve gizliliği açısından kritik bir adımdır.

2.4. Steganografi ve Filigranlamanın Karşılaştırılması

Filigranlama, steganografi ile yakından ilişkilidir; ancak ikisi arasında bazı farklar vardır. Filigranlama esas olarak görüntünün kimlik doğrulamasıyla ilgilenirken, steganografi verilerin gizlenmesiyle ilgilenir. Gömülü filigran mesajları genellikle telif hakkı gibi ana görüntü bilgileriyle ilgilidir ve bu nedenle kapak görüntüsüne bağlanırlar. Filigran, kapak görüntüsüne eklenen gizli bilgilerin varlığından haberdar olan ve bu bilgileri kaldırmak isteyebilecek kullanıcılar için kullanılır. Steganografideki gizli mesajlar ise genellikle ana görüntü ile ilgili değildir. Bu mesajlar, önemli bilgilerin kötü niyetli kişiler tarafından algılanamaması için tasarlanmıştır. Filigranlamada, gömülü bilgi görüntünün bir niteliği ile ilgilidir ve görüntü hakkında ek bilgi veya özellikler iletir. Burada asıl önemli olan şey, görüntünün kendisidir. Steganografide ise gömülü mesajın görüntü ile hiçbir ilgisi yoktur; görüntü sadece mesajı iletmek için bir araç olarak kullanılır. Steganografide önemli olan şey, iletilmek istenen gizli mesajdır.

Filigran uygulamasında, görüntü algısal kalitesi yani izleyicinin gözünde görüntünün ne kadar iyi göründüğü ve sağlamlık yani filigranın silinmeden veya bozulmadan kalabilmesi arasında bir denge sağlanır. Örneğin, filigran eklerken görüntünün çözünürlüğü düşebilir veya renkleri bozulabilir. Bu tür kısıtlamalar, gömülen bilginin kapasitesini azaltma eğilimindedir. Steganografi uygulamasında ise durum farklıdır; burada gizli mesajın aktarımı esastır ve gizli bilgiyi saklama kapasitesi yani mesajın boyutu, genellikle sağlamlık ve görüntü kalitesi kadar önemlidir. Steganografide görüntü kalitesi önemli olsa da, mesajın algılanmadan saklanabilmesi daha kritik bir önceliktir.

Dolaysıyla steganografi ve filigranlama, farklı amaçlar için kullanılan iki ayrı gizleme teknolojisidir. Her iki yöntem de verilerin gizlenmesi ile ilgilenir; ancak kullanım amaçları ve yöntemleri bakımından önemli farklılıklar gösterirler. Steganografi, verinin gizliliğini koruma amacına hizmet eder. Steganografinin temel amacı, gizli bilgiyi görünmez hale getirerek yetkisiz erişimi engellemektir. Bu sayede verilerin üçüncü şahıslar tarafından tespit edilmesini zorlaştırır ve böylece veri güvenliğini

sağlar. Filigranlama ise belgelerin veya içeriğin sahipliğini doğrulamak ve özellikle telif hakkı koruması ve sahteciliği önlemek için kullanılır. Bir içerik, izinsiz olarak kullanıldığında veya çoğaltıldığında, içindeki filigran sayesinde orijinal sahibine ait olduğu kolayca kanıtlanabilir.

Bu iki kavramın karşılaştırmalı bilgileri, Tablo 2.1'de ayrıntılı olarak sunulmuştur. Bu tablo, steganografi ve filigranlamanın kullanım amaçlarını ve yöntemlerini karşılaştırarak, her iki teknolojinin de farklı ihtiyaçlara nasıl cevap verdiğini göstermektedir.

Tablo 2.1: Steganografi ve Filigranlamanın Karşılaştırılması.

Özellik	**Steganografi**	**Filigranlama**
Amaç	İletişimi gizli tutmak	Mülkiyeti doğrulamak
Gizli Veri	Gözetimsiz olarak gizli taşınır	Bilinçli veya bilinçsiz olarak taşınır
Başarısızlık Senaryosu	Gizli mesajın tespit edilmesi	Filigranın kaldırılması veya değiştirilmesi
Çıktı/Sonuç	Gizli mesajı içeren Stego dosyası	Gömülü veya görünmez filigran dosyası
Sahiplik	Sahipliği doğrulamaz	Sahipliği doğrular
Dayanıklılık	Dayanıklılık ön planda değildir	Dayanıklılık korunması gereken esas amaçtır

Tabloda gösterildiği gibi Steganografi, gizli mesajın tespit edilemezliğini sağlamaya odaklanır. Steganografide gizli veri, bir taşıyıcı ile birlikte denetimsiz olarak taşınır ve Stego dosyası şeklinde bir çıktı üretir. Steganografi aracılığıyla mesajın kimden geldiğini ya da hangi kuruma ait olduğunu belirlemek mümkün değildir. Ayrıca, gizli mesaj tespit edilirse steganografi başarısız sayılır. Öte yandan filigranlama, içeriğe filigran olarak isimlendirilen gizlenmiş veri ekleyerek sahipliğin doğrulanmasını amaçlar. Filigran görünür ya da görünmez olabilir ve şirket logosu ya da sahiplik bilgileri gibi mülkiyet bilgilerini içerebilir. Filigranlama, filigranlı bir dosya ile sonuçlanır ve filigranın kaldırılması veya değiştirilmesi bir başarısızlık olarak kabul edilir.

Filigranlama, içerik sahipliğinin doğrulanması için kullanılan bir teknolojidir ve filigranlı içeriğin, izinsiz kopyalanma, değiştirilme, yeniden boyutlandırılma ve sıkıştırılma gibi çeşitli saldırılara karşı dayanıklı olması gerekmektedir. Steganografi ise verilerin gizliliği ve güvenliği ön planda olduğu durumlarda tercih edilir. Sonuç olarak, steganografi aktarılan verinin güvenliği ön planda olduğu durumlarda tercih edilirken, filigranlama içerik sahipliğinin doğrulanması gerektiğinde kullanılır.

2.5. Literatür İncelemesi

Bu literatür taraması, steganografi, filigranlama ve kriptografi teknolojilerinin bir araya getirilmesiyle geliştirilen ekran filigranlama yöntemlerinin önemini vurgulamaktadır. Bu teknikler, hassas bilgilerin gizliliğini korumak ve veri sahipliğini doğrulamak için yaygın olarak kullanılmaktadır. Steganografi yöntemleri, verinin gizliliğini sağlamak amacıyla içeriği diğer veri taşıyıcılarının içine gizlice gömerek kullanılır. Bu yöntem, gizli mesajın varlığını tespit edilmeden saklamayı hedefler. Filigranlama ise içeriğe benzersiz tanımlayıcılar ekleyerek sahipliği doğrular ve izlenebilirlik sağlar. İçeriğin izinsiz kullanımı durumunda, filigranın varlığı orijinal sahibin kimliğini kanıtlamak için kullanılabilir. Kriptografi ise verilerin güvenli bir şekilde şifrelenmesini ve iletilmesini kolaylaştırır. Bu yöntem, bilgilerin yetkisiz erişimden korunmasına yardımcı olur ve güvenli veri iletişimini sağlar. Bu çalışma steganografi, filigranlama ve kriptografi gibi teknolojilerin ekran filigranı alanına nasıl entegre edildiğini açıklamakta ve veri güvenliğine katkılarını ortaya koymaktadır.

2.5.1. Bilgi Gizlemede Kullanılan Yöntemler

Günümüz dünyasında veri gizleme giderek artan bir önem kazanmaktadır. Bilgi çağının hızla ilerlemesiyle birlikte, özel ve hassas verilerin korunması önemli bir gereklilik haline gelmiştir. Bu bağlamda, filigranlama, şifreleme (kriptografi) ve steganografi gibi yöntemler veri güvenliğini sağlamak ve yetkisiz erişime karşı koruma sağlamak için önemli araçlar olarak öne çıkmaktadır. Filigranlama, içeriğin sahipliğini doğrulamak ve izlenebilirlik sağlamak amacıyla kullanılırken; kriptografi, verilerin güvenli bir şekilde şifrelenmesini ve iletilmesini sağlar. Steganografi ise verileri diğer veri taşıyıcılarına gizlice gömerek iletişim gizliliğini korur. Bu yöntemler veri bütünlüğünü ve güvenliğini korumak için son derece etkili ve pratiktir.

Filigranlama öncelikle belgelere tanınabilir bir görüntü veya desen gömülerek tanımlama sağlar. Bunu sağlayabilmek için bir ortama benzersiz bir bilgi parçasını, ortamın fark edilir şekilde değişmesine neden olmadan eklenmesi gerekir. Bu yöntem, kimlik kartları, pasaportlar, banknotlar ve diğer güvenlik belgelerinde sahteciliği ve değişiklikleri önlemek için kullanılır. Dijital filigranlar, dijital hakların korunmasına yardımcı olur ve verilerin izlenmesine ve tespit edilmesine olanak sağlayarak sahipliği doğrular.

Şifreleme (kriptografi) verileri anlaşılmaz bir biçime dönüştürerek gizlilik, bütünlük, kimlik doğrulama ve inkâr etmeme gibi temel özellikler sunar. Şifrelenmiş veriler yetkisiz erişime karşı korunarak veri güvenliğini sağlar ve sadece doğru anahtarla deşifre edilebilir.

Steganografi ise mesajların, dosyaların veya görüntülerin diğer mesajlar, dosyalar veya görüntüler içinde gizlenmesini sağlayan bir yöntemdir. Bu yöntem, gizli mesajı dışarıdan normal bit görüntü veya dosya gibi gösterirken içinde verileri gizler. Bu sayede veriler yetkisiz taraflarca tespit edilmeden iletilir.

Dijital bir görüntü oluşturulurken, görüntü sahibini tanımlayan bilgileri içeren bir filigran eklenmesi mümkündür. Bu, görüntünün veri içeriğini steganografik yöntemlerle manipüle ederek yapılır ve sonuç olarak görüntünün kendisi değişmeden sahibine ait veriler korunur. Dijital görüntüyü elde eden diğer kişiler, içinde ek bilgi olduğunu görsel olarak tespit edemezler. Bu yöntem, izinsiz kullanım durumunda görüntü sahibini belirlemek için kullanılabilir. Filigran genellikle telif hakkıyla korunan dijital medyayı korumak için kullanılır. Steganografi bireysel gizliliği artırabilir; ancak şifreleme ile aynı işlevi yerine getiremez, özel iletişim için bir yöntem sunar. Fakat bu yöntem sadece gizli iletişim tespit edilmediği sürece etkilidir. Eğer bir kişi kurumun izleme sistemlerine maruz kalmadan iletişim kurmak istiyorsa, o zaman dijital steganografi iyi bir çözümdür.

Filigranlama, şifreleme ve steganografi gibi üç yöntem, veri korumasında daha yüksek bir güvenlik seviyesi sağlamak için birleştirilebilir (R. Gupta ve diğ., 2014). Örneğin, mesajlar önce şifrelenerek anlaşılmaz bir formatta çevrilir. Daha sonra, bu şifrelenmiş metin bir örtü ortamına steganografi yöntemleri ile gömülebilir. Bu bütünleşik yaklaşım, veri gizleme süreçlerinde güvenlik, kapasite ve dayanıklılık hedeflerini başarıyla karşılar. Bu yöntemler, hassa verilerin korunmasında ve yetkisiz erişimle

mücadelede önemli rol oynamaktadır. Teknolojinin ilerlemesi ile birlikte, veri koruma ihtiyacı da artmaktadır. Dolaysıyla, filigranlama, şifreleme ve steganografi gibi teknikler, güvenlik açısından kritik öneme sahip araçlar haline gelmiştir.

2.5.2. Filigranlamada Kullanılan Yöntemler

Bu kısımda, araştırmanın temelini oluşturan konuyla ilgili literatürün kapsamlı bir incelemesi sunulmaktadır. Çalışmanın odaklandığı konu çerçevesinde yapılan akademik çalışmalar, önceki araştırmaların sonuçları ve bu alandaki önemli teorik yaklaşımlar ele alınmıştır. Bu kapsamda yapılan çalışmalarda; Guan ve arkadaşları, ekran çekimine dayanıklı görüntü filigranlama (Secreen Shooting Resilience Image Watermarking, SSRIW) algoritmalarının kapsamlı bir incelemesini sunularak bu alanda daha fazla araştırma yapılması gerektiğini vurgulamıştır (Guan ve diğ., 2023). Bu konudaki tartışma, baskı-tarama ve ekran-çekim saldırılarına karşı dayanıklı bir teknik oluşturmanın zorluğu Xie ve arkadaşları tarafından metin filigranlama konusuna doğru genişletilmiştir (Xie ve diğ., 2019). Dayanıklı resim ve metin filigranlama için kullanılan özel yöntemler ise sırasıyla (Shimpi & Gumaste, 2015) ve (Yakushev ve diğ., 2021) tarafından ileri sürülmüştür. Yakushev'in yöntemi, ekran kamerası saldırılarına karşı koruma sağlamak için filigranları metindeki görüntü satır aralığına entegre ederken, Shimpi'nin ayrık dalgacık dönüşümü (DWT) tabanlı çözümü ise lokal senkronizasyon bozma saldırılarına karşı dayanıklı olacak şekilde geliştirilmiştir.

Bir başka araştırmada, görüntü filigranlamanın konvolüsyonel sinir ağları (Convolutional Neural Network, CNN) kullanılarak nasıl güçlendirilebileceğine ve çeşitli saldırılara karşı ne derece savunmasız olduğuna odaklanmıştır (Singh & Singh, 2024). Geometrik değişiklikler, sıkıştırma ve sinyal işleme dahil olmak üzere filigran bütünlüğünü tehlikeye atabilecek yaygın saldırılara genel bir bakış sunulmuştur. Swati G. ve diğ. (S. Gupta ve diğ., 2019), tersine çevrilebilir filigranlama yaklaşımlarına odaklanıp dört kategoriye ayrılan çeşitli yöntemlerin bir karşılaştırmasını sunarak güncel araştırmaları analiz etmiştir. Filigranların değiştirilmiş alanlarının tespit edilmesinin zor olduğu ortaya konmuş olsa da blok bağımlılığına sahip tekil değer ayrıştırma (Singular Value Decomposition, SVD) tabanlı kırılgan filigranlamanın, özellikle tıbbi resim güvenliğinde önemli bir yere sahip olduğu ortaya konmuştur. Bu çalışma, görsel güvenliği için geri döndürülebilir filigranlama algoritmalarına,

kapsamlı incelemeler ve karşılaştırmalı değerlendirmeler de dahil olmak üzere ayrıntılı bir genel bakış sunmaktadır.

Diğer bir incelemeye göre, filigranlamada en yaygın yöntem, filigranı kaplama nesnesinin en az anlamlı bitlerine (Least Significant Bit, LSB) gömmektir (Jain1 & Johari2, 2014). LSB yöntemi, kırpma, istenmeyen gürültü ekleme veya kayıplı sıkıştırma gibi dönüşümlere karşı dayanıklı olsa da her pikselin LSB bitlerini bire ayarlayabilen daha sofistike bir saldırı, kaplama nesnesi üzerinde önemsiz bir etki ile filigranı tamamen yok edebilir. Sonuç olarak algoritması bilinen bir yöntem kolayca değiştirilebilir. Geleneksel LSB yöntemine göre daha sofistike bir yaklaşım ise, belirli bir anahtara dayalı, filigran gömmek için kullanılacak pikselleri belirleyen rastgele sayı üreteci kullanmak olduğu ortaya atılmış olsa da bu algoritma LSB'lerin sabit bir değerle değiştirilmesine karşı hala savunmasızdır. Diğer bir incelemede ise, multimedya dosyalarının yasadışı kullanımdan korunmasında görünür ve görünmez filigran tekniklerinin kullanışlılığı vurgulanmaktadır (Chopra, 2012). Görsel kaliteden ödün vermeden bir sinyalin medyaya nasıl gömüleceğinden bahsedilmekte ve pikselleri en az anlamlı bitleriyle değiştiren LSB tekniğine vurgu yapılmaktadır. Kendilerine göre, veri güvenliğini ve görüntü bütünlüğünü garanti altına almak için doğru filigran tekniğini seçmek hala zordur. Geometrik bozulmaya direnmek için yoğunluk tabanlı ölçekle değişmeyen özellik dönüşümü (Improved-Scale-Invariant Feature Transform, I-SIFT) algoritması ve filigranı farklı bölgelere gömmek için küçük boyutlu bir şablon algoritması kullanan bir şema önermiştir (Fang ve diğ., 2019). Li ve arkadaşları, özellik bölgesi filtreleme modelini SuperPoint (Feature Region Filtering System, FRFS) sinir ağları, kuaterniyon ayrık Fourier dönüşümü (Quantized Discrete Fourier Transform, QDFT) ve tensör ayrıştırması (Tensor Decomposition, TD) ile birleştirerek bu yaklaşımı daha da geliştirmiştir (Li ve diğ., 2021).

Chen ve arkadaşları, özellik tabanlı bir senkronizasyon yöntemiyle sağlam bir filigranlama şeması geliştirerek ekran kamerası sürecine odaklanmıştır (Chen ve diğ., 2020). Bilgi gömme ve otomatik tanıma için nokta matris desenlerine dayalı bir yöntem önermiş, güçlü sağlamlık ve yüksek çıkarma verimliliği göstermiştir (Kang ve diğ., 2023). Bai ve arkadaşları çalışmalarında, frekans alanında Ayrık Dalgacık Dönüşümü (Discrete Wavelet Transform, DWT) ve Tekil Değer Ayrışımı (Singular Value Decomposition, SVD) ile Yönlendirilmiş FAST (Features from Accelerated

Segment Test) ve Döndürülmüş BRIEF (Binary Robust Independent Elementary Features) (Oriented FAST and Rotated BRIEF, ORB) özellik noktaları entegre edilerek, ekran görüntüsü fotoğrafları için hızlı ve güvenilir bir filigranlama tekniği sunmuşlardır (Y. Bai ve diğ., 2023). Bu yaklaşımla, özellik noktalarını hızlı bir şekilde bulmak ve filigranı çok çözünürlüklü bir alana gömerek sağlamlığı artırmak hedeflenmiştir. Algoritmanın dayanıklılık, kapasite ve zamansal karmaşıklık açısından mevcut yaklaşımlara göre üstünlüğü deneysel bulgularla gösterilmiştir.

Nikolaidis ve Pitas kullandığı yöntem ile "görünmez" bir sinyalin resmin içine gizlendiği dijital filigranlama yoluyla telif hakkı koruması sunmuştur (Nikolaidis & Pitas, 1998). Bu yöntem, rastgele seçilen piksellerin uzamsal alan yoğunluğunun değiştirilmesiyle gerçekleştirilmiştir. Filigran sinyalinin yüksek frekanslardaki enerji içeriğini azaltarak ve insan görsel sisteminin özelliklerini dikkate alarak, filigran JPEG (Joint photographic Experts Group) sıkıştırmasına ve alçak geçiş filtrelemesine dayanıklı olacak şekilde yerleştirilmiştir. Önerilen tekniklerin etkinliği, gerçek fotoğraflar üzerinde yapılan ve yaygın görüntü değişikliklerine karşı dayanıklı, sağlam ve göze çarpmayan filigranları gömmek için nasıl kullanılabileceklerini gösteren deneylerle doğrulanmıştır. Cox ve arkadaşları, filigranın bağımsız ve özdeş dağılımlı Gauss rastgele vektörü (Gaussian Random Vector, GRV) olarak tasarlanmasını önermektedir (Cox ve diğ., 1997). Bu tekniğinin kayıplı sıkıştırma, filtreleme, dijital-analog ve analog-dijital dönüştürme, yeniden niceleme ve kırpma, ölçekleme, öteleme ve döndürme gibi yaygın geometrik dönüşümler gibi çeşitli sinyal işleme işlemlerine karşı dayanıklı olduğu savunulmuştur. Bu sağlamlığın, tespit sırasında dönüştürülmüş filigranlı görüntü ile karşılaştırma için orijinal görüntünün mevcut olmasına bağlı olduğu vurgulanmaktadır.

Zhou ve arkadaşları çalışmalarında, adli bilişim alanında dijital filigranlama üzerine yapılan kapsamlı araştırmaları özetlemiştir (Zhou & Lv, 2011). Bu, aktif ve pasif adli bilişim yöntemleri arasında bir karşılaştırmanın yanı sıra hem sağlam hem de kırılgan filigran algoritmalarının adli bilişim senaryolarında uygulanmasını içermektedir. Adli Bilişim bağlamında dijital filigranlama tekniklerinin etkinliğini, güvenilirliğini veya uygulanabilirliğini artırmayı amaçlamışlardır. Başka bir incelemede, akıllı telefonlar aracılığıyla önemli bilgilerin kötü niyetli bir şekilde fotoğraflanarak sızdırılmasını önlemek amacıyla özel olarak tasarlanmış bir filigranlama tekniği önerilmiştir (Gu ve diğ., 2022). Önerilen yöntemde, filigran gömme bölgesi seçiminde yoğunluk tabanlı

ölçekle değişmeyen özellik dönüşümü (Scale-invariant feature transform, SIFT) algoritması kullanılarak özellik bölgeleri oluşturulmuştur. Bu yaklaşım, filigranın görüntünün ana içeriğine daha fazla odaklanmasını sağlayarak filigranın etkinliğinin artırılması sağlanmıştır. Filigran gömme kuvveti için Sadece Fark Edilebilir Değişiklik (Just Noticeable Difference, JND) modeli kullanılarak filigran gömme yoğunluğu sınırlandırılarak görüntünün parlaklığı ve dokusu dikkate alınıp uygulanmış ve filigranın dayanıklılığı ile görünmezliği arasında bir denge kurulmuştur.

Gohshi ve arkadaşlarının incelemesinde, dijital teknolojilerin ilerlemesiyle içerik oluşturmanın kolaylaştığını ancak aynı zamanda yasa dışı kopyalamayı da mümkün kıldığını vurgulamaktadır (Gohshi ve diğ., 2005). Dijital Hak Yönetimi (Digital Rights Management, DRM) gibi yöntemler içeriği şifrelerken, ekran tekrar çekimlerine karşı koruma sağlamadığından, çalışmalarında öncelikle ticari kameraların özellikleri detaylıca incelenmiş ve deneylerle orijinal ve tekrar çekilmiş görüntüler arasındaki farklar gözler önüne serilmiştir. Sonuç olarak, ekran tekrar çekimlerine karşı dayanıklı bir filigranlama yöntemi önererek filigran gömme ve çıkarma süreçleri detaylıca açıklanmıştır. Başka bir çalışmada, dijital görüntüler için etkili, güvenli ve görünmez bir filigranlama tekniği geliştirmek ve böylece filigranlanmış görüntünün kalitesini artırmak amacıyla, dijital görüntüleri dalgacık dönüşümleri kullanılarak filigranlanma yöntemi kullanılmıştır (Author ve diğ., 2013). Bu filigranlama tekniğinin etkinliği, filigranlı görüntünün Piksel Sinyal Gürültü Oranı (Peak Signal-to-Noise Ratio, PSNR) ile doğrulanmış ve orijinal görüntü ile filigranlı görüntünün insan gözlemciler tarafından görsel olarak ayırt edilemez olduğunu göstermiştir. Bu araştırmalardan her biri, dijital varlıklarınızı korumak için güçlü filigranlama yöntemleri oluşturmanın ne kadar önemli olduğunu vurgulamaktadır. Bu araştırmaların özeti Tablo 2.2'de sunulmuştur.

Tablo 2.2: İncelenen Filigranlama Yöntemlerinin Özeti.

Yazar	Çalışma	Yöntem/Algoritma	Bulgular
Cox ve diğ. (1997)	Filigranın GRV olarak tasarlanması	GRV	Yaygın geometrik dönüşümlere karşı dayanıklılık sağlanmıştır.
Nikolaidis & Pitas (1998)	Görünmez sinyali resme gizleyerek telif hakkı koruması	Rastgele Seçilen Piksel Yoğunluğu	JPEG sıkıştırması ve alçak geçiş filtrelemesine karşı dayanıklı filigran oluşturulmuştur.
Gohshi ve diğ. (2005)	Ticari kameralarla ekran tekrar çekimlerine karşı dayanıklı filigranlama yöntemi	Ticari Kamera Analizi, Filigran Gömme ve Çıkarma	Ekran tekrar çekimlerine karşı dayanıklı filigranlama yöntemi önerilmiştir.

Tablo 2.2 - devam.

Yazar	Çalışma	Yöntem/Algoritma	Bulgular
Zhou & Lv (2011)	Adli bilişimde dijital filigranlama araştırmaları	Aktif ve Pasif Adli Bilişim	Adli bilişim senaryolarında filigranlama tekniklerinin etkinliği incelenmiştir.
Chopra (2012)	Görünür ve görünmez filigranlama tekniklerinin kullanışlılığı	LSB, SIFT	LSB tekniği ile veri güvenliği ve görüntü bütünlüğü sağlanması zor olmuştur.
Author ve diğ. (2013)	Dalgacık dönüşümleri kullanarak dijital görüntüler için filigranlama	Dalgacık Dönüşümleri	Filigranlanmış görüntünün kalitesi artırılmış ve PSNR ile doğrulanmıştır.
Jain & Johari (2014)	En az anlamlı bitlere (LSB) dayalı filigranlama	LSB	LSB yönteminin dönüşümlere dayanıklı olduğu, ancak sofistike saldırılara karşı savunmasız olduğu ortaya konmuştur.
Shimpi & Gumaste (2015)	Ayrık Dalgacık Dönüşümü (DWT) tabanlı filigranlama	DWT	Lokal senkronizasyon bozma saldırılarına karşı dayanıklı bir çözüm sunulmuştur.
Fang ve diğ. (2019)	I-SIFT ve şablon algoritması kullanarak filigran gömme	I-SIFT	Görsel kaliteden ödün vermeden filigranın gömülmesi sağlanmıştır.
Xie ve diğ. (2019)	Metin filigranlama teknikleri	Metin Filigranlama	Baskı-tarama ve ekran-çekim saldırılarına karşı dayanıklı tekniklerin oluşturulmasının zorluğu tartışılmıştır.
Gupta ve diğ. (2019)	Tersine çevrilebilir filigranlama yöntemlerinin karşılaştırılması	Tekil Değer Ayrıştırma (SVD)	Blok bağımlılığına sahip SVD tabanlı kırılgan filigranlamanın tıbbi resim güvenliğinde önemli olduğu gösterilmiştir.
Chen ve diğ. (2020)	Ekran kamerası sürecine odaklanan filigranlama	Özellik Tabanlı Senkronizasyon	Güçlü sağlamlık ve yüksek çıkarma verimliliği gösterilmiştir.
Yakushev ve diğ. (2021)	Metin aralığına entegre edilmiş filigranlar	Görüntü Satır Aralığına Filigran	Ekran kamerası saldırılarına karşı koruma sağlanmıştır.
Li ve diğ. (2021)	FRFS, QDFT ve TD ile geliştirilmiş filigranlama	SuperPoint, QDFT, TD	Dayanıklılık ve çıkarma verimliliği artırılmıştır.
Gu ve diğ. (2022)	Akıllı telefonlar aracılığıyla kötü niyetli fotoğraf çekimini önlemeye yönelik filigranlama	SIFT, JND	Filigranın etkinliği artırılmış ve görünmezlik sağlanmıştır.
Guan ve diğ. (2023)	Ekran çekimine dayanıklı görüntü filigranlama (SSRIW) algoritmalarının kapsamlı incelemesi	SSRIW	Ekran çekim saldırılarına karşı daha fazla araştırma yapılması gerektiği vurgulanmıştır.
Bai ve diğ. (2023)	DWT ve SVD ile ORB özellik noktaları kullanarak filigranlama	DWT, SVD, ORB	Ekran görüntüsü fotoğrafları için hızlı ve güvenilir filigranlama sağlanmıştır.
Singh & Singh (2024)	Konvolüsyonel Sinir Ağları (CNN) kullanarak görüntü filigranlama	CNN	Geometrik değişiklikler, sıkıştırma ve sinyal işlemenin filigran bütünlüğüne etkisi incelenmiştir.

Dijital görüntü filigranlamanın güvenliği ve dayanıklılığını artırmak amacıyla önerilen yöntem, görüntünün anahtar noktalarını tespit etmek için yoğunluk tabanlı ölçekle değişmeyen özellik dönüşümü (Scale-invariant feature transform, SIFT) algoritması

kullanılacak ve bu noktalar üzerinde filigran gömme işlemi gerçekleştirilecektir. Bu yöntemin temelinde, filigranların belirli anahtar noktalara gömülmesi ve kuaterniyon ayrık Fourier dönüşümü (Quantized Discrete Fourier Transform, QDFT) ile tensör ayrıştırması (Tensor Decomposition, TD) tekniklerinin kullanılması yatmaktadır.

Anahtar noktalara dayalı filigranlama, görüntünün önemli bölgelerine odaklanarak filigranın etkili bir şekilde gizlenmesini ve dayanıklılığını sağlamayı hedeflemektedir. Yoğunluk tabanlı ölçekle değişmeyen özellik dönüşümü (Scale-invariant feature transform, SIFT) algoritması, görüntünün özellik noktalarını belirlemede yüksek doğruluk sağladığından, filigranın bu noktalara gömülmesi güvenilir bir çözüm sunmaktadır. Filigran gömme işleminin tensör ayrıştırması (Tensor Decomposition, TD) kullanılarak yapılması, filigranın görüntüde daha homojen bir şekilde dağıtılmasını ve geometrik bozulmalara karşı daha dirençli olmasını sağlamaktadır.

Önerilen yöntemin etkinliği, çeşitli saldırılara karşı yapılan testlerle doğrulanmıştır. Filigran gömme ve çıkarma süreçleri sırasında, görüntünün anahtar noktalarının korunması ve filigranın bu noktalara entegre edilmesi, filigranın görünmezliğini artırmakta ve saldırılara karşı dayanıklılığını güçlendirmektedir. Bu yöntem hem filigranın etkinliğini artırmakta hem de görüntü kalitesini korumaktadır. Böylece önerilen yöntem, dijital varlıkların korunmasında etkili ve güvenilir bir araç olarak kullanılabilir.

3. ÖNERİLEN YÖNTEM İÇİN EKRAN FİLİGRANI SEÇİMİ

Filigranlama yöntemleri çoklu ortam dosyalarına veya metin belgelerine uygulanmasına göre iki kategori altında toplanabilir. Ekranlarda görüntülenen metin tabanlı filigranların görünmez olması ve metnin görsellerine sorunsuz bir şekilde entegre edilmesi gerekir. Bu tip görüntüler için temel yaklaşımlar, filigranları piksel değerlerinin en az anlamlı bitlerine yerleştirmeyi (Bender ve diğ., 1996; Nikolaidis & Pitas, 1998; Van Schyndel ve diğ., 1994) ve algılanamayan renk değişikliklerini kullanmayı içerir. Ancak, masa üstü kameralar, bağımsız dijital veya analog kameralar veya akıllı telefon kameraları gibi cihazların bu değişiklikleri yakalama kabiliyeti konusunda endişeler ortaya çıkmaktadır. Alternatif bir yöntem (Caronni, 1995) bitişik piksellerin parlaklığını değiştirerek filigranları kodlamaktır. Bu yöntemde, filigranın geri alınabilmesi için orijinal görüntünün bulunması şarttır, çünkü orijinal ve filigranlı görüntüler arasındaki parlaklık farkı kullanılarak filigran geri elde edilebilmektedir. Bu yöntem, orijinal görüntünün her zaman erişilebilir olmasını gerektirir, aksi takdirde filigranı geri almak imkânsız hale gelir. Bu yöntemin aksine, bizim yaklaşımımız filigranın geri alınması için orijinal görüntünün varlığını gerektirmez. Bu sayede, orijinal görüntüye erişim olmadığında bile filigranlı veriyi doğrulamak mümkün olur.

Birçok çoklu ortam filigran tekniği, görüntülerin frekans spektrumu gibi dönüştürülmüş alanlarında çalışır (Cox ve diğ., 1997; Shieh ve diğ., 2004; Tsui ve diğ., 2008) ve insanlar tarafından tespit edilmesi zor olan ince değişikliklere izin verir. Ancak, genellikle bu filigranlar metin belgelerinde fark edilebilir (Alattar & Alattar, 2004). Bu nedenle, frekans alanlı filigranlama önerdiğimiz yöntem için çok uygun değildir. Bizim yaklaşımımıza benzer şekilde, yazıcı teknolojisi de yarı-steganografik teknikler kullanarak çıktı üzerinde görünmez sarı noktalarla baskı ayrıntılarını gizler (Embar ve diğ., 2014). Bizim önerdiğimiz yöntem, bilgisayar ekranındaki bir filigranın içine bilgi gizleyerek yazıcı teknolojisinde kullanılan mantığı takip eder. Literatür incelemesi göz önünde bulundurulduğunda, mevcut çalışmalar üç yöntem üzerinde yoğunlaşmaktadır. Bu üç farklı yöntemin temel özellikleri ve uygulamaları incelenmiş, her birinin avantajları ve sınırlamaları ele alınmıştır.

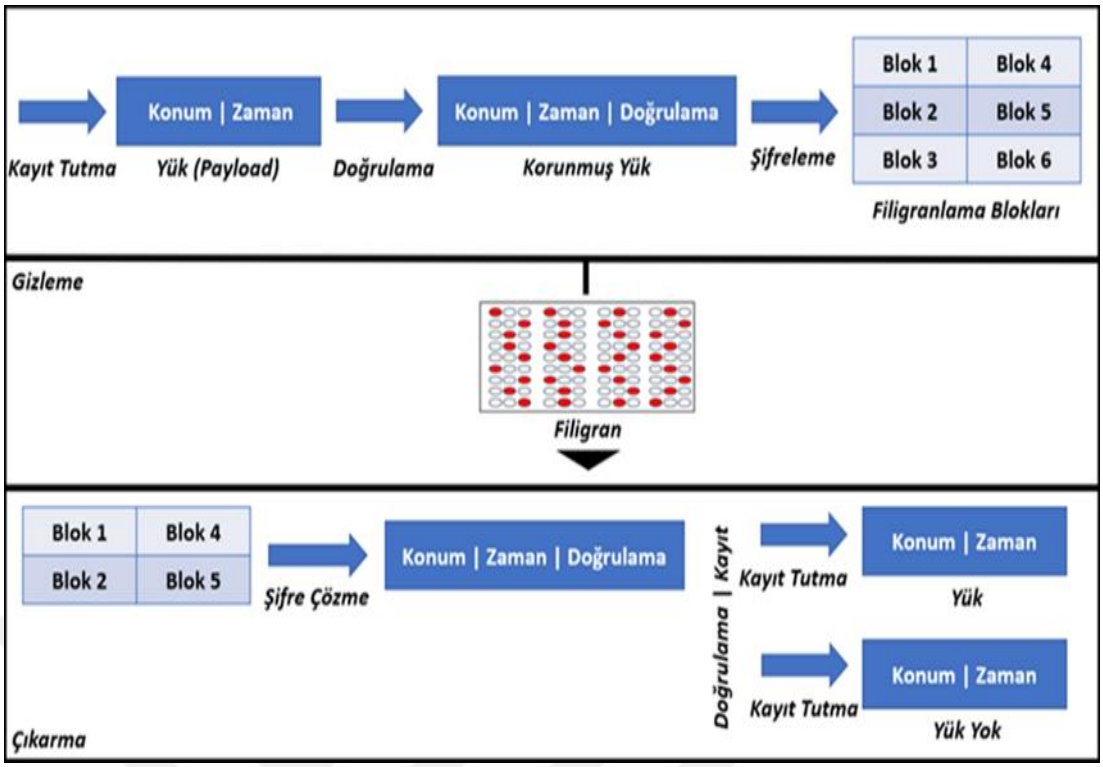
3.1. Ekran Filigranlama Yöntemlerinin İncelenmesi

İlk yaklaşım, insan gözünün dijital kameralara kıyasla hafif parlaklık değişikliklerine karşı duyarsızlığından faydalanmaktadır. İçerikten bağımsız olan bu yöntem, filigranları ekranlardaki metin içeriğine görünmez bir şekilde yerleştirir ve olası bir veri ihlali durumunda adli soruşturmalara yardımcı olur. Filigranlar, görüntülenen belgelerin resimlerinden çıkarılarak ihlal detaylarının belirlenmesini kolaylaştırır.

Bu yönteme göre, filigran gömme işleminde benzersiz bir bit dizisi gizli verileri temsil etmek için kullanılır. Gizli veri, bilgisayar adı, bilgisayar zamanı gibi belirleyici verilerdir. Bu bit dizisi, kriptografik bir sağlama toplamı (hash) ile güvenli bir yük oluşturur. Kriptografik sağlama toplamı, verilerin bütünlüğünü doğrulamak için kullanılan bir dijital imzadır. Örneğin, SHA-256 gibi bir hash fonksiyonu, bir veri parçasının benzersiz bir özetini üretir. Bu özet, veri değiştirildiğinde tamamen farklı bir değer alır, bu nedenle veri bütünlüğü bu yolla korunur. Güvenli yük, bilgisayar ekranına gömülü filigran sembolleri oluşturmak için özel bir konvolüsyonel kodlayıcı ile kodlanır. Konvolüsyonel kodlayıcı, bu filigran sembollerini ekranın piksel yapısına gömerek gizler. Bu sayede, normal kullanıcılar tarafından fark edilmeden, ekranın görüntüleri üzerinden filigran çıkarılabilir.

Çıkarma işleminde, gömülü sembollerin kodu çözülerek korumalı yük elde edilir. Korunan yük, daha önce filigranlama işleminde kullanılan bit dizisinin, ekran görüntülerinden geri alınması anlamına gelir. Kriptografik kimlik doğrulama özeti doğrulanır. Bu işlem, orijinal hash toplamının geri alınan veri ile karşılaştırılmasıdır. Eğer doğrulama başarılı olursa, gizlenmiş veri bilgileri döndürülür. Aksi takdirde, sonuç verilmez ve bu durum filigranın manipüle edildiği veya bozulduğu anlamına gelir (Gugelmann et al. 2018).

Bu şekilde, filigran normal kullanım sırasında görünmez kalır, ancak ekranda gösterilen belgelerin resimlerinden sonradan çıkarılabilir. Bu yöntem, bir kuruluşun elde edilen sızdırılmış resimlerden veri sızıntısının yerini ve zamanını belirlemesine olanak tanır ve veri ihlallerinin idari ve/veya adli soruşturulmasını büyük ölçüde kolaylaştırır. Şekil 3.1'de önerilen filigran yönteminin iş akış şeması gösterilmektedir.



Şekil 3.1: Filigran İş Akış Şeması (Birinci Yöntem).

(Gugelmann ve diğ., 2018)'den uyarlanmıştır.

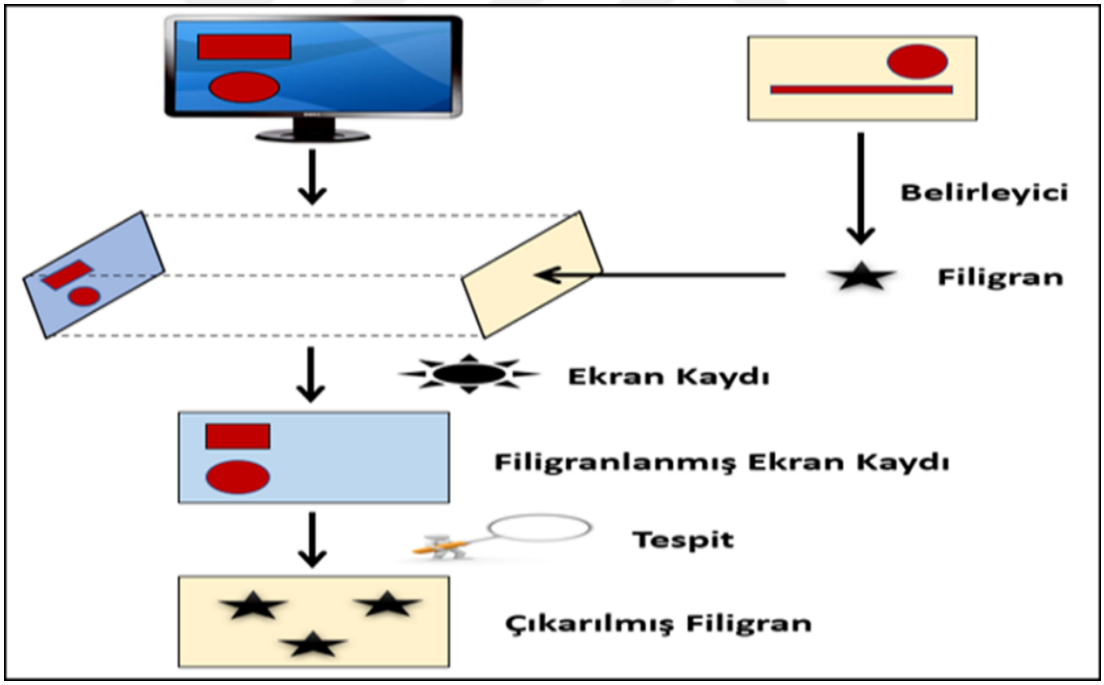
Şekilde görüldüğü gibi, filigran ekleme işleminde önce bilgisayar, kullanıcı ve zamanı tanımlayan bit dizisi oluşturulmaktadır. Oluşturulan bu bit dizisinin hata tespiti ve bütünlük kontrolü için bir kriptografik kontrol özeti hesaplanarak korumalı bir yük (payload) oluşturulup kodlayıcıya verilir. Korumalı yük uyarlanmış bir konvolüsyonel kodlayıcı kullanılarak kodlanıp oluşturulan filigran sembolleri bilgisayar ekranının piksel yapısına yerleştirilir. Filigran çıkarma işleminde ise; elde edilen sızdırılmış fotoğraftan önce filigran sembolleri çıkarılır. Kodlanmış olan bu filigran sembolleri sistemde kullanılan algoritma ile çözülerek korumalı yük çıkarılır. Çıkarılan yükün kriptografik doğrulama özeti teyit edilir ve doğrulama özeti doğru ise bilgisayar, kullanıcı ve zaman bilgileri döndürülür.

İkinci yaklaşım, gerçek zamanlı bir ekran filigranlama yöntemidir ve bir kaplama katmanı kullanır (Piec & Rauber, 2014). Bu yöntem, insan görme sisteminin zafiyetinden faydalanır. Ekrandaki içeriğin üzerine algılanamayan bir filigran yerleştirir ve ekran değişikliklerine minimum gecikmeyle uyum sağlar. Bu uyarlanabilir yöntem, özel donanım gerektirmeden çalışır ve çeşitli bilgisayar sistemlerinde kullanılabilir. Yani, filigranlama işlemi için ek bir cihaz veya yüksek

performanslı bir donanım gerekmez. Yazılım tabanlı bir çözüm olduğundan, bu yöntem birçok işletim sistemi ve ekran türü ile uyumlu hale getirilebilir.

Algoritmanın basitliği, yalnızca düşük hesaplama karmaşıklığı sağlamakla kalmayıp aynı zamanda gerçek zamanlı işlemeye de olanak tanıyan önemli bir özelliktir. Ekran değişiklikleri ile filigran algoritmasının adaptasyonu arasındaki neredeyse algılanamaz gecikme, yüksek uyarlanabilirlik dinamiklerinin bir göstergesidir. Bu durum, kullanıcıların filigranı fark etmeyeceği ve normal kullanım deneyimlerinin kesintiye uğramayacağı anlamına gelir. Gecikmenin filigranlı ekranın boyutuyla orantılı olduğunu belirtmek gerekir; bu da farklı ekran boyutlarında ölçeklenebilir bir performansa işaret eder. Daha büyük ekranlar, daha fazla veri ve daha karmaşık hesaplamalar gerektirebilir, bu da hafif bir gecikmeye neden olabilir.

Şekil 3.2'de önerilen filigran yönteminin iş akışı gösterilmektedir ve bu şema, filigranın nasıl yerleştirildiğini ve ekran değişikliklerine nasıl uyum sağladığını detaylandırmaktadır.



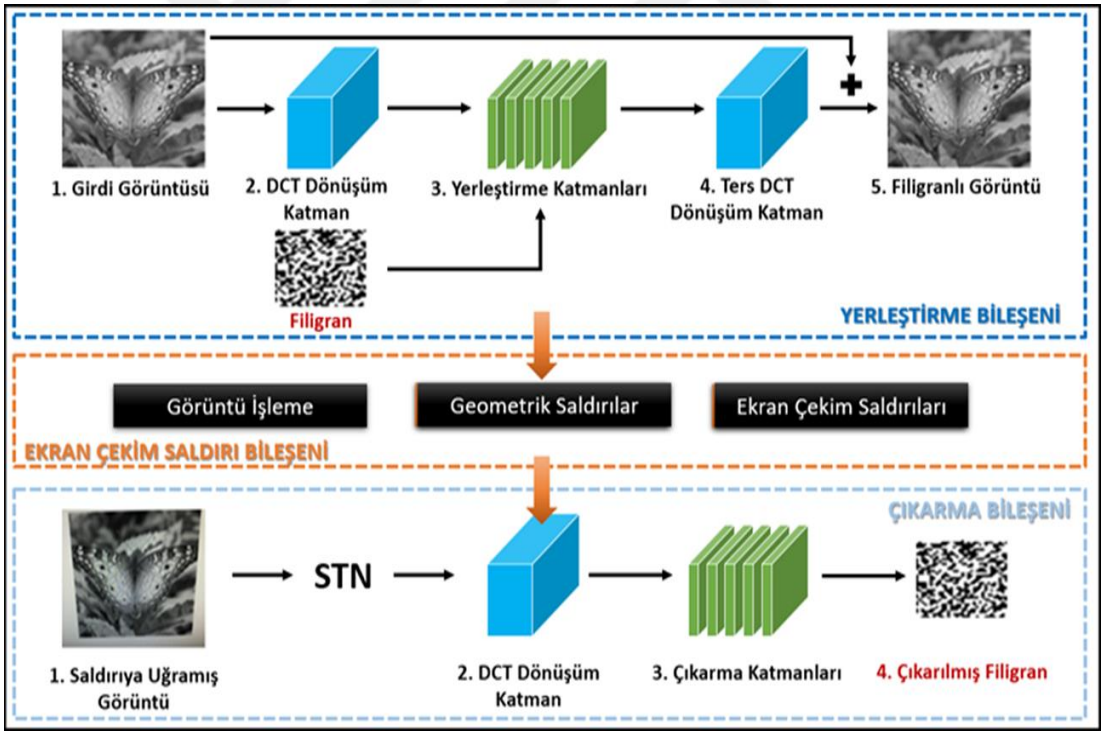
Şekil 3.2: Filigran İş Akış Şeması (İkinci Yöntem).

(Piec & Rauber, 2014)'den uyarlanmıştır.

Şekil 3.2'de görüldüğü gibi, sistem, İnsan Görsel Sistemi (Human Visual System, HVS) özelliklerini kullanarak üst üste binen katmanın rengini ve opaklığını değiştirmekte, bu da o anda görüntülenen görüntünün parlaklığının değişmesine neden olmaktadır. Ekranın değiştiği an ile filigran algoritmasının yeni ekran görüntüsüne

adapte olduğu an arasında neredeyse hiç fark edilmeyen bir gecikme olmaktadır. Algoritmanın basit tutulması sayesinde düşük hesaplama karmaşıklığı ve gerçek zamana yakın işleyiş elde edilmiştir.

Üçüncü yaklaşım ise, derin sinir ağlarından yararlanan bir frekans alanı filigranlama tekniği olan Gürültü İçindeki Dijital Kanıtlar için Yapısal Benzerlik (Structural Similarity for Digital Evidence in Noise, SSDeN) yöntemini önermektedir (R. Bai et al. 2022). Bu yöntem, ekran görüntülerinin izinsiz kullanımını engellerken görüntü kalitesinden ödün vermez. SSDeN yöntemi, tespit edilebilirlik ve görüntü kalitesinin bozulması gibi geleneksel filigranlama yöntemlerinde sıkça karşılaşılan sorunları çözmeyi hedeflemiştir. Bu yenilikçi yöntem, görüntü kalitesini korurken yetkisiz ekran yakalamaya karşı güçlü bir koruma sağlamakta ve yüksek performanslı bir çözüm olarak öne çıkmaktadır. Bu yöntem, filigranın varlığını belirginleştirmeden etkili bir koruma sağlayarak, ekran görüntülerinin izinsiz kullanılmasını zorlaştırır. Şekil 3.3'de SSDeN yönteminin filigranlama akış şeması gösterilmiştir.



Şekil 3.3: Filigran İş Akış Şeması (Üçüncü Yöntem).

(R. Bai ve diğ., 2022)'den uyarlanmıştır.

Şekil 3.3'de verilen sistem dört aşamada çalışır: veri kümesi ön işleme, filigran gömme, filigranlı verilerin ayrılması ve filigran çıkarma. Ön işleme aşamasında veriler hazırlanır, sıkıştırılır ve Ayrık Kosinüs Dönüşümüne (Discrete Cosine Transform,

DCT) tabi tutulur. DCT, veriyi frekans bileşenlerine ayırarak filigranın eklenmesi için uygun bir temel oluşturur. İkinci aşama olan filigran gömme, filigranın her piksele karşılık gelen DCT katsayılarına eklenmesini içerir. Bu işlem, filigranın görüntüde görünmez kılınmasını ve aynı zamanda sağlam bir şekilde yerleştirilmesini sağlar.

Üçüncü aşama, filigranlı verilerin ayrılmasıdır. Bu aşamada, frekans alanı öznitelikleri kullanılarak filigranlı bilgiler çıkarılır. Bu işlem, filigranlı verilerin diğer verilerden ayrılmasını ve analiz edilmesini kolaylaştırır. Son aşama olan filigran çıkarma, filigranlı verilerden filigranın çıkarılmasıyla orijinal görüntünün kurtarılması sağlanır. SSDeN yöntemi, ekran görüntülerinin kalitesinden ödün vermeden güvenliğini artırmak için derin sinir ağları ve frekans alanı yöntemlerini kullanır. Bu bileşenlerin sinerjisi, SSDeN Framework'ü ekran yakalama koruması alanında son teknoloji bir çözüm olarak konumlandırmaktadır.

3.2. İncelenen Yöntemlerin Karşılaştırılması

Aşağıda yer alan muhtelif filigranlama yöntemlerinin incelenmesinde, üç farklı yaklaşımın temel özellikleri, uygulamaları, avantajları ve sınırlamaları detaylı bir şekilde ele alınmaktadır. Bu yöntemlerden elde edilen bilgiler, Tablo 3.1'de özetlenmiştir ve günümüz filigranlama tekniklerinin etkinliğine ve karşılaşılan zorluklara ışık tutmaktadır.

İlk yöntem (Gugelmann ve arkadaşları, 2018), insan gözünün parlaklık değişimlerine duyarsızlığını kullanarak metin içeriğine görünmez filigranlar yerleştirir. Bu teknik, veri ihlallerinde adli incelemelere yardımcı olur ve görüntülerden filigran çıkarma yöntemiyle ihlal detaylarının belirlenmesini sağlar.

İkinci yöntem (Piec ve Rauber, 2014), canlı ekran filigranlama tekniği kullanarak ekran değişikliklerine minimum gecikme ile adapte olur. Bu yöntem, gerçek zamanlı filigranlama sağladığı için özellikle dinamik içeriklerin korunmasında avantaj sağlar. Özel donanım gerektirmemesi ve çeşitli bilgisayar sistemlerinde uygulanabilir olması önemli avantajlardır.

Üçüncü yöntem (R. Bai ve arkadaşları, 2022) olan SSDeN, derin sinir ağları ve frekans alanı yöntemlerini kullanarak filigranlama yapar. Bu yöntem, veri seti ön işleme, filigran yerleştirme, filigranlı veri ayrıştırma ve filigran çıkarma olmak üzere dört

aşamadan oluşur. Bu teknik, görüntü kalitesini koruyarak izinsiz ekran görüntülerinin kullanımını engeller.

Tablo 3.1'de, bu üç yöntemin karşılaştırmalı analizi yapılmıştır. Tablo, her bir yöntemin temel özelliklerini, uygulama alanlarını, sağladığı avantajları ve karşılaşılan sınırlamaları içermektedir. Bu şekilde, her bir yöntemin güçlü ve zayıf yönleri ortaya konulmakta ve filigranlama tekniklerinin genel etkinliği hakkında daha geniş bir perspektif sunulmaktadır. Bu analiz, farklı senaryolarda hangi filigranlama yönteminin daha uygun olduğunu belirlemeye yardımcı olmaktadır. Ayrıca, kullanılan yöntemlerin ayrıntılı bulguları ve açıklamaları da sunulmaktadır.

Tablo 3.1: Filigranlama Yöntemlerinin Karşılaştırılması.

Araştırma Makalesi	Metodoloji	Ana Özellikler	Uygulama	Avantajlar	Kısıtlamalar
(Gugelmann ve diğ., 2018) İçerikten Bağımsız Metin Filigranlama	Metin içeriğine filigran yerleştirme, İnsan gözünün parlaklık değişimlerine duyarsızlığını kullanır.	Görünmezlik, veri ihlallerinde adli incelemelere yardımcı olur; görüntülerden çıkarılması ihlal detaylarını belirlemede yardımcı olur.	Adli incelemeler, veri ihlali analizi.	İnsan gözü özelliklerini kullanır, içerikten bağımsızdır.	Kullanılabilirlik ekran teknolojileri arasındaki farklılıklardan etkilenebilir.
(Piec & Rauber, 2014) Canlı Ekran Filigranlama ile Üst Katman	Canlı ekran filigranlama, ekran değişikliklerine minimum gecikme ile adapte olan bir üst katman kullanır.	Gerçek zamanlı, özel donanım gerektirmez, çeşitli bilgisayar sistemlerine uygundur.	Genel ekran filigranlama uygulamaları.	İnsan görsel sistem özelliklerinden faydalanır, ekran değişikliklerine minimum gecikme ile adapte olur.	Verimlilik, ekran üzerindeki değişikliklerin karmaşıklığına bağlıdır.
(R. Bai ve diğ., 2022) SSDeN Çerçevesi-Derin Sinir Ağı ile Frekans Alanı Filigranlama	Filigranlama için derin sinir ağları ve frekans alanı işlemlerini kullanır. Veri seti ön işleme, filigran yerleştirme, filigranlı veri ayrıştırma ve filigran çıkarma olmak üzere dört aşamada işler.	Görüntü kalitesini bozmadan izinsiz ekran görüntülerinin kullanımını engeller.	Ekran görüntüsü güvenliğini artırma.	Derin sinir ağı entegrasyonu, frekans alanı işlemleri, görüntü kalitesini koruma.	Kullanılabilirlik gerçek dünya senaryo testlerine tabidir; potansiyel güvenlik açıkları ele alınmamıştır.

İncelenen ilk yöntem (Gugelmann ve diğ., 2018), test edilen tüm akıllı telefonlar için tüm filigran verilerinin değiştirilmemiş fotoğraflardan başarıyla alınabildiği sonucuna varmıştır. Görüntülerde yapılan değişikliklere rağmen kodlanmış veriler yine de çıkarılabilmiştir. Ayrıca yöntem, akıllı telefonlar tarafından çekilen filigranlı görüntülerin kırpılmasına karşı kayda değer bir dayanıklılık göstermiştir. Bu da

yöntemin korunan verilerin parmak izini takip ve analiz etmedeki etkinliğinin altını çizerek veri ihlallerinin adli soruşturmasını önemli ölçüde kolaylaştırmaktadır. Bu yöntem; insan gözünün parlaklık değişimlerine duyarsızlığını kullanarak metin içeriğine görünmez filigranlar yerleştirme metoduna dayanmaktadır. Bu teknik, filigranların metin içeriğinden bağımsız olarak eklenmesine olanak tanır ve böylece filigranlar metnin anlamını veya okunabilirliğini etkilemez. Filigranların görünmez olması, izinsiz kullanımları tespit etmek için etkili bir yöntemdir ve veri ihlallerinde, görüntülerden filigran çıkarma yöntemi ile ihlal detayları belirlenebilir, bu da adli incelemelere yardımcı olur. Ancak, farklı ekran teknolojileri arasındaki parlaklık ve kontrast farklılıkları, filigranın algılanabilirliğini etkileyebilir. Bu durum, yönteminin bazı cihazlarda etkinliğini azaltabilir.

İncelenen ikinci yöntem (Piec & Rauber, 2014), canlı ekran filigranlama tekniğini kullanır. Bu teknik, ekran değişikliklerine minimum gecikme ile adapte olan bir üst katman kullanarak çalışır. Bu sayede, gerçek zamanlı filigranlama yapılabilir. Bu yöntemde, algılanamazlık ve sağlamlık açısından değerlendirmeler yapılmıştır. Filigran bölgesinin boyutu orta veya küçük olarak ayarlandığında, filigran tüm kullanım senaryolarında fark edilmeden kalmış, görünürlük yalnızca daha büyük bölge boyutları için gerçekleşmiştir. Bu durum, filigranın görünürlük seviyesi ile korunacak içeriği içeren bölgelere yerleştirme doğruluğu arasındaki dengeyi vurgulamaktadır. Sağlamlık değerlendirmesi, değiştirilmemiş ekran görüntülerine sahip tüm test senaryoları için filigranın kaldırılmasının mümkün olduğunu ortaya koymuştur. Özellikle, daha büyük bölge boyutlarının saldırı girişimlerine karşı daha fazla direnç sağladığı, ancak daha küçük filigran boyutlarının kırpma gibi işlemlere daha iyi dayandığı gözlemlenmiştir. Bu yöntem ile filigranlar gerçek zamanlı olarak eklenir, böylece, özellikle dinamik içeriklerin korunmasında avantaj sağlamaktadır. Ayrıca özel donanım gerektirmemesi, çeşitli bilgisayar sistemlerinde kolayca uygulanabilir olmasını sağlar. Ancak, ekran üzerindeki değişikliklerin karmaşıklığına bağlı olarak filigranlamanın verimliliği değişebilir. Karmaşık ekran görüntülerinde yöntem etkili olmayabilir.

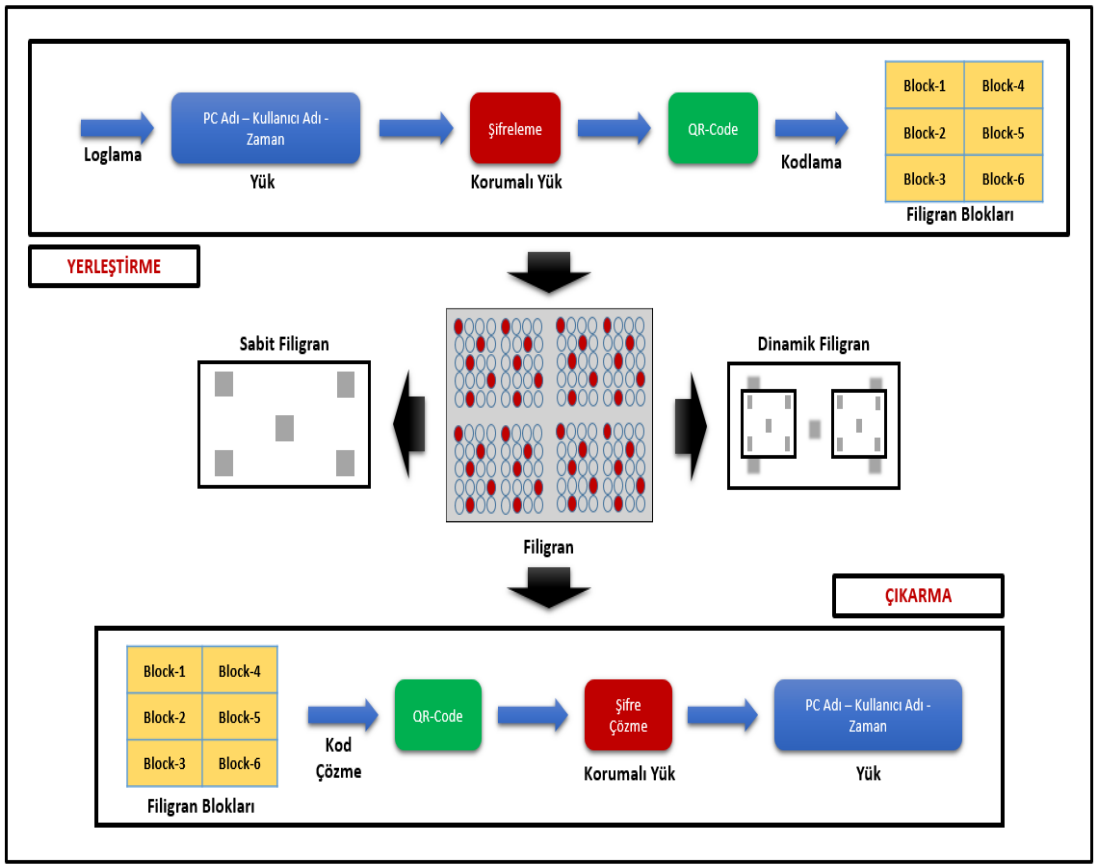
İncelenen üçüncü yöntem (R. Bai ve diğ., 2022) ile derin sinir ağları ve frekans alanı işlemleri kullanılarak filigranlama yapılmıştır. Yöntem, veri seti ön işleme, filigran yerleştirme, filigranlı veri ayrıştırma ve filigran çıkarma. Olmak üzere dört aşamalı bir süreçten oluşur. Makalede deneysel çalışmalara odaklanmıştır. Deneyler, binlerce

nesne kategorisini kapsayan geniş etiketli görüntü koleksiyonuyla tanınan ve bilgisayarla görme araştırmalarında bir ölçüt olarak hizmet veren ImageNet veri kümesi üzerinde gerçekleştirilmiştir. Bu bağlamda araştırmacılar, SSDeN Çerçevesinin performansını titizlikle değerlendirmek için Tepe Sinyal-Gürültü Oranı (Peak Signal-to-Noise Ratio, PSNR), Yapısal Benzerlik İndeksi (Structural Similarity Index Measure, SSIM) ve Ortalama Karesel Hata (Mean Squared Error, MSE) gibi temel ölçütleri kullanmışlardır. Milyonlarca yüksek çözünürlüklü görüntüden oluşan ImageNet, önerilen çerçevenin farklı görsel içeriklerdeki yeteneklerinin kapsamlı bir şekilde değerlendirilmesini sağlayarak etkinliğinin sağlam ve kapsamlı bir şekilde analiz edilmesini sağlar. Sonuçlar, SSDeN Çerçevesinin sağlam bir filigranlama yöntemi olarak etkinliğini kanıtlamıştır. Farklı ölçeklendirme ve JPEG sıkıştırma oranlarında yapılan sağlamlık testleri SSDeN Çerçevesinin yüksek dayanıklılığını göstermiştir. Bu çalışma, verilerin korunmasında derin sinir ağı tabanlı filigranlama tekniklerinin potansiyel etkinliğinin altını çizmektedir. Yöntemde kullanılan derin sinir ağı entegrasyonu ve frekans alanı işlemleri, filigranlama sırasında görüntü kalitesini korur ve yüksek kaliteli görüntüleri bozmadan izinsiz ekran görüntülerinin kullanımını engelleyebilir. Ancak, yöntemin uygulanabilirliği, laboratuvar ortamından gerçek dünya senaryolarına geçişte test edilmelidir. Makalede potansiyel güvenlik açıkları tam olarak ele alınmamıştır, bu da yönteminin güvenliğini sorgulamaya açık bırakır.

İncelenen bu çalışmalar, dijital içeriklerin güvenliğini sağlama ve izinsiz kullanımını engelleme konusunda önemli katkılar sunmaktadır. Gugelmann ve diğ. (2018) tarafından önerilen yöntem, özellikle adli incelemelerde kullanılabilecek görünmez filigranlama tekniği ile öne çıkmaktadır. Piec ve Rauber (2014), canlı ekranlarda gerçek zamanlı ve donanım bağımsız filigranlama sağlarken, R. Bai ve diğ. (2022) ise derin öğrenme teknikleri ile yüksek kaliteli ve güvenli bir çözüm sunmaktadır. Her bir yöntemin kendine özgü avantajları ve kısıtlamaları bulunmakta olup, uygulanacak senaryoya göre uygun yöntem seçilmelidir.

4. YENİ YAKLAŞIM: MATERYAL VE METOT

Dijital verinin güvenliği alanında, veri ihlallerini ve ekran içeriğinin yetkisiz kullanımını tespit etmek ve önlemek çok önemli hale gelmiştir. Mevcut filigranlama yöntemleri bu zorluğun çeşitli yönlerini ele alırken, sınırlamalarının üstesinden gelen kapsamlı bir yaklaşıma ihtiyaç vardır. Bu çalışmada, yalnızca daha önce tartışılan yöntemlerin eksikliklerini gidermekle kalmayan, aynı zamanda dijital suçluları tespit etmede ileri düzeyde güvenlik ve esneklik sunan yeni bir sistem önerilmiştir. Önerilen sistem Şekil 4.1'de gösterilen yöntemden faydalanarak geliştirilmiştir (KERMAN & ŞİMŞEK, 2024).



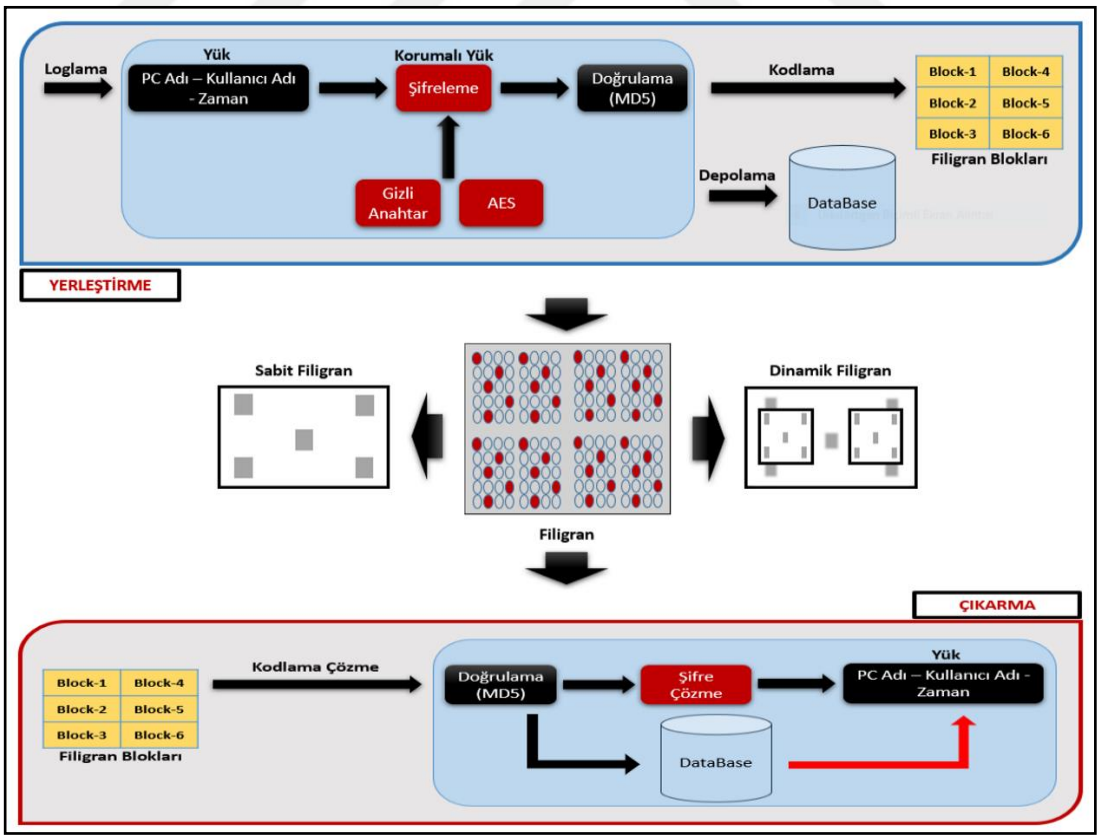
Şekil 4.1: Filigran İş Akış Şeması.

(KERMAN & ŞİMŞEK, 2024)'den uyarlanmıştır.

Önerilen ekran filigranlama yönteminin uygulanması için Python programlama dili kullanılmıştır. Python, önerilen yaklaşımımızın önemli bileşenleri olan görüntü

işleme, makine öğrenimi ve dinamik davranış entegrasyonunu kolaylaştıran zengin bir kütüphane ve araç ekosistemi sunmaktadır. Ayrıca, Python'un okunabilirliği ve kullanım kolaylığı, üzerinde çalışılan problemin karmaşıklığıyla iyi bir uyum içindedir.

Çalışmada seçilen yöntem, içerik uyarlamalı filigranlama ve gerçek zamanlı dinamik katman entegrasyonunu bir araya getirmektedir. Bu kapsamlı yaklaşım, mevcut yöntemlerin, belirli ekran teknolojilerine bağımlılığı, yüksek hesaplama gücü ve özel donanım gereksinimi gibi bazı sınırlamalarını aşmayı ve dijital suçluları tespit etmek için etkili bir çözüm sunmayı amaçlamaktadır. İçeriğe uyarlanabilir filigranlama, içerik özelliklerini dikkate alarak akıllı gömme sağlar, algılanamazlığı korurken görünürlüğü optimize eder. Gerçek zamanlı dinamik kaplama yalnızca içerik değişikliklerine uyum sağlamakla kalmaz, aynı zamanda bilgisayar ekranında açılan uygulama pencerelerinin boyutlarının küçültülmesi, konumlarının değiştirilmesi gibi kullanıcı etkileşimlerine göre güncellenir. Bu sayede, dijital suçluların belirli bir örüntüyü veya filigran yerleşimini tahmin etmeleri zorlaşır. Önerilen filigran gömme ve çıkarma sürecinin iş akışı Şekil 4.2'de gösterilmektedir.



Şekil 4.2: Önerilen Filigranlama Yöntemi İş Akış Şeması.

Geliştirilen uygulama aracılığıyla, filigranların görüntülere dinamik olarak gömülmesi ve bilgilendirici içeriğin gerçek zamanlı olarak eklenmesi için yenilikçi bir yöntem sunulmaktadır. Kullanılan yöntem ile görüntü işleme, kriptografi, steganografi ve filigranlama teknikleri harmanlanarak etkileşimli bir filigranlama çözümü sunulmuştur. Uygulama ile sadece sabit bir şekilde ekrana eklenen görünmeyen filigranlar değil, kullanıcı tarafından açılan uygulama pencerelerine de ayrıca görünmeyen dinamik filigran eklenmektedir. Bu şekilde eklenilen dinamik filigran, kullanıcı davranışlarına karşı koruma sağlamaktadır. Örneğin, açılan uygulama pencerelerinin ekran içerisinde farklı yerlere hareket ettirilmesi ile dinamik filigran da pencere ile hareket etmektedir. Bu yöntem, bir pencere formu uygulaması içinde bağlam uyarlamalı filigranlama ve gerçek zamanlı dinamik katmanların entegrasyonunu kapsamaktadır. Şifrelenmiş meta verileri kapsayan bilgiler oluşturulduktan sonra, görüntülere steganografi ve filigranlama teknikleri kullanılarak gizli filigran olarak yerleştirilir ve tamamlayıcı bilgileri ileten gerçek zamanlı kaplamalarla tamamlanır.

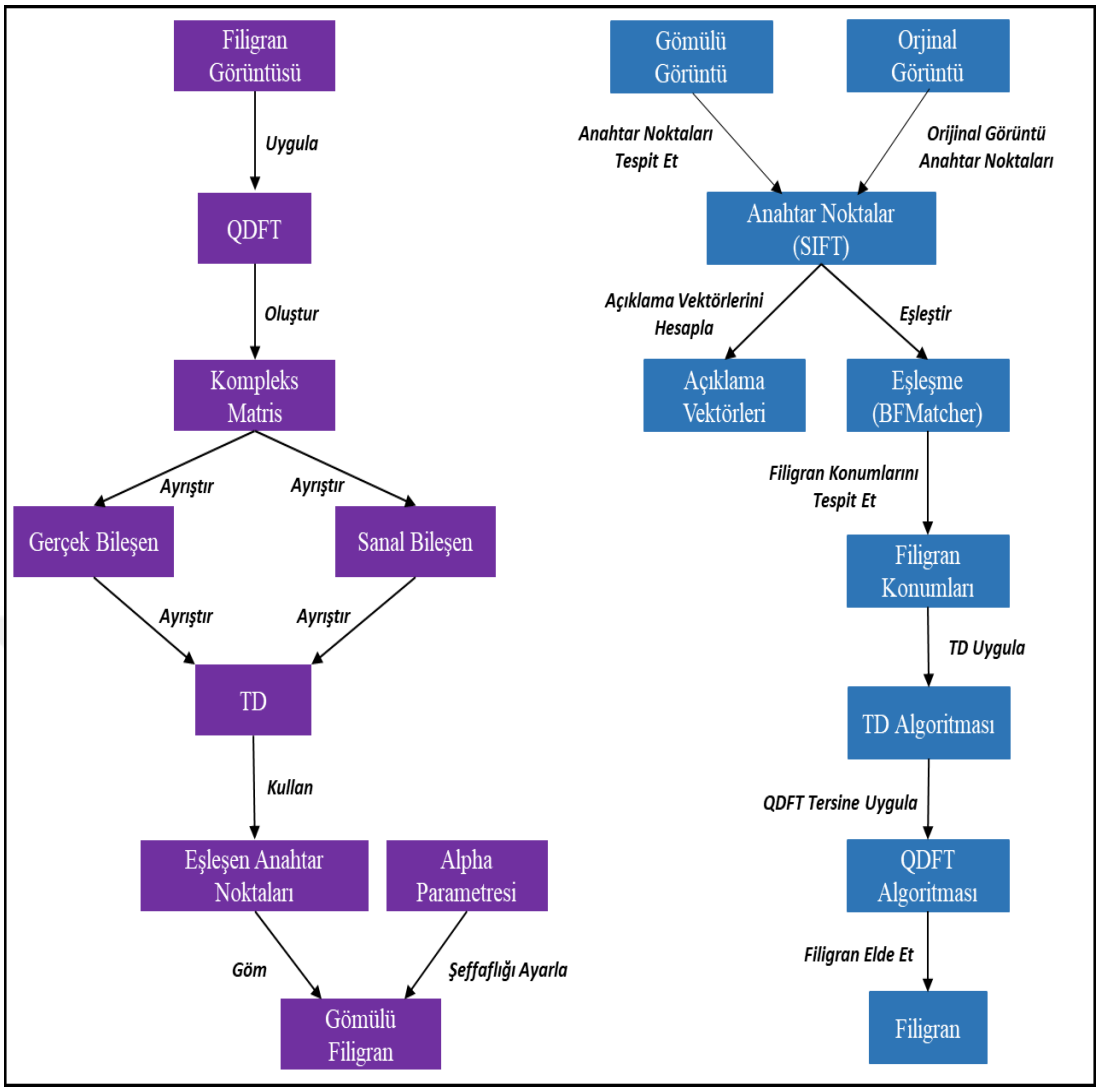
Geliştirilen uygulama, kullanıcı bilgisayarının ekranında şeffaf bir katman oluşturarak belirli verileri gizli bir şekilde görüntüler ve bu verileri güvenli bir şekilde şifreleyip saklar. Kullanılan yöntem, Python programlama dili ile geliştirilmiş ve PyQt5, Cryptography, Steganography ve MySQL gibi kütüphaneler kullanılmıştır. Öncelikle, sistemde kullanılacak gerekli kütüphaneler ve modüller projeye dâhil edilmiştir. Bu kütüphaneler, sistem işlevselliği ve veri güvenliğini sağlamak için kritik öneme sahiptir. PyQt5, grafik kullanıcı arayüzü (GUI) bileşenlerinin oluşturulmasında kullanılmıştır. Cryptography kütüphanesi, verilerin güvenli bir şekilde şifrelenmesi ve çözülmesi işlemlerini gerçekleştirirken, MySQL kütüphanesi ise veritabanı işlemleri için kullanılmıştır.

Ekrana gizli bilgi yerleştirilmiş filigran yerleştirilmeden önce şeffaf katman olarak kullanılacak resim dosyasının hazırlanması işlemi bir defaya mahsus bir şekilde gerçekleştirilir. Bu resim dosyası gizli bilgilerin dinamik olarak ekleneceği ana fonksiyonda sabit olarak kullanılmıştır. Bu kapsamda, öncelikle kullanılacak resim dosyasının anahtar noktaları tespit edilmiştir. Bu anahtar noktalar, filigran gömme ve çıkarma işlemlerinde referans olarak kullanılmıştır. Anahtar noktalar, görüntülerin belirgin özelliklerini temsil eder. Burada, SIFT (Scale-Invariant Feature Transform) algoritması kullanılarak hem anahtar noktalar hem de bu noktaların açıklama

vektörleri hesaplanır. Daha sonra, BFMatcher (Brute-force Matcher) algoritması kullanılarak filigran ve görüntü arasındaki anahtar noktalar eşleştirilir. Eşleştirme sırasında, her bir eşleşme için bir uzaklık ölçüsü hesaplanır ve bu ölçü, diğer en iyi eşleşmeyle karşılaştırılarak değerlendirilir. Uzaklık oranı bir eşleşmenin ne kadar güvenilir olduğunu belirlemekte kullanılır ve belirli bir eşik değeri altındaki eşleşmeler iyi eşleşme olarak kabul edilir. Genel olarak, uzaklık oranı için önerilen eşik değeri 0.7'dir (Bay ve diğ., 2006; Lowe, 2004; Mikolajczyk & Schmid, 2005). Bu çalışmada eşik değeri 0,5 olarak seçilmiştir. Filigranlama sürecinde doğruluk ve güvenilirlik ön planda olduğundan ve sabit bir resim dosyası kullanıldığından, performans ve hız kaygısı olmaksızın daha düşük eşik değeri tercih edilmiştir.

Filigran, QDFT (Quantized Discrete Fourier Transform) ve TD (Tensor Decomposition) kullanılarak hazırlanır. Bu adımda, filigran görüntüsü QDFT'ye tabi tutulur ve sonuç olarak kompleks bir matris elde edilir. Bu matris, gerçek ve sanal bileşenleri içerir. Daha sonra, bu bileşenler TD'ye ayrıştırılarak gerçek ve sanal bileşenler elde edilir. Bu işlem, filigranın frekans bileşenlerini elde etmek için kullanılır. Eşleşen anahtar noktaların koordinatları kullanılarak filigran görüntüye gömülür. Her bir eşleşme için, filigranın gerçek ve sanal bileşenleri belirli bir konumda görüntüye eklenir. Eklenen bileşenlerin şeffaflığı, alpha parametresiyle ayarlanır. Bu parametre, filigranın görüntü üzerinde ne kadar belirgin olacağını kontrol etmek için kullanılır. Bu süreç, görüntüye filigranın başarıyla gömülmesini sağlar.

Filigran çıkarma adımında ise, yine aynı anahtar noktalar kullanılarak işlem yapılır. İlk olarak, filigran gömülmüş görüntüdeki anahtar noktalar SIFT (Scale-Invariant Feature Transform) algoritması ile tespit edilir ve açıklama vektörleri hesaplanır. Ardından, BFMatcher algoritması ile bu anahtar noktalar ve açıklama vektörleri, orijinal görüntüdeki anahtar noktalar ile eşleştirilir. Eşleşme sonrasında, filigranın gömülü olduğu konumlar tespit edilir. Bu konumlar kullanılarak, QDFT ve TD algoritmaları tersine uygulanarak filigran çıkarılır. İlk olarak, TD uygulanarak filigranın gerçek ve sanal bileşenleri ayrıştırılır. Daha sonra, QDFT tersine uygulanarak bu bileşenler birleştirilir ve filigran elde edilir. Bu adımlar sonucunda, filigranın başarılı bir şekilde çıkarılması sağlanır. Geliştirilen yöntemin algoritması Şekil 4.3’de gösterilmektedir.



Şekil 4.3: Önerilen Filigranlama Yönteminin Algoritması.

Uygulamanın temel işlevi, kullanıcı bilgisayarında belirli verileri toplamak ve bunları şifrelemektir. Bu veriler arasında bilgisayar adı, kullanıcı adı ve mevcut zaman bilgisi bulunmaktadır. Bu bilgiler, gizli verilerin üretiminde kullanılır ve daha sonra şifrelenir. Şifreleme işlemi için öncelikle bir şifreleme anahtarı oluşturulur. Bu anahtar, Fernet şifreleme yöntemi kullanılarak üretilmiştir ve daha sonra verilerin şifrelenmesinde kullanılmıştır. Şifrelenmiş verilerin güvenliğini sağlamak ve bütünlüğünü doğrulamak için MD5 algoritması kullanılarak bir hash değeri hesaplanmıştır. Hız, performans ve yaygın uyumluluk sebeplerinden dolayı MD5 algoritması seçilmiştir. MD5, hızlı bir şekilde hesaplama yapılabilen bir hash fonksiyonudur ve birçok sistem ve yazılımda yaygın olarak desteklenir. Bu, mevcut sistemlerle entegrasyonun daha kolay olmasını sağlamaktadır. Verilerin güvenli bir

şekilde saklanması için MySQL veritabanı kullanılmıştır. Veritabanında saklanan veriler Şekil 4.4'de gösterilmiştir.

id	data	encryption_key	encrypted_data	hash_value	timestamp
1	IB001-1132 ofkerman 2024-09-05 00:52:50	o0NJ9_UTyQpzkwrlA5ykw4D8	gAAAAABm2NayYi8CEl_BMDbSKKE6zEv10ltxEk	F0E0EA4C8A0B9EFA7C136E3D2994546D	2024-09-05 00:52:50
2	IB001-1132 ofkerman 2024-09-05 00:52:50	0cz2XfFt8EkgKWFov1GINrExtc	gAAAAABm2Nay-r2JOrjL_CE8TVZgAp5TJuzttW	513B175A8F919D3A8CF15D7823480D37	2024-09-05 00:52:50
3	IB001-1132 ofkerman 2024-09-05 00:52:50	vYeNryYjRdgwU83atyWE3Beh	gAAAAABm2NayyOawFZf-J-lanuWq41CPuUL-cq	5040E6DAAF458E9239833FD5B241A4C2	2024-09-05 00:52:50
4	IB001-1132 ofkerman 2024-09-05 00:52:50	q80wJw0IPt9iSPRXpMlurVACF	gAAAAABm2Nayr4wDZpz8EhwpGadrt3xTnMN3	051F46F3EFD358C6A0DAB4478E606599	2024-09-05 00:52:50
5	IB001-1132 ofkerman 2024-09-05 00:52:50	gLOZ4nHfuTCIS29TXy20U4UkV	gAAAAABm2NayENbUSpc3coUUFYjdQUKDAp5z	D5714E488917820E8EA64D6C0662373F	2024-09-05 00:52:50
6	IB001-1132 ofkerman 2024-09-05 00:52:50	KecuSIxtsd93aX8KJWjo3UgQYP	gAAAAABm2NayrTmpG3W-Dt6QOhi964i46Qdh	B285EB0E0EE3FEC33919071C22C3F187	2024-09-05 00:52:50
7	IB001-1132 ofkerman 2024-09-05 00:52:50	rqf35lazWH6MHU6VyHEfuvisN	gAAAAABm2NayVE1koBVSMBIEYiNasw3wIGR2I	01F76E47E8928B71CC84F7F54F99A417	2024-09-05 00:52:51
8	IB001-1132 ofkerman 2024-09-05 00:52:51	N4Ae_oipEYE_mBJtvqYIqTMz6	gAAAAABm2NazgSdf43jO2LM6105viybdpRQSU	955E250B5D2F7DA460E774F6BF9C6D25	2024-09-05 00:52:51
9	IB001-1132 ofkerman 2024-09-05 00:52:51	VjTu_azHe7lS94-NLExCFw4k5G	gAAAAABm2Naz0Cswamx90lx9bfKoUmeNKykS	729FB64C4EBB357099259F08668E2814	2024-09-05 00:52:51
10	IB001-1132 ofkerman 2024-09-05 00:52:51	KE93IBvb-tYceTDIVol6x3lY1KOY	gAAAAABm2Nazt67QOj2_W9ejGJ7rMlWtMTt9	A8B2F8EFAD705A56876BA54280F406E7	2024-09-05 00:52:51

Şekil 4.4: Veritabanında Saklanan Bilgiler.

Veritabanı, gizli veriler, şifreleme anahtarı, şifrelenmiş veriler, hash değeri ve zaman damgası bilgilerinin saklanması için yapılandırılmıştır. Tablo 4.1'de gösterildiği gibi bu alanların her biri, veri tipleri ve gereklilikleriyle birlikte veritabanında yer alır.

Tablo 4.1: Veritabanı Tablo Yapısı ve Veri Tipleri.

Alan Adı	Veri Tipi	Gereklilikler
secret_data	TEXT	NULL olamaz, gizli verilerin saklandığı alan
encryption_key	TEXT	NULL olamaz, şifreleme anahtarının saklandığı alan
encrypted_data	TEXT	NULL olamaz, şifrelenmiş verilerin saklandığı alan
hash_value	VARCHAR(32)	NULL olamaz, MD5 hash değerinin saklandığı alan
timestamp	TIMESTAMP	NULL olamaz, veri kaydının zaman damgası

Veri güvenliği açısından, şifrelenmiş veriler ve şifreleme anahtarlarının saklanması, verilerin yetkisiz erişime karşı korunmasını sağlar. Veri bütünlüğü açısından, MD5 hash değerlerinin saklanması, verilerin bütünlüğünün doğrulanmasını ve değiştirilip

değiştirilmediğinin kontrol edilmesini sağlar. Ayrıca, verilerin organize bir şekilde saklanması ve gerektiğinde kolayca erişilebilir olması, uygulamanın verimliliğini ve kullanılabilirliğini artırmaktadır. Son olarak, mevcut zaman bilgisinin saklanması, verilerin güncel ve geçerli olduğunun teyit edilmesine yardımcı olur. Bu nedenlerle, veritabanı yapılandırması, verilerin güvenli ve bütün bir şekilde saklanmasını, yönetilmesini ve gerektiğinde erişilmesini sağlar. Yazılım, veritabanına veri eklemek ve lüzumlu tabloları oluşturmak için gerekli fonksiyonları içerir. Böylece, her bir veri kaydı, zaman damgası ile birlikte veritabanına kaydedilir.

Ekranda şeffaf bir katman oluşturmak için özel bir PyQt5 aracı geliştirilmiştir. Bu araç, belirli bir aralıkla güncellenir ve ekrandaki gizli verileri görüntüler. Araç, kullanıcının dikkatini dağıtmadan veya ekranın görünümünü bozmadan çalışacak şekilde tasarlanmıştır. Ayrıca araç, belirli bir aralıkla gizli bilgi alanında tuttuğu bilgisayar adı, kullanıcı adı ve zaman bilgilerini güncellemek ve veritabanına yeni veri eklemek için zamanlayıcılar kullanır. Bu zamanlayıcılar, belirli aralıklarla çalışarak bu bilgilerin sürekli olarak güncellenmesini ve güvenli bir şekilde saklanmasını sağlar.

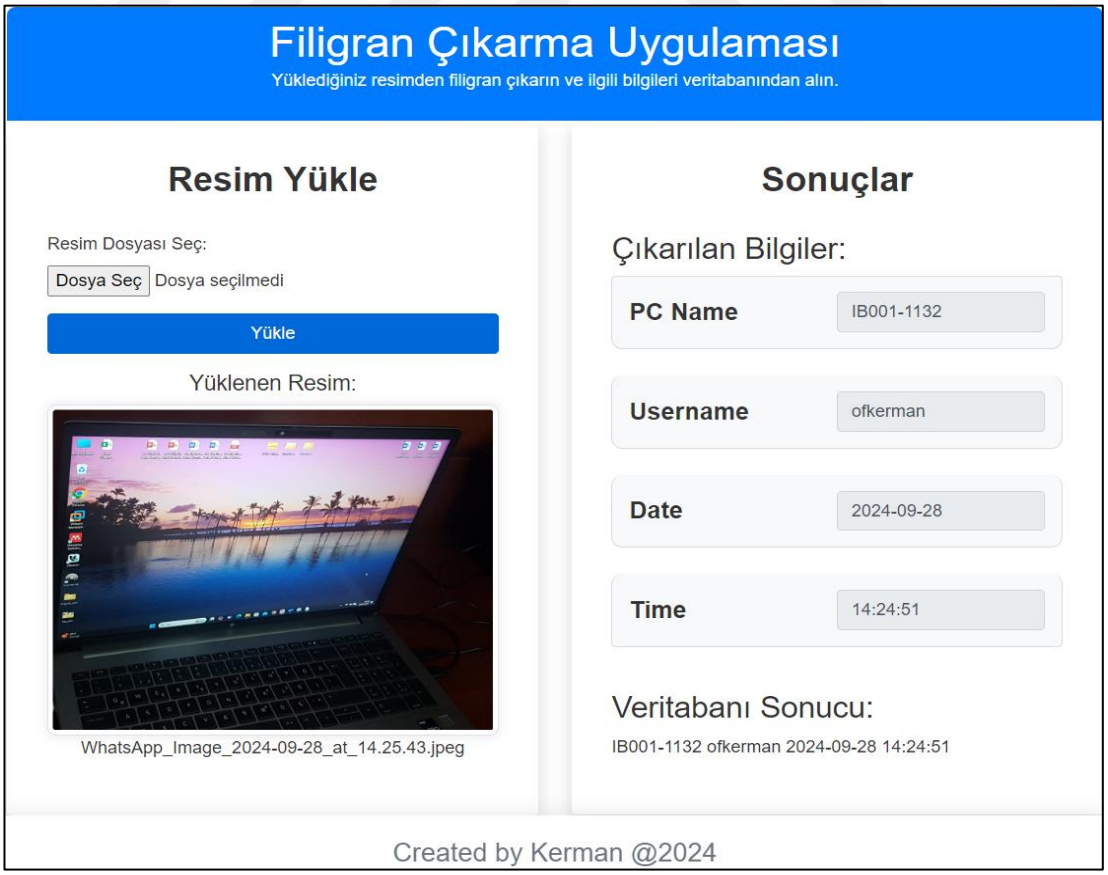
Ana fonksiyon, tüm bu bileşenleri bir araya getirir ve uygulamayı başlatır. Uygulamanın başlamasıyla birlikte veritabanındaki tablo yapısı ve veri tipleri kontrol edilir ve veritabanı hazır hale getirilir. Uygulama, bilgisayar ekranında farklı konumlarda filigranlar oluşturarak bunları görünmez bir şekilde ekler. Uygulama arka planda sürekli olarak çalışır. Bu sayede, olası bir ihlal durumunda, ihlali gerçekleştiren kullanıcı ve ihlalin zamanı veri tabanına kaydedildiğinden, ihlali gerçekleştiren kullanıcı kolaylıkla tespit edilebilir ve dijital suçlular ile yaptıkları ihlaller ilişkilendirilebilir.

Uygulama, arka planda kullanıcı müdahalesine gerek kalmadan çalışarak olası ihlal durumlarında ilgili kullanıcıyı tespit etmeyi amaçlar. Özellikle, içeriğe uyarlanabilir filigran işlevi, uygun filigran gömme noktalarını ayırt etmek için görüntü özelliklerini incelerken, gerçek zamanlı dinamik kaplama işlevi görüntüyü dikkatli bir şekilde izler ve canlı kaplamalar uygular. Bu sayede, ihlali gerçekleştiren kullanıcıyı ve ihlalin zamanını tespit ederek, dijital suçlular ile yaptıkları ihlalleri ilişkilendirmeye yardımcı olur ve bu tespit edilebilirlik ayrıca caydırıcı bir etki de yaratabilir.

Uygulamanın kullanıcı tarafından kapatılmasını önlemek amacıyla uç nokta politika yöneticisi (Endpoint Policy Orchestrator, ePO) ve grup politika yöneticisi (Group

Policy Orchestrator, GPO) gibi güvenlik yöntemleri entegre edilmiştir. Ayrıca, siber saldırganların sistemlere erişim sağladıktan sonra kalıcılıklarını sürdürebilmek için sıkça başvurdukları bir teknik olan işlem kimliğine (Process ID) göç yöntemi de bu uygulama için kullanılmaktadır. Bu yöntemle uygulama, Windows işletim sisteminin temel işlemlerinden biri olan Windows Gezgini sürecine entegre edilir. Böylece, uygulamanın çalıştığı işlem Windows Gezgini'nin PID'sine taşınır. Bu yöntem, uygulamanın hem arka planda fark edilmeden çalışmasına olanak tanır hem de işletim sistemiyle entegre olduğu için kapatılması ya da durdurulması neredeyse imkânsız hale gelir. Bu sayede kullanıcı, manuel olarak uygulamayı durduramaz ya da kapatamaz; dolayısıyla uygulama sürekli çalışır ve işlevlerini kesintisiz olarak yerine getirir.

Bu çalışmanın bir parçası olarak, elde edilmiş bir resim dosyasından filigranın çıkarılması ve içeriğinin okunması amacıyla ayrı bir Python kodu geliştirilmiştir. Bu kod, OpenCV, MySQL, Flask, Steganaliz ve Tesseract gibi açık kaynaklı kütüphaneleri kullanarak, resim dosyasından elde edilen bilgilerin işlenmesini sağlar. Filigran çıkarma için geliştirilen web uygulaması aşağıdaki Şekil 4.5'de gösterilmiştir.



Şekil 4.5: Filigran Çıkarma Uygulaması.

İlk olarak, çıkarma fonksiyonu tanımlanmıştır. Bu fonksiyon, bir resim dosyası yolu alır ve bu resim dosyasından filigranı çıkarmak için işlem yapar. Resim dosyası, OpenCV kütüphanesi aracılığıyla yüklenir, gri tonlamalı bir versiyona dönüştürülür. Ardından, Tesseract Kütüphanesi ve steganaliz yöntemleri kullanılarak bu gri tonlamalı resimden metin okunur ve çıkarılan metin bir dize olarak döndürülür. Daha sonra, daha önceden tanımlanan sorgu adlı fonksiyon sayesinde, veritabanından hash değerine karşılık gelen bilgilerin alınmasını sağlar. MySQL veritabanına bağlanmak için gerekli bilgiler kullanılarak bir bağlantı kurulur ve ardından hash değeri veritabanına sorgulanır. Eğer veritabanında bu hash değerine karşılık gelen bir bilgi bulunursa, bu bilgi döndürülür. Aksi halde, None değeri döndürülür. Böylece bu iki fonksiyon kullanılarak veri elde etme işlemi gerçekleştirilir.

Bu uygulama, resim dosyalarından filigran çıkarılması ve bu filigranın içeriğinin işlenmesi için etkili bir araç sağlar. Ayrıca, filigranın içeriğinin veritabanında sorgulanması ve ilgili bilgilerin alınması için de kullanılabilir. Bu işlem, kullanıcıların belirli bir resim dosyasına gömülmüş gizli bilgileri geri almasına ve bu bilgilerin doğruluğunu kontrol etmesine olanak tanır. Özellikle kurum ağlarında bulunan güvenlik cihazları ve diğer tüm bilişim sistemlerinde oluşan logların toplandığı SIEM (Security Information and Event Management) ürünleri ile entegre bir şekilde çalışarak dijital suçluların tespit edilmesi ve olayla ilişkilendirilmesinde çapraz doğrulama yapılmasına olanak sağlar. Bu tür bir işlem, özellikle dijital güvenlik ve adli bilişim alanlarında önemli bir rol oynamaktadır ve çeşitli uygulamalarda kullanılabilir.

5. DEĞERLENDİRME

5.1. İncelenen Yöntemlerin Değerlendirmesi

Üç farklı yöntemin incelenmesi, filigran tekniklerinin manipülasyona karşı duyarlılık, algılanabilirlik ve sağlamlık açısından sınırlamaları üzerine tartışmaları gündeme getirmekte ve güvenilirliklerinin tam olarak garanti edilemeyebileceğini göstermektedir. Bu bulgular, filigran teknolojilerinin dijital içerik telif hakkı ve güvenliğini korumak için tam bir çözüm sunamayabileceğini göstermektedir.

İlk yöntemde (Gugelmann ve diğ., 2018), insan gözünün parlaklık değişimlerine karşı duyarsızlığından faydalanarak ekranlardaki metin içeriğine görünmez filigran yerleştirilmesi, adli soruşturmalara yardımcı olma potansiyeli taşımaktadır. Ancak yöntem, filigranların değişmemiş fotoğraflardan geri alınabileceğini vurgulamaktadır. Bu durum, filigranların yüzeysel bir şekilde yerleştirildiği anlamına gelir ve yetkisiz kişiler tarafından kolayca çıkarabilme riski doğurur. Ayrıca, filigranların farklı işletim sistemleri ve grafik kartlarında aynı şekilde algılanamayacağı bir gerçektir. Bu durum, filigranların bazı cihazlarda etkili olmasını sağlarken, diğer cihazlarda algılanmasını zorlaştırabilir. İşletim sistemi ve donanım farklılıkları, yöntemin genel etkinliğini azaltmaktadır. Yöntemin uygulanması, karmaşık kriptografik işlemler ve konvolüsyonel kodlama gerektirmektedir. Bu işlemler, özellikle düşük performanslı cihazlarda zaman alıcı olabilir ve kullanıcı deneyimini olumsuz etkileyebilir. Ayrıca, gerçek zamanlı veri koruma gereksinimi olan senaryolarda yöntem yetersiz kalabilir.

İkinci yöntemde (Piec & Rauber, 2014), filigran görünürlüğünü ve sağlamlığını değerlendiren bir çalışma yapılmıştır. Çalışma, filigranların belirli boyutlarda kullanıldığında fark edilmediğini ancak daha büyük boyutlarda tespit edilebildiğini ortaya koymuştur. Bu durum, filigran görünürlüğü ile korunan içerik içeren bölgelere doğru yerleştirme arasında bir denge kurulması gerektiğinin altını çizmektedir. Bununla birlikte, çalışma, filigranın değiştirilmemiş ekran görüntülerinden kolayca çıkarılabileceğini de göstermiştir. Bu durum filigranın dayanıklılığı ve etkin koruma kabiliyeti konusunda ciddi endişelere yol açmaktadır. Ekranın belirli bölgelerinde küçük katmalar yerine tam ekran katman kullanılması kullanıcıyı sınırlamakla

kalmayıp aynı zamanda filigranın tespit edilebilirliğini arttırmaktadır. Bu yöntemin sınırlamaları ve koruma eksiklikleri tartışma konusu olabilir.

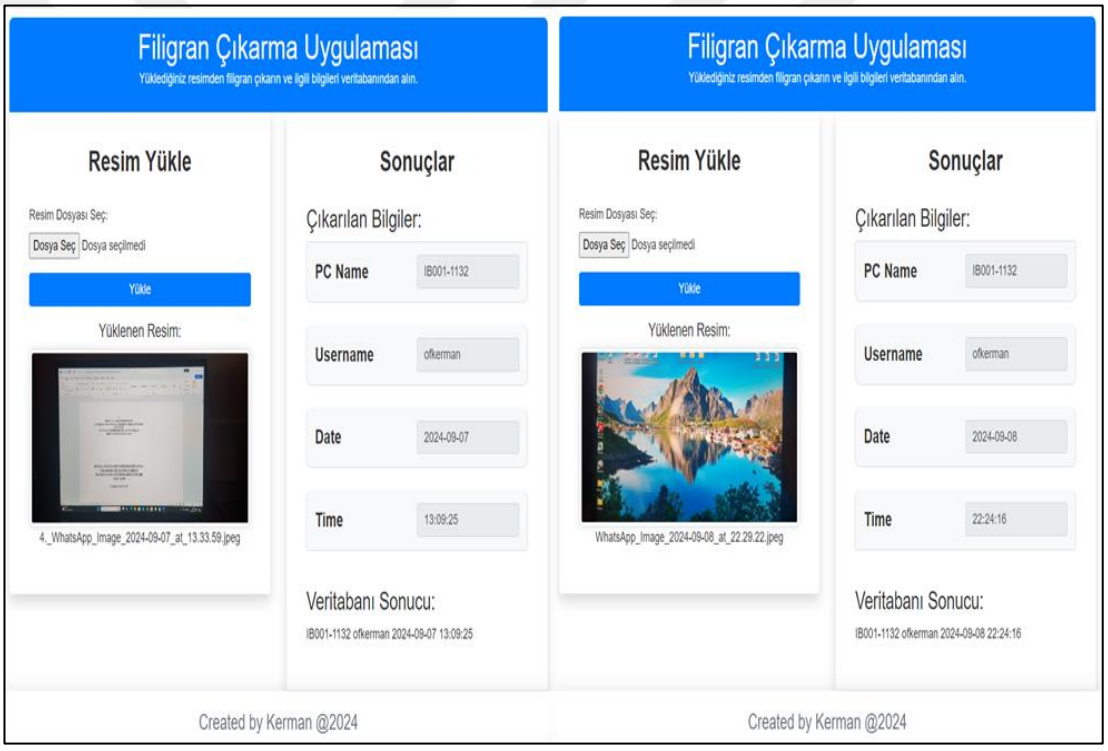
Üçüncü yöntem (R. Bai ve diğ., 2022) bir filigranlama yöntemi olan SSDeN Çerçevesini incelemiştir. Deneysel çalışmalar bu yöntemin etkinliğini göstermiştir. Ancak incelemede de belirtildiği gibi sağlamlık testleri çeşitli ölçekleme ve JPEG sıkıştırma oranları altında gerçekleştirilmiştir. Sonuçlar, SSDeN Çerçevesinin yüksek dayanıklılık sergilediği sonucuna varmıştır. Bununla birlikte, bu testlerin gerçek dünya senaryolarını tam olarak yansıtıp yansıtmadığı konusunda tartışmalar ortaya çıkabilir. Gerçekte, çeşitli saldırılar ve manipülasyon yöntemleri potansiyel olarak filigranı atlayabilir. Bu nedenle, bu yöntemin gerçek dünya uygulamalarında gerçekten ne kadar etkili ve güvenilir olduğunu tespit etmek için daha fazla araştırma ve tartışma gerekebilir.

5.2. Önerilen Yöntemin Değerlendirmesi

Önerilen Ekran Filigranlama yaklaşımı, veri ihlalleri ve ekran içeriğinin yetkisiz kullanımı ile uğraşan dijital suçluları tespit etmek için yeni ve gelişmiş bir yöntemi temsil etmektedir. Mevcut filigranlama tekniklerinin sınırlamalarını ele alarak ve yenilikçi özellikler ile hibrit bir yaklaşımı entegre ederek dijital güvenliğin gelişen zorluklarına sağlam ve uyarlanabilir bir çözüm sunmaktadır. Filigranda kullanılan resim dosyası değişmeyen sabit bir dosya olarak düşünülmüştür. Ekrana görünmeyen filigran eklemeden önce şeffaf katman için kullanılacak resim dosyasının anahtar noktaları ve özellik bölgeleri bir defaya mahsus tespit edilmektedir. Bu noktalara gizli bilgiler steganografik yöntemlerle dinamik olarak eklenmektedir. Yani, eklenen gizli bilgi belirli sürelerde değişmekte ve her değişen gizli bilgi için ayrı kriptografik gizli anahtar kullanılmaktadır. Burada üretilen gizli bilgi, gizli anahtar, şifrelenmiş bilgi ve bundan elde edilen doğrulama (hash) değeri veritabanına anlık olarak zaman damgalı olarak kaydedilmektedir. Veritabanı kullanımı elde edilen bilginin doğruluğunu kanıtlamak için sisteme entegre edilmiştir. Steganografik yöntemlerden En küçük anlamlı bit (LSB), Tensör ayrıştırma (TD) ve Ayrık kosinüs dönüşümü (DCT) yöntemleri yine hibrit olarak kullanılmıştır. Bu yöntemlerden özellikle Tensör ayrıştırma metodunun, bulanıklaştırma, ölçeklendirme, JPEG, döndürme, lens ve aydınlatma gibi manipülasyonlara karşı en dayanıklı yöntem olduğu tespit edilmiştir (Li ve diğ., 2021). Ayrıca birden fazla anahtar noktasına ve özellik bölgesine gizli

bilginin eklenmesi sayesinde çekim bozulmalarına karşı da önlem alınmıştır. Böylece filigranın sağlamlığı, duyarlılığı ve algılanamamazlığı arttırılmıştır.

Önerilen metodun bir demonstrasyonu olarak geliştirilen ilk prototip, temel saldırılara karşı başarılı bir şekilde filigranlandığını göstermiştir. İlk değerlendirme sonuçlarına göre, filigran uygulaması çalışırken cep telefonuyla çekilen orijinal görüntü, filigran çıkarma adımları uygulanarak analiz edilmiştir. Bu süreçte, cep telefonuyla çekilen fotoğraf üzerinde ilk olarak filigranın varlığı ve dayanıklılığı test edilmiştir. Orijinal fotoğrafın çeşitli manipülasyonlara tabi tutulmadan önceki hali, filigranın başarıyla eklendiği ve filigran çıkarma adımları sonucunda gizli bilgilerin doğru bir şekilde kurtarıldığı görülmüştür. Bu aşamada elde edilen sonuçlar, Şekil 5.1'de detaylı bir şekilde gösterilmiştir.

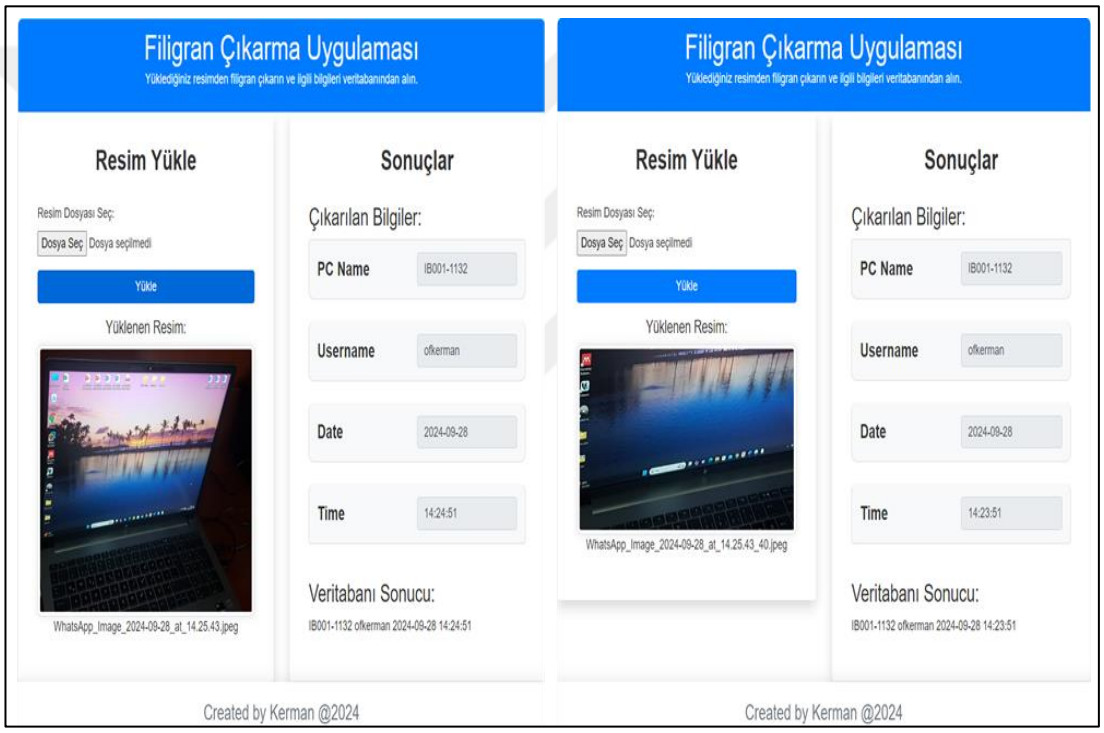


Şekil 5.1: Orjinal Görüntüden Tespit.

Şekil 5.1, filigran eklenmiş orijinal görüntünün ve filigran çıkarma işlemi sonrasında elde edilen verilerin görsel bir temsilini içermektedir. Bu aşama, filigran ekleme ve çıkarma işlemlerinin temel adımlarını ve elde edilen başarıyı ortaya koymaktadır.

Orijinal fotoğrafın farklı manipülasyonlara tabi tutulmasıyla birlikte filigranın dayanıklılığı daha ileri düzeyde test edilmiştir. Özellikle, filigranlı görüntü %40 oranında kırpılmış ve bu kırpma işlemi sonrasında bile filigranın gizli bilgileri koruma kapasitesinin devam ettiği gözlemlenmiştir. Kırpma işlemi, filigranın sadece belirli bir

bölümünün korunmasına rağmen, bu bölümdeki filigranın hala işlevsel olduğu ve gizli bilgilerin çıkarılabildiği sonucunu ortaya koymuştur. Ayrıca, görüntü çeşitli açılardan çekilmiş ve %20'ye varan parlaklık ayarlamaları gibi temel fotoğraf manipülasyonlarına tabi tutulmuştur. Bu manipülasyonların ardından, filigrana gömülü bilgilerin hala kurtarılabildiği kaydedilmiştir. Özellikle, perspektif değişiklikleri ve parlaklık ayarlamalarının filigran üzerindeki etkisi incelenmiş ve filigranın bu tür değişikliklere karşı da dayanıklı olduğu görülmüştür. Bu manipülasyonlarla elde edilen yeni görüntü, tekrar filigran çıkarma uygulamasına sokulmuş ve aynı başarılı sonuçlar elde edilmiştir. Şekil 5.2'de çeşitli manipülasyonların görüntüleri gösterilmiştir.

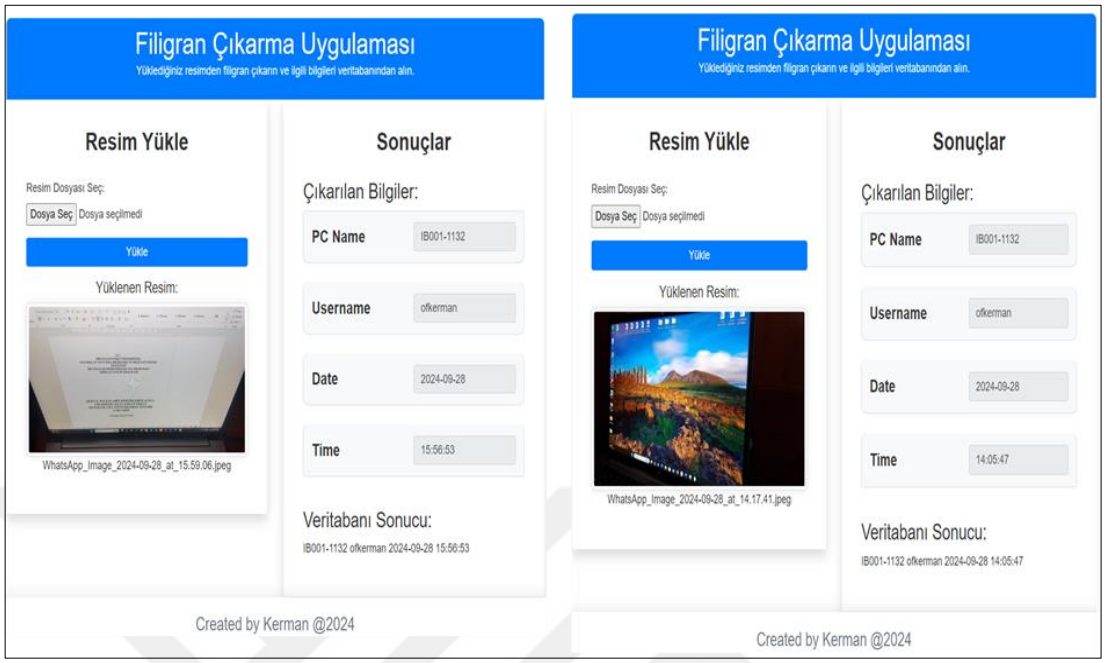


Şekil 5.2: Manipülasyonlu Görüntüden Tespit.

Şekil 5.2, manipülasyonlara tabi tutulmuş görüntülerin filigran çıkarma işlemi sonrasında elde edilen verilerle birlikte gösterildiği bir görsel sunum içermektedir. Bu şekil, filigranın kırpma ve açısal çekim gibi yaygın manipülasyonlara karşı dayanıklılığını ve gizli bilgileri koruma kapasitesini net bir şekilde ortaya koymaktadır. Bu bulgular, önerilen metodun çeşitli manipülasyonlara rağmen etkin bir şekilde çalıştığını ve filigranın güvenilir bir koruma sağladığını kanıtlamaktadır.

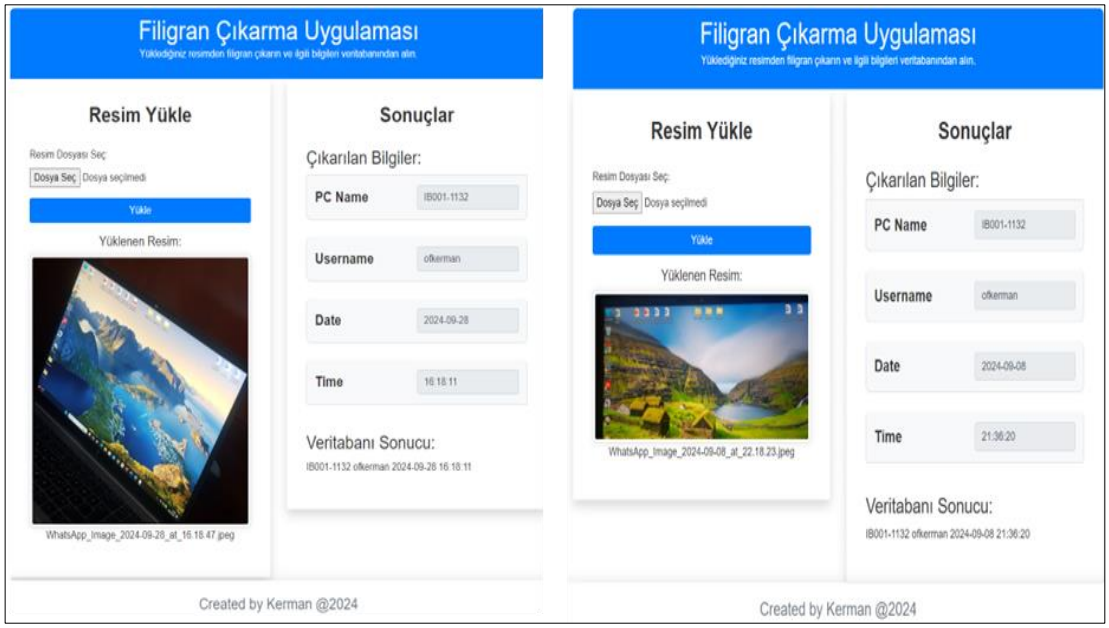
Şekil 5.3 ve Şekil 5.4'te sunulan görsellerde, filigranın çeşitli manipülasyonlar karşısında gösterdiği performans detaylı olarak incelenmiştir. Yatay ve dikey

perspektif çekimlerinde, ekran görüntüsünün açısal değişikliklere rağmen filigran dayanıklılığını ve gizli bilgileri koruma kapasitesini koruduğu gösterilmiştir.



Şekil 5.3: Manipülasyonlu Görüntüden Tespit.

Aynı zamanda, ekranın yalnızca kısmi bir bölgesinin çekilmesi gibi senaryolarda da filigran başarılı bir şekilde tespit edilebilmiştir. Ekranın döndürülmesi veya çevrilmesi gibi manipülasyonlara karşı yapılan testlerde de filigranın dayanıklılığı kanıtlanmış ve filigran bütünlüğü bozulmamıştır. Bu testler, önerilen yöntemin farklı saldırı ve manipülasyonlara karşı ne denli güvenilir olduğunu ortaya koymaktadır.



Şekil 5.4: Manipülasyonlu Görüntüden Tespit.

Sonuç olarak, önerilen yöntem ile geleneksel filigran algoritmalarının yanı sıra kriptografik ve steganografik yöntemlerin avantajlarından en iyi şekilde faydalanılmıştır. Bu sayede, ekran görüntüsü alarak veri sızıntısı yapan kişiyi tespit etmeyi amaçlayan ve özel bilgileri koruyan etkili bir mekanizma oluşturulmuştur. Bu yaklaşım, ekran çekimi yoluyla veri sızıntısı yapılan resimlerden dijital suçlunun kimliğini belirlemeyi ve bu kişiyi olayla ilişkilendirmeyi sağlamaktadır.

Bu yöntem, kurumda kullanılan diğer bilişim sistemlerinin oluşturduğu logların toplandığı Güvenlik Bilgileri ve Olay Yönetimi (Security Information And Event Management, SIEM) aracı ile entegre bir şekilde çalıştırılabilir. Böylece, önerilen filigranlama yöntemi ile elde edilen gizli bilgiler SIEM loglarıyla karşılaştırılarak doğrulanabilir ve işlenilen dijital suçun kim tarafından, hangi bilgisayarda ve ne zaman işlendiğinin kesinliği sağlanabilir.

Sızıntı kaynağının tespiti noktasında, ekran filigranlama yöntemi ile elde edilen bulgular, SIEM aracı olmasa bile, kurum ağlarında kullanılan diğer güvenlik sistemlerinin log kayıtları ile çapraz doğrulamaya tabi tutulabilir. Bu sayede, sızıntının kesin kaynağı daha net ve güvenilir bir şekilde belirlenebilir. Bu kapsamda; ağ trafiği izleme sistemleri, kullanıcı etkinlik kayıtları ve erişim logları gibi farklı veri kaynakları bir araya getirilerek kapsamlı bir analiz yapılabilir. Böylece, güvenlik ihlallerinin hızlı ve etkili bir şekilde tespit edilip, gerekli önlemlerin alınması sağlanır.

Ayrıca, bu yöntem sayesinde idari ve adli soruşturmalarda delil olarak kullanılabilecek zaman damgalı ham loglar kolaylıkla tespit edilebilir. Bu durum, kurumların ekran çekimi yoluyla gerçekleştirilen güvenlik olaylarına karşı daha hazırlıklı olmasını ve bu tür güvenlik ihlallerine karşı daha etkili bir şekilde mücadele edebilmesini sağlar. Kurumlar, bu kapsamlı yaklaşım sayesinde ekran çekimi kaynaklı güvenlik açıklarını minimize ederek, bilgi güvenliğini en üst düzeyde koruma altına alabilirler.

5.3. Deneysel Bulgular

Yapılan testlerde önerilen ekran filigranlama yöntemi, toplam 100 çekimden 98'inde başarılı olmuştur. Özellikle açısal çekim, kırpma, parlaklık değişikliği ve mesafe gibi yaygın manipülasyonlar uygulanmasına rağmen filigran algılama ve bilgi çıkarma işlemlerinin büyük bir çoğunluğu doğru sonuç vermiştir. Yalnızca aşırı manipülasyonlar (örneğin, %45'in üzerinde döndürme veya %50'den fazla çözünürlük

kaybı) durumunda filigranın dayanıklılığında kısmi bir azalma gözlemlenmiştir. Bu sonuçlar, filigran algoritmasının cep telefonuyla çekilen görüntülerde oldukça dayanıklı olduğunu ve gizli bilgileri koruma konusunda etkili bir çözüm sunduğunu göstermektedir. Tablo 5.1, çeşitli manipülasyon türlerinin filigranın başarısı üzerindeki etkilerini göstermektedir.

Tablo 5.1: Çeşitli Manipülasyonların Filigranın Başarısı Üzerindeki Etkileri.

Manipülasyon Türü	Açıklama	Başarı Oranı (%)	Açısal Çekim (Üst)	Açısal Çekim (Alt)	Açısal Çekim (Sağ)	Açısal Çekim (Sol)
Kırpma	Görüntünün %40 oranında kırpılması, kalan filigranın gizli bilgileri koruma kapasitesini test eder.	%98	Başarılı	Başarılı	Başarılı	Başarılı
Parlaklık Ayarı	Görüntüde %20'ye kadar parlaklık değişikliği, filigranın gizli bilgileri üzerindeki etkisini test eder.	%96	Başarılı	Başarılı	Başarılı	Başarılı
Açısal Çekim	Farklı açılardan (üst, alt, sağ, sol) yapılan çekimler, filigranın dayanıklılığını değerlendirmek için kullanılır.	%98	%95 (0°-70°)	%94 (0°-45°)	%96 (0°-80°)	%93 (0°-80°)
Dikey Perspektif	Ekranın yukarıdan ve aşağıdan çekimlerinde filigranın dayanıklılığı test edilir.	%95	%95 (0°-70°)	%94 (0°-45°)	-	-
Yatay Perspektif	Ekranın sağdan ve soldan çekimlerinde filigranın dayanıklılığı değerlendirilir.	%96	-	-	%96 (0°-80°)	%93 (0°-80°)

Yapılan testler, filigran teknolojisinin farklı manipülasyon ve saldırı türlerine karşı gösterdiği dayanıklılığı kapsamlı bir şekilde incelemektedir. Örneğin, görüntünün %40 oranında kırpılması durumunda filigranın başarı oranı %98 olarak belirlenmiştir. Bu bulgu, filigranın gizli bilgileri koruma kapasitesinin yüksek olduğunu göstermektedir. Görüntüde %20'ye kadar yapılan parlaklık ayarları da filigranın dayanıklılığını %96 başarı oranıyla koruduğunu ortaya koymaktadır. Farklı açılardan yapılan çekimlerde tatmin edici sonuçlar elde edilmiştir; örneğin, 0° - 70° aralığında yapılan üst açısal

çekimlerde filigran %95'lik bir başarı ile etkili bir şekilde korunmuştur. Dikey ve yatay perspektiflerde de benzer başarı oranları elde edilmesi, filigranın çeşitli açılara karşı dayanıklı olduğunu göstermektedir.

Saldırılara karşı filigran teknolojisinin dayanıklılığını test etmek, bu güvenlik yönteminin gerçek dünya senaryolarında ne kadar etkili olduğunu anlamak açısından kritik bir öneme sahiptir. Farklı saldırı türleri, filigranın algılanabilirliğini ve koruma kapasitesini doğrudan etkileyebilir. Bu nedenle, filigranların çeşitli manipülasyonlara ve saldırılara nasıl tepki verdiği detaylı olarak incelenmiş, belirli koşullar altında filigranın sağlamlığını ve güvenilirliğini ölçmek amacıyla kapsamlı testler gerçekleştirilmiştir. Tablo 5.2, saldırı türlerinin filigranın algılanma oranı üzerindeki etkilerini göstermektedir.

Tablo 5.2: Saldırı Türlerinin Filigranın Algılanma Oranı Üzerindeki Etkileri.

Saldırı Türü	Açıklama	Algılama Oranı (%)	Başarı Oranı (%)	Sonuç
Mesafe (Kamera ile Ekran Arası)	**30 - 120 cm** arası mesafede filigran başarıyla algılanmıştır.	%95	%95	Mesafe arttıkça algılama oranında azalma gözlemlenmiştir.
Bulanıklık	**5x5 kernel** ile bulanıklaştırma sonrası filigran algılanabilmiştir.	%85	%92	Bulanıklığın etkisi sınırlıdır, gizli bilgiler kurtarılmıştır.
JPEG Sıkıştırma	**%10 - %90** kalite aralığında JPEG sıkıştırma yapılmıştır.	%88	%90	Yüksek sıkıştırmada bilgi kaybı artmıştır.
Döndürme	**%0 - %45** arası döndürme filigranı etkilememiştir.	%90	%93	Büyük açılarda algılama oranı düşmüştür.
Renk Değiştirme	**Grayscale dönüşüm** sonrası filigran algılanabilir durumda kalmıştır.	%94	%94	Filigran renkten bağımsız şekilde çalışmıştır.
Kısmi Ekran Çekimi	Belirli ekran bölümlerinde filigran uygulanabilirliği test edilmiştir.	%80	%85	Filigran, ekranın belirli bölümlerinde başarıyla algılanmıştır.

Saldırı türleri üzerinde yapılan testlerde, kamera ile ekran arasındaki mesafenin filigranın algılanma oranına etkisi incelenmiştir. 30 cm ile 120 cm arasındaki çekimlerde filigranın algılanma başarı oranı %95 olarak belirlenmiştir. Mesafenin artması durumunda algılama oranında bir azalma gözlemlenmiş, bu da sistemin etkinliğini etkileyen bir faktör olduğunu ortaya koymuştur. Ayrıca, 5x5 kernel ile yapılan bulanıklaştırma işlemleri sonrasında filigranın başarı oranı %92 olarak belirlenmiştir; bu durum filigranın bulanıklık altında bile dayanıklı olduğunu

göstermektedir. JPEG sıkıştırma işlemlerinde %10 - %90 kalite aralığında filigran bilgilerinin %90'a kadar başarıyla geri kazanılması, filigranın sıkıştırma işlemlerine karşı dayanıklılığını ortaya koymaktadır. Döndürme işlemleri %0 - %45 aralığında filigranı etkilemezken, daha büyük döndürme açılarında algılama oranında düşüş gözlemlenmiştir. Görüntü grayscale'e çevrildiğinde filigranın algılanabilirliği test edilmiştir ve sonuçlar, renk dönüşümünün filigran üzerindeki etkisinin minimal olduğunu ortaya koymuştur. Son olarak, kısmi ekran çekimlerinde ise ekranın sadece belirli bölgelerinin çekilmesine rağmen %85 başarı oranı ile %80 algılama oranına ulaşıldığı, bu tür çekimlerde bile filigranın etkili olduğu belirlenmiştir.

Sunulan saldırı türleri ve başarı oranları, filigran teknolojisinin gerçek dünya uygulamalarında karşılaşabileceği durumları yansıtmaktadır. Bu bağlamda, test sonuçları, filigran teknolojisinin çeşitli manipülasyon ve saldırı senaryolarına karşı ne ölçüde dayanıklı olduğunu göstermekte ve böylece uygulayıcıların daha güvenli sistemler geliştirmelerine yardımcı olmaktadır. Örneğin, ekran kırpma, parlaklık ayarı, açısal çekim ve mesafe gibi gerçek hayatta sıkça karşılaşılabilecek durumların simülasyonu, filigranın güvenliğini ve etkinliğini artırma konusunda önemli bilgiler sunmaktadır. Bu tür testler, uygulayıcıların sistemlerini bu tür potansiyel saldırılara karşı nasıl koruyabilecekleri ve filigran teknolojisini hangi durumlarda en etkili bir şekilde kullanabilecekleri hakkında fikir sahibi olmalarını sağlar. Böylece, geliştiriciler ve güvenlik uzmanları, filigran teknolojisinin sağlamlığını göz önünde bulundurarak daha güvenli, dayanıklı ve etkili sistemler oluşturma fırsatını elde ederler. Bu yaklaşım, sadece mevcut sistemlerin iyileştirilmesine değil, aynı zamanda gelecekteki potansiyel saldırılara karşı daha proaktif önlemler alarak güvenlik standartlarının yükseltilmesine de katkı sağlamaktadır.

5.4. Literatüre Etkileri

Önerilen yöntem, ekran filigranlama alanında literatüre çok önemli katkılar sunmakta ve hem teorik hem de uygulamalı açıdan çeşitli yenilikler içermektedir. Geleneksel filigranlama yöntemleri genellikle yalnızca tekil manipülasyonlara karşı dayanıklılığı test ederken, bu çalışma birden fazla manipülasyonu aynı anda içeren senaryolar üzerinden filigranın sağlamlığını değerlendirmektedir. Örneğin, açısal çekim, kırpma ve parlaklık değişikliği gibi birden fazla manipülasyonun bir arada uygulanması durumunda dahi filigranın başarılı bir şekilde korunması ve çıkarılması, literatürde

eksik kalan bir alanı doldurarak daha kapsamlı bir test yaklaşımı sunmaktadır. Bu yönüyle önerilen yöntem, gerçek dünya senaryolarında filigranın çoklu manipülasyonlara karşı direncini artırarak daha etkin bir koruma sağlamaktadır.

Geliştirilen sistemin bir diğer önemli özelliği, sabit filigranlar yerine dinamik olarak değişen ve her ekran görüntüsü veya harici çekim sırasında farklı bilgileri şifreleyip ekleyen bir yapıya sahip olmasıdır. Bu yaklaşım, filigranın statik bir yapıda kalmasının yarattığı zayıflıkları ortadan kaldırarak, dinamik içeriklerle gerçek zamanlı ve içerikten bağımsız bir koruma sunmaktadır. Her bir ekran görüntüsünde farklı verilerin eklenmesi, suistimal edilme riskini büyük ölçüde minimize etmekte ve iç tehditlere karşı daha güçlü bir koruma sunmaktadır. Dinamik içerik ekleme yeteneği, suçluların filigranları geçersiz kılma olasılığını ciddi şekilde azaltarak dijital suçluları tespit etme konusunda önemli bir yenilik sunmaktadır. Bu yaklaşım, filigranın statik kalmasının getirdiği güvenlik açıklarını ortadan kaldırarak daha esnek ve güvenilir bir çözüm oluşturmaktadır.

Gerçek zamanlı ve içerikten bağımsız filigranlama avantajı, literatürdeki diğer yöntemlerin büyük bir kısmının genellikle statik veya içerikle bütünleşik filigran yapıları kullandığı düşünüldüğünde, oldukça belirgin bir yenilik sağlamaktadır. Önerilen metodoloji ile filigran, ekrandaki mevcut içerikten bağımsız bir şekilde uygulanmakta ve algılanmaması sağlanmaktadır. Bu yaklaşım, özellikle dijital içerik manipülasyonlarının yaygın olduğu senaryolarda, filigranın dijital suistimal riskini büyük ölçüde azaltmaktadır. Bu özellik, statik filigran kullanan diğer yöntemlere göre çok daha esnek ve güvenli bir çözüm sunmakta ve filigranların tespit edilmesini zorlaştırarak güvenliği bir adım ileriye taşımaktadır.

Ayrıca, önerilen sistemin çoklu filigran basma yeteneği de literatüre önemli bir katkı sunmaktadır. Uygulama, ekranın çeşitli yerlerine aynı anda birden fazla filigran yerleştirilebilmekte ve her filigran farklı dinamik bilgiler içermektedir. Bu çoklu filigranlama yapısı, tek bir filigranın farkedilmesi veya manipüle edilmesi durumunda bile ekran üzerinde kalan diğer filigranlar yoluyla korumanın devam etmesini sağlayarak dijital suçlara karşı çok daha sağlam bir güvenlik katmanı sunmaktadır. Çoklu filigranlama, tekil filigran kullanan yöntemlere göre daha dirençli bir yapı sunarak literatürdeki boşlukları doldurmakta ve dijital suistimal girişimlerine karşı daha kapsamlı bir koruma sağlamaktadır.

Önerilen metodun hibrit bir yapıya sahip olması da önemli bir yenilik olarak öne çıkmaktadır. Sistem, farklı algoritmaların avantajlarını bir araya getirerek daha dayanıklı ve esnek bir filigranlama mekanizması sunmaktadır. Hibrit yöntemler, tek bir algoritmanın zayıflıklarını diğer algoritmaların güçlü yönleriyle telafi ederek, manipülasyonlara karşı daha yüksek bir direnç sağlamaktadır. Bu durum, literatürdeki diğer yöntemlere kıyasla, hem dayanıklılığı hem de güvenliği artırarak, gerçek dünya uygulamalarında daha etkili bir çözüm ortaya koymaktadır.

Bunlara ek olarak, önerilen metodun SIEM (Güvenlik Bilgileri ve Olay Yönetimi) gibi kurumsal güvenlik çözümleri ile entegre çalışabilmesi, yalnızca filigranın tespit edilmesini değil, aynı zamanda dijital suistimalin kesin kaynağının belirlenmesini de kolaylaştırmaktadır. Bu entegrasyon, güvenlik ihlallerinin daha kapsamlı ve güvenilir bir şekilde tespit edilmesine olanak tanıyarak, literatüre nadir görülen bir katkı sunmaktadır. Böylece, potansiyel güvenlik tehditleri daha hızlı analiz edilmekte ve proaktif önlemler alınarak organizasyonel güvenlik duruşu güçlendirilmektedir.

Sonuç olarak, önerilen yöntem, gerçek zamanlı, içerikten bağımsız ve çoklu filigran basma gibi yenilikçi özellikleriyle mevcut filigranlama yöntemlerine kıyasla önemli avantajlar sunarak veri sızıntılarına karşı daha gelişmiş bir koruma mekanizması oluşturulmasına katkı sağlamaktadır. Özellikle çoklu manipülasyonlara karşı dayanıklılığı, hibrit algoritma kullanımı, dinamik içerik ekleme yeteneği ve kurumsal güvenlik sistemleri ile entegrasyon gibi nitelikleriyle bu yöntem, hem akademik hem de pratik uygulamalar açısından önemli bir yenilik ve gelişme sunmaktadır. Çalışma, dijital güvenlik alanında yeni bir yaklaşım geliştirerek gelecekteki araştırmalar ve uygulamalar için güçlü bir temel oluşturma potansiyeline sahiptir.

6. SONUÇ ve GELECEKTEKİ ÇALIŞMALAR

Bu çalışmada, ekran içeriğinin korunması için algılanamayan düşük yoğunluklu bir filigranlama tekniği geliştirilmiştir. Önerilen düşük yoğunluklu filigranlama tekniği, ekran içeriğine algılanamayan bir filigran ekleyerek, veri hırsızlığına karşı etkili bir savunma mekanizması sağlamaktadır. Bu tekniği daha da geliştirmek için, yüksek hata oranları, tekdüze olmayan hata dağılımları ve parçalı ekran şekilleri de dâhil olmak üzere ekran filigranının özel zorluklarıyla başa çıkmak için evrişim kodlarına dayalı bir kodlama şemasının geliştirilmesi gibi belirli alanlarda daha fazla çalışma gerekebilir.

Bilgisayar ekranlarında fark edilebilir dijital izler bırakmadan veri hırsızlığına karşı koymak için gizli filigranlar oluşturmanın birincil hedefiyle, veri ihlalleriyle bağlantılı tespit bilgilerinin, orijinal içerikte gizli filigranlar içeren sızdırılmış görüntülerden geriye dönük olarak alınmasına olanak tanımaktadır. Elde edilen bu bilgiler daha sonra hem adli hem de idari soruşturmalarda ikna edici kanıtlar olarak kullanılabilir.

Özellikle, gelecekteki çalışmalar, çok katmanlı filigranlama, davranışsal analiz entegrasyonu, makine öğrenmesi ve derin öğrenme gibi yenilikçi tekniklerin bir araya getirilmesini öngörmektedir. Bu birleşik yöntem, filigranlama sürecini daha önce görülmemiş güvenlik ve uyarlanabilirlik seviyelerine yükseltmeyi amaçlamaktadır. Çok katmanlı filigranlama ile birlikte, farklı bilgi katmanlarının yerleştirilmesi ve davranışsal analiz ile anormalliklerin tespit edilmesi, daha etkili bir güvenlik önlemi sağlayacaktır. Ayrıca, filigran eklenecek resim dosyalarının anahtar noktalarını tespit etmede literatürde var olan klasik yöntemlerin kullanılması yerine derin öğrenme tekniklerinin kullanımıyla, resimlerden anahtar nokta tespiti gibi detaylı bilgilerin elde edilmesi ve bu bilgilerin filigran stratejilerinin iyileştirilmesinde kullanılması hedeflenmektedir.

Birden fazla bilgi katmanı yerleştirmek, bilgisayar ekranına yerleştirilecek filigranların konumlarını tespit etmek için davranışsal analiz entegrasyonunu sağlamak ve bu sayede filigranlama stratejilerini iyileştirerek veri hırsızlığı tespitini geliştirmek için makine öğreniminden yararlanarak oluşturulacak yaklaşım, dinamik

bir tehdit ortamına karşı esnek bir koruma sağlayarak dijital güvenlik alanında önemli bir rol oynayacaktır. Ayrıca, elde edilen verilerin adli ve idari soruşturmalarda kanıt olarak kullanılabilmesi, bu tekniklerin güvenilirliğini ve etkinliğini daha da artıracaktır. Gelecekteki çalışmaların, bu alanlarda daha derinlemesine ve kapsamlı bir araştırma yaparak, dijital içeriklerin korunması konusundaki mevcut zorlukları daha etkili bir şekilde ele alması beklenmektedir.

KAYNAKÇA

Alattar, A. M., & Alattar, O. M. (2004). *Watermarking electronic text documents containing justified paragraphs and irregular line spacing* (E. J. Delp III & P. W. Wong, Eds.; p. 685). https://doi.org/10.1117/12.527147

Author, C., Dayalin Leena, G., & Selva Dhayanithy, S. (2013). Robust Image Watermarking in Frequency Domain. In *International Journal of Innovation and Applied Studies* (Vol. 2, Issue 4). http://www.issr-journals.org/ijias/

Bai, R., Li, L., Zhang, S., Lu, J., & Chang, C.-C. (2022). SSDeN: Framework for Screen-Shooting Resilient Watermarking via Deep Networks in the Frequency Domain. *Applied Sciences*, *12*(19), 9780. https://doi.org/10.3390/app12199780

Bai, Y., Li, L., Zhang, S., Lu, J., & Emam, M. (2023). Fast Frequency Domain Screen-Shooting Watermarking Algorithm Based on ORB Feature Points. *Mathematics*, *11*(7), 1730. https://doi.org/10.3390/math11071730

Bay, H., Tuytelaars, T., & Van Gool, L. (2006). *SURF: Speeded Up Robust Features* (pp. 404–417). https://doi.org/10.1007/11744023_32

Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). Techniques for data hiding. *IBM Systems Journal*, *35*(3.4), 313–336. https://doi.org/10.1147/sj.353.0313

Caronni, G. (1995). Assuring Ownership Rights for Digital Images. In *Verläßliche IT-Systeme* (pp. 251–263). Vieweg+Teubner Verlag. https://doi.org/10.1007/978-3-322-91094-3_16

Chen, W., Ren, N., Zhu, C., Zhou, Q., Seppänen, T., & Keskinarkaus, A. (2020). Screen-Cam Robust Image Watermarking with Feature-Based Synchronization. *Applied Sciences*, *10*(21), 7494. https://doi.org/10.3390/app10217494

Chopra, D. (2012). Lsb Based Digital Image Watermarking For Gray Scale Image. *IOSR Journal of Computer Engineering*, *6*(1), 36–41. https://doi.org/10.9790/0661-0613641

Chugh, G., & Student, M. T. (2013). Information Hiding-Steganography & Watermarking: A Comparative Study. In *International Journal of Advanced Research in Computer Science* (Vol. 4, Issue 4). www.ijarcs.info

Cox, I. J., Kilian, J., Leighton, F. T., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, *6*(12), 1673–1687. https://doi.org/10.1109/83.650120

Embar, M., McHugh, L. F., & Wesselman, W. R. (2014). Printer watermark obfuscation. *Proceedings of the 3rd Annual Conference on Research in Information Technology*, 15–20. https://doi.org/10.1145/2656434.2656437

Fang, H., Zhang, W., Zhou, H., Cui, H., & Yu, N. (2019). Screen-Shooting Resilient Watermarking. *IEEE Transactions on Information Forensics and Security*, *14*(6), 1403–1418. https://doi.org/10.1109/TIFS.2018.2878541

Gohshi, S., Nakamura, H., Ito, H., Fujii, R., Suzuki, M., Takai, S., & Tani, Y. (2005). *A New Watermark Surviving After Re-shooting the Images Displayed on a Screen* (pp. 1099–1107). https://doi.org/10.1007/11552451_152

Gu, S., Han, J., Sun, X., & Cao, Y. (2022). Robust Watermarking of Screen-Photography Based on JND. *Computers, Materials & Continua*, *71*(3), 4819–4833. https://doi.org/10.32604/cmc.2022.023955

Guan, H., Huang, Y., Zhang, S., & Liu, J. (2023). A Survey of Screen Shooting Resilient Image Watermarking Algorithms. *2023 International Conference on Culture-Oriented Science and Technology (CoST)*, 12–17. https://doi.org/10.1109/CoST60524.2023.00012

Gugelmann, D., Sommer, D., Lenders, V., Happe, M., & Vanbever, L. (2018). Screen watermarking for data theft investigation and attribution. *2018 10th International Conference on Cyber Conflict (CyCon)*, 391–408. https://doi.org/10.23919/CYCON.2018.8405027

Gupta, R., Gupta, S., & Singhal, A. (2014). Importance and Techniques of Information Hiding : A Review. *International Journal of Computer Trends and Technology*, *9*(5), 260–265. https://doi.org/10.14445/22312803/IJCTT-V9P149

Gupta, S., Baraskar, R., & Agrawal, S. (2019). A survey on Reversible Watermarking Techniques for Image Security. *International Research Journal of Engineering and Technology*. www.irjet.net

Hoda, M. N., Bharati Vidyapeeth's Institute of Computer Applications and Management (New Delhi, I., & Institute of Electrical and Electronics Engineers. Delhi Section. (2014). *Proceedings of the 8th INDIACom, 2014 International Conference on Computing for Sustainable Global Development (05th - 07th March, 2014) : INDIACom-2014*.

Jain1, J., & Johari2, P. (2014). Digital Image Watermarking Based on LSB for Gray Scale Image. In *IJCSNS International Journal of Computer Science and Network Security* (Vol. 14, Issue 6).

Kadian, P., Arora, S. M., & Arora, N. (2021). Robust Digital Watermarking Techniques for Copyright Protection of Digital Data: A Survey. *Wireless Personal Communications*, *118*(4), 3225–3249. https://doi.org/10.1007/s11277-021-08177-w

Kang, S., Jin, B., Liu, Y., & Wang, Z. (2023). Research on Screen Shooting Resilient Watermarking based on Dot-Matric. *2023 2nd International Conference on Big*

Data, Information and Computer Network (BDICN), 194–199. https://doi.org/10.1109/BDICN58493.2023.00048

KERMAN, Ö. F., & ŞİMŞEK, A. (2024). Screen Watermark: A Novel Approach in Detecting Digital Criminals. *Gazi Journal of Engineering Sciences*, *9*(3), 612–621. https://doi.org/10.30855/gmbd.0705091

Li, L., Bai, R., Zhang, S., Chang, C.-C., & Shi, M. (2021). Screen-Shooting Resilient Watermarking Scheme via Learned Invariant Keypoints and QT. *Sensors*, *21*(19), 6554. https://doi.org/10.3390/s21196554

Lowe, D. G. (2004). Distinctive Image Features from Scale-Invariant Keypoints. *International Journal of Computer Vision*, *60*(2), 91–110. https://doi.org/10.1023/B:VISI.0000029664.99615.94

Mehan, V., Dhir, R., & Brar, Y. S. (2013). A Spatial Domain Approach of Fingerprinting for Colored Digital Images SUBJECT CLASSIFICATION TYPE (METHOD/APPROACH) Fingerprinting Council for Innovative Research. In *Peer Review Research Publishing System Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY* (Vol. 11, Issue 1). www.cirworld.com,

Mikolajczyk, K., & Schmid, C. (2005). A performance evaluation of local descriptors. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *27*(10), 1615–1630. https://doi.org/10.1109/TPAMI.2005.188

Nikolaidis, N., & Pitas, I. (1998). Robust image watermarking in the spatial domain. *Signal Processing*, *66*(3), 385–403. https://doi.org/10.1016/S0165-1684(98)00017-6

Orebaugh, A. D. (2004). *Steganalysis: A Steganography Intrusion Detection System*.

Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding-a survey. *Proceedings of the IEEE*, *87*(7), 1062–1078. https://doi.org/10.1109/5.771065

Piec, M., & Rauber, A. (2014). Real-Time Screen Watermarking Using Overlaying Layer. *2014 Ninth International Conference on Availability, Reliability and Security*, 561–570. https://doi.org/10.1109/ARES.2014.83

Priyadharsini, S., & Thamizhmaran, K. (2023). A study of data security using cryptography. *International Journal of Engineering in Computer Science*, *5*(1), 19–22. https://doi.org/10.33545/26633582.2023.v5.i1a.84

Shieh, C.-S., Huang, H.-C., Wang, F.-H., & Pan, J.-S. (2004). Genetic watermarking based on transform-domain techniques. *Pattern Recognition*, *37*(3), 555–565. https://doi.org/10.1016/j.patcog.2003.07.003

Shimpi, M. R., & Gumaste, P. S. V. (2015). Digital Image Watermarking Resilient to Local Desynchronization Attacks. In *IJSRD-International Journal for Scientific Research & Development*| (Vol. 3). www.ijsrd.com

Simmons, G. J. (1979). Symmetric and Asymmetric Encryption. *ACM Computing Surveys*, *11*(4), 305–330. https://doi.org/10.1145/356789.356793

singh, G., Singh, H., & Singh, A. K. (2024). A Review Paper on Network Security and Cryptography. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4482635

Singh, H. K., & Singh, A. K. (2024). Digital image watermarking using deep learning. *Multimedia Tools and Applications*, *83*(1), 2979–2994. https://doi.org/10.1007/s11042-023-15750-x

Tsui, T. K., Zhang, X.-P., & Androutsos, D. (2008). Color Image Watermarking Using Multidimensional Fourier Transforms. *IEEE Transactions on Information Forensics and Security*, *3*(1), 16–28. https://doi.org/10.1109/TIFS.2007.916275

Van Schyndel, R. G., Tirkel, A. Z., & Osborne, C. F. (1994). *A DIGITAL WATERMARK*.

Xie, G., Liu, Y., Xin, G., & Yang, P. (2019). *Review on Text Watermarking Resistant to Print-Scan, Screen-Shooting* (pp. 140–149). https://doi.org/10.1007/978-3-030-24271-8_13

Yakushev, A. Y., Markin, Y. V., Fomin, S. A., Obydenkov, D. O., & Kondrat'ev, B. V. (2021). Text documents screen watermarking by changing background brightness in the interline spacing. *Proceedings of the Institute for System Programming of the RAS*, *33*(4), 147–162. https://doi.org/10.15514/ISPRAS-2021-33(4)-11

Zhang, Y. (2009). Digital watermarking technology: A review. *2009 International Conference on Future Computer and Communication, FCC 2009*, 250–252. https://doi.org/10.1109/FCC.2009.76

Zhou, G., & Lv, D. (2011). An Overview of Digital Watermarking in Image Forensics. *2011 Fourth International Joint Conference on Computational Sciences and Optimization*, 332–335. https://doi.org/10.1109/CSO.2011.85