T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
FEN BİLİMLER ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİMDALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİMDALI

DİJİTAL DOKUMAN GÜVENLİĞİNİN FARKLI BİYOMETRİ TEKNOLOJİLERİ İLE SAĞLANMASI

Yüksek Lisans Tezi

Hazırlayan

Mehmet Kıvılcım KELEŞ

Tez Danışmanı

Prof. Dr. Ali GÜNEŞ

İstanbul - 2014

T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
FEN BİLİMLER ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİMDALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİMDALI

DİJİTAL DOKUMAN GÜVENLİĞİNİN FARKLI BİYOMETRİ TEKNOLOJİLERİ İLE SAĞLANMASI

Yüksek Lisans Tezi

Hazırlayan

Mehmet Kıvılcım KELEŞ

Tez Danışmanı

Prof. Dr. Ali GÜNEŞ

İstanbul - 2014

T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ
MÜDÜRLÜĞÜ'NE

Tez Onay Belgesi

Enstitümüz Bilgisayar Mühendisliği Anabilim Dalı, Bilgisayar Mühendisliği (Tezli) Yüksek Lisans Programı **Y1113.010009** numaralı öğrencisi **MEHMET KIVILCIM KELEŞ'** in **"DİJİTAL DÖKÜMAN GÜVENLİĞİNİN FARKLI BİYOMETRİ TEKNOLOJİLERİ İLE SAĞLANMASI"** adlı tez çalışması Enstitümüz Yönetim Kurulunun Lisans Tezi olarak kabul...edilmiştir.

Öğretim Üyesi Adı Soyadı	İmzası
Tez Savunma Tarihi : 19.12.2014	
1) Tez Danışmanı :Prof. Dr. Ali GÜNEŞ	
2) Jüri Üyesi :Yrd.Doç.Dr.Metin ZONTUL	
3) Jüri Üyesi :Yrd.Doç.Dr.Atakan ERDEM	

Not: Öğrencinin Tez savunmasında **Başarılı** olması halinde bu form **imzalanacaktır**. Aksi halde geçersizdir.

ÖN SÖZ

Tez çalışması kapsamında dijital doküman güvenliğinin farklı biyometri teknolojileri ile sağlanması konusu teknik açıdan detaylı olarak incenmiştir.

Bu çalışmanın hazırlanması esnasında bana yol gösteren, bu alanda çalışmam için beni teşvik eden, yardımlarını ve desteğini benden esirgemeyen değerli danışman hocam Prof. Dr. Ali GÜNEŞ' e teşekkür ederim.

İstanbul, 2014 Mehmet Kıvılcım KELEŞ

İÇİNDEKİLER

ŞEKİLLER TABLOSU

KISALTMALAR

LSB En Önemsiz Bite Ekleme (Least Significant Bit Insertion)

SD Döngü Sayısı

SB Veri Bloğundaki Kelime Sayısı

SA Anahtardaki Kelime Sayısı

DCT Ayrık Kosinüs Teoremi (Discrete Cosine Transform)

WAV Windows Audio Visual

AIIF Audio Interchange File Format

TABLOLAR TABLOSU

1. GİRİŞ

Son yıllarda network altyapısının iyileşmesi ve bulut teknolojilerinin gelişmesi ile dijital ortama aktarılan dokümanlar ve dokümanlardaki bilgi güvenliği oldukça önemli bir konu olarak incelenmektedir. İnternetin yaygınlaşması güvenlik açıklarını beraberinde getirmiş, bunun sonucu olarak da dijital veri güvenliği önemli bir boyut kazanmıştır. Dijital ortama taşınan dokümanların çalınması, yetkisiz kullanıcılar tarafından açılması, içindeki bilgilere erişilmesi ve değiştirmesi telafisi çok güç sonuçlar doğurabilmektedir. Bu durum dokuman gizliliğinin ihlali ve bilginin çalınması gibi durumlar doğurabilmektedir.

Dijital veri güvenliğini sağlamak amacıyla çeşitli koruma mekanizmaları geliştirilmiş, yeni teknoloji ve uygulamalar ortaya çıkmıştır. Günümüzde en sık kullanılan teknoloji şifrelemedir. Bu teknoloji de korunması istenen veri, şifreleme algoritmaları ve bir anahtar yardımı ile anlaşılmaz hale dönüştürülmektedir. Ancak şifrelerin zaman içinde kırılabilmesi, unutulması veya çalınması durumları sıklıkla karşımıza çıkmaktadır. Zaman içinde veri güvenliği için şifrelerin tek başına yeterli olmadığını göstermektedir. İşte bu noktada steganografi bilimi gündeme gelmektedir.

Steganografi kökleri binlerce yıl öncesine dayanan bir bilim dalıdır [2]. Steganografi, bir nesne içerisine veri gizlenmesi olarak tanımlanır[1]. Görüntü dosyaları üzerinde bilgi gizlemek için geliştirilmiş yöntemleri üç ana başlıkta inceleyebiliriz. Bunlar;

1- En önemsiz bite ekleme,
2- Maskeleme ve filtreleme,
3- Algoritmalar ve dönüşümler [3].

1.1. Tez Çalışmasının Amacı

Bu tez çalışmasında dijital dokümanlardaki bilgi güvenliği için kullanılan kimlik doğrulama yöntemlerinden Damar Tanıma Sistemi ve Parmak izi tanıma sistemi

ele alınmıştır. Damar Tanıma veya Parmak izi tanıma sistemin de kişilerin biyometrik görüntülerinin birbirinden farklı olması baz alınarak dijital dokümanın güvenliği sağlanmıştır.

1.2. Tez Çalışmasının Kapsamı

Tezin ilk bölümünde tezin amacı ve kapsamı anlatılmıştır. İkinci bölümde literatür araştırmaları sonucunda biyometrinin amacı, özellikleri ve biyometri teknolojileri hakkında detaylı teorik bilgi verilecek, üçüncü bölümde dijital dokümanların yapısı incelenmiştir. Dördüncü bölümde steganogrpy ise çeşitleri ve yöntemleri hakkında bilgi verilmiştir. Beşinci bölümde şifreleme yöntemleri başlığı altında şifreleme çeşitleri ve dijital doküman şifreleme ile ilgili bilgi verilmiştir. Altıncı ve yedinci bölümde ise yapılan uygulama çalışması ve bu çalışmalar neticesinde sonuç ve öneriler tartışılmıştır.

2. BİYOMETRİ

Biyometri, kelime kökeni olarak iki kelimenin türetilmesinden oluşmuştur. Bunlar Yunanca'dan ‘‘Bios’’ (hayat) ve ‘‘metron’’ (ölçü) kelimelerinin birleşimden Biyometri kelimesi oluşmuştur.

Biyometri günümüzde insanları birbirinden ayırt etme ve kimlik tespiti yapmak üzere geliştirilmiş bir teknolojidir. Biyometri teknolojisinde temel olarak kişinin sadece kendisinin sahip olduğu, fiziksel veya davranışsal özellikleri ile kendisi olduğunu kanıtlamaya yarayan, fizyolojik ayırıcı özelliklerini kullanır.

Birçok yeni teknolojinin geliştirilmesinde olduğu gibi biyometrinin de gelişiminde güvenlik unsuru öncülük etmiştir[6].

2.1. Biyometrinin Amacı

Biyometri uygulayıcılarının genel amacı kişilerin kimliklerini doğrulayabilmeleri için, kopyalanamayacak veya taklit edilemeyecek fizyolojik özelliklerinin kullanmalarını sağlamaktır. Ancak biyometrik sistemlerin oluşturulabilmesi için bazı standart ölçüler kullanılmalıdır. Biyometrik ölçüler olarak adlandırılan bu ölçülerin şifrelerde kullanımı için INCITS (International Committee for Information Technology Standarts-Uluslararası Bilgi Teknolojileri Standartları Komitesi) tarafından oluşturulmuş uluslararası bir standart mevcuttur [15]. Bu standartların başlıcaları ISO/IEC 19794 ve ISO/IEC 19795 standartları bulunmakta olup bunların dışında FBI gibi kalite onayı veren kurumlarda bulunmaktadır.

2.2. Biyometri Teknolojilerin Özellikleri

Biyometri teknolojilerin gelişiminin de güvenliğin en üst seviyeye taşıma amacı öncülük etmektedir. Tüm biyometrik sistemler aşağıda açıklanmış olan beş özelliğe sahip olmalıdır [16]:

i. Evrensellik özelliği: İnsanların biyometrik tanımlana bilen özelliğe sahip olmasıdır[16].
ii. Eşsiz olma özelliği: Biyometrik özelliğin insandan insana farklılık göstermesidir[16].
iii. Süreklilik özelliği: Eşsiz olan özelliklerin zamanla değişmemesi aynı kalmasındır16].
iv. Elde edilebilirlik özelliği: Biyometrik özelliğin sensörler ile alınabilmesi özelliğidir[16].
v. Kabul edilebilirlik özelliği: İnsanların biyometrik doğrulanmayı ve kayıt edilmesine itiraz etmemelidirler[16].

2.3. Biyometri Teknolojileri

Teknolojinin de gelişmesi ile birçok farklı biyometri teknolojisi geliştirilmiştir. Bu teknolojilerden DNA, Avuç damar izi, Parmak damar izi, İris, Retina, Parmak izi, Ses tanıma, Kulak izi, Avuç izi, El geometrisi, Yüz tanıma, Koku tanıma, Kavrama şekli ve basıncı tanıma, Yürüme biçimi, Ayak izi, İmza, Beyin dalgaları ve Klavyeye basma şiddeti ve hızı en çok bilinen ve kullanılan teknolojilerdir. Günümüzde en yaygın kullanılan biyometrik tanıma sistemi parmak izi ve avuç izidir. Parmak izi ve avuç izi, elde edilmesinin kolay olması ve kriminal alanda da kullanılıyor olması önemli tercih sebebidir. Biyometrik yaklaşımlar içinde avuç içi ve parmak damar izi diğer modellere göre yeni bir biyometrik özelliktir. Damar izi teknolojisi diğer biyometriklere göre en büyük avantajı taklit edilmesinin zor olması ve avuç içi veya parmak damar izi özelliklerinin karakteristik, kalıcı ve dış faktörlerden daha az etkilenebilir olmasıdır. İris ve retina teknolojileri kullanım zorlukları, renkli gözlük veya lenslerin doğrulamayı zorlaştırması bu teknolojinin yaygın kullanım alanlarının oluşmaması ile sonuçlanmıştır. El geometrisi ve Yüz tanıma teknolojileri ortam şartlarından etkilenmesi ve teknolojinin yanlış doğrulama yapmasına neden olabilecek tehditler sık karşılaşılmaktadır. Koku tanıma, Kavrama şekli ve basıncı tanıma, Yürüme biçimi, Ayak izi, İmza, Beyin

dalgaları ve Klavyeye basma şiddeti ve hızı gibi teknolojiler gelişme evresinde olan teknolojilerdir.

Farklı biyometri teknolojileri geliştirilmiş olmasına rağmen genel yaklaşım olarak hepsi birbirine teknolojik olarak yakındır. Biyometrik tanıma sistemlerinde, ilk adım görüntüyü kaydetmektir. Bu görüntü sayısal koda çevrilir. Bu kod şifreleme algoritmaları kullanarak şifreleme işlemi yapılır ve bilgisayara kayıt işlemi yapılır. Kullanıcı herhangi bir biyometrik cihaz kullanarak kendini sisteme kaydeder. Kullanıcının kendini sisteme tanıttığı veri ile doğrulama aşamasında üretilen veri birbiriyle birebir aynı olma şansı yoktur [5]. Biyometri teknolojilerinde kişi doğrulaması için kayıt olan sayısal kod ile üretilen kodun birbiriyle belirli oranda tutması yeterlidir.

2.4. Parmak ve Avuç İzi

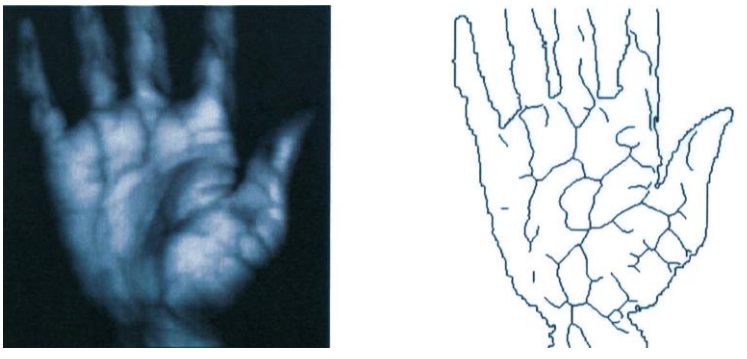
Parmak ve avuç izi teknolojisi güvenlik, personel takibi gibi pek çok alanda karşımıza çıkmakta ve herhangi bir şifre gereksinimini ortadan kaldırmaktadır. Bu teknolojide parmağın ve avucun dış yüzeyindeki gözle görünen girintili ve çıkıntılı deri tabakasının bir yüzeye bastırılması ile ortaya çıkan görüntüdür. Bu görüntü kişiye özel olduğu gibi parmağın veya avucun dış yüzeyinde oluşabilecek kesik ve yanıklardan etkilenen bir yapıdadır. Derinin epidermis tabakasında yer alan bu kavisli çizgilere tepe ve çizgilerin arasında kalan boşluklar ise vadi olarak tanımlanmaktadır[11]. Tepe çizgileri ani sonlanabildiği gibi bazıları ikiye ayrılarak devam ederler bu noktaya çatal nokta adı verilmektedir.

Şekil 1. Parmak izi Görüntüsü[13]

Şekil 2. Avuç izi Görüntüsü[14]

2.5. Parmak ve Avuç Damar İzi

Parmak ve Avuç içi damar tanıma teknolojisi, insan uzuvlarındaki damarlarının diziliş yapısının her insanda farklı olmasından yola çıkılarak kişiyi tanımaya yönelik geliştirilmiş bir teknolojidir. Bu teknolojide 700 ila 1000 nm dalga boyunda kızılötesi ışık gönderilerek damar yapısı ortaya çıkarılır. Kanda bulunan hemoglobinin gönderilen kızılötesi ışığı soğurması ile damar görüntüsü elde edilir. Damar tanıma teknolojilerinde kandaki hemoglobin kullanıldığından dolayı canlılık analizi yapılabilmektedir. Damar izi algılayıcı sensörü ile edilen görüntü, biyometrik api ile128 veya 256 bit AES (Advanced Encryption Standart) algoritmasıyla şifrelenerek güvenli sayısal bir değere dönüştürülür.



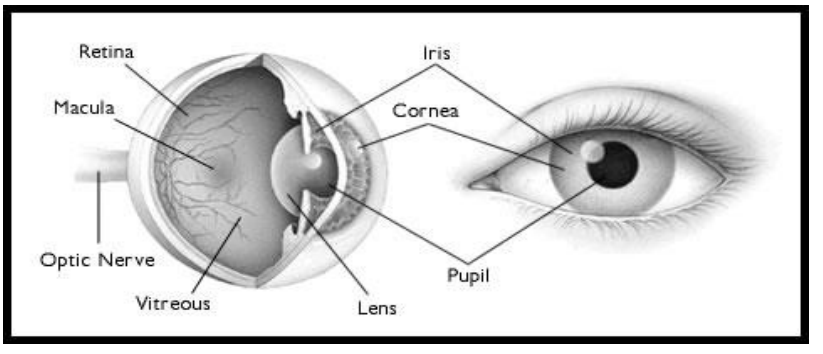
Şekil 3. Yakın Kızılötesi ve Damar Şablonu Görüntüsü[12]

2.6. İris ve Retina

İris, göz bebeği etrafında yer alan renkli halkaya verilen isimdir. İris taramada kullanıcı ile algılayıcı sensör ile fiziksel temas olmadan yaklaşık 15-20 cm uzaklıktan CCD kamera kullanılarak tarama yapılabilmektedir. Bilinenin aksine, İris tanıma sistemi kişiye zarar vermez. Lazer ya da benzeri görüntü alma tekniklerine ihtiyaç duymadan basit bir CCD kamera ile görüntü alınabilmektedir[18]. İris teknolojisi en güvenilir biyometri teknolojilerinden biridir.

Retina tanıma işlemi iris tanımadan farklı olup, göz bebeği arkasındaki damar tabakanın tanınmasıdır. Retina örneği alma sırasında kişinin belirli bir noktaya bakması retina alma ve tanıma işlemini zorlaştırmakta ve yöntemin az tercih edilmesine yol açmıştır.

Doksanlı yılların ortalarında yeniden tasarımla son haline gelmiş olup gelişmiş bağlanıla bilirlik ve kullanıcı arabirimi sağlamaktadır, ama yine de marjinal bir biyometrik teknoloji olarak görülmektedir [20]. İris ve retina tanıma teknolojilerinde tanıma yapılacak kişilerde gözlük ve lens kullanıyorsa ya da okuyucu ile göz temasına girmekten endişe duyuluyorsa uygulanması zor bir yöntemdir.



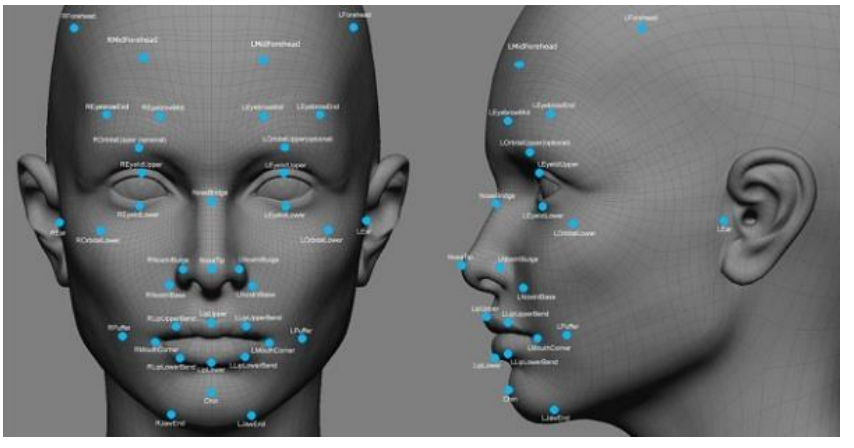
Şekil 4. İris ve Retina [19]

2.7. Yüz Tanıma

Biyometrik sistemlerin temel amacı insanları birbirlerinden ayırt etmektir. İnsanlar birbirlerini yüzlerinden ayırt ederler. Yüz tanıma sistemi neredeyse insanlık tarihiyle yaşıt bir biyometrik ayırt etme yöntemidir. Yüz tanıma teknoloji konusunda temel anlamda kullanılan iki yöntem vardır. Bunlar;

1. Yüz Metriği Yöntemi
2. Yüz Parçaları Yöntemi

Yüz Metriği Yönteminde, yüz üzerinde bulunan organlar arasındaki mesafelerden sayısal ifade çıkarılmaya çalışılır.
Yüz Parçaları Yönteminde ise yüz 150 parçaya bölünür ve bu parçalardan 40 tanesinin belirleyiciliği diğer parçalardan daha fazladır. Bu 40 parçadan başlayarak yüz tanımlanmaya çalışılır. Bu yöntem yüz metriği yöntemine göre yeni bir yöntem olup araştırmacılar tarafından geliştirilmektedir [10].

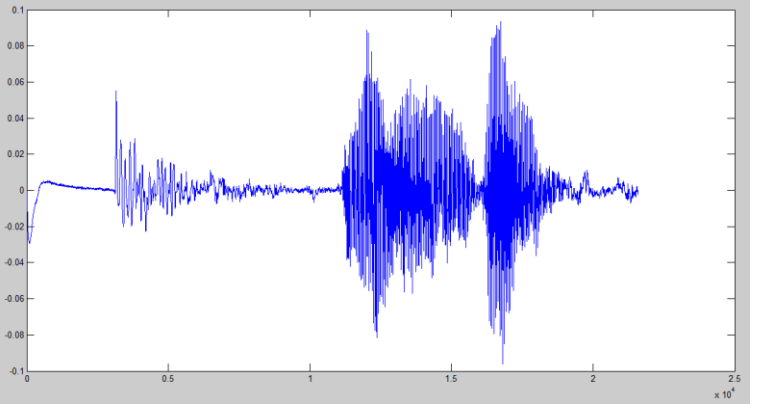


Şekil 5. Yüz Tanıma[24]

2.8. Ses Tanıma

Ses tanıma teknolojisi, incelenen ses sinyalinin içinde barındırdığı karakteristik özelliklerinden, tanınması hedeflenen sese ait unsurları, çeşitli sayısal sinyal işleme teknikleri uygulanarak belirler. Her bir ses karakteristiği, bir öznitelik vektörü ile ifade edilir. Bu özniteliklerden ses tanıma veri tabanı oluşturulur.

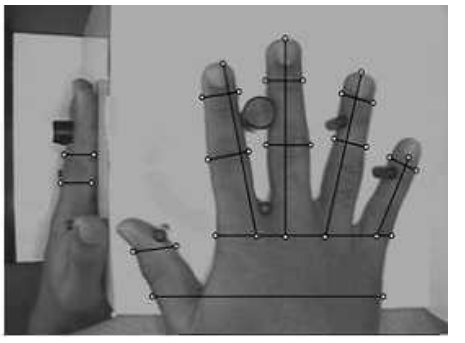
Veri talebi sırasında kullanıcı tarafından sisteme sunulan örüntü, veri tabanındaki kayıtlar ile karşılaştırılır. Eşleştirme işleminin sonucu, sistemin nihai karar mekanizmasına aktarılır ve yetki talebi olumlu ya da olumsuz olarak belirlenir [22].



Şekil 6. Ses Tanıma[23]

2.9. El Geometrisi

El geometrisi tanıma yönteminde tanıma yapılacak kişilerin elinin veya iki parmağının geometrik yapısından bir algoritma ile vektör elde edilir. Bu algoritma ile parmakların genişliği, uzunluğu ve eni gibi ayırt edici özellikleri kullanılmaktadır. Bu teknolojide tanıma oranı yüksek bir yöntem olmakla birlikte dış ortam faktörlerinden etkilenmesi nedeniyle kullanım açısından sıkıntılar doğurabilmektedir.



Şekil 7. El Geometrisi Tanıma[25]

2.10. Biyometri Teknolojisinin Avantajı

Biyometri teknolojinin gelişmesi ile birlikte kişilerin yaşantısında birçok avantajlar sağlamıştır. Bunlar;

- Kimlik saptaması yapılacak kişinin bizzat bulunma gerekliliği ile ileri seviye güvenlik sunması,
- Kendini tanıtmaya yönelik fiziksel bir tanıtıcıya ihtiyaç kalmaması ve kimlik sahteciliğin önüne geçilmesi,
- Şifre/Pin ve benzeri gizli ve saklanması gereken bilgilerin ezberleme ve hatırlama sorunları,

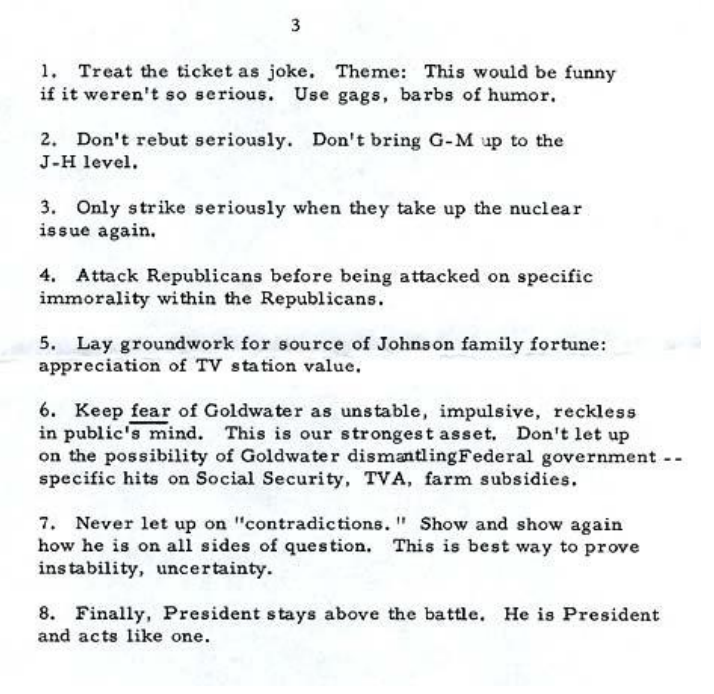
Bilgi teknolojilerinin gelişimi ve internetin yaygın olarak kullanımı ile bazı kişisel verilerin ve gizli bilgilerin yetkisiz kullanıcıların erişimini engellemek şifre, pin, imza ve kimlik kartı gibi konvensiyonel yöntemler ile sağlamak zorlaşmıştır. Biyometrik sistemler kişileri doğrudan tanıdıkları ve düşük yanılma payı sundukları için yüksek güvenlik uygulamalarının vazgeçilmez unsuru olacaktır.

3. DİJİTAL DOKÜMANLARIN YAPISI

Bilgisayar ortamında dijital dokümanlar farklı formatlarda saklanırlar. Bilinen tüm farklı doküman tipleri birer resim dosyası olarak saklana bilinmektedir. Bu resim dosyaları üç ana sınıf altında renkli, gri tonlamalı ve siyah beyaz tonlamalı olarak sınıflandırıla bilinir. Eğer dijital dokuman bir resim dosyası ise kayıplı ve kayıpsız sıkıştırma yöntemleri kullanılarak farklı formatlarda saklanabilmektedir. Bu formatlar 24 bit renkli,8 bit renkli,4 bit renkli,8 bit gri tonlamalı,4 bit gri tonlamalı veya 1 bit olarak siyah beyaz olarak saklanabilirler.

3.1. Siyah Beyaz Tonlamalı Dokümanlar

Siyah beyaz tonlamalı dokümanlar yalnızca iki değerden oluşan resimlerdir. Bu tür görüntülerde her piksel sadece veya beyaz renkten meydana gelmektedir.



3

1. Treat the ticket as joke. Theme: This would be funny if it weren't so serious. Use gags, barbs of humor.

2. Don't rebut seriously. Don't bring G-M up to the J-H level.

3. Only strike seriously when they take up the nuclear issue again.

4. Attack Republicans before being attacked on specific immorality within the Republicans.

5. Lay groundwork for source of Johnson family fortune: appreciation of TV station value.

6. Keep fear of Goldwater as unstable, impulsive, reckless in public's mind. This is our strongest asset. Don't let up on the possibility of Goldwater dismantlingFederal government -- specific hits on Social Security, TVA, farm subsidies.

7. Never let up on "contradictions." Show and show again how he is on all sides of question. This is best way to prove instability, uncertainty.

8. Finally, President stays above the battle. He is President and acts like one.

Şekil 8. Siyah Beyaz Doküman[26]

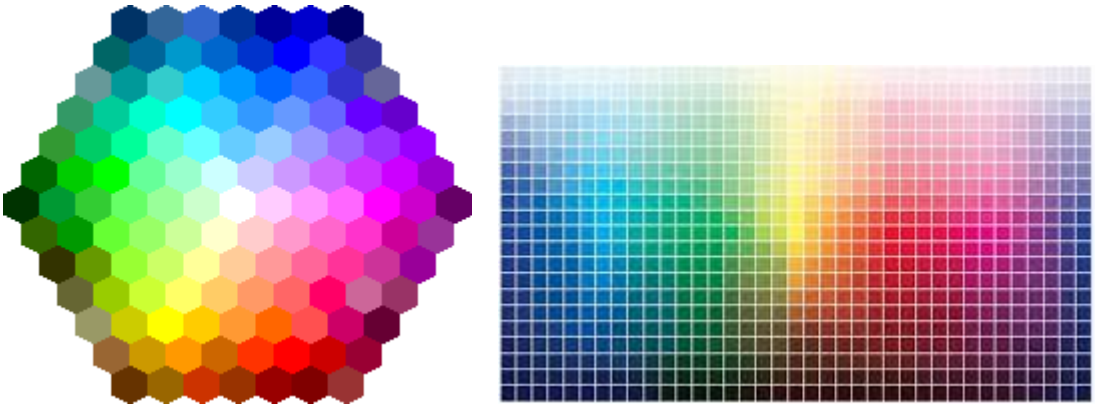
3.2. Gri Tonlamalı Dokümanlar

Gri tonlamalı dokümanlar siyah beyaz tonlamalı resimlerdeki iki ana renklere ek olarak grinin tonları da kullanılır. Bu ton geçişlerindeki renler kod ile ifade edilir ve her bir geçiş renk tonunun bir kod karşılığı vardır. Bu kodlar 0 ile 255 arasındadır. Beyaz 0, siyah 255 değerini alırken aradaki değerler siyah ve beyaz arasında kalan grinin ton değerleridir. Bu resimlerdeki, 256 gri değeri bir byte olarak tanımlanır. Tek görüntü matrisi ile ifade edilir[17].

Şekil 9. Gri Ton Renk Paleti

3.3. Renkli Dokümanlar

Renkli dokümanlar üç ana sınıfta 24 bit renkli,8 bit renkli ve 4 bit renkli olarak oluşturula bilinirler. 24 bit veya 8 bit Renkli dokümanlarda bütün renk değişimleri üç temel rengin birleşmesiyle elde edilir. Bu renkler kırmızı (R), yeşil (G) ve mavi (B) renkleri veya bu renklere ait geçiş tonlarıdır. Bu renklerde, resimde kullanılan renkleri içeren 256 renkli bir palet taşırlar. 24 bit renkli dokümanlarda her piksel bu palette bir renge karşılık gelen 3 baytlık değer taşır. Bundan dolayı, 24 bit renkli dokümanlar bilgi saklamak için en fazla alanı sağlamakta ve farklı şifreleme olanakları için çok seçenek sağlamaktadır.



Şekil 10. Renk Paleti

4. STEGANOGRPHY

Steganograpy kelime anlamı olarak “ kaplanmış yazı” demektir. Steganography’nin amacı gizlenmek istenen gizli mesaj, veri ya da bilginin varlığını saklanılacak dijital veride ufak değişiklikler yaparak saklamaktır. Bir örnek ile açıklamak gerekirse bir manzara resmi içeresine fark edilmeyecek

Steganography ve cryptogarphy çok sık karıştırılan kavramlar olup birbirlerinden farklı kavramlardır. Cryptography’de amaç mesajın içeriğini saklamak iken Steganography’de ise amaç mesajın varlığını saklamaktır. Gizlenmek istenen mesaj yada veri şifrelenip sonra da steganographic yöntemlerle saklana bilinir.

4.1. Steganografi Kullanım Çeşitleri

Steganografi kullanım alanları açısından genel olarak üçe ayrılmaktadır[7]. Bunlar aşağıdaki gibidir:

− Metin (text) steganografi
− Ses (audio) steganografi
− Görüntü (image) steganografi

4.2. Metin (Text) Steganografi

Metin steganografi veri gizlenecek ortamın metin (text) olduğu steganografi türüdür. Metin (text) stegnografi uygulanabilmesi için çeşitli yöntemler vardır. Bunlar şu şekilde sınıflandırılabilir [28];

− Açık Alan Yöntemleri (Open Space Methods)

- Satır Kaydırma Kodlaması
- Kelime Kaydırma Kodlaması

- Gelecek Kodlaması

− Yazımsal Yöntemler (Syntactic Methods)
− Anlamsal Yöntemler (Semantic Methods)

4.3. Ses (Audio) Steganografi

Ses sinyalleri içerisine veri gizleme oldukça zor bir konudur. İnsan işitme sistemi frekans aralığı yüzünden, ses sinyalleri üzerinde uğraşırken ses dosyalarının hangi karakteristiklere sahip olduklarını bilmemiz gerekmektedir.

Ses dosyaları iki ana özelliğe sahiptirler[27]:
− Basit nicelendirme yöntemi: Bu yöntem yüksek kaliteli sayısal seslerin 16-bit doğrusal nicelendirmesi ile kullanılır. Bu dosyalara örnek WAV ve AIIF gösterile bilinir.
− Geçici seçme oranı yöntemi: En çok kullanılan ses oranları 8 kHz, 9.6 kHz, 10 kHz, 12 kHz, 16 kHz, 22.05 kHz ve 44.1 kHz ‘dir. Frekans aralığının kullanılabilecek en üst değerleridir.

Başka bir sayısal gösterim ve algılama formatı ISO MPEG-Audio dur. Bu yöntemde sinyal istatistiği değiştirilerek ses korunur fakat sinyal değiştirilmiş olur [29].

4.4. Görüntü (Image) Steganografi

Steganografi resim dosyalarında yaygın bir biçimde kullanılmaktadır. Bu nedenle resim steganografisi konusunda farklı teknikler geliştirilmiştir.
Görüntü dosyalarının içerisine bir metin gizlenebileceği gibi bir resim dosyasının içine bir başka resmi de gizlemek mümkündür.
Gizlenmek istenen veriyi bir resme gömme (ya da gizleme) işleminde iki farklı resim kullanılmaktadır. Bu resimlerden ilki örtü verisi (cover image) olarak

adlandırılır. Örtü verisi gizlenmek istenen veri ya da bilgiyi içinde saklayacak ana resim dosyasıdır[38]. Diğer resim ise gizlenmek istenen bilgi, veri veya resim dosyadır. Bu dosya ise stego olarak adlandırılmaktadır.

Saklanmak istenen veri, metin, şifrelenmiş metin, resim veya bit dizisi gibi birçok farklı nesne saklanabilir. Gömme işlemi sonucunda "stego resim" adı verilen dosya oluşur.

4.5. Veri Gömme Yöntemleri

Resimlerde birçok farklı yöntem ile bilgi gizlenebilir. Veri gömme işlemi sırasında kullanılan yöntemleri, kullanılan veriyi dikkate alarak iki başlık olarak inceleyebiliriz[30]. Bunlar;

i- Image Domain tekniği
ii- Transform Domain Tekniği

Image Domain tekniği işleminde işlem yapılan resim dosyasındaki piksel değerleri, data gömme işleminde doğrudan kullanılır. Bu tekniğe en önemsiz bite ekleme (Least Significant Bit Insertion) örnek olarak verebiliriz.
Transform Domain tekniği, kapak verideki değişimler üzerinde gömme işlemini uygular[30]. Bu tekniğe, JPEG sıkıştırmadaki DCT katsayıları üzerinde veri gömme işlemini örnek verebiliriz.

4.6. En Önemsiz Bite Ekleme Yöntemi (Least Significant Bit Insertion)

Veri gömme yöntemlerinde en önemsiz bite ekleme yöntemi sık olarak kullanılmaktadır. Bu yöntemin mantığı görüntüdeki bir pikselin bir byte'nın son biti değiştirmek ve böylece en önemsiz bitin yerine gizlenmesini istediğimiz verinin bitleri belirlenmiş olan bir fonksiyon ile birer birer yerleştirmektir. Bu yöntemde değişik yapılan bit en az anlamlı biti olmasından dolayı değişimler insan gözü tarafından algılanamamaktadır.

4.6.1. Gri Tonlamalı Resimlerde LSB Yönteminin Uygulanması

Gri tonlamalı resimlerde her piksel 1 byte ile temsil edilmektedir. 1 byte içerisinde 0 (siyah) ile 255 (beyaz) arasında tam sayı değerlere karşılık gri rengin tonları karşılık gelmektedir. Örneğin, renk değeri 190 olan bir pikselin içine ikilik sayı sistemindeki 1 değeri saklandığında oluşan piksel değeri aşağıda gösterilmektedir.

190	ikilik tabanda gösterilişi	10111110
191	Bilgi saklanmış veri	1011011**1**

Yukarıdaki iki renk değeri arasında gözle fark edilemeyecek kadar az bir değişim vardır. Son bitin 1 ya da 0 olması gözle görülebilir bir fark yaratmamaktadır.

4.6.2. 8-bit Renkli Resimlerde LSB Yönteminin Uygulanması

8 bit renkli resimlerde bir piksel 1 byte olarak kullanılmaktadır. Saklama yapılacak alan çok kısıtlı olduğundan saklama ortamını çok değiştirmeyecek şekilde saklanacak veri seçilmelidir. Son bite ekleme işlemi yapılan görüntüde renk girişi değişmektedir. 8 bit renkli resimlerde dört renk kullanılır. Bunlar;

- Beyaz,
- Kırmızı,
- Mavi
- Yeşildir

Renk paletinde ise sırasıyla Beyaz 0 veya (00), Kırmızı 1 veya (01), Mavi 2 veya (10), Yeşil ise 3 veya (11) gösterilmektedir.

Örnek vermek gerekirse bir görüntünün pikselleri “beyaz, beyaz, mavi, mavi ,” (00 00 10 10) olsun, 10 sayısının ikilik tabanda 1010 olarak gösterilir bu değer

piksellere saklanılmak istenildiğinde, yapılan işlem sonucunda görüntünün yeni pikselleri aşağıdaki gibi olmaktadır[7].

01 00 11 10

Renk paletinde ise kırmızı, beyaz, yeşil ve mavi renkleri olarak görülmektedir[31]. Piksellerdeki renkler çok değiştiğinden, insan gözü ile fark edilebilir olmaktadır bu ise kabul edilemezdir. Uzmanları bu sebepten dolayı 8 bitlik renkli görüntüler kullanmak yerine gri tonlamalı görüntüleri tercih etmektedirler[29].

4.6.3. 24-bit Renkli Resimler ve LSB yönteminin uygulanması

24 bit renkli görüntülerde bir piksel 3 byte içermektedir. Bir piksel üç ana renkten meydana gelmektedir. Bunalar;

- Kırmızı,
- Yeşil,
- Mavi' dir.

Bu üç ana renge pikselin RGB değeri denilmektedir. En önemsiz bite ekleme yönteminden bir byte'ta son biti değiştirilerek bir piksel'de maksimum 3 bit veri gizlene bilinir.

1024x768 piksel boyutunda ve 24 bit derinliğindeki bir resim de, bilgi saklana bilinecek 2.359.296 bit vardır.

Örnek olarak saklamak istediğimiz bir biyometrik verinin 1 byte.ının ikili sistemdeki değeri: 101101101 olsun.

Biyometrik verinin saklanacağı resmin 3 pikselinin değeri:

10010101 00001101 11001001
10010110 00001111 11001010
10011111 00010000 11001011

Resmin içine “101101101” biyometrik veri gizlendiğinde oluşan yeni piksel değerleri aşağıdaki gibi olmaktadır.

10010101 00001100 11001001
10010111 00001110 11001011
10011111 00010000 11001011

Bilginin gömülmesinden sonra bitlerin eklendiği sekiz bayttan sadece dördünde değişiklik meydana geldiği görülmektedir.

4.7. Siyah Beyaz Resimlerde Veri Gizleme

Siyah beyaz resimler üzerinde steganografi uygulamak renkli ve gri tonlamalı resimlere göre daha zor bir işlemdir.

Örnek olarak, boyutu 72×28 piksel olan bir resmi ele alalım.

Bu resmin her pikseli bir bitte saklanır. Her bitte siyah 0 ile ifade edilirken, beyaz ise 1 ile ifade edilir. Resmin bir byte’ında, sekiz piksel gizlene bilinir. Örnek dosyanın toplam hacmi 256 bayttır.

$$boyut = \frac{72 * 28bit}{8} byte + 4byte = 256byte$$

Siyah-Beyaz resimlerdeki ana amaç, daha az fark edilen pikselleri değiştire bilmektir. Çünkü renkli ve gri düzey görüntülerde, renkler ton farkları ile küçük değişimlerle değişirken, siyah-beyaz görüntülerde siyah ve beyaz dışında başka bir ton olmadığında bu mümkün değildir. Örnek verecek olursak, beyaz bir alanda siyah bir nokta koyduğumuzda bu hemen fark edilecektir. Bu yüzden, siyah beyaz resimlerde veri gizlemek için piksel rengindeki değişme nedeniyle dikkat çekmeyecek bir bölge belirlenmelidir.

Önerilen yöntemde, önce görüntü N*N boyutlu eşit boyutlara bölünür, her bir bloğun Steganografiye uygun olma oranı yüzdesel olarak hesaplanır.

Bizim örneğimizde 3*3 boyutlu bloklara parçalayacağız. Her bir bloğun her durum için steganografiye uygunluk yüzde oranı hesaplanır[32].

Bloklar için hesaplanan uygunluk yüzde oranı, belli bir yüzdenin değerinden fazla ise, bu blokta gizlenmek istenen verinin bir biti bu blokta gizlenir. Bilgileri gizlemek için, önce bloktaki beyaz noktaların sayısı hesaplanır. Gizlenmek istenilen veri bitin değeri “1” ise, beyaz hanelerin sayısı çift olmalı, dolayısıyla bu sayı tek ise, 3*3 bloğun ortadaki hanesinin değerini ters yapmakla, beyaz hanelerin sayısı çift olur[32]. Böylece bilgilerden “1” değeri bu blokta gizlenir[32].

Aksi durumu ele alırsak, “0” değerini saklamak için, beyaz hanelerin sayısı tek olmalı, dolayısıyla bu sayı çift ise, 3*3 bloğun ortadaki hanesinin değerini ters yapmakla, beyaz hanelerin sayısı tek olur[32]. Bu sayede “0” değeri bu blokta gizlenmiş olur[32].

Bu örneğimizde veri saklama kapasitesi maksimum 27 bayt olabilir.

$$\frac{72*28bit}{9} = 216bit \Rightarrow \frac{216}{8} = 27bayt$$

5. ŞİFRELEME YÖNTEMİ

Şifreleme bilimi güvenlik unsurunun temel konusudur. Veri iletişimi esnasında, iletilen verinin aradaki bir etken tarafından olduğu gibi elde edilememesi için verinin anlamsız bir biçime dönüştürülmesine şifreleme, bu dönüştürme işleminde kullanılan algoritmalar ise şifreleme algoritmaları olarak bilinmektedir. Şifreleme yaklaşımları simetrik ve asimetrik olmak üzere ikiye ayrılır [33]. Tezimizde biyometrik verilerin şifrelenmesi için simetrik şifreleme algoritmalarını, görüntü şifreleme algoritmaları için ise karmaşık resim şifreleme algoritmalarını kullanacağız.

5.1. Simetrik Şifreleme Algoritmaları

Simetrik şifreleme algoritmaları geleneksel algoritmalar olup, gizli anahtara bağlıdır. Simetrik şifrelemede, şifreleme anahtarı ile şifre çözme anahtarı aynıdır.

Simetrik şifreleme algoritmalarından DES, 3DES ve AES algoritmaları en bilinen ve kullanılan algoritmalardır.

5.1.1. DES

DES 1977 yılında IBM tarafından geliştirilmiş bir algoritma olup, NIST tarafından ticari ve diğer bazı uygulamalarda kullanılmak üzere yayınlanmıştır[34]. Bu algoritmada 56 bitlik anahtar kullanılarak 64 bitlik veri bloklarını 64 bitlik şifreli veri bloklarına dönüştürmektedir [34]. 64 bitlik veri bloğundan bir başlangıç dizilimi elde edilmekte, 56 bitlik anahtar ise, her bir döngüde kullanılmak üzere 16 adet 48 bitlik anahtarlara dönüştürülmekte ve her döngü içerisinde bu anahtarlar kullanılarak bir sonraki döngüye girdi olmak üzere 64 bitlik çıktılar oluşturulmaktadır [34].

5.1.2. 3DES

DES algoritmasını birden fazla şifreleme ile daha güvenli yapma yöntemi 3DES olarak adlandırılmaktadır [34]. 3DES algoritmadasın da 2 anahtar kullanılmaktadır. Mesaj ilk anahtarla şifrelenip, ikinci anahtar ile deşifre edilip tekrar ilk anahtarla şifrelenerek şifreli hale dönüştürülür. Şifreli bir mesaj ise ilk anahtar ile deşifre edilip, ikinci anahtarla şifrelenerek son olarak tekrar ilk anahtarla deşifre edilip orijinal veriye dönüştürülmektedir [34].

5.1.3. AES

AES algoritması DES ve 3DES algoritmalarına göre daha yeni bir algoritmadır. DES algoritmasının anahtar uzunluğunun kısa olması, 3DES algoritmasının da yavaş olması yeni bir şifreleme algoritmasını ihtiyacını gündeme getirmiştir [34]. Bu algoritmada 128 bit, 192 bit veya 256 bitlik anahtarlarla şifreleme yapılabilmektedir. Algoritmada kullanılacak döngü sayısı SD olmak üzere;

SD = 6 + max(SB + SA)

şeklinde hesaplanır [34]. Bu formülde SB veri bloğundaki 32 bitlik kelime sayısını, SA ise anahtardaki 32 bitlik kelime sayısını ifade eder.

5.2. Görüntü Şifreleme Algoritmaları

Görüntü dosyaları metin dosyalarından farklı olduğu için geleneksel algoritmalar resimleri şifrelemek için yavaş kalmaktadırlar.
Görüntü şifreleme algoritmaları üç temel fikre dayanmaktadır[35].

- Değer dönüşümü

- Yerel permütasyon
- Değer dönüşümü ve yerel permütasyon kombinasyonları.

5.2.1. Karmaşık Resim Şifreleme Algoritması

Chang ve Chen tarafından sunulan karmaşık bir sisteme dayalı yeni bir resim şifreleme yöntemidir [8]. Bu algoritma herhangi bir veri kaybı olmadan, yer değiştirme özelliğini kullanan bir şifreleme algoritmasıdır.

MxN büyüklüğündeki bir görüntüyü f fonksiyonu ile gösterirsek. (x, y) f görüntüsünün koordinatlarını göstermek üzere 0< x < M-1, 0< y < N-1 olacak şekilde f(x, y), görüntüsünün (x, y) noktalarındaki gri görüntü seviyesini göstermektedir.

Algoritma tanımları aşağıdaki şekildedir.

Tanım 1: ROLRJ■p : f — f eğer /=0 ise f resmindeki i.satırı (0 < i < M-1), p piksel sola, /=1 ise p piksel sağa döndürmek için tanımlanmıştır [9].

Tanım 2: ROUDJ^p : f — f eğer /=0 ise f resmindeki j. sütun (0 < j < N-1), p piksel yukarıya, 1=1 ise p piksel aşağıya döndürmek için tanımlanmıştır [9].

Tanım 3: ROURf ^ p : f — f f resmindeki (x, y) pozisyonundaki pikselleri döndürmek için tanımlanmıştır, öyle ki; x + y = k, 0 < k < M + N - 2, eğer 1=0 ise aşağı-sol yönünde p piksel, 1=1 ise yukarı-sağ yönünde p piksel döndürmek için tanımlanmıştır [9].

Tanım 4: ROULk ^p : f — f f resmindeki (x, y) pozisyonundaki pikselleri döndürmek için tanımlanmıştır, öyle ki; x - y = k, -(N - 1) < k < M- 1, eğer 1=0 ise yukarı-sol yönünde p piksel, 1=1 ise aşağı-sağ yönünde p piksel döndürmek için tanımlanmıştır[8].

Örneğin 5x7 boyutundaki aşağıda verilen resmi ele alalım.

ROLR22(f), ROUR^2(f) ve ROUL2 0\f) işlemlerinin sonuçları sırasıyla şekil 11'de gösterilmektedir [10].

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35

a) Orjinal Resim

1	2	3	4	5	6	7
8	9	10	11	12	13	14
20	**21**	**15**	**16**	**17**	**18**	**19**
22	23	24	25	26	27	28
29	30	31	32	33	34	35

b) Sağa – Sola Öteleme

1	2	3	4	5	**18**	7
8	9	10	11	**24**	13	14
15	16	17	**30**	19	20	21
22	23	**6**	25	26	27	28
29	**12**	31	32	33	34	35

c) Sola Aşağı – Yukarı Öteleme

1	2	**19**	4	5	6	7
8	9	10	**27**	12	13	14
15	16	17	18	**35**	20	21
22	23	24	25	26	**3**	28
29	30	31	32	33	34	**11**

d) Sağa Aşağı – Yukarı Öteleme

Şekil 11. Karmaşık Resim Şifreleme Algoritması

5.2.2. Ayna Benzeri Resim Şifreleme Algoritması

Resmin piksellerinin karıştırılmasına dayalı bir yöntemdir. Temelde bir algoritma ile yer değiştirme özelliğini kullanan bir resim şifreleme algoritmasıdır. Ayna benzeri görüntü şifreleme algoritması Jiun- Guo ve Jui-Cheng Yen tarafından geliştirilmiştir[36].

MxN boyutundaki resmi f fonksiyonu olarak tanımlarsak, f(x,y), $0 < x < M-1$, $0 < y < N-1$, f resminin (x,y) koordinatındaki gri ton seviyesini belirtir.[35].
Ayna benzeri resim şifreleme algoritmasını 8 adımda tanımlanmaktadır.[35].

Adım 1: başlangıç oktası x(0) ve k=0 olan bir 1-D kaotik sistem seçilir[35].
Adım 2: Seçilen kaotik sistem için karmaşık bir dizi üretilir[35].
Adım 3: Kaotik sistemden binary bir dizi üretilir. 4., 5., 6. ve 7. adımlar: ikili diziye göre yer değiştirme fonksiyonları ile görüntü pikselleri yeniden düzenlenir[35].
Adım 4:

```
For i= 0: M/2 - 1
For j = 0: N/2 - 1
If b(k) = 1
yer değiştir f(i,j) ve f(i+M/2, j+N/2);
End
k = k+1;
end
end
For i=M/2 : M-1
For j = 0 : N/2- 1
If b(k) = 1
yer değiştir f(i,j) ve f(i-M/2, j+N/2);
End
k = k+1;
end
end
```

Adım 5:

For i=0 : M/2-1

For j = 0 : N- 1

If b(k) = 1

yer değiştir f(i,j) ve f(i+M/2, j);

End

k = k+1;

end

end

Adım 6:

For i=0 : M-1

For j = 0 : N/2- 1

If b(k) = 1

yer değiştir f(i,j) ve f(i, j+N/2);

End

k = k+1;

end end

Adım 7:

For i=0 : M-1

For j = 0 : N/4- 1

If b(k) = 1

yer değiştir f(i,j) ve f(i, j+N/4);

End

k = k+1;

end

end

For i=0 : M-1

For j = N/2 : (3/4)xN- 1

If b(k) = 1

yer değiştir f(i,j) ve f(i, j+N/4);

End

k = k+1;

end

end

Adım 8: Algoritmayı durdur[35].

Pikseller üzerinde aynı yer değiştirme işlemi, aynı karmaşık dizi vasıtasıyla iki defa uygulanırsa orjinal resim elde edilmektedir [36].

5.2.3. Brie Resim Şifreleme Algoritması

Brie algoritması, karmaşık resim şifreleme sistemini kullanan bir resim şifreleme algoritmasıdır.

Bu algoritma, bit ötelemesinden dolayı değer dönüşümü ve kendi içerisinde yerel permütasyon özelliğini kullanmaktadır[35].

MxN boyutundaki resmi f fonksiyonu olarak tanımlarsak, f(x,y), 0<x< M-1, 0<y<N-1 ve (x,y) koordinatları f resminin gri tonlama seviyesini belirtmektedir.

ve G={0, 1, 2, 3, ...255} gri resim dizisi olarak tanımlanmaktadır[35].

Tanım 1: ROLRp^q : G — G ikili gösterimin her bir dönüşümlü biti olmak üzere,

x € G için eğer p=0 ise q bit küçük seviyeli bitten yüksek seviyeli bite, p=1 ise yüksek seviyeli bitten düşük seviyeli bite doğru bir bit öteleme işlemi yapılmaktadır[35]. Diğer bir deyişle;

$$ROLR_p^q(x = b_7b_6b_5b_4b_3b_2b_1b_0) = \begin{cases} \sum_{i=0}^{7} b_i x 2^{(i-q+8)\bmod 8} & p=0 \\ \sum_{i=0}^{7} b_i x 2^{(i+q)\bmod 8} & p=1 \end{cases}$$

şeklinde ifade edilmektedir [37]. Algoritma 6 adımdan oluşmaktadır.

Adım 1: M, N, a ve P parametreleri belirlenir[35].

Adım 2: Karmaşık bir sistem ve onun başlangıç değeri x(0) tanımlanır[35].

Adım 3: Kaotik bir sistemden x(0), x(1),x(2),... dizisi üretilir[35].

Adım 4: x(0), x(1), x(2), b(0),b(1),b(2).... bit dizisi üretilir[35].

Adım 5:

For x: 0 To (M-1) DO For y: 0 TO (N-1) DO

p = b(N x (x+y));

q = a + P * b(N x(x+ y +1)); /'(x, y) = ROLRp

(f (x, y));

Adım 6: Algoritmayı durdur [37].

6. UYGULAMA

Çözüm uygulaması 3 temel adımdan oluşmaktadır.

1- Biyometrik okuyucu sensörleden biyometrik veri elde edilmesi
2- Biyometrik verinin dijital dokümanın içeresine gömülme işlemi
3- Dijital dokümanı şifrelenme işlemi

Çözüm uygulaması .net platformu üzerinde C# yazılım dili ile geliştirilmiştir. Biyometri sistemi olarak parmak izi ve avuç damar izi yöntemleri tercih edilmiştir. Parmak izi tercih edilmesinin nedeni; yaygın kullanım alanı ve parmak izi biyometrik verisinin boyutunun küçük olması iken avuç damar izi biyometrisinin kullanılma nedeni ise güvenlik düzeyinin yüksek olması ve dış faktörlerden en az etkilenen biyometri teknolojisi olmasıdır.

Geliştirilmiş olan uygulamada sırasıyla aşağıdaki işlemler uygulanmıştır.
Parmak izi ve avuç damar izi biyometri sensörlerinden üretilen biyometrik data AES şifreleme algoritması ile 128 bit şifreleme tekniği ile şifrelenmiştir.
Resim formatları dışındaki farklı formatlı dijital dokümanlar işlem öncesi resim formatına çevrilip farklı dijital doküman formatları tek bir formatta birleştirilmiştir.
Dijital dokümanların içine biyometrik veri gömme işleminde en önemsiz bite ekleme yöntemi tercih edilmiştir. Bu yöntem ile belge üzerinde gözle ayırt edilemeyecek biçimde, biyometrik veri dokümanın içerisine eklenmiştir.
Biyometrik veri ekli doküman karmaşık resim şifreleme algoritması ile şifrelenerek “mkk” uzantılı bir dosya formatı oluşturulur.
Şifreleme işlemi yapılan dokümana tekrar erişilmek istenildiğinde uygulama üzerinden kişinin biyometrik verisi ile doküman içerisine gömülmüş biyometrik veri ile karşılaştırılır. Biyometrik doğrulama doğru ise dijital doküman görüntülenir.

6.1. Uygulama Mimarisi

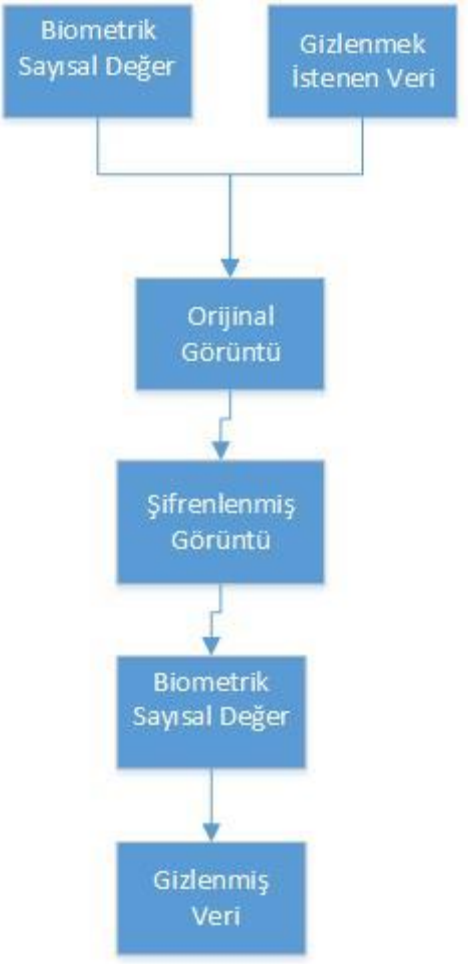
Güvenliği sağlanacak dijital dokümanın uygulama mimarisi aşağıdaki adımlardan oluşmaktadır.

1- Kullanıcı uygulamayı açar.
2- Güvenliği sağlanılmak istenen doküman seçilir.
3- Biyometrik okuyucu sensör üzerinden biyometrik veri alınır.
4- Doküman ile ilgili bilgiler (oluşturulma tarihi, saati vb.) otomatik alınır.
5- Güvenliği sağlanacak dokümanın içerisine biyometrik veri ve doküman ile ilgili veriler dokümanın içerisine gömülür.
6- Yeni formatta şifrelenmiş dosya çıktısı oluşur.

Güvenliği sağlanmış dijital dokümana erişim uygulama mimarisi aşağıdaki adımlardan oluşmaktadır

1- Kullanıcı uygulamayı açar.
2- Görüntülenmek istenen doküman seçilir.
3- Biyometrik okuyucu sensör üzerinden biyometrik veri alınır.
4- Dokümanın içerisine biyometrik veri ile erişim talebinde bulunan kişinin biyometrik verisi ile karşılaştırılır.
5- Erişim yetkisi var ise şifrelenmiş görüntü çıktısı deşifre edilir.
6- Erişim yetkisi yok ise uyarı mesajı verilir.

Parmak izi veya Avuç damara izi sayısal verileri ile görüntülerin şifrelenmesi ve görüntünün içine veri gizlenmesi için kullanılan uygulama mimarisi Şekil 12’de gösterilmektedir.



Şekil 12. Uygulama Mimarisi

7.**SONUÇ VE ÖNERİLER**

Bu çalışmada, kullanım oranı hızla artan dijital dokümanların güvenliği Parmak izi biyometrik verisi veya avuç damar izi biyometrik verisi kullanılarak şifrelenmesi anlatılmıştır.

Bu bölümde iki biyometrik verinin şifrelemede kullanılmasıyla elde edilen sonuçları ele alınmaktadır.

Program ile yapılan test çalışmalarında değişik boyutlardaki 24 bit resimler karmaşık şifre algoritması kullanılarak şifrelenmiş, parmak izi veya avuç damar izi verileri ve dokümanın oluşturulma tarih saat bilgileri resmin içine gizlenmiştir.
Yapılan çalışmada gizlenmek istenen parmak izi verisi için farklı parmak izi sensörleri kullanılmış ve sensör cinsine göre parmak izi biyometrik verisinin 0,5-1 KB arası olduğu gözlemlenmiştir. Gizlenmek istenen Avuç damar izi biyometrik verisinin 2-3 KB arası olduğu tespit edilmiştir.

Biyometrik sayısal veri en önemsiz bite ekleme yöntemi kullanılarak resim içine gizlendiğin de resmin üzerinde gözle görünür bir bozulma olmadığı tespit edilmiştir.

Test amacıyla Windows 7 64 bit işletim sisteminde Intel i7 2.3 GHz işlemci ve 8GB ana belleğe sahip bilgisayar üzerinde çalıştırılmış ve Parmak izi veya Avuç Damar izi verisinin alınması dâhil şifreleme işleminin ortalama 2 saniye olduğu tespit edilmiştir.

Tablo 1 de, 24 bit renkli üç farklı bitmap resim için önce avuç damar izi sayısal datası kullanılarak şifreleme işlemi yapılmış ve süre ölçülmüştür. Aynı üç resim için parmak izi sayısal datası kullanılarak işlem tekrar edilmiş ve bu süreler karşılaştırılmıştır.

Bu uygulama ile birlikte resim dosyaları içerisine biyometrik veri saklanabileceğini, biyometrik veri ile birlikte bulut veya internet ortamında bulunan dosyaların ve içerisindeki verinin güvenliğini şifre gibi geleneksel yöntemler yerine bir üst güvenlik seviyesi olan biyometri kullanarak güvenliği arttırılabileceğini görmüş olduk.

Bu çalışma ile web ortamında dolaşan dijital dokümanların içeriğine yetkisiz kişilerce erişilmesini biyometrik olarak engelleyebilecek daha güvenli bir sistem çalışması sunulmuştur.

Tablo 1. Avuç damar izi ve Parmak izi ile şifreleme karşılaştırma tablosu

Resim	Resmin Boyutu	Şifrelenen Veri Boyutu [Byte]		Şifreleme Süresi [sn]	Şifre Çözme Süresi [sn]
Örnek1.bmp	2420X3464	Avuç Damar İzi	2393	2,6	2,5
		Parmak İzi	512	0,9	0,8
Örnek2.bmp	1976X1147	Avuç Damar İzi	2142	2,1	2,2
		Parmak İzi	480	0,6	0,6
Örnek3.bmp	1964X11101	Avuç Damar İzi	2215	2,0	1,9
		Parmak İzi	510	0,7	0,6

KAYNAKÇA

[1] Petitcolas F.A.P., Anderson R.J., Kuhn M.G., “Information Hiding–A Survey”, Proceedings of the IEEE,Special Issue on Protection of Multimedia Content, 87(7):1062-1078,July 1999.

[2]. Caldwell, 2nd Lt. J., “Steganography”, CROSSTALK The Journal of Defense Software Engineering, 25-27 (2003).

[3] Sellars D., “An Introduction to Steganography”, Student Papers, 1999. http://www.cs.uct.ac.za/courses/CS400 W/NIS04/papers99/dsellars/index.html

[4] Biyometrik Sistemler ve El Tabanlı Biyometrik Tanıma Karakteristikleri 6th International Advanced Technologies Symposium (IATS’11), 16-18 May 2011, Elazığ, Turkey.

[5] J. D. Woodward, Jr., N.M. Orlans, P. T. Higgins,—Biometricsǁ, McGraw-Hill, 2003.

[6] R. Brunelli, D. Falavigna, Person identification using multiple cues, IEEE Trans. Pattern Anal. Mach. Intell. 955–966, 1995.

[7] Andaç ŞAHİN, Ercan BULUŞ, M.Tolga SAKALLI - 24-BİT RENKLİ RESİMLER ÜZERİNDE EN ÖNEMSİZ BİTE EKLEME YÖNTEMİNİ KULLANARAK BİLGİ GİZLEME Trakya Univ J Sci, 7(1): 17-22, 2006 ISSN 1305-6468.

[8] CHANG C.C., Hwang M.S., Chen T.S.,2001, A new encryption algorithm for image cryptosystems, The Journal of Systems and Software 58 (2001) 83-91

[9] Erdal Güvenoğlu, Nurşen Suçsuz - Yer Değiştirme ve Değer Dönüştürme Özelliğine Sahip Görüntü Şifreleme Algoritmalarının Analizi - IX. Akademik Bilişim Konferansı Bildirileri 31 Ocak - 2 Şubat 2007 Dumlupınar Üniversitesi, Kütahya.

[10] ÖZTÜRK İ, Soğukpınar İ, 2004. Analysis and Comparison of Image Encryption Algorithms, IJIT Volume 1 Number 2 ISSN:1305 - 239X.

[11] Ayan, K. And Demir, Y. E. ”Öznitelik Tabanlı Otomatik Parmak İzi Tanıma” Eleco International Conference On Electrical And Electronics Eng., 2004

[12] Palm Secure, http://www.compactsecure.eu/ru/palmsecure-products/palmsecure-sdk.html, Erişim Tarihi: 29.10.2014.

[13] Parmak İzi Çözümleri, http://www.bersisteknoloji.com.tr/parmakizi.htm, Erişim Tarihi: 29.10.2014.

[14] Milyonlarca SGK'lının Avuç İçi İzi Alınacak, http://www.hport.com.tr/saglik/milyonlarca-sgk-linin-avuc-ici-izi-alinacak, Erişim Tarihi: 29.10.2014.

[15] Biyometri standardları, http://www.slidefinder.net/b/biyometri_bektas/13993600, Erişim Tarihi: 29.06.2014.

[16] Ergen, B. ve Çalışkan, A., 2011. Biyometrik Sistemler ve El Tabanlı Biyometrik Tanıma Karakteristikleri, 6th International Advanced Technologies Symposium (IATS'11), Fırat Üniversitesi, Elazığ, Turkey, 16-18 May.

[17] Yavuz Gözde, Plaka tanıma sistemi, Yüksek lisans tezi, Sakarya üniversitesi, Temmuz 2008.

[18] Yıldız, F. ve Baykan, N. A., 2011. Çapraz İlişki Metoduyla İris Tanıma, Selçuk Üniversitesi Teknik Bilimler Meslek Yüksekokulu Teknik-Online Dergi, 10, 19-37.

[19] Anatomy of the eye, http://www.retinasurgery.co.uk/anatomy.html, Erişim Tarihi: 29.08.2014.

[20] BILGISAYAR DESTEKLI KIMLIK TESPIT SISTEMLERINDE BIOMETRIK YÖNTEMLERIN DEGERLENDIRILMESI, http://ab.org.tr/ab03/tammetin/46.pdf , Erişim Tarihi: 19.08.2014.

[21] Veri ve Ağ Güvenliği http://k.domaindlx.com/kirbas/e_is/Veri_ve_Ag_Guvenligi.pdf , Erişim Tarihi: 19.08.2013.

[22] Dede, G. ve Sazlı, M. H., 2009. Biyometrik Sistemlerin Örüntü Tanıma Perspektifinden İncelenmesi ve Ses Tanıma Modülü Simülasyonu, EEBBM Ulusal Kongresi (Elektrik – Elektronik-Bilgisayar ve Biyomedikal Mühendisliği 13. Ulusal Kongresi ve Fuarı), 'Teknolojide Buluşuyoruz', ODTÜ, Ankara, 23-26 Aralık.

[23] Ses Tanıma, http://www.mcu-turkey.com/ses-tanima-3/, Erişim Tarihi: 29.08.2014.

[24] Yüz tanıma Sistemleri, http://www.teknoger.com/category/bilim, Erişim Tarihi: 24.09.2014.

[25] PARMAK DAMAR TANIMA TEKNOLOJİSİ YÜKSEK LİSANS TEZİ Songül ŞAN ELAZIĞ, 2013.

[26] Lyndon Baines Johnson Presidential Library and Museum, DNC Series II, Box 224 http://www.conelrad.com/daisy/documents.php , Erişim Tarihi: 22.09.2014.

[27] GÖRÜNTÜ STEGANOGRAFİDE KULLANILAN YENİ METODLAR VE BU METODLARIN GÜVENİLİRLİKLERİ Andaç ŞAHİN, Doktora Tezi, Edirne, 2007

[28] Popa R., "An Analysis of Steganographic Techiques", Ph.D Thesis, 1998.

[29] Sellars D., "An Introduction to Steganography", Online book, 1999.

[30] Johnson N.F, Jajodia S., "Exploring steganography: Seeing the Unseen", Computer, 31, no 2:26-34, February 1998.

[31] Johnson N. F., Jajodia S., "Stegananalysis of Images Created Using Current Steganography Software", Second Information Hiding Workshop held in Portland, Oregon, USA, April 15-17, 1998. Proceedings LNCS 1525, 273-289, Springer-Verlag, 1998.

[32] Steganografi'de İlke ve Yöntemler ve Küçük Siyah-Beyaz Görüntüleri için Bir Steganografi Yöntem Mir Mohammad Reza Alavi Milani, Sahereh Hosein Pour, Hüseyin Pehlivan,XIII Akademik Bilişim Konferansı Bildirileri(2011).

[33] Sağıroğlu Ş., Alkan,M.,"Her Yönüyle Elektronik imza(e-imza)",Grafiker,Ankara,3,5,33 (2005).

[34] Kaufman, C., Perlman, R., Speciner, M., "Network Security Private Communication in a Public World 2nd ed.", Prentice Hall, New Jersey,62-65,81-84,109,140-141 (2002).

[35] Yer Değiştirme ve Değer Dönüştürme Özelliğine Sahip Görüntü Şifreleme Algoritmalarının Analiz Erdal Güvenoğlu, Nurşen Suçsuz, IX Akademik Bilişim Konferansı, Kütahya, 2007.

[36] GUO J.I., Yen J.C., 1999, A new mirror like image encryption algorithm and its VLSI architecture, Department of Electronics Engineering National Lien-Ho College of Technology and Commerce.

[37] YEN J.C, Guo J.I,1999, A new ıimage encryption algorithm and its VLSI architecture, IEEE.

[38] RESİM İÇERİSİNDEKİ GİZLİ BİLGİNİN RQP STEGANALİZ YÖNTEMİYLE SEZİLMESİ Andaç ŞAHİN* , Ercan BULUŞ* , M. Tolga SAKALLI* ve H. Nusret BULUŞ*, IX Akademik Bilişim Konferansı, Edirne, 2007.

ÖZET

KELEŞ Mehmet Kıvılcım, Dijital Dokuman Güvenliğinin Farklı Biyometri Teknolojileri İle Sağlanması, Bilgisayar Mühendisliği Yüksek Lisans Tezi, İstanbul, 2014

Günümüzde fiziksel dokümanların saklanması, erişimi ve kullanım konularında çeşitli zorluklar vardır. Bilişim ve iletişim teknolojilerindeki gelişmeler fiziksel dokümanların dijital olarak saklanmasını gündeme gelmiştir. Sonuçta birçok kurum ve kuruluş dokümanlarını dijital ortama taşımıştır. Ancak dokümanların dijital ortama taşınması bu alandaki sorunları toptan çözmemiş, aksine yeni sorunların ortaya çıkmasına neden olmuştur. Dijital ortama taşınan dokümanların çalınması, yetkisiz kullanıcılar tarafından açılması ve içindeki bilgilere erişilmesi telafisi çok güç sonuçlar doğurabilmektedir. Bu durum dokuman gizliliğinin ihlali ve bilginin çalınması gibi durumlar doğurabilir. Bu çalışmada, dijital doküman oluşturulma aşamasında veya oluşturulduktan sonra biyometrik yöntemlerle nasıl güvenliğinin sağlanabileceği üzerinde durulmuştur. Çalışmada, avuç damar izi okuyucular kullanılarak oluşturulan biyometrik veriyi, dijital filigran yöntemi ile saklamak ve dokümanı bu şekilde şifreleme konusu ele alınmıştır. Çalışmada dijital bir doküman avuç damar izi teknolojisi kullanarak Steganografi yöntemi ile şifrelenmektedir. Doküman güvenliğinin sağlanması, erişimi ve ilk oluşturanın tespit edilmesi konusunda da, Parmak izi ve avuç damar izi teknolojileri karşılaştırılarak başarı oranları karşılaştırılmaktadır.

Anahtar Kelimeler: Doküman güvenliği, Dijital filigran, Şifreleme, Avuç Damar izi, Parmak izi

ABSTRACT

KELEŞ Mehmet Kıvılcım, DOCUMENT SECURITY BY USING DIFFERENT BIOMETRICS TECHNOLOGIES, Computer Engineering Master Thesis, İstanbul, 2014

Today, storage, access and usage of the physical documents present various difficulties. The emergences of information and communication technologies have enabled physical documents to be stored as digitally. As a result, many agencies and institutions have moved their physical documents to digital environment. However, transformation of documents to digital media did not solve the problems relating to document, but has led to the emergence of new problems. When these documents are digitized, unauthorized access to the information may present risky consequences. This situation may result in violation of secrecy and theft of information on the document. In this study, we will discuss how security can be achieved by using biometric methods during or after the creation of digital documents. In this study, we will cover the use of palm vein biometric data being used as a digital watermark, in order to secure the document with this encryption method. Also, we will analyze how palm vein data is used as steganography method for encryption and recognition technology in digital documents. These methods are used in providing security of the document for access, and also to identify the creator. Fingerprint and palm vein technologies are compared in regards to their success rates.

Key words: Document security, Palm Vein, Fingerprint, Watermarking, Biometry, Encryption**.**