BİYOMETRİK VERİLERDE KESİKLİ DALGACIK DÖNÜŞÜMÜNE DAYALI FİLİGRAN TEKNİKLERİNİN ANALİZİ

Foday JORH

Yüksek Lisans Tezi

Dr. Öğr. Üyesi Barış ÖZYER

Bilgisayar Mühendisliği Anabilim Dalı

2020

T.C.
ATATÜRK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

BİYOMETRİK VERİLERDE KESİKLİ DALGACIK DÖNÜŞÜMÜNE DAYALI FİLİGRAN TEKNİKLERİNİN ANALİZİ

(Analysis of Watermarking Techniques Based on Discerete Wavelet Transformation in Biometric Data)

YÜKSEK LİSANS TEZİ

Foday JORH

Danışman: Dr. Öğr. Üyesi Barış ÖZYER
İkinci Danışman: Dr. Öğr. Üyesi Claude FACHKA

Erzurum
Temmuz, 2020

Ek-3. Kabul ve Onay Tutanağı Sayfası

KABUL VE ONAY TUTANAĞI

Foday Jorh tarafından hazırlanan "Biyometrik Verilerde Kesikli Dalgacık Dönüşümüne Dayalı Filigran Tekniklerinin Analizi" başlıklı çalışması 06 / 07 / 2020 tarihinde yapılan tez savunma sınavı sonucunda başarılı bulunarak jürimiz tarafından Bilgisayar Mühendisliği Ana Bilim Dalı, Bilgisayar Mühendisliği Bilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir.

Jüri Başkanı:	Prof.Dr. A.Samet Haşıloğlu *Atatürk Üniversitesi*
Danışman:	Dr. Öğr. Üyesi Barış Özyer *Atatürk Üniversitesi*
Jüri Üyesi:	Dr. Öğr. Üyesi Saeid Agahian *Erzurum Teknik Üniversitesi*
Jüri Üyesi:	Dr. Öğr. Üyesi Tolga Aydın *Atatürk Üniversitesi*
Jüri Üyesi:	Dr. Öğr. Üyesi Ahmet Çoskunçay *Atatürk Üniversitesi*
İkinci Tez Danışmanı	Assist. Prof. Dr. Claude Fachka *University of Dubai*

Enstitü Yönetim Kurulunun 12/12/2019 tarih ve 48/17 sayılı kararı.

Bu tezin Atatürk Üniversitesi Lisansüstü Eğitim ve Öğretim Yönetmeliği'nin ilgili maddelerinde belirtilen şartları yerine getirdiğini onaylarım.

Unvan Ad SOYAD

Enstitü Müdürü

Not: Bu tezde kullanılan özgün ve başka kaynaklardan yapılan bildiriş, çizelge, şekil ve fotoğrafların kaynak olarak kullanımı, 5846 sayılı Fikir ve Sanat Eserleri Kanunundaki hükümlere tabidir

ETİK BİLDİRİM VE İNTİHAL BEYAN FORMU

*Tez türünü giriniz. Ör. Yüksek Lisans veya Doktora*Tezi olarak *Danışmanın Ünvanı Adı Soyadı* danışmanlığında sunulan "*Tezin başlığını girmek için tıklayın*" başlıklı çalışmanın tarafımızdan bilimsel etik ilkelere uyularak yazıldığını, yararlanılan eserlerin kaynakçada gösterildiğini, Fen Bilimleri Enstitüsü tarafından belirlenmiş olan Turnitin Programı benzerlik oranlarının aşılmadığını ve aşağıdaki oranlarda olduğunu beyan ederiz.

Tez Bölümleri	**Tezin Benzerlik Oranı (%)**	**Maksimum Oran (%)**
Giriş	*Tezdeki benzerlik oranın yazınız*	**30**
Kuramsal Temeller	*Tezdeki benzerlik oranın yazınız*	**30**
Materyal ve Yöntem	*Tezdeki benzerlik oranın yazınız*	**35**
Bulgular	*Tezdeki benzerlik oranın yazınız*	**20**
Tartışma	*Tezdeki benzerlik oranın yazınız*	**20**
Tezin Geneli	*Tezdeki benzerlik oranın yazınız*	**25**

Not: *Yedi kelimeye kadar benzerlikler ile Başlık, Kaynakça, İçindekiler, Teşekkür, Dizin ve Ekler kısımları tarama dışı bırakılabilir. Yukarıdaki azami benzerlik oranları yanında tek bir kaynaktan olan benzerlik oranlarının* ***%5'den*** *büyük olmaması gerekir.*

Beyan edilen bilgilerin doğru olduğunu, aksi halde doğacak hukuki sorumlulukları kabul ve beyan ederiz.

Tez Yazarı (Öğrenci)	**Tez Danışmanı**
Öğrenci Adını ve Soyadını yazmak için tıklayınız	Danışmanın Unvanını Adını ve Soyadını yazmak için tıklayınız
Tarih girmek için burayı tıklayınız	Tarih girmek için burayı tıklayınız
İmza:	İmza:

***** Tez ile ilgili YÖKTEZ'de yayınlamasına ilişkin bir engelleme var ise aşağıdaki alanı doldurunuz.

☐ Tezle ilgili patent başvurusu yapılması / patent alma sürecinin devam etmesi sebebiyle Enstitü Yönetim Kurulunun …./…/…. tarih ve ……. sayılı kararı ile teze erişim 2 (iki) yıl süreyle engellenmiştir.

☐ Enstitü Yönetim Kurulunun …./…/…. tarih ve ……. sayılı kararı ile teze erişim 6 (altı) ay süreyle engellenmiştir

TEŞEKKÜR

Bu çalışmanın yapılmasında bana her türlü desteği veren, değerli yardımlarını ve anlayışını esirgemeyen, bilgi ve deneyimleriyle bana yol gösteren, danışmanım Sayın Dr. Öğretim Üyesi Barış ÖZYER'e teşekkür ederim.

Çalışmalarım esnasında fikri ve teknik olmak üzere, öneri ve yardımlarla bulunan, hep desteğini gördüğüm Sayın Dr. Öğretim Üyesi Mohammad Reza MİLANİ'ya, samimi katkıları için Sayın Dr. Claude FACHKHA ve tezin İngilizceden Türkçeye çevirisine desteği ve bana ayırdığı zaman için değerli arkadaşım İsmail Kamil KARAKAŞ'a teşekkür ederim.

Bize bu çalışmada her kullanılan biyometrik veri kümesini sağladığı için J. Fierrez, J. Ortega-Gracia, D. Torres-Toledano ve J. Gonzalez - Rodriguez'e teşekkür ederim.

Ayrıca, Yurtdışı Türkler ve Akraba Topluluklar Başkanlığı (YTB) tarafından Türkiye Bursları kapsamında verilen burs (Burs no: 16GM000094) ve Laboratuvar imkânları ile sağladığı teçhizat ve destekler içi Atatürk Üniversitesi Bilgisayar Mühendisliği Bölümüne teşekkür ederim.

Bana her zaman maddi ve manevi destek veren sevgili aileme teşekkür ederim.

Foday JORH

ÖZET

YÜKSEK LİSANS TEZİ

BİYOMETRİK VERİLERDE KESİKLİ DALGACIK DÖNÜŞÜMÜNE DAYALI FİLİGRAN TEKNİKLERİNİN ANALİZİ

Foday JORH

Danışman: Dr. Öğr. Üyesi Barış ÖZYER
İkinci Danışman: Dr. Öğr. Üyesi Claude FACHKA

Amaç: Bu tez çalışmasında, biyometrik verilerin gömülmesi ve çıkarılması için kesikli dalgacık dönüşümü (KDD) frekans bantlarını değerlendirir ve analiz edilmiştir.

Yöntem: Bu çalışma filigran görüntüsünü gömmek ve çıkarmak için KDD ile birleştirilmiş tekil değer ayrıştırması (TDA) kullanılmıştır. kesikli dalgacık dönüşümü (KDD) frekans bandında biyometrik verilerin gömülmesi ve çıkarılması için alfa harmanlama yaklaşımı kullanılarak ve kullanılmadan tek seviyeli ve çok seviyeli filigran teknikleri incelenmiş ve analiz edilmiştir.

Bulgular: Sağlamlığını incelemek ve sıkıştırma fonksiyonunun filigranlı görüntünün bütünlüğünü yok edip etmediğini kontrol etmek için sıkıştırma ve dekompresyon yaklaşımlarının performansı analiz edilmiştir. Ayrıca, farklı alt bantlarda filigran tekniklerinin görüntü işleme ve geometrik saldırılara karşı ne kadar sağlam olduğunu araştırılmıştır.

Sonuç: Deneysel sonuçlar incelendiğinde, çok düzeyli KDD ve TDA filigranlama yaklaşımının tek düzeyli fligran yöntemlerinden daha sağlam olduğu gözlemlenmiştir. Yüksek yoğunluklu alfa değerinde KDD frekans bandları yaklaşık katsayı bandına (LL) baskın olduğu gözlemlenmiştir. Yoğunluk değeri azaldığında ise diğer bantlarda daha kararlı olduğu gözlemlenmiştir. Önerilen yaklaşımın kararlılığını ve verimliliğini kontrol etmek için, biyometrik veri kümesinin ürettiği sonuçları Lena (konak görüntüsü) ve Baboon (filigran görüntüsü) veri kümeleri ile karşılaştırmıştır.

Anahtar Kelimeler: ayrık dalgacık dönüşümü; tekil değer ayrışma; kapak resmi; filigran; stego-görüntü;

Temmuz 2020, 58 sayfa

ABSTRACT

MASTER THESIS

ANALYSIS OF WATERMARKING TECHNIQUES BASED ON DISCERETE WAVELET TRANSFORMATION IN BIOMETRIC DATA

Foday JORH

Adivsor: Dr. Öğretim Üyesi Barış ÖZYER
Co-Advisor: Assit. Prof. Dr. Claude FACHKA

Purpose: The thesis evaluates and analyses the discrete wavelet transform (DWT) frequency bands for embedding and extracting of the biometric data.

Method: for embedding and extracting of the biometric data the DWT single-level and multilevel watermarking approach with and without the use of alpha blending approach. In addition, singular value decomposition (SVD) combined with DWT is used to embed and extract the watermark image.

Findings: The performance of compression and decompression approaches has been analyzed to examine the robustness and to check whether the compression function does destroy the integrity of the watermarked image. We investigate the proposed approach to understand how robust the watermarked on different sub-band is against the image processing and geometric attacks.

Results: The experimental results show that the DWT multi-level and SVD watermarking approach is more robust than the other watermarking methods implemented in this paper. The DWT bands dominate the approximate coefficient band (LL) in high-intensity alpha value. When the intensity is reduced, the coefficient standout to be very robust against the remaining bands. In other to check how robust and efficient our algorithm is, we used public dataset such as Lena (host image) and the Baboon (watermark image) to test and constrast the results generated by the biometric dataset.

Keywords: Discrete Wavelet Transform; Singular Value Decomposition; Cover image; Watermark

July 2020, 58 pages

İÇİNDEKİLER

TABLOLAR DİZİNİ

ŞEKİLLER DİZİNİ

SİMGELER ve KISALTMALAR DİZİNİ

Semboller

cA	Yaklaşık katsayısı
cD	Köşegen katsayısı
cH	Yatay Katsayısı
cV	Dikey katsayısı

Kısaltmalar

BER	Bit Hata Oranı
DCT	Ayrık Kosinüs Dönüşümü
KDD	Ayrık Dalgacık Dönüşümü
MSE	Ortalama Kare Hatası
NC	Normalleştirilmiş Korelasyon
PSNR	Tepe Sinyal Gürültü Oranı
TDA	Tekil Değer Ayrışımı

GİRİŞ

İnternet'in hızlı büyümesi, hassas verilerin depolanması, işlenmesi ve okunmasıyla ilişkili potansiyel güvenlik tehditleri hakkındaki endişeleri artırmıştır. Telif haklarına yönelik güvenlik tehditleri, bilgi sistemlerine yetkisiz erişimi ve diğer güvenlik sorunları türlerini tespit etmek son yıllarda veri güvenliği ile ilgilenen araştırmacıların ilgilendiği konuların başında gelmektedir (Khan, Zhang, and Tian, 2004)(Jain and Nandakumar, 2012). Biyometrik uygulamalar tarafından kullanılan verilerin gizliliğini olası tehditlere, yani bilgisayar korsanlarına ve sosyal mühendislere karşı korumak için etkili yöntemlere ihtiyaç duyulmaktadır (Ibm, 2003),(Nandakumar, Jain, and Nagar, 2008) ve (Jain and Nandakumar, 2012). Bununla birlikte, bilgi hırsızlığı ve casuslukda dahil olmak üzere, verileri hedef alan siber saldırıların katlanarak büyümesi, veri sağlayıcıları, veri sahipleri, hizmet sağlayıcıları, hükümetler ve diğer kuruluşların karşılaştığı kritik bir sorun teşkil etmektedir. Bu nedenle, filigran oluşturma, verilerin sahipliğini doğrulamak, verilerin orijinalliğini ve bütünlüğünü korumak için uygun bir seçenek olduğu kabul edilmektedir. Dijital filigranın geliştirilmesi gerek resmi kurumların (bankalar, devlet kurumları vb.) gerekse multimeyda kurumları için (televizyon, sosyal media, internet vb.) dünya çapında ağ üzerinden verilerin korunması ve izlenmesini gerekli hale getirmiştir. Geleneksel yöntemler yani tek şifre kullanımı, güvenliği tek başına çözüm üretemediği, bu nedenle, biyometrik kimlik ve doğrulama sisteminin geliştirilmesi veri güvenliği için ihtiyaç haline gelmiştir. Çoğu şirketin geleneksel güvenlik sisteminden biyometrik sisteme geçmesinin bir başka nedeni de, birden fazla kimliğe (örneğin pasaport) sahip kişilerin tanınmasına ve tespitine karşı önlem almaktır. Biyometrik sistemler farklı kimlikler kullanan sahte bireyleri tespit etmemize yardımcı olmaktadır.

Bu tez çalışmasında, biyometrik imgelerdeki frekans bantlarından hangilerinin veri bütünlüğü ve belirli bir bandın sağlam olduğu, ayrıca bozunma ve gömülme mukavemeti bakımından sağlam olduğunu belirlemek için ayrı dalgacık dönüşümünün (KDD) tabanlı frekans bantlarını inceledik. Ayrıca, tek ve çok seviyeli filigranlama yaklaşımları, farklı gömme güçleri kullanılarak ayrıntılı olarak analiz ettik. Son olarak, gömme işleminde alfa oyunlarının sağlamlık ve algılanamazlık düzeyini belirlemek için KDD ve tekil değer ayrıştırma (TDA) algoritmasının farklı alfa (gömme mukavemeti) yoğunluklarının testlerini gerçekleştirdik.

Motivasyon

Son yıllarda digital ortamda kullanıcı sayısının artması ile beraber dijital güvenlik çok önemli bir konu haline gelmiştir. Veri ve bilgilerin özellikle internet ortamında korunmasında gereklidir. Bu motivasyon ile biyometrik verilerin dijital fligran basma teknikleri ile incelenmesi amaçlanmıştır. Dijital filigran basma, dijital bilgiyi aynı veya farklı bir ortam olan başka bir ortama katmayı içeren bir bilim sanat olup veri güvenliği sağlamada bir yol olarak kullanılmaktadır. Filigran alanında, filigranı kasıtlı ve kasıtsız saldırılara karşı güvenli bir şekilde öneren ve zahmetsizce çalışan farklı çalışmalarla bulunmaktadır. Dalgacık dönüşüm alanı filigranlama teknikleri hakkında çeşitli öneriler ve uygulamalar vardır. Dalgacık dönüşüm alanı, dijital filigranlamada en kullanışlı tekniktir çünkü görüntü işleme dallarında Ayrık Fourier Dönüşümü (DFT) ve Ayrık Kosinüs Dönüşümü (DCT) gibi tekniklerden daha iyi performans göstermiştir. Bu, parmak izi, yüz, iris, avuç içi baskısı ve benzeri gibi biyolojik kalıtsal özelliklerin kullanımını içerir. Biyometrik güvenliğin icadından bu yana, şifre paylaşımı araçlarını büyük ölçüde ortadan kaldırmıştır. Biyometrik güvenlik sistemi yürürlükte olduğundan, internet üzerinden iletim sırasında sinyal işleme, gürültü ve diğer saldırı modlarına karşı biyometrik özelliklerin güvence altına alınması gerekmektedir.

Tezin Amacı

Bu tez çalımasında amacımız, ayrık dalgacık dönüşümünü kullanarak biyometrik verileri gizlemek ve güvence altına almak için en verimli frekans bandını incelemektir. Bu amaçla tez kapsamında farklı fligram ayrışma tekniklerini test ettik ve inceledik. Ayrık dalgacık dönüşümünü frekans alanı tekniğiyle birleştirdik. Öte yandan, gömme mukavemetinin yoğunluğu üzerinde ayrıntılı analizler gerçekleştirdik. Amacımız gömme gücünü farklı güçler göre verimliliğini incelemek ve filigran görüntüsünün en verimli algılanamazlığı hangi seviyede oluşturacağını gösterebilmektir.

Ayrık dalgacık dönüşüm alanı, esas olarak yaklaşık katsayıya (LL) odaklanan gizli görüntüyü filigranlamak için kullanılır (Hasan, Ngah, and Salleh, 2013)(Sharma and Swami, 2013) and (AL-Nabhani et al. 2015). KDD' nin diğer algoritmalarla kombinasyonunu içeren çalışmalarda gömme tekniğini kullanmıştır (Lai and Tsai, 2010) and (Araghi, Manaf, and Araghi, 2018). Literatürdeki çalışmalarda gözelemlediğimiz kadarı ile sadece LL bandına gömme işleminin gerçekleştirildiği, diğer bandların kullanılmadığı anlaşılmaktadır. Bu tez çalışmasında gömme işleminin biyometrik verilerde neden diğer bandlarda uygulanmadığını araştırmayı amaçladık. Bu bizi ilk yaklaşıma götürerek LL frekans bandının diğer bantlardan (HH, HL, LH) daha sağlam bir bant olup olmadığını belirlememize yardımcı olacağı varsayımını öne sürdük. Ayrıca, bulgularımızın sadece tek seviyeli filigran ayrışma tekniğine

dayanmaması nedeniyle çok seviyeli ayrışma filigranını analiz ettik. Daha sonra tek seviyeli ayrışmayı çok seviyeli ayrışmaya göre karşılaştırdık. Yaklaşımımız biyometrik verilerin depolanmasında dalgacık paket ayrışması kullanılarak çift takviye yaklaşımının önerildiği çalışmaya dayanmaktadır (Rzouga Haddada, Dorizzi, and Essoukri Ben Amara, 2017a). Bu çalışmada, " WPD filigran tekniğini kullanmak KDD tekniğini kullanmaktan daha güçlüdür." sonucuna varmışlardır. Bizde çalışmamızda sırrı (filigran) gömmek ve çıkarmak için tekil değer ayrışma (TDA) ile çok seviyeli KDD kullanılarak biyometrik ve genel verisetleri üzerinde deneylerimizi gerçekleştirdik.

Son olarak, gömme yaklaşımına analiz ettikten sonraki adım, bazı görüntü işleme, gürültü, filtre ve geometrik saldırılara karşı filigran görüntü verimliliğini inceledik. Önerilen tekniklerin söz konusu saldırılara karşı ne kadar sağlam olduğunu değerlendirdik. Aynı zamanda, gömme gücünün (Alfa) farklı güç üzerindeki etkilerini inceledik.

Teze Katkı

Bu tez kapsamında, KDD frekans bantlarının farklı tipteki fligran atakları üzerindeki etkileri incelendi ve analiz edildi. Bu ataklar geometrik, gürültü, filtre ve kırpma gibi saldırılardır. KDD' yi TDA algoritması ile birleştirerek tek seviyeli, çok seviyeli frekans bandlarında ayrıntılı analizleri yapıldı. Thanki and Borisagar (2015), (Lai and Tsai, 2010) ve (Araghi *et al.* 2018) filigranın gömülmesinde yaklaşık katsayı kullanılabileceğini önerdi. Bu çalışmaları göz önüne alarak, bu tezde gömme kuvvetinin algılanamazlığın sağlanmasında LL bantlarında etkisini inceledik. Güç ve sınırlamaları gömmek için birden fazla gücü test ettik. Çok düzeyli filigran tekniğinde, Sharma ve Swami'nin çalışmasına dayanan alfa karıştırma filigran şemasını ekledik (Sharma ve Swami, 2013). Tüm KDD frekans bantları için deneyler gerçekleştirdik ve sonuçlarımız LH bandında daha yüksek olduğunu gösterdik. Ayrıca tek seviyeli alfa harmanlamasını da ekledik. Tek ve çok seviyeli alfa harmanlamasını doğruluğunu karşılaştırdık.

Hem tek hem de çok seviyeli ayrışma KDD'deki sonuçlarımıza göre, yüksek frekanslı bant, filigranlı görüntülere uygulanan saldırıların zorunluluğuna karşı daha iyi performans verdiğini gözlemledik.

KURAMSAL TEMELLER

Neredeyse tüm araştırmacılar, biyometrik verileri güvence altına almak konusunda ortak bir noktaya sahiptir. Her biri modern teknolojideki kilit rollerden biri olan güvenlik konusunda tehlikenin olduğunu görüşündedir (Lu *et al.* 2008; Rzouga Haddada et al, 2017a; Shoniregun and Crosier, 2008; Więcław, 2009). Çoğu araştırmada filigran, steganografi, şifreleme ve kriptografi teknikleri kullanılmıştır. Bazıları tek başlarına amaçlarına ulaşmak için bir yöntem kullanırken, bazıları ise filigran algoritması veya kriptografi ve hatta şifreleme ile steganografinin kombinasyonunu kullanmışlardır.

Hasan et al, (2013) 'de, bir donanım görüntü sıkıştırma mimarisi yaklaşımı için KDD kullanan çok seviyeli bir ayrışma şeması önermiştir. KDD'den bahsedilir ve ayrıca VHSIC (çok yüksek hızlı entegre devre) ve donanım açıklama dili (VHDL) tabanlı uygulama ile sentezlenir. Amaç ve hedefleri, JPEG2000 uygulaması için gerekli olan çok seviyeli KDD ayrıştırmasının donanım açıklamasıdır. Çok seviyeli görüntü ayrışması, (Zargar, 2014) 'de kullanılan eğilimdir.,Bu çalışmada konak görüntüsü iki kez ayrıştırılır (ikinci seviye ayrıştırma) ve konak görüntüsü, gizli kapak görüntüsüne gömülmeden önce JPEG sıkıştırma algoritması kullanılarak sıkıştırılır. Filigran ise yalnızca bir kez ayrıştırılır. (Hasan *et al.* 2013; Zargar, 2014)'de ana dalgacık, yani, HAAR dalgacık kullanılmaktadır. Bu çalışmalarda, gizlenecek görüntü (filigran görüntüsü) KDD kullanılarak HL alt bandına gömülmüştür. Üçüncü seviye ayrıştırma yaklaşımı (Sharma and Swami, 2013)'de çalışılmıştır. Ve çalışmaları, düşük frekanslı (LL) alt-bant üzerine odaklanmıştır. Bu çalışmada hem kapak görüntüsü hem de gizli görüntü eşit olarak ayrıştırılmış ve gizli görüntünün gömülmesi ve çıkarılması LL alt bandında yapılmıştır.

HVS (Human Visual system) kullanılarak görüntü filigranı için önerilen bir metodolojidir. Kapak görüntü taşıdığı daha yüksek bir gömme kapasitesine nasıl ulaşabileceklerini ve aynı anda filigranın görünmez olduğundan emin olmalarını sağlamaktır. Işık algılama alanlarına gelince gözlerin kendi etkileri vardır. (örneğin, yüksek çözünürlüklü bantlar söz konusu ve metinsel sınıflandırma söz konusu olduğunda, göz gürültüye cevap vermede çok sessizdir (Fang and Chen, 2009). Göz gürültüye cevap vermekten daha az, görüntünün kenarlarına dikkat eder, parlaklık düşük ve yüksek yoğunluğa bağlı olarak kendi avantaj ve dezavantajları). Yazarlar, sağlamlığın nasıl artırılacağı ve süreç boyunca iyi görsel görünürlük sağlayan filigran yoğunluğunu tanıtmakta ve incelemektedir.

Başka bir makalede, yazar asimetrik filigran kullanmıştır(Ahmed and Siyal, 2005; Nandakumar *et al.* 2008). Bu prosedürde Legendre önerilmiştir (Ahmed and Siyal, 2005; Nandakumar *et al.* 2008). Legendre dizilerinin yaptığı şey, diziyi yerleştirmek için özel anahtarı kullanması ve genel anahtar dizinin uzunluğunu içermesidir. Başka bir araştırmada (Nandakumar *et al.* 2008), bu planın kendi eksiklikleri olduğu tespit edilmiştir. Bu, dizinin yalnızca asal sayılarda (N'nin asal uzunluğu) bulunduğunu gösterir. Yazar ayrıca filigranın simetrik ve asimetrik ekstraksiyon yöntemi için bir hibrit filigran tekniği de önermiştir. Bu yazıda hem özel hem de halka açık filigran gömme şeması uygulanmıştır (Ahmed and Siyal, 2005). İlk olarak, filigran spektrum tekniği kullanılarak orijinal görüntüde özel filigran gizlenir, daha sonra KDD yardımıyla genel filigranı kullanarak filigran olan birincil görüntüye erişilir. Böylece, son filigran görüntü elde etmek için aynı filigran görüntüde hem genel hem de son filigranı içerir. Özel filigranın kullanımı, halkın saldırgan tarafından saldırıya uğradığı veya imha edildiği bir durumda mülkiyeti kanıtlamaktır. Kamusal filigran planının kullanımı, görüntüye gömülü filigran bilgisine sahip olan herkesin, ayıklama ayrıcalığına sahip olmasını sağlamaktır. Örneğin, alıcı ile satıcı arasındaki iş yerinde. Filigranlı görüntünün ve genel anahtarın ICA (Bağımsız Bileşen Analizi) kullanılarak elde edildiği genel filigranı görüntüyü çıkarmak için aynı ortak anahtar tekrar kullanılır (Ahmed and Siyal, 2005). ICA'nın kullanımı, kör kaynak ayırma (BSS) performansına yardımcı olmaktır. Özel anahtar şemaya gelince, hem şifreleme hem de şifre çözme, yayılı spektrum tekniklerinin kullanımı ile öncüdür.

Hu *et al.* (2014)'te steganalizin filigran basma üzerindeki etkileri hakkındabir çalışma gerçekleştirmiştir. Yazarlar, tamamen gizli imaj üzerindeki etkisine odaklanmak yerine, bir oyun teorisi önermektedir. Oyun teorisinde, saldırganların (steganalysis) etkilerini ve kazara yapılan saldırıları (diğer bir deyişle kasıtsız) hesaplamak için yanlış negatif olasılık üzerine yoğunlaşmıltır. Bu yazının önerisine dayanarak (Hu *et al.* 2014) BER (bit hata oranı) yanlış negatif olasılık incelenmiştir. FNP (yanlış negatif olasılık), filigranı gerçekten içine alan ve aynı zamanda detektör (filigran detektörü) tarafından doğru şekilde çıkarılmayan kapağa karşılık gelir. BER ayrıca steganaliz ve yanlışlıkla yapılan saldırılar altında da hesaplanır. Deneysel sonuçlarında yanlış negatif olasılığın tespitine dayanarak verimli olduğu gözlemlenmiştir. Amaç, steganalizin ne yaptığını veya kasıtsız saldırıları tespit etmektir. Öte yandan, sonuçlar önerilen yöntemin, gizli filigranın steganaliz teknikleri kullanılarak kasıtsız saldırıdan geçmesi durumunda filigran tespitinin güvenilirliğini ölçebileceğini göstermiştir (Hu *et al.* 2014). Steganalizin temel işlevi, ortam içinde gömülü bilgi olup olmadığını tespit etmektir (görüntü, metin, ses, video vb.). Steganalizin gizli bir iletişim tespit ettiği bir noktada, gizli iletişimden kaçınmak için imha edebilir.

Zhang, Gao, Jiang, Zhang ve Zhang (2011)'te, metinsel ve sayısal verileri kullanan ilişkisel bir veri tabanındaki filigran sistemi önermiştir. Çalışmada toplana veri kümesinin dezavantajı bulunmaktadır. Diğer multimedya verilerini karşılaştırdığımızda, veri tabanının küçük bir yedekliliği vardır ve bu, gizli bitin gömülmesinde oldukça zordur. Filigran basma algoritması, ana odaklanmanın, sayı taban sisteminin içindeki ikili bir görüntüyü saklamak üzerine olduğu önerilmiştir. Ek olarak, metin aynı zamanda rastgele bir kelime sayısına gizlenir. Yukarıda bahsedilenlerle, yöntemleri, alt küme ekleme, değiştirme ve silme türü saldırı gibi saldırılaradayanıklığı incelenmiştir. Aynı yaklaşımla kullanan bir başka makalede (Solanas and Domingo-Ferrer, 2006), sayısal olmayan veri tabanlarının bozulmasını önlemek ve en aza indirgemek için bir öneride bulunulmuştur. Sebebi şudur; sayısal olmayan veri tabanlarını değiştirmek çok zordur. Çünkü herhangi bir değişiklik verileri etkileyebilir. Önerilerinde, bilgi sahiplerinin sayısal olmayan veri tabanlarının korunmasında eş anlamlılık işlevini belirtmelerini sağlayan filigran işlevlerini içermektedir. Ek olarak, (Thangadurai and Sudha Devi, 2014), bazı değerleri başka bir değere değiştirmeye yardımcı olarak bazı özellikleri kategorize eden bir filigrantekniği geliştirdiler.

Rzouga Haddada *et al.* (2017a) 'deki yazarlar, biyometrik verilerin korunmasında daha güçlü bir takviye yöntemi önermiştir. Başka bir deyişle, eldeki bilgileri korumak için aynı filigran tekniklerinin bir kombinasyonunu iki kez kullandılar. Filigran yaklaşımı bir arada olsa bile filigranın sağlamlığının performansını geliştiremediler. Bu yöntemde, parmak izi minutisi yüz görüntüsüne gömülmeden önce çıkarılır. Bu filigranın ilk adımını verir. Ardından yüz filigranı ikili hale getirilir ve parmak izine gömülür (bu durumda orijinal parmak izine yerleştirilir). Çok modlu veri tabanına dayanananaliz ve testler yapılmıştır. Önerdikleri sistemlerin faktörlere göre avantajı doğrulama, görsel kalite (bozulmayan), karmaşıklık ve sağlamlıktır. Önerilen sistemin amacı, doğrulama planının güvenlik seviyesini arttırmaktır. Filigran görüntüsünü mahvetmeden hem kapak (konak) görüntüsünü hem de filigranı alıyor (bu, görüntünün orijinal özelliklerini koruyarak ve hala görüntüsünü koruyarak).

Yang, Hu, Wang, Yang, and Shu, (2013) 'de biyometrik mobil ödeme yaparken ne kadar güvenli olduğuna dair bir çözüm önerileri sunmuştur. Eski sistemi (yani şifre veya PIN ve Jetonlar) karşılaştığını ve kusurlu olduğunu gördüklerini karşılaştırın. Biyometrik teknolojiyi kullanarak mobil ödemeyi en iyi şekilde yapabilecekleri konusunda biyometrik şifreleme sistemini kullanan bir sistem önerdiler. Sistem (şifreleme sistemi) yüksek güvenlik performansı, entegre bir sistem ile tanınma doğruluğu ve sosyal kabul edilebilirlik sunar. Hangi sistemi daha verimli hale getirir? Biyometrik tabanlı sistem ve kullanışlılığını ve zorluklarını anlama detayı üzerine derinlemesine bir incelemeyapılmıştır. Ayrıca çok modlu biyometrik

ödeme sistemi araştırılmıştır (Burrows and Zadeh, 2016). Aynı şekilde, kullanıcının şifre ve belirteçle karşılaştırması çok uygundur. Bir şifre durumunda, unutulabilir ve belirteç kaybedilebilir veya çalınabilir ancak biyometrik olamaz. Öte yandan, biyometrik bilginin yararlarını ayrıntılı olarak açıkladılar. Algılayıcının canlı algılama tesisleri ile yapıldığı bir durumda, taklit etme ve benzeri işlemler zor veya neredeyse imkânsızdır.

Bu yazıda amaç, cep telefonlarında steganografiyi incelemektir(Anusree and Binu, 2015). Bugünün dünyasında bu iki iyi bilinen platformu Android ve IOS Apple kullanılmıştır Ayrıca, bilgileri gizlemek için farklı türlerde steganografi tekniği kullanarak eserler yarattılar ve daha sonra gizli verileri tespit edip etmeyeceklerini araştırmak için steganografik aracı kullandılar (Anusree and Binu, 2015). Cep telefonlarında adli bir steganografik üs ile gelip kendilerini meydan okuyorlar. Adli araçların çoğu kontrol edilirken bilgisayar tabanlıdır. Steganografi, terör ve bilgisayar korsanları tarafından en yaygın kullanılan tekniktir, çünkü adli olmayan medyadaki verileri gizler ve iletişimin gerçekleştiğini fark etmeyi çok zorlaştırır. Örneğin, cep telefonlarında steganografi kullanılıyorsa, verileri elde etmek çok zor olacaktır, ancak aynı yazılımda verileri çıkarmak için geliştirilebilir veya kanıtın altına düşerse daha fazla araştırma için polise verilmesi istenebilir.

Anusree and Binu (2015) 'de çoklu sırlar için filigran kombinasyonu ile görsel tonlama Halftoning kullanarak biyometrik gizlilik önerdi. Dijital Yarı Tonlama, bir görüntüyü mesafeden bakıldığında sürekli bir görüntüye benzeyen noktalı bir diyagram olarak taklit eden bir mekanizmadır. Sırrı (biyometrik veri) bölünmüş ve farklı görüntülerde saklamaktır. Birinin sır bölünmesinden kurtulabilmesi durumunda, bu yine de gizli bilgiyi değiştirmez. Şifre çözme mekanizması benzersizdir ve gizlenmiş bilgileri alabilmek için mevcut olan tüm sırları gerektirir. Başka bir deyişle, şifre çözme VCS tarafından hisse XOR ile birlikte sağlanabilir.

Ibm, (2003) ve Yang *et al.* (2013) Sadece somut gerçeğe ulaşmak için yeni bir yöntem önermiştir. Bu çalışmada VCS metin görüntülerine ve parmak izi görüntüsüne uygulanmıştır. Tüm tekniklerin şifresi çözüldüğü zaman, görsel gözlem söz konusu olduğunda, hem orijinal görüntü hem de çıkarılan görüntü aynıdır. Yüz görüntüsüne gelince 640 * 480 boyutunda kullanılır. İşlemde, yapraklar oluşturuldu ve görüntü VCS kullanılarak gömüldü ve şifresi çözüldüğünde aynı gizli görüntü üretildi. Filigran teknikleri kullanılarak orijinal ve elde edilen görüntüler üzerinde analizler yapılmıştır (Anusree and Binu, 2015; Rzouga Haddada *et al.* 2017b; Yang *et al.* 2013). Sadece basit VCS ile durmazlar (Anusree and Binu, 2015), aynı zamanda farklı VbS türlerini farklı Halftoning kullanarak gizleyerek birden fazla gizli görüntü de uygularlar. Yüz görüntüleri farklı bir frekans kullanılarak yeniden oluşturulur. Deneysel sonuçlara göre, f (frekans) ne kadar yüksekse PSNR'nin o kadar düşük olduğunu gösterir.

Deneyde kullanılan sistem ayrıca kusur ve ilmekli delikleri görmek için incelenmiştir. Bu, paylaşılan anahtarlarla karşılaşıldığında çıkarılan görüntünün sağlam olacağını gösterir. Paylaşım anahtarlarının karşılanmadığı denemenin bir göstergesinde, çıkarma, orijinal sırdan farklıdır. VCS, bir görüntünün iki görüntüye bölünmesini içerir. Görüntülerin iki görüntüye bölünmesi anlamına gelmez. N görüntüsünde ayrılabilir. Bu, belirli sayıda paylaşılan kişiyle (bu durumda kullanıcının) gizli mesajların şifresini çözebileceğini veya açabileceğini ve hisse sayısından (N-1) daha düşük bir şeyin sırrı açamayacağını veya şifresini çözemeyeceğini söyleyen gizli paylaşımlara geri döner. VCS'nin yardımıyla, görüntünün tamamı her alt pikselden yararlanılarak işlenir. Alt piksellerdeki gerekli adımlar, her piksel için rastgele seçilir. Bu süreç nedeniyle, Brüt-kuvvet saldırısını neredeyse imkânsız kılıyor. Deneylerine dayanarak, sonuç şifreli görüntüyü tek bölmenin hala ana gizli görüntünün bilgisini ifşa edemediğini gösterlimiştir.

Whitelam, Osia ve Bourlai, (2013) ile ilgili olarak, biyometrik verileri korumak için büyük bir adım atılmıştır. Filigranlı görüntünün biyometrik verilerinin ortadaki bir adamla temas ettiğinde, temas halindeki görüntüden şüphelenebilir veya araştırabilir. Ancak steganografinin yardımı ile çözümü çok zor olurdu. Steganografi tekniklerinde, herhangi bir şeyden şüphelenmeyi daha da zorlaştıran, adli tabiri anlam ifade etmeyen bir görüntü kullanılır (Shoniregun and Crosier, 2008). Yüz / parmak izi filigranlı görüntünün steganografi teknikleri kullanılarak bilinmeyen başka bir görüntünün içine gömülmesi, steganografi görüntüsünde rastgele yenidenoluşturulmuştur. Buna ek olarak, bu durum sırrı bulmayı çok zorlaştırır. Kayıp görüntü kalitesini ölçmek için PSNR kullanıldı (Ibm, 2003; Jain and Nandakumar, 2012; Khan *et al.* 2004; Nandakumar *et al.* 2008; Shoniregun and Crosier, 2008). Bu, konak görüntüsünün gömmeden önce görüntü ile karşılaştırıldığında tam bir görünüme sahip olması gerektiğine yardımcı oldu. Bu nedenle, izinsiz izleyici hiçbir şeyden şüphelenmez. Kodlama bölümlerinde, biyometrik görüntü RGB'den gri tonlamalı bir görüntüye dönüştürülür. Görüntünün gradyanını verilen bir nokta etrafında kontrol eden ve aynı zamanda çevresinin etrafındaki çapraz şeklinin standart sapmasını kontrol eden formüle edilmiş bir denklem kullanılır. Öte yandan, kodlanacak bitleri düzenlerken gradyan görüntünün sağlamlığını ve standart sapmayı ayarlamaya yardımcı olan parametreler bulunmaktadırKod çözme bölümüne gelince, gömülü bitleri almak için dikkatli olunması gerekir. Bunu başarabilmek için gömülü bit(ler)in yerleştirildiği yer bilinmelidir. Bu da yazarın kod çözme prosedürlerini hafifleten gizli bir anahtar yaratmasına yol açar. Bunun nedeni, kod çözmenin, hatalı bitler verebilecek filigranın çıkarılmasından dolayı bir dizi adımın yaklaştırılmasına dayanmasıdır. Böylece, kesin görüntüyü elde edemez.

Nandakumar *et al.* (2008)'te, bir çerçevenin modifikasyonu yapılıp ve genelleştilmiştir. Böylece biyometrik veri çalışmasının gerekli olduğu farklı ortamlarda çalışabilme imkânı bulunmuştur. Yoğun ve katı güvenlik sağlamak için çok modlu doğrulama uygulanmıştır (Ibm, 2003). Her iki biyometrik özelliğin de orijinal görüntülere göre doğrulandığı yer. Çok modlu biyometrik verilerle çalışmak. Filigran ve steganografi ile birleşimini, güvenliği artırmaya yardımcı olan çok katmanlı bir çerçeve ile birleştirmeyi önerdiler.

Ouslim, Sabri ve Mouhadjer, (2013)'da biyometrik verilerin bir bilgisayar ağında saldırı olmadan ve hatta tespit edilmeden nasıl transfer edilebileceği incelenmiştir. Ayrıca sensörlerin bulunduğu olası saldırı yerlerini de vurguladılar. Bu yazıda kullanılan görüntü sıkıştırma türü JPEG uzantısıdır. Algoritmalarına dayanarak çok verimlidir. Görsel gözlem aynı zamanda, orijinal görüntü ile filigran basılan görüntüyü karşılaştıran Tepe Sinyali-Gürültü Oranı (PSNR) kullanılarak ölçülmüştür. Buna ek olarak, JPEG sıkıştırması uyguladılar, görüntülerdeki çok sayıda sıkıştırma faktörünü analiz edilmiştir. Geometrik dönüşüm açısından sağlamlık, döndürme, kesme ve çeviri testleri incelenmiştir.

Bu alanlarda titizlikle incelemeye yönelik bir güvenlik ve performans analizi yapılmıştır: Histogram analizi, gizli anahtarın hassasiyetini analiz etmek, şifreli görüntü ile orijinal görüntü arasındaki korelasyon (Shoniregun and Crosier, 2008). Steganografi çoğu zaman kriptografi konusu ile ilişkilidir. Steganografiden şüphelenildiği durumda steganografiyle birleştirilen kriptografi, veri güvenliğinde hayati bir rol oynayabilir. Bunun nedeni, steganografiyi tespit etmenin mümkün olması, ancak bilginin şifresini çözmeye çalışan birinin kriptografik şifrelemesini çözmek için hala anahtara ihtiyacı olacak (Thangadurai and Sudha Devi, 2014). Steganografik teknikler veya şemalar filigran bilgisinde çok kullanılmaktadır. Amacı, bilgiyi gizlemek değil, bir medyanın hak sahibini korumaktır (telif hakkı). Steganografide kapak görüntüsünün seçimi de çok önemlidir. Araştırmalar, bunun adli tıpla alakası olmadığını göstermiştir (Burrows and Zadeh, 2016; Kumar and Kumar, 2010; Shirali-Shahreza and Shirali-Shahreza, 2008; Thangadurai and Sudha Devi, 2014; Yan and Ping, 2009).

Şifreleme çok önemli olmasıyla beraber (Ashokarajan, Angelinjosphia, Gayathri, Rajendran, and Anandhakumar, 2014), verilerimizi güvende tutmaya yardımcı olur. İçindeki gömülü verilerin incelenmesine izin veren teknik özellikleri yoktur. Öte yandan, Kriptografik teknikler (Jain and Nandakumar, 2012) şifreli alanların eşleştirilmesinde destek ve yardım sağlar, algılama yaklaşımlarında sensörün canlılığını korur ve son olarak tüm kimlik doğrulama planının bütünlüğünün korunmasına yardımcı olur.

Hepimizin bildiği gibi ATM, işlemlerde önemli bir rol oynayan kullanıcı kartı, ATM pin FİLİGRAN İŞLEMİNİN GENEL AKIŞ ŞEMASI edilecek bir sistem önerdiler. Bu sistemde, yüksek gizlilik politikaları ile aynı anda bir sürecin kolektif sorumluluğuna ulaşmak için bir araya getirilen güvenlik modu bize filigran yolu açar. Bu, bireyin veya bir şeyin mülkiyetini bilmenin en iyi metodolojisini sağlar ve destekler. Daha sonra pin kodunu parmak izi düzeniyle eşleştirdiler. Ardından pin kodu (ATM) yeni bir tanımlamaya göre yeniden düzenlenir.

Çalışmalarında (Rzouga Haddada *et al.* 2017b) pin kodu için dizinin konumlandırılmasıyla parmak izi yoluyla desenlerin oluşturulmasıdır. Her yakalanan parmak izi (Tarayıcıya Göre), çeyreğe (16 çeyrek) ayrılmıştır. Eski konvansiyonel ATM işleminde herhangi bir değişiklik yapılmamıştır. Kullanıcının kart detayını girmesi istendiğinde (pin numarası), bu noktada, bir kullanıcıdan (sistem tarafından) kimlik bilgilerini girmesi istendiğinde, sistem aynı kriptografik tekniklerine odaklanan yeni bir anahtar oluşturur. Bu anahtarlar daha sonra kullanıcının kimliği için daha yararlıdır. Bu işlemler sunucu sonunda uygulanabilir.

Alkhathami, Han and Van Schyndel (2013), parmak görüntüsünü ayrı bir kosinüs dönüşümü kullanarak çift filigranla sabitlemek için bir algoritma önermişlerdir. Gömme işleminden önce ve filigran görüntüsünü çıkardıktan sonra filigran görüntüsünü karşılaştırır ve karşılaştırırlar. Sonuç olarak elde edilen görüntü orijinal görüntüye benzemektedir. Sağlamlığı sağlamak için tuz ve biber gürültüsü saldırı tekniği ugulanmıştır. Yöntemlerinde, parmak izi görüntüsü, iki filigran yerleştirilerek ve aynı zamanda parmak izi yapısını mutlaka tahrip etmeden korunmuştur. Filigran ve tekniklerinin parmak izini etkileyip etkilemediğini kontrol etmek için resimler üzerinde inceleme ve analizler yapılmıştır. Benzerlikler, bunun hiçbir etkisi ve imhası olmadığını göstermektedir. Uygulamanın öte yandan, birinin orijinalliğini ve bütünlüğünü kanıtlamak için parmak izi kullanmak en hızlı ve doğru yaklaşımdır.

DCT algoritması, filigranlı görüntünün parmak izine gömülmesine yardımcı olmak için geliştirilmiştir. Parmak izi görüntüsü, filigranın parmak izine kolayca yerleştirilmesini sağlamak için DCT tabanlı bir algoritma ile bölünmüştür.

Bu makalede (Islam, Sayeed, and Samraj, 2008) eldeki güvenliği ve gizliliği azaltan bir sistem önerdiler. Filigranın kombinasyonuyla iki farklı biyometrik özellik kullanan biyometrik kimlik doğrulama stratejisinden ve kişinin kimlik doğrulamasında yardımcı olan gizli parola şifrelemesinden oluşur. Yazarlar, bu kadar çok saldırıyı ve gizli dinlemeyi engellemenin en iyi yolunu araştırdılar. Araştırmacılar biyometrik sistemlerin farklı saldırı türlerine açık olduğunu fark ettiler. Bu nedendenle, çoğu çalışma biyometrik şablonun en iyi şekilde ne kadar güvenli

olabileceğine odaklanmaktadır. Bu çalışmada, Şifreleme uygun bir şifreleme mekanizması ile kullanılır. Herhangi bir kimlik doğrulama yöntemi ile şablonun ortaya çıkarılacağından emin olurlar.

Bilgisayar korsanları, kulak misafiri, spam gönderenler, kimlik avcıları, vb. Teknolojik alanda herhangi bir modern gelişimdeki boşlukları, sahibine (DOS) erişimi reddeden ya da bilgi edinerek rakibe satarak keşfetmek için buradalar. Güvenliğin araştırılmasının zor bir alan olmasının nedeni budur. (Alkhathami *et al.* 2013) 'de Ayrık Dalgacık Dönüşümü (KDD), gizli şifre şifrelemenin (WHPE) birleştirilmesi için kullanılır.

Steganografi, bilgi gizlenmesinde önemli bir rol oynar. Bu makalede KDD tabanlı görüntü steganografisinin amacı, gizli mesajı (yani CH, CV ve CD) gömme ve bilgileri gizledikten sonra üretilen bu bantların her birini hesaplamak için PSNR kullanarak farklı bir incelemeyi incelemektedir (Kumar and Kumar, 2010). Deneysel sonuçlarına göre, gizli mesajın CD bandına gömülmesi diğerlerinden daha yüksek gürültü verdiği gözlemlenmiştir.Lu *et al.* (2008), filigran kaotik bir harita kullanılarak şifrelenir. Şifrelemeden sonra, biyometrik görüntüler anahtarları üretmek için kullanılır. Bu daha sonra kayıpsız veri gizleme yönteminin yardımıyla avuç izi görüntüsüne yerleştirilir. Son olarak, avuç izi görüntüsünü elde ettikten sonra, steganografik tekniği kullanarak avuç izini gizlemek için filıgranlı görüntüsü kullnılmıştır. Çalışmalarında aynı zamanda, havzanın aşırı segmentasyon sorunu algoritmasına cevap bulmak için diğerinde, FCM (Fuzzy C-Means) uygulanmıştır. Şifre çözme işlemlerinde, XOR işlemini kullanarak şifrelemenin tersini uygulanmıştır. Avuç izini şifreleme sürecinde kullanılan aynı gizli anahtar olan filıgranlı görüntüsü, avuç izini tekrar çözmek için kullanılır. Yazar, önerilen yaklaşım şemasını doğrulamada avuç içi doğruluk tabanının tanıma sistemini iyileştirebilir.

Thanki and Borisagar (2015)'de yazarlar, teklifle karşılaşmadan önce ayrıntılı bir soruşturma yaptılar. Biyometrik sistemin depolanması (veri tabanı) ve kimlik doğrulama yeri (yani sensör diğer bir deyişle, eşleyici modülü) arasındaki biyometrik bilginin kırılganlıklarını araştırdılar. CS (sıkıştırıcı Algılama) teorisi çerçevesine dayanan bu tür güvenlik açığının güvenliğini karşılayacak seyrek filigran tekniklerini kullanarak yeni bir yöntem geliştirdiler. Deneysel raporlarında, seyrek filigran basma metodolojisinin biyometrik sistemin doğrulama ve doğrulama uygulaması üzerinde bir etkisi olmadığını göstermektedir. Dijital filigran, sahip olma, telif hakkı ve aynı zamanda, sahtekârlık gibi saldırılara karşı çözüm ve biyometrik sistemin geçiş kanalındaki biyometrik şablona saldırılar için çözüm olma eğilimidir. Teklifte seyreklik, DCT (Kesikli Kosinüs Dönüşümü), sıkıştırma algılamasında (CS) sağlanır ve Filigran üssü teorisi KDD (Kesikli Dalgacık Dönüşümü) kullanılır. Algoritma, parmak izi

görüntüsünü sahtekârlığa ve modifikasyon saldırılarına karşı koruyan ulaşılabilir bir güvenlik sağlayabilir.

Bu çalışmada Aparna and Ayyappan (2015), Deffie Hellman anahtar değişim algoritması yardımıyla görüntü filigranı önerdi ve uyguladı. Kullanılan filigran basma tekniği ayrık kosinüs dönüşümüdür (DCT). Kapak görüntüsündeki bilgilerin gömülmesi ve ters DCT de filigranın çıkarılmasında kullanıldı. Aynı blok bazlı görüntü filigranı, kriptografik algoritma kombinasyonu ile önerilmektedir. Bu süreçte filigran görüntüsünün kapak görüntüsüyle gömüleceği bir yer bulmak. Deffie Hellman Anahtar Değişimi algoritmasını kullanan bir anahtar üretimi de var. Anahtar, filigran parçalarının gömülü olduğu kapak görüntüsündeki yerin bulunmasına yardımcı olur. Bir blok görüntü tabanı filigranı ve blok dışı bir filigran gömme sistemi arasında bir karşılaştırma yaptılar. Bu da blok temelinin blok olmayanlara göre daha verimli ve sağlam olduğunu göstermektedir. Diğer araştırmalarda, iletim sürecinde hangi tekniklerin en iyi olduğunu bilmeyi çok zorlaştıran birçok saldırı olduğunu göstermektedir.

Yazar, şifreleme ve filigran tekniklerini, anahtarların yardımıyla çok verimli olan geçiş sırasında biyometrik verileri güvence altına alma sürecinde birleştiren bir yöntem önerdi (Aparna and Ayyappan, 2015). Anahtarın şifrelenmesinde asimetrik algoritma kullanılır. Şifreleme yöntemlerini kullanmanın asıl amacı filigranı şifrelemektir. DCT dönüşüm şemasını kullanan önerilen sistemlerinde, hem kapak hem de filigran görüntüsü frekans alanına değiştirilir. Bu elde edildikten sonra, sonuç 32 * 32 bloğa bölünür. Ardından, anahtarları oluşturmak / üretmek için Deffie Hellman anahtar değişim algoritması, filigranın gizleneceği konumu bulmayı gerektirir.

Tareef and Al-Ani (2015)'de bir saldırganın zaten mevcut bir filigranda başka bir filigran başlatması durumunda doğrulamayı kanıtlayacak yeni bir sistem önerdi. Önerilen sistem, TDA ve KDD filigran sistemi ile birlikte çok iyi bir seyrek kodlama tabanlıdır. İki veya insanın mülkiyet, yetkili olmayan okuyucu, FPD (Yanlış pozitif tespit) ve benzeri şeyleri talep ettiği bir durumda, ciddi güvenlik tehditlerini ve saldırılarını ele almaktadır. Saldırgan filigranını eklemeye çalıştıysa, sahibi yine de sözlüğüne atıfta bulunduğunu ve filigranının (Saldırganını) yerleştirmeyi başardıktan sonra bile söz konusu olduğunu ispatlayabilir. Çıkartma işlemi, sahte filigranı çıkarması ile sonuçlanacaktır.

Gizli görüntüyü kapak görüntüsüne gizlemek için tekil değer ayrıştırma (TDA) algoritması ile birlikte KDD kullanılarak filigran basma için sağlam teknik önerildi (Kaur and Jindal, 2014). Bu çalışmada hem kapak hem de gizli görüntü, HAAR dalgacık kullanılarak ayrıştırılırdı ve daha sonra Yüksek frekanslı alt bant (yani HH) daha sonra TDA metodolojisi ile ayrıştırılırdı. Buna ek olarak, ayrışma gerçekleşmeden önce görüntüyü düzeltmek için bir

medyan filtre işlevi kullanıldı. Başka bir çalışmada (Siddiqui and Kaur, 2017) hibrit KDD ve TDA filigran yaklaşımı önerilmiştir. Kapak görüntü LL, LH, HL ve HH bantlarına ayrıştırılmıştır. Ardından LL alt bandı 4. seviyeye ayrıştırılmıştır. Bu noktada HH alt bandı alınır ve TDA'ye geçirilmiştir. Ardından filigran görüntüsü, matrisleri oluşturmak için TDA algoritmasına geçirilir. Ayrıca, daha sonra zaten ayrışmış LL alt bandı kullanılarak konak görüntüsüne gömülmüş benzersiz bir imza oluşmuştur. Sunulan algoritma, birçok saldırıya dayanabildiği gözlemlenmiştir. Konak görüntüsü seviye 2'ye bölünür ve HH alt bandı (yüksek frekans) seçilir. Bununla birlikte, (Araghi ve diğerleri, 2018) içinde ayrışan HH bandı bloğa bölünür ve daha sonra her bloğa TDA uygulanır Deneylerinden elde edilen sonuçlara dayanarak, ikinci seviye filigranlama planlarının uygulanan saldırılara karşı daha sağlam olduğunu vurgulamıştır (Kaur and Jindal, 2014).

Adli raporlara göre, iki parmak izi en az 12 eşdeğer minutiden oluştuğunda, aynı parmaktan çıktığı düşünülmektedir (Więcław, 2009). Bu yazıda yazar, minutia eşleştirme sistemlerinden bahsediyor, parmak izinin önemini ve aynı şekilde minutia'nın oynadığı rolü ele alıyor.

MATERYAL ve METOT

Materyal

Bu tez çalışmasında biyometrik veri olarak yüz ve parmak izi görüntülerinden oluşan Fvc2002 ve FEI veri setleri kullanılmıştır (Yang *et al.* 2013). Fvc2002, biyometrik sistem Laboratuvarı (Bologna Üniversitesi), Michigan Eyalet Üniversitesi örüntü tanıma ve görüntü işleme Laboratuvarı ve ABD Ulusal test Merkezi'nden (San Jose Eyalet Üniversitesi) alınmıştır. Veritabanı DB1, DB2, DB3 ve DB4 oluşturur. Her veritabanı 110 parmak izi genişliğinde ve derinlikte parmak izi başına 8 örnek (yani, 880 parmak izi görüntüsünden oluşur). TIF, 256 gri düzey ve sıkıştırılmamış biçimi. Görüntü boyutu veritabanına bağlı olarak değişir. Parmak izinin her satırı farklı açılarda bir parmak konumunu temsil eder. Şekil 1 veri kümesi DB1_A'dan seçilen birkaç parmak izi görüntüsünü temsil eder.

Şekil 1. Örnek parmak izi görüntüleri (Yang *et al.* 2013)

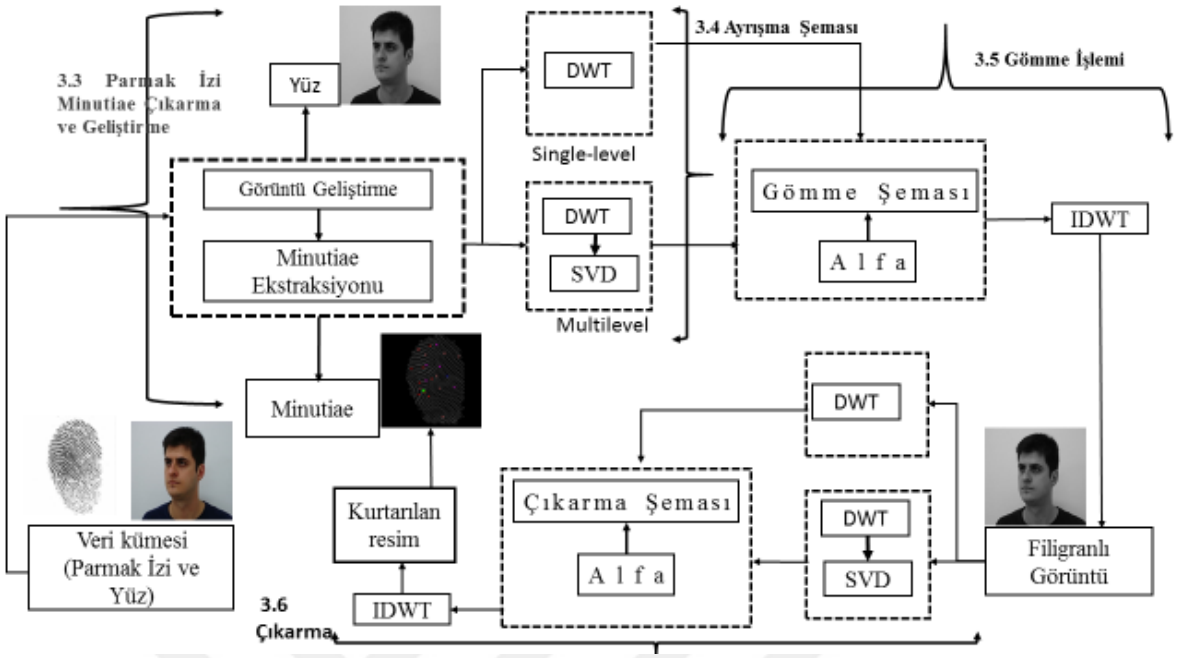
Yüz veri kümesi 702 görüntüden oluşmaktadır. Boyut 640 x 480 piksel ve görüntü türü JPEG'DİR. FEI yüz veritabanı São Bernardo do Campo, São Paulo, Brezilya FEI yapay zeka laboratuvarında Haziran 2005 ve Mart 2006 arasında çekilen yüz görüntülerin bir dizi içeren bir Brezilyalı yüz veritabanıdır. 200 kişiden her biri için 14 görüntü, toplam 2800 görüntü var. Tüm görüntüler renklidir ve yaklaşık 180 dereceye kadar profil dönüşü ile dik bir ön konumda beyaz homojen bir arka plana karşı çekilir. Ölçek yaklaşık %10 değişebilir ve her görüntünün orijinal boyutu 640x480 pikseldir. Tüm yüzler ağırlıklı olarak farklı bir görünüm, saç modeli ve süslemeleri ile 19 ila 40 yaş arası, FEI öğrenciler ve personel tarafından temsil edilmektedir. Erkek ve bayan deneklerin sayısı tamamen aynıdır ve 100'e eşittir. Şekil 2 FEI yüz veritabanından görüntü varyasyonları bazı örnekler göstermektedir.

Şekil 2. Veri setinden örnek yüz görüntüleri (FEI University, 2013)

Deneylerimizi Windows 8.1 işletim sisteminde MATLAB 2018b yazılımını kullanarak gerçekleştirdik.

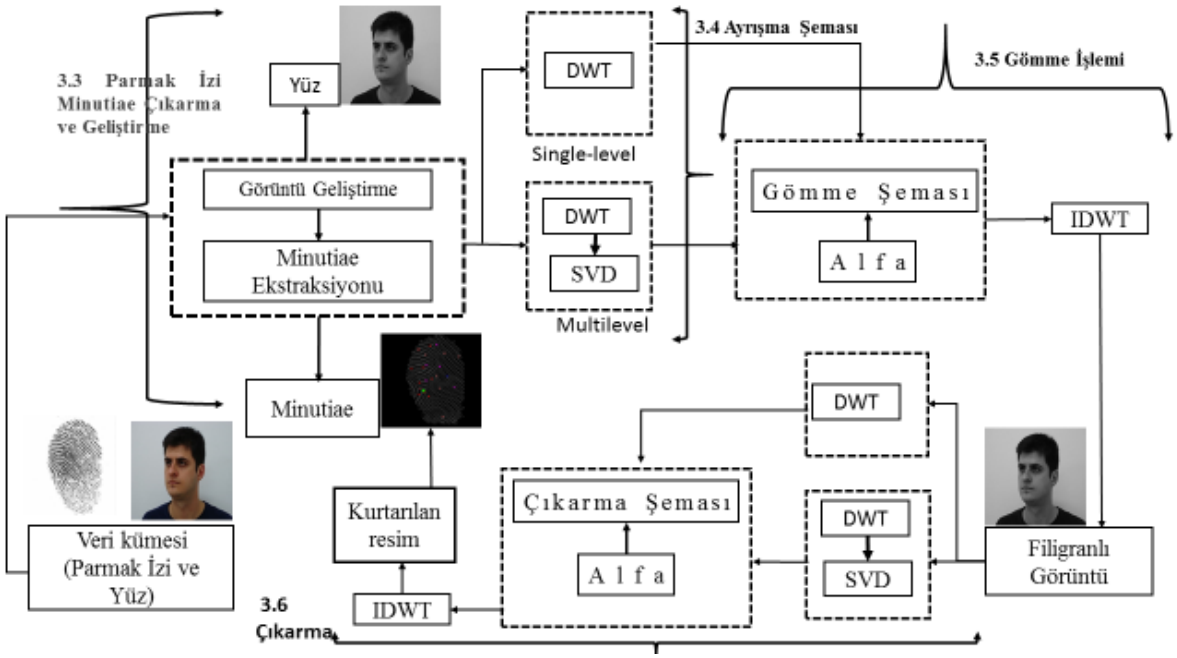
Yöntemler

Şekil 3



Şekil 3. Damgalama işleminin genel akış şeması.

'de önerilen sistemin akış şeması gösterilmektedir. İlk olarak parmak izi çıkarma ve geliştirme işlemi gerçekleştirilecektir. Daha sonra tek seviyeli ve çok seviyeli KDD ayrıştırması işlemi tamamlanacaktır. Gömme işleminden sonra fligran görüntülerin çıkarım işlemi gerçekleştirilecektir.



Şekil 3. Damgalama işleminin genel akış şeması.

Parmak İzi Minutiae Çıkarma ve Geliştirme

Minutiae tabanlı parmak izi eşleme algoritması, parmak izi kümeleri arasında

minutiae'ların hizalanmasına ve alınmasına yardımcı olan parmak izlerinden minutiae çıkarmak için kullanılır. Minutiae, adli tıp uzmanlarının ve güvenlik ajanslarının, bir kişinin farklı ülkelerde kimliğini benzersiz bir şekilde kanıtlamasına yardımcı olduğu için yaygın olarak kullanılmaktadır. Parmak izi özelliği çıkarma, minutiae gösterimi ve kaydı, parmak izi algoritması (Abraham, Kwan, and Gao, 2011) ile eşleşen en önemli bileşenlerden biridir. Parmak izi algoritmasına dayanarak, minutiaları çıkarmak için gerekli özellikler vardır. Bunlar görüntü tonları, görüntü geliştirme işlemleri, ön işlem ve son işlem ve özellik kümesi çıkarma algoritmasıdır. Görüntü geliştirme algoritmasında, Fourier alanı önceden filtrelenmiş görüntü ile uygulanır. Bunun nedeni, bize parmak izi görüntüsünü (Tao, Chongmin, Zain, and Abdalla, 2014)'de olduğu gibi tam boyutlu görüntünün filtre erişilebilirliği ile katlama izni vermesidir. Bunlar, sırt bölümleme, sırt yönelimi, sırt frekansı ve sırt filtresini içerir. Her parmak izi pikseli için global bir eşik değeri uygulanır:

$$\boldsymbol{I_{(x,y)}} = \begin{cases} \mathbf{1}\ \boldsymbol{if}\ \boldsymbol{I(x,y)} \geq \boldsymbol{t}, \\ \mathbf{0}\quad \boldsymbol{otherwise} \end{cases} \qquad \textbf{(1)}$$

Ek olarak, filtreleme aşaması görüntünün doğrudan düzeltilmesini sağlar. Örneğin, istenmeyen gürültünün aynı anda çıkarılması önemli ayrıntıların (örn. Minutia ve çıkıntılar) çıkarılmasını önler. Eşikleme aşaması, görüntü geliştirme ve çiftleştirmede çalışır. Genel olarak, parmak izi tabanlı sistem benzersiz özellik eşleşmesine odaklanır (Chakraborty ve Rao, 2012; Rzouga Haddada ve diğerleri, 2017b).

Parmak izi çıkarma işleminde, görüntüler gri tonlamaya ve daha sonra ikili görüntüye dönüştürülür. Gri tonlama görüntüsünün ikilileştirilmesi, herhangi bir adım atılmadan önce ana yaklaşımdır. İkili görüntü, morfolojik inceltme işlemi sırtlarından geçirilir, yapısı 1 piksel kalınlığına düşürülür. Bu, minutiae'ların saptanmasına yardımcı olur. Minutia konumunu bulmak için, elde edilen ikili görüntümüz p pikselinin her birini analiz eder. Bu, Rut Ovitz geçiş numarasını üretmek için saat yönünde saat yönünün tersine çevrilmiş 8 mahallenin (3 x 3 penceresindeki piksel) saat yönünün tersine çevrilmesiyle elde edilir. Sırtların çıkması durumunda parmak izinin yapısı piksel kalınlığına kadar çıkarılır. Bu iskelet olarak da bilinir ve minutiaların saptanmasına yardımcı olur. Bu makaledeki minutiae bazlı ekstraksiyon algoritması, aşağıdaki formülü kullanarak (Abraham *et al.* 2011) içindeki metodolojiyi takip eder:

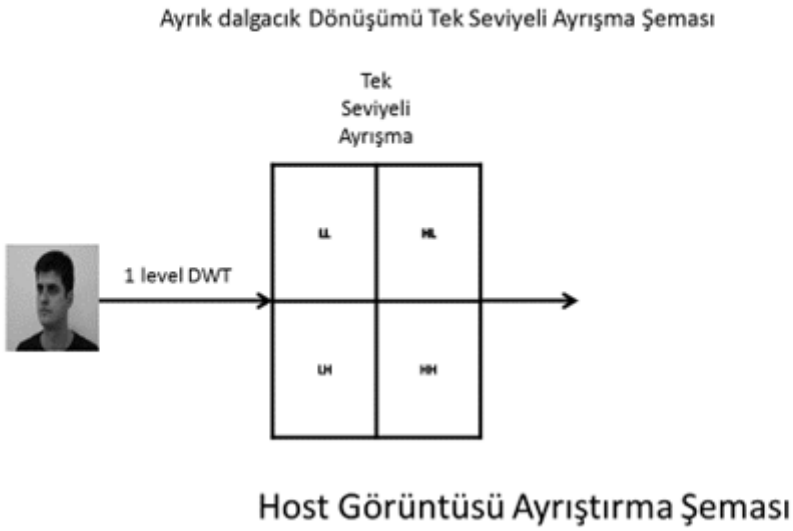
$$n(p) = \frac{1}{2} \sum_{i=1\ldots8} |val(p(_{i\ mod\ 8})) - val(p\_(i-1))| \qquad (2)$$

Ayrışma Şeması

İki biyometrik veriyi (yüz ve parmak izi) ayrık dalgacık dönüşümünü kullanarak ayrıştırdık. Yaklaşımın gömülmesi için önemli bir süreç. Bu, KDD frekans alt bantlarında biyometrik ayrıştırmaya yardımcı olur. Bu önemli adımlar olmadan, filigranı host (yani yüze) gömemeyiz. Hem host hem de filigran görüntüleri yaklaşık katsayı (LL), Yatay katsayı (LH), Dikey Katsayı (HL), Çapraz Katsayı (HH) olan frekans bantlarına ayrılır. Tüm bu işlemleri tek seviyeli, çok seviyeli filigranlama, çok seviyeli alfa karıştırma ve çok seviyeli KDD ve TDA filigranlama yaklaşımı ile ayarlıyoruz. Ayrıştırma yaklaşımının doğru anlaşılması için her ayrışmayı blok diyagramda temsil ediyoruz.

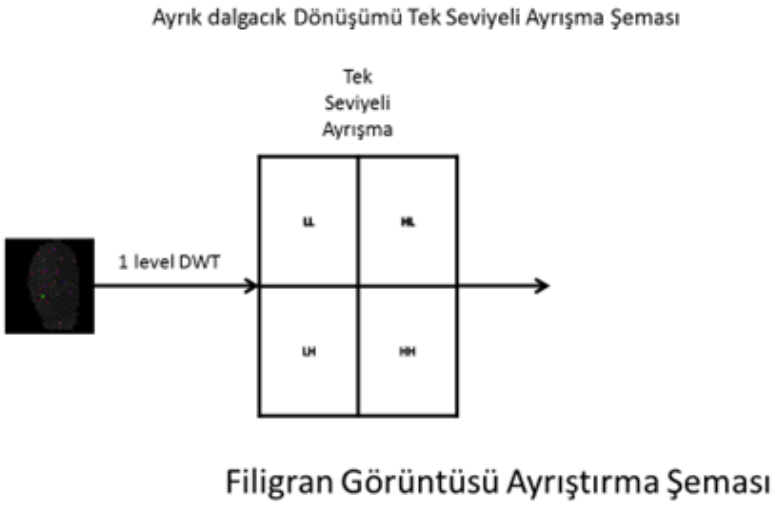
Tek seviyeli KDD ayrıştırması

Tek seviyeli filigran ayrışmasında, host görüntüsü yalnızca 4 × 4 KDD frekans bloklarıdır. Bu frekans alt bantları LL, LH, HL ve HH'dir. Şekil 4, host ayrışmasını temsil eder.



Şekil 4. Görüntü ayrıştırması bloğu

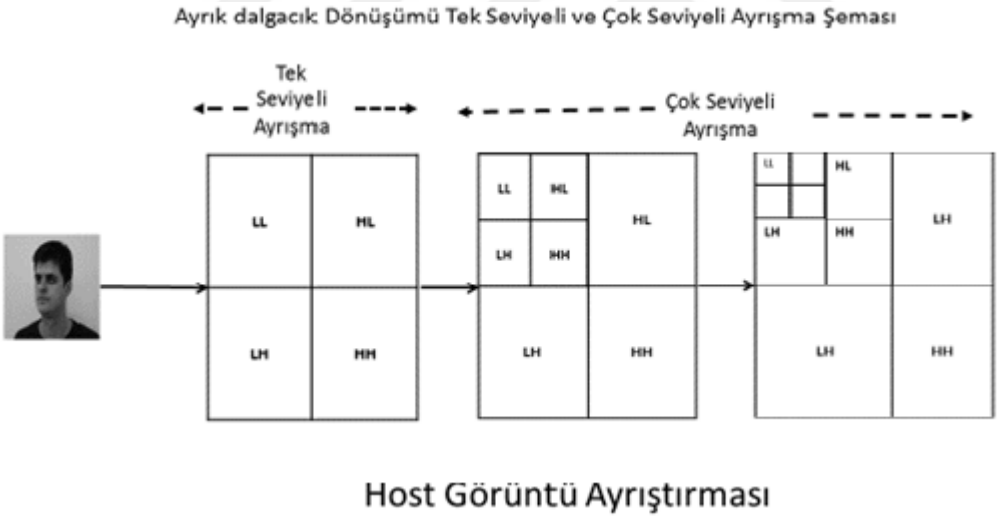
Filigran görüntüsünün ayrışması durumunda 4×4 KDD frekans blokları oluşur. Bu frekans alt bantları LLw, LHw, HLw ve HHw'dir. Şekil 5, filigran görüntüsünün ayrışmasını temsil eder.



Şekil 5. Filigran ayrışma bloğu

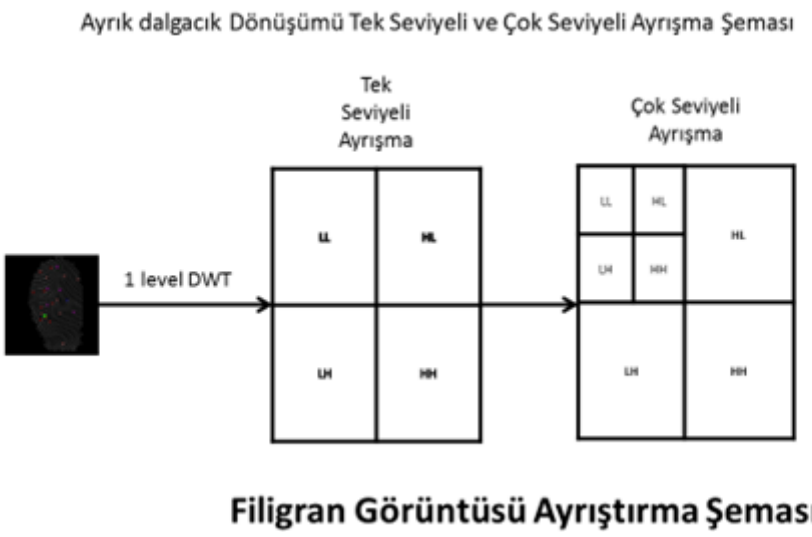
Çok seviyeli KDD ayrıştırması

Çok düzeyli filigran ayrıştırma şemasında, konak görüntüsünü KDD 3. düzey ayrışma kullanarak ayrıştırırız. Bu durumda, önce LL bandını ayrıştırırız ve daha sonra aynı KDD 3. seviye ayrışmasını kullanarak kalan bandı ayrıştırırız. Şekil 6 host görüntüsünün çok seviyeli ayrışmasının blok diyagramını göstermektedir.



Şekil 6. Çoklu görüntü ayrıştırma bloğu

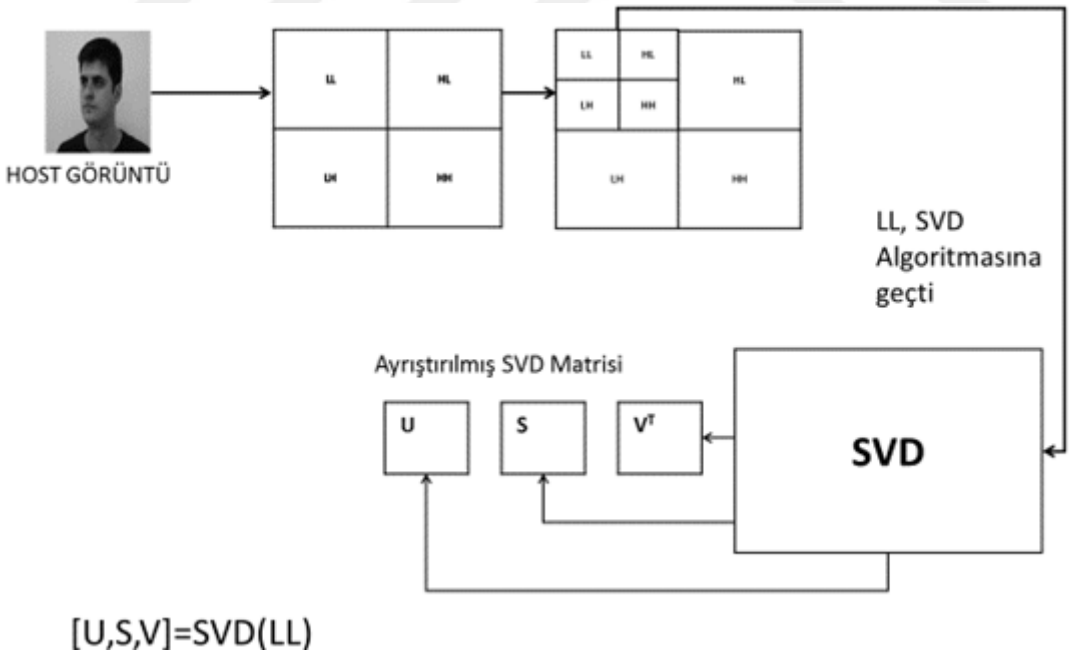
Çok düzeyli filigran ayrıştırma şemasında, KDD 1. düzey ayrışma kullanarak filigran görüntüsünü ayrıştırırız. Şekil 7, filigran görüntüsünün ayrışmasının blok diyagramını göstermektedir.



Şekil 7. Çok düzeyli filigran görüntü ayrıştırma bloğu

Çok seviyeli KDD ve TDA ayrıştırması

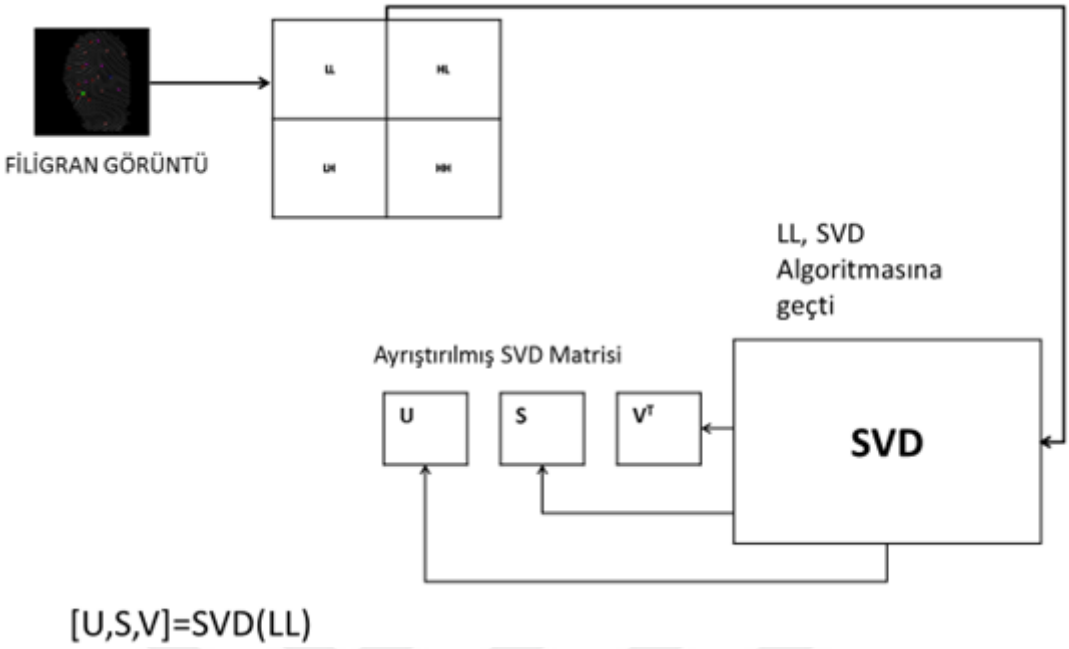
Çok seviyeli filigran ayrıştırma şemasında, konak görüntüsünü KDD 3. düzey ayrışma kullanarak ayrıştırırız. Bu durumda, önce LL bandını ayrıştırırız. Daha sonra aynı KDD 3. seviye ayrışma kullanarak kalan bant ayrıştırılır. TDA algoritması, dik ve tekil matris oluşturmak üzere KDD LL bandını ayrıştırmak için kullanılır. Şekil 8, host görüntüsünün KDD çok seviyeli ayrışmasının ve TDA ayrışmasının blok diyagramını göstermektedir.



Şekil 8. KDD-TDA ayrışma bloğu

Filigran görüntüsü durumunda, filigran görüntüsü 2. seviye KDD ayrışması kullanılarak ayrıştırılır. KDD LL bandını alınır, dik ve tekil matrisi oluşturmak için TDA algoritmasına

geçirilir. Kalan bantlar için aynı işlem tekrarlanır. Şekil 9 ost görüntüsünün KDD çok seviyeli ayrışmasının ve TDA ayrışmasının blok diyagramını göstermektedir.



Şekil 9. KDD-TDA filigran görüntü ayrıştırma bloğu

Ek olarak, KDD ve TDA filigran yaklaşımında, KDD ayrışması elde edildikten sonra, hedeflenen bant da TDA algoritması kullanılarak ayrıştırılır. Bunun nedeni, teknikteki tüm çelişkili gerekliliklerin anlaşılması ve elde edilmesinin zor olmasıdır. Bu nedenle, verimli bir sonuç elde etmek için bu iki algoritmayı birleştirdik. (Siddiqui and Kaur, 2017) 'de LL (yani, CA) ayrıştırılır ve içinde (Sharma and Swami, 2013) HL ayrıştırılır. Böylece, aynı bantla ayrışmaya başladık ve diğer frekans bantlarını, yani LH, HL ve HH'yi daha da ayrıştırdık. Hepsi HAAR dalgacık kullanılarak ayrıştırılır. Bkz. Şekil 10 orijinal konaklar ve filigran (yani, minutia ekstraksiyonu). Ayrıca çok seviyeli ayrıştırma uyguladık (yani 2., 3. ve 4.). Bunun nedeni, KDD frekans bandından hangisinin minutileri gizlemede en etkili olduğunu karşılaştırmak ve karşılaştırmak istiyoruz.

Konak görüntü

Filigran görüntü

Şekil 10. Konak ve filigran görüntüleri

Gömme İşlemi

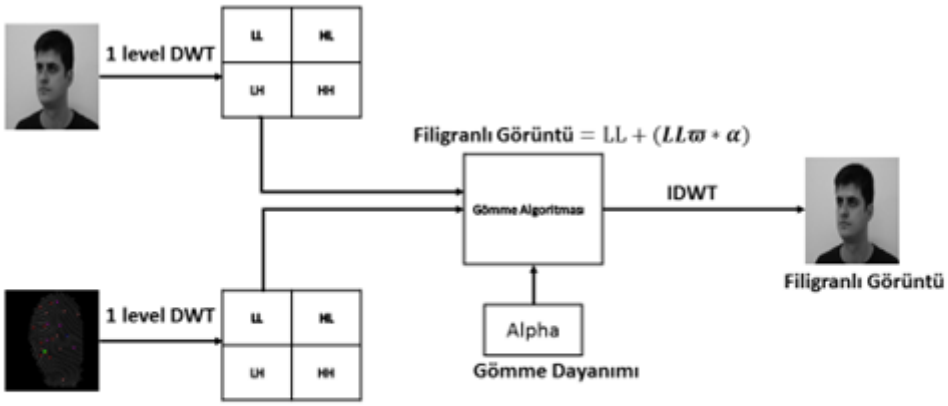
Bu, işlemin gizli (filigran) görüntünün konağa (kapak) yerleştirildiği işlemdir. Öncelikle tüm yaklaşımlarda LL bandı başlatılacak daha sonra tüm metotlarımız için kalan KDD bandı uygulanacaktır. İlk olarak, sırrın (filigranın) LL bandı ve konak, filigranlı görüntünün elde edilmesi için gömme gücü, yani alfa ile birlikte alınır. İkincisi, alfa harmanlama filigranı kullanımını çok düzeyli filigranla olduğu gibi uygulanır. (Sharma and Swami, 2013). Ek olarak, aynı alfa karışımını tek seviyeyle uygulandı. İşlem, ana görüntünün LL'sinin, K tuşu ve gizli (filigran) LL bandından filigranlı görüntünün oluşturulması için gömme gücü ile birlikte geçirilmesidir. En son uygulanan ise kombinasyon KDD ve Tekil Değer Ayrıştırma tekniklerinin kullanılmasıdır. Dördüncü seviye ayrışma frekans bandı alınır, daha sonra TDA algoritmasına geçirilir ve aynısı sır için yapılır (yani LL). Hem Konak LL hem de gizli LL'nin tekil değeri, sırrımızı oluşturmak için gömme gücüyle (alfa) alınır. Bu da filigranlı görüntüyü elde etmek için konak görüntüsüne gömülü olacaktır. Sonunda, filigran görüntüsünü oluşturmak için sırrı elde etmek için hem konağın hem de filigran görüntüsünün tekil değerini alfa ile birlikte kullandık. Bu sır, konak görüntüsüne eklenecek kesin gizli alt bandımızı yeniden oluşturmak için konak görüntüsünün ortogonal matrisi ile birlikte kullanılacaktır. **Denklem 2**, tekli ve çok seviyeli KDD ayrışmamız için kullanılan genel filigran formülüdür. Alfa harmanlama yaklaşımı durumunda, K anahtarı ana bantla manipüle edilir, bkz. **Denklem 3.** Gömme yaklaşımında aşağıdaki Şekil 11, tezimizin uygulanması için gömme sürecini temsil etmektedir. Bu, tek düzeyli filigranlama, çok düzeyli filigranlama, çok düzeyli alfa harmanlama filigranlama ve son olarak çok düzeyli KDD ve TDA filigran gömme bloğunu içerir. Ayrıca her seviyeyi diyagramlarla açıklıyoruz.

$$Watermarked = \lambda + (\varpi\eta * \alpha) \tag{3}$$

$$Watermarked = K\lambda + (\varpi\eta * \alpha) \tag{4}$$

λ, host görüntüsünün ayrıştırılmış amaçlanan frekans bandını temsil ettiğinde, $\boldsymbol{\varpi\eta}$, host görüntüsünün içine yerleştirilmeye hazır filigran görüntüsünün amaçlanan frekans bandını temsil eder ve $\boldsymbol{\alpha}$ bu gömme yoğunluğunu belirleyen alfa (yani gömme gücü) olarak bilinir. Tüm bu adımlar, diğer tüm KDD ayrıştırma bantları için tekrarlanır. KDD'nin diğer tüm alt bantları uygulandı ve her alt bandı gizli imajımı gizlemek ve hangi bantlar arasında en iyi sonucu vereceğini değerlendirmek için kullanıldı.

Tek seviyeli KDD gömme

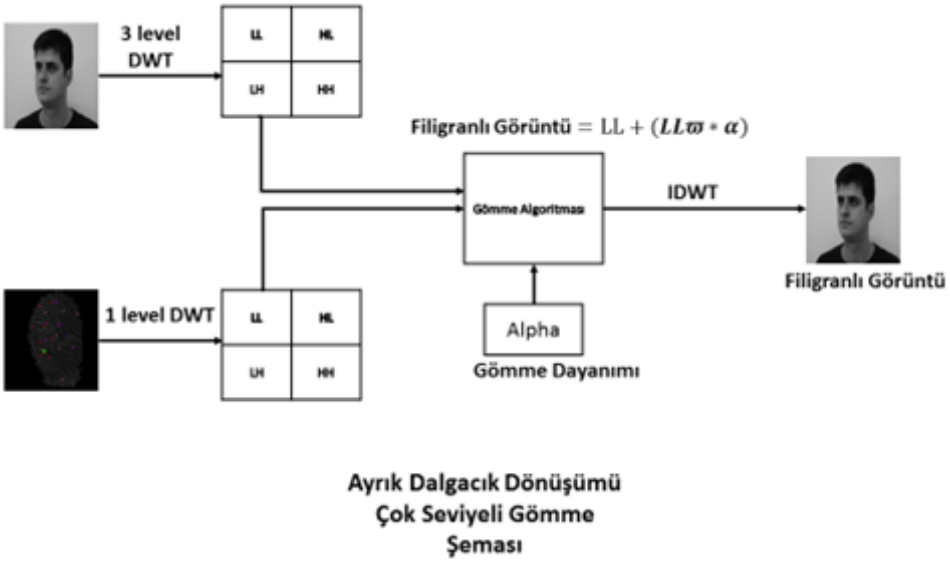


Ayrık Dalgacık Dönüşümü
Tek Seviyeli Gömme
Şeması

Şekil 11. Tek seviyeli KDD gömme yaklaşımı

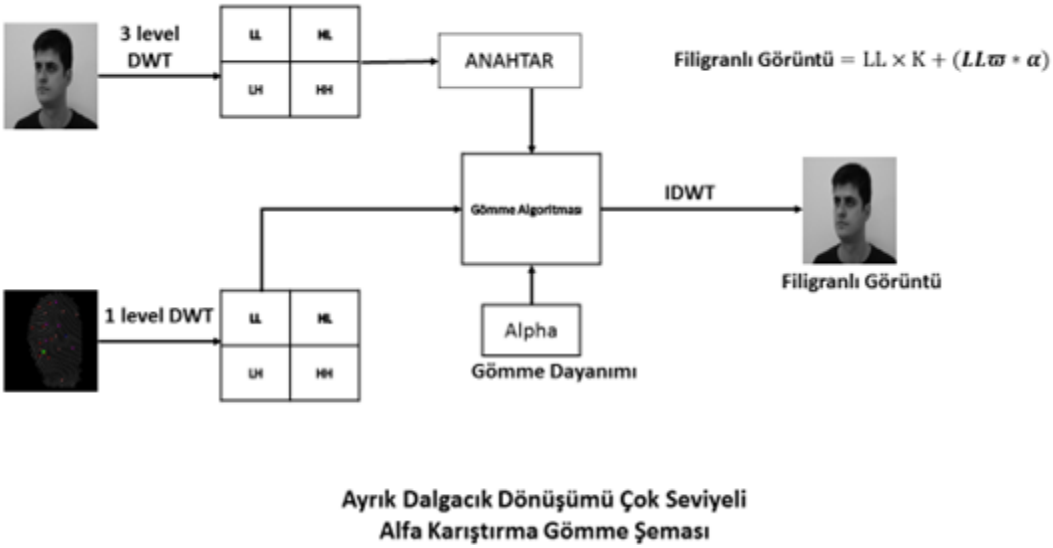
Tek seviyeli filigran içine gömme, hem host görüntüsünün hem de filigran görüntüsünün zaten ayrıştırılmış bandının kullanımını içerir. İlk gömme, filigranlı bandı oluşturmak için hem yerleşik hem de filigran görüntüsünün KDD LL bandı ile gömme kuvveti (alfa) ile başlar. Bu filigranlı bant, filigranlı görüntüyü oluşturmak için ters ayrık dalgacık dönüşümü kullanılarak host görüntüsüne geri yerleştirilir. Şekil 12 tek seviyeli filigran kullanarak gömme işlemini temsil eder.

Çok seviyeli KDD gömme



Şekil 12. Çok seviyeli gömme yaklaşımı

Çok düzeyli filigran içine gömme, hem host görüntüsünün hem de filigran görüntüsünün zaten ayrıştırılmış bandının kullanılmasını içerir. Bununla birlikte, hem host görüntüsü hem de filigran görüntüsü farklı bir ayrışma düzeyine girer. İlk yerleştirme, host'ın KDD LL bandı 3. düzeyde ve filigran görüntüsü tek düzeyde başlar. Ayrıştırılan filigran bandı, gömülme mukavemeti (alfa) ile birden fazladır ve daha sonra filigranlı bandı oluşturmak için ana görüntü ayrışmış banda eklenir. Bu filigranlı bant, filigranlı görüntüyü oluşturmak için ters ayrık dalgacık dönüşümü kullanılarak host görüntüsüne geri yerleştirilir. Şekil 13, çok seviyeli filigran kullanarak gömme işlemini göstermektedir.

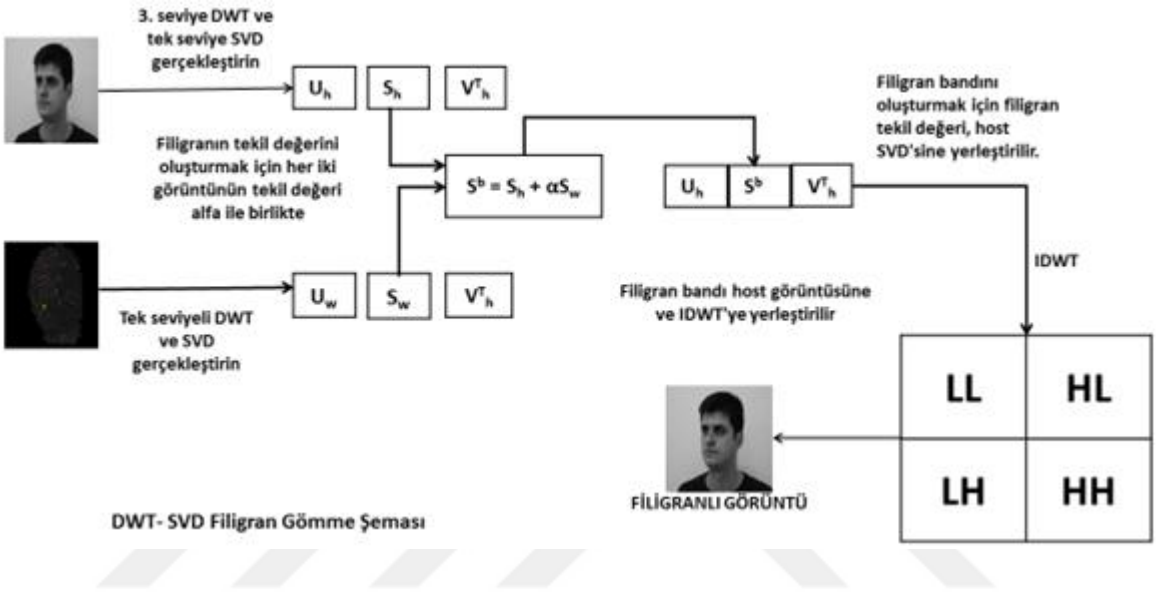


Şekil 13. Çok seviyeli alfa karıştırma yaklaşım

Çok düzeyli filigran içine gömme, hem ana makine görüntüsünün hem de filigran görüntüsünün zaten ayrıştırılmış bandının kullanılmasını içerir. Bununla birlikte, hem konak görüntüsü hem de filigran görüntüsü farklı bir ayrışma düzeyine girer. İlk yerleştirme, konağın

KDD LL bandı 3. düzeyde ve filigran görüntüsü tek düzeyde başlar. Ayrıştırılmış filigran bandı gömülme mukavemeti (alfa) ile çokludur. Daha sonra ana görüntüye ayrışan bant da K tuşu ile katlanır. Her iki çarpma işleminin sonucu filigranlı bant oluşturmak için eklenir. Bu filigranlı bant, filigranlı görüntüyü oluşturmak için ters ayrık dalgacık dönüşümü (IKDD) kullanılarak konak görüntüsüne geri yerleştirilir. Şekil 14, tek seviyeli filigran kullanarak gömme işlemini göstermektedir.

Çok seviyeli KDD ve TDA gömme



Şekil 14. KDD-TDA çok seviyeli gömme yaklaşımı

Çok düzeyli filigran içine gömme, hem host görüntüsünün hem de filigran görüntüsünün ayrıştırılmış bandının kullanımını içerir. Bununla birlikte, hem host görüntüsü hem de filigran görüntüsü farklı bir ayrışma düzeyine girer. İlk yerleştirme, host'ın KDD LL bandı 3. düzeyde ve filigran görüntüsü tek düzeyde başlar. Ayrıştırılan host görüntü bandı, iki dik matris ve tekil matrisin TDA bloklarını oluşturmak için TDA algoritmasına geçirilir. Aynı işlem zaten ayrıştırılmış filigran görüntü bandı için tekrarlanır. Host görüntüsünün tekil değeri, filigran görüntüsünün çoklu olarak alfa ile tekil değerine eklenir. Bu filigran bandını oluşturur. Bu filigran bandı, konumu oluşturmak için host görüntüsünün iki dik matrisine yerleştirilir. Son olarak, değer konak görüntüsüne eklenir ve ardından filigranlı görüntüyü oluşturmak için ters ayrık dalgacık dönüşümü (IKDD) uygulanır. Şekil 15, çok düzeyli KDD ve TDA filigranlama kullanılarak gömme işlemini temsil eder.

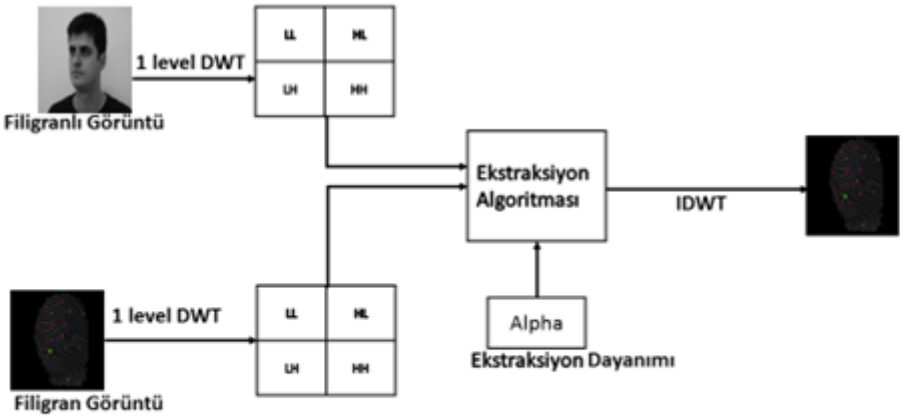
Çıkarma

Tüm resimle kör filigran yöntemini kullanılarak çıkarıldı, gizli resim (filigran) tespit edildiğinde orijinal resim geçerli değildir. Yapıldığı gibi (Araghi *et al.* 2018; Siddiqui and Kaur, 2017). Filigran görüntülerimizi görüntü işleme ve geometrik saldırılarla test ettik. Sonra ekteki

görüntüden sırrı çıkarmaya çalıştı. Her şey ayarlandıktan sonra PSNR, normalleştirilmiş korelasyon, MSE ve Bit Sırrı Oranını orijinal sır ile kurtarılan sır ile karşılaştırdık.

$$ext = (\text{filigranlı} - \varpi\eta)/\alpha \tag{5}$$

Tek seviyeli KDD çıkarma

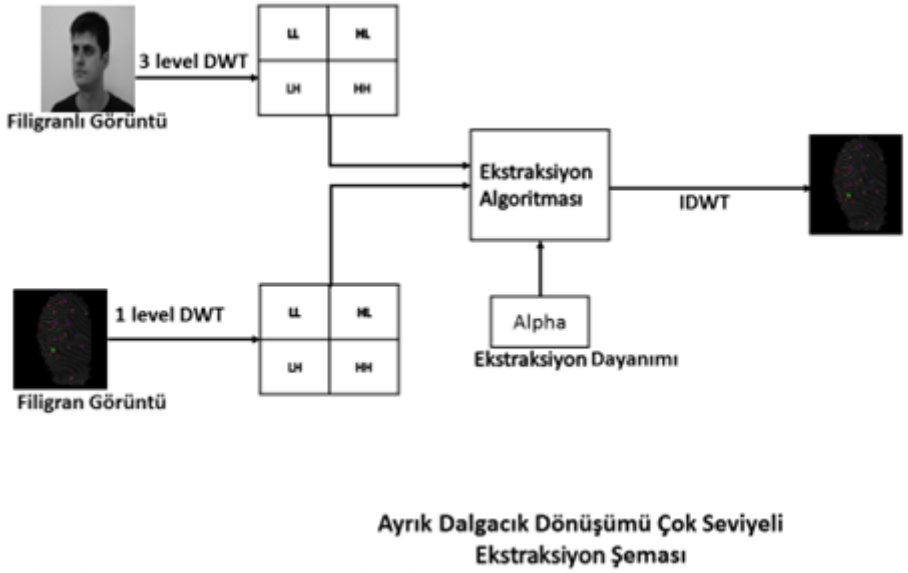


Ayrık Dalgacık Dönüşümü Tek Seviyeli Ekstraksiyon Şeması

Şekil 15. Tek seviyeli ekstraksiyon yaklaşımı bloğu

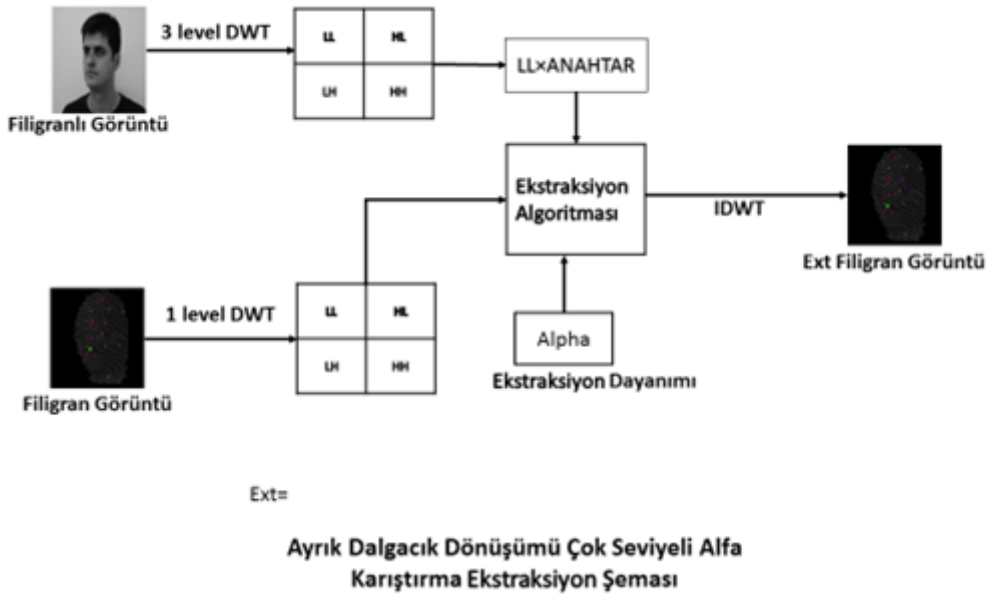
Tüm deneylerimizde kör filigranlama tekniğini kullandık. Bu teknik, ekstraksiyon için konağın bulunmasını gerektirmez. Tek seviyeli filigran çıkartma yaklaşımında, filigranlı görüntü 1. seviye KDD ve filigran kullanılarak ayrıştırılır. Gerekli bant alınır (yani LL). Böylece, filigranlı bant, filigran banttan Alfa'ya (ekstraksiyon gücü) bölünür. Kurtarma filigran bandını üretiyoruz. Bu bant filigran görüntüsüne yerleştirilecek ve daha sonra filigran görüntüsünü kurtarmak için ters ayrık dalgacık dönüşümü (IKDD) uygulanacaktır. Şekil 16, filigranlı görüntü tek düzeyli filigranlamadan filigran görüntüsünü çıkarma işlemini temsil eder.

Çok seviyeli KDD Çıkarma



Şekil 16. Çok seviyeli KDD ekstraksiyon yaklaşımı bloğu

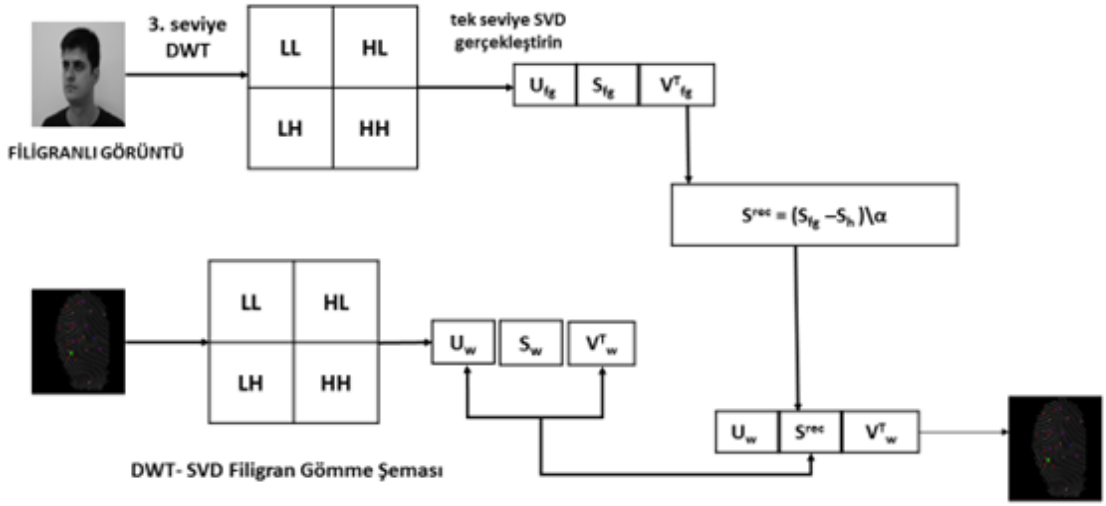
Çok düzeyli filigran çıkartma yaklaşımında, filigranlı görüntü 3. seviye KDD kullanılarak ayrıştırılır ve filigran aynı zamanda 1. seviye KDD kullanılarak ayrıştırılır. Gerekli bant alınır (yani LL). Kalan bantlar için aynı adımlar tekrarlanır. Ayrıştırılmış filigranlı bant, ayrıştırılmış filigran banttan Alfa'ya (ekstraksiyon gücü) bölünür. Bu noktada, kurtarılan filigran bandını üretebiliriz. Bu bant filigran görüntüsüne yerleştirilecek ve daha sonra filigran görüntüsünü yeniden oluşturmak için ters ayrık dalgacık dönüşümü (IKDD) uygulanacaktır. Şekil 17, filigranlı görüntü tek düzeyli filigranlamadan filigran görüntüsünü çıkarma işlemini temsil eder.



Şekil 17. Çok seviyeli alfa harmanlama ekstraksiyon yaklaşımı

Çok düzeyli alfa harmanlama filigran çıkarma ekstraksiyonu yaklaşımında, filigranlı görüntü 3. seviye KDD kullanılarak ayrıştırılır ve filigran da 3. seviye KDD kullanılarak ayrıştırılır. Gerekli bant alınır (yani LL). Geri kalan tüm bantlar için aynı adımlar tekrarlanır. Ayrıştırılmış filigranlı bant K anahtarıyla çarpılır ve daha sonra ayrıştırılmış filigran banttan Alfa'ya (ekstraksiyon gücü) bölünür. Bu noktada, kurtarılan filigran bandı üretilir. Bu bant filigran görüntüsüne yerleştirilecek ve daha sonra filigran görüntüsünü yeniden oluşturmak için ters ayrık dalgacık dönüşümü (IKDD) uygulanacaktır. Şekil 12, filigranlı görüntü tek düzeyli filigranlamadan filigran görüntüsünü çıkarma işlemini temsil eder.

Çok seviyeli KDD ve TDA çıkarma

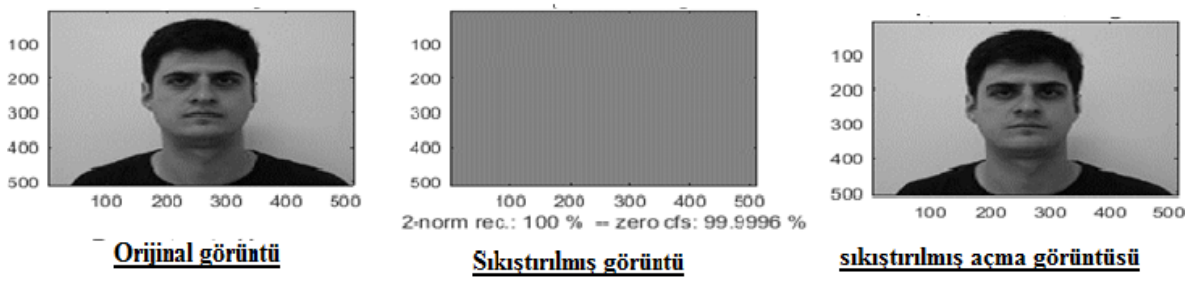


Şekil 18. KDD-TDA ekstraksiyon yaklaşımı

Çok düzeyli KDD ve TDA filigran çıkarma işlemi yaklaşımında, filigranlı görüntü 3. seviye KDD kullanılarak ayrıştırılır ve filigran aynı zamanda 1. seviye KDD kullanılarak ayrıştırılır. LL bandını başlangıç uygulaması olarak alındı ve daha sonra kalan ayrık dalgacık dönüşüm bantları denendi. Ayrıştırılan filigranlı bant TDA algoritması yoluyla geçirilir ve tekil değer seçilir. Ayrıştırılan filigran bandı TDA algoritması yoluyla da geçirilir. Zaten ayrıştırılmış filigranlı görüntünün tekil değeri, orijinal ana görüntünün tekil değerinden çıkarılır ve daha sonra Alfa'ya bölünür. Bu noktada, filigran bandının tekil değerini yeniden yapılandırabiliriz. Bu tekil değer, filigranın iki dikey matris değeri ile birlikte yeniden düzenlenir ve daha sonra filigran görüntüsünü yeniden oluşturmak için ters ayrık dalgacık dönüşümü (IKDD) uygulanır. Şekil 19, filigranlı görüntü tek düzeyli filigranlamadan filigran görüntüsünü çıkarma işlemini temsil eder.

ARAŞTIRMA BULGULARI ve TARTIŞMA

Deneylerimizde KDD-TDA olan iki algoritmayı birleştirildi. Bu işlemde, tüm gizli görüntüler tüm KDD bantlarında, yani LL, LH, HL ve HH'de gizlenmiştir. Normalleştirilmiş Korelasyon ve Bit Hata Oranı'nı hesaplandı. Analizlerde, LL bandı diğer gruplara kıyasla en düşük değerleri üretti. Bunun nedeni, görüntünün tüm önemli bilgilerini içeren bir alan olmasıdır (Araghi *et al.* 2018; Hasan *et al.* 2013; Kaur and Jindal, 2014; Sharma and Swami, 2013; Siddiqui and Kaur, 2017; Tao *et al.* 2014; Zargar, 2014). Böylece, bant üzerindeki herhangi bir manipülasyon, nesneyi büyük ölçüde etkileyebilir. Filigranlı görüntüye tuz ve biber, Poisson, benek gürültüsü, Gauss gürültüsü, Kırpma, JPEG sıkıştırma, Gauss Filtresi, Ortalama Filtre, Medyan Filtresi, Netleştirme, Dönme, Yumuşak ve Sert Eşik saldırıları uygulandı. Uygulanmadan önce, NC formülü kullanılarak orijinal filigran ve sıkıştırılmış görüntünün ilişkisini karşılaştırdık. Şekil 19'da korelasyon, sıkıştırma işlevinin filigranımızı yok etmediğini gösterilmiştir.



Şekil 19. Sıkıştırılmış ve sıkıştırılmış açma filigranlı

İşlemler yapıldıktan ve sırrı çıkardıktan sonra, orijinal filigranı ve geri kazanılmış filigran görüntüsünü BER ve Normalleştirilmiş Korelasyon aşağıdaki formülleri kullanarak karşılaştırdık. En yüksek BER'in yaklaşık olarak %2 olduğunu ve diğerlerinin % 0'dan az olduğunu fark ettik. Orijinal filigran ile geri kazanılmış filigran görüntüsü arasındaki korelasyon değeri, filigranlanan görüntünün uygulanan saldırılardan geçtikten sonra 1 değerini ve 1'e yakın diğerlerini oluşturur (yani, 0.9). Kombinasyon yaklaşımları, gizli imajımızı saldırılardan etkilenmekten korumanın iyi ve etkili bir yolunu sağlar. Sonuçlarımızı ayrıca (Kazemivash and Moghaddam, 2017; Lai and Tsai, 2010; Tareef and Al-Ani, 2015) ve (Rzouga Haddada *et al.* 2017a) gibi evraklarla karşılaştırdık.

$$MSE = \sum_{i=0}^{N-1} \sum_{J=0}^{N-1} \frac{[I1(i,j)-I2(i.j)]\text{^}2}{M*N} \quad (6)$$

$$PSNR = 10 \log 10 \frac{255\text{^}2}{MSE} \quad (7)$$

$$NC = \frac{\sum_{i=1}^{N1} \sum_{j=1}^{N2} (W(i,j)\ X\ W^*(i,j))}{\sum_{i=1}^{N1} \sum_{j=1}^{N2} (i,j)^2} \quad (8)$$

$$BER = \frac{\sum_{i=1}^{N1} \sum_{j=1}^{N2} (W(i,j) \oplus W^*(i,j))}{N1 * N2} \quad (9)$$

İki görüntü arasındaki sinyal parazit oranını hesaplamak için PSNR ve MSE Denklem 5 ve Denklem 6 matrisleri kullanıldı. PSNR değeri ne kadar yüksek olursa, görünmezlik o kadar iyi olduğu gözlendi. Diğer kalan bantlarda uygulandı ve PSNR ve MSE değerleri hesaplandı. NC (normalleştirilmiş korelasyon) Denklem 7 filigran ile Konak, filigran ve geri kazanılmış filigran görüntüsü arasındaki ilişkiyi hesaplamak için kullanılır. BER Denklem 8, görüntüler arasındaki bit hata oranını hesaplandı.

Gözlemimizde, düşük frekansla uygulanan saldırıların çoğunda (yani saldırının yüzde yoğunluğu) LL bandının diğerlerine göre daha sağlam olduğu doğrulandı. Ancak, yüzde yoğunluğu yüksek olduğunda, LH ve HL frekans bantlarının LL bandına göre daha sağlam olduğu fark edildi. Öte yandan, TDA tekniğini seçmemizin nedeni, nesneyi (örneğin, görüntü, ses vb.) bir kenardan diğerine inceleme ve analiz etme kabiliyetine sahip olmasıdır. Tekil değer, senkronizasyonun kaldırılmasından etkilenmez. Başka bir deyişle, birçok saldırıya karşı istikrarı nedeniyle, tekil değer üzerinden hesaplamalar yapıldı. Tek kademeli ve çok seviyeli filigran gömme sistemi uygulandı. Kesintisiz dalgacık dönüşümü etki alanı sonuçları Tablo 1, Tablo 2, Tablo 3 ve Tablo 4'de gösterilmiştir.

Tablo 1. HH bandının normalleştirilmiş sonucu

No.	Konak görüntü	Filigran	PSNR	Korelasyon
1	480*640	64*64	81.25	1
2	480*640	128*128	69.28	1
3	480*640	256*256	56.94	1

Tablo 2. LH bandının normalleştirilmiş sonucu

No.	Konak görüntü	Filigran	PSNR	Korelasyon
1	480*640	64*64	62.73	1
2	480*640	128*128	53.79	1
3	480*640	256*256	47.00	1

Tablo 3. HL bandının normalleştirilmiş sonucu

No.	Konak görüntü	Filigran	PSNR	Korelasyon
1	480*640	64*64	66.00	1
2	480*640	128*128	57.55	1
3	480*640	256*256	51.02	1

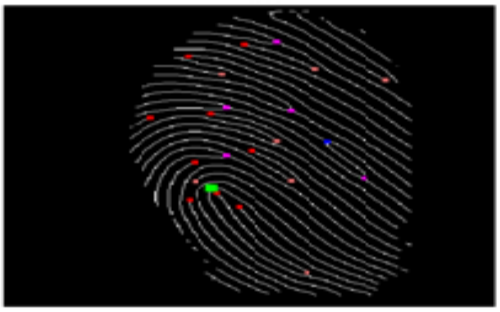
Tablo 4. LL bandının normalleştirilmiş sonucu

No.	Konak görüntü	Filigran	PSNR	Korelasyon
1	480*640	64*64	61.38	1
2	480*640	128*128	58.58	1
3	480*640	256*256	56.88	1

Bununla birlikte, çok seviyeli filigran yaklaşımının, tek seviyeli daha sağlam olduğunu gözlemledik. Bunun nedeni, tek seviyeyle ilgili yapılan tüm saldırıların, medyan filtreler ve JPEG sıkıştırması haricinde filigran (gizli) görüntüyü kolayca tahrip edebilmesi veya tahrip edebilmesidir. Bununla birlikte çok düzeyli birçok saldırıya dayanabildiğini gözlemledik. Ancak en büyük sorunu geometrik saldırılara dayanamamasıdır (örneğin kırpma, Rotasyon vb.). Tüm yaklaşımlarımızda, tüm KDD frekans bantlarını test ettik.

Parmak izi ve yüz görüntüsü veri seti deneylerimizde kullanıldı. İlk olarak, her iki görüntü de RGB'den gri tonlamaya geçmek için bir görüntü geliştirme algoritması ile geçirildi. Deneyimiz boyunca gri tonlamalı görüntülerle çalışıldı. Kullanılan veri setimiz FVC2002DB1_B ve FCV2002DB2_B (Biometric System Laboratory, 2013) 'ten (Rzouga Haddada *et al.* 2017a)'de kullanıldığı gibi. Veri tabanında dört (4) veri kümesi bulunur. 388 * 374 piksel boyutunda 80 parmak izi görüntüsü ve BMP görüntü formatı içeren DB1_B veri kümesi adını test ettik ve çalıştık. Bunları 64 x 64,128 x 128 ve 256 x 256 piksel arasında değişen farklı boyutlarda (Tareef and Al-Ani, 2015) ve yüz görüntüsünde (FEI University, 2013) normalize ettik. Bu normalizasyonun nedeni, eklenecek görüntünün boyutunun gerçekten önemli olup olmadığını kontrol etmektir. Sonuçlar, filigran görüntüsünün konağa göre boyutunun gerçekten önemli olduğunu göstermektedir. Filigranın boyutuna göre PSNR'nin değeri düşer. Örneğin, Tablo 1, Tablo 2, Tablo 3 ve Tablo 4. Şekil 20'de orijinal parmak ve minutiaları gösterilmiştir.

Orijinal parmak izi görüntüsü



Çıkarılan ayrıntıları

Şekil 20. Orijinal parmak izin ve çıkarılmış minutia

Çok Düzeyli Filigran Yaklaşımı

Ana görüntü ve filigranlı (stego-ımage) görüntüsü arasındaki PSNR ve MSE değerini hesaplar TABLO 5 de gösterilmiştir.

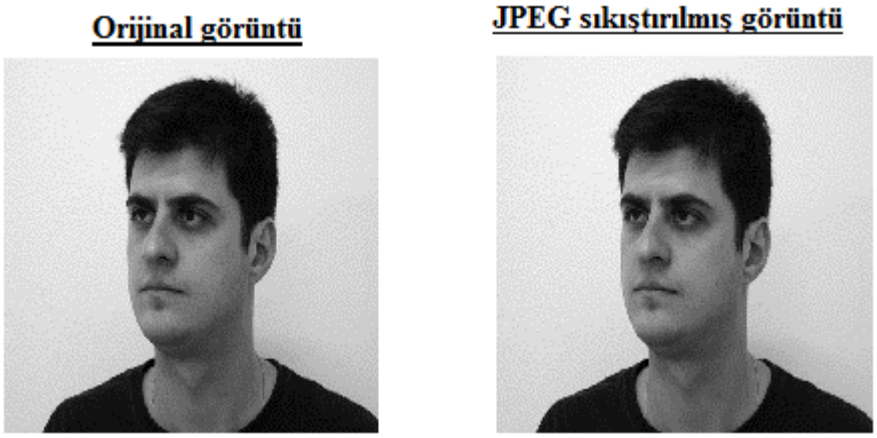
Tablo 5. Çok seviyeli filigran sonucu

BANT	PSNR	MSE
HL	72.92	0.00
HH	70.98	0.01
LH	70.83	0.01
LL	66.99	0.01

KDD'yi kullanan üçüncü filigran seviyesin Tablo 6 gösterilmiştir. Daha önce herhangi bir saldırı olmadan tek seviyeli KDD üzerinde çalıştığımız önceki çalışmalarımızla karşılaştırıldığında, çoklu seviyelere kıyasla daha iyi sonuçlar ortaya çıkmıştır. Veri kümemizi (yani yüz ve parmak izi görüntüsü) kullanarak, en iyi sonucu üreten bant HL bandı ve daha sonra HH bandıdır. Bu yaklaşımda, filigran görüntüsü üçüncü seviyede gizlenir (3. seviye ayrıştırma). Bu yöntemde, LH (yatay katsayısı) ve LL (yaklaşık katsayısı) düşük sonuçları üretmektedir. HL alt bandında, MSE değer üreteci sıfırdır. Diğer üç bant, MSE'lerinde 0.01 değeri elde edilmiştir.

Tablo 6. Farklı filigran seviyesi

	SEVİYE 1	SEVİYE 2	SEVİYE 3
PSNR	296,90	302,83	308,67
MSE	1,338e-25dB	3,412e-26dB	8,892e-27dB

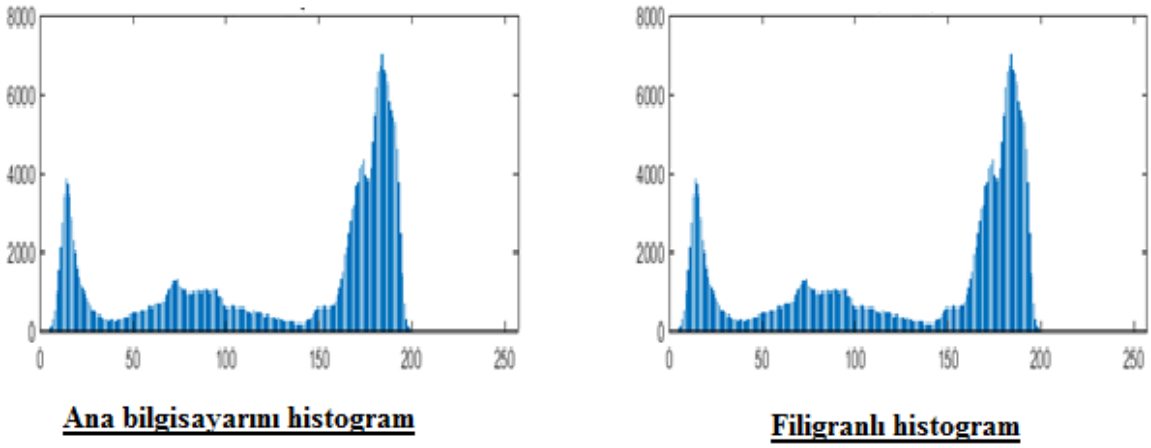


Şekil 21. Orijinal yüz ve JPEG sıkıştırılmış orijinal görüntü

Aşağıdaki tüm diyagramlar orijinal görüntüyü, filigran görüntüsünü, filigranlı görüntüsünü ve çıkarılan filigran görüntüsünü temsil eder. LL diyagramı ve histogramları sırasıyla aşağıda verilmiştir. Şekil 22 ve Şekil 23'e bakınız.

LL bandı

Şekil 22. LL filigranli görüntü



Şekil 23. LL filigran histogrami

Tüm bantların filigran görüntülerinden yapılan gözlem, filigran görüntülerinin hepsinin konak görüntülerine benzediğini göstermektedir. Bu filigran ilk yaklaşımını kanıtlamıştır.

Sırrı konak görüntüsüne yerleştirdikten sonra, HL bandındaki filigranlı görüntüye işlemler uygulandı. Kırpma, Rotasyon ve Gaussian gibi işlemler ile kırpılan görüntü, kimlik bilgilerinin çoğunu kaybettiği Şekil 24'de gösterilmiştir.

Şekil 24. Çok seviyeli filigran kirpilmiş görüntü

Ayrıca filigranlı görüntüye rotasyon yaklaşımını 5 ° ve 15 ° de uyguladık. Bu noktada filigran neredeyse tahrip olmuştur. Bu işlemdeki orijinal filigran ile çıkarılan filigranı karşılaştırmak tamamen farklıdır. Filigranlı görüntüye beyaz bir Gauss gürültüsü eklendi ve elde edilen görüntü kırpma ve rotasyondan daha iyi olduğu gözlemlendi, bkz. Şekil 24 ve Şekil 25'e bakınız.

Şekil 25. Çok seviyeli filigran gauss gürültüsü

Alfa Karıştırma Sonucu

Alfa değerini harmanlamayı (Sharma and Swami, 2013) K değerinin 0,2 ile 2 arasında değiştiği ve Q'nun (gömme gücü) deney boyunca sabit kaldığı ve q'nun 0,009 olduğu gibi uygulandı. Sonuçlarımızı karşılaştırmak için sadece çok seviyeli filigran yaklaşımı kullanıldı. Ayrıca aynı yöntemi tek seviyeli bir KDD tekniği ile karşılaştırıldı. Filigran uygulamasından elde edilen sonuçlara göre, K = 0,99 ve q = 0,009, filigranla ev sahibi arasındaki PSNR için en iyi sonucu ürettiği gözlemlendi. LL bandının ve HL bandının karşılaştırılması yapıldı. Yaklaşık katsayının sonucundan biraz daha yüksek olduğu gözlemlendi. Ayrıca, önerdiğimiz diğer grupları (yani HL ve HH) karşılaştırdıklarından daha yüksek olduğu gözlemlendi(Sharma and Swami, 2013). Yetersiz boşluk nedeniyle uygulanan alfa harmanlama yaklaşımımızın birkaç

diyagramını gösteriyoruz. Tablo 7, Tablo 8, Tablo 9 ve Şekil 26 alfa harmanlama ve resimsel gösterimin sonucunu göstermektedir.

Tablo 7. Alfa harmanlama sonucunun ve referans kağıdının karşılaştırılması

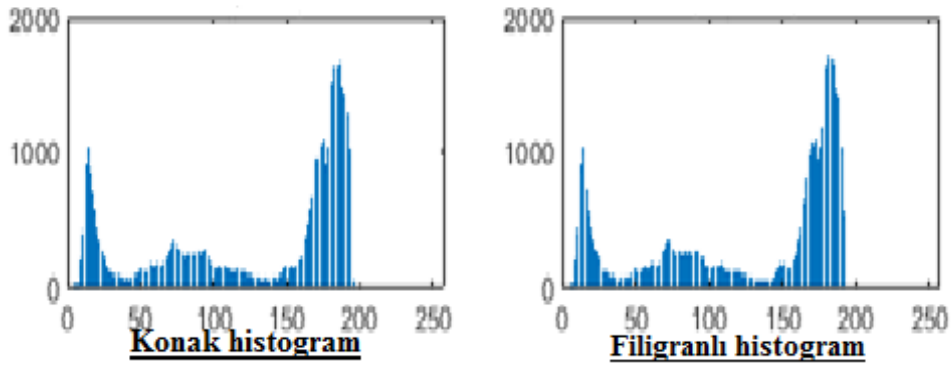
K	Q	PSNR	MSE	PSNR	MSE	PSNR (Sharma and Swami, 2013)	MSE (Sharma and Swami, 2013)
0.2	0.009	6.95	3215.89	6.95	3215.89	8.06	10167.720
0.5	0.009	11.04	5151.97	11.04	5151.97	12.22	3900.448
0.75	0.009	17.07	1287.42	17.07	1287.42	18.45	928.642
0.85	0.009	21.51	462.37	21.51	462.37	23.18	312.882
0.99	0.009	45.36	1.91	45.36	1.91	48.78	0.860
1.25	0.009	17.04	1296.77	17.04	1296.77	17.62	1123.906
1.5	0.009	11.02	5177.67	11.02	5177.67	11.81	4290.97
2.0	0.009	5.01	20691.89	5.01	20691.89	5.89	16763.99

Alfa harmanlama deneyi sonucunda, uygulanan anahtarlara dayanan diyagramları temsil eder. Her diyagramda anahtar bulunan ana bant birden fazla, filigranlı görüntüyü oluşturmak için gömme kuvvetine sahip birden fazla filigran bandı bulunur. Burada histogram analizini kullanarak orijinal ana görüntüsünü filigranlı görüntü ile karşılaştırdık.

0.2'deki K'ye dayanarak, filigranlı görüntünün konak görüntüsü kadar net olduğunu fark ettik. Histogram analizini kullandığımızda, daha geniş bir bilgi parçası **Hata! Başvuru kaynağı bulunamadı.** üretir. Bu nedenle, bu K = 0.2'nin filigranı konak görüntüsüne gömmek için etkili bir anahtar olmadığını gösterir **Hata! Başvuru kaynağı bulunamadı.**. Konakla k arşılaştırıldığında görüntü hala net değildi. K = 0.75 ve 0.85'te, filigranlı görüntü, konak görüntüsüyle karşılaştırıldığında daha parlak bir görüntü üretmeye başlar. Şekil 26 filigranlı görüntünün**Hata! Başvuru kaynağı bulunamadı.** histogram analizlerini gösterir. Bu noktada K = 0.2 ve 0.5'ten çok daha iyi sonuçlar verdiğini gördük.

Filigranlı görüntü K=0.99

Şekil 26. Alfa karıştırma K = 0.99



Şekil 27. Orijinal görüntü ve K = 0.99 filigranli histogram

Ayrıca, K = 0,99'u uyguladığımızda, filigranlı görüntü tam olarak konak görüntüsü gibi görünür. Tüm uygulamamızda bu, tüm ayrı dalgacık dönüşüm bantlarının en iyi sonucu verdiği seviyedir. Şekil 28 alfa harmanlanmış filigranlı görüntüyü temsil eder ve Şekil 29 konak görüntünün ve filigranlı görüntünün histogram analizini gösterir. Son olarak, K değerini 1.25, 1.5 ve 2'ye yükselttiğimizde, filigranlı görüntü kalitesini özellikle K = 1.5 ve 2 olduğunda kaybetmeye başladı. Bu seviyede, filigranlı görüntü k = 1.25'e kıyasla tamamen kayboldu. **Hata! Başvuru kaynağı bulunamadı.**

Normalleştirilmiş korelasyon, filigranlı görüntüler ve histogramlardan elde edilen sonuçlara dayanarak, anahtar K'nin filigranlı görüntüyü gerçekten etkilediğini fark ettik. Bu, LL frekans bandının görüntünün en özelliklerini içerdiğini anlamamızı sağlar.

Tablo 8. Sharma ve Swami (2013) ile HL bizim düzeylı sonucu

K	Q	PSNR	MSE	PSNR	MSE	PSNR (Sharma and Swami, 2013)	MSE (Sharma and Swami, 2013)
0.2	0.009	38.61	8.95	38.61	8.95	8.06	10167.720
0.5	0.009	38.98	8.22	38.98	8.22	12.22	3900.448
0.75	0.009	39.17	7.87	39.17	7.87	18.45	928.642
0.85	0.009	39.22	7.79	39.22	7.79	23.18	312.882
0.99	0.009	39.24	7.75	39.24	7.75	48.78	0.860
1.25	0.009	39.17	7.86	39.17	7.86	17.62	1123.906
1.5	0.009	38.98	8.22	38.98	8.22	11.81	4290.97
2.0	0.009	38.30	9.62	38.30	9.62	5.89	16763.99

LL frekans bandının sonuçları ile HL bandının karşılaştırıldığında, K tuşu filigran görüntüyü gerçekten etkilememiştir. PSNR değeri 38dB ve 39dB aralığındadır. Bu filigran için iyi bir algılanamazlık sonucu göstermektedir.

Tablo 9. Sharma and Swarmi (2013) ile HH bizim çok düzeyli sonucu

K	Q	PSNR	MSE	PSNR	MSE	PSNR (Sharma and Swami, 2013)	MSE (Sharma and Swami, 2013)
0.2	0.009	50.07	0.64	50.07	0.64	8.06	10167.720
0.5	0.009	50.51	0.58	50.51	0.58	12.22	3900.448
0.75	0.009	50.73	0.55	50.73	0.55	18.45	928.642
0.85	0.009	50.78	0.54	50.78	0.54	23.18	312.882
0.99	0.009	50.81	0.54	50.81	0.54	48.78	0.860
1.25	0.009	50.73	0.55	50.73	0.55	17.62	1123.906
1.5	0.009	50.50	0.58	50.50	0.58	11.81	4290.97
2.0	0.009	49.69	0.70	49.69	0.70	5.89	16763.99

HH frekans bandında Alfa harmanlama ile PSNR değerlerinin diğer tüm bantlar arasında en yüksek olduğunu fark edildi. Bu, HH bandının Alfa harmanlama filigran yaklaşımı ile ilgili en algılanamaz olduğunu gösterdi.

TDA ve KDD'nin Deneysel Sonucu

Bu yaklaşımda, bir veri tabanı sisteminin tam bir biyometrik modunu elde etmemiz için, her veri setinden 80 yüz görüntü ve 80 parmak izi görüntüsü seçtik. Her bir parmak izi ve bir kişiye ait yüz görüntüsü gibi davranan bir simülasyondur. Kapak, 512 * 512 piksel boyutundaki bir yüz görüntüsü ve boyutlardaki filigran görüntüsüdür (yani 64 * 64,128 * 128 piksel). Bu iki boyut neredeyse bütün uygulamalarda kullanıldı. Konak ve filigran görüntülerinin tümü gri tonlamalıdır. Bir teori (Araghi *et al.* 2018) "filigranlamada çoklu algoritmanın kombinasyonunun diğer yaklaşımların potansiyel sorunu üzerinde gerçekten etkili olabileceğini" söylemektedir. Deney sürecinde teoriyi doğruladık. Tek seviyeli, KDD ve TDA yaklaşımlı çok seviyeli filigranların sonucu referans değerimiz olarak kullandık. Filigran görüntünüzü gizlerken tüm KDD bandını inceledik ve analiz ettik. Buna ek olarak, filigranlı görüntü, algoritmanın sağlamlığını ve algılanabilirliğini değerlendirmemize yardımcı olmak için bazı sinyal işlemelere ve geometrik işlemlere geçirilir ve sırasıyla filigranlandı. Yukarıdaki Denklem 4, Denklem 3 ve Denklem 5'te normalleştirilmiş korelasyon, PSNR ve BER değerlerini hesaplamada kullanıldı. Önerilen (TDA ve KDD) ve kâğıt (Rzouga Haddada *et al.* 2017a) sonuç Tablo 10 ve Tablo 11'de görülebilir.

Tablo 10. LL-LH ve Rzouga Haddada et al.(2017) açılan görüntülerin sonuçları

Attacks	PSNR	NC	PSNR	NC	PSNR (Rzouga Haddada *et al.* 2017a)	Korelasyon (Rzouga Haddada *et al.* 2017a)
	LL bant		LH bant		WPD	
Saldırı olmadan	Inf.	1	Inf.	1	34.48	1
Sıkıştırma % 70	50.62	0.99	52.79	1	33.92	0.81
Sıkıştırma % 80	53.22	0.99	53.13	1	34.14	0.94
Tuz ve Biber 0.5%	37.94	1	36.24	1	27.44	0.98
Benek gürültü 0.5%	38.58	1	35.44	1	32.82	0.98

Tablo 11. HL-HH ve Rzouga Haddada *et al.*(2017) açılan görüntülerin sonuçları

Attacks	PSNR	NC	PSNR	NC	PSNR (Rzouga Haddada *et al.* 2017a)	Correlation (Rzouga Haddada *et al.* 2017a)
	HL Band		HH Band		WPD	
Saldırı olmadan	Inf.	1	Inf.	1	34.48	1
Sıkıştırma % 70	48.05	1	35.20	1	33.92	0.81
Sıkıştırma % 80	48.02	1	36.78	1	34.14	0.94
Tuz ve Biber 0.5%	37.88	1	33.29	1	27.44	0.98
Benek gürültü 0.5%	36.94	1	32.58	1	32.82	0.98

Çok düzeyli KDD ayrıştırması ve TDA kullanarak yaptığımız sonuçla, sonucumuz daha yüksek PSNR değeri oluşturur ve korelasyonumuz diğer bantlarda 1 veya tam 1 olarak kapatıldı. Kör ekstraksiyon yaklaşımı önerilen yöntemimizde uygulanmaktadır. Bazı görüntü işleme saldırılarıyla geçtikten sonra elde edilen görüntülerin sonuçları Tablo 12 ve Tablo 13'de verilmiş ve (Lai and Tsai, 2010) ve (Tareef and Al-Ani, 2015) çalışmaları ile karşılaştırılmıştır. Normalleştirilmiş Korelasyon ve Bit Hata Oranı Filigran görüntüsü ve kurtarılan görüntü arasında hesaplanır. Sonuçlarımız, KDD ve TDA metodolojisini kullanan Medyan Filtrelere ve Ortalama Filtrelemeye karşı daha sağlam olduğu gözlemlenmiştir.

Tablo 12. LL-LH sonuçlarımız bildiriler (Lai and Tsai 2010) ve (Tareef and Al-Ani 2015)

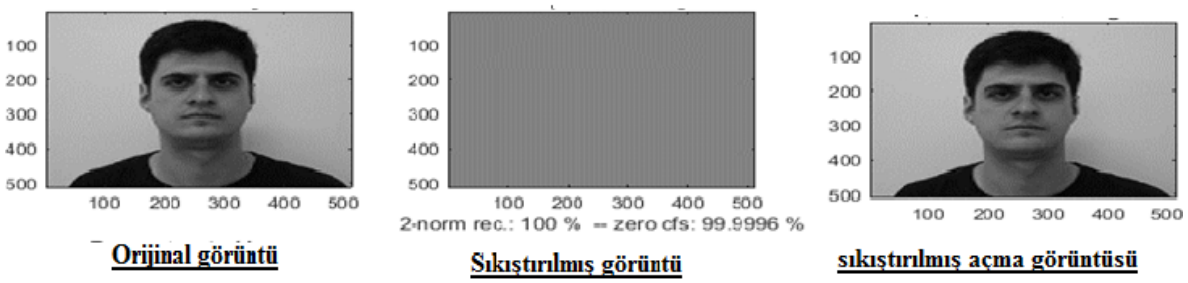
Band	LL	LH	(Lai and Tsai, 2010)	(Tareef and Al-Ani, 2015)
	NC	NC	NC	NC
Saldırı olmadan	1	1	-	-
Tuz ve Biber (0.01)	1	1	0.9470	0.9823
Tuz ve Biber (0.1)	1	1	0.7978	0.9113
Gauss Gürültüsü (0.01)	0.9963	1	0.8736	0.9681
Gauss Gürültüsü (0.1)	0.9960	1	0.8000	0.8619
Benek gürültü (0.01)	1	1	0.9762	0.9838
Benek gürültü (0.1)	0.9596	1	0.8219	0.9541
JPEG sıkıştırma 50%	1	1	0.9841	0.9852
Ortalama Filtre (3*3)	1	1	0.9402	0.9757
Medyan Filtre (3*3)	0.9994	1	0.9702	0.9817
Kırpma TL	0.9960	1	-	-
Kırpma C	NaN	1	-	-
Kırpma BR		1	-	-
Rotasyon 45^0	NaN	1	0.8717	0.9763
Rotasyon 270^0	1	1	0.9727	0.9867
Yumuşak eşik (0.4)	1	1	0.9491	0.9297
Sabit eşik (0.4)	1	1	0.9450	0.9490
İmge keskinleştirme	1	1	0.9663	0.9769

Tablodan da görüleceği üzere normalleştirilmiş korelasyon (NC) tarafından verilen sonucun diğer bantlarda (yani HH, HL, LH) LL'ye kıyasla daha yüksek olduğunu gözlemledik. Ayrıca NC saldırısını test ettik ve Tablo 12'de herhangi bir saldırı yapılmadan önce tüm değerlerin 1 olduğunu ve saldırılardan sonra değerlerin saldırı türüne ve saldırıların yoğunluğuna bağlı olarak değiştiğini göstermektedir. Şekil 28, çıkartılan filigran görüntüsünün maksimum NC değerlerine ilişkin farklı saldırıları, ana yoğunluk, filigran, stego-görüntü ve çıkarılan gizli görüntüleri gösteren saldırı türlerine göre göstermektedir.

Şekil 28. Filigranlı görüntüye uygulanan farklı saldırı türlerinin örnekleri

Tablo 13. HL-HH sonuçlarımız bildiriler (Lai and Tsai, 2010), (Ali and Mhn 2014), (Tareef and Al-Ani, 2015)ve Siddiqui, A., and Kaur, A. (2017)

HL-HH Bantlar	HL	HH	(Lai and Tsai, 2010)	(Ali and Mhn 2014)	(Tareef and Al-Ani, 2015)	Siddiqui, A., and Kaur, A. (2017)
	NC	NC	NC	NC	NC	NC
Saldırı olmadan	1	1	-	-	-	-
Tuz ve Biber (0.01)	1	1	0.9470	-	0.9823	-
Tuz ve Biber (0.1)	1	1	0.7978	-	0.9113	-
Gauss Gürültüsü (0.01)	1	1	0.8736	0.8589	0.9681	-
Gauss Gürültüsü (0.1)	1	1	0.8000	-	0.8619	-
Benek gürültü (0.01)	1	1	0.9762	-	0.9838	-
Benek gürültü (0.1)	1	1	0.8219	-	0.9541	-
JPEG sıkıştırma 50%	1	1	0.9841	0.9607	0.9852	-
Ortalama Filtre (3*3)	1	1	0.9402	0.9191	0.9757	0.881
Medyan Filtre (3*3)	1	1	0.9702	0.9495	0.9817	0.881
Kırpma TL		1	-	-	-	-
Kırpma C		1	-	-	-	0.947
Kırpma BR		1	-	-	-	-
Rotasyon 45^0	1	1	0.8717	-	0.9763	0.881
Rotasyon 270^0	1	1	0.9727	-	0.9867	-
Yumuşak eşik (0.4)	1	1	0.9491	-	0.9297	-
Sabit eşik (0.4)	1	1	0.9450		0.9490	
İmge keskinleştirme	1	1	0.9663	0.8893	0.9769	



Şekil 29. Sıkıştırılmış ve sıkıştırılmış açma filigranli

Tablo 14. Çıkarılan görüntülerin KDD and TDA genel sonuçları

KDD-TDA LL BANT			HL		LH		HH	
	NC	BER	NC	BER	NC	BER	NC	BER
Saldırı olmadan	1	0	1	0	1	0	1	0
Tuz ve Biber (0,01)	1	0.0245	1	0.0179	1	0.0186	1	0.0175
Poisson Gürültüsü	1	0.0197	1	0.0176	1	0.0185	1	0.0167
Benek G (0,001)	1	0.0149	1	0.0143	1	0.0152	1	0.0131
Benek G (0,005)	1	0.0201	1	0.0172	1	0.0169	1	0.0154
Benek G (0,009)	1	0.0207	1	0.0183	1	0.0189	1	0.0169
Gauss G (0,001)	1	0.0171	1	0.0202	1	0.0209	1	0.0206
Gauss G (0,005)	0.9973	0.0164	1	0.0203	1	0.0215	1	0.0203
Gauss G (0,009)	0.9963	0.0158	1	0.0211	1	0.0207	1	0.0206
Kırpma TL	0.9960	0.0156	1	0.0036	1	0.0008	1	0.0016
Kırpma C	NaN	0.1094	1	0.0041	1	0.0009	1	0.0016
Kırpma BR		0.1012	1	0.0038	1	0.0011	1	0.0014
Sıkıştırma % 80	0.9998	0.0091	1	0.0097	1	0.0124	1	0.0002
Sıkıştırma % 75	0.9999	0.0093	1	0.0100	1	0.0126	1	0.0009
Sıkıştırma % 50	1	0.0136	1	0.0013	1	0.0043	1	0.0017
G-Filtresi (5*5)	1	0.0203	0.9999	0.0002	1	0.0000	1	0.0003
G- Filtresi (3*3)	1	0.0208	0.9999	0.0002	1	0.0000	1	0.0003

Genel Veri Kümesi Uygulaması

Diğer bir yandan tezimizde kullanılan tekniğin sağlamlığını ve algılanamazlığını değerlendirmek ve analiz etmek için Lena ve Babun görüntü gibi genel veri kümesini kullanıldı. Tablo 15. çok seviyeli KDD kullanan deney sonuçları ve Tablo 16. çok seviyeli KDD ve TDA sonuçlarını gösterilmiştir.

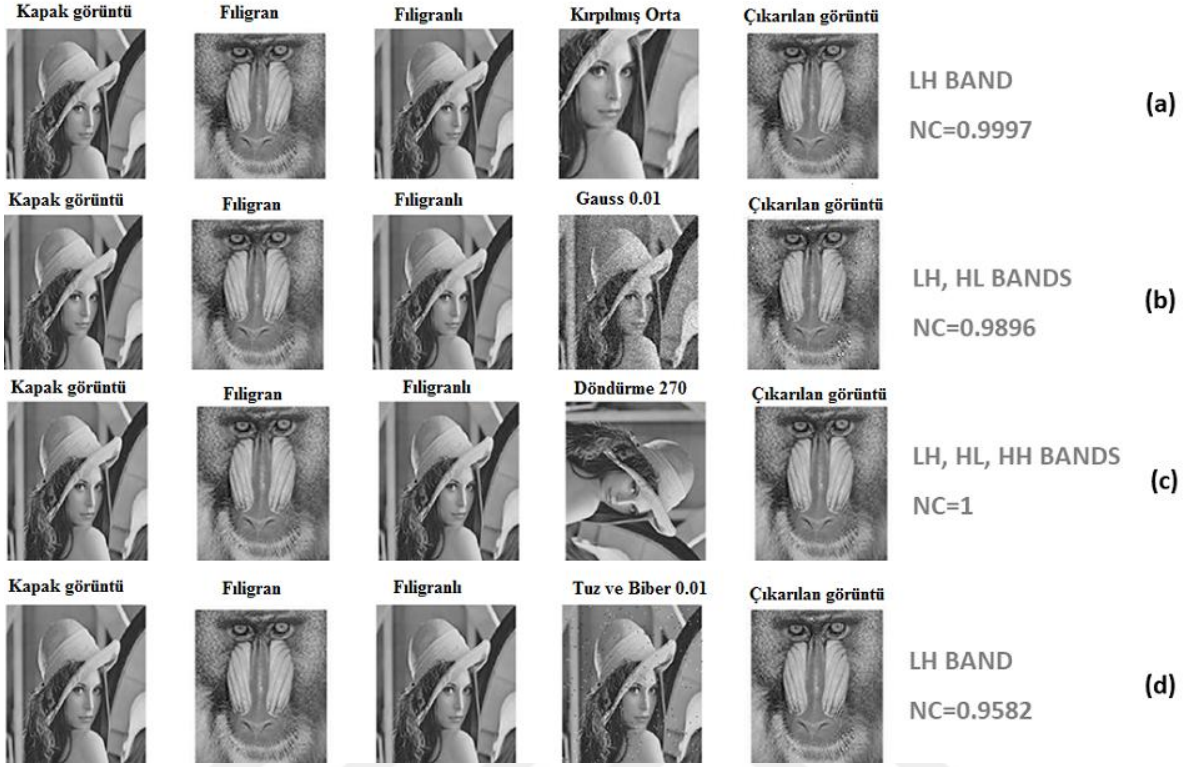
Tablo 15. Genel veri kümesiyle çok düzeyli KDD damgalama

KDD LL BAND			HL		LH		HH	
	NC	BER	NC	BER	NC	BER	NC	BER
Saldırı Olmadan	1	0	1	0	1	0	1	0
Tuz ve Biber (0,01	0.9798	0.1969	0.9958	0.1604	0.9957	0.1568	0.9837	0.1492
Poisson Gürültüsü	0.9400	0.2278	0.9678	0.2245	0.9671	0.2247	0.8224	02446
Benek Gürültüsü (0,001)	0.9653	0.2056	0.9878	0.1953	0.9877	0.1985	0.9885	0.1947
Benek Gürültüsü (0,005)	0.9413	0.2237	0.9718	0.2165	0.9729	0.2169	0.9739	0.2170
Benek Gürültüsü (0,009)	0.9182	0.0207	0.9621	0.2222	0.9593	0.2221	0.9628	0.2227
Gauss Gürültüsü (0,001)	0.9367	0.2358	0.9194	0.2340	0.9184	0.2340	0.9177	0.2346
Gauss Gürültüsü (0,005)	-	-	0.9149	0.2355	0.9198	0.2343	0.9156	0.2346
Gauss Gürültüsü (0,009)	-	-	0.9220	0.2350	0.9179	0.2345	0.9172	0.2342
Sol Üst Kırpılmış	0.7015	0.2551	0.9775	0.2004	0.9674	0.1924	0.9973	0.1537
Orta Kırpılmış	0.7897	0.2565	0.9676	0.2111	0.9656	0.1995	0.9971	0.1583
Sağ alt kırpılmış	-	-	0.9690	0.2032	0.9692	0.1924	0.9973	0.1578
Sıkıştırma 80	0.9783	0.1938	0.9932	0.1806	0.9956	0.1733	0.9977	0.1549
Sıkıştırma 75	0.9771	0.1987	0.9915	0.1854	0.9953	0.1754	0.9976	0.1549
Sıkıştırma 50	0.9752	0.2131	0.9862	0.1922	0.9909	0.1813	0.9977	0.1551
Gauss Filtresi (5x5)	0.9670	0.2110	0.9999	0.0002	0.9801	0.1263	0.9989	0.1201

Tablo 16. KDD-TDA genel verileri lena ve babun

Band	LL	LH	HL	HH
	NC	NC	NC	NC
Saldırı olmadan	1	1	1	1
Tuz ve Biber (0.01)	0.9982	0.9985	0.9987	0.9966
Tuz ve Biber (0.1)	0.8172	0.9582	0.9563	0.9431
Gauss Gürültüsü (0.01)	0.9608	0.9896	0.9896	0.9826
Gauss Gürültüsü (0.1)	0.6299	0.9903	0.9901	0.9821
Benek gürültü (0.01)	1	0.9986	0.9987	0.9966
Benek gürültü (0.1)	0.8595	0.9623	0.9608	0.9471
JPEG sıkıştırma 50%	1	1	1	1
Ortalama Filtre (3*3)	0.9972	1	1	1
Medyan Filtre (3*3)	0.9994	1	1	1
Kırpma TL	0.6907	0.9986	0.9608	1
Kırpma C	0.8889	0.9997	0.9992	1
Kırpma BR	0.6201	0.9985	0.9968	1
Rotasyon 45^0	0.7107	0.9943	1	1
Rotasyon 270^0	0.9989	1	0.9995	0.9999
Yumuşak eşik (0.4)	1	1	1	1
Sabit eşik (0.4)	1	1	1	1
İmge keskinleştirme	0.9979	1	1	1

Şekil 30, çıkarılan filigran görüntüsünün maksimum NC değerlerine ilişkin ilgili yoğunluğu ve Konak, filigran, stego-görüntü ve çıkarılan gizli görüntüleri gösteren saldırı türüyle farklı saldırıları gösterir.



Şekil 30. Filigranlı görüntü ve maksimum NC değerleri ve bantları dahil olmak üzere karşılık gelen çıkarılan filigranlara farklı saldırılar. a) Kırpılmış merkez gürültü B) Sıfır ortalama ve 0.01 varyanslı gauss gürültüsü c) Dönüş 270 D) 0.01 yolsuzluk ile tuz ve biber gürültüsü

SONUÇ

Bu tez çalışmasında, ayrı dalgacık dönüşüm alanı ve tekil değer ayrışımı kullanarak çok seviyeli bir filigran yaklaşımını önderdik. Tüm KDD frekans bantları, gizli gömme sırasında ayrı dalgacık dönüşüm bantlarını değerlendirmek ve analiz etmek için tek düzey, çok düzeyli filigran ve alfa harmanlama filigranı arasında değişen filigran görüntüsünü gömmek için kullandık. Özellikle, gömülme mukavemeti derecesi ne kadar az olursa, yaklaşık katsayının o kadar iyi ve algılanamaz olduğunu gözlemledik. Diğer grupların gücü ne olursa olsun, gözler değişiklikleri fark edemez. Yukarıda belirtilen tüm testler, farklı bantlarda ve farklı ayrışma seviyelerinde gerçekleştirildi.

Özet olarak, sırrın gömülmesinde birden fazla algoritmanın kombinasyonu ile çok seviyeli KDD kullanılarak filigranlamanın tek bir algoritmaya kıyasla daha sağlam olduğunu gözlemledik. Önerdiğimiz yöntem, LL bandındaki rotasyon saldırısı dışında bu makalede test edilen neredeyse tüm saldırılara dayanabilir. Daha sonra, LH, HL ve HH yapılan tüm deneylerdeki saldırılara dayanır. Mükemmel ve verimli filigranlamayı artırabilecek önemli gerçeklerin filigran görüntüsünün ve tonunun boyutu (yani Pürüzsüzlük, pürüzlülük vb.) olduğunu fark ettik. Tüm görüntülerimizi farklı tonlarda test ettik. Pürüzlü veya gürültülü görüntülerin gürültüsüz görüntüyle karşılaştırıldığında PSNR değeri daha düşük filigranlı bir görüntü oluşturduğunu gözlemledik. Deneyimiz sırasında, LL bandında, gömme kuvveti yüksek güce sahipse, filigranlı görüntünün algılanamazlığını etkilediğini fark ettik. Böylece filigranlı görüntüyü daha az sağlam hale getirir. Yoğunluğu (yani gömme mukavemeti) 0.01, 0.001 ve 0.0001'e düşürdükçe, fark edilemezliğin mükemmel olduğunu fark edildi. PSNR değeri de yüksektir. Bu grupla, manipülasyonu bu alfa aralığında yapmanın daha iyi olacağı sonucuna varıldı. Buna ek olarak, KDD kullanarak çok düzeyli filigranlamanın tek seviyeli filigranlama ile karşılaştırıldığında iyi sonuç vermesine rağmen fark edildi. Bununla birlikte, KDD diğer algoritmalarla birlikte pratik bir etki yarattığı gözlemlendir.

KAYNAKLAR

Abraham, J., Kwan, P., and Gao, J. (2011). Fingerprint Matching using A Hybrid Shape and Orientation Descriptor. *INTECH Open Source| Open Minds*.

Ahmed, F., and Siyal, M. Y. (2005). A hybrid-watermarking scheme for asymmetric and symmetric watermark extraction. *2005 Pakistan Section Multitopic Conference, INMIC*. https://doi.org/10.1109/INMIC.2005.334402

AL-Nabhani, Y., Jalab, H. A., Wahid, A., and Noor, R. M. (2015). Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network. *Journal of King Saud University - Computer and Information Sciences*, *27*(4), 393–401. https://doi.org/10.1016/j.jksuci.2015.02.002

Alkhathami, M., Han, F., and Van Schyndel, R. (2013). Fingerprint image protection using two watermarks without corrupting minutiae. *Proceedings of the 2013 IEEE 8th Conference on Industrial Electronics and Applications, ICIEA 2013*. https://doi.org/10.1109/ ICIEA.2013.6566540

Anusree, K., and Binu, G. S. (2015). Biometric privacy using visual cryptography, halftoning and watermarking for multiple secrets. *2014 IEEE National Conference on Communication, Signal Processing and Networking, NCCSN 2014*. https://doi.org/10.1109/NCCSN.2014.7001156

Aparna, J. R., and Ayyappan, S. (2015). Image watermarking using diffie hellman key exchange algorithm. *Procedia Computer Science*. https://doi.org/10.1016/ j.procs.2015.02.109

Araghi, T. K., Manaf, A. A., and Araghi, S. K. (2018). A secure blind discrete wavelet transform based watermarking scheme using two-level singular value decomposition. *Expert Systems with Applications*, *112*, 208–228. https://doi.org/10.1016/j.eswa.2018.06.024

Ashokarajan, R., Angelinjosphia, R., Gayathri, P. V. S., Rajendran, T., and Anandhakumar, P. (2014). A novel approach for secure ATM transactions using fingerprint watermarking. *2013 5th International Conference on Advanced Computing, ICoAC 2013*. https://doi.org/10.1109/ICoAC.2013.6922010

Biometric System Laboratory. (2013). Fingerprint Verification Competition. *FCV2002DB*, (August), 1. Retrieved from https://biolab.csr.unibo.it/fvcongoing/ UI/Form/Home.aspx

Burrows, C., and Zadeh, P. B. (2016). A mobile forensic investigation into steganography. *2016 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2016*. https://doi.org/10.1109/CyberSecPODS.2016. 7502340

Fang, W. S., and Chen, K. (2009). A wavelet watermarking based on HVS and watermarking capacity analysis. *1st International Conference on Multimedia Information Networking and Security, MINES 2009*, *2*(1), 141–144. https://doi.org/10.1109/MINES.2009.196

FEI University. (2013). The FEI face database and fingerprint images. Retrieved from Facedatabase website: http://fei.edu.br/cet/facedatabase.html

Hasan, K. K., Ngah, U. K., and Salleh, M. F. M. (2013). Multilevel decomposition Discrete Wavelet Transform for hardware image compression architectures applications. *Proceedings - 2013 IEEE International Conference on Control System, Computing and Engineering, ICCSCE 2013*, 315–320. https://doi.org/10.1109/ICCSCE.2013. 6719981

Hu, Z., She, K., Wang, J., and Tang, J. (2014). Game theory based false negative probability of embedded watermark under unintentional and steganalysis attacks. *China Communications*, *11*(5), 114–123. https://doi.org/10.1109/CC.2014.6880467

Ibm, T. J. (2003). *Biometrics recognition: Security and Privacy Concerns*. 33–42. Retrieved from http://cyber.sci-hub.bz/MTAuMTEwOS9tc2VjcC4yMDAz LjExOTMyMDk=/ 10.1109%40MSECP.2003.1193209.pdf

Islam, M. R., Sayeed, M. S., and Samraj, A. (2008). Biometric template protection using watermarking with hidden password encryption. *Proceedings - International*

Symposium on Information Technology 2008, ITSim. https://doi.org/ 10.1109/ITSIM.2008.4631572

Jain, A. K., and Nandakumar, K. (2012). Biometric authentication: System security and user privacy. *Computer*, *45*(11), 87–92. https://doi.org/10.1109/MC.2012.364

Kaur, R., and Jindal, S. (2014). Robust digital image watermarking in high frequency band using median filter function based on DWT-SVD. *International Conference on Advanced Computing and Communication Technologies, ACCT*, 47–52. https://doi.org/10.1109/ACCT.2014.93

Kazemivash, B., and Moghaddam, M. E. (2017). A robust digital image watermarking technique using lifting wavelet transform and firefly algorithm. *Multimedia Tools and Applications*, *76*(20), 20499–20524. https://doi.org/10.1007/s11042-016-3962-5

Khan, M. K., Zhang, J., and Tian, L. (2004). Protecting Biometric Data for Personal Identification. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *3338*, 629–638. https://doi.org/10.1007/978-3-540-30548-4_72

Kumar, V., and Kumar, D. (2010). Performance evaluation of DWT based image steganography. *Advance Computing Conference (IACC), 2010 IEEE 2nd International*, 223–228. https://doi.org/10.1109/IADCC.2010.5423005

Lai, C., and Tsai, C. (2010). *Digital image watermarking using discrete wavelet transform and singular value decomposition. IEEE Transactions on instrumentation and measurement, 59(11), pp.3060-3063. 59*(11), 3060–3063.

Lu, Y., Li, X., Qi, M., Li, J., Fu, Y., and Kong, J. (2008). Lossless and content-based hidden transmission for biometric verificaion. *Proceedings - 2008 2nd International Symposium on Intelligent Information Technology Application, IITA 2008*. https://doi.org/10.1109/IITA.2008.351

Nandakumar, K., Jain, A. K., and Nagar, A. (2008). Biometric template security. *Eurasip Journal on Advances in Signal Processing*, *2008*. https://doi.org/10. 1155/2008/579416

Ouslim, M., Sabri, A., and Mouhadjer, H. (2013). Securing biometric data by combining watermarking and cryptography. *2013 2nd International Conference on Advances in Biomedical Engineering, ICABME 2013*. https://doi.org/10.1109/ICABME. 2013.6648877

Rzouga Haddada, L., Dorizzi, B., and Essoukri Ben Amara, N. (2017a). A combined watermarking approach for securing biometric data. *Signal Processing: Image Communication*. https://doi.org/10.1016/j.image.2017.03.008

Rzouga Haddada, L., Dorizzi, B., and Essoukri Ben Amara, N. (2017b). A combined watermarking approach for securing biometric data. *Signal Processing: Image Communication*, *55*(March), 23–31. https://doi.org/10.1016/j.image.2017.03.008

Sharma, P., and Swami, S. (2013). Digital Image Watermarking Using 3 level Discrete Wavelet Transform. *Conference on Advances in Communication and Control Systems*, *2013*(Cac2s), 129–133.

Shirali-Shahreza, S., and Shirali-Shahreza, M. (2008). Improved collage steganography. *Proceedings - 4th IEEE International Conference on Emerging Technologies 2008, ICET 2008*, 223–227. https://doi.org/10.1109/ICET.2008.4777504

Shoniregun, C. A., and Crosier, S. (2008). *Securing Biometrics Applications*.

Siddiqui, A., and Kaur, A. (2017). A secure and robust image watermarking system using wavelet domain. *Proceedings of the 7th International Conference Confluence 2017 on Cloud Computing, Data Science and Engineering*, *6*, 599–604. https://doi.org/10.1109 /CONFLUENCE.2017.7943222

Solanas, A., and Domingo-Ferrer, J. (2006). Watermarking non-numerical databases. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/ 11681960_24

Tao, H., Chongmin, L., Zain, J. M., and Abdalla, A. N. (2014). Robust image watermarking theories and techniques: A review. *Journal of Applied Research and Technology*, *12*(1), 122–138. https://doi.org/10.1016/S1665-6423(14)71612-8

Tareef, A., and Al-Ani, A. (2015). A highly secure oblivious sparse coding-based watermarking system for ownership verification. *Expert Systems with Applications*. https://doi.org/10.1016/j.eswa.2014.09.055

Thangadurai, K., and Sudha Devi, G. (2014). An analysis of LSB based image steganography techniques. *2014 International Conference on Computer Communication and Informatics: Ushering in Technologies of Tomorrow, Today*, *ICCCI 2014*, 3–6. https://doi.org/10.1109/ICCCI.2014.6921751

Thanki, R., and Borisagar, K. (2015). Sparse Watermarking Technique for Improving Security of Biometric System. *Procedia - Procedia Computer Science*, *70*, 251–258. https://doi.org/10.1016/j.procs.2015.10.083

Whitelam, C., Osia, N., and Bourlai, T. (2013). Securing multimodal biometric data through watermarking and steganography. *2013 IEEE International Conference on Technologies for Homeland Security, HST 2013*. https://doi.org/10.1109/THS.2013.6698977

Więcław, Ł. (2009). A Minutiae-Based Matching Algorithms In Fingerprint Recognition Systems. In *Journal Of Medical Informatics and Technologies* (Vol. 13).

Yan, W., and Ping, L. (2009). A New Steganography Algorithm Based on Spatial Domain. *2009 Second International Symposium on Information Science and Engineering*, 171–176. https://doi.org/10.1109/ISISE.2009.8

Yang, W., Hu, J., Wang, S., Yang, J., and Shu, L. (2013). Biometrics for securing mobile payments: Benefits, challenges and solutions. *Proceedings of the 2013 6th International Congress on Image and Signal Processing, CISP 2013*. https://doi.org/10.1109/CISP.2013.6743950

Zargar, A. J. (2014). *Digital Watermarking using Discrete Wavelet Techniques with the help of Multilevel Decomposition Technique*. *101*(2), 25–29.

Zhang, L., Gao, W., Jiang, N., Zhang, L., and Zhang, Y. (2011). Relational databases watermarking for textual and numerical data. *Proceedings 2011 International Conference on Mechatronic Science, Electric Engineering and Computer*, *MEC 2011*, 1633–1636. https://doi.org/10.1109/MEC.2011.6025791

ÖZGEÇMİŞ

Kişisel Bilgiler	
Adı Soyadı:	Foday JORH
Doğum tarihi:	10 Ocak 1989
Doğum Yeri:	Banjul/Gambiya
Uyruğu:	Gambiyalı
Adres:	Kazım Karabekir Erkek Yurdu Üniversite Mahallesi Çat Yolu Caddesi No:70 Yakütiye/ERZURUM
E-mail:	foday.jorh161@ogr.atauni.edu.tr
Eğitim	
Lise:	Ndows Kapsamlı Lisesi
Lisans:	University of The Gambia, Computer Science
Yüksek Lisans:	Atatürk Üniversitesi, Bilgisayar Mühendislik Fakültesi
Yabancı Dil Bilgisi	
İngilizce:	İyi
Yayınlar	
1	Jorh F., Özyer B., Fachkha C., (2020). Analysis of Biometric Data Using Watermarking Techniques.Turkish Journal of Electrical Engineering And Computer Sciences, DOI: 10.3906/elk-2002-155 (Accepted)