T.C.

FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİYOMETRİK GÖRÜNTÜLERDE KİMLİK DENETİMİ İÇİN ŞİFRELEME TEKNİKLERİ KULLANILARAK DAMGALAMA

Muhammet Ali USER

Yüksek Lisans Tezi

ADLİ BİLİŞİM MÜHENDİSLİĞİANABİLİM DALI

Adli Bilişim Bilim Dalı

TEMMUZ 2022

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Adli Bilişim MühendisliğiAnabilim Dalı

Yüksek Lisans Tezi

BİYOMETRİK GÖRÜNTÜLERDE KİMLİK DENETİMİ İÇİN ŞİFRELEME TEKNİKLERİ KULLANILARAK DAMGALAMA

Tez Yazarı
Muhammet Ali USER

Danışman
Dr. Öğr. Üyesi Mustafa KAYA

TEMMUZ 2022
ELAZIĞ

T.C.
FIRATÜNİVERSİTESİ
FENBİLİMLERİENSTİTÜSÜ

Adli Bilişim Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

Başlığı:	Biyometrik Görüntülerde Kimlik Denetimi için Şifreleme Teknikleri Kullanılarak Damgalama
Yazarı:	Muhammet Ali USER
İlk Teslim Tarihi:	04.06.2022
Savunma Tarihi:	04.07.2022

TEZ ONAYI

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına göre hazırlanan bu tez aşağıda imzaları bulunan jüri üyeleri tarafından değerlendirilmiş ve akademik dinleyicilere açıkyapılan savunma sonucunda OYBİRLİĞİ ile kabul edilmiştir.

		İmza	
Danışman:	Dr. Öğr. Üyesi Mustafa KAYA Fırat Üniversites Teknoloji Fakültesi		Onayladım
Başkan:	Doç.Dr. Fatih ERTAM Fırat Üniversitesi Teknoloji Fakültesi		Onayladım
Üye:	Dr.Öğr.Üyesi Aytuğ BOYACI Milli Savunma Üniversitesi Hava Harp okulu		Onayladım

Bu tez, Enstitü Yönetim Kurulunun ...../...../20..... tarihli toplantısında tescillenmiştir.

İmza

Prof. Dr. Kürşat Esat ALYAMAÇ
Enstitü Müdürü

BEYAN

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım "Biyometrik Görüntülerde Kimlik Denetimi için Şifreleme Teknikleri Kullanılarak Damgalama" Başlıklı Yüksek Lisans Tezimin içindeki bütün bilgilerin doğru olduğunu, bilgilerin üretilmesi ve sunulmasında bilimsel etik kurallarına uygun davrandığımı, kullandığım bütün kaynakları atıf yaparak belirttiğimi, maddi ve manevi desteği olan tüm kurum/kuruluş ve kişileri belirttiğimi, burada sunduğum veri ve bilgileri unvan almak amacıyla daha önce hiçbir şekilde kullanmadığımı beyan ederim.

04.07.2022

Muhammet Ali USER

ÖNSÖZ

İnternet; alışverişten bankacılık işlemlerine, eğitimden evden çalışmaya kadar, hayatımızın her alanında kullanılmaktadır. Bireysel internet işlemleri, özel ve kamu kuruluşlarında yapılan tüm internet haberleşmesinde şifreler kullanılmaktadır. Şifre kullanımı internet iletişimi dışında; şirketler, bankalar, askeri binalar, emniyet binaları gibi yüksek güvenlik isteyen binalarda da kullanılmaktadır. Yüksek güvenlik gerektiren bu alanlarda kullanılan şifrelerin çalınma veya deşifre edilme ihtimalinden dolayı şifreler çok iyi kriptolanmalıdır.

Binalara veya sistemlere girişte kimlik doğrulama veya denetiminde sistemin en zayıf noktası olan şifreleme işleminde; RSA şifreleme, steganografi ve DWT damgalama kullanarak oluşabilecek güvenlik zafiyetlerinin önüne geçilmiştir. Şifre güvenliği için RSA kriptolama yapılarak metin dosyası haline getirilerek steganografi ile örtü resmine gizlenir, bu örtü resmi biyometrik veri içerisine DWT damgalama ile damga yapılarak şifre ve kullanıcı bilgisi güvenliği sağlanmıştır. Biyometrik görüntülerde kimlik denetimi için şifreleme teknikleri kullanılarak damgalama çalışması yüksek güvenlik gerekli olan alanlarda ideal bir kullanım olarak ortaya çıkmıştır.

Bu tez çalışması süresince bilgi ve tecrübelerinden faydalandığım tez hocam Dr. Öğr. Üyesi Mustafa Kaya'ya teşekkürlerimi sunarım.

Ankara Üniversitesi Tıp Fakültesi Adli Tıp Ana Bilim Dalı Başkanı Prof. Dr. Gürol CANTÜRK hocama her türlü soruma cevapları ve ilgilenmesinden dolayı teşekkürlerimi sunarım.

Muhammet Ali USER
ELAZIĞ, 2022

İÇİNDEKİLER

Sayfa

ÖZET

Biyometrik Görüntülerde Kimlik Denetimi için Şifreleme Teknikleri Kullanılarak Damgalama

Muhammet Ali USER

Yüksek Lisans Tezi

FIRAT ÜNİVERSİTESİ
Fen Bilimleri Enstitüsü

Adli Bilişim MühendisliğiAnabilim Dalı

Temmuz 2022, Sayfa: xiii +54

Günümüzde binalara veya sistemlere giriş için sırasıyla ilk olarak şifre kullanılmıştır. Şifrelerin çalınma veya elde edilmelerden sonra güvenlik seviyesini artırmak için biyometrik veriler kullanılmıştır. Daha yüksek güvenlik için günümüzde akıllı kart, biyometrik veri ve şifre kullanılarak yüksek güvenlik sağlanması hedeflenmiştir. Bu yüksek güvenlik istenen kısımlarda kimlik denetiminin en zayıf noktası olan şifrenin korunması gerekir. Bu amaçla çalışmada biyometrik verilerinin kimlik denetimi için sisteme girilecek şifre RSA kriptolama yapılıp metin dosyası haline getirilerek steganografi ile örtü resmi içerisine gizlenerek damga resmi elde edilmiş elde edilen damga DWT damgalama ile biyometrik veri içerisine yerleştirilmiştir.

Biyometrik veriler, şifreleme çeşitleri ve damgalama çeşitleri araştırılarak; İmge kalite ölçümü PSNR ile MSE hakkında bilgi verilmiştir. Şifrelemede ise RSA şifrelemenin matematiksel açıklaması ve uygulaması yapılmıştır. Damgalamada ise DWT kullanılarak gerekli aitlik koruması sağlanmıştır. Kriptolama, steganografi ve damgalama da MATLAB programı kullanılmış ve sonuçları verilmiştir.

Anahtar Kelimeler: Biyometrik Veri 1, RSA 2, DWT 3

ABSTRACT

Watermarking By Using Encryption Techniques for Authentication in Biometric Images

Muhammet Ali USER

Master's Thesis

FIRAT UNIVERSITY
Graduate School of Natural and Applied Sciences

Department of Digital Forensic Engineering

July 2022, Pages: xiii + 54

Today, passwords are used first, respectively, to enter buildings or systems. Biometric data is used to increase the level of security after passwords are stolen or obtained. For higher security, it is aimed to provide high security by using smart card, biometric data and password. In the parts where this high security is required, the password, which is the weakest point of the authentication, must be protected. For this purpose, in the study, the password to be entered into the system for the authentication of biometric data was made into a text file by RSA encryption and hidden in the cover image with steganography, and the stamp image was obtained and the stamp was placed in the biometric data with DWT stamping.

By investigating biometric data, encryption types and stamping types; Information about image quality measurement PSNR and MSE is given. In encryption, the mathematical explanation and application of RSA encryption has been made. In stamping, the necessary protection of ownership is provided by using DWT. The MATLAB program was used in encryption, steganography and stamping and the results were given.

Keywords: Biometric Data 1, RSA 2, Discrete Wavelet Transform 3

ŞEKİLLER LİSTESİ

Sayfa

TABLOLAR LİSTESİ

Sayfa

SİMGELER VE KISALTMALAR

Kısaltmalar

ADD :Ayrık dalgacık dönüşümü
AES : Gelişmiş şifreleme standardı
AFD : Ayrık fourier dönüşümü
AKD : Ayrık kosinüs dönüşümü
BER : Bit hata oranı
CDMA : Sayısal damganın görüntünün tamamına eklenmesi
DCT : Ayrık kosinüs dönüşümü
DES : Veri şifreleme standardı
DFT : Ayrık fourier dönüşümü
DNA : Deoksiribo nükleik asit
DSA : Dijital imza algoritması
DWT : Ayrık dalgacık dönüşümü
ECC : Eliptik eğri şifreleme
EME : Geliştirme ölçüm hatası
IDEA : Ulusal veri şifreleme algoritması
JPEG : Birleşik fotoğraf uzmanları grubu
KVKK : Kişisel verileri koruma kanunu
LSB : En düşük basamaklı bit
MAE : Ortalama mutlak hata
MSE : Ortalama karesel hatası
NC : Normalizasyon katsayısı
NCC : Normalleştirilmiş çapraz korelasyon
NN : Sinir ağı
OKH : Ortalama kare hatası
PSNR : İşaret gürültü oranı
RC4 : Rivest şifreleme 4
RMSE : Kök ortalama kare hatası
ROI : İlgi bölgesi
RONI : İlgi alanı olmayan bölge
SDD : Sürekli dalgacık dönüşümü
SHA256: Güvenli hash algoritması 256 bit
SNR : Sinyal-gürültü oranı
TDD : Ton doygunluk değeri
UIQI : Evrensel görüntü kalitesi indeksi

1. GİRİŞ

Günümüzde kimlik doğrulama bina girişleri ile herhangi bir sisteme giriş veya veri haberleşmesinde kullanılan gizlilik getiren her yerde gerekli olan denetimdir. Kimlik doğrulama işlemleri için kırılgan damgalama, özet fonksiyonları ve sır paylaşımları gibi yöntemler kullanılarak yapılmaktadır. Biyometrik veri ile sağlanan güvenlik sistemleri geliştirmek için şifre kullanmak, kullanılan şifreyi şifreleme algoritmaları ile gizleyen ve damgalayan çalışmadır.

Teknolojik gelişmeler kişilerin aitlik bilgilerinin tutulmasını zorunlu hale getirmiştir. Kişisel verilerin korunması kanunu ile bu verilerin başka kişi ve kurumların ellerine geçmeden sadece verilere izin verilen kişilerin ulaşması hedeflenmektedir. Kişisel verilerin gizliliği ve bu bilgiler taşınır iken gerekli korunmanın sağlanması çok önemlidir.

Verilerin gizlenmesi çok eskilere dayanmaktadır. M.Ö 1900 yıllarında verilerin gizlenmesi için uğraşılmıştır. Yakın tarihimize bakıldığında 1917 yılında 1. Dünya Savaşında kullanılmak için Joseph Mauborgne ve Gilbert Vernam tarafından Vernam şifresi bulunmuştur. 1918 yılında telsiz haberleşmesinde kullanılan ADFGVX şifrelemesi bulunmuştur.1929 yılında ise lineer cebire dayanan Hill şifresi ortaya konulmuştur. 1940-1944 İkinci Dünya Savaşında Almanlar ENIGMA, İngilizler TYPEX, Amerikalılar SIGABA, Japonlar RED&PURPLE veri gizleme cihazları bulunmuştur. 1970 yılında ise Demon ve Lucifer veri şifrelemesi bulunmuş günümüzde kullanılan DES şifrelemesinin temeli ortaya çıkmıştır. 1977 Ronald Rivest, Adi Shamir ve Leonard Adleman, RSA algoritması geliştirilmiştir. Sırasıyla 1980 yılında ROT13, 1985 yılında ECC, 1990 yılında IDEA, 1995 yılında SHA-1 ve 2000 yılında AES bulunmuştur [1].

RSA ve DWT ile yapılmış çalışmalara bakıldığında Varghese ve Kamal çalışma konusu olan DWT alan damgalaması ile birleştirilmiş gelişmiş RSA uygulamasında; dijital görüntü içerisine gizli bilgileri gizlemek için gelişmiş RSA algoritmasını damgalama teknikleriyle birleştiren bir çerçeve sunmaktadır. RSA şifreli veriler ve damgalama, Ayrık Dalgacık Dönüşümü (ADD) algoritması kullanılarak bir Ton Doygunluk Değeri (TDD) renkli görüntüsünün içine yerleştirilmiştir. Dalgacık dönüşümünün doğruluğu, yeniden yapılandırma sonrasında Ortalama Kare Hatası (OKH), Korelasyon ve Tepe Sinyali / Gürültü Oranı hesaplanarak belirlenmiştir. Görünmez sağlam damgalama DWT kullanarak orijinal verileri değiştirmeden bırakmıştır. Orijinal düz metin, çıkarılan şifreli metin üzerine gelişmiş RSA şifre çözme algoritması uygulanarak elde edilmiştir. Yapılan çalışma sonrası gelişmiş RSA algoritmasının hesaplama hızını ve DWT tabanlı damgalama teknolojisinin sağlamlığını birleştirmiş. Bu verimli teknikleri birleştirerek bilgi güvenliği sağlanabilmiştir [2].

Venkatram, Reddy, Kishore ve Shavya ‘nın yaptığı çalışmada RSA-DWT kullanılarak hastanın MR gibi tıbbi görüntülerini şifreleyerek damgalama yapılmıştır. Hasta bilgilerini korumak için bu yol seçilmiştir. Tıbbi görüntülere damga eklemek dikkatli olmayı gerektirdiği belirtilmiştir.

Hastanın tıbbi bilgileri, görüntü şifreleme ve şifre çözme için RSA algoritması kullanılarak gerçekleştirilmektedir. Medikal görüntüler, 2D Ayrık Dalgacık Dönüşümü kullanılarak dönüşüm alanında şifrelenmiş hasta görüntüsü ile damgalanır. Ana tıbbi görüntü ve damgalanmış görüntüsü dalgacık alanına dönüştürülür ve karıştırılır. Son olarak bu damgalı tıbbi görüntüler şifre çözme için kullanılacak gizli anahtar ile birlikte internet üzerinden iletilmiş alındığında gömülü şifrelenmiş filigran 2DWT ve şifre çözme anahtarı kullanılarak çıkarılmıştır. Önerilen damgalama tekniklerinin sağlamlığı, damgalı tıbbi görüntülere çeşitli saldırılar ile test edilmiş, Peak-Signal-to-Noise oranları ve normalize edilmiş çapraz korelasyon katsayıları, damgalı medikal görüntülerin ve çıkartılmış hasta görüntülerinin kalitesine erişmek için hesaplanmıştır. Sonuçlar dört farklı seviyede (1,2,3,4) dört dalgacık (haar, db, symlets, bior) kullanılarak tek tuş kullanılarak bir hasta görüntü damgalamaya sahip üç tip tıbbi görüntü için üretilmiştir. Deneysel sonuçlarda RSA-DWT 'nin normal DWT ye göre daha üstün olduğu ortaya koyulmuştur [3].

Khamy, Korany, El-Sherif yaptığı çalışma kapak sesinin birkaç çoklu alt banda ayrıştırıldığı Ayrık Dalgacık Dönüşümü alanındaki örnek karşılaştırmasına dayanan verimli bir damgalama şeması önermektedir. Seçilen detay katsayıları, gömme şifresi görüntü bitine bağlı olarak bir eşik değeri ile değiştirilmiştir. Bu yaklaşım, üzerinde RSA şifrelemesi gerçekleştirmek için orijinal bir görüntü bileşeni kullanılmış, ardından şifreleme bitleri, önceden belirlenmiş bir eşik değerine göre ses sinyalinin ayrıntı bileşenlerine gömülmüştür. Algoritmanın performansı saldırılara karşı kapsamlı bir şekilde tahmin edilmiş ve önerilen algoritmanın sağlamlığını kanıtlamak için simülasyon sonuçları sunulmuştur. Deneysel sonuçlarına bakıldığı zaman iyi bir PSNR ve yüksek veri gömme kapasitesi ortaya koyduğu test edilmiştir [4].

Nagpal, Bhushan, Mahajan çalışmasında ise Sinir Ağı, DWT ve RSA kullanan tıbbi görüntüler için geliştirilmiş dijital görüntü damgalama üzerine çalışma yapılmıştır. Görüntü damgalaması için üç teknik yani; DWT, Neural Network (NN) ve RSA şifreleme kullanılmıştır. Sonucunda önerilen tekniğin performansı MATLAB R2010a ortamında PSNR, MSE, BCR, BER ve NCC bazında ölçülmüştür [5].

Kumari ve Yadav ise Biyometrik Steganografi ve biyometrik olmayan stenografi sunmuş. Dış görünüm alanı ve kenar pikselleri değerlendirilmiş ve RSA algoritması ile şifrelenen gizli veriler belirli bir alana gömülmüştür. Veriler tüm görüntü yerine belirli bir bölgeye gömülü olduğundan stego görüntüsünün güvenliği ve kalitesi artırılmıştır [6].

Garg, Gupta ve Khatri 'nin LSB-RSA ve 3-DWT algoritması kullanan ATM işlemi için parmak izi damgalama ve steganografi çalışmasında, dijital görüntülerin telif hakkı koruması ve kimlik doğrulaması sağlamak için damgalama teknolojisiyle parmak izi doğrulama yöntemlerinin kombinasyonu önerilmektedir. Daha iyi doğruluk için teknik önerirken DWT 'yi RSA ve LSB ile birleştirilmiştir. Bu çalışmada; yanlış eşleşme oranını, yanlış kabul oranını, ortalama kare hatası,

doğruluk ve tepe sinyal gürültü oranı incelenmiş DWT ve RSA uygulamasında yüksek değerler elde edilmiştir [7].

Bhargava, Mukhija 'nın LSB, DWT ve RSA kullanarak görüntü ve metini gizleme stenografisi çalışmasında kriptografi ve Steganografi' nin bilgilerin karıştırıldığı ve buna ek olarak görüntü işleme yoluyla başka bir ortamdaki iç görüleri kapsadığı yeni stratejiler sunmuştur. Şifrelenmiş resim, LSB bitlerinin DWT stratejilerinin kullanılması yoluyla, başka bir görüntüde gizlenmiştir. MATLAB platformunda tercih edilen, kriptografi ve Steganografi düzenlemeleri setinin kullanılmasıyla uygulanılmıştır. PSNR ve MKE'yi hesaplanmış, ayrıca kapak resminin ve stego resminin entropisini hesaplanmıştır [8].

Kadhim Bermani'nin çalışması ise DWT, DCT ve RSA' ya dayalı yüksek güvenlikli Steganografi modeli çalışmasında, birden fazla algoritmanın kullanıldığı başka bir görüntüde kapak resmi görüntüye gizli görüntüyü gizlemek için yüksek güvenlikli model önermiştir. Ayrık dalgacık dönüşümü algoritması ve uygulanan DCT algoritması, gizli görüntüyü sıkıştırmak ve gizli görüntünün gizlenmesi için daha fazla alan sağlamak ve şifrelemeye RSA algoritması uygulanmış ve daha güvenli olması sağlanmıştır. Bu modelin kalitesini hesaplamak için PSNR ve MSE gibi belirli kalite ölçümlerinde CR kullanılmış DWT ve RSA yüksek güvenli olduğu ortaya konulmuştur [9].

Divya' nın DWT-SVD ve RSA şifreleme kullanarak Telif Hakkı Koruması için hibrit dijital görüntü damga oluşturma çalışmasında mevcut yöntemlerin çoğu, sağlamlık ve yerleştirme kapasitesine odaklanır, güvenliği gözden kaçırır. Bu makale, büyük gömme kapasitesi, iyi sağlamlık ve yüksek hesaplama verimliliği temelinde gizli verilerin güvenliğini garanti etmek için karıştırma algoritması DWT ve RSA asimetrik şifreleme algoritmasına dayalı yeni bir dijital görüntü damgalama modeli ortaya koymuştur. Deneylerinde; RSA' nın şifreleme algoritmalarının damgalama görüntüsüne uygulanmasını ve ana bilgisayar görüntüsü üzerinde Ayrık Dalgacık Dönüşümünün ve Tekil Değer Ayrıştırmasının hibrit ayrıştırmasının gerçekleştirilmesini içermektedir ve damgalama düşük frekanslı alt banda gömülmüştür [10].

Kishore, Venkatram, Sarvya, Reddy Dalgacık etki alanında RSA şifrelemesi kullanarak tıbbi görüntü damgası oluşturma çalışmasında MRI, CT ve ultrason olmak üzere üç tür tıbbi görüntünün şifreleme tabanlı tıbbi görüntü damgalaması kullanılmaktadır. Bu uygulamada kullanılan damga hasta görüntüsüdür. Damga hasta görüntüsü, RSA algoritmasına sahip bir genel anahtar şifrelemesi kullanılarak şifrelenir. Kapak resmi, damga eklenecek standart çözünürlükte tıbbi bir resimdir. RSA şifreli hasta görüntüsü, dalgacık dönüşüm alanındaki tıbbi kapak görüntüsüne yerleştirilir. Ters dalgacık dönüşümü, damga olarak hasta görüntüsüne sahip damgalı bir tıbbi görüntü oluşturmak için uygulanır. Damgalı görüntü hem görsel kalitede hem de nicelikli olarak PSNR ve normalize çapraz korelasyon kullanılarak test edilmiştir [11].

Solanki, Malik, Chhikara'nın DWT ve RSA kullanarak RONI(Region of Non Interest, ilgi alanı olmayan bölge)medikal Görüntü damgalama çalışması önerilen çalışma hasta bilgilerini CT taraması veya MRI görüntüsü olabilecek tıbbi görüntünün kendisinde saklamak üzeredir. İlk olarak görüntünün ROI (Region of Interest, ilgi bölgesi) ve RONI' sini belirlemek için iki ana aşamaya ayrılmıştır. Buraya, ROI, tıbbi görüntünün bilgi kısmı olarak tanımlanır ve RONI, MRI görüntüsünün bilgi olmayan kısmı olarak tanımlanır. Kullanıcının değerli bilgileri görüntüden yok etmesini önleyecektir. Damgalama, RSA kullanılarak şifrelenir. İkinci aşama, görüntüyü RONI'ye gizlemek üzeredir. Bu tür bilgileri gizlemek için DWT tabanlı bir yaklaşım kullanılır. Genel Koşullar ROI' nin korunması ile birlikte DWT ve RSA kullanarak medikal görüntülere iki yönlü güvenlik sağlamaktır [12].

Biyometrik görüntülerde kimlik denetimi için şifreleme teknikleri kullanarak damgalama yapılmıştır. Kimlik denetimi için biyometrik veri kullanılmış; yüksek güvenlik için biyometrik veri ile şifre kullanılmış sistemin en zayıf noktası olan şifreyi RSA şifreleme ile şifrelenmiş daha sonra biyometrik veriye DWT ile damgalanarak güvenlik önlemi alınmıştır.

Bu çalışmanın ikinci bölümde biyometrik veriler tanıtılmıştır. Biyolojik veriler olarak fizyolojik ve davranışsal olarak ikiye ayrılmış fizyolojik olanlar parmak izi tanıma, parmak damar izi, el geometrisi, yüz tanıma, göz tanıma, DNA tanıma olarak tanıtılmıştır. Davranışsal biyometrik veriler olarak ise ses, konuşma tarzı, tuş vuruş hızı, imza olarak ele alınmıştır.

Üçüncü bölümde ise damgalama ve damgalama çeşitleri hakkında bilgi verilmiştir. Damgalamada özellikle sayısal damgalama olan LSB, DWT, DCT, DFT SVD damgalama metotları incelenmiş tez konusu olan DWT ayrıntılı olarak ele alınmıştır. Damgalama hata oranları işaret gürültü oranı, normalizasyon, bit hata oranı hakkında bilgi verilmiştir. Yine diğer bir konu olan sayısal damgalamaya yapılan saldırılar olan gürültü ekleme, kırpma, JPEG kayıplı sıkıştırma, tekrar damgalama geometrik saldırılar, ölçekleme gibi saldırılar hakkında bilgi verilmiştir.

Dördüncü bölümde ise şifreleme hakkında bilgi verilmiştir. Özellikle şifreleme çeşitleri olarak simetrik anahtarlama, blok şifreleme, açık anahtar şifreleme, şifreleme protokolleri hakkında bilgi verilmiştir. RSA şifreleme detaylı anlatılmış RSA şifrelemeye yapılan saldırı çeşitleri olan yan kanal saldırıları ve kripto analiz saldırıları hakkında bilgi verilmiştir.

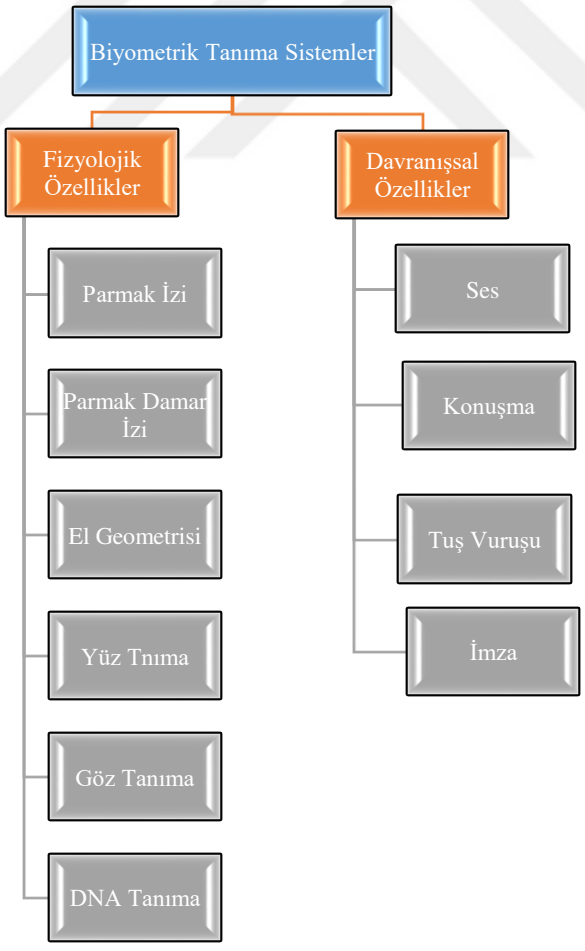
Beşinci bölümde ise parmak izi verisi RSA ile şifreleme, LSB yöntemi ile steganografi ve DWT ile damgalama işlemi yapılmıştır. MATLAB sonuçları ve çıktıları verilmiştir.

Altıncı bölümde materyal ve metotlar kısmında elde edilen bulgular verilip konun önemi anlatılmıştır.

2. BİYOMETRİK VERİLER

Biyometrik veriler kişiye özgü özellikler olarak üç kısımdan oluşmaktadır ve bu veriler fizyolojik özellikler, davranışsal özellikler ile biyokimyasal olarak ifade edilmektedir. En çok kullanılan ise fizyolojik ve davranışsal özelliklerdir. Şekil 2.1'de belirtildiği gibi fizyolojik özellikler; parmak izi, parmak damar izi, el geometrisi iç/dış, yüz tanıma, göz tanıma, DNA tanıma olarak ifade edilmiştir. Davranışsal özellikler ise ses, konuşma tarzı, tuş vuruşu, imza olarak ortaya çıkmıştır. Rakhımov, Biyometrik veri olarak yüz tanıma verisi kullanılarak biyometrik veriler ile kimliklendirmenin güvenli olarak yapıldığının bir örneğini ortaya koymuştur [13].

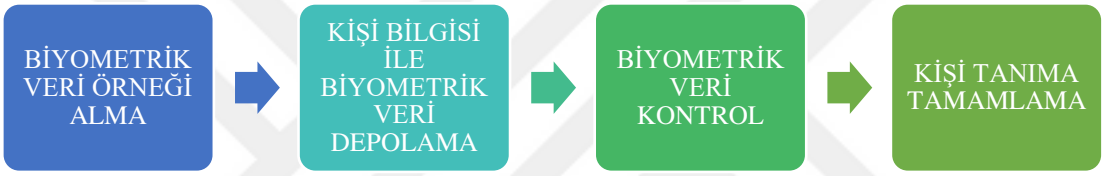
Biyometrik kelimesinin açılımına bakıldığı zaman ise "Bio" (yaşam) ile "Metron" (Ölçüm) kelimelerinin birleşiminden meydana gelmiştir. Sensörler ile elektrik sinyaline çevrilen biyometrik veriler elektronik devreler vasıtasıyla sayısal işarete dönüştürülerek bilgisayarda işlendikten sonra veri tabanına kayıt yapılıp kişi tanıma için kullanılmaktadır. Parmak izi okuyucu gibi sensörü olan devrede parmak kapasitesinden faydalanarak parmak izi belirlenen devreler vardır. [14,15].



Şekil 2.1. Biyometrik tanıma sistemleri

2.1. Parmak İzi Tanıma

Parmak izi her insanda farklı olduğu için kişileri ayırt etmek için kullanılan biyometrik veri çeşididir. Parmak izi verisi parmak izi cihazı ile sensörler ile elde edildikten sonra veri tabanına kayıt edilir. Daha sonra veri tabanına kayıt yapılan parmak izi verileri personel takibi gibi işlemlerde kullanılmaya hazırdır. Artık personel parmak izini okutup sistemde kayıtlı olan veri tabanı ile kontrol edilerek kayıtlı personel olduğu ve giriş çıkış saatleri kayıt altına alınır. Şekil 2.2' de biyometrik bir sistemin oluşumunun blok diyagramı görülmektedir. Blok diyagramda ilk olarak biyometrik veri sensör ile alınmaktadır, daha sonra sırayla biyometrik veri depolama, kimlik testi için gelen kişinin biyometrik verisi ile hafızadaki biyometrik verinin kontrolü yapıldıktan sonra biyometrik veri karşılaştırması yapılarak kişi tanıma işlemi bitirilmiştir [15].



Şekil 2.2. Biyometrik sistem yapısı

2.1.1. Parmak İzi Örneği ve Diğer Biyometrik Veriler ile Karşılaştırılması

Örnek bir parmak izi Şekil 2.3 verilmiştir. Biyometrik görüntülerde kimlik denetimi için şifreleme teknikleri kullanarak damgalama tezimde parmak izi üzerine şifreleme ve damgalama yapılacağından diğer biyometrik veriler ile karşılaştırılması tablo 2.1 verilerek günlük hayattaki durumu hakkında bilgi sahibi olunacaktır [16].

Şekil 2.3. Parmak izi örneği [16]

Tablo 2.1. Biyometrik verilerin karşılaştırılması [15]

Biyometrik Kaynak	Evrensellik	Ayırt Edicilik	Süreklilik	Bulunabilirlik	Performans	Kabul Edilebilirlik	Sistemi Atlatma
Yüz	Y	D	O	Y	D	Y	Y
Parmak İzi	O	Y	Y	O	Y	O	O
El Geometrisi	O	O	O	Y	O	O	O
Damar	O	O	O	O	O	O	D
İris	Y	Y	Y	O	Y	D	D
Retina	Y	Y	O	D	Y	D	D
İmza	D	D	D	Y	D	Y	Y
Ses	O	D	D	O	D	Y	Y
Yüz Termogramı	Y	Y	D	Y	O	Y	D
DNA	Y	Y	Y	D	Y	D	D

Y: Yüksek, O: Orta, D: Düşük

Tablo 2-1 göre;

Evrensellik: Biyometrik verinin insanda bulunma durumunu gösterir. Parmak izini örnek alır isek yaygınlık orta işaretlenmiştir sebebi ise insanların parmak izleri zamanla yanma veya diğer dış etkenlerden bozulacağındandır.

Ayırt Edicilik: Biyometrik verilerden kişiyi belirtme özelliğini belirtmektedir.

Süreklilik: Biyometrik kaynağın direncini belirtir.

Bulunabilirlik: Biyometrik verilerin işlenmesi ve bulunabilirliğini gösterir.

Performans: Biyometrik elemanlarının doğruluk yüzdesi, hızı ve sağlamlığını anlatır.

Kabul Edilebilirlik: Biyometrik verinin günlük hayatta kabul görme derecesini gösterir.

Sistemi Aldatma: Biyometrik kaynaklar ile sistemi aldatabilme ihtimalini belirtir [15].

2.1.2. Parmak İzi Sistemlerinin KVKK Uygunluğu

Parmak izi verileri veri tabanına kopya edildiğinde veri tabanına yapılan saldırılarda çalınma riski olduğundan, parmak izi verileri direkt veri tabanına saklama yerine matematiksel bir algoritmadan geçirilip, çıkarılan takip numarası veri tabanına saklanarak, veri tabanına yapılan saldırılarda veri tabanı ele geçirilse bile parmak izine ulaşılmayacak, takip numaralarına ulaşılacak bu takip numarası hiçbir işe yaramayacaktır. Kişi verileri koruma kanuna göre kişisel veri niteliği olan parmak izi verileri saklanmayıp kanuna uygun işlem yapılmış olacaktır [17].

2.2. Parmak Damar İzi

Parmak damar izi koyucular parmakta bulunan damarları okuyup sayısal forma dönüştüren cihazlardır. İnsanlardaki damar sistemi de kişileri ayırt eden ve kişiye özgü bilgidir. İkiz kardeşlerde bile damar sistemi farklıdır. Parmak damar izi parmak izine göre daha belirgindir çünkü parmak izi zamanla elde oluşan yaralanma ve yanma gibi sebeplerden bozulabilir ama parmak damar izinde böyle bir sakınca yoktur. Parmak izinin kullanılmasının amacı ise kişilerin işlediği suçlarda parmak izi taraması yapılıp suçlu olup olmadığı tespitinde çok faydalı olduğundan kullanılması çok uygun olmaktadır. Parmak damar izi okuma sistemi hastanelerde kullanılarak bu sistem sayesinde kişiler başkasının yerine muayene olmasının önüne geçilmesi planlanmıştır. Şekil 2.4 parmak damar izi okuma cihazı görülmektedir. Cihaz incelendiğinde mavi ile çizilmiş kısımda parmak izi taraması yapıldığı anlaşılmaktadır [18].

Şekil 2.4. Parmak damar izi okuma cihazı [18]

Parmak damar izi okuma cihazı yanında avuç içi damar okuma sistemleri vardır. Avuç içi damar okuma çalışması parmak damar izi okuma cihazı ile aynı olup kızılötesi ışık ile damarlar okunup sayısal formu dönüştürülüp işlenmesi prensibi ile çalışmaktadır. Avuç içi damar okuma cihazı şekil 2.5 gösterilmiştir. Avuç içi damar okuma cihazlarında birden fazla sensör kullanılarak hız ve hata payı düşük bir okuma yapılmaktadır [19].

Şekil 2.5. Avuç içi damar okuma cihazı [19]

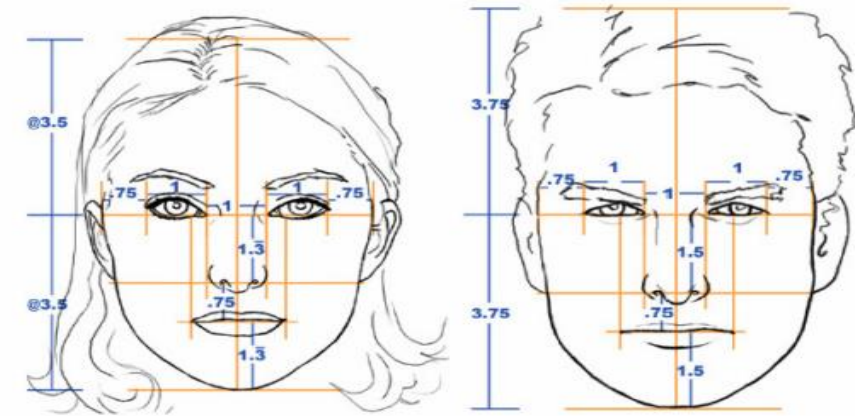
2.3. El Geometrisi

Elin geometrik yapısı kişilerde farklılık gösterdiği için biyometrik veri olarak kullanılmaktadır. El geometrik fiziksel yapısı kimlik tanıma yerine kimlik doğrulama için kullanılmaktadır. El geometrisi tanıma sistemlerinde el tanıma sistemine konulan elin üç boyutlu olarak ölçülerek sisteme kayıt edilerek ölçülmesi prensibine dayanır. El geometrisi ile tanıma parmak izi gibi benzersiz biçimde değildir. El geometrisi kişi tanıma yerine kişi doğrulama işlemlerinde daha uygundur. El geometrisi tanıma sistemine yerleştirilen elin uzunluk kalınlık ve eğrilik gibi özellikleri dikkate alınarak ölçümü yapılır. Şekil 2.6 gösterilen el geometrisi tanıma cihazı ile elin yapısal özelliği sensör ile elde edilerek biyometrik veriler elde edilmektedir [20,21].

Şekil 2.6. El geometrisi tanıma cihazı [20]

2.4. Yüz Tanıma

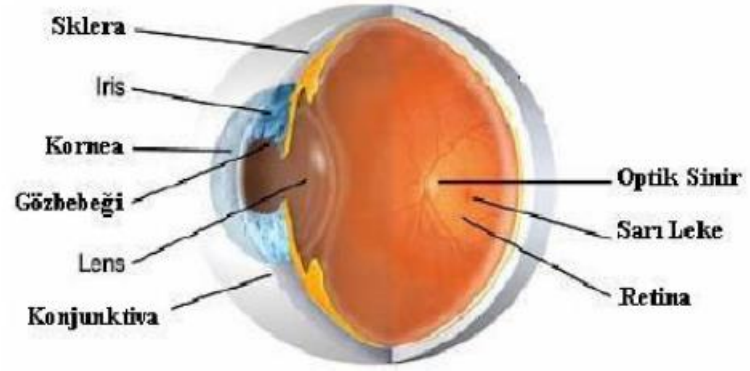
Yüz tanıma sistemi altın oran prensibine göre çalışır. Kamera ile fotoğrafı çekilen resimler şekilde görüldüğü gibi burun ile alın, göz ile dudaklar, burun ile çene arası uzaklıklar dikkate alınarak veri sistemine kayıt edilir, kayıt işleminden sonra her kontrolde kayıt edilen resimler veri tabanı kontrol edildikten sonra uyum sağlanıp sağlanmamasına göre çıkış verilir. Yüz tanıma sistemleri hareketli görüntü veya sabit görüntüye göre çeşitlilik kazanmış günümüzde iki sistemde kullanılmaya başlanmıştır. Şekil 2.7 ise yüz tanıma sistemlerinde kullanılan yüz hatlarının yapısı görülmektedir. [22,23].



Şekil 2.7. Yüz tanıma sistemi [23]

2.5. Göz Tanıma

Göz tanıma sistemlerine başlamadan gözün yapısı incelenmelidir. Gözün yapısına bakılırsa ön tarafta kornea, kırmızı ile gösterilen yeri iristir. Sarı ile gösterilen kısım ise retinadır. Şekil 2.8 retina ve irisin yeri tam olarak anlaşılabilir. İnsanlarda iris ve retina farklılık gösterdiği için biyometrik veri olarak kullanılmaktadır [24]. Biyometrik veri olarak iris tanıma ve retina tanıma incelenirse;



Şekil 2.8. Gözün yapısı [24]

2.5.1. İris Tanıma

Gözdeki iris Şekil 2.8 görüleceği üzere gözün ön tarafında bulunan renkli kısmıdır. Gözün renkli kısmı iris olduğu için belli bir uzaklıktan fotoğrafı çekilerek iris bilgileri dijital veriye çevrilerek kullanılır. İris deseni iki gözde farklı olduğu için iki göz için iris deseni alınmalı veya hangi göz için alınıyorsa sistem ona göre algoritma üretilmelidir. Parmak izi biyometrik verisi

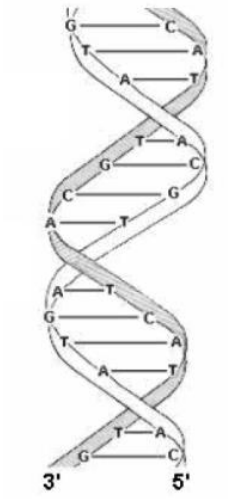
referans nokta sayısı 70 gibi kabaca bir değer oluşurken iris tanımada bu üç katı kadar olmaktadır [25].

2.5.2. Retina Tanıma

Şekil 2.8 ‘den görüleceği üzere gözdeki retina, sarı renkle görülen belirtilen kısmıdır. Retina üç dokudan meydana gelmektedir. Bunlar epitel, iris, endotel dokudur. Bu dokuların aynı çıkma olasılığı çok düşüktür. Retina tanıma sisteminde gözün kamera ile çekimi yapılır. Elde edilen resim sayısal veriye çevrilmesidir. Retina taraması yapılırken hareket yapılmaması gerekmektedir. Maliyeti yüksek olduğu için güvenliğin üst seviyede olduğu yerlerde kullanılır. Retina tarama sisteminin yanılma payı yaklaşık sıfırdır [26].

2.6. DNA Tanıma

Şekil 2.9’ da şematik şekli olan DNA canlıda canlılık işlevlerini yerine getirmesi için gerekli olan genetik bilgileri taşıyan nükleik asittir. Tüm temel bilgilerin saklandığı birim olarak kabul edilebilir. İnsanda DNA anne babadan çocuğa geçer. Her insanda farklı DNA özelliği olduğu biyometrik veri olarak kullanılabilir. DNA analizi uzmanlık gerekli olduğu için özel laboratuvarlarda yapılır [27].



Şekil 2.9. DNA yapısı ve eşleşmesi [27]

DNA biyosensörleri hastalıkların tedavisi için kullanılabilir, bunun yanında maliyetlerinin düşük olması ve hassasiyetlerinin yüksek olması avantajı vardır [28].

DNA çekirdekli her hücrede bulunduğundan asayiş olaylarında polisler olay yerindeki biyolojik verileri alarak (kan, tükürük, meni vb) DNA analizi yapmaktadırlar. Alınan verilerin DNA analizlerinden kime ait olduğu bulunarak olaydaki şüphelilere ulaşılmaya çalışılır [29].

2.7. Ses, Konuşma Tarzı, Tuş Vuruşu, İmza Davranışsal Biyometrik Veriler

Davranışsal biyometrik veriler insana özgüdür ve elde edilmesi basit verilerdir. Fizyolojik biyometrik veriler gibi ayrıntılı donanıma ihtiyaç duymadan fiziksel hareketlere dikkat edilerek elde edilen verilerdir. Bu veriler uygun algoritmalarla tanıma sistemi ortaya çıkarılarak tanıma işlemi yapılabilir [30].

3. DAMGALAMA (WATERMARKING)

Biyometrik verilerin damgalanması yapılacağı için, ikinci bölümde biyometrik veriler incelenmiş, damgalama işlemi temel bilgileri elde edilmiştir. Damgalama gönderilecek veriler içerisine (ses, resim, yazı… vb.) verinin sahibi olanın ismi veya logosunun gizlenmesi ile teklif hakkının korunması hedef alınmıştır. Stenografi gibi veri gizleme işlemidir. Damgalamada gizlenen verinin kırılma veya yok edilmesi zorlaştırılır [31].

Damgalama işleminde damgayı görüntü, ses, resim vb. içerisinden çıkarılırken güvenlik anahtarı istenebilir, ek güvenlik önlemi açısından önemlidir. Damgalama işleminde damga görünür veya görünmez olarak eklenebilir. Bilgisayar ortamında birçok damgalama yöntemi vardır.

3.1. Genel Damgalama Teknikleri

Damgalama teknikleri ve terimlerinin daha iyi anlaşılması için damgalama ile ilgili temel bilgilerin bilinmesi gerekir.

3.1.1. Damgalama Terminolojisi

Herhangi bir sistem tasarlanır iken bu sistemin belli başlı bölümleri bulunmaktadır. Sistemi anlamak için bu bölüm gerekli bilgilerin bilinmesi gereklidir [32,33].

- **Taşıyıcı (örtülü) Dosya:** Verinin saklandığı dosyadır.
- **Güvenlik Anahtarı:** Güvenlik anahtarının bulunduğu yerdir.
- **Görülür Damgalama:** Verilerde damganın belli olduğu dosyalardır.
- **Görülmez Damgalama:** Dosyalarda damganın görülmediği dosyalardır.

3.1.2. Temel Damgalama

Şekil 3.1 ile damgalama şekil 3.2 ise damga çıkarma işlemleri ana hatları ile ortaya konulmuştur. Temel damgalama olayı steganografi ile aynı sayılabilir. Damgalamada gizli damgalama ve açık damgalama olarak ikiye ayrılmış olsa da, amaç gönderilen verinin kime ait olduğunun bilinmesidir bunun temel şeması aşağıdadır [32,33].

Şekil 3.1. Damgalama işlemi

Şekil 3.2. Damga geri elde etme

3.1.3. Damgalamanın Temel Gereksinimleri

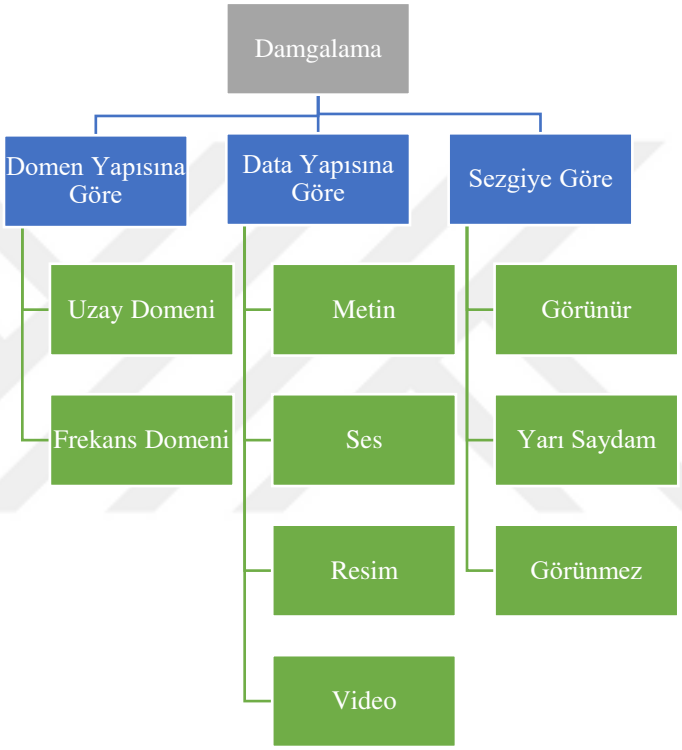
Damgalamada bazı gereksinimlere ihtiyaç olur. Bu her uygulamada farklı olsa bile genel olarak sağlamlık (Robustness), fark edilemezlik (Imperceptibility), kapasite (Capacity), güvenlik (Security), düşük karmaşıklık (Low Complexity) olarak ifade edilebilir. Şekil 3.3 damgalama özellikleri gösterilmiştir [33-36].

Şekil 3.3. Damgalamanın özellikleri

- **Sağlamlık (Robustness) :** Dosyanın saldırılara karşı dayanıklılığıdır.
- **Kapasite (Capacity):** Damga sınırını belli eder.
- **Fark edilemezlik (Imperceptibility):** Saldırılara karşı damganın silinmemesidir.
- **Düşük karmaşıklık (Low Complexity):** Damganın belirgin ve az karmaşık olmasıdır.

3.2. Damgalama Yöntemlerinin Sınıflandırılması

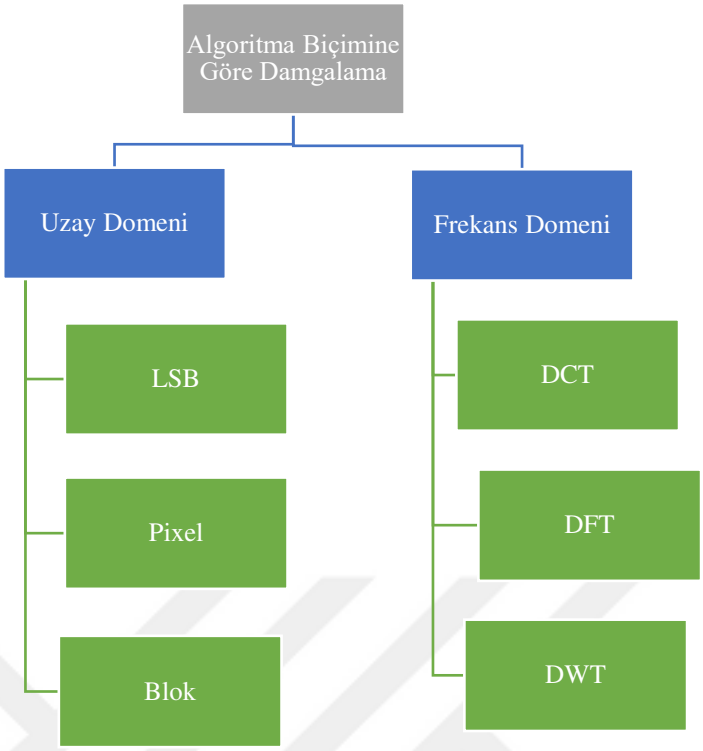
Damgalama algoritma düzlemine göre, veri ortamına göre ve algıya göre olmak üzere temelde 3 çeşit olarak ayırım yapılabilir. Algoritma düzlemine göre uzay domeni ve frekans domeni olmak üzere 2 çeşittir. Veri ortamına göre ise metin, ses, resim, video olmak üzere 4 çeşittir. Algıya göre damgalama ise; görünür, yarı saydam, görünmez şeklindedir. Görünmez damgalama ise dayanıklı ve kırılgan olarak ikiye ayrılmıştır. Dayanaklı damgalama ise özel anahtarlı ve kamusal anahtarlı olarak ikiye ayrılmıştır. Şekil 3.4 ayrıntılı gösterilmiştir [31].



Şekil 3.4. Damgalama sınıflandırılması

3.2.1. Algoritma Düzlemine Göre Damgalama

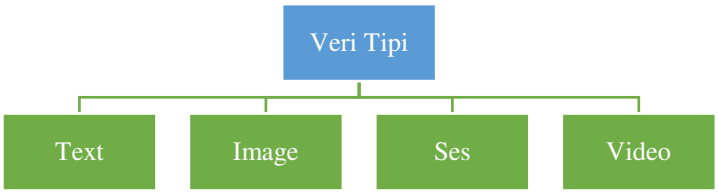
Algoritma düzlemine göre damgalama uzaysal ve frekans şeklinde ikiye ayrılır. Uzaysal damgalama LSB piksel ve blok olmak üzere ikiye ayrılabilir. LSB en değersiz bite veri ekleme metodu olduğundan sıkışma ve veri küçültme gibi durumlarda bozulmalar olacağı için genellikle kullanılmaz. Sayısal damgalama yöntemlerinden olan frekans düzleminde DFT, DCT, DWT diğer bölümlerde ayrıntılı incelenecektir. Verilerin sıkıştırılma gibi durumlarında dayanıklı olduğu için kullanılır. Şekil 3.5 algoritma düzlemine damgalama biçimleri gösterilmiştir [31-37].



Şekil 3.5. Algoritma düzlemine göre damgalama

3.2.2. Veri Cinsine Göre

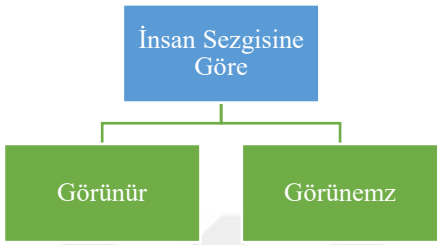
Yazı, resim, ses, video olmak üzere 4 çeşittir. Damgalanacak verinin türünü belirtmektedir. Damgalanacak veri metin şeklinde yazılardan oluşabilir resim, ses ve video doyası şeklinde olabilir. Şekil 3.6 'da kullanılan veri çeşitleri gösterilmiştir [31-37].



Şekil 3.6. Veri cinsine göre damgalama

3.2.3. İnsan Algısına Göre

Görülebilir ve görülemez olmak üzere iki çeşittir. ÖSYM sınavlarında olduğu damgalamanın görülmesi istenir. Telif hakları gibi durumlarda ise damgalama görünmez kopya edilme durumunda kimden olduğu görünmez damgalama ile ortaya konulur. Şekil 3.7'de İnsan algısına göre veri işlenmesi gösterilmiştir [33-37].



Şekil 3.7. İnsan algısına göre damgalama

3.2.4. Sağlamlık

Güçlü, yarı kırılgan, kırılgan olmak üzere 3 çeşittir. Sağlamlık durumu ise damganın kırılma durumunu ortaya koymaktadır. Kırılgan damgalamada damga silinebilir ve başka damgada yapılabilir. Yarı kırılgan damgalamada damganın silinmesini zorlaştırmak içindir. Güçlü damgalamada telif hakları saklanması gibi damganın silinmesinin önlenmesi için kullanılır. Sağlamlık damgalamanın saldırılara karşı durumunu ortaya koymaktadır. Dayanaklı damgalama saldırıya göre değişir, sıkıştırma gibi durumda frekans domeni iyi olmakla birlikte geometrik saldırı olan döndürme durumlarında uzay domeni daha iyi olabilir. Damganın boyutu saldırılarda koruma için önemli bir ayrıntıdır. Damga dayanaklığına göre damgalama çeşitleri Şekil 3.8' de belirtilmiştir [33-37].

Şekil 3.8. Sağlamlık

3.2.5. Dayanıklı Damgalama

Yapılan çalışmalarda damgalamanın saldırılara dayanıklı olması istenmiştir. Fakat hem dayanaklı hem de bütün görüntünün bozulmadan gitmemesi de önemli bir konu olarak ortaya çıkmaktadır. Örnek bir çalışma olarak Kazan S. ve Vural C.'in yaptığı sayısal görüntü damgalama yöntemlerinin jpeg sıkıştırma karşısında dayanıklılığının karşılaştırılması çalışmasında, sayısal bir görüntüye damgalanmış JPEG sıkıştırması tabi tutulmuş CDMA, bloklara ayırma işlemleri ve frekans uzayı uygulanarak dayanıklılık araştırılmıştır. Frekans domeni uygulanmış bu uygulamalara CMDA ve bloklara ayırma yöntemi uygulanarak hem uzay domeni hem de frekans domeni çalışmasında CMDA' nın iyi sonuç verdiği ortaya çıktığını belirtmişlerdir [38].

3.2.6. Kırılgan Damgalama

Bazı uygulamalarda saldırılarda damga bozularak okunamayacak hale gelmelidir. Y. Şahin, G. Ulutaş, M.B. İmamoğlu'nun yaptığı ilişkisel veri tabanlarının bütünlük kontrolü için, ayrık kosinüs dönüşümü tabanlı kırılgan sıfır damgalama şeması çalışmasında ise saldırılarda internet sisteminin kontrolü altına alınarak damga güvenli hale getirilmesi amaçlanmıştır. Kullanılan yöntemde AKD kullanılmıştır. Bu çalışmada veri tabanından ayrı bir damga kullanılmış bu veri tabanı saldırıya uğradığında damga kırılacağı için orijinal damga ile karşılaştırılması yapılarak veri tabanına yapılan saldırı yapılıp yapılmadığı anlaşılmıştır [39].

3.2.7. Yarı Kırılgan Damgalama

Yarı kırılgan damgalama algoritması kırılgan ve dayanaklı damgalamaya göre zordur. Yarı kırılgan damgalamada dayanıklı damgalama gibi saldırılara karşı dayanıklı yasal olmayan durumlarda kırılgan olması istenir [33].

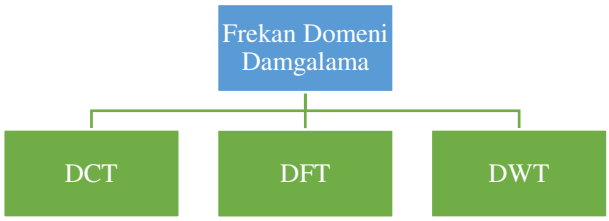
3.2.8. Görülmez Damgalama

Bu damgalamada taşıyıcı içerisine damga görülmez olarak eklenmiştir. Taşıyıcıyı bozmayacak şekilde damga eklenir [33].

3.2.9. Görülebilir Damgalama

Bu damgalama türünde görüntü üzerinde damga görünür halde bulunmasıdır. Buna örnek olarak TV kanallarında TV simgesinin görünür olarak verilmesidir [33].

3.3. Sayısal Damgalamada Kullanılan Yöntemler



Şekil 3.9. Sayısal damgalama yöntemleri

Görüntü işaretlerinde uzay domeninde tüm özellikleri ortaya çıkmamış olabilir. Tüm özelliklerini ortaya çıkarmak için frekans domenine geçilir. Sayısal damgalamada genellikle frekans domeni olan DWT, DCT, DFT kullanılmaktadır. Şekil 3.9 sayısal damgalama çeşitleri belirtilmiştir [40].

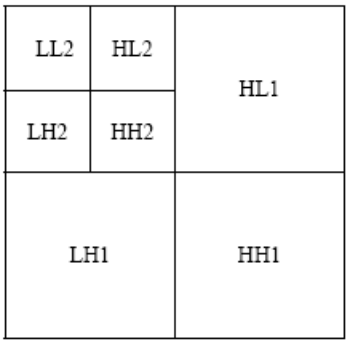
3.3.1. Ayrık Dalgacık Dönüşümü (ADD)

Ayrık dalgacık dönüşümünün iki temel kullanım alanı vardır. Bunlar veri sıkıştırma ve gürültü gidermedir. Dalgacık dönüşümü verilen bir resmi farklı frekans bileşenlerine bölerek, her bileşenin işlenmesine olanak sağlar. Sinyal devamlı yüksek ve alçak frekans olarak ikiye bölünür ve bölünme sonrası işaret LL, HL, LH, HH frekanslarda farklı boyutlarda pencereler elde edilir. Bu sayede düşük frekansların yüksek zaman aralığı, yüksek frekansların düşük zaman aralığı dikkate alınarak işlem yapılır.

Ayrık Dalgacık Dönüşümü;

- Ayrık dalgacık dönüşümü
- Sürekli dalgacık dönüşümü

olarak ikiye ayrılarak incelebilir. Bir resme tek seviyeli ADD uygulandığında HL ile LH bandına damga eklenir. Sağlamlığı artırmak için LL kısmı kullanılır. HH bandı sıkıştırma için uygun değildir fakat HH kırpma ve keskinleştirme gibi durumlarda kullanılabilir. ADD dönüşümde devamlı yüksek ve alçak frekansa bölündüğü için bu yüksek ve alçak frekansların bulunması için filtreler kullanılır ve dönüşüm devamlı düşük frekanstan devam etmektedir. Şekil 3.10' da ise DWT dönüşüm sistemi ilkesi belirtilmiştir [33-41].



Şekil 3.10. Dalgacık dönüşümü [41]

ADD denklemi 3.1 ve 3.3 de verilmiştir. Burada α>0 ve βϵR olmak üzere α parametresi frekansı, β parametresi zamanı, δ dalgacık fonksiyonunu ve DD (α, β) dalgacık dönüşümdür [40].

$$DD(\alpha,\beta) = \frac{1}{\sqrt{\alpha}} \int_{-\infty}^{+\infty} F(t)\delta(\overline{\left(\frac{t-\beta}{\infty}\right)}\, dt \quad (3.1)$$

$$\delta_{\alpha,\beta}(t) = \frac{1}{\sqrt{\alpha}}\delta\left(\frac{t-\beta}{\alpha}\right) \quad (3.2)$$

3.1 ve 3.2 denklemlerin birleşimi ile

$$DD(\alpha,\beta) = \int_{-\infty}^{+\infty} f(t)\overline{\delta_{\alpha,\beta}(t)}dt \quad (3.3)$$

Ters Dalgacık dönüşümü (TDD) ise;

$$C_\delta = \int_{-\infty}^{+\infty} \frac{|\delta_{(\alpha)}|^2}{|\alpha|}\, dw < \infty \quad (3.4)$$

$$TDD(t) = \frac{1}{\delta_\infty}\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty}\frac{1}{\alpha^2}DD(\alpha,\beta)\delta_{\alpha,\beta}(t)d\alpha d\beta \quad (3.5)$$

3.3.2. Ayrık Kosinüs Dönüşümü (AKD)

AKD damgalama dönüşüm boyutunda data gizlenebilir. Denklem (3.6) ve (3.7) ile AKD katsayıları bulunur. (3.6) Formülünün uygulanması ile elde edilecek AKD katsayıları pozitif ve negatif olarak etiketlendirilmiştir [39]

$$F(u,v) = \left(\frac{4}{N.M}\right)^{\frac{1}{2}} \text{w(i)w(j)}*$$

$$\sum_{i=0}^{N-1}\sum_{j=0}^{M-1} cos\left[\frac{\pi.u}{2.N}(2i+1)\right] cos\left[\frac{\pi.v}{2.M}(2j+1)\right].f(i,j) \quad (3.6)$$

(3.6) formülünde N satır, M sütün sayısını, f(i, j) ise matrisin hücre değerini F(u,v) hücre için AKD katsayılarıdır. W(k) ise (3.7) formüle ile değer almaktadır [39].

$$w(k) = \begin{cases} \frac{1}{\sqrt{2}} & k = 0\ durumunda \\ 1 & Diğer\ durumlarda \end{cases} \quad (3.7)$$

Sonuç olarak ilk AKD katsayısı alçak frekans (DC) diğerleri orta ve yüksek frekansı (AC) oluşur. Zig-Zag kodlama ile AKD algoritması oluşturulur. Veri sıkıştırması gerekli durumlarda kullanılan damgalama yöntemidir. Renkli hareketsiz görüntü için kullanılan JPEG sıkıştırma algoritmasını kapsar uygulamaları ve tüm bileşenlerini açıklar.8x8 boyutundaki görüntü parçası bire bir dönüşüm kullanılarak frekans boyutuna taşınır. Bu taşıma sonucu gerekli işlemler yapılarak ayrık kosinüs dönüşümü elde edilmiş olur [33-42].

3.3.3. Ayrık Fourier Dönüşümü (AFD)

Fourier dönüşümünde sinyal farklı durumlarında bulunan sinüs değerlerinin toplamı olarak ifade edilir. Fourier dönüşümü ile frekans domaine geçiş yapılır bu sayede zaman domaininde yapılamayan birçok işlem gerçekleştirilir [40-43].

AFD' nin k=0, 1,…, N-1 olmak üzere N adet ayrık frekans değeri için hesabı denklem 3.8 verilmiştir [40].

$$Xk = \sum_{n=0}^{N-1} X[n] e^{-J2\pi kn/N} \quad (3.8)$$

Ters ayrık fourier dönüşümü ise n=0,1,….,N-1 olmak üzere Denklem 3.9 ile temsil edilir [33,40,44].

$$X[n] = \sum_{k=0}^{N-1} Xk e^{J2\pi kn/N} \quad (3.9)$$

3.4. Damgalamada Kullanılan Hata Oranları

Damgalama uygulamalarında damgalama sonunda ne kadar bir bozulma olduğunun tespiti için belli oranlar mevcuttur. İşaret-Gürültü Oranı (PSNR), Bit Hata Oranı (BER), Normalizasyon Katsayısı (NC) kullanılarak damgalama hata oranları ortaya konulur [40].

3.4.1. İşaret Gürültü Oranı (PSNR-Peak Signal to Noise Ratio)

Orijinal resim ile işlem görmüş resim arasındaki farkı yani gürültü belirtir. Resmin işlem gördükten sonra oluşan kaliteyi belirtir. Desibel olarak belirtir. Aşağıdaki formül ile hesaplanır. MATLAB programında psnr () komutu ile bulunur [40-45].

$$PSNR = 10\text{x}\log_{10}\frac{255^2}{MSE} \tag{3.10}$$

Buradaki MSE; orijinal resim ile damgalanmış resim arasındaki piksel uygunluk oranıdır. MATLAB 'ta immse () ile bulunur [40,45].

$$MSE = \frac{1}{MxN}\sum_{i=0}^{m-1}\sum_{j=0}^{N-1}[I(i,j) - K(i,j)]^2 \tag{3.11}$$

3.4.2. Normalizasyon Katsayısı (NC-Normalization Coefficient)

Orijinal damga ile işlem sonucu elde edilen damga arasındaki uyumu ölçmek için kullanılır. Benzerlik hakkında bilgi vermek için kullanılan katsayı denilebilir [40].

$$NC = \frac{\sum_{i=1}^{N}\sum_{J=1}^{N}[X(i,j)*X\prime(,i,j)]}{\sum_{i=1}^{N}\sum_{j=1}^{N}[X(i,j)]^2} \tag{3.12}$$

3.4.3. Bit Hata Oranı (BER-Bit Error Rate)

Veri haberleşmesinde gönderilen bitlerdeki hata oranını gösterir. Damgalamada ise orijinal resim ile damgalanmış resim arasındaki bit hata oranı olarak tarif edilebilir [40].

$$BER = \frac{HATALI\ BİT\ SAYISI}{TOPLAM\ BİT\ SAYISI} \tag{3.13}$$

3.5. Sayısal Damgalama Uygulamalarına Yapılan Hücumlar

Sayısal damgalamada saldırılara karşı dayanıklılığı için aşağıdaki saldırılara maruz bırakılır. Bu saldırılar damganın yok edilmesi içinde kullanılanlar arasındadır. Aşağıda özellikle kullanılan saldırılara örnektir [46].

- Gürültü Ekleme
- Kırpma
- JPEG kayıplı sıkıştırma
- Tekrar Damgalama

- Geometrik Saldırılar (yatay, dikey eksen ve açılı döndürme)
- Satır ve Sütun silinmesi
- Ölçekleme

3.5.1. Gürültü Ekleme

Damgalı resim pikselinde damga ile ilgili bilgiler vardır. Damgalı resimdeki her piksel resmi bozmayacak şekilde değiştirilir bu sayede damga belli olmayacak seviyeye gelir [46].

3.5.2. Kırpma

Özellikle görünür damgalamada resimde kırpma yapılarak damganın anlaşılamaz hale getirilmeye çalışılır. Gözle görünür damgalamada kırpma ile damgayı çıkarma işlemi çok basittir [40-46].

3.5.3. JPEG kayıplı sıkıştırma

Resim sıkıştırmada JPEG çokça kullanılmaktır. JPEG sıkıştırmada amaç DCT kullanılarak yüksek frekanslı bileşenlerinin sıkıştırılması ile damganın yok edilmesi hedeflenmiştir [46]

3.5.4. Tekrar Damgalama

Damgalanmış görüntüye tekrar bir damgalama yapılarak ilk yapılan damgalamanın yok edilmesi ve yeni bir damganın ortaya çıkmasının sağlanmasıdır [46].

3.5.5. Geometrik Saldırılar

Yatay eksende veya dikey eksende 180º döndürülerek resimde kayıp olmadan elde edildiği saldırılardır. Açılı döndürme ise saat yönünde veya tersi yönünde döndürülerek damganın zarar verilmesi ile sağlanır [46].

3.5.6. Satır ve Sütun Silinmesi

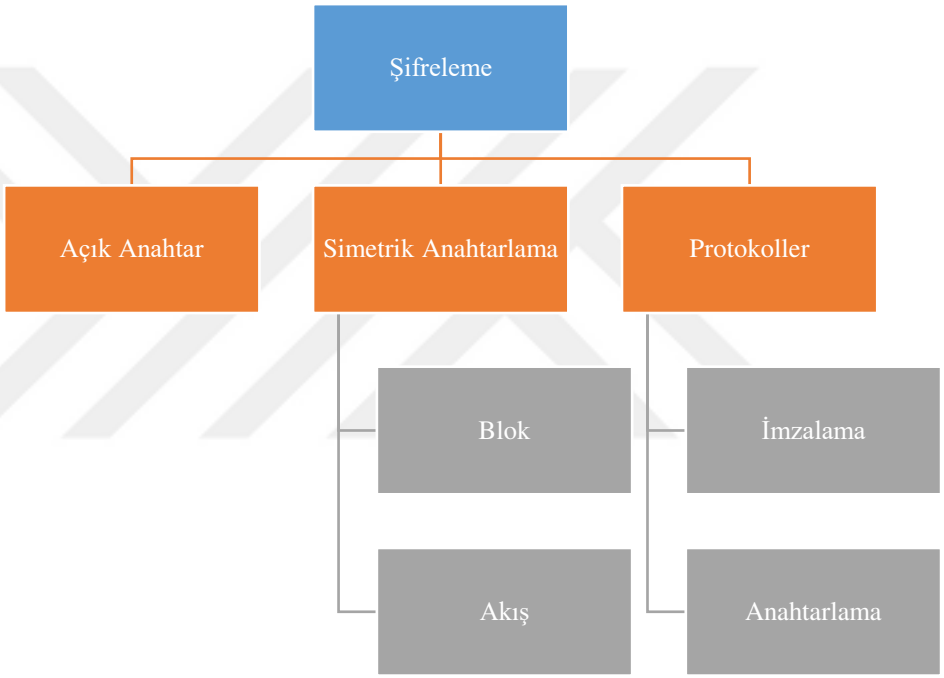
Damgalanmış resmin satır veya sütunları bir önceki ile değiştirilmesi veya silinerek damganın kaybolması sağlanır [40-46].

3.5.7. Ölçekleme

Yüksek çözünürlüklü bir resmin çözünürlüğünün azaltılması ile damganın yok edilmesi sağlanır. Bu işlem için resimler tekrar taranarak veya çözünürlüğü düşünülerek damganın yok edilmesi [46].

4. ŞİFRELEME VE ŞİFRE ÇÖZME YÖNTEMLERİ

Biyometrik sistem güvenliğinde şifreden damga oluşturulmasında şifreleme çeşidine dikkat edilmelidir. Damgalama işleminden önce kriptoloma yapılması için bu bölümde şifreleme incelemesi yapılacaktır. Şifreleme kriptoloji olarak ilgilenilmiş ve geliştirilmeye çalışılmış konudur. Bazı bilgileri sadece alıcı ile göndericinin bilmesi 3. kişilerin bilmemesi istenmiştir. Bu istekten dolayı çok çeşitli şifreleme çeşitleri ortaya çıkmıştır. Şifreleme çeşitleri şekil 4.1 ayrıntılı verilmiştir [47].



Şekil 4.1. Şifreleme bilimi

4.1. Simetrik Anahtarlama

Simetrik anahtarlamada iki tarafın alıcı ve vericinin bildiği anahtar ile yapıldığı şifreleme türüdür. Genel olarak iki aşamada takip edilebilir, blok şifreleme ve akış şifrelemedir [47].

4.1.1. Blok Şifreleme (Block Cipher)

Blok şifrelemede veriler eşit uzunlukta bloklara ayrılır ve bu bloklar eş zamanlı olarak şifrelenir [48].

Blok Şifreleme çeşitleri ise;

Hill Şifreleme (Hill Cipher): Bu şifreleme blok matris şifrelemesidir. İlk olarak anahtar şifre matrisi belirlenir, daha sonra şifrelenecek kelimeler harf sırasına göre numaralandırılır. Gerekli matris çarpımları sonucu 29 sayısından büyükse mod29 ile mod alınarak şifreli metin elde edilir. Şifreli metni çözülmesinde ise anahtar matrisin determinantı alınır daha sonra anahtar matrisin bir derecesinden matrisler yazılır. Yeni oluşan matrislerinde determinantı alınır, kofaktörleri oluşturulur sonra transpozu alınır, gerekli işlemler yapılarak şifre çözme işlemi yapılmış olur [48].

- **Permutasyon Şifrelemesi** (Permutation Cipher): Basit şifreleme metotlarındandır harflerin yerlerinin değiştirilerek blok matris mantığı kullanılarak yapılır [48].
- **DES (Data Encryption Standard, Veri Şifreleme Standarttı)**: Büyük verilerin şifrelemesinde kullanılır. Blok şifreleme mantığı vardır. Her blok 8 bit uzunluğunda olmak suretiyle toplam 64 bittir. Yeni gelişmeler ile 128 bit kadar çıkmaktadır [48]
- **Feistel Şifrelemesi (Feistel Cipher):** Şifreleme ve şifre çözme benzer sayılır tek farkı anahtar sırasıdır [48].
- **Balon balığı şifrelemesi (Blowfish Cipher):** DES şifrelemesi patentli olmasına karşı ücretsiz kullanılması için sunulmuştur. 16 adımdan oluşan feistel ağı kullanılmaktadır [48].
- **Kamelya Şifrelemesi (Camella Cipher):** AES şifrelemesi ile karşılaştırılacak kadar hızlı şifreleme yapabilecek durumdadır. Feistel ağında 128 şifreleme için 18 tur 256 şifreleme için 24 tur kullanmasıdır [48].
- **Playfair Şifrelemesi:** Çok basit bir şifreleme şeklidir. Alfabelerin sıra ile numaralandırılıp matris işlemlerinin yapılması ile elde edilen şifrelemedir [48].
- **RC/4 Şifrelemesi:** Veri güvenliği için kullanılan 64 bitlik feistel ağını 18 geçiş ile şifreleme yapılmıştır [48].

4.1.2. Akış Şifreleme (Stream Cipher)

Simetrik şifreler blok ve akış şifreler olarak ayrılmaktadır [49]. Bu şifrelemedeki yöntem olarak bir akış kullanmaktır. Yani her şifreleme birimindeki işlem bir önceki şifreleme işlemine bağlıdır [50].

4.2. Açık Anahtar Şifreleme (Public Key Cryptography)

Asimetrik şifreleme yöntemi olarak bilinir. 2 adet şifresi bulunur. Bu şifrelerden birisi herkese açık (açık, Public key) diğeri ise gizli (private, gizli) şifredir [51].

Açık anahtarlamalı şifrelemede bir kişiye yollanacak olan mesajın açık şifre ile şifrelenerek yollanması ve ancak alıcı tarafın gizli şifresi ile açılabilmesidir [51].

- Diffie-Hellman
- RSA
- El Gamal

Şeklinde özetlenebilir [51,52].

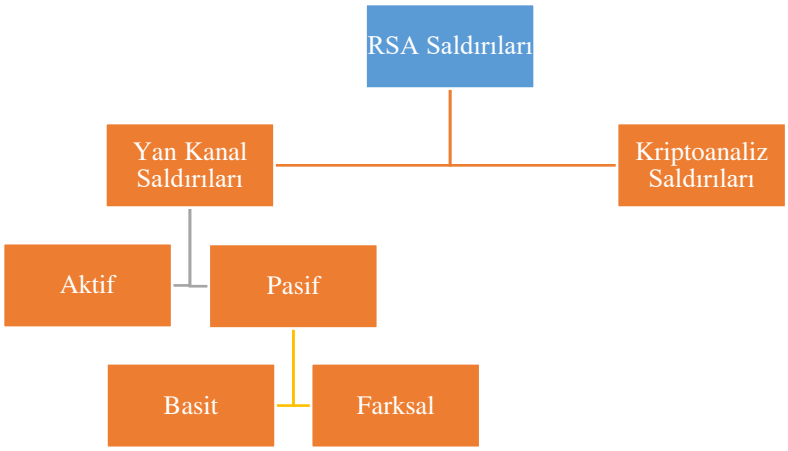
4.3. RSA Şifreleme

Yapılacak uygulamada RSA şifreleme kullanılacağı için ayrıntılı RSA şifreleme açıklanacaktır. Açık anahtarlı şifreleme yöntemi olan RSA, 1977 yılında Ron **R**ives, Adi **S**hamir ve Leonard **A**ldeman tarafından bulunmuştur [53]. Bir Örnek ile açıklanır ise;

- Asal iki sayı seçilir a=61 ve b= 53 seçilsin
- n=a*b=61*53=3233 n**=3233**olarak n sayısı bulunmuş olur
- q=(a-1)*(b-1)=60*52=3120 q**=3120** bulunmuş olur.
- 1<e<q = 1<e<3120 e ile 3120 aralarında asal bir sayı seçilir **e=17** seçilsin.
- d*e=1 mod(n)= 2753*17=1mod3233 olduğundan **d=2753** olur.
- A sayısı ASCII karşılığı m=65 bu sayı RSA olarak şifrelenecek
- ş.m=m^emod(n)=65^{17} mod3233=2790 olarak bulunur
- Şifre çözmek için deşifreli metin d.m=ş. m^d mod(n) =2790^{2753} mod3233
- d.m=65 ASCII sayısı bulunur bu da şifrelenecek olan A sayısıdır.

4.4. RSA Şifreleme Sistemine Yapılan Saldırılar

Gizli verilerin şifrelenmesi için RSA şifrenizi kırmak ve gizli verilere ulaşmak için saldırılar yapılmaktadır. Sisteme zarar verecek kripto analiztin gizli anahtarı bulmasıdır. İki asal sayının çarpımı olan n'nin asal çarpanlara ayrılarak asal sayı olan p ve q' nin hesaplanması ve p, q, e kullanılarak d'nin bulunmasıdır. Şekil 4.2 'de RSA şifrelemeye yapılan saldırılar sınıflandırılmıştır [54].



Şekil 4.2. RSA şifreleme sistemine yapılan saldırılar

RSA şifreleminin kırılması çok zordur. Sebebi büyük asal sayılar kullanıldığı için bunu kırmak için büyük matemetiksel işlemler gereklidir [54].

Bu başlık altında sadece basit ve farksal saldırılardan bahsedilecektir.

Pasif saldırı ile RSA şifreleme sisteminin çalışmasına istemeyerek dışarıya ulaşan bilgiler ile şifreye ulaşıp bilgilere ulaşılması sağlanması hedef alınmıştır [54-56].

Aktif yan kanal saldırı ise pasif yan kanala zor bir işlemdir. Aktif yan kanalda RSA şifrelemeye müdahale vardır [54-56]. Pasif yan dal saldırıları [54-57];

- Zamanlama saldırıları
- Güç analiz saldırıları
- Akustik (ses) saldırıları
- Elektromanyetik analiz saldırıları
- Çarpanlara ayırma saldırıları
- İkinci dereceden kalbur yöntemi
- Küçük e saldırıları
- Kuantum hesaplama gücü ile yapılan saldırılar
- Hata analiz saldırıları

Olarak sıralanabilir [54].

4.4.1. Zamanlama Saldırıları

RSA şifreleme algoritması çalışır iken işlem sürelerine bakılarak şifrenin kırılması hedeflenmiştir. Şifreleme yapan cihazın zamanlama işlemleri dikkat edilerek şifre kırılması esasına dayanır [54-57].

4.4.2. Güç Analiz Saldırıları

Elektromanyetik alan tarafından oluşan akımdan dolayı veriler oluşturularak şifreli metne ulaşılması hedef edinilmiştir [54-57].

4.4.3. Akustik (ses) Saldırıları

RSA şifreleme ve şifre çözme işlemlerinde oluşan sesler dinlenip cihazlar yardımı ile veri elde etme yöntemidir [54-57].

4.4.4. Elektromanyetik Alan Analizi Saldırıları

RSA şifre işleme cihazının çıkardığı elektromanyetik dalgalar analiz edilerek şifrelenen veriye ulaşılması hedeflenmiştir [54-57].

4.4.5. Çarpanlara Ayırma Saldırısı

Çarpanlara ayırma yöntemi ile tek tek deneme yapılarak hesaplama yöntemidir. Herhangi bir n sayısının en küçük asal sayıdan başlanarak bütün asal sayılarının bölünüp bölünemeyeceğinin analiz yapılması ile şifrenin elde edilmesi amaç edinilmiştir [54-57].

4.4.6. İkinci Dereceden Kalbur Yöntemi

Veri güvenliğinde çarpanlara ayırma işleminin zorluğu üzerine dayanan şifre kırma yöntemidir. Asal çarpanlarına ayrılacak n sayısının çarpanlarından en büyük seçilerek gerekli işlemler yapılarak şifre kırma hedef alınmıştır [54-57].

4.4.7. Küçük e Saldırısı

RSA şifrelemenin basamağında kullanılan e sayısının küçük seçildiği durumda şifreli haberleşmeyi dinleyenlerin çinli kalan teoremi ile şifre çözülmesi saldırısıdır [54-57].

4.4.8. Kuantum Hesaplama Gücü ile Yapılan Saldırılar

Kuantum bilgisayarlar ve n sayısının çarpanlarına ayrılıp Sher algoritması kullanılarak şifre kırılması hedeflenmiştir [54-57].

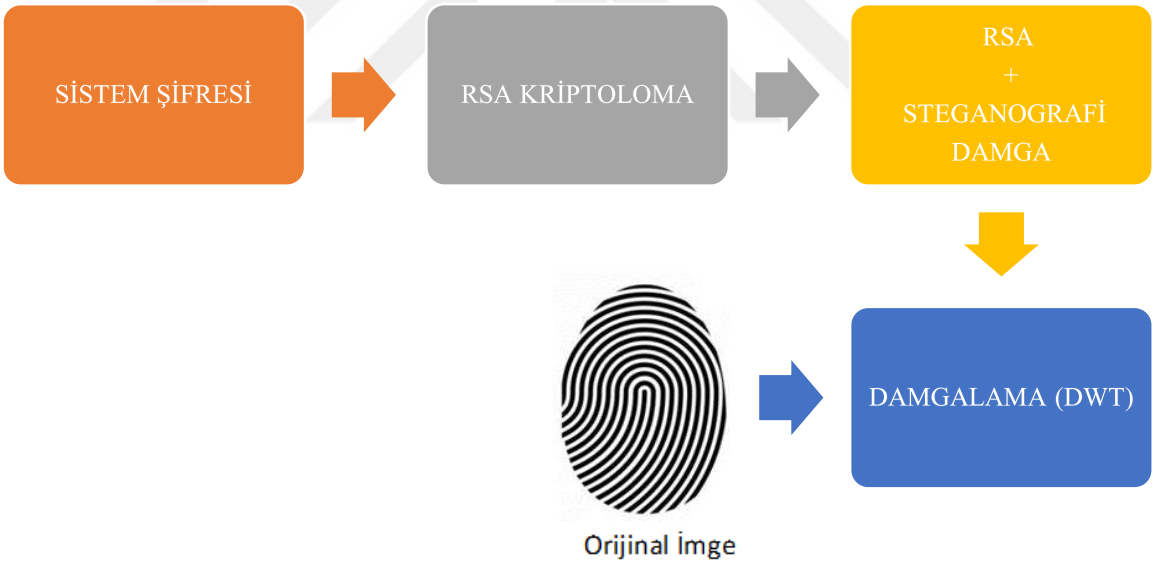
4.4.9. Hata Analiz Saldırıları

RSA algoritmaları çalışır iken sıcaklık, ışık gibi çevreden kaynaklı etkenler değiştirilerek hatalı çalıştırılarak şifreyi kırılması olayıdır [54-57].

5. MATERYAL VE METOT

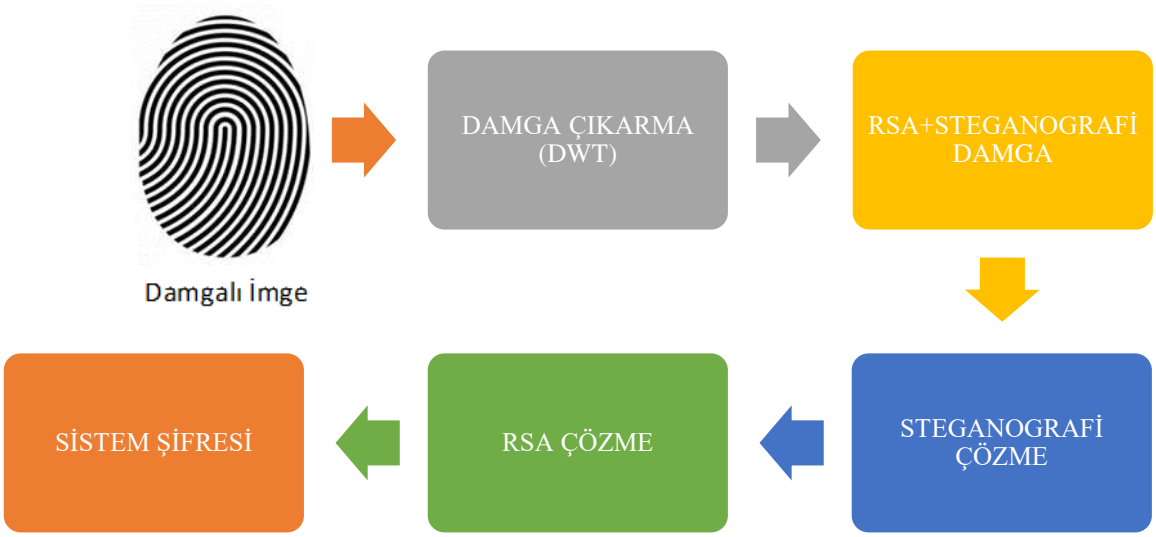
Bu bölümde tezin nasıl yapılacağı hakkında bilgi verilecek ve hangi özelliklerden faydalanacağı hakkında bilgi verilecektir. Biyometrik görüntülerde kimlik denetimi için şifreleme teknikleri kullanarak damgalama işlemi blok diyagramı şekil 5.1 ve şekil 5.2' de gösterilmiştir.

Kimliklendirme; herhangi bir sistemde veya bina girişlerde kişileri belli etmek için kişiye özel benzersiz ve sadece kişiyi temsil edecek bilgilere ihtiyaç vardır bu bilgiler T.C kimlik numarası gibi kişiyi tanıtan bilgiler olmalıdır. Yapılan çalışmada kişiyi tam olarak temsil etmesi için herkeste tek belirgin olan parmak izi verisi ile kişiye özel şifre ile kimliklendirme yapılmıştır. Parmak izi verisi ile birlikte kullanılan şifrenin kimliklendirme işleminde güvenliği sağlamak için RSA kriptolama ile sistem şifresi kriptolanmıştır, kriptolama gizliliği için LSB steganografi yapılarak damga oluşturulmuş; DWT ile damgalama yapılmıştır. Şekil 5.1' de kimliklendirme de kullanılan sistem şifresi ve parmak izi verisinin güvenliği ve kimliklendirme aşamaları gösterilmiştir.



Şekil 5.1. Veri gizleme (imge kimliklendirme)

Kimlik Doğrulama; sistemde kayıtlı kişi bilgileri ile sisteme giriş yapacak kişinin bilgileri alınarak; kayıtlı bilgi ile elde edilen bilgiler karşılaştırılarak uygunluk arama işlemi kimlik doğrulama olarak ifade edilir. Kimlik doğrulama işleminde sistemde kayıtlı olan şifre ile damgalı parmak izi verisi ile kişinin girdiği şifre ve parmak izi verisi karşılaştırılarak kimlik doğrulaması tamamlanmış olacaktır. Kimlik doğrulaması güvenlik aşaması şekil 5.2 gösterilmiştir.



Şekil 5.2. Veri çıkarma (imge doğrulama)

5.1. Biyometrik Veri

Biyometrik veri olarak parmak izi verileri kullanılacaktır. Şekil olarak şekil 5.3'deki gibi parmak izi verisi kullanılacaktır. Parmak izi verisi ayırt edici bir özelliktir. Parmak izi parmakta yara veya yanma gibi durumlar olmadıkça bozulmayan biyometrik veridir. Parmak izi verileri veri tabanına kayıt edildikten sonra parmak izi verisi alınarak veri tabanı ile karşılaştırılarak kimlik tespiti yapılır. Kimlendirme ve kimlik doğrulama işlemlerinde parmak izi verisi kullanılması sebebi kullanılma sıklığı ve parmak izi cihazlarının pazarında satın alınma çokluğu nedeni ile seçilmiştir. Uluslararası biyometrik grubun biyometrik veri talep analiz grafikleri incelendiğinde parmak izi, yüz tanıma, el geometrisi, iris tanıma, ses tanıma, DNA tarama, imza olarak sıralanmaktır. Parmak izi verisi cihazı talebi üst sırada yer almaktadır. Parmak verisi tanıma cihazlarına talep yaklaşık olarak %25 ile %30 arasında olmaktadır. Parmak izi verisi ile kimliklendirme yaygın olarak kullanıldığı için tez konumuzda biyometrik veri olarak parmak izi kullanılmıştır [13].

Şekil 5.3. Örnek parmak izi verisi [58]

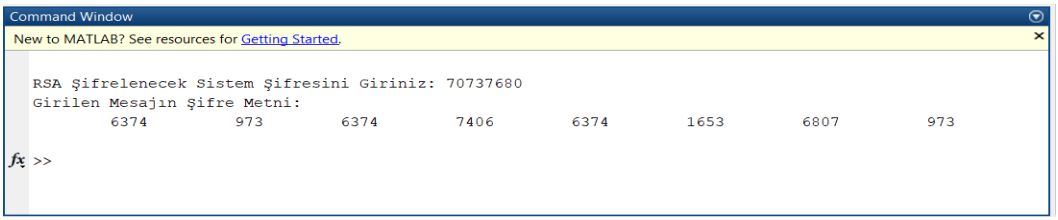
5.2. RSA Şifreleme

Tez konumuzda RSA kriptoloma kullanılmasının sebebi diğer şifreleme sistemleri araştırılmış uzun olmayan verileri kriptolomak için RSA uygun olduğu ortaya çıkmıştır. Şifrelemenin asal sayılarla yapılan genel ve özel şifrenin kırılması zor olmasıdır. RSA kriptolamada özel şifreden genel şifre elde edilebilir genel şifreden özel şifre elde edilmesi çok zordur. Bu sebepten dolayı şifrenin kırılması için mutlaka özel şifrenin ele geçirilmesi gerekir. Bu durumdan dolayı özel şifre bilgisi olan kişilerin bu şifreyi saklaması çok önemlidir. Günümüzün bile en gelişmiş bilgisayarları bile RSA şifresini kırmakta zorlanmaktadır.

Tez konusu çalışmamızda RSA şifrelemesinde ilk olarak p ve q gibi asal sayı belirlenir. MATLAB ile yapılan programımızda örnek sistem şifremiz 70737680' dir. RSA şifreleme sonucunda 7 için 6374, 0 için 973, ..gibi RSA kodları elde edilmiş ve RSA anahtarları ile birlikte txt dosyasına kaydı yapılır. Şekil 5.4 şifreleme çıkış ekranında 70737680 şifre ASCII koduna çevrildikten sonra RSA kodlanmış hali gösterilmiştir.

RSA Algoritması pseudo kodu (Şifreleme)

- Başla
- p ve q değeri gir
- n=p*q
- f(n)=(p-1)*(q-1)
- e değerini bul
- d değerini bul
- Şifrelenecek metni gir
- Metin uzunluğunu bul
- Girilen her karakteri şifrele
- Şifrelenmiş metni *.txt dosyasına kopyala



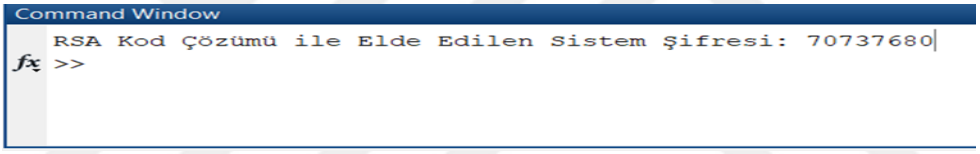
Şekil 5.4. Şifreleme çıkış ekranı

Şifrelenmiş txt dosyası kullanılarak RSA şifre çözme işlemi ile sistem şifresi tekrar elde edilir. RSA kripto çözme işlemimizde özel şifremiz sayesinde kriptolanmış bilgileri ASCII koduna

çevirme işlemi yapılmıştır. ASCII koduna çevrilen veriler ASCII karakter çevirimi ile sistemde kullanılan şifre verisi elde edilmiştir. Şekil 5.5'de RSA kod çözme ekranı gösterilmiştir. RSA kod çözme işlemi için pseudo kodu ile işlemin yapılış biçimi görülmektedir.

RSA Algoritması pseudo kodu (Şifre Çözme

- Başla
- Şifrelenmiş txt dosyasını oku
- p ve q sayısını oku
- n=p*q
- f(n)=(p-1)*(q-1)
- e değerini bul
- d değerini bul
- Her bir karakterin şifresini çöz
- Şifresi çözülmüş mesajı ekrana yaz.
- Şifresi çözülmüş metini txt olarak sakla



Şekil 5.5. Şifresi çözülmüş metin

5.3. Steganografi

Steganografi gizli mesajların resme gizlenmesi olarak ifade edilebilir. Yapılan çalışmada RSA şifreleme ile şifrelenmiş olan sistem şifresini örtü resmine gizleme yapılmıştır.

Steganografi yöntemlerinden LSB kullanılarak RSA kodlaması gizlenmiştir. LSB yönteminde, resim pixel olarak ifade edilir. Bu her bir pixelin en değersiz bitlerine gizlenecek olan veriler eklenerek elde edilir. İyi yapılmış bir steganografi ile verileri algılamak zor olmaktadır. Steganografi kullanılmasında genel kanı şudur hibrit bir çalışmada bilginin saklandığı resme bakan kişi sadece resmi göreceği için gizli bilgiler görmediğinden sistem koruması sağlanacaktır. Sadece resim görüldüğü için şifre kırılması ile uğraşılmayacaktır.

LSB Steganografi pseudo kodu

- Başla
- Örtü resmini gir
- RSA şifreli txt dosyasını gir
- Örtü resmi pixellerine ayır
- Örtü resmi pixellerinin LSB bitlerine karakter bitlerini gir

- Gizlenmiş örtü resmini sakla

RSA algoritması ile kriptolanmış olan bilgiler steganografi ile örtü resmine gizleme yapıldıktan sonra tekrar olarak örtü resme gizlenmiş olan gizli bilgiler ters Steganografi bilgileri kullanılarak tekrar elde edilebilir.

LSB Steganografi ile gizli metni çıkarma pseudo kodu

- Başla
- Gizli metni olan örtü resmini gir
- Örtü resmini pixellerine ayır
- Her pixellin LSB bitini oku
- Okunan LSB bitlerini birleştir
- Birleşmiş metni txt dosyası olarak sakla

5.4. Ayrık Dalgacık Dönüşümü ile Parmak İzi Damgalama

Ayrık dalgacık dönüşümü iki temel kullanım alanı vardır bunlar veri sıkıştırma ve gürültü gidermedir. Dalgacık dönüşümü, verilen bir resmi farklı frekans bileşenlerine bölerek her bileşenin işlenmesine olanak sağlar. Sinyal devamlı yüksek ve alçak frekans olarak ikiye bölünerek elde edilir. Çalışma konumuzda DWT kullanılması sebebi sağlamlığıdır. DWT damgalamanın sağlamlığı frekans domeninde işlem yapılması ve resim içerisindeki damganın çok iyi gizlenmesidir. Parmak izi verisine RSA şifre damgası birleştirilerek hibrit RSA, LSB, DWT koruması sağlanmıştır [33-40].

DWT Damgalama pseudo kodu

- Basla
- Biyometrik veri resmini gir
- Damga resmini gir
- Biyometrik veriye damga resmini yerleştir. (dwt2)
- Damgalanmış resmi sakla

DWT Damgalama bulma pseudo kodu

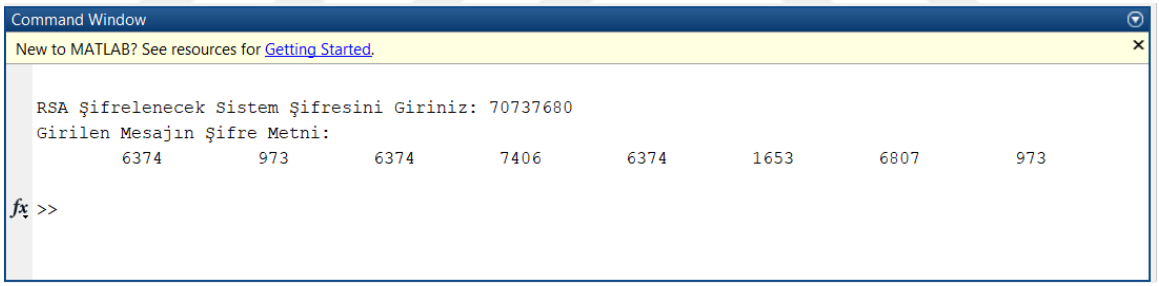
- Başla
- Biyometrik veri resmini gir
- Damgalı resmi gir
- Damgalı resimden idwt2 ile damga elde et.
- Damgayı sakla

6. BULGULAR VE TARTIŞMA

Yapılan çalışma ile ilgili yöntem ve araştırma biçimi beşinci bölümde incelenmiştir. Beşinci bölümde açıklanan bilgiler ile araştırma uygulamamız yapılmıştır. Biyometrik görüntülerde kimlik denetimi için şifreleme teknikleri kullanarak damgalama çalışmasında; DWT, RSA, LSB steganografi uygulamaları kullanılmış, elde edilen sonuçlar ekran çıktısı olarak verilerek biyometrik görüntülerde kimlik denetimi için şifreleme teknikleri RSA ve LSB steganografi verileri damga olarak elde edilip DWT ile damgalanarak kimlik denetimi ve doğrulaması güvenli olarak yapıldığı ortaya konulacaktır.

6.1. Sistem Şifresinin RSA Algoritması ile Kriptolaması

Biyometrik sistemlerde biyometrik veriler parmak izi, retina, yüz tanıma gibi sistemler kimlik tanıma için kullanılır. Güvenliği artırmak için kimlik tanıma işleminde biyometrik verinin yanında sistem şifresi ile güvenlik artırılması sağlanır. Kullanılacak şifrenin istenmeyen kişilerin eline geçmemesi için RSA algoritması ile kriptolama yapılır. Yapılan çalışmada sistem şifresinin RSA ile kodlanmış halinin ekran görüntüsü Şekil 6.1'de görülmektedir.

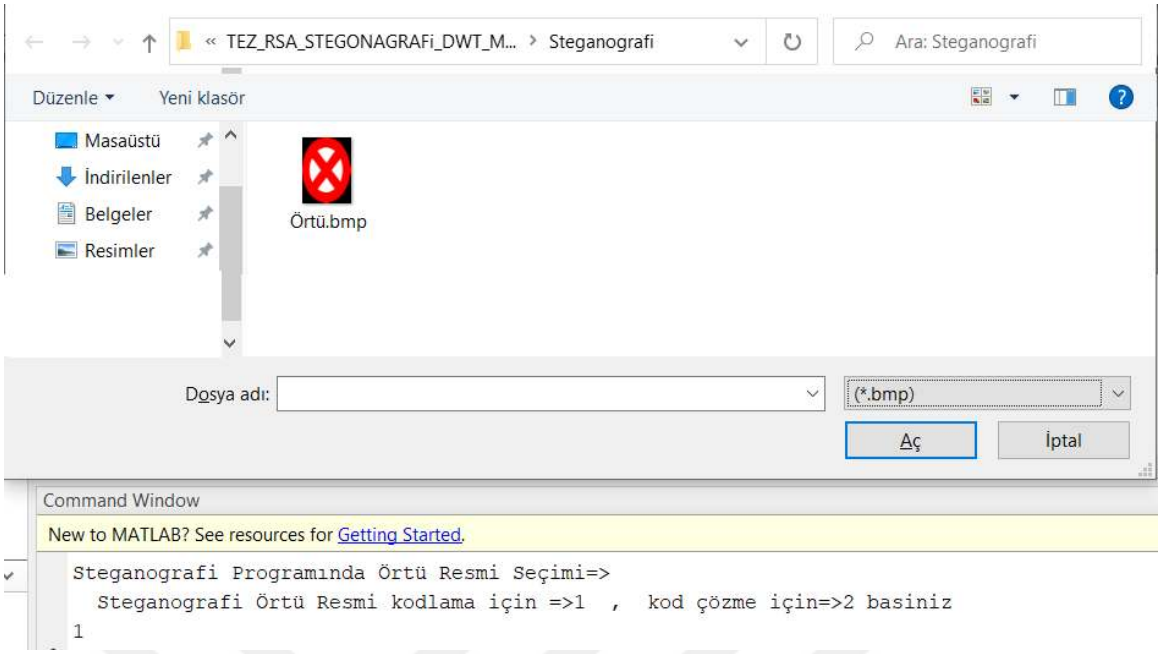


Şekil 6.1. MATLAB RSA şifreleme görüntüsü

MATLAB ile yazılmış olan RSA programımız sistem şifresini, n, e, d, p, q gibi RSA bilgilerini not defterine (txt dosyası) yazarak şifreli bilgiler dosyası oluşturulur. Bu not defteri dosyası şifre çözülür iken gerekli bilgileri taşır.

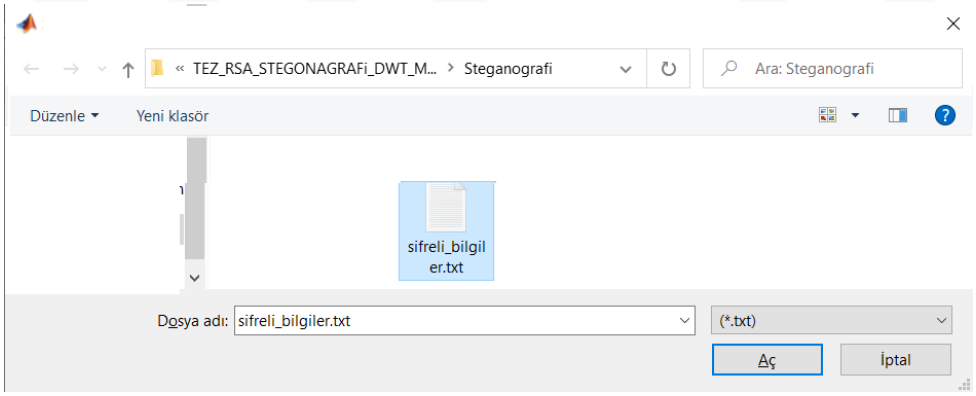
6.2. RSA Şifrelemesinin Steganografi ile Gizlenmesi

RSA bilgileri not defteri dosyasına kayıt edildikten sonra ek bir kodlama ile örtü resmi içerine saklama işlemi yapılır. Bu işlemin yapılış ekran görüntüleri ise şekil 6.2' de örtü resmi şekil 6.3' de ise seçimi yapılıp LSB steganografi işlemine tabi tutulur.



Şekil 6.2. Steganografi örtü resmi seçimi

RSA ile txt olarak şifrelenmiş veriler LSB yöntemi kullanılarak LSB steganografi ile örtü resminin her bir pixelinin en düşük değerli bitlerine yerleştirme işlemi yapılır.



Şekil 6.3. Steganografi gizlenecek txt dosyası seçimi

Şekil 6.3 ise RSA ile gizlenecek olan not defteri şeklinde txt dosyası görülmektedir. Txt dosyasında şifrelenmiş veriler ile birlikte p ve q asal sayıları e, d, n gibi RSA şifreleme bilgileri olan özel anahtar bilgileri bulunmaktadır. Gizlenecek veri ve RSA özel şifre bilgileri örtü resmine gizlenmesi için şifreli olarak txt dosyasında bulunmaktadır. Şekil 6.4' de ise LSB Steganografi işleminin yapılmış hali görülmektedir.

Şekil 6.4. RSA bilgilerinin örtü resmine gizlenmesi

Şekil 6.4 ile örtü resmine şifreli bilgilerin bulunduğu txt dosyasının LSB steganografi birleştirilerek gizlenmiş yeni örtü resminin elde edilmiş hali görülmektedir. Sonuçta DWT damgalama için gerekli olan damga elde edilmiştir.

6.3. RSA ve Steganografi ile Gizlenmiş Bilgilerin DWT ile Damgalanması

RSA ve LSB steganografi ile örtü resmine gizlenmiş olan sistem şifresini damga olarak kullanarak DWT kullanarak biyometrik veri olan parmak izine damgalanmasıdır. Şekil 6.5 ile damgalama işleminin bitmiş hali görülmektedir.

Şekil 6.5. DWT ile biyometrik parmak izi verisi damgalanması

Biyometrik parmak izi verimiz RSA ile kodlanmış steganografi ile örtü resmine saklanmış olan damgamız elde edilmiş. Bu elde edilen damga DWT ile parmak izi verimize gizlenmiş olmaktadır. Şekil 6.5 ‘de DWT damgalama işleminin son hali görülmektedir.

Damgalanmış olan biyometrik parmak izi verimizden sıra ile damganın elde edilmesi, elde edilen damga dan steganografi RSA şifreli sistem not defteri çıkarılarak daha sonra RSA kod çözme ile sistem şifresini edilmesi yapılacaktır.

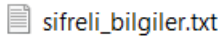
6.4. DWT ile Damgalanmış Biyometrik Veriden Damga Çıkarma

Damgalanmış biyometrik veriden DWT kullanılarak tekrar damga elde edilmiştir. DWT ile damga çıkarma işlemi sonucu elde edilen damga şekil 6.6 gösterilmiştir.

Şekil 6.6. DWT ile damga çıkarma

6.5. Steganografi ile Damgadan Sistem Dosyası Elde Edilmesi

Steganografi ile damga olarak kullanılacak örtü resmine sistem dosyası gizlenmiştir. Steganografi kullanılarak damgadan sistem dosyasının çıkarılması yapılacaktır. Programı çalıştırdığımızda şekil 6.7'deki metin dosyası olan txt dosyası elde edilir.

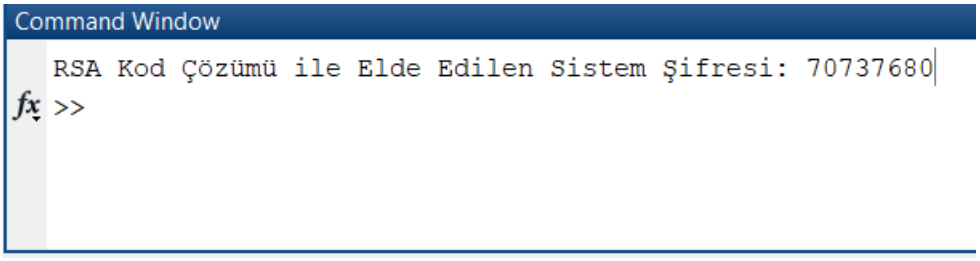


Şekil 6.7. Steganografi ile damgadan elde edilen txt dosyası

Steganografi kullanılarak damga örtü resmi içerisine gizlenmiş olan txt dosyasının elde edilmiş dosya şekil 6.7 'de gösterilmiştir.

6.6. RSA Kod Çözme ile Sistem Şifresinin Elde Edilmesi

Steganografi ile damgalı örtü resminden txt dosyası elde edildikten sonra RSA kod çözme ile sistem şifresini elde edilir. Şekil 6.8 RSA kod çözme sonucu ilk verilen sistem şifresine ulaşılmış olur.



Şekil 6.8. RSA kod çözme elde edilen sistem şifresi

6.7. Biyometrik Veri ve Damganın Gürültülere Karşı Dayanıklılığı

Testlerimizde kullanılacak gürültü çeşitleri gauss(gaussian), tuz &biber (salt & pepper), yerel değişken (localvar), benek(speckle), atış (poisson), hareket izi (motion blur), aşındırma(erosion), genişletme(dilation) 8 ayrı gürültü çeşidine biyometrik veri ve damgayı maruz bırakıp dayanaklılığı test edilecektir. Yapılacak testler ise PSNR, MSE, RMSE, Evrensel Görüntü Kalitesi İndeksi (UIQI), EME (Orijinal Resim), EME (Gürültülü Resim), Pearson Korelasyon Katsayısı (orijinal ve gürültülü resim), Pearson Korelasyon Katsayısı (orijinal resimler arası), SNR, MAE testlerine sonuçlarına yer verilecektir. Tablo 6.1' de ise parmak izi, damgalı parmak izi, damgaya yapılan testler için PSNR, MSE testleri karşılaştırılmalı verilmiştir [59].

Tablo 6.1. Biyometrik verilerin gürültü testleri

Noise	Gauss		Tuz &Biber		Yerel Değişken		Benek		Atış		Hareket İzi		Aşındırma		Genişletme	
Test Verileri	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE
Parmak İzi	14	2339	17	1127	15	1812	17	1070	27	124	-	4483	15	1980	15	1980
Damgalı Parmak İzi	14	2319	17	1170	15	1816	17	1086	27	128	-	4470	15	1965	15	1965
Damga	14	2322	17	1186	15	1784	21	460	29	70	-	685	25	165	25	165

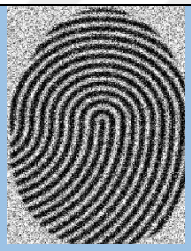
Orijinal biyometrik veri olan parmak izi verisi, damgalı parmak izi verisi ve damga resmine sırası ile gauss, tuz&biber, yerel değişken, benek, atış, hareket izi, aşındırma, genişletme gürültüleri

uygulanmış her bir gürültü sonucunda kalite ölçümü için PSNR, MSE genel bir değerlendirme tablo 6-1 verilmiştir. Tablomuz incelendiğinde veri değerlerimiz çok iyi olduğu yapılan şifreleme ve DWT işleminin gürültü ile etkilenmesinin çok az olduğu ortaya çıkmıştır. Buna örnek olarak parmak izi verimiz ile damgalı parmak izi verimizin PSNR değerleri 14-17 arasında birbirine çok yakındır bunun sebebi DWT damgalamanın uygunluğu göstermektedir.

6.7.1. Orijinal Parmak İzi Verisinin Gürültülere Karşı Dayanıklılığı

RSA şifreleme, Steganografi, DWT damgalama gibi hiçbir işleme tabi tutulmayan giriş biyometrik verisi olan orijinal parmak izi verisine 8 adet gürültü gauss(gaussian), tuz & biber (salt & pepper), yerel değişken (localvar), benek(speckle), atış (poisson), hareket izi (motion blur), aşındırma(erosion), genişletme(dilation) sıra ile uygulanarak değişim kalite faktörleri test edilecektir. Tablo 6.2'de ve Tablo 6.3 'de orijinal parmak izi verisine uygulanan gürültüler ve test sonuçları verilmiştir

Tablo 6.2. Orijinal parmak izi gürültü testi-1

 Orijinal Resim	 Gauss	 Tuz Biber	 Yerel Değişken	 Benek
PSNR	+14,474dB	+17.64411 dB	+15.58314 dB	+17.86693 dB
MSE	2339,156	1127.377	1812.03282	1070.99297
RMSE	48,364	33.576	42.56798	32.72603
UIQI	0,63150	0.713	0.66125	0.71816
EME- Orijinal	0,71784	0.717	0.71784	0.71784
EME- Gürültülü	6,939	0.354	6.29134	3.96842
Pearson Korelasyon Katsayısı (Gürültülü)	45380,231	49766.956	47238.93518	50204.85088
Pearson Korelasyon Katsayısı (Orijinal)	53928	53928	53928	53928
SNR	-10,684dB	-7.514 dB	-9.57580 dB	-7.29201 dB
MAE	37,155	6.180	30.47310	23.64246

Tablo 6.3. Orijinal parmak izi gürültü testi-2

 Orijinal Resim	 Atış	 Hareket İzi	 Aşınma	 Genişletme
PSNR	+27.20529 dB	-	+15.19786 dB	+15.19786 dB
MSE	124.72423	4483.35397	1980.13184	1980.13184
RMSE	11.16800	66.95785	44.49867	44.49867
UIQI	0.77684	0.13078	0.71516	0.71516
EME- Orijinal	0.71784	0.71784	0.71784	0.71784
EME- Gürültülü	2.14381	12.03906	0.89514	0.89514
Pearson Korelasyon Katsayısı (Gürültülü)	53456.61249	32537.96936	48167.72506	48167.72506
Pearson Korelasyon Katsayısı (Orijinal)	53928	53928	53928	53928
SNR	2.04635 dB	-13.51017 dB	-9.96108 dB	-9.96108 dB
MAE	7.76133	53.01230	19.93844	19.93844

Orijinal parmak izi verisini test etmek için kullanılan beyaz gauss gürültüsü olarak testi yapılmıştır. Sigma değeri 0.005, IQI0.63374 (**I**mage **Q**uality **I**ndex, Resim Kalite İndeksi) alınarak gürültü uygulanmıştır. Gürültü sonrası kalite ölçüm değerlerine bakıldığında PSNR değeri 14,474, MSE değeri 2339,156 çıkmıştır, parmak izi verimizde çok bozulma olmamıştır.

Parmak izi verisine tuz&biber gürültüsü uygulanmıştır. Sigma değeri 0,05 IQI değeri 0,71327 olarak gürültü uygulanmıştır. Tuz&biber gürültü uygulamasında parmak izi verimize siyah ve beyaz noktalar eklendiği için tuz ve biber gürültüsü oluşmuştur. PSNR 17,644, MSE 1127,377 ve diğer test sonuçlarına bakıldığında tuz&biber gürültü testi değerlenmesi yeterli seviyededir.

Yerel değişken gürültüsü parmak izi verisine beyaz gauss gürültüsüne değişken olarak I sıfır ortalamalı, yerel değişken V eklenmesi ile bulunur. V,I aynı boyutta dizi oluşturur. Gürültü sonrası değerlere bakıldığında PSNR 15,583 MSE 1812,032 değerleri oluşmuştur.

Benek gürültüsü ile parmak izi verisine koyu ve parmak izler konularak gürültü oluşturulmuştur. Gürültü oluşturulurken sigma 0,05 IQI 0,71816 olarak alınarak gürültü oluşturulmuştur. Gürültü sonrası kalite testinde PSNR 17,866 MSE değeri 1070 olarak elde edilmiştir.

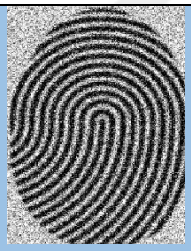
Atış gürültüsü diğer adıyla foton gürültüsü resim elde edilirken ışık yet1erli olmadığında ortaya çıkan gürültü çeşididir. Poisson denklemi kullanıldığı için poisson gürültüsü olarak ta ifade

edilir. Tablolar incelendiğinde diğer gürültü çeşitlerine göre en yüksek değerler elde edilmiştir. PSNR 27,205 MSE 12,724 olarak ortaya çıkmış kalite testi üst seviyede olmuştur

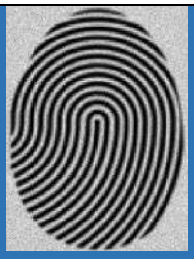
6.7.2. Damgalı Parmak İzi Verisinin Gürültülere Karşı Dayanıklılığı

Damgalı parmak izi veri değerleri gürültülere karşı dayanıklılık durumuna bakıldığında RSA şifreleme, steganografi, DWT damgalama ile işlem görmüş damganın eklenmesi ortaya çıkan yeni görüntü olmasına karşın işlem görmemiş parmak izi verisi ile yakın değerler elde edilmiştir. Gauss, tuz & biber, yerel değişken, benek, atış, hareket izi, aşınma, genişletme gürültülerine karşı ideal PSNR değerleri elde edildiği tablo 6.4 ve tablo 6.5 görülmektedir.

Tablo 6.4. Damgalı parmak izi verisinin gürültülere karşı dayanıklılığı-1

 Orijinal Resim	 Gauss	 Tuz Biber	 Yerel Değişken	 Benek
PSNR	+14.51076 dB	+17.48165 dB	+15.57292 dB	+17.80295 dB
MSE	2319.54976	1170.34860	1816.29976	1086.88847
RMSE	48.16170	34.21036	42.61807	32.96799
UIQI	0.63264	0.70623	0.65942	0.71334
EME- Orijinal	64.32425	64.32425	64.32425	64.32425
EME- Gürültülü	7.94162	13.44215	7.53469	78.97617
Pearson Korelasyon Katsayısı (Gürültülü)	45766.95767	49950.30574	47535.27087	50518.95658
Pearson Korelasyon Katsayısı (Orijinal)	54399	54399	54399	54399
SNR	-10.40114 dB	-7.43026 dB	-9.33898 dB	-7.10896 dB
MAE	37.33053	6.42544	30.92807	24.08145

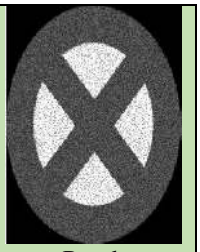
Tablo 6.5. Damgalı parmak izi verisinin gürültülere karşı dayanıklılığı-2

 Orijinal Resim	 Atış	 Hareket İzi	 Aşınma	 Genişletme
PSNR	+27.07054 dB	-	+15.23024 dB	+15.23024 dB
MSE	128.65480	4470.62799	1965.42090	1965.42090
RMSE	11.34261	66.86275	44.33307	44.33307
UIQI	0.77454	0.12267	0.71941	0.71941
EME- Orijinal	64.32425	64.32425	64.32425	64.32425
EME- Gürültülü	32.82793	10.67592	65.32962	65.32962
Pearson Korelasyon Katsayısı (Gürültülü)	53897.30703	32231.26206	48486.37547	48486.37547
Pearson Korelasyon Katsayısı (Orijinal)	54399	54399	54399	54399
SNR	2.15863 dB	-13.25079 dB	-9.68166 dB	-9.68166 dB
MAE	8.11097	53.00794	19.80660	19.80660

6.7.3. Damganın Gürültülere Karşı Dayanıklılığı

Tablo 6.6 ve Tablo 6.7' de DWT damgalama işlemi öncesi kullanılan damganın gürültülere karşı dayanıklılığı ölçülerek sonuçlar gösterilmiştir. İncelemesi yapılan damgaya gauss, tuz & biber, yerel değişken, benek, atış, hareket izi, aşınma, genişletme gürültüleri uygulanmış kalite değerlenmesi ise PSNR, MSE, RMSE, UIQI, EME, pearson korelasyon katsayısı, SNR, MAE test uygulanmış test sonuçlarına bozulmalardan az etkilendiği ortaya çıkmıştır. Test uygulamalarında literatürde kullanılan oranlar dikkate alınmış örnek uygulamalar üzerinde gürültü ve kalite oranları incelenmiştir [59].

Tablo 6.6. Damganın gürültülere karşı dayanıklığı-1

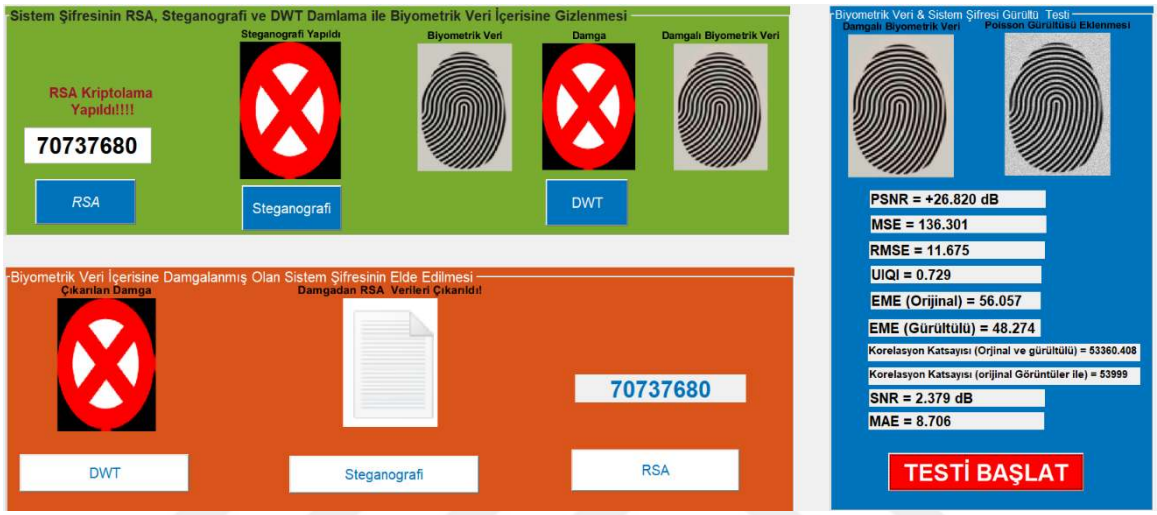
 Orijinal Resim	 Gauss	 Tuz Biber	 Yerel Değişken	 Benek
PSNR	+14.50507 dB	+17.42250 dB	+15.65004 dB	+17.80295 dB
MSE	2322.59066	1186.39726	1784.33204	1086.88847
RMSE	48.19326	34.44412	42.24135	32.96799
UIQI	0.12480	0.25256	0.13670	0.71334
EME- Orijinal	4.92960	4.92960	4.92960	64.32425
EME- Gürültülü	3.23289	3.05165	5.84030	78.97617
Pearson Korelasyon Katsayısı (Gürültülü)	44836.58023	49700.86019	46960.75255	50518.95658
Pearson Korelasyon Katsayısı (Orijinal)	54399	54399	54399	54399
SNR	-10.69034 dB	-7.77292 dB	-9.54537 dB	-7.10896 dB
MAE	35.17710	6.30682	28.65175	24.08145

Tablo 6.7. Damganın gürültülere karşı dayanıklığı-2

 Orijinal Resim	 Atış	 Hareket İzi	 Aşınma	 Genişletme
PSNR	+29.65835 dB	-	+25.98548 dB	+25.98548 dB
MSE	70.89982	685.97739	165.17029	165.17029
RMSE	8.42020	26.19117	12.85186	12.85186
UIQI	0.39344	0.41131	0.89078	0.89078
EME- Orijinal	4.92960	4.92960	4.92960	4.92960
EME- Gürültülü	11.55338	8.18531	4.95176	4.95176
Pearson Korelasyon Katsayısı (Gürültülü)	54113.02861	51557.94653	53729.27729	53729.27729
Pearson Korelasyon Katsayısı (Orijinal)	54399	54399	54399	54399
SNR	4.46293 dB	-5.39372 dB	0.79006 dB	0.79006 dB
MAE	5.46213	14.23197	2.40404	2.40404

6.8. Biyometrik Görüntülerde Kimlik Denetimi için Şifreleme Teknikleri Kullanılarak Damgalama Tez Konusu Program Çıktısı

Şekil 6.9' da tez konusu olan biyometrik görüntülerde kimlik denetimi için şifreleme teknikleri kullanılarak damgalama işlemi için kullanılan MATLAB programlarının MATLAB guide birleştirilmiş hali görülmektedir. Şekildeki her bir uygulama test edilmiş test işlemlerinden sonra grafik ara yüz programında birleştirilmiştir.



Şekil 6.9. Tezde kullanılan programların MATLAB guide birleştirilmiş hali

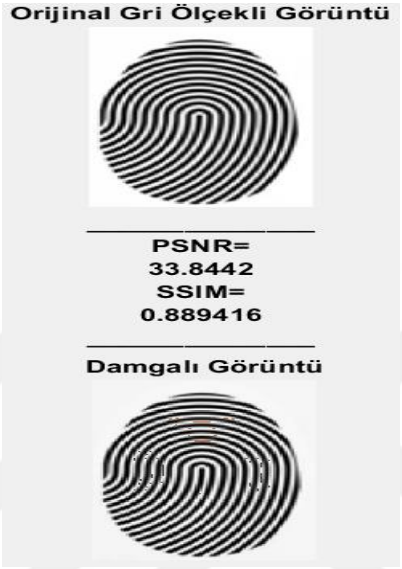
Yapılan uygulamalar literatürde ve MATLAB kütüphanelerinde bulunan programlarla test edilmiş aynı bulgular elde edilmiştir [59,60,61,62]

6.9. Biyometrik Görüntülerde Kimlik Denetimi için Şifreleme Teknikleri Kullanılarak Damgalama Tez Konusu Kalite Testi

Parmak izi verisine uygulanan RSA, LSB steganografi, DWT damgalama sonucunda elde edilen biyometrik veri ile ilk aşamada kullanılan parmak izi verisinde oluşabilecek kayıpları ve orijinal parmak izinde oluşan bozulmaların değerlendirmesi için PSNR ve SSIM değerleri ile çalışmanın değerlendirilmesi yapılacaktır. Şekil 6.10 2 da tez çalışmasının PSNR ve SSIM test değerleri verilmiştir. PSNR değeri 8 bit çalışmalar için 30 – 50 dB arası kaliteli bir çalışma olduğu ortaya koymaktadır. PSNR değeri tepe sinyal gürültü oranını temsil ettiğinden kalite testi için önemli bir ölçüttür. Orijinal parmak izi ile damgalanmış parmak izi arası PSNR değeri 33,84 dB değeri elde edilmiş başarılı bir sonuç ortaya çıkmıştır.

SSIM değeri ise resimdeki bozulmayı görsel algıya göre değerlendirme yapmak için kullanılır. Görsel olarak görüntünün ne kadar bozulduğunu test etmek için kullanılır. PSNR gürültü testi yapılır iken SSIM görüntünün görsel bozulma miktarı hakkında bilgi verir. $0<SSIM<1$ arası

değerler arasında değerlendirilir SSIM=1 orijinal resmi ifade eder. 0 değeri ise görsel olarak resmin çok kötü olduğunu ifade eder. Orijinal parmak izi ile damgalı parmak izi arasında ölçülen SSIM=0,8327 olarak elde edilmiş ve görüntü bozulması çok az olduğu kabul edilebilir değerler arasında olduğu ortaya çıkmıştır [63,64].



Şekil 6.10. Tez Uygulaması PSNR-SSIM kalite testi

Tablo 6.8'de benzer farklı çalışmalarda elde edilmiş PSNR değerleri görülmektedir. 1. Sırada verilen PSNR değeri tez çalışma konumuz olan biyometrik görüntülerde kimlik denetimi için şifreleme teknikleri kullanarak damgalama uygulamamız sonunda giriş parmak izi ile damgalı çıkış parmak izi arasında yapılan ölçüm sonucudur. Tablo incelendiğinde 4,5,7 numaralı çalışmalardan tez çalışmamız daha iyi değerler verdiği 2,3,6 numaralı çalışmalara ise yakın değerler aldığı görülmektedir. 8,9,10 numaralı değerler ise gauss gürültüsü altında alınan değerlerdir. Damgalı parmak izi çalışmamız gauss gürültü sonunda alınan PSNR değeri 14,51 dB olarak elde edilmiştir. İnceleme yapıldığında gürültü altında dahi çalışmamız olumlu sonuç vermiştir. 8,9,10 numaralı gauss gürültüsü çalışmasında resimler sadece gürültü eklenerek ölçüm yapılmıştır. Tez çalışmamız olan damgalı parmak izi görüntü RSA, LSB, DWT, 3 işleme tabi tutulduktan sonra gauss gürültü testi yapılmıştır.

Tablo 6.8. Tez konusu çalışmanın benzer çalışmalar ile karşılaştırması

S.NO	ÇALIŞMA ADI	PSNR(dB)
1*	Biyometrik Görüntülerde Kimlik Denetimi için Şifreleme Teknikleri Kullanılarak Damgalama	33,84
2	RSA-DWT Based Medical Image Watermarking For Telemedıcıne Applications Ultrasound(US) [3]	46,34
3	A security enhanced robust audio steganography algorithm for image hiding using sample comparison in discrete wavelet transform domain and RSA encryption [4]	41,73
4	Data Hiding using Skin Detection, DWT Technique and RSA with Bit Shift Method (baby.jpg-flowr.jpg)[6]	33,66
5	Medical Image Compression and Encryption Using Adaptive Arithmetic Coding, Quantization Technique and RSA in DWT Domain (Table -3, Image #11)[65]	29,81
6	Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques (average-) [66]	40,31
7	An efficient lossy cartoon image compression method (bee-4C) [67]	25,55
8	Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study [63] -lena	14,18
9	Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study [63] -Barbara	15,48
10	Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study [63] -Cameramen	15,28

7. SONUÇLAR

Bu tez çalışmasında biyometrik veriler, damgalama çeşitleri, Kriptoloma çeşitleri ve steganografi incelenmiştir. Damgalama çeşitleri olarak LSB, DWT, DCT, DFT incelenmiş bu sayısal damgalama metotlarından DWT damgalama ile kişinin bilgileri damgalanmıştır. Biyometrik veri olan parmak izine kişi bilgisi eklenmiştir.

Sistem veya haberleşme güvenliği için kullanılan biyometrik veri ve sistem şifresi kimliklendirme işlemlerinde sistemin ve haberleşmenin en zayıf noktası olan şifrenin korunması işlemi yapılmıştır. Sistem şifresi RSA kriptoloma ile metin dosyasına dönüştürülmüş bu metin dosyası steganografi ile örtü remine gizlenmiş ve DWT damgalama için damga elde edilmiştir. Elde edilen damga DWT damga ile biyometrik veri içerisine gizlenmiştir.

Gauss(gaussian), tuz &biber (salt & pepper), yerel değişken (localvar), benek(speckle), atış (poisson), hareket izi (motion blur), aşındırma(erosion), genişletme(dilation) 8 ayrı gürültü çeşidine biyometrik veri ve damgayı maruz bırakıp dayanaklılığı test edilmiştir. Kalite testleri PSNR, MSE, RMSE, Evrensel Görüntü Kalitesi İndeksi (UIQI), EME (Orijinal Resim), EME (Gürültülü Resim), Pearson Korelasyon Katsayısı (orijinal ve gürültülü resim), Pearson Korelasyon Katsayısı (orijinal resimler arası), SNR, MAE testleri yapılmıştır.

Biyometrik görüntülerde kimlik denetimi için şifreleme teknikleri kullanarak damgalama çalışmasının testi incelendiğinde;

Orijinal parmak izine uygulanan gürültüler sonucu elde edilen PSNR değerleri 14 – 27 dB arasındadır.

Damgalı parmak izi verisine uygulanan gürültüler sonucunda elde dilen PSNR değerleri 14 – 27 dB arasındadır.

Damganın gürültülere karşı testinde elde edilen PSNR değerleri 14 – 29 dB arasındadır. PSNR verileri incelendiğinde RSA kriptoloma, LSB steganografi, DWT damgalama işlemi uygulanan biyometrik veri gürültü testi sonucunda elde edilen PSNR değerleri ile hiçbir işlem yapılmayan orijinal biyometrik verinin test değerleri karşılaştırıldığında iki farklı biyometrik verinin gürültü testleri çok yakın olduğu tespit edilmiştir. Test değerleri değerlendirildiğinde yapılan tez çalışmasının gürültülere karşı dayanıklı olduğu belirlenmiştir.

Tez konusu çalışmasının diğer kalite testi ise girdi parmak izi verisi ile çıktı parmak izi verisi arasında oluşan gürültü ve görüntü bozulmaları testidir. Tez konusu çalışmamız PSNR ve SSIM testleri yapılarak PSNR=32,74 dB SSIM değeri 0,832 olarak bulunmuştur. Her iki testte çalışma konusu ideal değerlerde olduğu ortaya konulmuştur.

ÖNERİLER

Biyometrik verilerin damgalama ve sonra şifreleme işlemi yapılma işleminde saldırılar ve diğer damgalama ve şifreleme metotları incelenerek PSNR oranı nasıl değiştiği incelenebilir. Bu biyometrik verilerin güvenliği sağlanmasında parmak izi verisi kullanılmıştır. Diğer biyometrik veriler olan parmak damar izi, el geometrisi, yüz tanıma, göz tanıma (iris, retina), DNA tanıma gibi veriler üzerine sağlıklı çalışması deney edilebilir.

Sistem şifresi korunması üzerine bir çalışma yapılmıştır. Biyometrik verinin korunma yolları ile sistem şifresi korunması birleştirilebilir.

KAYNAKLAR

[1] Yeşilbaş, E.(2016). Cebirsel Kriptoloji Yöntemleri ve Bazı Uygulamaları,Yüksek Lisans Tezi,Recep Tayyip Erdoğan Üniversitesi,Fen Bilimleri Enstitüsü

[2] Varghese, S., & Kamal, L. (2012). Enhanced RSA combined with DWT domain watermarking. International Journal of Modern Engineering Research, 2(2), 18-20.

[3] Venkatram, N., Reddy, L. S. S., Kishore, P. V. V., & Shavya, C. H. (2014). RSA-DWT Based Medical Image Watermarking For Telemedicine Applicatıons. Journal of Theoretical & Applied Information Technology, 65(3).doi: 10.5815/ijmecs.2016.04.06

[4] El-Khamy, S. E., Korany, N. O., & El-Sherif, M. H. (2017). A security enhanced robust audio steganography algorithm for image hiding using sample comparison in discrete wavelet transform domain and RSA encryption. Multimedia Tools and Applications, 76(22), 24091-24106.doi 10.1007/s11042-016-4113-8

[5] Nagpal, S., Bhushan, S., & Mahajan, M. (2016). An enhanced digital image watermarking scheme for medical images using neural network, DWT and RSA. International Journal of Modern Education and Computer Science, 8(4), 46.doi 10.5815/ijmecs.2016.04.06

[6] Kumari, J., & Yadav, K. (2017). Data Hiding using Skin Detection, DWT Technique and RSA with Bit Shift Method. C.04,Sayı 05, Mayıs

[7] Garg, M., Gupta, S., & Khatri, P. (2015, November). Fingerprint watermarking and steganography for ATM transaction using LSB-RSA and 3-DWT algorithm. In 2015 International Conference on Communication Networks (ICCN) (pp. 246-251). IEEE.

[8] Bhargava, S., & Mukhija, M. (2019). Hide Image and Text Using LSB, DWT and RSA Based On Image Steganography. Ictact Journal on Image & Video Processing, 9(3).doi:10.21917/ijivp.2019.0275

[9] Bermani, A. K. (2017). High Security Steganography Model Based on DWT, DCT and RSA. Journal of Engineering and Applied Science, 12, 8875-8881.doi: 10.3923/jeasci.2017.8875.8881

[10] Divya, G., Rao, T. D., (2020) Hybrid Digital Image Watermarking for Copyright Protection using DWT-SVD and RSA encryption.Dogo Rangsang Research Journal,UGC Care Group I Journal,ISSN : 2347-7180,Vol-10 Issue-08 No. 01 August 2020

[11] Kishore, P. V. V., Venkatram, N., Sarvya, C., & Reddy, L. S. S. (2014, August). Medical image watermarking using RSA encryption in wavelet domain. In 2014 First International Conference on Networks & Soft Computing (ICNSC2014) (pp. 258-262). IEEE.

[12] Solanki, N., Malik, S. K., & Chhikara, S. (2014). Roni medical image watermarking using DWT and RSA. International Journal of Computer Applications (0975-8887), 96(9). C.19, sayi 9.

[13] Rakhımov, A.(2017). Biyometrik Sistemlerin Bilgi Güvenliği,Yüksek Lisans Tezi, Ankara Üniversitesi, Fen Bilimleri Enstitüsü

[14] Çelebi, A.T.(2008).Biyometrik Tanıma, Yüksek Lisans Tezi,Kocaeli Üniversitesi,Fen Bilimleri Enstitüsü

[15] Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on circuits and systems for video technology, C.14(1),sayi 1, 4-20.

[16] Sönmez, E. B., Özbek, N. Ö., & Özbek, Ö. (2007). Avuç izi ve parmak izine dayalı bir biyometrik tanıma sistemi. Akademik Bilişim Konferansları.

[17] Tolun, Y.(2020). Kişisel Verilerin KVKK ve GDPR Kapsamında Korunması,Yüksek Lisans Tezi,Kırıkkale Üniversitesi, Sosyal Bilimleri Enstitüsü, Hukuk Ana Bilim Dalı

[18] ŞAN, S.(2013). Parmak Damar Tanıma Teknolojisi,Yüksek Lisans Tezi,FıratÜniversitesi, Fen Bilimleri Enstitüsü

[19] Yalçın, N., &Gürbüz, F. (2015). Biyometrik güvenlik sistemlerinin incelenmesi. Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 3(2), 398-413.

[20] Kukula, E. P., Gresock, B. P., Elliott, S. J., & Dunning, N. W. (2007, June). Defining habituation using hand geometry. In 2007 IEEE Workshop on Automatic Identification Advanced Technologies (pp. 242-246). IEEE.

[21] Chaudhary, D. R., & Sharma, A. (2012, December). Hand geometry based recognition system. In 2012 Nirma University International Conference on Engineering (NUiCONE) (pp. 1-5). IEEE.

[22] Varol, A., &Cebe, B. (2011). Yüz Tanıma Algoritmaları Algorithms Of Face Recognition. In 5th International Computer & Instructional Technologies Symposium.22-24 September 2011, Fırat University, Elazığ- Turkey

[23] Kurt, B.(2007). Bilgisayar ile Psikolojik Durum Değerlendirilmesi,Yüksek Lisans Tezi, Karadeniz Teknik Üniversitesi,Fen Bilimleri Enstitüsü

[24] Çelebi, A.T.(2008). Biyometrik Tanıma,Yüksek Lisans Tezi,Kocaeli Üniversitesi,Fen Bilimleri Enstitüsü

[25] Akhan, N.(2004). Bilgisayar Destekli İris Tanıma,Yüksek Lisans Tezi,Selçuk Üniversitesi,Fen Bilimleri Enstitüsü

[26] Manav, C.(2010). Görüntü İşleme Yardımı İle Kimlik Tespiti,Yüksek Lisans Tezi,Gazi Üniversitesi,Fen Bilimleri Enstitüsü

[27] Emir Diltemiz, S.(2006).DNA'yı Tanıma Bölgelerine SahipMoleküler Baskılanmış PolimerTekniğine DayalıBiyosensör Geliştirilmesi, Doktora Tezi, Anadolu Üniversitesi, Fen Bilimleri Enstitüsü

[28] Doğru, E.(2017).Karbon Fiber Esaslı DNA Biyosensör Tasarımı,Doktora Tezi,İstanbul Teknik Üniversitesi,Fen Bilimleri Enstitüsü

[29] Biyolojik İnceleme Şube Müdürlüğü, https://www.egm.gov.tr/kriminal/biyolojiuzmanlik Erişim tarihi:17.02.2020

[30] Gümüş, F., Ata, O., &Balık, H. H. (2018). Davranışsal biyometrinin 5 yılı: Kimlik doğrulama ve anomali tespit uygulamaları. Fırat Üniversitesi Mühendislik Bilimleri Dergisi, 30(1), 345-364.

[31] Furat, M.(2006).Sayısal Ortamlarda Veri Damgalanması veGeri Eldesi,Yüksek Lisans Tezi,Mustafa Kemal Üniversitesi,Fen Bilimleri Enstitüsü

[32] Erözen, A.T.(2018).Çoklu-Biyometrik Verilerle Görüntü Damgalama,Doktora Tezi, Yıldız Teknik Üniversitesi, Fen Bilimleri Enstitüsü

[33] Yalman, Y. Ertürk, İ.Akar, F. Çetin, Ö.(2014). Veri Gizleme,1.Baskı,Beta,İstanbul

[34] Chouse, C., &Albayrak, S., Dayanıklı Sayısal Resim Damgalama. https://www.emo.org.tr/ekler/2cbf4730aeac1d6_ek.pdf Erişim Tarihi:13.01.2021.

[35] Macit, H.B.(2019). Mobil Cihaz Görüntüleri İçin Entropi TabanlıKırılgan Damgalama Metodu Geliştirilmesi,Doktora Tezi,Süleyman Demirel Üniversitesi,Fen Bilimleri Enstitüsü

[36] Abdullatif, M., Zeki, A. M., Chebil, J., & Gunawan, T. S. (2013, March). Properties of digital image watermarking. In 2013 IEEE 9th international colloquium on signal processing and its applications (pp. 235-240). IEEE.

[37] Sıddık, O.(2013).Radon Transform Temelli Gizli Olmayan Dayanıklı Filigranlar,Yüksek Lisans Tezi,Çankaya Üniversitesi,Fen Bilimleri

[38] Kazan, S., & Vural, C. (2016). Sayısal Görüntü Damgalama Yöntemlerinin Jpeg Sıkıştırmasına Karşı Dayanıklılığının Karşılaştırılması. Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, 2(1).

[39] Şahin, Y., Ulutaş, G., & İmamoğlu, M. B. (2018). İlişkisel veritabanlarının bütünlük kontrolü için ayrık kosinüs dönüşümü tabanlı kırılgan sıfır damgalama şeması. Pamukkale University Journal of Engineering Sciences, 24(5).

[40] Doğan, Ş. (2011). Yeni Bir Sayısal Damgalama Tekniği ile Biyometrik Uygulamalar, Doktora Tezi, Fırat Üniversitesi, Fen Bilimleri Enstitüsü

[41] Elbaşı, E. İmgelerde DWT ile Damgalama Metodu. Academia Accelaration the world ' sresearh, erişim tarihi:22/05/2022

[42] Raid, A. M., Khedr, W. M., El-Dosuky, M. A., &Ahmed, W. (2014). Jpeg image compressionu sing discrete cosine transform-A survey. arXivpreprint arXiv:1405.6147.

[43] Aydın, İ, BMÜ-357 Sayısal Görüntü İşleme ders notu, Frekans domain'inde İşlemler

[44] Pereira, S., Ruanaidh, J. J. K. O., Deguillaume, F., Csurka, G., &Pun, T. (1999, June). Template based recovery of Fourier-based watermark susinglog-polar and log-logmaps. In Proceedings IEEE international conference on multimedia computing and systems (Vol. 1, pp. 870-874). IEEE.

[45] Karamanjı, A., Q., ,(2018),Steganografi Kullanarak Görüntü Güvenlik Yöntemi, Yüksek Lisans Tezi, Gaziantep Üniversitesi,Fen Bilimleri Enstitüsü

[46] Oğuz, C. (2006). Görüntü İşaretleri İçin Yeni Bir Sayısal Damgalama Yöntemi, Yüksek Lisans Tezi, İstanbul Üniversitesi, Fen Bilimleri Enstitüsü

[47] Ural, U.Örenç,Ö.(2019). Şifreleme ve Şifre Çözme Yöntemleri,3.Baskı,Pusula,İstanbul

[48] Güleryüz İ,H,(2014).Gri Seviye Görüntülerde Kriptografik Uygulamalar, Yüksek Lisans Tezi, Fırat Üniversitesi, Fen Bilimleri Enstitüsü

[49] Sakallı, M. T., Buluş, E., Şahin, A., &Büyüksaraçoğlu, F. (2007). Akış Şifrelerinde Tasarım Teknikleri ve Güç İncelemesi. IX. Akademik Bilişim Konferansı Bildirileri 31 Ocak-2 Şubat 2007.

[50] Çakır, B.(2012),Akış Şifreleme Algoritmalarının Karşılaştırmalı Olarak İncelenmesi, Yüksek Lisans Tezi, Hacettepe Üniversitesi, Fen Bilimleri Enstitüsü

[51] Kırımlı.M, (2007). Açık Anahtar Kartografisi ile Sayısal İmza Tasarımı ve Uygulaması, Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü

[52] Diker, A., & Varol, A. (2013, May). E-Ticaret ve güvenlik. In 1st İnternational Symposium on Digital Forensics and Security (ISDFS'13) (pp. 20-21).

[53] Yerlikaya, T., Gençoğlu, H., Emir, M. K., Çankaya, M., &Buluş, E. (2013). RSA Şifreleme Algoritmasi ve Aritmetik Modül Uygulaması. İstanbul Aydın Üniversitesi Dergisi, 3(9), 95-104.

[54] Engin, S. (2020). RSA Şifreleme Yöntemi ve Özellikleri Üzerine, Yüksek Lisans Tezi, Erciyes Üniversitesi, Fen Bilimleri Enstitüsü

[55] Aghayev, M. (2017). Kriptoloji ve Veri Şifreleme Teknikleri Üzerine, Yüksek Lisans Tezi, Ege Üniversitesi, Fen Bilimleri Enstitüsü

[56] Hatun, E. (2018). Raspberry Pı Üzerinde Gerçeklenmiş RSA Algoritmasına Yan Kanal Analizi, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü

[57] Altıner, H., & Şaykol, E. Veri Güvenliğinde Tempest Saldırı Türleri Üzerine Tarihsel Bir İnceleme. Beykent Üniversitesi Fen ve Mühendislik Bilimleri Dergisi, 6(2), 121-152.

[58] Parmak İzi ile Ödeme yapılacak, Örnek Parmak İzi, http://www.suzmehaber.com/haber/parmak-izi-ile-odeme-yapilacak-1358,Erişim tarihi:23.05.2020

[59] Michael Chan (2022). Image Error Measurements (https://www.mathworks.com/matlabcentral/fileexchange/29500-image-error-measurements?s_tid=srchtitle_Image%20Error%20Measurements%20_1), MATLAB Central File Exchange. Erişim tarihi:29 Mayıs 2022

[60] Shaun Gomez (2022). Implementation of RSA Algorithm (https://www.mathworks.com/matlabcentral/fileexchange/38439-implementation-of-rsa-algorithm), MATLAB Central File Exchange. Erişim Tarihi: 11 Haziran 2022.

[61] Shivendra Singh (2022). Image Watermarking using DWT (https://www.mathworks.com/matlabcentral/fileexchange/67510-image-watermarking-using-dwt), MATLAB Central File Exchange. Erişim Tarihi: 11 Haziran 2022.

[62] CS 534 Steganography Project, https://sites.google.com/site/cs534steganographyproject/home/matlab-code-and-examples Erişim Tarihi: 11 Haziran 2022.

[63] Sara, U., Akter, M., & Uddin, M. S. (2019). Image quality assessment through FSIM, SSIM, MSE and PSNR—a comparative study. Journal of Computer and Communications, 7(3), 8 18.

[64] Hussam Ali (2022). PSNR CHECK (https://www.mathworks.com/matlabcentral/fileexchange/50833-psnr-check), MATLAB Central File Exchange. Retrieved June 26, 2022.

[65] Hussein, N. H., & Ali, M. A. (2022). Medical Image Compression and Encryption Using Adaptive Arithmetic Coding, Quantization Technique and RSA in DWT Domain. Iraqi Journal of Science, 2279-2296.

[66] Wahab, O. F. A., Khalaf, A. A., Hussein, A. I., & Hamed, H. F. (2021). Hiding data using efficient combination of RSA cryptography, and compression steganography techniques. IEEE Access, 9, 31805-31815.

[67] Jeromel, A., & Žalik, B. (2020). An efficient lossy cartoon image compression method. Multimedia Tools and Applications, 79(1), 433-451.

ÖZGEÇMİŞ

Muhammet Ali USER

[redacted]