KOCAELİ ÜNİVERSİTESİ * FEN BİLİMLERİ ENSTİTÜSÜ

GÖRÜNTÜ SIKIŞTIRMA VE İNTERNET ÜZERİNDEN GÜVENLİ AKTARIM SİSTEMİ

YÜKSEK LİSANS

Bilgisayar Müh. Kadir İMAMOĞLU

Anabilim Dalı: Bilgisayar Mühendisliği

Danışman: Yrd.Doç.Dr. Ahmet SAYAR

KOCAELİ, 2011

KOCAELİ ÜNİVERSİTESİ * FEN BİLİMLERİ ENSTİTÜSÜ

GÖRÜNTÜ SIKIŞTIRMA VE İNTERNET ÜZERİNDEN GÜVENLİ AKTARIM SİSTEMİ

YÜKSEK LİSANS TEZİ

Bilgisayar Müh. Kadir İMAMOĞLU

Tezin Enstitüye Verildiği Tarih: 17 Mayıs 2011

Tezin Savunulduğu Tarih: 09 Haziran 2011

Tez Danışmanı

Yrd.Doç.Dr. Ahmet SAYAR

(.....)

Üye

Doç.Dr. Hasan OCAK

(.....)

Üye

Yrd.Doç.Dr. İbrahim ÖZÇELİK

(.....)

KOCAELİ, 2011

ÖNSÖZ VE TEŞEKKÜR

Bilgisayarların son yıllarda birçok farklı amaç için kullanılabilir hale gelmesi, birçok alanda bilgisayar kullanımının inanılmaz bir biçimde artmasına neden olmuştur. Bilgisayar teknolojisindeki hızlı gelişmeler ve uygulama alanlarının çok çeşitli olması çeşitli sorunları da beraberinde getirmektedir.

Günümüzde çok yaygın olan gelişmelerden bazıları verinin, hızlı ve güvenli aktarımı olmuştur. Bu çalışmada farklı türdeki görüntü verilerinin İnternet üzerinden güvenli ve hızlı aktarımı üzerinde çalışılmıştır. Tez kapsamında geliştirilen uygulamada, Kocaeli bölgesinin çok boyutlu (bantlı) uzaktan algılama uydu verisi, İnternet üzerinden güvenli ve hızlı aktarım için yapılan testlerde kullanılmıştır.

Uzaktan algılama yöntemi ile kaydedilen geniş alanlara ait, çok boyutlu, tekrarlanabilir sayısal verilerden elde edilen uydu görüntüleri, daha çok yeryüzü kaynaklarının belirlenmesi, takibi ve analizleri gibi alanlarda kullanılmaktadır. İnternet üzerinden bu sayısal görüntü verilerine erişilmek istenildiğinde, görüntülerin bilgisayara indirilmesi dikkate değer bir zaman ve büyük miktarda bilgisayar belleğinin kullanımını gerektirmektedir. Ayrıca askeri, sağlık vb amaçlar için internet üzerinden yapılan sayısal görüntü aktarımlarında ciddi güvenlik tedbirlerinin alınması gereği ortaya çıkmıştır.

Bu tez kapsamında, İnternet üzerinden görüntü aktarımında ortaya çıkan hız, bilgisayar kapasitesi ve güvenlik sorunları ele alınmıştır. Bu sorunların çözümü için sayısal sertifikaların kullanıldığı "Güvenli Görüntü Aktarım Sistemi" geliştirilmiştir. Güvenli görüntü aktarımının daha hızlı olabilmesi için görüntüler, "Temel Bileşenler Analizi" ve "Dalgacık Tabanlı Dönüşüm" gibi sıkıştırma teknikleri kullanılarak kapladıkları alan azaltılmaya çalışılmıştır.

Tez konusunun ve çalışmanın ana hatlarının belirlenip hazırlanması aşamalarında bana her türlü desteği veren danışman hocam Sayın Yrd. Doç. Dr. Ahmet SAYAR' a ve her zaman bana destek olan aileme teşekkürü bir borç bilirim.

İÇİNDEKİLER

ÖNSÖZ VE TEŞEKKÜR i
İÇİNDEKİLER ii
ŞEKİLLER DİZİNİ iv
TABLOLAR DİZİNİ vi
SİMGELER VE KISALTMALAR LİSTESİ vii
ÖZET viii
İNGİLİZCE ÖZET ix
BÖLÜM 1. GİRİŞ 1
1.1. Tez Çalışmasının Amacı 2
1.2. Tez Çalışmasını Oluşturan Bölümler 3
BÖLÜM 2. TEMEL ANLATIMLAR 4
2.1. Güvenli Veri Aktarımı 4
2.1.1. Güvenli haberleşme bileşenleri 4
2.1.1.1. Güvenlik tehditleri 5
2.1.1.2. Güvenlik tedbirleri 7
2.1.1.3. Güvenlik yöntemlerinin karşılaştırılması 8
2.1.2. Şifreleme 8
2.1.3. Elektronik imza ve sayısal sertifikalar 9
2.1.4. Güvenilir bilişim 13
2.2. Görüntü Sıkıştırma 15
2.2.1. Dalgacık tabanlı sıkıştırma 17
2.2.2. Temel bileşenler analizi 23
BÖLÜM 3. BENZER ÇALIŞMALAR 27
3.1. Güvenli Veri Aktarımı İle İlgili Örnekler 27
3.1.1. Ülkemizdeki kamu kurumlarında e-imza kullanımı 27
3.1.2. Estonya'da avrupa parlementosu seçimlerinin e-seçim ile yapılması 28
3.1.3. Güvenli elektronik senet (e-senet) sistemi 29
3.1.4. Belediyelerde rol tabanlı sertifika kullanımı 30
3.1.5. Güncel güvenilir bilişim uygulamaları ve yaklaşımları 32
3.2. Görüntü Sıkıştırma İle İlgili Örnekler 34
3.2.1. Parmak izi görüntülerinin daha az bir alanda saklanması 34
3.2.2. Aşamalı veri iletimi 35
3.2.3. JPEG 2000 görüntü sıkıştırma standardı 36
3.2.4. Landsat görüntüsünün bantlar arası ilişkilerin azaltılarak sıkıştırılması 37
3.2.5. Kayıpsız görüntü sıkıştırma yöntemlerinin karşılaştırılması 39
BÖLÜM 4. MİMARİ YAPI VE UYGULAMA 40
4.1. Güvenli Görüntü Aktarım Sistemi 40
4.2. Görüntü Sıkıştırma Uygulaması 46
4.2.1. Dalgacık tabanlı dönüşüm yöntemi ile görüntü sıkıştırma 47
4.2.2. Temel bileşenler analizi yöntemi ile görüntü sıkıştırma 49
4.3. Güvenli Görüntü Aktarım Yazılımı (GGAY) 51
4.4. Test Senaryosu ve Sistemin Değerlendirilmesi 54

4.4.1. Dagacık tabanlı sıkıştırma yöntemi ile yapılan testler 54
4.4.1.1. Test senaryosu 54
4.4.1.2. Dalgacık tabanlı dönüşüm senaryosu test sonuçları 56
4.4.2. Temel bileşenler analizi yöntemi ile yapılan testler 60
4.4.2.1. Test senaryosu 60
4.4.2.2. Temel bileşenler analizi senaryosu test sonuçları 62
4.4.3. Gerçeklenen testlerin değerlendirilmesi 64
BÖLÜM 5. SONUÇ VE DEĞERLENDİRME 65
KAYNAKLAR 68
EKLER 72
ÖZGEÇMİŞ 124

ŞEKİLLER DİZİNİ

Şekil 2.1: Normal mesaj akışı 5
Şekil 2.2: Gizlilik ihlali 6
Şekil 2.3: Bütünlük ihlali 6
Şekil 2.4: Kimlik doğrulama ihlali 6
Şekil 2.5: İnkar edememezlik ihlali 7
Şekil 2.6: Süreklilik ihlali 7
Şekil 2.7: Açık anahtarlı imzalama 11
Şekil 2.8: Ünlü matematikçi Emmy Noether' in sıkıştırılmış görüntüleri 15
Şekil 2.9: Görüntü Verisi 16
Şekil 2.10: Dalgacık tabanlı sıkıştırmanın yapısı 22
Şekil 2.11: PCI' ın uygulanması 24
Şekil 2.12: PCI veri noktaları 26
Şekil 3.1: Bolonya belediyesi pilot projesinin sistem mimarisi 32
Şekil 3.2: FVC2000, parmak izi doğrulama yarışmasında kullanılan veri 35
Şekil 3.3: JPEG 2000' in uygulama alanları 37
Şekil 3.4: Landsat 7 uydu görüntüsünün bantları 38
Şekil 3.5: Şu anki katsayıların tahmini için adaylar 39
Şekil 4.1: Güvenli sıkıştırılmış görüntü aktarım sistemi temel çalışma yapısı 41
Şekil 4.2: Görüntü sıkıştırma adımları 42
Şekil 4.3: Güvenli Görüntü Aktarım Sistemi (GGAS) 42
Şekil 4.4: Güvenli görüntü indirme 43
Şekil 4.5: OpenSSL ile oluşturulan sunucu sertifikası 44
Şekil 4.6: Sayısal Sertifikalar ile Güvenli Görüntü Aktarım Sistemine giriş 45
Şekil 4.7: MATLAB' ta hazırlanan DTD yöntemi ile görüntü sıkıştırma programı . 47
Şekil 4.8: Dalgacık tabanlı sıkıştırma yapan Java paketinin oluşturulması 48
Şekil 4.9: PCA dönüşümü yapılan Landsat uydu görüntüsü 49
Şekil 4.10: PCA dönüşümü adımları 50
Şekil 4.11: PCA dönüşümünün çalışması 50
Şekil 4.12: PCA dönüşümünün çalışması 51
Şekil 4.13: Yönetim modülü giriş erkranı 52
Şekil 4.14: Yönetim modülü uydu görüntüleri listeleme ekranı 52
Şekil 4.15: Yönetim modülü kullanıcılar listesi ekranı 53
Şekil 4.16: Kullanıcı modülü uydu görüntüleri ekranı 53
Şekil 4.17: Dalgacık tabanlı sıkıştırma yöntemi test senaryosu 54
Şekil 4.18: DTD test senaryosunda kullanılan uydu görüntüsü 55
Şekil 4.19: Farklı ebatlardaki görüntülerin yüklenme zamanları 57
Şekil 4.20: Farklı ebatlardaki verilerin sıkıştırılma zamanları 57
Şekil 4.21: Farklı ebatlardaki verilerin indirilme zamanları 58
Şekil 4.22: Sıkıştırma işlemi öncesi ve sonrası verilerin boyutları 59
Şekil 4.23: Sıkıştırılmış ve sıkıştırılmamış görüntülerin indirilme zamanları 60
Şekil 4.24: Temel bileşenler analizi yöntemi test senaryosu 61
Şekil 4.25: TBA test senaryosunda kullanılan Landsat uydu görüntüsü 62

Şekil 4.26: Farklı bileşen sayılı görüntünün sıkıştırma ve indirme zamanları..... 63
Şekil 4.27: Temel bileşen sayısına göre indirilme zamanları 63

TABLOLAR DİZİNİ

Tablo 2.1: Güvenlik Yöntemlerinin Karşılaştırılması 8
Tablo 3.1: Landsat 7 uydusunda bantların dalga genişlikleri 38
Tablo 4.1: Tez_Contacts tablosu 46
Tablo 4.2: Tez_Images tablosu 46
Tablo 4.3: Tez_Users tablosu 46
Tablo 4.4: Farklı verilerin yüklenme, sıkıştırılma ve indirilme zamanları 56
Tablo 4.5: Farklı ebatlardaki verilerin sıkıştırılması 58
Tablo 4.6: Sıkıştırılmamış ve sıkıştırılmış görüntülerin indirilme zamanları 59
Tablo 4.7: Landsat görüntülerinin boyutları, sıkıştırılma ve indirilme zamanları 62

SİMGELER VE KISALTMALAR LİSTESİ

Kısaltmalar

AAA	: Açık Anahtar Altyapısı
AB	: Avrupa Birliği
ABD	: Amerika Birleşik Devletleri
AIK	: Attestation Identity Key
BPP	: Bit per pixel
CA	: Certificate Authority
DCT	: Discrite Cosinus Transformation
DWT	: Discrite Wavelet Transformation
EK	: Endorsement Key
EMSCB	: European Multilaterally Secure Computing Base
ESHS	: Elektronik Sertifika Hizmet Sağlayıcısı
EZW	: Embedded Zerotree Wavelet
FBI	: Federal Bureau of Investigation
GB	: Giga Byte
GGAS	: Güvenli Görüntü Aktarım Sistemi
HTTPS	: Secure Hypertext Transfer Protocol
IAIK	: Institute for Applied Information Processing and Communications
ISO	: International Organisation for Standardisation
ITU	: International Telecommunication Union
JPEG	: Joint Photographic Expert Group (Ortak Fotoğraf Uzman Grubu)
KB	: Kilo Byte
MÖ	: Milattan Önce
OpenTC	: Open Trusted Computing
PCA	: Principle Component Analyses (Temel Bileşenler Analizi)
PERMIS	: PrivilEge and Role Management Infrastructure Standards Validation
PCR	: Platform Configurator Registers
PKI	: Public Key Infrastructure
PKCS	: Public Key Cryptography Standards
RSA	: Rivest, Shamir, & Adleman
SRK	: Storage Root Key
SSL	: Secure Socket Layer
TB	: Tera Byte
TCG	: Trusted Computing Group
TCPA	: Trusted Computing Platform Alliance
TLS	: Transport Layer Security
TPM	: Trusted Platform Module
TSS	: Trusted Computing Group Software Stack
W	: Dönüşüm Matrisi
WBC	: Wavelet Based Compression
WWW	: World Wide Web

GÖRÜNTÜ SIKIŞTIRMA VE İNTERNET ÜZERİNDEN GÜVENLİ AKTARIM SİSTEMİ

Kadir İMAMOĞLU

Anahtar Kelimeler: Güvenilir Bilişim, Sayısal Sertifikalar, Güvenli Görüntü Aktarımı, Görüntü Sıkıştırma, Dalgacık Tabanlı Dönüşüm, Temel Bileşenler Analizi

Özet: Uzaktan algılama ve bilgisayar güvenliği konularında son yıllarda oldukça hızlı bir şekilde ilerlemeler kaydedilmiştir. Özellikle son 15 yılda uydularla uzaktan algılama, uyduların çözünürlüğünün yarım metre'nin altına inmesi ve maliyetlerin azalmasından dolayı ticari olarak daha yoğun kullanılmaya başlanmıştır.

Bilgisayar güvenliği konusunda, eskiden büyük şirketlerin kendi başlarına ürettikleri güvenlik çözümleri günümüzde yeterli olmamaktadır. Artık büyük şirketler ve araştırma yapan kurumlar bir araya gelip ortak çözümler üretmeye başlamışlardır. Ortak üretilen güvenlik çözümlerinden bir tanesi de güvenilir bilişim alanında yapılan çalışmalardır.

Uzaktan algılama ile elde edilen görüntülerin işlenip analiz edilmesi birçok yerde yaygınlaşarak kullanılmaktadır. Internet' in giderek yaygınlaşması ile beraber sayısal görüntü iletimi günümüzde önemli konulardan birisi haline gelmiştir. Belli kapasitede bant genişliğine sahip ağlardan sayısal görüntüleri daha hızlı iletebilmek için görüntü sıkıştırma algoritmalarına ihtiyaç duyulmaktadır.

Bu tez çalışmasında, İnternet üzerinden güvenli ve sıkıştırılmış görüntülerin hızlı aktarımı gerçekleştirilmiştir. Bu amaçla güvenli bir görüntü aktarım sistemi uygulaması geliştirilmiştir. Internet üzerinden görüntülerin güvenli bir şekilde aktarılmasında, sayısal sertifikalar ve güvenilir bilişim gibi yeni gelişen teknolojiler kullanılmıştır. Görüntü sıkıştırmada "Temel Bileşenler Analizi" ve "Dalgacık Tabanlı Dönüşüm" teknikleri kullanılarak görüntü verilerinin kapladığı alan azaltılmış ve sıkıştırılan bu görüntülerin İnternet üzerinden daha hızlı aktarımı sağlanmıştır.

IMAGE COMPRESSION AND SECURE TRANSMITTING SYSTEM OVER INTERNET

Kadir İMAMOĞLU

Keywords: Trusted Computing, Digital Certificates, Secure Image Transmission, Image Compression, Wavelet Based Transformation, Principle Component Analysis

Abstract: In recent years, many rapid developments in remote sensing and computer security have been made. Especially in the last 15 years, commercially using satellites for remote sensing has been increased intensively due to the decrease in the resolution of satellite images to half a meter and reduction in costs.

The existing security solutions for security related issues produced by several big companies for recent years are not adequate today. Now the big companies and research institutions have begun to come together to produce joint solutions. One of the common security solutions produced is in the field of trusted computing.

Processing and analyzing the images obtained by remote sensing is used increasingly in a wide range of places. As the internet is becoming popular and widespread all around the world, the transmission of digital images has become one of the important issues today. In order to send an image over a certain bandwidth capacity networks, digital images are compressed with image compression algorithms to increase the transmission rate.

In this thesis, secure and fast transmission of compressed images over the internet has been made. For this purpose, a secure image transmission application has been developed. In the secure transmission of images over the internet, new developing technologies such as digital certificates and trusted computing are used. By using "Principal Component Analysis" and "Wavelet Based Transformation" for compression of image, the disk usage of the image has been reduced which enables us to transmit these images over the internet faster.

BÖLÜM 1. GİRİŞ

Son yıllardaki hızlı gelişmeler ile bilgisayarlar, merkezi bilgi işleme birimlerinden artık her evde bulunan ve Internet bağlantısının olduğu kişisel bilgisayarlara dönüştüler. Günümüzde birçok kimse diz üstü bilgisayar, cep bilgisayarı veya cep telefonu taşımakta ve sanal olarak dünyanın geri kalanı ile gerçek zamanlı bağlantı halinde olabilmektedir. Bu bağlamda bizler toplumumuzun e-ticaret, e-iş ve e-devlet gibi bileşenler ile e-topluluğa dönüştüğüne şahit olmaktayız. Bütün bu yenilikler, bilgi sistemlerine olan bağlılığımızın arttığını göstermektedir. Bununla beraber bu gelişmeler, virüslerin yayılması, kesintileri, truva atları, hizmetleri devre dışı bırakan ataklar gibi birçok yeni zayıflıklar ve riskleri beraberinde getirmektedir.

Bilgi güvenliği sistemlerinde yapılan son araştırmalar beraberinde yenilikçi çözümler getirdi. Bu çözümlerden bazıları protokol ve algoritmalardaki (RSA, TLS, SSL, SHA1, MD5 gibi) şifreleme ile ilgili geliştirmeler, sayısal sertifikalar, güvenlik duvarları, virüslere karşı yazılımlar ve saldırı tesbit sistemleridir. Buradaki teknolojiler sayısal kimliklerin belirlenmesi, güvenli kanalların oluşturulması, bilinen virüslerin tesbiti ve ağ güvenliği için oldukça önemlidir. Yeni gelişen teknolojiler, ilk başlarda bilgi sistemlerini daha güvenli tutmasına rağmen, zaman geçtikçe bu sistemleri güvenliğinin sağanması zorlaşmaktadır. Belli bir zaman sonrada çok iyi bilinen güvenlik açığı saldırıları, güvenli olduğu düşünülen bu sistemlere yönelik hızla artmaya başlamaktadır [1].

Internet ağının tüm dünyada hızla yaygınlaşması bu ağ ortamında internet tarayıcıları üzerinde çalışacak İnternet tabanlı birçok değişik güvenlik uygulamasına olan ihtiyacı ortaya çıkarmıştır. Yeni geliştirilen uygulamaların internet tarayıcılarında çalışabilmesi sayesinde, kullanıcıların istedikleri platformda (Windows, Linux, Mac, UNIX, IPhone, Android, Windows CE vb.) çalışabilmelerine olanak sağlanmış oldu. Yani platform bağımsızlığı sağlanmış olmaktadır. Böylece İnternet ortamı için geliştirilen bu tür uygulamalar, hemen hemen İnternet'e bağlanan tüm kişilerin

kullanabilmesini mümkün kılmış oldu. Internet ağının ortaya çıkmasından önce geliştirilen uygulamalar genelde tek bir platformda çalıştıklarından fazla yaygınlaşamamışlardır.

Uydu teknolojilerindeki hızlı gelişmeler ve maliyetlerin azalması ile haberleşme ve uzaktan algılama gibi birçok alanda bu teknolojinin kullanımı yaygınlaşmıştır. Uydulardan elde edilen güncel görüntüler, gerçek zamanlı Coğrafi Bilgi Sistemleri oluşturulmasında kullanılmakta ve bu sistemler birçok kişi tarafınadan yaygın olarak kullanılmaya başlanmıştır.

Uzaktan algılama yöntemi ile elde edilen uydu görüntülerinin bilgisayarda kapladığı alan bazen çok büyük (GB' lar mertebesinde) olmaktadır. Dolayısı ile bu görüntülerin İnternet üzerinden bir noktadan başka bir noktaya aktarılması, bant genişliklerinin az olmasından dolayı çok zaman alabilmektedir. Buna ek olarak bazı gizlilik taşıyan uygulamalarda bu uydu görüntülerinin şifrelenerek güvenli bir kanal üzerinden sadece yetkili kişilere aktarılması gerekmektedir.

1.1. Tez Çalışmasının Amacı

Tez çalışmasında, İnternet üzerinde çalışan bir Güvenli Görüntü Aktarım Sistemi (GGAS) geliştirilmesi amaçlanmıştır. Burada görüntülerin güvenli aktarılması yanında daha hızlı nasıl aktarılabilineceği üzerinde de araştırmalar yapılmıştır. Uydu görüntüleri sıkıştırılarak daha az yer kaplamaları ve daha hızlı iletilebilinmesi amaçlanmıştır. Geliştirilen güvenli sistemde, sadece sayısal sertifikaları tanımlanan kullanıcıların, bu güvenli sistemde yer alan sıkıştırılmış uydu görüntülerine erişimlerinin sağlanması amaçlanmıştır.

Sonraki aşamada sıkıştırılan uydu görüntülerinin İnternet üzerinde güvenli bir şekilde nasıl aktarılabilineceği üzerine araştırma ve çalışmalar yapılmıştır. Uydu verilerini güvenli bir ortamdan aktarabilmek için istemci – sunucu mimarisine göre İnternet ortamında çalışan "Güvenli Görüntü Aktarım Sistemi" uygulaması geliştirilmiştir. Uygulamada aktarılan görüntülerin hızlı bir şekilde iletilebilinmesi için uydu görüntüsündeki bant sayısını azaltan "Temel Bileşenler Analizi" ve "Dalgacık

Tabanlı Dönüşüm" adlı yöntemler kullanılarak bu görüntülerinin sıkıştırılması gerçekleştirilmiştir.

Geliştirilen güvenli görüntü aktarım sistemi ile uydu görüntüleri güvenli bir şekilde sisteme yüklenip arşivelenebilinmekte ve bu yüklenen görüntülerine sadece yetkili kişiler erişilebilmektedirler. Sadece yetkili kişilere güvenli görüntü dağıtımı yapabilmek için sayısal sertifikaların kullanıldığı bir alt yapı geliştirilmiştir. Sistemde tanımlı kullanıcı ve görüntü bilgilerini, saklamak ve yönetmek için bir veritabanı alt yapısı tasarlanmıştır.

Kişilerin güvenliğini sağlayan sayısal sertifikalar, geliştirilen güvenlik sistemi tarafından her kullanıcı için ayrı ayrı oluşturulmaktadır. Oluşturulan bu sayısal sertifikalar, sistemi kullanacak kullanıcılara güvenli kanallardan imza karşılığında teslim edilmektedir. Sayısal sertifikası eline ulaşan kullanıcı bu sertifikayı kendisi için oluşturulan özel şifre ile internet tarayıcısına yükler. Daha sonra güvenli sistemin İnternet adresine güvenli bir şekilde TLS protkolü üzerinden (HTTPS) bağlanır. Sertifikası olmayan yada bu sistem tarafından tanımlanmamış bir kullanıcı, sisteme bağlanmaya çalıştığında erişim hatası meydana gelecektir.

1.2. Tez Çalışmasını Oluşturan Bölümler

Bu tez beş ana bölümden oluşmaktadır. Tezin birinci bölümü olan giriş bölümünde tez konusu hakkında genel bilgi verilmektedir. İkinci bölümde güvenli haberleşme, güvenilir bilişim, şifreleme teknikleri ve görüntü sıkıştırma ile ilgili temel anlatımlar yer almaktadır. Üçüncü bölümde literatür özeti ve şu anki durumun saptaması yapılmaktadır. Dördüncü bölümünde, tez kapsamında geliştirilen güvenli görüntü aktarım sistemi uygulaması anlatılmaktadır. Bu bölümde ayrıca görüntülerin aktarılması ve sıkıştırılmaları ile ilgili zaman, görüntü kalitesi ve boyut gibi alanlara göre yapılan performans analizleri yer almaktadır. Beşinci bölümde ise tez çalışmasının sonuç ve öneriler kısmı yer almaktadır.

BÖLÜM 2. TEMEL ANLATIMLAR

Bu bölümde tez çalışmasında kullanılan Güvenli Veri Aktarımı ve Görüntü Sıkıştırma konuları üzerinde temel anlatılmlar yer almaktadır. Güvenli Veri Aktarımı başlığı altında güvenli haberleşme, şifreleme, sayısal sertifikalar, elektronik imza ve güvenilir bilişim gibi konular yer almaktadır. Görüntü Sıkıştırma başlığında ise görüntü sıkıştırma yöntemlerinden, dalgacık tabanlı görüntü sıkıştırma ve temel bileşenler analizi yöntemleri ele alınarak anlatılmaktadır.

2.1. Güvenli Veri Aktarımı

Güvenli veri aktarımı bölümü, güvenli haberleşme, şifreleme, sayısal sertifikalar, elektronik imza ve güvenilir bilişim gibi konulardan meydana gelmektedir. Güvenli haberleşme bölümünde, güvenlik ile ilgili var olan tehditlerin bilinmesi ve bu tehditlere karşı alınması gereken tedbirlerden oluşur. Var olan farklı güvenlik yöntemlerinin bazılarıda karşılaştırılmıştır. Şifreleme bölümünde ise şifreleme ile ilgili temel bilgiler anlatılmaktadır. Sayısal sertifikalar başlığında kişisel, sunucu ve kök sertfikaları ile sertfikasyon işleminin nasıl gerçeklendiği anlatılmaktadır. Elektronik imza bölümünde, sayısal sertifikalar ile elektronik imzanın nasıl yapıldığı anlatılmaktadır. Son olarak güvenilir bilişim bölümünde yeni bir oluşum olan güvenilir bilişim platformu hakkında genel bilgiler anlatılmaktadır.

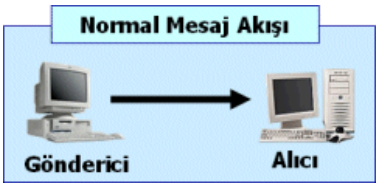
2.1.1. Güvenli haberleşme bileşenleri

İki tarafın güvenli bir şekilde haberleşebilmesi için, güvenlikle ilgili çeşitli beklentiler vardır. Bu beklentiler haberleşmenin temel bileşenleri olarak adlandırılır. Bu temel bileşenler gizlilik, bütünlük, kimlik doğrulama, inkar edememezlik ve haberleşmenin sürekliliğidir [2].

Gizlilik, taşınan bilginin içeriğinin gizli kalmasıdır. Günlük hayatta kullanılan mühürlü zarfı gizlilik için örnek olarak verilebilir. Bütünlük, taşınan bilginin içeriğinin yolda değiştirilememesini sağlar. Örnek olarak imza, barkod ve damgalama verilebilir. Kimlik doğrulama ile bilgiyi gönderen kişinin kimliğinin doğruluğundan emin olunur. Kimlik doğrulaması için günlük hayatta kullanılan noter, kimlik kartı ve trafik ehliyeti örnek verilebilir. İnkâr edememezlik özelliği, bilgiyi gönderen veya işleyen kişinin yaptığı işi sonradan inkar edememesidir. Buna örnek olarak imza, alındı ve onay gibi günümüzde kullanılan yazılı ifadeler verilebilir. Süreklilik bileşeni ise haberleşmenin kesintiye uğramadan yapılması sağlar. Günlük hayatta, haberleşmenin sürekliliğini sağlamak için farklı, birbirine alternatif iletişim yollarının kullanılması örnek olarak verilebilir.

2.1.1.1. Güvenlik tehditleri

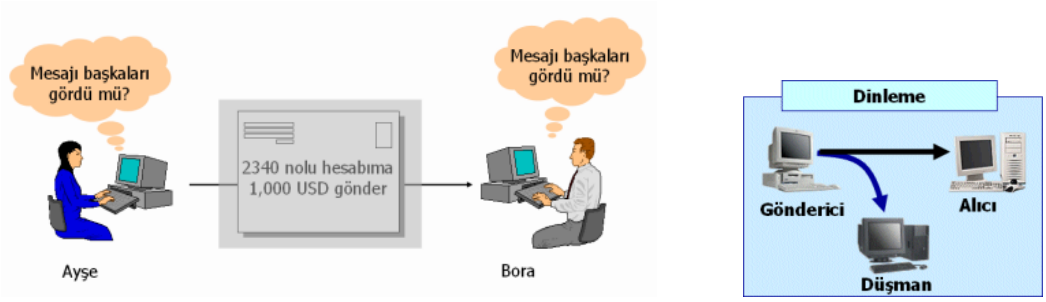
Haberleşen iki taraf; bilgisayar ağları, kablolu veya kablosuz iletişim kanalları kullanarak bir bilgi mesajını bir taraftan diğer tarafa Şekil 2.1' de gösterildiği gibi iletirler.



Şekil 2.1: Normal mesaj akışı

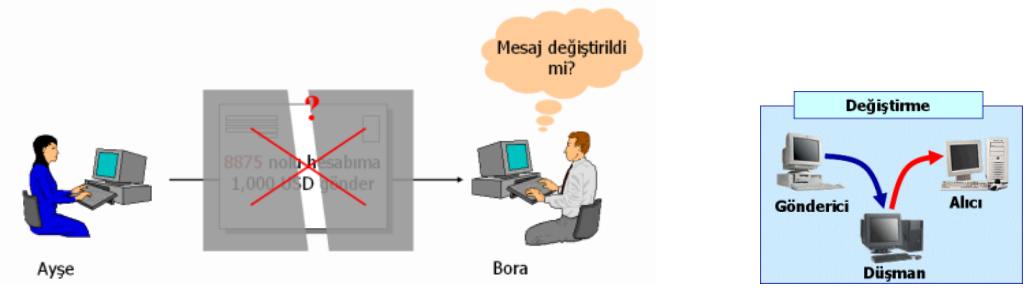
Elektronik ortamda haberleşen taraflar çeşitli güvenlik tehditleri ile karşı karşıya kalırlar. Bu güvenlik tehditleri gizlilik, bütünlük, kimlik doğrulama, inkar edememezlik ve süreklilik ile ilgili yapılan ihlallerdir. Bu ihlaller aşağıda sırası ile anlatılmaktadır [2].

Gizlilik İhlali: Haberleşme kanalını dinleyen saldırgan gönderici ile alıcı arasındaki mesaj trafiğini Şekil 2.2' de gösterildiği gibi dinleyebilir ve elde ettiği mesajları okuyarak bu haberleşmenin gizliliğini bozar. Bu tehdit, dinleme tehdidi olarak da bilinir.



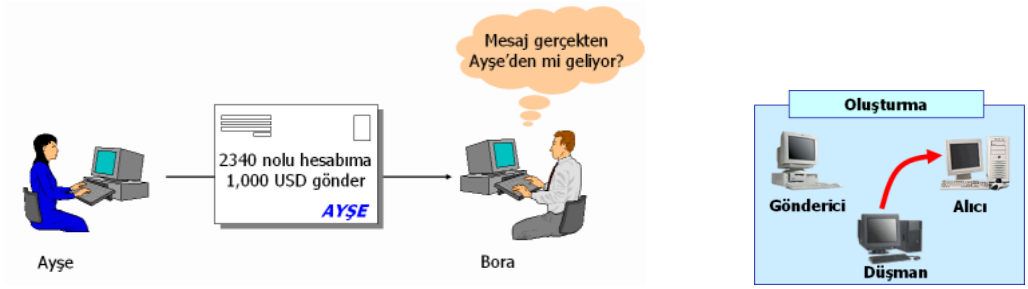
Şekil 2.2: Gizlilik ihlali

Bütünlük İhlali: Haberleşmeye müdahale edip göndericinin mesajlarını değiştiren saldırgan, alıcıya giden mesajı istediği şekle sokabilir. Şekil 2.3' de gösterilen bu tehdit mesajın bütünlüğünü bozan değiştirme tehdidi olarak da bilinir.



Şekil 2.3: Bütünlük ihlali

Kimlik Doğrulama İhlali: Saldırgan, alıcıya göndericinin kimliğini taklit ederek bir mesaj gönderebilir. Bu durumda eğer alıcı güvenilir bir kimlik doğrulaması yapmıyorsa Şekil 2.4' te gösterildiği gibi yanlış mesajlarla kandırılabilir. Bu tehdit oluşturma tehdididir.



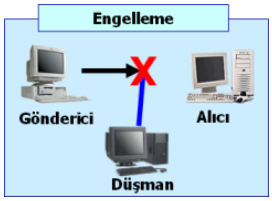
Şekil 2.4: Kimlik doğrulama ihlali

İnkar Edememezlik İhlali: Mesajı gönderen veya alan tarafın bu işi yaptığını inkar etmesi Şekil 2.5' de gösterildiği gibi söz konusu olabilir. Bu kötü niyetli girişimi boşa çıkaracak mekanizmalara ihtiyaç vardır.



Şekil 2.5: İnkar edememezlik ihlali

Süreklilik İhlali: Saldırgan, haberleşen iki taraf arasındaki hattı veya haberleşme araçlarını kullanılmaz hale getirerek haberleşmenin sürekliliğini Şekil 2.6' da gösterildiği gibi engellemeye çalışır.



Şekil 2.6: Süreklilik ihlali

2.1.1.2. Güvenlik tedbirleri

Elektronik haberleşmedeki tehditlere karşı yine bilgisayar ortamında güvenlik tedbirleri alınarak korunma sağlanabilir. Bu tehditlere karşı alınabilecek tedbirler ve kullanılabilecek yöntem ve araçlar aşağıda görülmektedir [2].

- Gizliliği sağlamak için veri şifreleme yöntemleri kullanılır.
- Bütünlüğü sağlamak için özetleme algoritmaları, mesaj özetleri, sayısal (elektronik) imzalar kullanılır.
- Kimlik doğrulaması için özetleme algoritmaları, mesaj özetleri, sayısal imzalar, sertifikalar kullanılır.

- İnkâr edememezlik için sayısal imzalar, işlem kayıtları kullanılır.
- Süreklilik için yedek sistemler, bakım, yedekleme, alternatif haberleşme kanalları kullanılır.

2.1.1.3. Güvenlik yöntemlerinin karşılaştırılması

Elektronik tehditlere karşı kullanılan yöntemlerden en önemli olanları anti-virüs programları, güvenlik duvarları, erişim denetimleri, şifreleme mekanizmaları ve açık anahtar altyapısıdır. Anti-virüs programları, CRC32 gibi "checksum" (bir çeşit özet) kullanarak bilgisayardaki programların kontrol dışı değiştirilip değiştirilmediğini kontrol ederler. Bu nedenle sadece bütünlük hizmetini verebilirler. Güvenlik duvarları, kimlik doğrulama yaparak belirli kaynaklara erişimi sınırlarlar. Bu nedenle sadece kimlik doğrulama ve gizlilik hizmetlerini sağlarlar. Şifreleme programları veya yöntemleri tek başlarına kullanıldığında sadece gizlilik hizmetini sağlayabilirler. Açık anahtar altyapısı; kimlik doğrulama, gizlilik, bütünlük ve inkar edememe hizmetlerini sağlayarak çok daha kapsamlı çözüm sunmaktadır. Bu güvenlik yöntemlerinin karşılaştırılmaları Tablo 2.1' de gösterilmektedir.

Tablo 2.1: Güvenlik Yöntemlerinin Karşılaştırılması

	Kimlik Doğrulama	**Gizlilik**	**Bütünlük**	**İnkar Edememe**
Anti-virüs			X	
Güvenlik Duvarları	X	X		
Erişim Denetimi	X	X		
Şifreleme		X		
Açık Anahtar Altyapısı	X	X	X	X

2.1.2. Şifreleme

Şifreleme, bir bilginin özel bir yöntemle değiştirilerek farklı bir şekle sokulması olarak tanımlanabilir. Şifreleme işlemi sonucunda ortaya çıkan yeni biçimdeki bilgi, şifre çözme işlemine tabi tutularak ilk haline dönüştürülebilir [2]. Şifreleme yöntemlerinde aranan bir takım özellikler vardır. Bu özellikler aşağıda listelenmiştir;

- Şifreleme ve şifre çözme işleminin zorluğu ihtiyaç duyulan güvenlikle doğru orantılı olmalıdır. Çok önemli olmayan bir bilginin şifrelenmesi için bilginin kendisinden daha fazla işgücü ve zaman harcanması verimli olmayacaktır.
- Anahtar seçimi ve şifreleme algoritması özel koşullara bağlı olmamalıdır. Şifreleme yöntemi her türlü bilgi için aynı şekilde çalışmalıdır.
- Sürecin gerçeklenmesi basit olmalıdır. Karışık bir sistemin gerçeklenmesi hem hatalara sebep olabilir hem de performans açısından tatmin edici olmayabilir.
- Şifrelemede yapılan hatalar sonraki adımlara yansımamalı ve mesajın tamamını bozmamalıdır. Haberleşme hattında meydana gelen bir hata bütün mesajın bozulmasına neden olmayacağı için bu özellik saldırılara karşı koruyucudur.
- Kullanılan algoritmanın karıştırma özelliği olmalıdır. Mesajın şifrelenmiş hali ile açık hali arasında ilişki kurulması çok zor olmalıdır.
- Kullanılan algoritmanın dağıtma özelliği olmalıdır. Mesajın açık hali şifreli hale gelirken içerdiği kelime ve harf grupları şifreli mesajın içinde olabildiğince dağıtılmalıdır.

Basit ve güvenli olmak üzere 2 çeşit şifreleme yöntemi vardır. Basit şifreleme yöntemleri, genellikle kâğıt kalem kullanılarak gerçekleştirilebilinen, çok karışık matematik temellere dayanmayan sistemlerdir. Basit şifreleme yöntemlerine Sezar Şifrelemesi örnek verilebilir.

Güvenli şifreleme yöntemleri elektronik sistemlerde kullanılır, ikili düzende saklanan ve taşınan bilgi üzerine uygulanır. Bu yöntem, klasik şifreleme yöntemlerinin zayıf yönlerini ortadan kaldıran ve kripto analize karşı dirençli olan algoritmalar ile gerçeklenir. Güvenli şifreleme yöntemlerine Simetrik ve Asimetrik şifreleme yöntemleri örnek olarak verilebilir. Basit ve güvenli şifreleme yöntemleri hakkında daha detaylı bilgi EK-E' de anlatılmaktadır.

2.1.3. Elektronik imza ve sayısal sertifikalar

Elektronik imza, 1970'lerin sonuna doğru asimetrik kriptografi kavramı ile ortaya çıkmış ve daha sonraları gelişecek olan internet gibi Dünya çapında yaygın

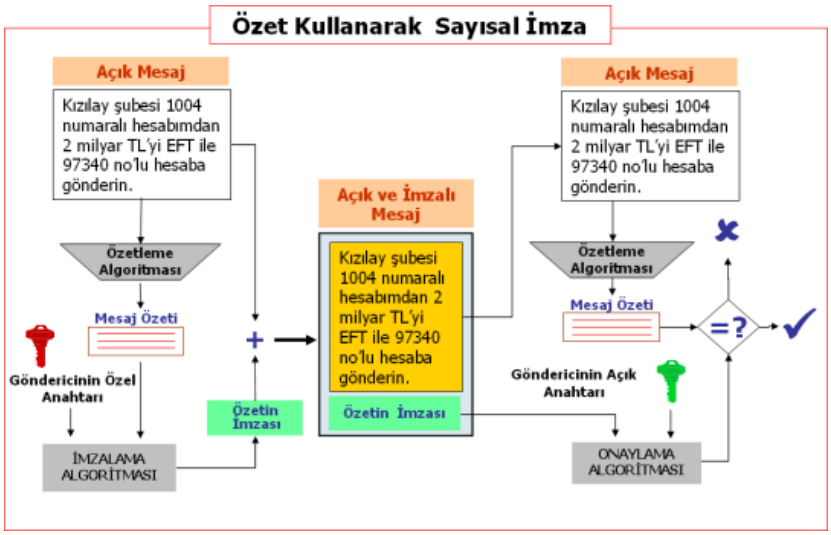
elektronik ortamlarda güvenli haberleşmenin önemli bir bileşeni olmuştur. Günümüzde elektronik imza bir takım kripto grafik algoritmalara ve özcük (hash) algoritmalarına dayanmaktadır. Elektronik imza ya da sayısal imza, başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veridir. Elektronik ortamlarda imza yerine kullanılabilen yasal kimlik doğrulama sistemidir. Bir bilginin üçüncü tarafların erişimine kapalı bir ortamda, bütünlüğü bozulmadan ve tarafların kimlikleri doğrulanarak iletildiğini elektronik veya benzeri araçlarla garanti eden harf, karakter veya sembollerden oluşur [3].

Elektronik imza, imzalanan metine göre farklılık gösterir ve içeriğin matematiksel fonksiyonlardan geçirilerek eşsiz olduğu düşünülen bir değer bulunması sureti ile elde edilir. Yani kişilerin, elle atılan imzada olduğu şekilde tek imzası yoktur; bunun yerine imzalamada kullanılan anahtarları vardır.

Elektronik imza için yaygınlıkla kullanılan yöntemlerin basında çift anahtarlı kriptografik yöntemler gelir. Çift anahtarlı bir kriptografik algoritmayla hazırlanan elektronik imza, hem gönderilen bilginin sayısal içeriğinin değiştirilmediğinin hem de gönderen tarafın kimliğinin ispatlanması için atılır. Gönderilecek mesajdan üretilen özetin sayısal içeriği ve gönderen tarafın kendi gizli anahtarına bağlı olarak oluşturulur

İmzalanacak mesaj öncelikle bir özet çıkarma (hash) algoritmasından geçirilir. Daha sonra bu mesaj özeti, imzayı atan kişinin gizli anahtarı kullanılarak çift anahtarlı kriptografik bir algoritmadan geçirilerek imza oluşturulur. Elektronik imza genellikle mesaja eklenerek karşı tarafa gönderilir veya saklanır. İmzayı oluşturma ve onaylama aşamalarının her ikisinde de kullanılan mesaj özeti, gönderilecek mesajdan matematiksel yollarla üretilen sabit uzunlukta sayısal bilgidir. Bu işlem özet fonksiyonu olarak bilinir. Özet fonksiyonları anlamsız ve sabit çıkış uzunluğu. Mesaj hangi uzunlukta olursa olsun MD5 fonksiyonu 128 bit uzunluğunda, SHA-1 fonksiyonu 160 bit uzunluğunda özet değeri üretir. Özet fonksiyonu geri dönüşümü olmayan bir fonksiyondur, diğer bir deyişle, herhangi bir mesajın özetine bakarak mesajın kendisini elde etmek mümkün değildir. Mesajdaki küçük değişiklikler bile

özette büyük değişikliklere yol açabilir. Ayni özeti veren herhangi iki farklı mesaj bulmak mümkün değildir. Böylelikle, her mesajın farklı bir özeti olması ve dolayısıyla mesajda yapılacak en ufak bir değişikliğin imzayı geçersiz kılması sağlanmış olur. Şekil 2.7' de mesaj özeti kullanarak açık anahtarlı imzalamanın nasıl yapıldığı anlatılmaktadır.



Şekil 2.7: Açık anahtarlı imzalama [3]

İmzalı mesajı alan taraf, gönderen tarafın açık anahtarını kullanarak mesajda en ufak bir değişikliğin olup olmadığını çok kısa ve hızlı çalışan bir imza doğrulama prosedürünü bilgisayarında çalıştırarak bulur. Elektronik imzanın doğruluğunu kanıtlamak için mesajı alan taraf, kendisine gelen mesajın ve elektronik imzanın sayısal içeriği ve gönderen tarafın açık anahtarını kullanır.

Alici taraf, gelen orijinal mesajdan yeniden elde edilen mesaj özetini, mesajla birlikte gelen elektronik imzanın, imzalayan kişinin açık anahtarıyla çözülmesinden elde edilen orijinal mesaj özetiyle karşılaştırılır. Bu özetlerin tıpatıp ayni olması, imzanın doğruluğunu gösterir.

Birçok kişi imzalı bir mesajı doğrulamak isteyebilir. Bu yüzden imzayı atan kişinin sertifikasının bu kişilere dağıtılmış olması gerekmektedir. Bunun için açık anahtarın içinde bulunduğu sertifika, imzalı mesajla birlikte alıcıya gönderilebileceği gibi, açık

anahtarlara ulaşım için en yaygın kullanılan yöntem sertifikaların herkesin ulaşabileceği dizin sunucularda tutulmasıdır.

Elektronik imza kriptogarfide bulunan temel birkaç işlevden birini sağlar. Bu temel işlevler iletilen mesajın gizliliği, mesajın bütünlüğü, tarafların kimliliğinin doğrulanması ve gönderilen veya alınan bir mesajın inkâr edilememesidir. Elektronik imza yalnız gönderilen mesaj inkârını önlemekle kalmaz, ayni zamanda imzaya ilişkin mesajın içeriğini de doğrular. Bir başka deyişle altında imza bulunan bir ıslak imzalanmış metin tahrifata açık olabilir ama sayısal imza ile bu mümkün değildir. Metindeki en küçük bir değişiklik anlaşılır ve imzayı geçersiz kılar [4]. Elektronik imza yaratma ve doğrulama prosedürü imzadan beklenen aşağıdaki gerekleri de yerine getirmektedir:

İmzalayanın doğrulanması: Açık ve gizli anahtar çifti güvenilir bir sertifika hizmet sağlayıcı tarafından onaylanmışsa, bu imzalayan kişinin kimliğinin doğruluğunu garanti eder. Söyle ki, elektronik imzanın yaratılması imzalayan kişinin gizli anahtarıyla yapılır. İmza doğrulama işleminin ise imzalayanın açık anahtarı dışında hile amaçlı başka birisinin açık anahtarını kullanarak yapılması kullanılan kriptografik algoritmaların matematiksel özeliğinden dolayı imkansizdir. Dolayısıyla kişinin gizli anahtarı ele geçirilmediği sürece elektronik imzanın başka birisi tarafından taklit edilmesi mümkün değildir. Bu bakımdan elektronik imza, kâğıt üzerindeki imzanın taklit edilme olasılığıyla karşılaştırıldığında daha güvenilirdir.

Mesajın doğruluğu: Elektronik imza, imzalanan mesajın başka bir şahıs tarafından değiştirilip değiştirilmediğini kâğıt üzerindeki imzadan daha kesin bir şekilde ortaya koyar. Çünkü onaylama prosedürü, mesajın bozulduğunu gelen mesajın özetiyle, imzalama sırasında oluşturulan orijinal mesaj özetini kıyaslayarak anlar.

Verimliliği: Kâğıt üzerindeki imzanın ispatı için uzun laboratuar çalışmalarının yapılmasının gerekliliğine karşın, elektronik imzanın doğrulanması daha önce de bahsedildiği gibi daha güvenilir ve çok kısa bir onaylama prosedürünün bilgisayarda çalıştırılmasıyla sağlanır.

Elektronik imzanın güvenliği ancak sahibinden başkasının gizli anahtarı kullanamamasının kesinleşmesiyle sağlanabilir. Çünkü çift anahtarlı kriptografi sisteminde güvenliğin sağlanması kişilerin gizli anahtarlarını iyi saklaması, açığa vurmamasına dayanır. Eğer bu şart sağlanmazsa gizli anahtarı elde eden başkaları kişinin adına imza atabilir. Gizli anahtarın başkalarının eline geçmesi durumunda bundan haberdar olan anahtar sahibinin yapması gereken, sertifikasını aldığı sertifika hizmet sağlayıcısına başvurarak sertifikasının geçerliliğini iptal etmesidir. Sertifika hizmet sağlayıcıları iptal edilen sertifikaları düzenli olarak oluşturdukları sertifika iptal listelerinde (SIL) yayınlarlar. Gizli anahtarın güvenli bir şekilde saklanmasının en iyi yöntemlerinden biri akıllı kart içinde tutmaktır. İmza programını, içindeki mikroçiplerde çalıştıran akıllı kartlar sayesinde imzalama işlemi sırasında gizli anahtar karttan dışarı çıkmaz. Kartın başka birisinin eline geçmesi olasılığına karşı da kart için ayrı güvenlik yöntemleri mevcuttur.

Türkiye'de 23 Ocak 2004 tarihli Resmi Gazete'de ilan edilen 5070 sayılı Elektronik İmza Kanunu'nda ve bu metinde geçen "elektronik imza" kavramı sayısal imzayı işaret etmektedir.

Sayısal sertifikalar, nüfus cüzdanı, ehliyet belgesi veya diğer kimlik belgeleri gibi kişinin internet üzerinde kimliğini ispatlaması için kullanılan elektronik dosyalardır. Başka bir deyişle kimliğin sayısal ispatıdır. Sayısal sertifikalar hakkında daha detaylı bilgi EK-F de yer almaktadır.

2.1.4. Güvenilir bilişim

Yeni gelişen teknolojiler sayesinde, bilgi sistemleri ilk başlarda daha güvenli olarak tutulabilinmekte ve bir süreliğine bu sistemlerin kırılması daha zor olmaktadır. Fakat belirli bir süre sonra iyi bilinen güvenlik açıklarına karşı saldırılar tekrar hızlı bir şekilde artmaya başlamaktadır [1]. Bu yeni saldırılar şirketlerin altyapılarında veya devletin sitelerinde ciddi zararlara neden olabilmektedirler. Bu durum CERT tarafından yayınlanan güvenlik vakaları raporlarından da anlaşılabilir. Örneğin 1992 yılında raporlanan güvenlik vakalarının sayısı 1000' den az iken 1999 yılında 10.000 civarına ve 2002 yılında 50.000 den büyük rakamlara ulaşmıştır.

Güvenlik vakalarının ana nedeni kullanıcı tarafında karmaşık geliştirme süreçlerinin olmasıdır. Buda karmaşık sistemlere güvenliği sağlamayı oldukça zorlaştırmaktadır. Güvenlik açıklıkları kodlardaki satır sayıları arttıkça artmaktadır. Bundan dolayı güvenlik sistemlerini oluşturmak gittikçe daha pahalı ve kullanımı daha zor olmaktadır.

Buradaki sorunlara çözüm olarak temel bir alt sistemin tanımlanması önerilmektedir. Bu alt sistemin ana fonksiyonlarını donanım üzerinden yüklenmektedir. Bunun gibi bir alt sistem karmaşık bir sistem için güvenin ana kaynağı olabilir. Güvenilir bilişim teknolojisinde bu alt sistem "güvenin kaynağı" diye adlandırılır. "Güvenilir" demek kişisel bilgisayarda çalışan yazılımların üçüncü taraflar tarafından güvenilmesidir ki bu bilgisayarda çalışan yazılımların sahibi tarafından değiştirilmediğini gösterir. Programlar birbirleri ile güvenilir bir şekilde iletişim kurarlar.

1970 ve 1980' li yıllar boyunca güvenilir bilişim konusunda yoğun araştırmalar yapılmıştır [5]. 1999 yılı ocak ayında "Trusted Computing Platform Alliance (TCPA)" önemli endüstri kuruluşları (Microsoft, Intel, IBM, HP ve AMD) tarafından kurulması ile bu konu dikkatleri üzerine çekmiştir. TCPA' nın ana amacı düşük maliyetli alt sistemler için güvenliği gerçekleştirmektir. Bu sıralarda bilgisayarların bir tanımlayıcıya sahip olup olmaması üzerine tartışmalar vardı [6]. TCPA, her "Trusted Platform Module (TPM)" içerisinde eşsiz bir tanımlayıcının yer almasını önerdi [7].

Şubat 2001 de TCPA tarafından belirlenen tanımlamaların 1.0 sürümü yayınlandı. Bu sayede, güvenli uygulama ve hizmetleri tasarlamak için gerekli temel blok yapısını ve kullanıcıya birçok özelliği sağladı. Bu özelliklerden bazıları verinin korumalı alanda saklanması, uygun olmayan yazılım tarafından veriye erişimin engellenmesi ve sistemde kurulan güvenin tanımlanmasıdır. İlk TPM yongası Nisan 2002 tarihinde tanıtıldı. TCPA, 2003 yılında araştırmalarına Trusted Computing Group (TCG) çatısı altında devam etme kararı aldılar. TCG' un ana amacı kullanıcıların önemli bilgilerini (veri, şifreler, anahtarlar vb) dışarından gelebilecek saldırılara ve hırsızlıklara karşı korumaktır. TCG, TCPA tarafından belirlenen tanımlamaları uyarladı ve burada belirlenen tanımlamaları değişik platformlarda

(PDA, sunucular, cep telefonları vb) kullanmak için geliştirecektir. TCG, yazılım ara yüz tanımlamalarını, geniş endüstri entegrasyonunda kullanacaktır [8]. TCG tanımlamaları, TPM yongasının oluşturulmasına katkıda bulunmaktadır [9].

Güvenilir platform modülü hakkında daha detaylı bilgi EK - G' de anlatılmaktadır.

2.2. Görüntü Sıkıştırma

Sayısal kameraların icat edilmesi ile beraber sayısal görüntülerin en çok kullanım alanları görüntü depolama, görüntü işleme ve aktarımıdır. Fakat görüntüleri oluşturan dosyalar bilgisayarın sabit diskinde fazla yer kaplayabilirler. 256x256 piksel ebatlarında olan gri ölçekli bir görüntünün saklaması gereken 65.536 adet eleman varken tipik 640x480 ebatlarındaki renkli bir görüntünün milyona yakın eleman bulunur [10].

İnternet üzerinden sayısal görüntülere erişilmek istenildiğinde, bu görüntüleri bilgisayara indirmek için dikkate değer bir zaman ve büyük miktarda bilgisayar belleğinin kullanımına ihtiyaç vardır. Görüntü sıkıştırma yöntemleri ile sıkıştırılan sayısal görüntülerin, depolanması ve bir yerden başka bir yere iletilmesi için daha az yere ve bant genişliğine ihtiyaç duyulacaktır [11].



Şekil 2.8: Ünlü matematikçi Emmy Noether' in sıkıştırılmış görüntüleri [12]

Birçok görüntünün yaygın olarak bilinen karakteristiği komşu piksellerin birbirleri ile ilişkili olmasıdır. Bundan dolayı görüntüde birbirleri ile daha az ilişkide olan yerlerin bulunması en önemli görevdir. Görüntü sıkıştırmanın temelinde gereksiz ve ilişkisiz olan kısımların azaltılması hedeflenmektedir. Görüntüde yer alan bazı tekrarlar ve insanlar tarafından fark edilemeyecek olan kısımlar silinebilir [12].



Şekil 2.9: Görüntü Verisi

Görüntü dosyalarının yapısı gereği içerisinde Şekil 2.9' de gösterildiği gibi ihtiyaç dışı ve gereksiz bilgiler bulunur. Bu bilgilerin boyutunun çok büyük olması sebebiyle aktarma ve saklama sorunları ortaya çıkar.

Sıkıştırma esnasında bu fazlalıklar atılırken orijinal bilgiden çok fazla uzaklaşmamaya özen gösterilir. Bu fazlalıkların nedenleri aşağıda anlatıldığı gibi uzaysal, spektral, anlık ve algılanabilen fazlalık olmak dört çeşittir.

Uzaysal fazlalık: Komşu pikseller arasındaki ilişkidir. Çoğu görüntülerde yan yana pikseller arasında keskin geçiş yoktur. Sıkıştırma yapmadan evvel, birbiriyle ilişkili pikseller (özellikle yan yana olanlar) tespit edilir.

Spektral fazlalık: Farklı renk bileşenlerinin birbirleriyle olan ilişkileridir. Renk bileşenleri farklı bile olsa çoğunlukla birbirleriyle ilişkilidir.

Anlık fazlalık: Video için birbirini takip eden çerçeveler arasındaki ilişkidir. Birbirini takip eden çerçeveler arasında çok büyük fark yoktur. Sadece hareket eden bölüm kadar fark vardır ve diğer bölümler genelde aynıdır. Sıkıştırma işlemi içerisinde bu aynı bölümler fazlalıktır.

Algılanabilen fazlalık: İnsanın görme sistemi her şeyi eşit olarak algılamaz. Uzaysal, spektral ve anlık kısıtlamalara bağlı kalarak görüntüde bazı gereksiz bilgiler atılabilir.

Bir görüntü içerisindeki gereğinden fazla ve önemsiz bilgiler, piksellerin birbirleriyle olan bağlılaşımıyla doğru orantılıdır. Dolayısıyla bu fazla ve gereksiz bilgiler ne kadar fazla olursa sıkıştırma oranı da o kadar fazla olacaktır. Sıkıştırılmamış

görüntülerin bazı dezavantajları vardır. Buna göre; sıkıştırılmamış görüntüler, çok fazla yer kaplarlar, aktarım için daha fazla bant genişliğine ve daha fazla zamana ihtiyaç duyarlar.

Sıkıştırmanın ana sebepleri (daha az yer kaplama, aktarımlarda daha az bant genişliği kullanma vb.) dışında bazı alt hedefleride vardır. Bu alt hedefler; işlemci ve bellek kullanımının en aza indirilmesi, aktarma hatalarının etkilerinin azaltılması, sıkıştırılmış versiyonun yazılım ve işlenmesinin desteklenmesi ve devam eden görüntü transferinin desteklenmesidir.

Sıkıştırmanın sınıflandırılması bazı bilim adamlarına göre farklılık göstermekle birlikte genel olarak kayıplı ve kayıpsız sıkıştırma teknikleri olmak üzere 2 çeşittir.

Kayıpsız sıkıştırmada, bilgi kaybı olmaz. Orijinal görüntü belli bir sure sonra istenirse tekrar elde edilebilir. Tıp görüntüleri ve arşivleme gibi alanlarda uygulanabilinmektedir. En çok bilinen kayıpsız sıkıştırma tekniği Huffman dır.

Kayıplı sıkıştırmada ise bilgi kaybı kabul edilebilir. Daha büyük oranlarda sıkıştırma yapabilmemize imkân verir. Başlıca uygulama alanları; ticari dağıtımlar (DVD) ve kayıpsız sıkıştırmanın yeterli sıkıştırma oranı sağlayamadığı yerlerde kısıtlı ortamlar oranlanır. Kayıplı sıkıştırma tekniğine ayrık kosinüs dönüşümü ile dalgacık tabanlı dönüşüm yöntemleri örnek verilebilir.

2.2.1. Dalgacık tabanlı sıkıştırma

Dalgacık dönüşümü yaklaşık 10-15 sene önce matematikçiler tarafından ortaya atılmış bir sinyal işleme tekniğidir. Tarihsel gelişim yönünden dalgacık analizi yeni kullanılmaya başlanmış bir yöntem olup, temeli Joseph Fourier'e kadar uzanmaktadır. Fourier dönüşümünün tersine, dalgacık dönüşümü ile her bir zaman aralığında sinyalin hem alçak hem de yüksek frekans bileşenlerini hesaplamak mümkündür. Bu yöntemle frekansı zamanla değişen sistemlerin analizi ve geçici durum analizleri hassas olarak yapılır [13].

Dalgacık serileri birçok farklı alana uygulanabilen bir yöntem olup, bunlar arasında uygulamalı matematik, sinyal işleme teknikleri, ses ve görüntü sıkıştırma teknikleri başta gelmektedir. Dalgacıklar ilk olarak Jean Morlet ve A. Grossman tarafından coğrafi bilgi sistemleri için kullanılmaya başlanmıştır. Gerçekte, dalgacıkların temel başlangıcı Joseph Fourier'e ve O'nun Fourier dönüşümüne kadar gitmektedir. 1807'den sonra Fourier denklemlerinin ortaya çıkmasıyla matematikçiler sinyali tanıma için frekans alanında çalışmaya yöneldiler. Dalgacıklar ilk olarak Haar dalgacık olarak adlandırılan Haar'ın tezinin ekler kısmında görülmüştür. Haar dalgacıklar bazı sınırlı uygulamalar için geçerli olup, bilinen en basit ve en eski dalgacık fonksiyonudur.

1977'lerde Esteban ve Galand yeni bir süzgeç kavramını ortaya attı ancak bu yolla ana sinyalin yeniden elde edilmesinde hata çok yüksekti. Dalgacık terimi ilk kez 1984'de Morlet ve Grossman tarafından kuantum fiziği çalışmalarında kullanıldı. 1987'de Mallat dalgacık ve süzgeç grupları arasındaki ilişkiyi ortaya çıkardı. Meyer kendi adıyla anılan ilk dalgacıkları ortaya attı. Bu Haar dalgacıkların aksine, sürekli uygulamalarda kullanılabilen bir fonksiyon idi. Yıllar geçtikçe, Ingrid Daubhecies bir takım dik tabanlı dalgacık serilerini ortaya atarak günümüzdeki birçok uygulamaya temel teşkil etmiştir. Tanım olarak, bir dalgacık, ortalama değeri sıfır olan ve zamanla sınırlı bir dalga şeklidir. Zaman ekseninde kaydırma ve ölçekleme parametreleri dalgacıkların temelini oluşturmaktadır [13].

Fourier serilerinin temel fonksiyonları sinüs ve kosinüs ifadelerinden meydana gelmektedir. Buna karşın çok sayıda dalgacık fonksiyonları vardır. Dalgacık dönüşümü değişik uzunluktaki bölgeleri kapsayan pencereleri içeren yeni bir teknik olarak karşımıza çıkmaktadır. Dalgacık metodu kullanarak bir sinyalin ayrıştırılması ve tekrar oluşturulması üç aşamadan oluşur. Bu aşamalar; ayrık wavelet dönüşümü kullanarak sinyalin bileşenlerine ayrılması, ortaya çıkan katsayıların eşik değer metotlarıyla yumuşatılması ve eşik değeri yapılmış ayrık dalgacık katsayılarından tekrardan orijinal sinyalin oluşturulması

Dalgacık tabanlı dönüşüm kodlamasında görüntü, bulunduğu boyuttan daha farklı bir boyuta aktarılır ve orada katsayılar kodlanır. Dönüşüm kodlaması sırasında görüntü

elemanları arasında bulunan ilişki azaltılmış olur. İlişki azaldığı zaman fazla bilginin devamlı kodlanmasına gerek kalmaz. Dönüşüm kodlamasının getireceği diğer bir avantaj ise görüntü enerjisinin büyük bir bölümünü daha küçük bir alana toplamasıdır. Bu özellik ile tüm katsayılar kullanılmadan kodlama yapılır [14].

Dalgacıklar, sayısal bilgileri (verileri) kodlamada kullanılan matematiksel bir yöntemi bize sağlar ve detayın seviyesine göre kademelere ayrılır. Bu kademeler bize veri aktarımının sürekli bir şekilde yapılmasını sağlarlar [15].

Dalgacık teorisinde iki boyutlu genişleme kümesi, tek boyutlu işaretleri zaman frekansında yerelleştirmek ve karakterize etmek için kullanılır. Fourier teorisindeki aynı ilkelere göre oluşturulmuştur. Dalgacık dönüşümü, sinyali ifade eden katsayıları bulmak için temel fonksiyonların bir kümesi ile iç çarpımları hesaplar. Bu bir lineer sistem olduğundan dolayı sinyal, temel fonksiyonların toplam ağırlıkları ile yeniden oluşturulabilir. Tek boyutlu Fourier'in temeli sadece frekansla sınırlandırılmıştır, fakat dalgacığın temeli iki boyutludur ve hem frekans hem de zaman ile sınırlandırılmıştır. Böylece bir sinyalin enerjisi genellikle birkaç dalgacık genişleme katsayısı ile ifade edilir.

Tek ölçekli fonksiyondan ya da dalgacıkların ölçeklenmesi ve dönüşümü ile oluşturulur. Çok çözünürlüklü koşulları sağlar. Bununla şu demek isteniyor. Eğer temel fonksiyonlar yarı genişlikte yapılmış ve genişliğinin yarısı kadar adımlar ile dönüştürülmüş ise onlar sinyallerin daha büyük bir sınıfı tam olarak ifade edeceklerdir ya da herhangi bir sinyal için daha iyi bir yaklaşım verebileceklerdir. DWT'nin etkin dönüşümü vardır. Düşük çözünürlüklü katsayılar, filter bankası diye bilinen bir ağaç yapısındaki algoritma ile daha yüksek çözünürlüklü katsayılar kullanılarak hesaplanabilir.

$$f(t) = \sum_{j,k} a_{j,k} 2^{j/2} \psi(2^j t - k) = \sum_{j,k} a_{j,k} \psi_{j,k}(t) \tag{2.1}$$

Yukarıda ayrık dalgacık dönüşümünüm formülü yer almaktadır. Burada iki boyutlu kümenin katsayıları $a_{j,k}$ dır.

k indeksi değiştikçe, dalgacıkların konumu ve ölçeklenmesi zaman ekseni boyunca hareket eder. j indeksi değiştikçe ölçeklerde dalgacıkların şekilleri değişir. Ölçek daha iyi oldukça (j daha geniş) zaman adımları daha küçük olur. Daraltılmış dalgacık ve daha küçük adımlar daha büyük çözünürlük ve detay ile ifade edilmesine izin verir.

Çoklu çözünürlük fikrini kullanabilmek için φ***(t)*** diye adlandırılan ölçek fonksiyonu dalgacık fonksiyonunu tanımlamak için kullanır.

$$\varphi.k(t) = 2^{j/2}\varphi(2^j t - k) \tag{2.2}$$

Fonksiyonların iki boyutlu ailesi esas ölçeklendirme fonksiyonundan ölçekleme ve dönüşüm yapılarak oluşturulur.

$$\varphi(t) = \varphi(t-k)\ k \in Z, \varphi \in L^2 \tag{2.3}$$

Değişik ölçekli fonksiyonların ölçekleri iç içedir ve biraz lineer cebir kullanarak yinelemeli ölçek fonksiyonu aşağıdaki gibi yazılabilir.

$$\varphi(t) = \sum_n h(n)\sqrt{2}\varphi(2\ t-n),\ n \in Z \tag{2.4}$$

Burada h(n) katsayıları, ölçeklendirilmiş katsayıları olan gerçel ya da karmaşık sayıların sıralı halidir. Ve kök iki ölçeklendirilmiş fonksiyonun standardını oluşturur.

Dalgacık fonksiyonu, kaydırılmış ölçek fonksiyonların ağırlıklarının toplanması şeklinde bazı h1(n) katsayıları için ifade edilebilir.

$$\psi(t) = \sum_n h_1(n)\sqrt{2}\varphi(2t-n),\ n \in Z \tag{2.5}$$

DWT' nin değişik karakteristiklerini gösteren beş çeşit gösterim vardır. Bu gösterimler aşağıdaki gibidir.

- Zaman alanı: Burada frekans ya da ölçekler hakkında bilgi verilmez.

- Üç boyutlu c(k), $d_j(k)$' nın j, k düzleminde çizimi.
- Zaman fonksiyonları, her ölçeğin k üzerinden toplanır. $f_j(t)$

$$f(t) = f_{j0} + \sum_j f_j(t) \tag{2.6}$$

$$f_{j0} = \sum_k c(k)\varphi(t-k) \tag{2.7}$$

$$f_j(t) = \sum_k d_j(k) 2^{j/2} \psi(2^j t - k) \tag{2.8}$$

- Zaman fonksiyonu olan $f_k(t)$ her dönüşümde k üzerinde toplanarak elde edilir.

$$f(t) = \sum_k f_k(t) \tag{2.9}$$

$$f_k(t) = c(k)\varphi(t-k) + \sum_j d_j(k) 2^{j/2} \psi(2^j t - k) \tag{2.10}$$

- Zaman ölçeği düzleminin bölünmesi eğer zaman dönüşüm indeksi ve ölçek indeksi sürekli değişken ise olabilir.

Dalgacık analizi çeşitli önemli yararları ortaya çıkarır. Bu yararlardan en önemlisi görüntü sıkıştırmadır. İlk başta koşulsuz temel nedene göre, genişleme katsayılarının ölçüsü birçok sinyaldeki j ve k kullanılarak düşürülebilir. Dalgacık genişlemesi daha doğru yerel açıklamalara ve sinyal özelliklerinin ayrılmasına izin verir. Sıkıştırma için DWT oldukça uygundur. İkinci olarak farklı dalgaların sonsuzluğu kişisel uygulamalara uygun tasarımlara izin verir.

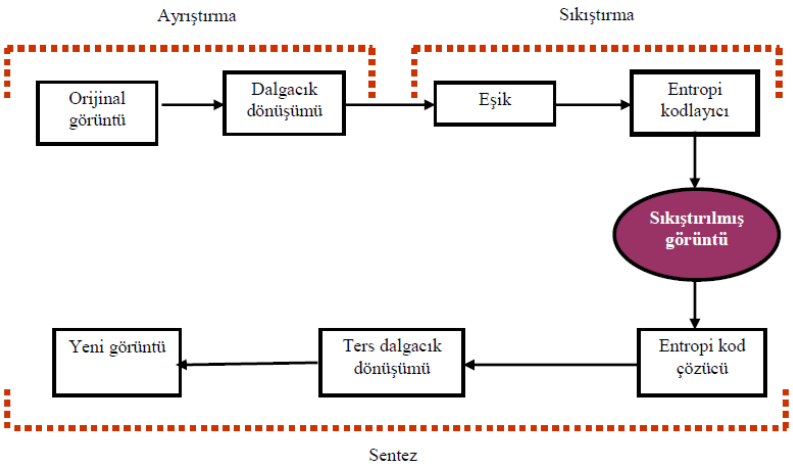
Ayrık kosinüs dönüşümü (DCT) kullanılarak yapılan sıkıştırma tekniğinde, görüntü önce bloklara ayrılır. Genellikle 8x8'lik olan bu bloklar oluşturulduktan sonra dönüşüm uygulanır ve kodlanır. Düşük sıkıştırma oranlarda iyi sonuç alınmasına rağmen, bu oran 1:50 civarında ve daha fazla olduğu durumlarda bloklar arası geçiş

tam olarak sağlanamadığından yeniden oluşturulan görüntüde bloklar açık şekilde belli olur.

Dalgacık tabanlı kodlamada ise görüntünün Ayrık Dalgacık Dönüşümü (DWT) alınarak kodlama yapılır. Dalgacık tabanlı sıkıştırmanın en önemli avantajı, yüksek sıkıştırma oranları elde edilmesidir. Böylelikle saklama alanı veya transfer bant genişliği yönünden oldukça avantaj sağlanmış olur. Dalgacık tabanlı sıkıştırmanın diğer avantajları şunlardır.

- Yüksek sıkıştırmalarda bloklama etkisi yoktur.
- Aktarma ve kodlama hatalarına karşı duyarlı olduğu gibi aktarmayı da kolaylaştırır.
- İnsanın görsel algılama sistemine daha fazla uyumluluk gösterir.
- Dönüşüm esnasında, görüntü işaretine değişik ölçekte defalarca dalgacıklar uygulandığı için yüksek sıkıştırma oranları elde edilebilir.
- Dalgacık dönüşümü, sıkıştırmadan önce etkili ayrıştırma sağlar.
- Dalgacık tabanlı sıkıştırma sistemi, görüntünün keskinleştirilmesi için parametrik kazanç kontrolü sağlar.
- Düşük bit hızlarında mükemmel çalışır.

Dalgacık tabanlı sıkıştırmanın temel yapısı Şekil 2.10' da gösterilmiştir.



Şekil 2.10: Dalgacık tabanlı sıkıştırmanın yapısı [15]

Dalgacık tabanlı sıkıştırmanın kullanılma nedenlerinden birisi görüntünün bloklanmaya ihtiyaç duyulmamasıdır. Diğer bir neden de dönüşüm hataları ile daha güçlü olurlar. Bir başka nedende görüntüdeki adım adım dönüşümü kolaylaştırır.

EK-D' de dalgacık tabanlı dönüşümü matrisler ile daha basit şekilde anlatan bölüm yer almaktadır.

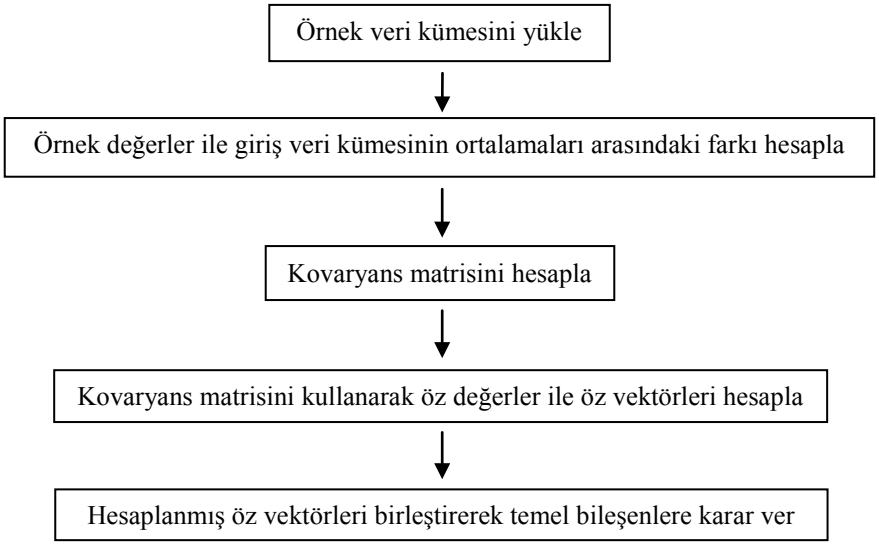
2.2.2. Temel bileşenler analizi

Temel Bileşenler Analizi (PCA) ' nin bir diğer adı Karhunen-Loeve metodudur [16]. PCA (Principal Component Analysis), görüntü tanıma, görüntü sınıflandırma ve görüntü sıkıştırma alanlarında kullanılan, bir değişkenler setinin varyans-kovaryans yapısını, bu değişkenlerin doğrusal birleşimleri vasıtasıyla açıklayarak, boyut indirgenmesi ve yorumlanmasını sağlayan, çok değişkenli bir istatistik yöntemidir. Çok boyutlu verilerde örüntü bulmak zor olduğundan PCA verilerin analiz edilmesinde çok güçlü bir araçtır [17]. PCA, orijinal verileri temel bileşen diye adlandırılan yeni verilere dönüştüren bir doğrusal dönüşümdür [18].

Bu yöntemde karşılıklı bağımlılık yapısı gösteren, ölçüm sayısı (n) olan (p) adet değişken; doğrusal, dikey (ortogonal) ve birbirinden bağımsız olma özelliklerini taşıyan (k) tane yeni değişkene dönüştürülmektedir. PCA, verideki gerekli bilgileri ortaya çıkarmada oldukça etkili bir yöntemdir. Yüksek boyutlu verilerdeki genel özellikleri bularak boyut sayısının azaltılmasını, verinin sıkıştırılmasını sağlar. Boyut azalmasıyla bazı özelliklerin kaybedileceği kesindir; fakat amaçlanan, bu kaybolan özelliklerin veri seti hakkında çok az bilgi içeriyor olmasıdır.

PCA yönteminin amacı, verinin çeşitliliğini daha iyi yakalayacak yeni bir boyut takımının bulunmasıdır. İlk boyut, mümkün olduğunca çok çeşitliği gösterecek şekilde seçilir. 2. Boyut, ilk boyuta dikey olacak şekilde ve yine mümkün olduğunca çok çeşitliliği gösterecek şekilde seçilir. PCA, çok boyutlu verileri sıkıştırmakta kullanılan, dönüşümü yapılmış verinin birbiri ile ilişkisinin olmadığı bir tekniktir. Bu dönüşüm sonucunda ortaya çıkan ilk bileşen en büyük değişimin olduğu bileşen iken sırası ile gelen diğer bileşenler azalan oranlarda değişime sahiptirler [19].

PCA, Şekil 2.11' de gösterilen akış diyagramında gösterildiği gibi çalışır. PCA, verinin boyutlarını azaltmayı sağlayan istatistiksel bir yöntemdir. Orijinal veriyi, temel bileşen diye adlandırılan yeni bir veriye dönüştüren doğrusal bir dönüşümdür. Her bileşen verinin farklı değişikliklerini içerir ve birbirleri ile ilişkisizdirler. Normalde ilk bileşen en büyük değişimi içerir. Birisi en büyük fark ile en yüksek uygun içerik bulunur. Bahsedilen yöntemde, birisi orijinal görüntünün 3 bandından daha fazla bilgi içerir.



Şekil 2.11: PCI' ın uygulanması

PCA yönteminin birkaç karakteristik özelliği vardır. Buna göre PCA' da verinin içindeki en güçlü örüntüyü bulmaya çalışır. Bu yüzden örüntü bulma tekniği olarak kullanılabilir. Çoğunlukla verinin sahip olduğu çeşitlilik, tüm boyut takımından seçilen küçük bir boyut setiyle yakalanabilir. Böylece PCA kullanarak yapılan boyut küçültme işlemleri, daha küçük boyutlu veri setlerinin ortaya çıkmasını sağlar ve böylece yüksek boyutlu verilere uygun olmayan teknikler bu yeni veri seti üzerinde rahatça çalışabilir. Verideki gürültüler, örüntülerden daha güçsüz olduklarından, boyut küçültme sonucunda bu gürültüler temizlenebilir. Bu özellik hem veri madenciliğinde hem de diğer veri analiz algoritmalarında özellikle kullanışlıdır.

PCA yönteminin çalışma yöntemi aşağıdaki 5 adımda anlatılmaktadır.

1. X piksel vektörünün m ortalama vektörünü hesapla

i = 1, 2, ..., N olmak üzere, $m = \frac{1}{N}\sum_{i=1}^{N} x_i$ (2.11)

2. Σ diye tanımlanan kovaryans matrisini hesapla

$$\Sigma = E\{(X-m)(X-m)^T\} \quad (2.12)$$

Burada $X = \{x_1, x_2, ..., x_N\}$ bir piksel matrisidir. E beklenti operator işlecidir ve T üs ifadesi transpozu ifade eder. Kovaryans matrisi aşağıdaki ifade ile bulunur.

$$E = \frac{1}{N}\sum_{i=1}^{N}(x_i - m)(x_i - m)^T \quad (2.13)$$

Aşağıdaki karakteristik denklemin çözümü kullanılarak kovaryans matrisinin Λ öz değerleri hesaplanır. Burada I matrisi NxN ölçülerinde özdeşlik matrisidir.

$$\Sigma - \lambda I = 0 \quad (2.14)$$

3. Öz değerleri aşağıdaki genel form biçiminde sırala;

$$\Lambda = \begin{bmatrix} \lambda_1 & 0 & 0 & . & . & . & 0 \\ 0 & \lambda_2 & 0 & . & . & . & 0 \\ 0 & 0 & \lambda_3 & . & . & . & 0 \\ . & & & & & & \\ . & & & & & & \\ . & & & & & & \\ 0 & 0 & 0 & . & . & . & \lambda_N \end{bmatrix} \quad (2.15)$$

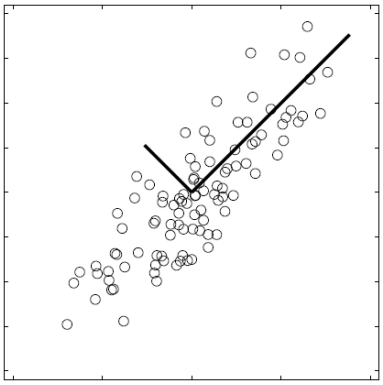
Burada $\lambda_1 > \lambda_2 > ... > \lambda_N$ şeklindedir. Giriş veri bantlarının sayısı ile öz değerlerin sayısı ile aynıdır. İlk öz değer olan λ_1 en büyük değişimi ve en büyük farkı içerir. Diğer öz değerler genelde çok daha küçüktür.

4. PCA görüntülerinin her temel bileşenini, orjinal görüntüdeki her pikseli kullanarak öz vektörleri aşağıdaki denklem ile oluştur.

$$Y = y_i = \sum_{j=1}^{N} a_{ij} x_j = a_{i1} x_1 + a_{i2} x_2 + \ldots a_{iN} x_N \tag{2.16}$$

Burada a_i değeri i = 1,2,..., N şeklinde olan bir öz vektördür. Spektral bantların her birinde uygun piksellerin verilen ağırlıkları toplamı PCA görüntüsündeki her pikselin yeni parlaklık değerini ifade eder.

Şekil 2.12' de gösterilen veri noktaları döndürülmüş dikey koordinat sisteminde gösteriliyor. Merkez veri noktalarının ortalamasıdır ve eksenler özvektörler tarafından oluşturulmaktadır.



Şekil 2.12: PCI veri noktaları [19]

Daha basit bir örnek ile PCA' ın uygulamalı anlatımı EK – C' de yer almaktadır.

BÖLÜM 3. BENZER ÇALIŞMALAR

Bu bölümde güvenli veri aktarımı ve görüntü sıkıştırma konuları ile ilgili yapılan literatür taramasısının özeti yer almaktadır.

Güvenli veri aktarımı ile ilgili belediyelerde sertifika kullanımı, ülkemizdeki kamu kurumlarındaki elektronik imza kullanımı, Estonya' daki elektronik seçim çalışmaları, güvenli elektronik senet alt yapı önerisi, güncel güvenilir bilişim uygulamaları ve yaklaşımları gibi konular üzerinde araştırmalar yapılmıştır.

Görüntü sıkıştırma konusunda ise FBI tarafından parmak izi verilerinin dalgacık tabanlı yöntemle nasıl sıkıştırıldığı, JPEG 2000 görüntü sıkıştırma standardı, Landsat görüntülerinde bantlar arasında ilişkinin azaltılarak sıkıştırılması, kayıpsız görüntü sıkıştırma yöntemlerinin karşılaştırılması ve aşamalı veri iletimi gibi konular ayrı başlıklar altında incelenmiştir.

3.1. Güvenli Veri Aktarımı İle İlgili Örnekler

3.1.1. Ülkemizdeki kamu kurumlarında e-imza kullanımı

E-imza kimlik doğrulama, gizlilik ve veri bütünlüğünü sağlayabilen alt yapısı ile gerçek hayatta ıslak imza ile yapılan her işin (kanunla hariç tutulanlar dışında: evlenme, tapu işlemleri, vb. gibi) e-ortam üzerinden güvenilir şekilde yapılabilmesini sağlamaktadır [20].

23 Ocak 2004 tarih ve 25355 sayılı Resmî Gazete'de yayımlanmış olan 5070 sayılı Elektronik İmza Kanunu'nda e-imza, başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri olarak tanımlanmıştır [21].

E-imza, tıpkı ıslak imzada olduğu gibi evrakla kişi arasında benzersiz bir ilişki kurar. İmzayı atacak kişiye özel anahtar ile birlikte imzalanacak olan belgenin, birtakım matematiksel işlemlerden geçirilmesi sonucunda oluşturulan ve imzalanacak veriye eklenen sayısal bir veri sayesinde sadece kişinin kimlik bilgisiyle değil ayrıca mesajın içeriği ile de ilişki kurar [22]. E-imza bilgilerin kolaylıkla silinip değiştirildiği e-ortam üzerinden gönderilen bir mesajın bir yerden bir yere giderken bozulmadan, değiştirilmeden, orijinal haliyle gitmesini sağlamada büyük rol oynamaktadır.

Ülkemizdeki kamu kurumlarında sayısal sertifikalar yardımı ile e-imza kullanımı gün geçtikçe artmaktadır. Sayısal sertifikalar e-imza' nın güvenilir ve geçerli olduğunu belirtir. E-İmza' nın kurumlarda kullanılabilnmesi için ek yazılımlara ihtiyaç vardır. Örneğin bir uygulamaya, e-imza özelliği vermek için o uygulamanın internet ortamına aktarılması ve e-imza ile entegreli çalışacak şekilde kodlanması gerekmektedir. E-sertifika sağlamak için bir Elektronik Sertifika Hizmet Sağlayıcısına (ESHS) başvurmak gerekmektedir. Kamu kurum ve kuruluşlarında kullanmaya yönelik sertifika başvuruları için yetkili kurum, TÜBİTAK'a bağlı Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü Müdürlüğüdür (UEKAE) [23].

Türkiye'de yürürlükte olan çok kullanıcılı pek çok e-imza uygulaması bulunmaktadır. Dış Ticaret Müsteşarlığı (DTM) bünyesinde yürütülen Dahilde İşleme Rejimi, Adalet Bakanlığı tarafından yürütülen UYAP bu konuda öne çıkan uygulamalardandır [24]. Ayrıca Bankacılık Düzenleme ve Denetleme Kurumu (BDDK), Çalışma ve Sosyal Güvenlik Bakanlığı, Devlet Demir Yolları işletmesi Genel Müdürlüğü (TCDD), Türkiye İstatistik Kurumu (TÜİK) gibi kurumlar hazırlıklarını yaptıkları veya test aşamasında olan projelerinde kullanmak üzere Kamu Sertifikasyon Merkezine e-sertifika başvurusunda bulunmuşlardır [25].

3.1.2. Estonya'da avrupa parlementosu seçimlerinin e-seçim ile yapılması

7 Haziran 2009 tarihinde Estonya, Avrupa Parlementosu seçimlerinde internet oylamasının kullanılmasına resmi onay vermiştir. Verilere gore bu oylamada

seçmenlerden %15'i geleneksel seçim yerine e-oylama'yı tercih etmiştir [26]. Oylamada kullanılan prosedür şu basamaklardan oluşmaktadır:

- Seçmen Kart okuyucusuna devlet tarafından kendine verilen kimlik kartını yerleştirip, ilgili web sayfasına bağlanır.
- Daha sonra kişi kimlik kartının PIN1 numarasını girerek kendini doğrular.
- Elektronik Oylama Sunucusu ilk etapta seçmenin oy kullanıp kullanamayacağını doğrular.
- İlgili doğrulama işlemleri başarı ile geçildiği takdirde seçmenin karşısına kendi oy vereceği bölge ile ilgili aday listesi çıkar.
- Seçmen tercihini yapar. Bu tercih şifrelenmiş bir şekilde aktarılır.
- Aynı zamanda seçmen tercihini bir de elektronik imzası ile doğrular. Bu işlem esnasında PIN 2 numarası kullanılır.
- Oy sayımı esnasında kişilerin elektronik imzaları anonimliği sağlamak adına kaldırılır. Yüksek seçim kurulu anonim elektronik oyları birlikte açar ve sayım işlemini tamamlar.

E-seçim sistemi Estonya' da 2002 yılından beri geliştirilmeye devam edilmektedir. Bu sistem ilk kez 2005 yılında belediye meclisi seçimlerinde kullanılmıştır. Dünya tarihinde ilk kez parlamento seçimleri İnternet üzerinden 2007 yılında Estonya' da gerçekleşmiştir.

3.1.3. Güvenli elektronik senet (e-senet) sistemi

Günümüz internet ortamında insanlar çeşitli belgelerini sayısal imza ile imzalayıp elektronik olarak iletebilmekte ve saklayabilmektedirler. Ülkemizde internet ortamına henüz taşınmayan uygulamalardan birisi de senet sistemidir. Klasik olarak insanlar borçları için bir senet kağıdı satın alıp bunu doldurup, imzalayıp, alacaklı kişiye teslim etmekte ve senetin vadesi gelince borçlarını ödemektedirler [27].

Bu araştırmada kağıt ortamındaki senet alışverişinin elektronik ortamda e-senet olarak güvenli bir şekilde gerçekleştirebilmesi için bir sistem önerilmektedir. Burada önerilen sistem, klasik sistemden daha güvenli, ve kullanımı her ilgili için daha esnek

ve kolaydır. Önerilen sistem XML sayısal imza kullanımı, standart kriptografik ve özcük algoritmalar, geliştirilen tekil kod ve protokol dizisinden oluşmaktadır. Bu sistemde e-senedin insanlar ve şirketler arasında alışverişinin en az kağıt tabanlı sistemdeki kadar veya daha fazla güvenlik ve kolaylık sağlanarak nasıl yapılacağı anlatılmıştır. Önerilen sistemde banka ve noter gibi özel kurumların durumları dahil edilmemiştir, sadece gerçek ve tüzel kişiler (insanlar ve şirketler) arasındaki senet alışverişi anlatılmıştır. Çünkü günlük hayatta bankalar ve noterler senet oluşturmazlar.

Bu bildiride sayısal imza ve XML standardı kullanılarak kağıt tabanlı senet alışverişinin internet ortamında yapılabilmesi için bir takım protokoller ve sistem geliştirilmiştir. E-senet olarak anılan bu sistem kağıt temelli senetten daha güvenli ve kullanışlıdır. Yapılan çalışmada senedin elektronik ortamda XML kullanılarak nasıl saklanacağı anlatılmıştır. Önerilen XML veri yapısında senet kullanıcılarının sayısal imzalarının XML sayısal imza standardı kullanılarak nasıl saklanacağı ve aynı şekilde nitelikli sertifikaların da nasıl bu yapı içinde olacağı anlatılmış ve son olarak e-senedin internet üzerinden senet kullanıcıları arasında alışverişinin nasıl olacağını belirleyen protokoller tanımlanmıştır.

3.1.4. Belediyelerde rol tabanlı sertifika kullanımı

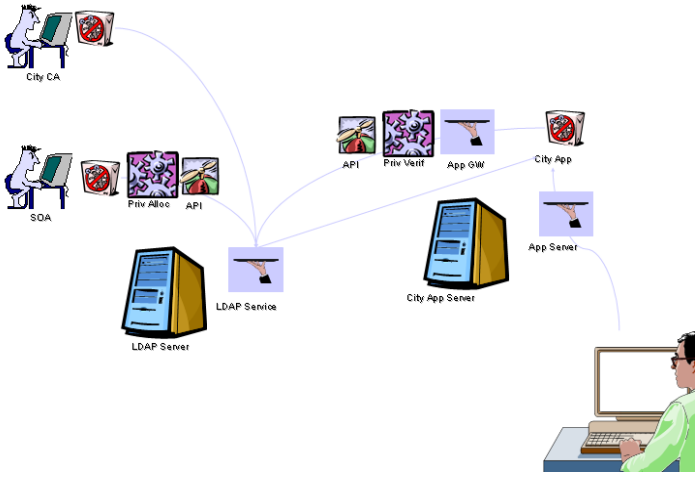
Avrupa Birliği tarafından desteklenen PERMIS (PrivilEge and Role Management Infrastructure Standards Validation) projesi kapsamında, ITU X.509 özellik sertifikalarını kullanan rol tabanlı bir erişim kontrol alt yapısı geliştirilmiştir [28]. Bu projede, bir İnternet uygulamasına erişen kullanıcıların uygulama üzerinde neler yapabileceklerini tanımlayan kullanıcı erişim hakları yönetimi sistemi geliştirilmiştir. O zamanlar bu amacı gerçekleştirmek standart bir çözüm bulunmadığı belirtilmektedir. Bu proje ile kullanıcıların, sayıları çok fazla olan şifrelerini hatırlamak zorunda kalmayacakları, daha iyi seviyede bir güvenlik ortamına sahip olacakları ve İnternet üzerinde gerçekleştirecekleri işlemlerin yasal olacağı belirtilmektedir.

Proje kapsamında üç bölge için pilot uygulamalar geliştirilmiştir. Bu pilot uygulamalar aşağıdaki gibidir [29].

- Sayısal Haritacılık: İtalya' nın Bolonya belediyesi, tüm şehir planlarını oluşturulan bu sistem ile tanımlı mimarların erişimine açtığı belirtilmektedir. Mimarlarda kendilerine verilecek olan sayısal sertifikalar yardımı ile bu sisteme giriş yapıp yeni bina plan onay talebini yapabileceği belirtilmektedir.
- E-teklif Projesi: İngiltere' nin Saltford belediyesi için gerçeklenen projede, sadece tanımlı tedarikçilerin internet üzerinden güvenli uygulamaya erişim izninin verildiği, bu uygulama üzerinden de bire bir teklif alındığı belirtilmektedir.
- Araba Kiralama Cezaları: Araba kiralama şirketleri kendi arabalarına kesilen cezaları belediyeden alıp, ceza kesilen araçta o gün hangi sürücünün olduğu belediyeye bildirileceği belirtilmektedir. Bu sistem için araba kiralama şirketlerine belediye tarafından sertifikalar dağıtılacaktır.

Bolonya belediyesi için geliştirilen projede, mimarların şehrin cadde ve sokak harita planlarını indirebilmelerine izin verilmek isteniyor. Mimarlar indirdikleri bu planları kullanarak yeni binalar için hazırladıkları planları şehir planlama ofisindeki sunuculara yüklerler ve bina lisansları için istekte bulunurlar. Mimarların bu sisteme güvenli bir şekilde erişip işlem yapabilmeleri için belediye tüm mimarlara sayısal sertifikalarını dağıtıyor. Mimarlarda sertifikalarını kullanarak sisteme güvenli bir şekilde giriş yapabileceği belirtilmektedir. Pilot projenin sistem mimarisi Şekil 3.1 de gösterilmiştir.

PERMIS projesi kapsamında geliştirilen bu uygulama ile eskiden kullanılan sistemi oldukça iyileşeceği belirtilmektedir. Bolonya'daki pilot projesi öncesinde planlar ve istekler belediyeye kağıt dökümanlar şeklinde posta kullanılarak gönderilmekdir. Evrakların posta ile şehir planlama ofisine ulaşması ve onaylanması işlemi için epey zaman gerektiği belirtilmektedir.



Şekil 3.1: Bolonya belediyesi pilot projesinin sistem mimarisi [30]

PERMIS projesi, AB tarafından EC ISIS programı kapsamında %50 oranında desteklenmiş ve EPSRC' den GR/M83483 nolu desteği almıştır. Proje, Bolonya Belediyesi koordinatörlüğünde, İtalya, İspanya ve İngiltereden 10 ortağın (Comune di Bologna, Engineering, BNL Multiservizi, City of Salford, University of Salford, TrueTrust, IMI, COCINB, LOCALRET ve SafeLayer) katılımıyla 1 Ocak 2001 – 31 Eylül 2002 tarihleri arasında gerçekleştirilmiştir.

3.1.5. Güncel güvenilir bilişim uygulamaları ve yaklaşımları

Günümüzde TPM yongasını kullanan çok az sayıda uygulama vardır. TPM den başka değişik güvenlik çözümleri de yer almaktadır. Bunlardan bazıları güvenlik duvarları, güvenlik yazılımları, kripto grafik hızlandırıcılar / yardımcı işlemciler ve güvenlik protokolleridir. Güvenlik çözümleri ile ilgili diğer yazılımlar gömülü yazılımlar, açılış bütünlük hizmetleri (Intel), Microsoft' un kendi işletim sistemlerindeki güvenlik hizmetleri, Java uygulamalarında kullanılan sandbox' lar, akıllı kartlar, parmak izi, biometrik, açık anahtar altyapısı ve sayısal imzadır. Tam bir güvenlik için burada belirtilen çözümlerin çoğu yetersizdir.

TPM ile ilgili özellikle son zamanlarda oraya çıkan açık kaynak kodlu, değişik proje çalışmalarını görmekteyiz. Bu projelerden bazıları, TPM emulator, TrouSers, Turaya, jTSS Wrapper ve Trusted GRUB dır. Aşağıdaki bu projeler anlatılmaktadır.

TPM Emulator, Linux altında yazılım tabanlı TPM yongasının simülasyonunu TCG tarafından belirtilen tanımlamalara göre yapar. Böylece eğitim ve deneme çalışmaları için TPM yongasına sahip olmayan kişilerin TPM yongasının özelliklerini test etmek imkanına kavuşmuş olmaktadır [31].

TrouSerS, Trusted Computing Group Software Stack (TCG TSS) tarafından tanımlanan uygulama projesidir [32]. Şu anda TSS 1.1 sürümü ile uyumludur. TrouSerS TSS uygulaması, RSA anahtar çiftlerinin üretilmesinde, RSA imzalama / doğrulama, verilerin bilgilerinin TPM içerisindeki PCR larda saklanması, belirli bir andaki PCR değerlerine göre verinin mühürlenmesi, rasgele sayı üretimi ve RSA anahtarlarının saklanmasında kullanılır. Uygulamalar TPM yongasına erişirken TrouSerS uygulamasını kullanırlar.

Güvenilir bilişim platformu sanallaştırma mimarisinden de yararlanır. İşletim sistemi sanal makine monitorü (hypervisor) içerisinde saklanır ki aynı anda birden fazla işletim sistemi bağımsız olarak çalışabilir. Buradaki sanal makineler birbirlerinden bağımsızdırlar. Hypervisor' un ana görevi bütün sanal makinelerin güçlü bir şekilden birbirlerinde izole edip bağımsız çalışmalarını sağlamaktır.

Sanallaştırılmış açık kaynak sistemlerinde TPM yongasını kullanan ilk TPM uygulaması örneği Turaya mimarisidir. Turaya, European Multilaterally Secure Computing Base (EMSCB) tarafından geliştirilmiştir [33]. Güvenilir bilişim özelliklerini destekleyen "Turaya.Crypt" ve "Turaya.VPN" olmak üzere iki modüle sahiptir. Turaya.VPN güvenilir iletişim istemcisidir ve kullanıcıya tamamen saydamdır. Turaya.Crypt sürücü şifreleme sistemidir ki sabit diskler ve USB bellekler için şifreleme imkanı vermektedir.

jTSS Wrapper, Java geliştiricilerinin Java üzerinden TPM yongasında güvenilir bilişim özelliklerine ve hizmetlerine erişmek için kullanılır [34].. Bu uygulama IAIK (the Institute for Applied Information Processing and Communications) tarafından geliştirilmekte ve OPEN TC (Open Trusted Computing) adlı AB projesi tarafından desteklenmektedir [35].

Trusted GRUB orijinal GNU GRUB açılış yükleyicisinin bir uzantısıdır [36]. TCG tarafından tanımlanan TPM özelliklerine destek sağlamak için üzerinde değişiklikler yapılmıştır. Trusted GRUB' ın ana özelliği istenen dosyaların açılış sürecinde ölçümlerinin yapılıp TPM içerisinde yer alan PCR kayıtçıları içerisine koyabilmesidir.

Günümüzde birçok ülke güvenilir bilişim üzerinde çalışmalarını yoğunlaştırmaktadır. Özellikle Almanya, ABD, Japonya ve Yeni Zelanda bu konuda çalışmalar yapmaktadırlar. ABD de savunma bakanlığı bilgisayar alımlarında ana kart üzerinde TPM yongasının bulundurulmasını zorunlu kılmıştır. Almanya ise açık kaynak sistemleri üzerinde güvenlik araştırmaları için özellikle son 10 yıldır büyük miktarda kaynak ayırarak araştırma şirketlerine destekler vermektedir.

Güvenilir bilişm gelecekte birçok alanda daha yaygın olarak kullanılacaktır. Bu kullanım alanlarından birisi masaüstü yada diz üstü bilgisayarların çalınması durumudur. Sistem içerisinde yer akan güvenilir bilişim alt yapısı sayesinde hırsızların verilere ulaşması engellenecektir. Diğer bir kullanım alanıda, işletim sistemi için uygun olmayan, bilinmeyen programların sertifikalar kullanılarak tesbit edilip kurulmalsının engellenmesidir. Böylece virus, solucan ve ileride ortaya çıkabilecek zayıflıkların sisteme bulaşması engellenmiş olunacaktır [37,38].

3.2. Görüntü Sıkıştırma İle İlgili Örnekler

3.2.1. Parmak izi görüntülerinin daha az bir alanda saklanması

FBI dalgacık tabanlı dönüşüm tekniği parmak izi görüntülerini daha hızlı işlemek ve saklamak için kullanır. FBI' ın üstesinden gelmeye çalıştığı bazı sorunlar vardı. Mesela ABD' de bir olay olduğunda incelenmesi gereken 200 milyondan fazla parmak izinin görüntüsü vardı. Bu görüntülere hergün 30.000 yeni görüntü ekleniyor ve bundan dolayı bu görüntüler arasında parmak izi aramak zaman almakta idi.

FBI parmak izi görüntülerinin bilgisayar ortamına aktarılmasının daha iyi bir çözüm olacağını, bununla birlikte bir parmak izinin kontrol edilmesi için bellekten 600 KB'

lık bir alanın gerekeceğini hatta en kötü ihtimalle tüm görüntü verilerinin saklanması için 2000 tera byte (TB)' lık bir alana ihtiyaç duyulabilineceği düşünülmüştü.

Bu sorunları aşmak için FBI dalgacık tabanlı sıkıştırmayı kullanmaya karar verdi. Dalgacık tabanlı sıkıştırma tekniğinde her görüntü orjinal boyutun sadece %7' sini kapladığı belirtiliyordu. Daha da şaşırtıcı olan parmak izin görüntüleri bakmak için çözüldüklerinde çok az bozulma oluyordu. Dalgacık tabanlı sıkıştırma kullanımı ile polis bir parmak izini 24 saat içerisinde kontrol edebilecekti.



Şekil 3.2: FVC2000, parmak izi doğrulama yarışmasında kullanılan veri [39]

Daha önceki çalışmalarda JPEG görüntü dosyası biçiminde sıkıştırma uygulanmaya çalışıldığı belirtilmektedir. Bu teknikte görüntü 8x8 piksel ebatlarında kare şeklinde bloklara ayrılıyor. Daha sonra verinin dönüşümü için Fourier dönüşümü kullanılmakta ve son aşamada da sıkıştırılmakta idi. Fakat bu teknik yerli değildi. Bu şekilde görüntülerin sıkıştırılması ile parmak izlerin yaklaşık %10' unda çizgi şeklinde sınırları olan kutucuklar oluşuyordu. Parmak izin karşılatırma algoritması karşılaştırılacak verilerin doğru olduğuna inanmaktaydı, fakat JPEG tekniği bu sürecin başarısını zayıflatmakta idi. Dalgacık tabanlı yöntemde ise kutucuklar ve bloklar oluşmuyor, görüntüde sadece belli bölgelerdeki detaylara değilde bir bütün olarak tümüne bakılıyordu. Bu gibi nedenlerden dolayı dalgacık tabanlı yöntem çok az bozulma ile mükemmel sıkıştırma oranlarına ulaşılmış ve fourier dönüşümüne göre daha başarılı olmuştur [40].

3.2.2. Aşamalı veri iletimi

Birçok insan sıksık İnternet' ten görüntüler indirir. Dalgacık tabanlı dönüşüm kullanılarak bu süreç dikkate değer bir şekilde hızlanır. Bir kişi bir görüntüyü

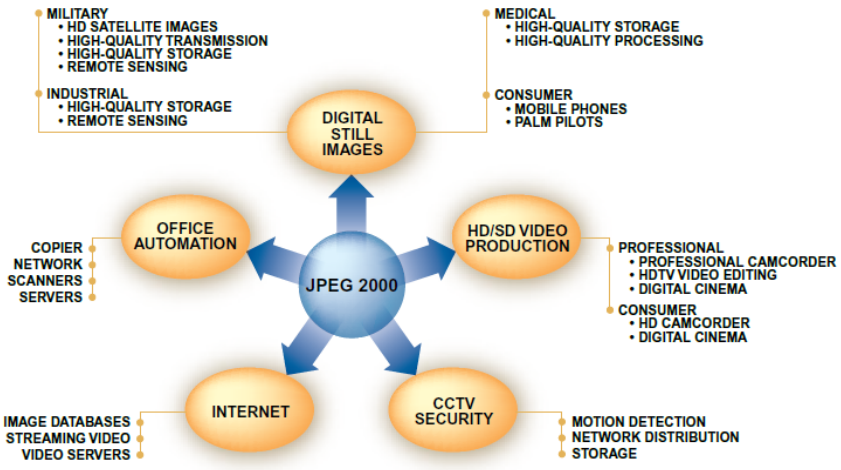
indirmek için üzerine tıkladığı zaman, kaynak bilgisayar dalga dönüşüm matrisini bellekten çağırır. Öncelikle genel yaklaşım katsayılarını ve daha geniş detay katsayılarını gönderilir. Daha sonra aşamalı bir şekilde daha küçük detay katsayıları gönderilir.

Bilgisayar bu bilgileri aldıkça aşamalı bir şekilde görüntü oluşturulmaya başlanır ve bu işlem orjinal görüntü tamamen oluşturulana kadar devam eder. Bu süreç kullanıcı görüntüyü almak istemediği zaman herhangi bir anda durdurabilir. Aksi takdirde kullanıcı görüntüyü ancak tüm görüntü indirildiği zaman görebilir. Çünkü sıkıştırılmış görüntü dosyası dikkate değer bir biçimde küçüktür ve indirilmesi daha az zaman alır [10].

3.2.3. JPEG 2000 görüntü sıkıştırma standardı

Çoklu ortam teknolojilerinin artan bir şekilde kullanılması, görüntü sıkıştırma gibi yeni özellikler kadar daha fazla performansa ihtiyaç duymaktadır. Hareketsiz görüntü kodlamasının belirli bir alanında bu ihtiyacı çözmek için JPEG2000 diye adlandırılan yeni bir standart geliştirilmektedir. Burada sadece bozulma oranının ve var olan standartlar içerisinde kişisel en üstün görüntü kalitesi performansının sağlanması hedeflenmemiştir, ayrıca şu anda var olan standartların verimli bir biçimde yada hiç çözülememiş özelliklerin gerçeklenmesi hedeflenmiştir [41].

JPEG 2000 formatına gore sıkıştırılan görüntüler birçok alanda kullanılabilir. Bu kullanım alanlarından birisi CCTV güvenlik sistemidir. Bu sistemde yüksek çözünürlüklü görüntüler bilgisayarlarda saklanırken, ağ üzerinde düşük çözünürlüklü görüntüler dolaşmaktadır. Güvenlik ekranlarında düşük kalitede fakat anlaşılabilir olan görüntüler gösterilmektedir. Eğer güvenlik operatörü bir durumdan şüphelenirse o görüntünün yüksek çözünürlüklü haline hemen ulaşabilir.



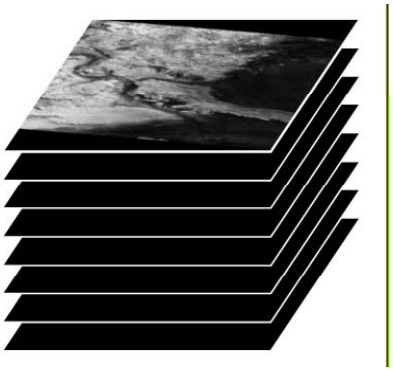
Şekil 3.3: JPEG 2000' in uygulama alanları [41]

Internet üzerinden dağıtılan görüntülerde CCTV güvenlik sistemindeki yapıya benzer çalışmaktadır. Küçük resimler düşük kalitede ziyaretçilere gösterilirken, büyük resimler en iyi kalitede gösterilmtektedir.

3.2.4. Landsat görüntüsünün bantlar arası ilişkilerin azaltılarak sıkıştırılması

Çok büyük verilerin aktarılması ve saklanması için gereken yüksek maliyet öncemli bir sorundur. Bu da şu anda veri sıkıştırmasında kullanılan etkili tekniklerin tasarımlarında önemli değişiklikler yapılmasını gerektirmektedir. Uydu görüntüleri, büyüklükleri bakımından önemli bir sorun olmuştur. Örneğin 8 bantlı bir Landsat 7 uydu görüntüsüne pankromatik bant da eklenirse genelde 600 MB' lık bir yere ihtiyaç duyulur. Uydu görüntülerinde bütün bilgiler önemli olduğundan buradaki sıkıştırmanın kayıpsız olması gerekmektedir.

Şu anda LOCO-I, SPIHT, CALIC, CREW, JPEG2000 ve MrSID (ticari amaçlı) gibi farklı çok iyi kayıpsız sıkıştırma teknikleri olmasına rağmen hala bu konuda geliştirmeler yapılabilineceği belirtilmiş. Landsat 7 uydusunda çok tayflı 8 bant bulunur. Bu bantlardan 1, 2 ve 3 nolu bantlar görünür, 4 nolu bant yakın kızılötesi, 5 ve 7 nolu bantlar kızılötesi kısa dalga ve bant 6.1 ile 6.2 termal biçimindedir. Şekil 3.4' te örnek bir Landsat 7 görüntüsü ve Tablo 3.1' deki tabloda ise her spekral bant için dalga boyları listelenmiştir.



Şekil 3.4: Landsat 7 uydu görüntüsünün bantları [42]

Tablo 3.1: Landsat 7 uydusunda bantların dalga genişlikleri

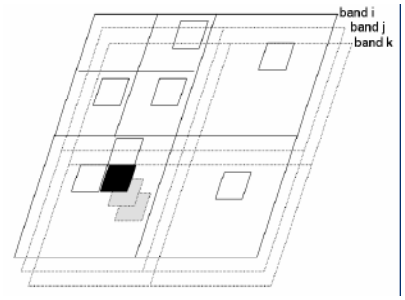
Bant	**Dalga genişliği**
1	0.45 − 0.52 μm
2	0.52 − 0.60 μm
3	0.63 − 0.69 μm
4	0.76 − 0.90 μm
5	1.55 − 1.75 μm
6	1,6.2 10.4 − 12.5 μm
7	2.08 − 2.35 μm

Çok tayflı olan görüntülerin bantları arasında yüksek bir ilişki vardır. Bu gerçek görüntü sıkıştırılmasında dikkate alınması gerekiyor. Şu anda var olan tekniklerde buna göre bir uydu görüntü kodlayıcısı genelde yoktur.

Buradaki çalışmada çoklu bant ilişkilerinden faydalanılarak çok tayflı görüntülerin kayıpsız olarak sıkıştırılması bu çalışmada ele alınmıştır. Yapılan çalışmada öncelikle her bant bloklara ayrılır ve bu bloklara dalgacık dönüşümü uygulanır. Burada dalgacık katsayıları, aynı sıra ve uzaysal konuma ait katsayıların lineer birleşiminin ortalaması ile tahmin ediliyor. Tahmin hataları entropi tabanlı kodlayıcı tarafından kodlanır. Burada aşağıdaki katkılar ortaya çıkmıştır;

- Diğer spektral bantların aynı konumlarının katsayıları, tahmin için elde edilen adayları kapsar.
- Ağırlığın hesaplanması, işlenen yer yüzü görüntüne bağlıdır.

- Hızlı bir blok sınıflandırması ve farklı bant sırası her yer yüzü görüntüsü için kullanılır



Şekil 3.5: Şu anki katsayıların tahmini için adaylar [42]

Burada kullanılan sıkıştırma ile görüntünün orijinal boyutunun yaklaşık dörtte birine kadar küçültme sağlandığı belirtilmektedir. Buradaki yöntem LOCO-I' e denk olduğu ve seçilen 3 görüntü için daha iyi sonuçlar elde edildiği belirtilmektedir. Ayrıca kayıpsız diğer sıkıştırma yöntemleri olan Winzip, JPEG2000 ve PNG' ye göre de üstün olduğu belirtilmiştir [42].

3.2.5. Kayıpsız görüntü sıkıştırma yöntemlerinin karşılaştırılması

Farklı dosya tipleri ile yapılan sıkıştırma testlerinin sonucunda, geliştirilen kayıpsız bir veri sıkıştırma algoritması olan RSSDC algoritmasının, kendisi gibi sözlük tabanlı bir yaklaşım kullanarak sıkıştırma yapan LZW algoritmasına göre daha iyi sıkıştırma oranları elde ettiği görülmüştür. Bu çalışmada, hem RSSDC algoritmasının hem de kayıpsız sıkıştırma için kullanılan diğer yöntemlerin, kayıpsız görüntü sıkıştırma için performansları test edilmiş ve belirli bir tip görüntü için hangi yaklaşımın daha iyi sonuç verdiği ortaya konmuştur.

Karşılaştırmada sıkıştırma zamanları göz önüne alınmamış, sadece sıkıştırma oranlarına bakılmıştır. Test yapılırken RSSDC, JPEG2000 ve WinRAR yöntemlerinin diğerlerine göre daha yavaş sıkıştırma yaptıkları gözlenmiştir. Karşılaştırma için 16 farklı görüntü dosyası, renk sayıları ve renk derinliklerine göre 5 farklı gruba ayrılmıştır. Belirli özelliklere sahip görüntü dosyalarının, belirli yöntemlerle daha iyi sıkıştırıldığını daha rahat gösterebilmek için böyle bir gruplamaya ihtiyaç duyulmuştur [43].

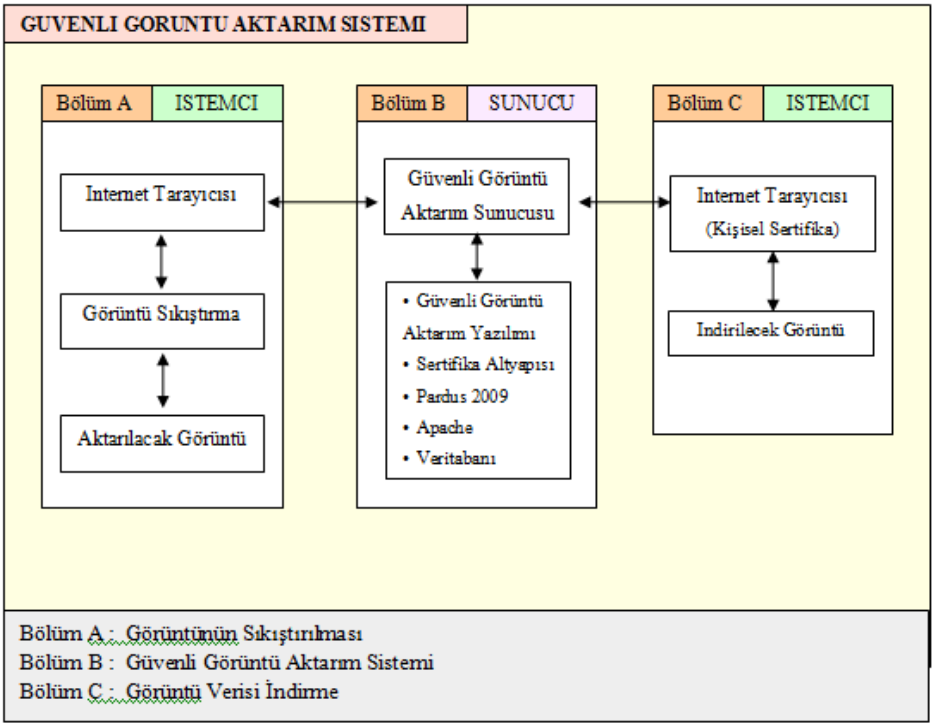
BÖLÜM 4. MİMARİ YAPI VE UYGULAMA

Bu bölümde güvenli görüntü aktarım sistemi, görüntü sıkıştırma uygulaması, güvenli görüntü aktarım yazılımı ve performans analizi başlıkları yer almaktadır.

Güvenli görüntü aktarım sistemi başlığında geliştirilen sistemdeki bileşenlerin birbirleri ile olan ilişkileri anlatılmaktadır. Görüntü sıkıştırma uygulması bölümünde ise temel bileşenler analizi ve dalgacık tabanlı görüntü sıkıştırma ile ilgili yapılan uygulamalar anlatılmaktadır. Görüntü aktarım yazılımı kısmında ise geliştirilen internet tabanlı görüntü aktarım uygulaması yer almaktadır. Performans analizi bölümünde, sıkıştırılan büyük görüntülerin sıkıştırılması için gereken zaman, sıkıştırma sonrası oluşan görüntü kalitesi ve sıkıştırılan görüntünün değişik büyüklüklerdeki değerlere gore iletilebilinmesi için gereken zaman bilgileri analiz edilmiştir.

4.1. Güvenli Görüntü Aktarım Sistemi

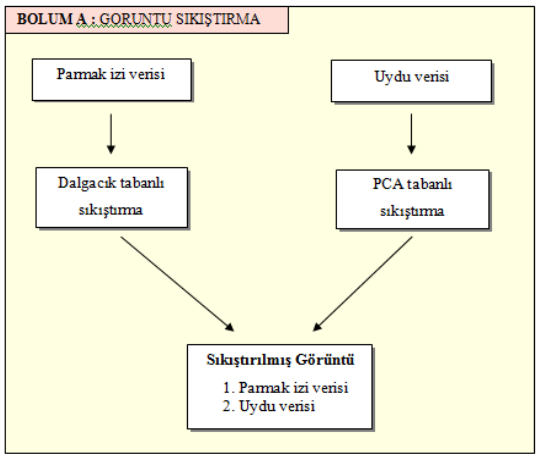
Tez kapsamında tasarımı ve kodlaması yapılan Güvenli Görüntü Aktarım Sistemi üç aşamadan meydana gelmektedir. Bu aşamalar Şekil 4.1' de gösterildiği gibi Bölüm A' da yer alan "Görüntü Sıkıştırma", Bölüm B' de gösterilen "Güvenli Görüntü Aktarım Sunucusu" ve Bölüm C' de gösterilen "Görüntü Verisi İndirme" aşamalarıdır. Bölüm A' da sıkıştırılan görüntüler öncelikle Bölüm B' de yer alan sunucuya yüklenmektedir. Sonraki aşamada ise Bölüm B' de tanımlı olan kullanıcılar kendi sertifikalarını kullanarak Bölüm C üzerinden internet tarayıcılarını kullanarak Bölüm B' ye yüklenmiş olan görüntülere ulaşabilmektedir.



Şekil 4.1: Güvenli sıkıştırılmış görüntü aktarım sistemi temel çalışma yapısı

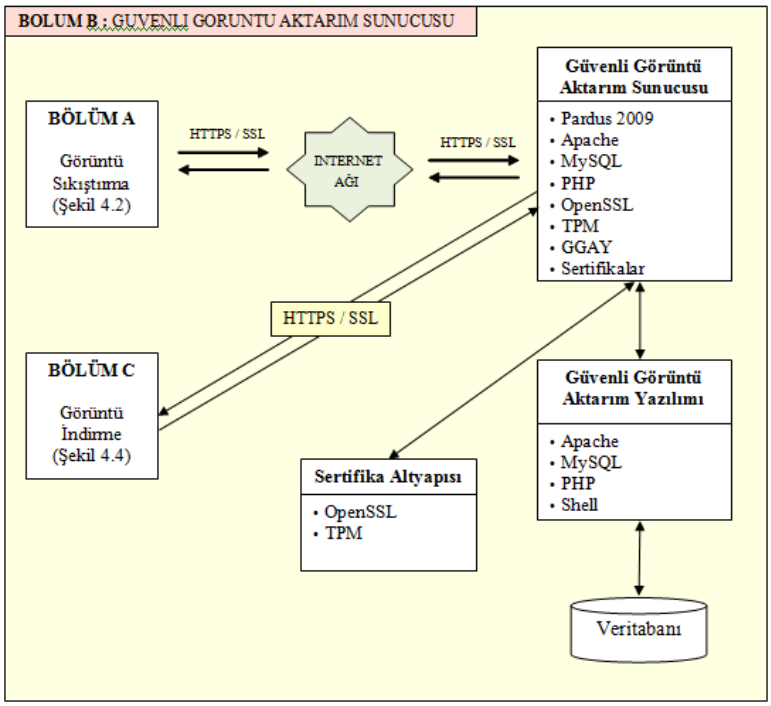
Görüntü sıkıştırma aşaması olan Bölüm A' da aktarılacak görüntüler, temel bileşenler analizi ve dalgacık tabanlı dönüşüm yöntemleri kullanılarak Şekil 4.2' de gösterildiği gibi sıkıştırılmaktadır. Uygulamada iki ayrı sıkıştırma yöntemi kullanılmıştır. Bunlardan birisi "Dalgacık Tabanlı Sıkıştırma" yöntemidir. Dalgacık Tabanlı Sıkıştırma yönteminde parmak izi verisi sıkıştırılmaktadır. Görüntü sıkıştırmada kullanılan diğer bir sıkıştırma yöntemi "Temel Bişenler Analizi" diğer adıyla PCA yöntemidir. Temel Bileşenler Analizi yönteminde uydu verisi sıkıştırılmaktadır.

Şekil 4.2' de gösterilen PCA tabanlı görüntü sıkıştırma işleminde Landast 5 TM uydu verisinin 179 / 32 nolu çerçevesine denk gelen KOCAELİ ilinin 2009 Eylül ayında kayıt edilmiş olan uydu verisi kullanılmıştır. Değişik karakteristikteki bu iki veri (parmak izi ve uydu verisi) bu aşamadan sonra güvenli ve hızlı aktarım girdisi olarak hazırdır.



Şekil 4.2: Görüntü sıkıştırma adımları

Geliştirilen güvenli görüntü aktarım sunucusunun çalışma yapısı Şekil 4.3' te daha detaylı olarak gösterilmiştir. Güvenli bir aktarım ortamı için sistemde Şekil 4.3' te gösterildiği gibi sayısal sertifikaların kullanıldığı bir sertifika alt yapısı geliştirilmiştir. Ayrıca görüntülerin güvenli bir şekilde depolanmasını ve yönetilmesini sağlayan güvenli görüntü aktarma yazılımı geliştirilmiş ve bir veritabanı alt yapısı tasarlanmıştır.



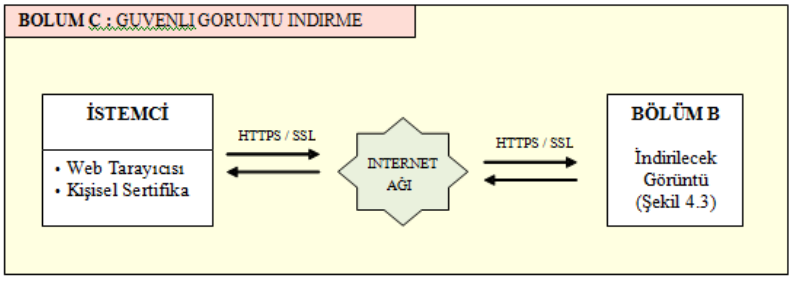
Şekil 4.3: Güvenli Görüntü Aktarım Sistemi (GGAS)

Güvenli Görüntü Aktarım Sisteminde öncelikle görüntü temel bileşenler analizi yada dalgacık tabanlı görüntü sıkıştırma tekniklerinden birisine göre sıkıştırılır. Daha sonra sıkıştırılan bu görüntü Şekil 4.3' teki Güvenli Görüntü Aktarım Sunucusuna yüklenir.

Güvenli görüntü aktarım sistemi sunucu ve istemci bilgisayarlarda çalışan yazılımlardan meydana gelmektedir. Şekil 4-3' de görüldüğü gibi Sunucu ve İstemci arasındaki iletişim İnternet ağı üzerinden HTTPS / SSL protokolü ile 443' üncü porttan çalışmaktadır. Bu protokolde sunucu ve istemci birbirlerinin sertifikalarını kullanarak şifrelenmiş olan bir hat üzerinden veri alış verişi gerçekleştirirler.

Kullanıcı sertifikalarının üretiminde sunucu bilgisayarında openSSL, TPM gibi uygulamalar kullanılırken, geliştirilen güvenli görüntü aktarım yazılımı için Apache, MySQL ve PHP yazılımları kullanılmaktadır. Sunucu bilgisayarın işletim sistemi ücretsiz olarak dağıtılan ve herhangi bir lisanslama maliyeti olmayan Pardus 2009.2 işletim sistemi kullanılmaktadır.

Bundan sonra yüklenen bu görüntüleri indirme hakkına sahip olan kullanıcılar Şekil 4.4' te gösterildiği gibi kişisel sertifikalarını kullanarak sisteme bağlanırlar. Burada kullanılan kişisel kullanıcı sertifikalarının daha önceden sisteme erişme hakkına sahip olacak olan kullanıcılara elden teslim edilmiş olması gerekmektektedir. Son aşamada da kullanıcı sistemden istediği görüntüleri güvenli kanal üzerinden indirebilmektedir.



Şekil 4.4: Güvenli görüntü indirme

İstemci tarafında bu sistemin çalışması için herhangi bir işletim sistemi ve en az HTML 3.0 desteği olan bir internet tarayıcısının (Internet Explorer, Mozilla Firefox,

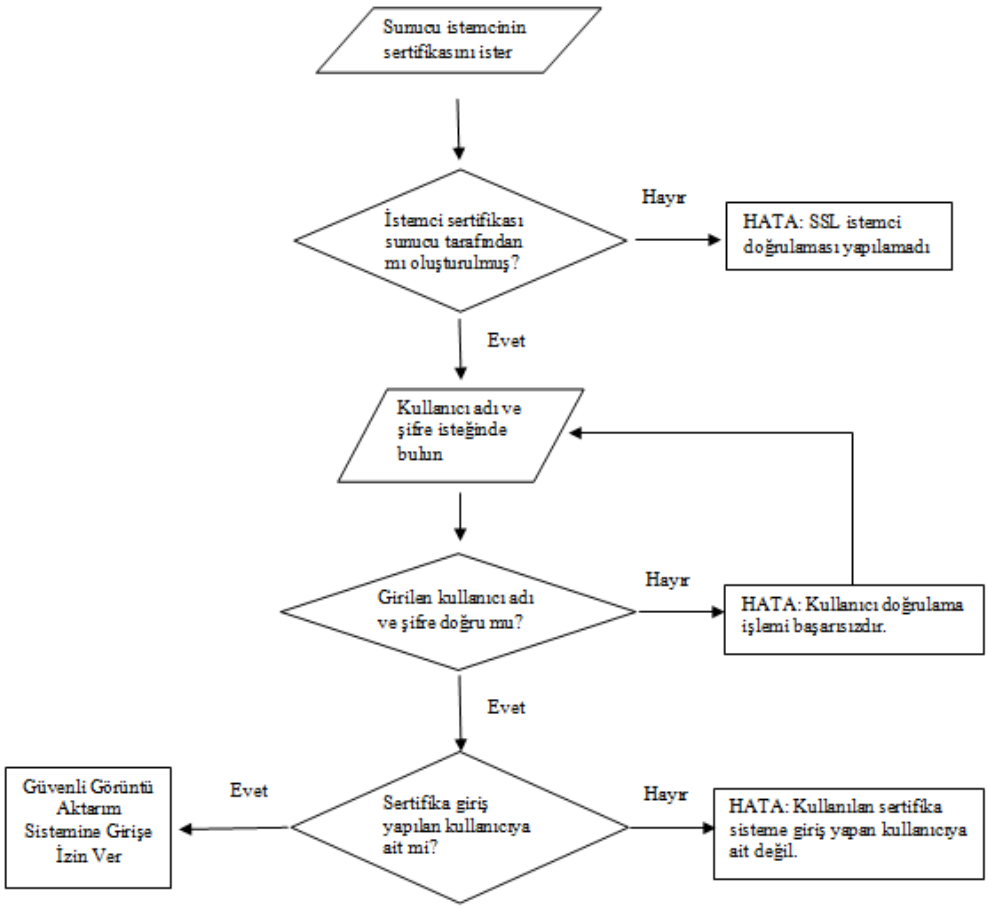
Safari, Google Chrome vb gibi) kullanılması gerekmektedir. Ayrıca güvenli görüntü aktarım sistemine bağlanacak olan kullanıcıya verilmiş olan sayısal sertifikanın, kullanıcının internet tarayıcısına yüklenmesi gerekmektedir.

Daha önceden de belirtildiği üzere İnternet üzerinden kullanıcılar ile yapılan veri transferlerinde SSL protokolü üzerinden gerçekleşmektedir. SSL protokolü üzerinden veri alışverişi yapabilmek için Şekil 4.3' te detayları gösterilen sunucuda openSSL aracı kullanılarak sertifika üretimi yapılması gerekmektedir. Geliştirmiş olduğumuz güvenli görüntü aktarım sistemi için üretilen sertifikanın görüntüsü Şekil 4.5' deki gibidir. Burada sertifikayı sunucuda kendimiz üretmek yerine dünya çapında sertifika üretimi ve dağıtımı yapan kuruluşlardan (Verisign gibi) satın alabilirdik. Ülkemizde de sertifika üretimi ve dağıtımı yapan bir çok kuruluş vardır. Hatta devlet tarafından kurulan, sertifika üretimi ve dağıtımı ile uğraşan TÜBİTAK – UEKAE bünyesinde yer alan Kamu Sertifika Merkezi bulunmaktadır.



Şekil 4.5: OpenSSL ile oluşturulan sunucu sertifikası

Geliştirilen yazılımda kişilerin güvenlik doğrulaması sayısal sertifikalar kullanılarak yapılmaktadır. Şekil 4.6.' da kullanıcılara dağıtılan sayısal sertifikalar kullanılarak, sertifika sahibi bir kullanıcının Güvenilir Görüntü Aktarım Sistemi' ne giriş için hangi aşamalardan geçmesi gerektiği anlatılmaktadır.



Şekil 4.6: Sayısal Sertifikalar ile Güvenli Görüntü Aktarım Sistemine giriş

Geliştirilen güvenli görüntü aktarım sisteminin veritabanı Tez_Contacts, Tez_Images ve Tez Users tablolarından meydana gelmektedir. Bu tablolarda yer alan alanlar ve açıklamaları Tablo 4.1, Tablo 4.2 ve Tablo 4.3' te yer almaktadır. Burada veritabanı olarak açık kaynak kodlu MySQL veritabanı kullanılmıştır.

Tez_Contacts tablosunda iletişim formu üzerinden kullanıcıların göndermiş olduğu mesajlar yer almaktadır. Yönetim panelinden system yöneticisi gönderilmiş olan bu mesajları görebilmektedir. Tez_Images tablosunda ise sisteme yönetim panelinden yüklenmiş olan sıkıştırılmış görüntüler (uydu veya parmak izi görüntüleri) yer almaktadır. Bu tabloda görüntülerin sunucudaki dosya sisteminde nerede bulunduğu da saklanmaktadır. Tez_Users tablosunda ise sistemi kullanacak olan kullanıcıların tanımlamaları yer almaktadır.

Tablo 4.1: Tez_Contacts tablosu

Alan adı	**Açıklaması**
id	Birincil anahtar
title	Mesajın başlığı
notes	Açıklama
namesurname	Ad ve soyad
email	E-posta adresi
createdate	Oluşturulma zamanı
lastupdate	Son güncelleme zamanı

Tablo 4.2: Tez_Images tablosu

Alan adı	**Açıklaması**
id	Birinci anahtar
title	Mesajın başlığı
notes	Açıklama
filePath	Yüklenen görüntünün sistemde saklandığı yer
thumbImg	Yüklenen görüntünün küçük tanıtıcı resmi
status	Görüntünün durumu (aktif / pasif)
createdate	Oluşturulma zamanı
lastupdate	Son güncelleme zamanı

Tablo 4.3: Tez_Users tablosu

Alan adı	**Açıklaması**
id	Birinci anahtar
uname	Kullanıcı adı
upass	Şifresi
firstname	Ad
lastname	Soyad
phone	Telefon
email	Kullanıcının e-posta adresi
notes	Açıklamalar
status	Kullanıcının durumu (aktif / pasif)
createdate	Oluşturulma zamanı
lastupdate	Son güncelleme zamanı

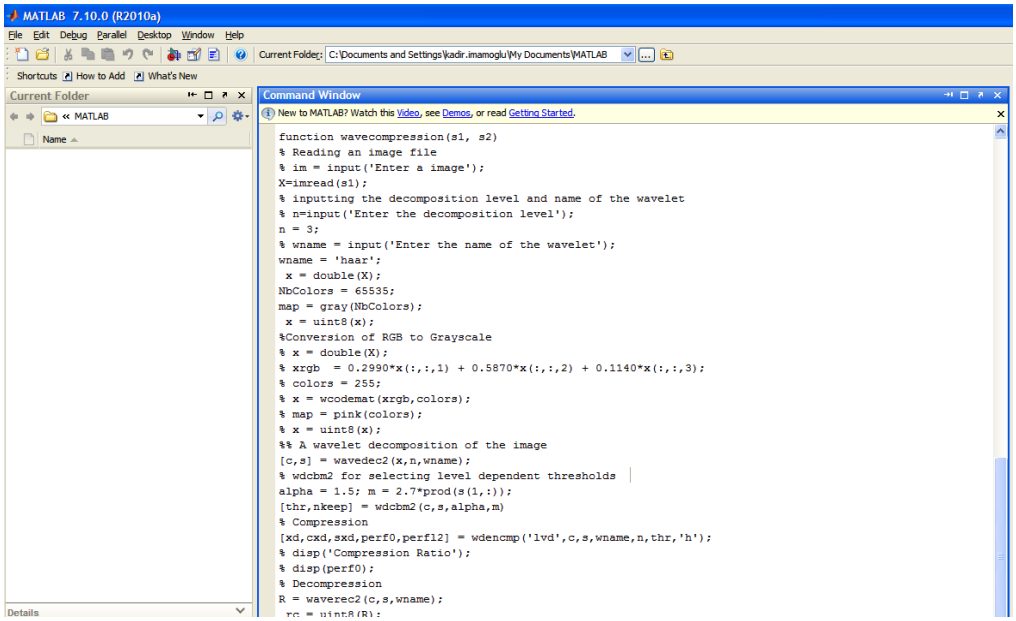
4.2. Görüntü Sıkıştırma Uygulaması

Bu bölümde dalgacık tabanlı ve temel bileşenler analizi yöntemlere göre görüntülerin nasıl sıkıştırıldıkları anlatılmaktadır. Burada geliştirilen uygulamalar Bölüm 2' de anlatılan temel anlatımlardan yararlanılarak hazırlanmıştır.

4.2.1. Dalgacık tabanlı dönüşüm yöntemi ile görüntü sıkıştırma

Dalgacık tabanlı dönüşüm yöntemine göre görüntü sıkıştırma işlemi için MATLAB programından yararlanıldı. MATLAB' ta hazırlanan program ile orjinal görüntü dosyası dalgacık tabanlı dönüşüm yöntemi kullanılarak, sıkıştırılmıştır. Yapılan çalışmada MATLAB' ın 2010a versiyonu kullanılmıştır.

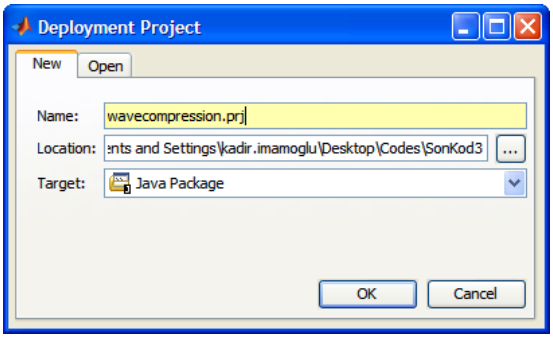
Şekil 4.7' de gösterilen MATLAB programında görüldüğü gibi görüntü sıkıştırma "wavecompression" adlı fonksiyon kullanılarak yapılmaktadır. Bu fonksiyon 2 parametre almaktadır. Bu parametrelerden ilki sıkıştırılacak orjinal görüntü dosyasının bulunduğu konumu belirtirken ikinci parametre ise sıkıştırılan görüntü dosyasının kopyalanacağı yeri belirtmektedir.



Şekil 4.7: MATLAB' ta hazırlanan DTD yöntemi ile görüntü sıkıştırma programı

DTD yöntemi kullanılarak görüntü sıkıştırma işleminin yapıldığı MATLAB kodunu İnternet tabanlı GGAS' de kullanabilmek için .JAR uzantılı JAVA paketi haline getirilmiştir. MATLAB kodlarının JAR paketi haline getirilmesi ile MATLAB programına olan bağımlılık ortadan kalkmaktadır. Böylece sistemin yer aldığı web sunucusunda MATLAB programının kurulmasına gerek kalmadan görüntü sıkıştırma işlemini gerçekleştirmiş olduk.

MATLAB kodunu JAR paketi haline getirmek için MATLAB programı içerisinde yer alan “Deployment Tool” adlı araç kullanılır. Bu aracı çalıştırmak için MATLAB komut satırında öncelikle “deploytool” komutu çalıştırılır. Ve karşımıza Şekil 4.8’ de gözüken ekran gelir. Bu ekranda MATLAB kodunu JAVA paketi haline dönüştürmek istediğimizi belirtiriz. Sonraki aşamada gelen ekranda MATLAB altında geliştirilen kodların deployment tool’ da oluşturulan java sınıfı içerisine eklenir. Ve build düğmesine basılarak, dalgacık tabanlı görüntü sıkıştırma işlemi yapan “wavecompression.jar” adlı java paketi oluşturulması sağlanır.



Şekil 4.8: Dalgacık tabanlı sıkıştırma yapan Java paketinin oluşturulması

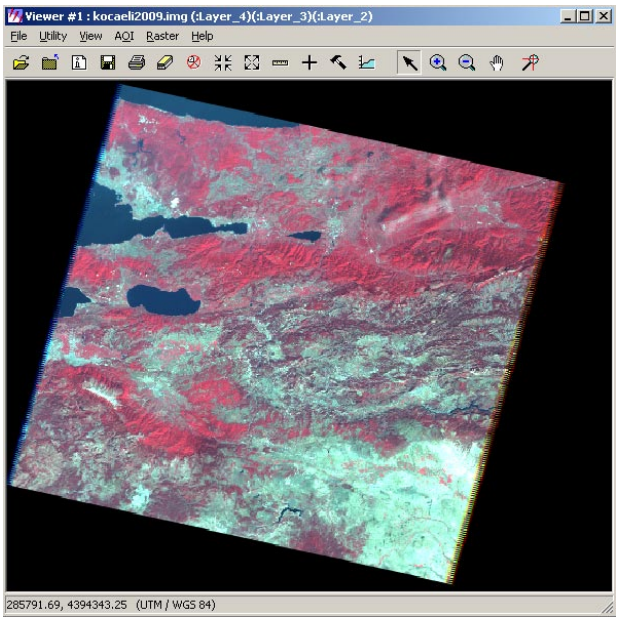
Oluşturulan “wavecompression.jar” adlı JAVA paketini kullanarak görüntü sıkıştırma işlemini komut satırından aşağıdaki gibi gerçekleştirilebiliriz. Aşağıdaki kodda gözüktüğü gibi MATLAB içerisinde yer alan “javabuilder.jar” adlı paketin yerinin classpath parametresinde tanımlanması gerekmektedir. “javabuilder.jar” adlı JAR paketi MATLAB 2010 içerisinde yer almaktadır.

```
java -cp wavecompression.jar;javabuilder.jar wavecompression.wavecomp
'c:\tez\resim.tif' 'c:\tez\yeni-resim.tif'
```

Son aşama olarak ise sıkıştırma işlemi için oluşturulan bu java paketin web tabanlı PHP uygulamasının içerisine entegre edilmesi gerekmekte idi. Bu entegrasyonu sağlamak için PHP içerisinde yer alan “system" komutu kullanılmıştır. Bu komut aracılığı ile yukarıda yazılan sistem komutu, uydu görüntülerinin yüklendiği yerde çalıştırılması sağlanıyor. Böylece uydu görüntüsü yüklendikten sonra MATLAB’ tan JAVA paketi haline çevrilen program aracılığı sıkıştırılır.

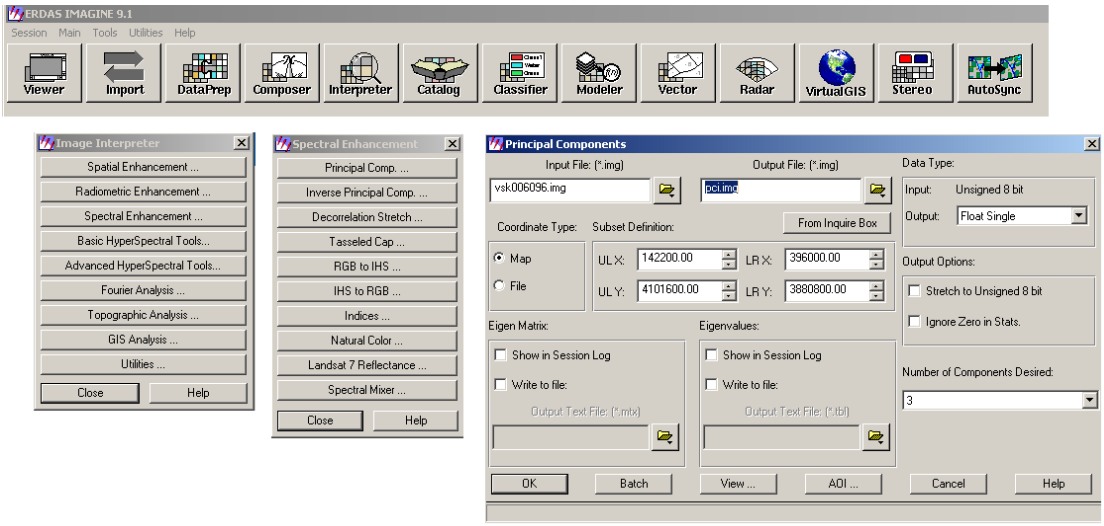
4.2.2. Temel bileşenler analizi yöntemi ile görüntü sıkıştırma

Temel bileşenler analizi ERDAS adlı görüntü işleme yazılımı kullanılarak gerkeçkleştirilmiştir. PCA analizi Şekil 4.9' da gösterildiği gibi Kocaeli ilinin 2009 yılında Landsat 5 uydusunun TM algılayıcısı ile çekilmiş uydu görüntüsü kullanılmaktadır.



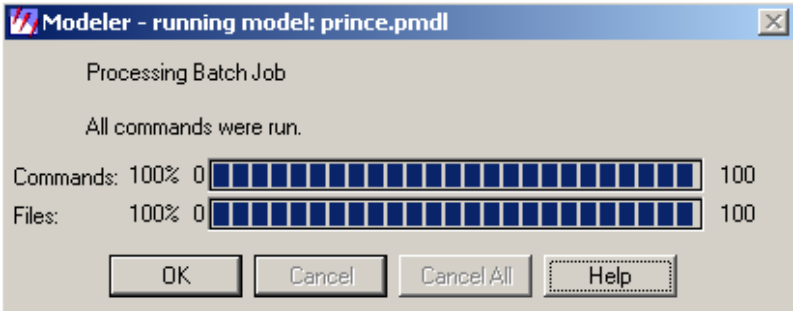
Şekil 4.9: PCA dönüşümü yapılan Landsat uydu görüntüsü

Temel bileşenler analizini yapabilmek için öncelikle ERDAS adlı görüntü işleme yazılımında Şekil 4.10 da gösterildiği gibi once üstteki Interpreter düğmesine basılır. Karşımıza principle components penceresi gelecektir. Bu pencerede dönüşüm işlemi yapılacak uydu görüntüsü girilir ve kaçtane PCA bileşenin kullanılacağı burada belirtilir. Aşağıdaki örnekte biz 3 tane bileşen kullanıyoruz.



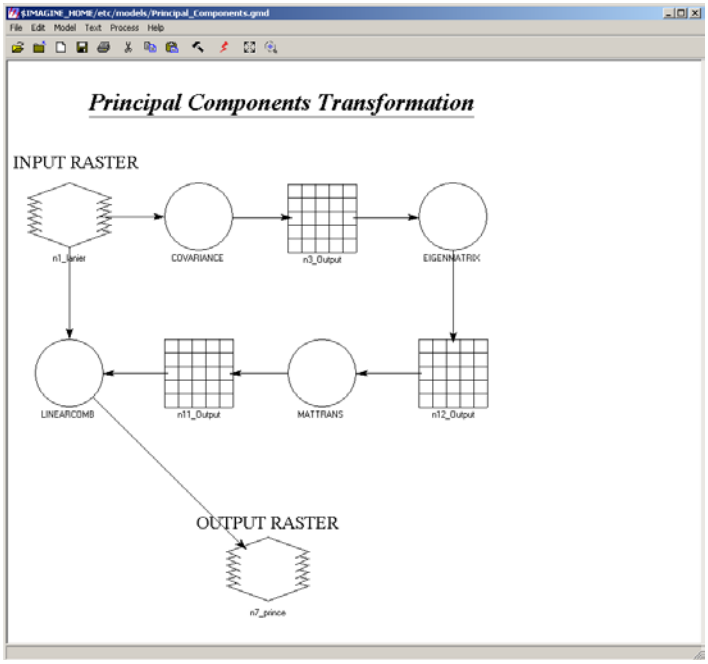
Şekil 4.10: PCA dönüşümü adımları

Şekil 4.7' deki gibi PCA analizini çalıştırdığımız zaman karşımıza Şekil 4.11' deki ekran gelir. Bu ekranda sıkıştırma işlemi tamamlandıktan sonar OK düğmesi aktif olur. Bu düğmeye basılarak işlem tamamlanır.



Şekil 4.11: PCA dönüşümünün çalışması

Şekil 4.12' de Erdas modeler bölümü kullanılarak hazırlanmış PCA dönüşünün modeli yer almaktadır.

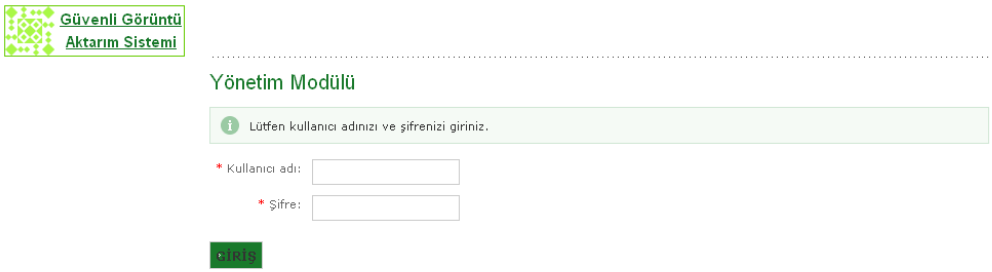


Şekil 4.12: PCA dönüşümünün çalışması

4.3. Güvenli Görüntü Aktarım Yazılımı (GGAY)

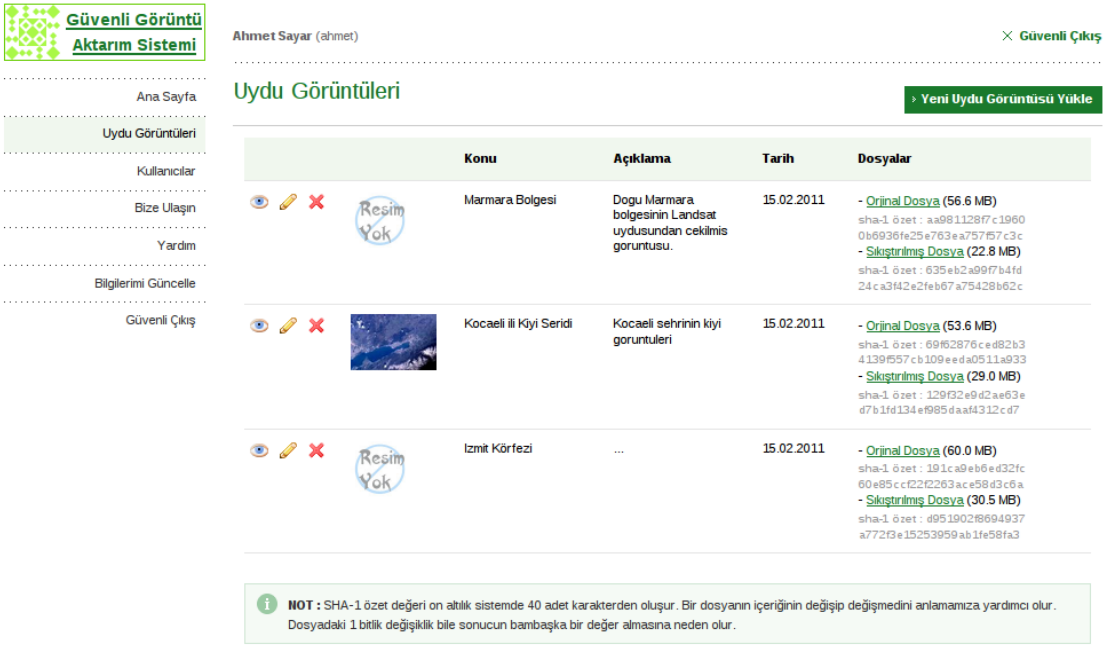
Sayısal sertifikalar kullanarak güvenli görüntü aktarımını sağlayan bu sistem Pardus 2009.1 [44] işletim sistemi altında geliştirilmiştir. Geliştirilen güvenli görüntü aktarım yazılımında programlama dili olarak PHP ve shell script, veritabanı olarak ise MySQL kullanılmıştır. Bu yazılımda uydu görüntülerinin güvenli bir şekilde saklanması ve dağıtımı yapılmıştır. Güvenli görüntü aktarım sistemine sadece sayısal sertifikası tanımlanmış olan kullanıcıların giriş yapabilmelerine izin verilmiştir. Sisteme giriş için tanımlanan kullanıcıların sayısal sertifikaları güvenli yollardan kendilerine ulaştırılmaktadır. Sayısal sertifikasını alan kullanıcılar bu sertifikalarını internet taraycısına ekleyip güvenli bir şekilde sisteme bağlanabileceklerdir.

GGAY' ı yönetim ve kullanıcı modüllerinden meydana gelmektedir. Yönetim modülüne Şekil 4-13' de gösterilen ekran üzerinden giriş yapılabilir. Bu modülde görüntü yükleme ve sistemi kullanacak olan kullanıcıların tanımlamaları yapılmaktadır. Yönetim panelinden tanımlanmış olan görüntüler ve kullanıcılar Şekil 4.14 ve Şekil 4.15' te gösterilmektedir. Kullanıcı modülünde ise tanımlı olan kullanıcılar sisteme giriş yaptıktan sonra Şekil 4.15' ten istedikleri görüntüleri güvenli bir şekilde indirebilmeleri sağlanmıştır.



Şekil 4.13: Yönetim modülü giriş erkranı

Aşağıda yönetim panelinde tanımlanan görüntüler yer almaktadır. Burada tanımlanan görüntüler ile ilgili konu başlığı, açıklaması, yüklendiği tarih ve durumu gibi alanlar yer almaktadır.



Şekil 4.14: Yönetim modülü uydu görüntüleri listeleme ekranı

Sertifikalı olan kullanıcıların listesi yönetim panelinde aşağıdaki ekrandaki gibi gözükmektedir.



Şekil 4.15: Yönetim modülü kullanıcılar listesi ekranı

Sertifikaları tanımlı olan kullanıcılar kullanıcı modülünden giriş yaptıklarında Şekil 4.16' teki ekrandan istedikleri görüntüleri güvenli bir şekilde bilgisayarlarına indirebilirler.



Şekil 4.16: Kullanıcı modülü uydu görüntüleri ekranı

GGAY' ında yer alan tüm kullanıcı ve yönetim ekranları EK – H' ta yer almaktadır.

4.4. Test Senaryosu ve Sistemin Değerlendirilmesi

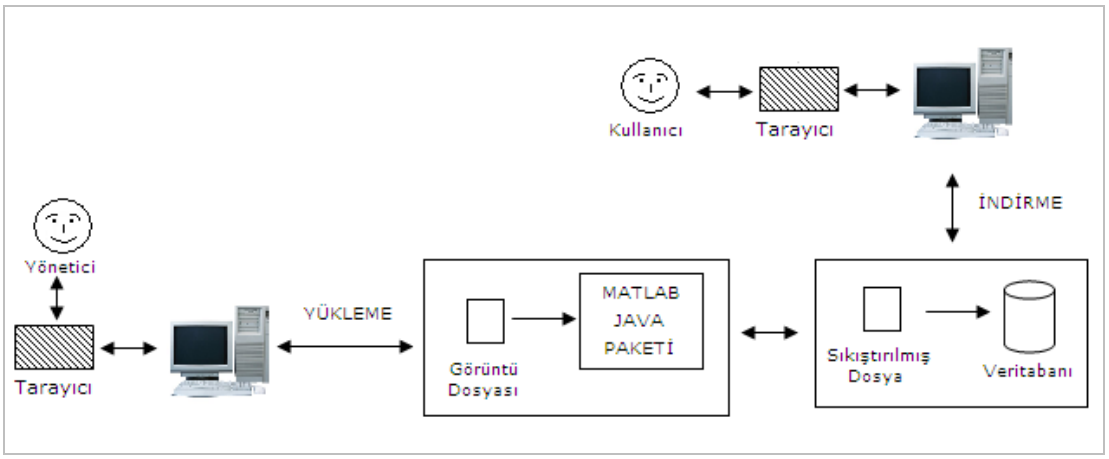
Bu bölümde, dalgacık tabanlı dönüşüm ve temel bileşenler analizi yöntemleri kullanılarak görüntü sıkıştırma işlemleri için çeşitli testler gerçekleştirilmiştir. Öncelikle gerçekleştirilecek olan testlerin nasıl yapılacağını gösteren test senaryoları oluşturulmuştur. Oluşturulan bu test senaryolar çalıştırılarak test sonuçları elde edilmiştir. Elde edilen test sonuçlarıda son kısımda değerlendirilmiştir.

4.4.1. Dagacık tabanlı sıkıştırma yöntemi ile yapılan testler

Dalgacık tabanlı görüntü sıkıştırma tekniği kullanılarak yapılan sıkıştırma, yükleme ve indirme ile ilgili testler bu bölümde yer almaktadır.

4.4.1.1. Test senaryosu

Bu test senaryosunda, görüntülerin sisteme yüklenmesi, sıkıştırılması ve indirilmesi için geçen zaman olmak üzere 3 farklı test yapılmıştır. Yapılan bu testlerden birincisi ve ikincisi Şekil 4.17' de gösterilen, yönetici tarafından yapılan görüntü dosyasının yüklenmesi ve sıkıştırılması testleridir. Üçüncü test ise sertifikası tanımlı kullanıcının tarayıcısı aracılığı ile yaptığı görüntülerin indirilmesi testidir.

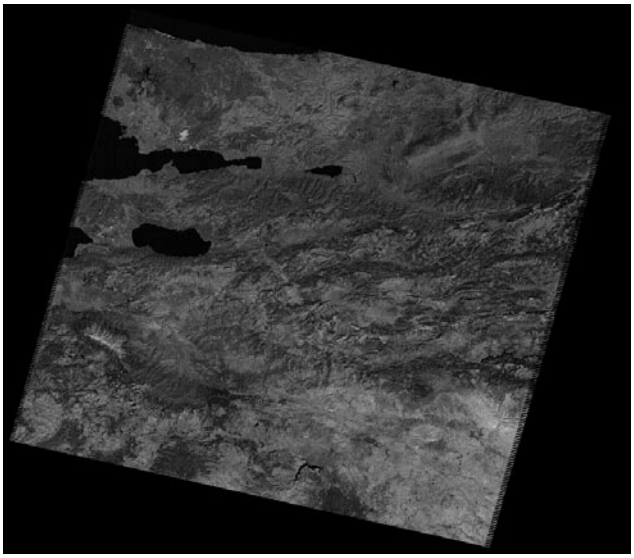


Şekil 4.17: Dalgacık tabanlı sıkıştırma yöntemi test senaryosu

Buradaki test senaryosunda görüntü sıkıştırma işlemi, Şekil 4.17' de gösterildiği gibi öncelikle sıkıştırılmamış görüntü dosyası web sunucusuna yüklenir. Daha sonra yüklenen bu dosya web sunucusu üzerinde çalışan MATLAB JAVA paketi aracılığı ile sıkıştırılıp sisteme kayıt edilmektedir. Sonraki aşamada ise kullanıcılar sisteme kayıt edilmiş olan bu sıkıştırılmış dosyayı web sunucusuna bağlanıp indirebilirler.

Dalgacık tabanlı dönüşüm yönteminin test senaryosunda Şekil 4.18 de gösterilen 2009 yılına ait KOCAELİ bölgesinin yer aldığı LANDSAT uydu görüntüsü kullanılmaktadır. Bu uydu görüntüsü NASA tarafından oluşturulmuş ve İNTERNET üzerinden ücretsiz dağıtılan GLOVIS veritabanından alınmıştır. GLOVİS veritabanından alınan LANDSAT uydu verisinin TIFF formatlı tek bir bant görüntü sıkıştırma testlerinde kullanılmıştır.

Kullanılan uydu görüntüsünün kapladığı alan 60 MB boyutunda ve çözünürlüğü 8441x7441 piksel ebatlarındadır. Farklı boyutlardaki görüntüleri oluşturmak için tekrar ebatlandırma yöntemleri ile yükseklik ve genişlik değerleri azaltılmıştır.



Şekil 4.18: DTD test senaryosunda kullanılan uydu görüntüsü

Burada görüntü sıkıştırma işlemi ile ilgili yapılan zaman ölçümü testlerinde web sunucusunda PHP programlama dilinde microtime() adlı zaman fonksiyonu kullanılmıştır. Bu fonksiyon ile sıkıştırma işlemi öncesi ve sonrasında zaman

değerleri ayrı ayrı değişkenlere alınarak saklanmıştır. Ve saklanan bu değişkenlerin aralarındaki fark hesaplanarak zaman ölçümü hesaplanmıştır.

Dalgacık tabanlı dönüşüm yöntemi için gerçekleştirilen testler, İNTERNET ortamında ADSL hattı kullanılarak yapılmıştır. Kullanılan ADSL hattının bant genişliği indirme / yükleme işlemi için 4096 Kbps / 960 Kbps hızlarındadır. Testlerde kullanılan istemci bilgisayarda 2 GB bellek ve 2.2 GHz AMD Turion işlemci ve Windows Vista işletim sistemi bulunmaktadır. Suncuda ise açık kaynak kodlu Pardus 2009.2 işletim sistemi, 1 GB bellek 2.0 GHz AMD işlemcisi yer almaktadır.

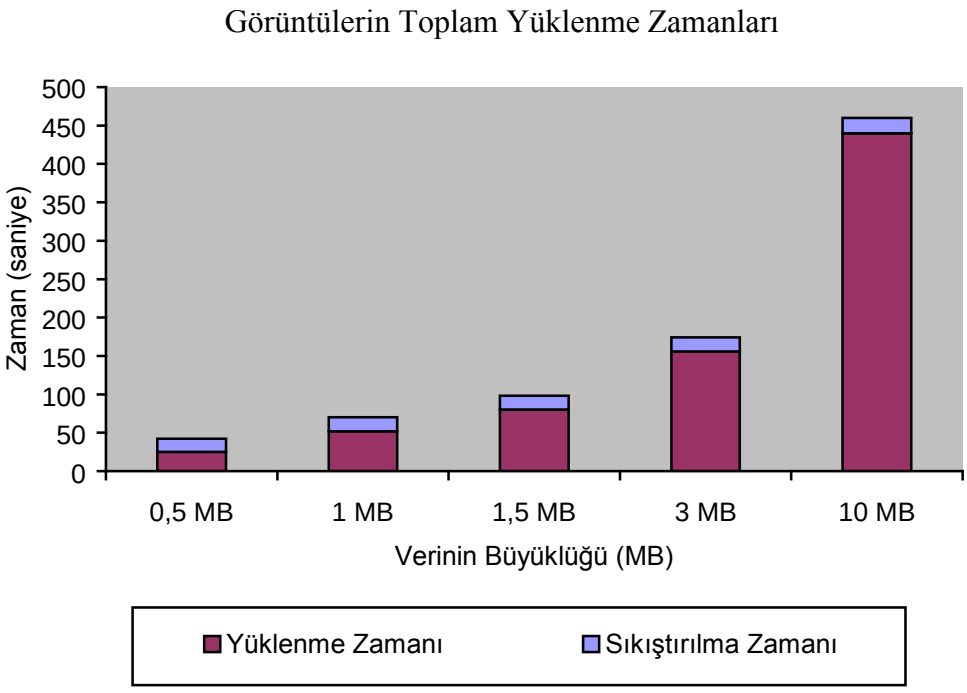
4.4.1.2. Dalgacık tabanlı dönüşüm senaryosu test sonuçları

Dalgacık tabanlı dönüşüm yöntemine göre yapılan testlerden elde edilen değerler Tablo 4.4' de gösterilmiştir.

Tablo 4.4: Farklı verilerin yüklenme, sıkıştırılma ve indirilme zamanları

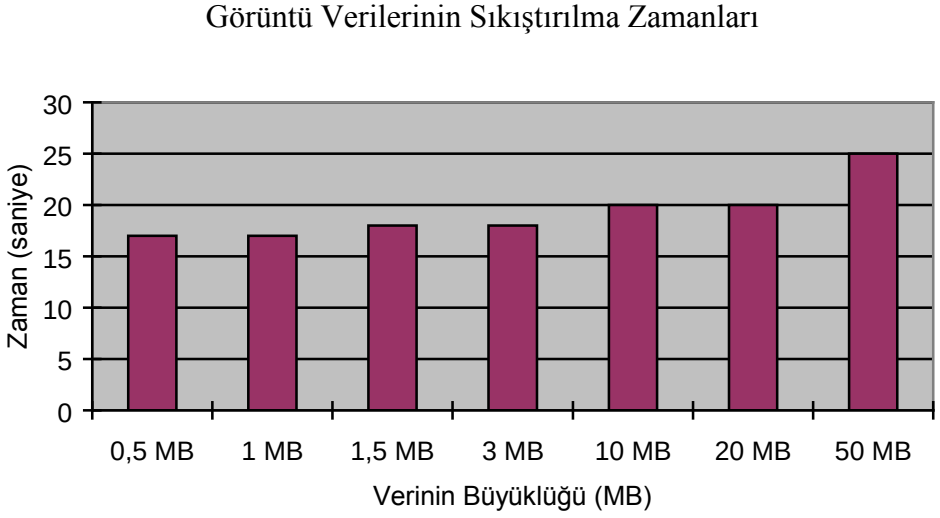
Yüklenen Verinin Büyüklüğü	Yükleme Zamanı	Sıkıştırma Zamanı	İndirme Zamanı
0,5 MB	25 sn	17 sn	7 sn
1 MB	52 sn	18 sn	13 sn
1,5 MB	1 dk 20 sn	18 sn	17 sn
3 MB	2 dk 36 sn	18 sn	33 sn
10 MB	7 dk. 20 sn	20 sn	1 dk. 41 sn
20 MB	14 dk. 31 sn	20 sn	3 dk. 32 sn
50 MB	35 dk 27 sn	25 sn	8 dk 50 sn

Tablo 4.4' de yer alan INTERNET ortamındaki veri aktarımı ile ilgili verilerin grafiği çizilirse Şekil 4.19' daki grafik elde edilir. Bu grafik incelendiğinde INTERNET ortamında büyük dosyaların yüklenmesi için dikkate değer bir zaman gereksinimi duyulmaktadır. Bu grafikte görüldüğü gibi görüntü sıkıştırma işlemi fazla zaman almamaktadır.



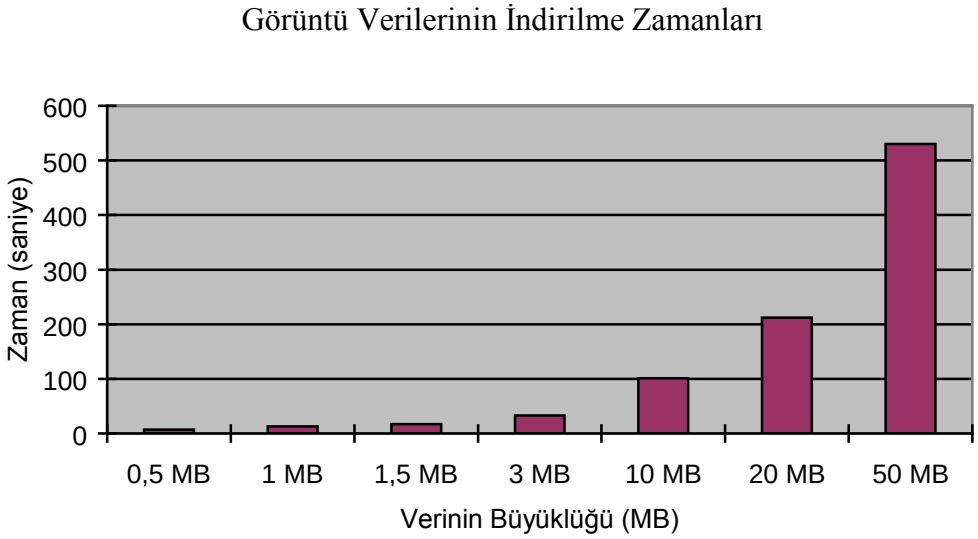
Şekil 4.19: Farklı ebatlardaki görüntülerin yüklenme zamanları

Şekil 4.20' de Tablo 4.4' de belirtilen görüntü dosyalarının sıkıştırılmaları için harcanan sürelerin saniye cinsinden grafiği çizilmiştir. Burada görüldüğü gibi dalgacık tabanlı yöntemde, büyük ve küçük dosyaların sıkıştırılmasında fazla zaman farkı yoktur.



Şekil 4.20: Farklı ebatlardaki verilerin sıkıştırılma zamanları

Şekil 4.21’ de çizilen görüntü verisinin indirilme zamanı test sonuçlarında görüldüğü gibi verinin kapladığı alan büyüdükçe bu verilerin INTERNET ortamından indirilmesi için gereken zaman doğru orantılı olarak artmaktadır.



Şekil 4.21: Farklı ebatlardaki verilerin indirilme zamanları

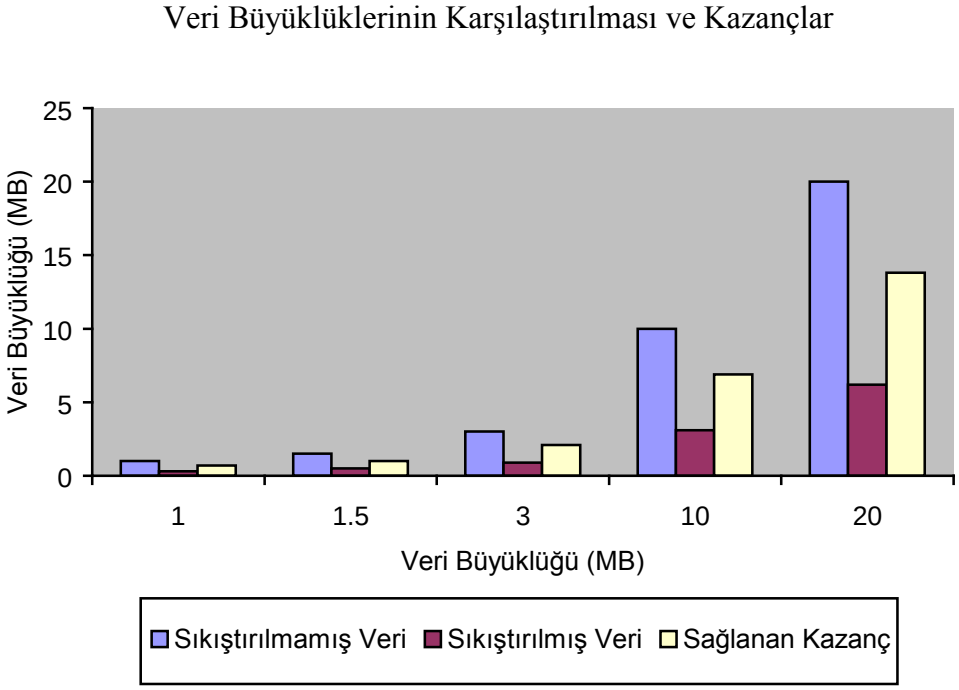
Tablo 4.5’ de farklı ebatlardaki görüntü verilerinin sıkıştırıldıktan sonra sağlanan kazanç değerleri MB cinsinden gösterilmiştir.

Tablo 4.5: Farklı ebatlardaki verilerin sıkıştırılması

Yüklenen Verinin Büyüklüğü (MB)	**Sıkıştırılan Verinin Büyüklüğü (MB)**	**Kazanç Sağlanan Büyüklük (MB)**
0,5 MB	0,1 MB	0,4 MB
1 MB	0,3 MB	0,7 MB
1,5 MB	0,5 MB	1 MB
3 MB	0,9 MB	2,1 MB
10 MB	3,1 MB	6,9 MB
20 MB	6,2 MB	13,8 MB
50 MB	14,7 MB	35,3 MB

Görüntü dosyalarının sıkıştırılmadan önce ve sıkıştırıldıktan sonra kapladıkları alanlar Şekil 4.22’ de sağlanan kazanç değerleri ile beraber gösterilmektedir. Burada

ayrıca görüntü sıkıştırma işlemi sonrasında veri büyüklüğünde sağlanan kazançlarda sarı renk ile gösterilmiştir.



Şekil 4.22: Sıkıştırma işlemi öncesi ve sonrası verilerin boyutları

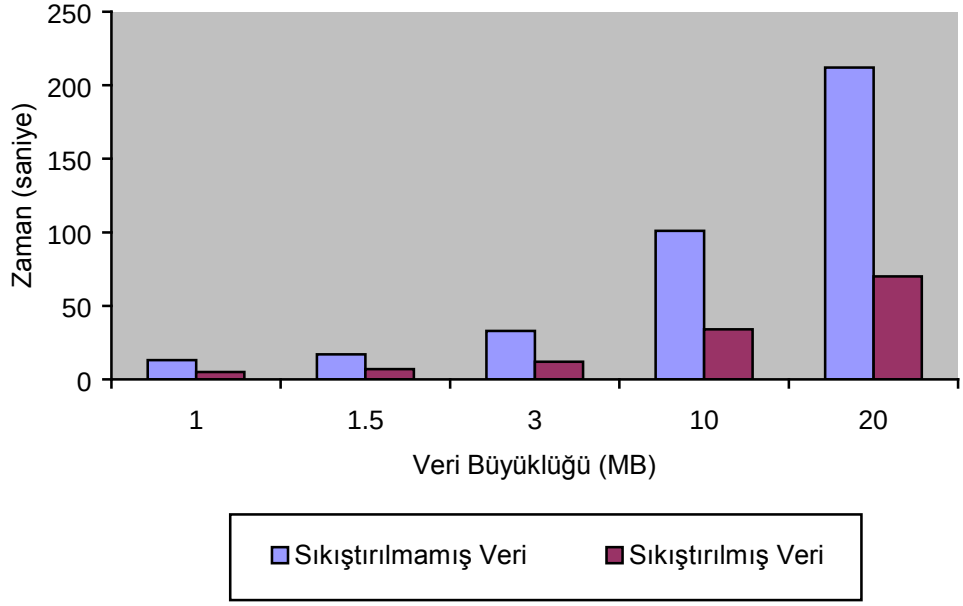
Sıkıştırılmış görüntülerin indirilme zamanlarını gösteren tablo aşağıda Tablo 4.6 da gösterilmiştir. Bu tablodan görüldüğü üzere sıkıştırılmış görüntünün indirilme zamanı sıkıştırılmamış görüntüye göre çok daha azdır.

Tablo 4.6: Sıkıştırılmamış ve sıkıştırılmış görüntülerin indirilme zamanları

Orjinal Verinin Büyüklüğü	**Sıkıştırılmış Verinin Büyüklüğü**	**Orjinal Verinin İndirilme Zamanı**	**Sıkıştırılmış Verinin İndirilme Zamanı**
0,5 MB	0,1 MB	7 sn	2 sn
1 MB	0,3 MB	13 sn	5 sn
1,5 MB	0,5 MB	17 sn	7 sn
3 MB	0,9 MB	33 sn	12 sn
10 MB	3,1 MB	1 dk. 41 sn	34 sn
20 MB	6,2 MB	3 dk. 32 sn	1 dk 10 sn
50 MB	14,7 MB	8 dk 50 sn	2 dk 55 sn

Şekil 4.23’ te sıkıştırılmış ve sıkıştırılmamış görüntülerin indirime zamanları grafiksel olarak gösterilmektedir. Burada mavi renkli çubuklar sıkıştırılmamış veriyi gösterirken, kırmızı renkli çubuklar sıkıştırılmış görüntüyü göstermektedir. Şekilde gözüktüğü gibi sıkıştırılmış olan görüntülerin kullanıcılar tarafından sunucudan indirilmesi daha hızlı gerçekleşmektedir.

Sıkıştırılmış ve sıkıştırılmamış görüntülerin indirilme zamanları



.

Şekil 4.23: Sıkıştırılmış ve sıkıştırılmamış görüntülerin indirilme zamanları

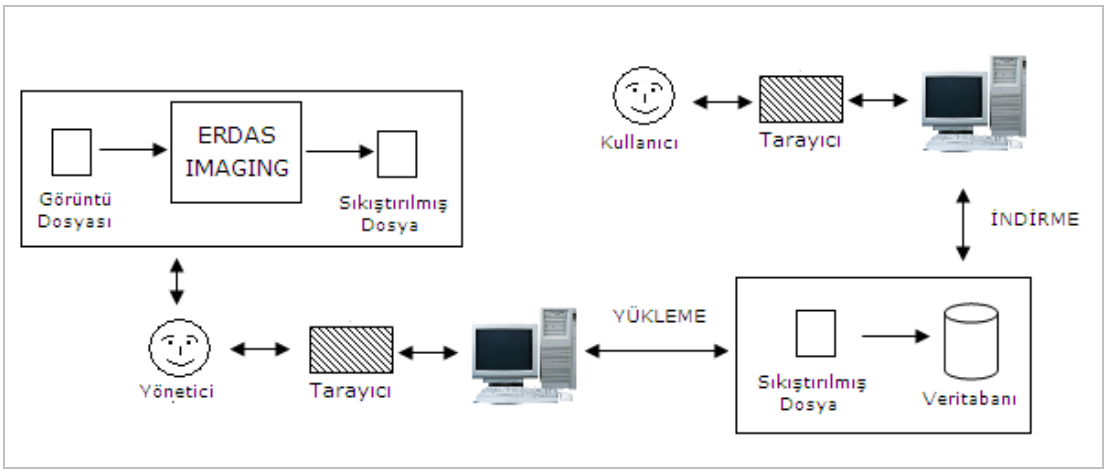
4.4.2. Temel bileşenler analizi yöntemi ile yapılan testler

Temel bileşenler analizi yöntemi kullanılarak yapılan görüntü sıkıştırma, yükleme ve indirme ile ilgili testler bu bölümde yer almaktadır.

4.4.2.1. Test senaryosu

Gerçeklenen test senaryosu, Şekil 4.24’ te detaylı bir şekilde gösterilmektedir. Burada sistem yöneticisi öncelikle Erdas adlı program ile kendi bilgisayarında uydu

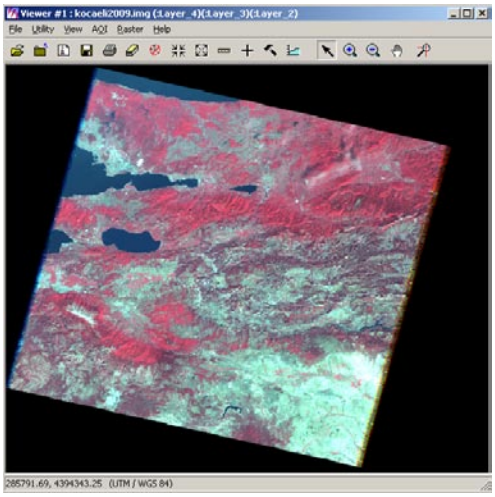
görüntüsünü sıkıştırmakta ve sıkıştırılan bu görüntü sunucuya aktarılmaktadır. Sunucuya aktarılan sıkıştırılmış görüntü kullanıcılar tarafından indirilmektedir.



Şekil 4.24: Temel bileşenler analizi yöntemi test senaryosu

Temel bileşenler analizi yöntemi kullanılarak gerçekleştirilen görüntü sıkıştırması test senaryosunda Kocaeli ilinin 2009 yılına ait Landsat 5 uydusunun TM algılayıcısı ile çekilmiş uydu görüntüsü kullanılmaktadır. Test senaryosunda kullanılan Landsat uydu görüntüsü 7 bant' tan meydana gelmekte ve kullanılan görüntü Şekil 4.25' te gösterilmiştir. Landsat uydu görüntüsünün 7 banttan meydana gelmesinden dolayı, görüntü dosyaları fazla yer kaplamakta ve dosyaların indirilmeleri için daha fazla zamana ihtiyaç duyulmaktadır.

Burada uydu görüntüsünün en önemli 2, 3, 4 ve 5 nolu bileşenleri kalacak şekilde görüntü sıkıştırma işlemleri ayrı ayrı yapılmıştır. Elde edilen sıkıştırılmış görüntülerin kapladıkları alanlar, sıkıştırılması ve indirilmesi için gereken süreler gerçekleştirilen testlerde hesaplanmıştır.



Şekil 4.25: TBA test senaryosunda kullanılan Landsat uydu görüntüsü

Temel bileşenler analizi yöntemi için gerçekleştirilen testler, İNTERNET ortamında ADSL hattı kullanılarak yapılmıştır. Kullanılan ADSL hattının bant genişliği indirme / yükleme işlemi için 4096 Kbps / 960 Kbps hızlarındadır. Testlerde kullanılan istemci bilgisayarda 2 GB bellek ve 2.2 GHz AMD Turion işlemci ve Windows Vista işletim sistemi bulunmaktadır. Suncuda ise açık kaynak kodlu Pardus 2009.2 işletim sistemi, 1 GB bellek 2.0 GHz AMD işlemcisi yer almaktadır..

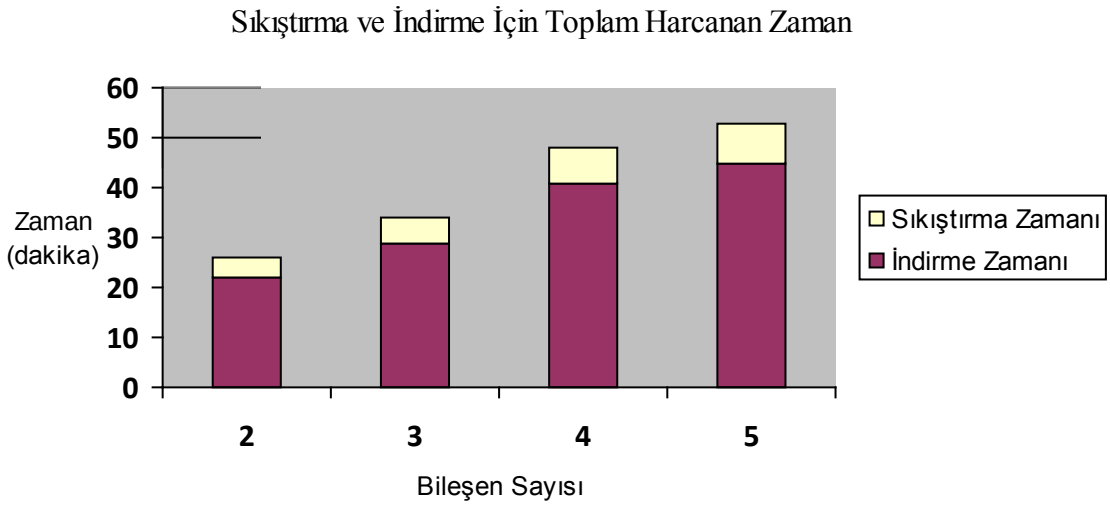
4.4.2.2. Temel bileşenler analizi senaryosu test sonuçları

Test senaryosunda belirtildiği gibi bir Landsat uydu görüntüsü için 2, 3, 4 ve 5 nolu bileşenlere göre ayrı ayrı sıkıştırma işlemi yapılmıştır. Sıkıştırma işlemleri yapıldıktan sonra Tablo 4.7' da belirtilen sonuçlar elde edilir.

Tablo 4.7: Landsat görüntülerinin boyutları, sıkıştırılma ve indirilme zamanları

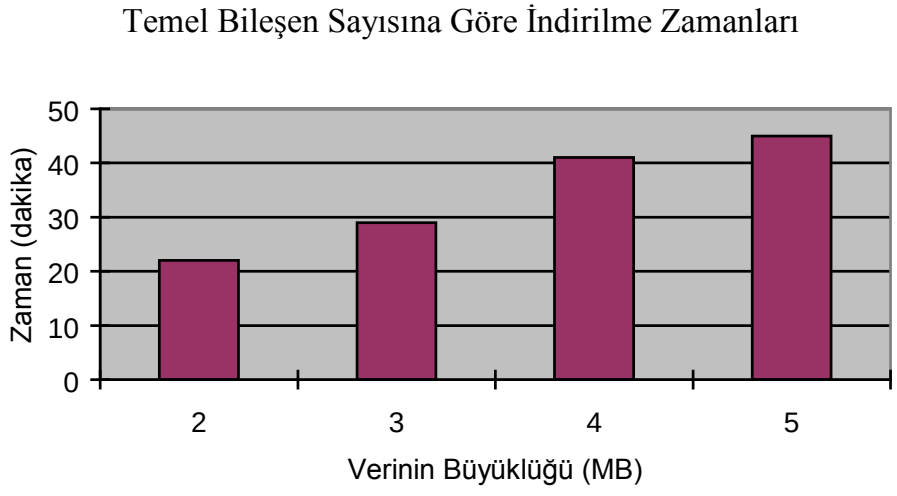
Temel Bileşen Sayısı	Boyut	Sıkıştırılma Zamanı	İndirilme Zamanı
2	136 MB	4 dk	22 dk
3	185 MB	5 dk	29 dk
4	242 MB	7 dk	41 dk
5	280 MB	8 dk	45 dk

Bu test senaryosunda 378 MB yer kaplayan Landsat uydu görüntüsü 2, 3, 4 ve 5 temel bileşen sayısına göre sıkıştırıldan sonra boyutu azalmış ve yüklenme zamanı hızlanmıştır. Temel bileşenler analizi yöntemine göre yapılan sıkıştırma sonucunda sıkıştırılan görüntülerin sıkıştırılması ve indirilmesi için harcanan süreler Şekil 4.26' da gösterilmektedir.



Şekil 4.26: Farklı bileşen sayılı görüntünün sıkıştırma ve indirme zamanları

Şekil 4.27' de en önemli 2, 3, 4 ve 5 tane temel bileşene göre sıkıştırılan uydu görüntü verilerinin sıkıştırmadan sonra kapladıkları alan ve iletimleri için gereken zaman ve gösterilmektedir.



Şekil 4.27: Temel bileşen sayısına göre indirilme zamanları

4.4.3. Gerçeklenen testlerin değerlendirilmesi

Bu bölümde gerçekleştirilen testler ile geliştirilen güvenli görüntü aktarım sisteminin ne kadar etkin çalıştığını göstermeye çalıştık. Sistemin performansını ölçmeye yönelik yapılan bu testlerde görüldüğü gibi sıkıştırılmamış büyük görüntülerin yüklenmesi ve indirilmesi için fazla zaman gerekmektedir. Sıkıştırma işlemi yapıldıktan sonra, sıkıştırılmış görüntülerin indirilmesi için ihtiyaç duyulan zamanın dikkate değer oranda azaldığı görülmüştür.

Kullanılan sıkıştırma tekniklerinden dalgacık tabanlı dönüşüm yöntemi temel bileşenler analizi yöntemine göre daha hızlı çalışmaktadır. Dalgacık tabanlı yöntem ile yapılan sıkıştırma işleminde herhangi bir uygulamaya gerek kalınmaması performansın artmasını sağlamıştır. Temel bileşenler analizi yöntemi ile yapılan sıkıştırmada ise Erdas adlı program kullanılmaktadır. Bu yöntemde sıkıştırma işlemi web tabanlı görüntü aktarım sistemi dışarısında yapıldığından yavaş çalışmaktadır.

Sisteme güvenlik ile ilgili eklenen özellikler görüntü sıkıştırma işlemini fazla etkilememektedir. Çünkü yapılan testlerin birisinde görüntü sıkıştırma işlemi sunucu içerisinde diğerinde ise daha görüntü aktarıma başlanmadan önce sunucu dışarısında istemcide yapılmaktadır. Burada gerçeklenen güvenlik sıkıştırılmış yada sıkıştırılmamış verilerin güvenli bir şekilde aktarımlasıdır.

BÖLÜM 5. SONUÇ VE DEĞERLENDİRME

Tez çalışması kapsamında, görüntü sıkıştırma ve internet üzerinden güvenli görüntü aktarımı olmak üzere başlıca iki ana konu üzerinde araştırmalar yapılmıştır.

Görüntü sıkıştırmada, temel bileşenler analizi ve dalgacık tabanlı dönüşüm yöntemleri kullanılarak uydu görüntüsü ve parmak izi verisi dosyalarının kapladıkları alanlar azaltılmıştır. Uydu görüntü dosyasının kapladığı alanın azalması ile internet üzerinden bir yerden başka bir yere görüntü aktarımının daha hızlı olması sağlanmıştır.

İnternet üzerinden çalışan güvenli görüntü aktarım sistemi, açık kaynak kodlu olan Pardus 2009.1 [44] işletim sistemi ve açık kaynak kodlu araçlar ve yazılımlar kullanılarak geliştirilmiştir. Geliştirilen yazılım ile uydu görüntülerinin güvenli bir şekilde arşivlenmesi, saklanması ve dağıtılabilinmesi sağlanmıştır. Kullanıcılar, güvenli görüntü aktarım sistemine, sadece kendileri için oluşturulan sayısal sertifikaları kullanarak giriş yapabilmektedirler. Sistemin açık kaynak ortamda çalışması nedeniyle bu sistemi kurmak isteyen kurumlar herhangi bir lisanslama ücreti ödemeleri gerekmemektedir. Bu da geliştirilen sistemin kurulum ve kullanım maliyetlerini büyük olçüde azalmasına neden olmaktadır.

Güvenli görüntü aktarım sistemine, MATLAB programı altında geliştirilen dalgacık tabanlı dönüşüm yöntemi kodları JAVA paketi haline çevrilerek internet tabanlı uygulamanın içerisine entegre edilmesi sağlanmıştır. Böylece GGAS' i çalışırken sunucuda, MATLAB gibi ek bir programa ihtiyaç duyulmaması sağlanmıştır.

Performans analizi başlığında anlatıldığı gibi uydulardan çekilmiş uydu görüntüleri gibi büyük dosyaların sıkıştırılması ve iletimi için fazla zaman gerekmektedir. Burada uydu görüntü verisinin en uygun eşik değere göre sıkıştırılmasına dikkat

edilmesi gerekmektedir. Böylece görüntü verisindeki bilgileri kullanamayacak kadar sıkıştırmamış yada kullanmayacağımız bilgileri bırakmamış oluruz.

Geliştirilen bu sistem birçok alanda kullanılabilir. Kullanım alanlarından birisi askeri amaçlı olabilir. Burada gizli askeri uydu görüntülerinin güvenli bir şekilde sisteme yüklenip sadece sertifikası tanımlı kişiler tarafından görülüp indirilmesi yapılabilir. Bazen görüntüler fazla yer kapladıklarından (GB' lar seviyesinde) sadece sıkıştırılmış uydu görüntülerinin sisteme yüklenmesi, bu görüntülere erişimin daha hızlı olmasını sağlayacaktır.

Diğer bir kullanım alanıda kurumlar arasında gizlilik gerektiren evrakların bu güvenli sistem kullanılarak aktarımı yapılabilir. Burada yine gizli evraklara erişme hakkı olacak kullanıcılar için sayısal sertifikalar oluşturulacak. Kullanıcılarda bu sertifikalar ile güvenli bir şekilde sisteme girip verilerin şifrelendiği bir kanal üzerinden evraklara ulaşacaklardır. Ayrıca bu evraklara kullanıcılarda yer alan sayısal sertifikalar kullanılarak sayısal olarak imza (e-imza) atma özelliği de geliştirilebilir. Bu sistemin yaygınlaşması ile kurumlar arasındaki evrak alışverişinde gereksiz kâğıt kullanımın önüne geçilecek ve işlemlerin hızlı gerçeklenmesine imkan verilecektir.

Son olarak emniyet birimlerinde hırsızlar yada şüpheli kişilerin parmak izlerinin saklanmasında ve takibinde bu sistem kullanılabilir. Öncelikle güvenli sisteme giriş yapabilecek yetkili Polis memurları için sayısal sertifikalar oluşturulacak ve dağıtımı yapılacaktır. Bu amaçla geliştirilecek sistemde şüpheli bir kişinin parmağı, parmak izi okuyucusu yardımı ile okutulacak ve internet üzerinden güvenli bir kanaldan sisteme gönderilecektir. Sistem üzerinde çalışacak parmak izi tanıma yazılımı aracılığı ile sistemde yer alan tüm parmak izi görüntülerde tarama yapılbilinecektır. Sistemde saklanacak parmak izlerinin dalgacık tabanlı dönüşüm gibi yöntemlerle sıkıştırılması sayesinde daha hızlı arama yapılabilinecek ve parmak izi görüntülerini saklamak için daha az yer gerekecektir.

Geliştirilmiş olan bu görüntü aktarım sisteminde 10 TB (Tera Byte) gib çok fazla büyüklüğe sahip dosyaların aktarılmasında bant genişliğinden dolayı çeşitli sorunlar

yaşanabilir. Bu sorunlardan birisi İnternet üzerinden görüntü aktarımı için sunucu tarafından belirlenen oturum zaman aşımı süresinin yetmemesidir. Bu tür bir durumda ya sunucudaki oturum zaman aşımı süresinin artırılması gerekmekte yada çok hızlı bant genişliğine sahip bir hatta ihtiyaç duyulmaktadır. Bazen bu iki durumdan hiç birini istediğimiz gibi ayarlamamız mümkün olmayabilir. Bu tür bir durum için ileride sistemde dosya aktarımı işi yarıda kalmış görüntülerin tekrar aynı görüntünün verilmesi halinde kaldığı yerden devam etmesinin sağlayacak bir modül programlanabilir.

Hazırlanmış olan tez çalışmasında ileride birçok geliştirme yapılabilir. Bu geliştirmelerden birisi USB şeklindeki depolama aygıtlarında sisteme bağlanacak olan kullanıcıların sertifikalarının saklanmasıdır. Bu depolama aygıtlarında sertifikalar güvenli bir şekilde saklanabilir ve browser ile uygulamaya erişilmek istenildiğinde sertikanın yer aldığı USB' nin takılması ve güvenlik kodunun girilmesi istenebilir.

Şu anda çok fazla yaygın kullanılmayan ve geliştirilme çalışmaları devam eden güvenilir bilişim de kullanılmakta olan TPM yongasının kullanımı çeşitlendirilebilir. TPM yongası temel anlatımlar bölümünde de anlatıldığı gibi birkaç Euro maliyeti olan temel kriptografik işlemleri yapabilmekteydi. İleride LOG dosyaları bu yongadan üretilecek olan anahtarlar ile imzalanıp şifrelemesi yapılabilir. İstemciden sunucuya doğru yapılan bağlantılar için uzaktan tasdikleme (remote attestation) özelliği eklenebilir. Böylece sadece TPM' i sisteme tanımlanmış olan cihazlardan bağlantı yapılması mümkün hale gelmiş olacaktır.

KAYNAKLAR

[1] Weis, R., Lucks, S., Bogk, A. "TCG 1.2 - fair play with the 'Fritz' chip?", **SANE2004**, Amsterdam, (2004).

[2] Açık Anahtar Altyapısı Eğitim Kitabı, TÜBİTAK UEKAE, [online], http://www.kamusm.gov.tr/tr/Bilgideposu/Belgeler/teknik/aaa/index.html, **(Ziyaret Tarihi: 20 Şubat 2010).**

[3] Diffie, W., Hellman, M., "New Directions in Cryptography", Information Theory, **IEEE Transactions,** 22, 29-36, (1976).

[4] Yıldırım, S.: "The Secure Electronic Legally Binding Promissory Note System", Yüksek Lisans Tezi, **Marmara Üniversitesi Fen Bilimleri Enstitüsü,** İstanbul,

[5] Jason Reid, Juan M. González Nieto, Ed Dawson and Eiji Okamoto, "Privacy and Trusted Computing", ***Proc 14th International Workshop on Database and Expert Systems Applications,*** IEEE, Los Alamitos, California, 383-388, Eylül (2003).

[6] STOA Panel, European Parliament: Development of Surveillance Technology and Risk of Abuse of Economic Information. Luxembourg, Nisan 1999 [online], http://www.cryptome.org/ stoa-r3-5.htm **(Ziyaret Tarihi: Haziran 2006).**

[7] Arnd Weber, Dirk Weber, "Legal Risk Assessment of Trusted Computing - A Review, Indicare Monitor", 2(12), Şubat (2006).

[8] TCG Specification version 1.2 Architecture Overview [online], http://www.trustedcomputinggroup.org **(Ziyaret Tarihi: Haziran 2006).**

[9] Takahisa Shirakawa, NEC's Attribute to "Trusted Computing", NEC Journal of Advanced Technology, Vol.2, No.1, Winter (2005).

[10] Ames, G., 2002, Image Compression [online], http://online.redwoods.cc.ca.us/ instruct/darnold/laproj/Fall2002/ames/paper.pdf, **(Ziyaret Tarihi: 14 Mart 2010).**

[11] Application to Image Compresion [online], University of Ottawa, http://aix1.uottawa.ca/~jkhoury/haar.htm **(Ziyaret Tarihi: 05 Nisan 2010).**

[12] Kharate, G. H., Ghatol, A.A., Rege, P.P., "Image Compression Using Wavelet Packet Tree", **ICGST-GVIP Journal**, Volume (5), Issue (7), 37-40, (2005).

[13] Coşkun, Ö., ÇÖMLEKÇİ, S., "Wavelet Teorisinin Medikal Alana Uygunlanmasi Üzerine Bir Ön Çalişma", **Akademik Bilişim 2007**, Dumlupınar Üniversitesi, 31 Ocak – 02 Şubat, (2007).

[14] Aksan, E., Doğan, S., "Dalgacık Tabanlı Görüntü Sıkıştırma Tekniği", ***Havacilik Ve Uzay Teknolojileri Dergisi***, 1(4), 47-53, (2004).

[15] Mulcany, C., "Image compression using the Haar wavelet transform", **Spelman Science and Math Journal**, 22-31, (1997).

[16] İnce, F., "Uzaktan Algılamada Sayısal Görüntü İşleme", **TUBITAK-MAM, ÖY - 86/02**, Ağustos, (1986).

[17] Lindsay I Smith, 2002, A tutorial on Principle Components Analysis [online], http://www.cs.otago.ac.nz/cosc453/student_tutorials/principal_components.pdf **(Ziyaret Tarihi: 05 Ocak 2010).**

[18] Chitwong, S., Witthayapradit, S., Intajag, S., Cheevasuvit, F., "Multispectral Image Classification Using Back-Propagation Neural Network In Pca Domain", **WSEAS Multi-Conference,** (2004).

[19] Yildirim, H., Alparslan, E., Özel, M. E., "Temporal Change Detection by Principal Component Transformation", **IEEE Xplore**, 1227-1229, (1995).

[20] Karakoçak, K., "Elektronik imza el kitabı", **Ankara Barosu**, ISBN:975-6037-49-0, (2006).

[21] "Elektronik İmza Kanunu" [online], http://www.mevzuat.adalet.gov.tr/html/1328.html, **(Ziyaret Tarihi: 12 Nisan 2010)**

[22] Selçuk, G.H., "E-devlet uygulamaları için e-imza formatları", **Ulusal Elektronik İmza Sempozyumu**, (2006).

[23] Kamu sertifikasyon merkezi [online], "http://www.kamusm.gov.tr/net/bilgiler/kurumsal/kimlik.jsp", **(Ziyaret Tarihi: 10 Mayıs 2010)**

[24] Altın, E., "Türkiye'de Elektronik İmza ve Elektronik Devlet Uygulamaları", ***Değişen Dünyada Bilgi Yönetimi Sempozyumu*****,** 150- 157, (2007).

[25] Sağıroğlu, S., Kabasakal D., Alkan M., "E-imzadan mobil imzaya geçiş sürecinde Türkiye", **Ulusal Elektronik İmza Sempozyumu**, 21-27, (2006).

[26] eVoting is gaining ground in Estonia [online], http://www.epractice.eu/en/news/292691 **(Ziyaret Tarihi: 10 Mayıs 2010).**

[27] Yıldırım, S., İnce, F., "Güvenli Elektronik Senet (e-Senet) Sistemi", **TBD Bilişim '08**, Ankara, Türkiye, 19-21 Kasım, 32-56, (2008).

[28] Chadwick, D.W., Otenko, A., "The PERMIS X.509 Role Based Privilege Management Infrastructure", Proceedings of SACMAT' 02, **ACM Press**, 135-140, (2002).

[29] The PERMIS Project, Pilot Sites [online], http://www.permis.org/en/index.html, **(Ziyaret Tarihi: Haziran 2010).**

[30] The PERMIS Project, What is PERMIS? [online], http://www.permis.org/files/Permis_COMPA_v0_6_ENG.zip, **(Ziyaret Tarihi: 10 Mayıs 2010).**

[31] TPM Emulator [online] , https://developer.berlios.de/projects/tpm-emulator **(Ziyaret Tarihi: Temmuz 2006).**

[32] TrouSerS [online], http://trousers.sourceforge.net **(Ziyaret Tarihi: Temmuz 2006).**

[33] European Multilaterally Secure Computing Base (EMSCB) [online], http://www.emscb.de/content/pages/turaya.htm **(Ziyaret Tarihi: Temmuz 2006).**

[34] jTSS Wrapper [online], http://trustedjava.sourceforge.net **(Ziyaret Tarihi: Temmuz 2006).**

[35] Open Trusted Computing (OpenTC) [online], http://www.opentc.net **(Ziyaret Tarihi: Temmuz 2006).**

[36] Trusted GRUB Loader [online], http://www.prosec.rub.de/trusted_grub.html **(Ziyaret Tarihi: Temmuz 2006).**

[37] İmamoğlu, K., Erol, V., Çetin, G., "Enabling Secure Platforms With Trusted Computing", ***Tehoss***, (2006).

[38] Siani, P., "Trusted Computing Platforms: TCPA Technology in Context.", **Prentice Hall**, 8, (2002).

[39] Grasemann, U., Miikkulainen, R., "Effective Image Compression using Evolved Wavelets", **ACM, Genetic and evolutionary computation conference,** 1961-1968, (2005).

[40] Lees, K., "Image Compression Using Wavelets", Yüksek Lisans Tezi, **The University of Sheffield Department of Computer Science**, Mayıs (2002).

[41] Skodrasa, A.N., Christopoulosb, C.A., Ebrahimic, T., "JPEG2000: The Upcoming Still Image Compression Standard," ***IEEE Signal Processing Mag.***, 18, 36-58, (2001).

[42] Acevedo, D. G., Ruedin, A. M. C., "Reduction of Interband Correlation for Landsat Image Compression", **IEEE Computer Society,** (2005).

[43] MESUT, A., CARUS, A., "Kayıpsız Görüntü Sıkıştırma Yöntemlerinin Karşılaştırılması", ***MBGAK***, 93-100, (2005).

[44] Pardus İşletim Sistemi [online], http://www.pardus.org.tr, Haziran (2010).

[45] Mortion, P., Peterson, A., "Image Compression Using the Haar Wavelet Transform", **Math 45 College of the Redwoods**, Dec 19, (1997).

[46] Akkaya, İ., "Kriptolojinin Geçmişi: Bir Şifreleme Algoritması Kullanmadan Önce Son Kullanım Tarihine Bakın", **Bilim ve Teknik Dergisi,** Yıl: 42, Sayı: 500, 24-27, (2009).

[47] Trusted Computing Group (TCG), "TCG Specification v1.2 Architecture Overview" [online], http://www.trustedcomputinggroup.org **(Ziyaret Tarihi: 15 Haziran 2006).**

[48] Heiko Rossnagel, Tobias Murmann, "How secure are current mobile operating systems?" ***Proceedings of the Eighth IFIP TC-6 TC-11 Conference on Communications and Multimedia Security,*** IFIP, 47–58, (2004).

EKLER

EK - A : Açık Anahtar Altyapısı İle İlgili Standartlar

Sayısal sertifikaların oluşturulmasında Açık Anahtar Altyapısı kullanılır. Açık anahtar altyapısında kullanılan veya konuyla ilgili olan standartlar ve açıklamaları aşağıda yer almaktadır.

- ITU X.509 : (ITU-T Recommendation X.509/ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks") Elektronik sertifikanın veri yapısını tarif eder. Bir sertifikanın içine yazılacak bilgilerin hangi sırada ve şekilde yazılacağını anlatır.
- ISO/IEC 7816 : (Identification Cards) Kimlik, kredi kartları ve akıllı kartların özelliklerini tarif eden standart ailesi.
- TS ISO/IEC 17799 : (Information technology - Code of practice for information security management) Bilgi Teknolojisi - Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri standardı.
- ISO/IEC 8824/ITU-T Recommendation X.680: (Information technology - Abstract Syntax Notation One (ASN.1)) ASN veri formatlama dili ile ilgili standartlar ailesi.
- RFC 2560 : (X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP) Çevrimiçi Sertifika Durum Bilgisi protokolü. Bir sertifikanın geçerlilik durumunu sorgulamak için kullanılır.
- RFC 3161 : (Internet X509 Public Key Infrastructure Time-Stamp Protocol) Zaman damgası protokolü. Bir verinin belirli bir tarihte var olduğunu ispat etmek için kullanılır.
- RFC 3279 : (Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile) Sertifika

ve sertifika iptal listesi profilinde kullanılacak algoritmaları ve nesne belirteçlerini tarif eder.

- RFC 3280 : (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile) Sertifika ve sertifika iptal listesi profili. Internette kullanılacak sertifikaların ve sertifika iptal listelerinin içeriğinin ne olacağını tarif eder.
- RFC 3647 : (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework) Sertifika ilkeleri ve sertifika uygulama esasları dokümanlarının nasıl yazılacağını tarif eder.
- RFC 3739 : (Internet X.509 Public Key Infrastructure Qualified Certificates Profile) Kanuni geçerlilik taşıyabilecek nitelikli elektronik sertifikalar için bir yapı tarif eder.
- RFC 3851 : (Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification) Elektronik imzalı ve/veya şifreli e-posta mesajlarının yapısını tarif eden standart.
- RFC 3852 : (Cryptographic Message Syntax - CMS) Elektronik imzalı ve/veya şifreli bilgilerin formatını tarif eden standart.
- RFC 4210 : (Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)) Sertifika taleplerinin ve alımlarının güvenli olarak yapılmasına imkan tanıyan bir standarttır.
- ETSI TS 101733 : (Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats) ETSI tarafından yayınlanan ASN tabanlı elektronik imza standardıdır.
- ETSI TS 101903 : (XML Advanced Electronic Signatures (XAdES)) ETSI tarafından yayınlanan XML tabanlı elektronik imza standardıdır.
- ETSI TS 101862 : (Qualified Certificate Profile) ETSI tarafından yayınlanan nitelikli elektronik sertifika standardıdır.

PKCS (Public Key Cryptography Standards) Standartları, RSA firması tarafından yayınlanmış ve kriptografi dünyasında yaygın kabul görmüş standartlardır.

PKCS 1: RSA açık anahtar algoritması kullanarak şifreleme ve sayısal imzalama işlemi yapılmasını tanımlar.

PKCS 3: Diffie-Hellman anahtar belirleme protokolünü tanımlar.
PKCS 5: Bir parola kelimesinden elde edilen gizli anahtarla şifrelemenin nasıl yapılacağını anlatır.
PKCS 7: Sayısal imzalama ve şifrelemede kullanmak üzere kriptografik yöntemleri destekleyen genel bir mesaj formatı tanımlar.
PKCS 8: Değişik açık anahtar algoritmalarında kullanılabilecek bir özel anahtar formatı tanımlar.
PKCS 9: Diğer PKCS standartlarında kullanılabilecek nitelik tiplerini tanımlar.
PKCS 10: Sertifika talep formatını tanımlar.
PKCS 11: Kriptografik cihazlarda (akıllı kart vb.) kullanılabilecek donanım bağımsız bir programlama kütüphanesini tanımlar. (Cryptoki adıyla da bilinir)
PKCS 12: Bir kullanıcının özel anahtarı, sertifikası gibi bilgileri saklamak ve taşımak için bir format tanımlar.
PKCS 13: Eliptik eğri kriptografi kullanarak şifreleme ve sayısal imzalamayı tanımlar.
PKCS 14: Pseudo-random sayı üretimini tanımlar (geliştirme aşamasında)
PKCS 15: PKCS11'i tamamlayan standarttır. Kriptografik cihaz tiplerini çeşitlendirir ve bu cihazların içinde saklanacak veri formatlarını belirler.

EK - B : Matlab'ta Hazırlanan PCA Kodları

Bu bölümde temel kavramlar bölümünde anlatılan PCA kısmının uygulaması yer almaktadır. Uygulama MATLAB programı kullanılarak hazırlanmıştır.

İki temel bileşen'e göre PCA dönüşüm kodları

```
Veri = [
   2.5000    2.4000
   0.5000    0.7000
   2.2000    2.9000
   1.9000    2.2000
   3.1000    3.0000
   2.3000    2.7000
```

```
   2.0000    1.6000
   1.0000    1.1000
   1.5000    1.6000
   1.1000    0.9000 ]

% temel bileşen sayısı
BilesenSayisi = 2;
% giriş matrisinin ebatlarını bul
[Satirlar, Sutunlar] = size(Veri);
% giriş matrisinin ortalamasını bul
m = mean(Veri);
% değerleri ortalamadan çıkararak giriş matrisini normalize et
DuzVeri = Veri-ones(size(Veri,1),1)*m;
% kovaryans matrisini hesapla
Kovaryans = cov(DuzVeri);
% Öz vektörleri (V) ve öz değerleri (D) kovaryans matrisinden hesapla
[V,D] = eig(Kovaryans);

% öz değerleri azalan biçimde sırala, öncelikle öz değer matrisindeki
% köşegenlerden değerleri al, idx değerleri öz vektörleri sıralamak
% için gerekli bilgikleri tutar.
[D,idx] = sort(diag(D));

D = D(end:-1:1)';
% öz vektörleri öz değerlere göre sırala
V = V(:,idx(end:-1:1));
% Kullanılacak temel bileşenleri seç
V2d=V(:,1:BilesenSayisi);

% son veri öz vektör ile normalize edilmiş değerlerin çarpımı ile oluşur
SonVeri=(V2d'*DuzVeri');

Kovaryans = Kovaryans
```

DuzVeri = DuzVeri
OzVektorler = V
OzDegerler = D
tranSonVeri = SonVeri'

İki temel bileşene göre PCA dönüşüm programının çıktı ekranı

Burada kovaryans, ortalaması alınmış veri, öz değer, öz vektör ve son dönüşüm verisi bulunmaktadır.

Kovaryans =

0.6166	0.6154
0.6154	0.7166

DuzVeri =

0.6900	0.4900
-1.3100	-1.2100
0.3900	0.9900
0.0900	0.2900
1.2900	1.0900
0.4900	0.7900
0.1900	-0.3100
-0.8100	-0.8100
-0.3100	-0.3100
-0.7100	-1.0100

OzVektorler =

0.6779	-0.7352
0.7352	0.6779

OzDegerler =

1.2840	0.0491

```
tranSonVeri =
    0.8280   -0.1751
   -1.7776    0.1429
    0.9922    0.3844
    0.2742    0.1304
    1.6758   -0.2095
    0.9129    0.1753
   -0.0991   -0.3498
   -1.1446    0.0464
   -0.4380    0.0178
   -1.2238   -0.1627
```

İki temel bileşene göre PCA dönüşüm programının çıktıları

Yukarıda yazılan programa ek olarak aşağıdaki kodlar konulunca ilgili verilerin grafiklerini elde ederiz.

```
x1 = [ ] ;
y1 = [ ] ;

for i = 1:10
  x1(i) = Veri(i, 1) ;
  y1(i) = Veri(i, 2) ;
end

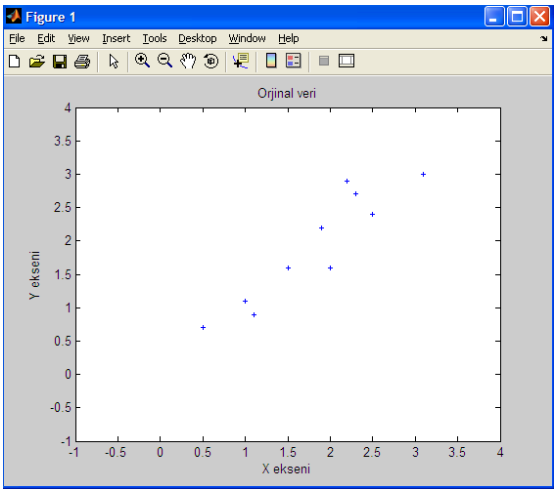
id = plot (x1, y1, '+' );
set (id, 'Marker', '+' )
set (id, 'MarkerSize', 3 )
set (id, 'Color', 'Blue' )
xlabel('X ekseni')
ylabel('Y ekseni')
title('Orjinal veri')
axis([-1 4, -1 4])
```

```
for i = 1:10
  x1(i) = DuzVeri(i, 1) ;
  y1(i) = DuzVeri(i, 2) ;
end

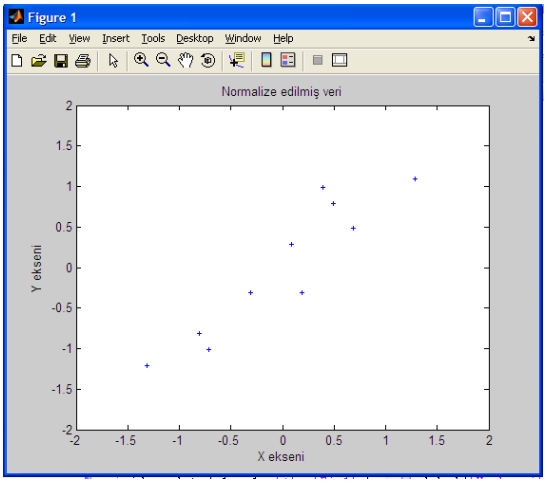
id = plot (x1, y1, '+');
set (id, 'Marker', '+' )
set (id, 'MarkerSize', 3 )
set (id, 'Color', 'Blue' )
xlabel('X ekseni')
ylabel('Y ekseni')
title('Normalize edilmiş veri')
axis([-2 2, -2 2])

for i = 1:10
  x1(i) = tranSonVeri(i, 1) ;
  y1(i) = tranSonVeri(i, 2) ;
end

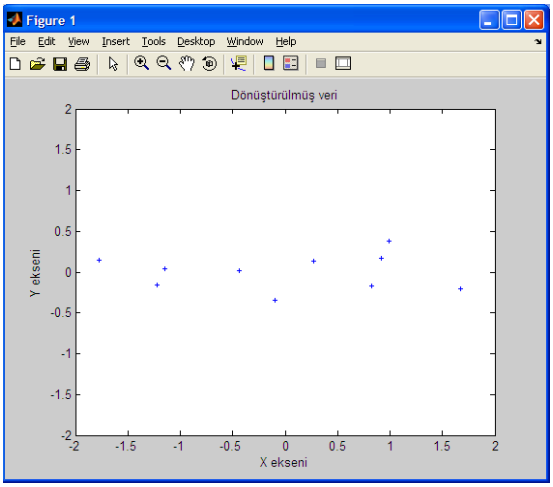
id = plot (x1, y1, '+');
set (id, 'Marker', '+' )
set (id, 'MarkerSize', 3 )
set (id, 'Color', 'Blue' )
xlabel('X ekseni')
ylabel('Y ekseni')
title('Dönüştürülmüş veri')
axis([-2 2, -2 2])
```



Şekil B1: Orijinal verinin grafiği



Şekil B2: Ortalaması alınmış verinin grafiği



Şekil B3: PCA dönüşümü sonucu oluşan verinin grafiği

Tek temel bileşen'e göre PCA dönüşüm kodları

Burada verimizi tek temel bileşene göre dönüştürmek istersek aşağıdaki MATLAB kodlarını kullanabiliriz.

```
Veri = [
   2.5000    2.4000
   0.5000    0.7000
   2.2000    2.9000
   1.9000    2.2000
   3.1000    3.0000
   2.3000    2.7000
   2.0000    1.6000
   1.0000    1.1000
   1.5000    1.6000
   1.1000    0.9000 ]

% temel bileşen sayısı
BilesenSayisi = 1;
% giriş matrisinin ebatlarını bul
[Satirlar, Sutunlar] = size(Veri);
% giriş matrisinin ortalamasını bul
m = mean(Veri);
% değerleri ortalamadan çıkararak giriş matrisini normalize et
DuzVeri = Veri-ones(size(Veri,1),1)*m;
% kovaryans matrisini hesapla
Kovaryans = cov(DuzVeri);
% Öz vektörleri (V) ve öz değerleri (D) kovaryans matrisinden hesapla
[V,D] = eig(Kovaryans);

% öz değerleri azalan biçimde sırala, öncelikle öz değer matrisindeki
% köşegenlerden değerleri al, idx değerleri öz vektörleri sıralamak
% için gerekli bilgikleri tutar.
```

```
[D,idx] = sort(diag(D));

D = D(end:-1:1)';
% öz vektörleri öz değerlere göre sırala
V = V(:,idx(end:-1:1));
% Kullanılacak temel bileşenleri seç
V2d=V(:,1:BilesenSayisi);

% son veri öz vektör ile normalize edilmiş değerlerin çarpımı ile oluşur
SonVeri=(V2d'*DuzVeri');

Kovaryans = Kovaryans
DuzVeri = DuzVeri
OzVektorler = V
OzDegerler = D
tranSonVeri = SonVeri'
```

Tek temel bileşene göre PCA dönüşüm programının çıktıları

```
Kovaryans =
    0.6166    0.6154
    0.6154    0.7166
DuzVeri =
    0.6900    0.4900
   -1.3100   -1.2100
    0.3900    0.9900
    0.0900    0.2900
    1.2900    1.0900
    0.4900    0.7900
    0.1900   -0.3100
   -0.8100   -0.8100
   -0.3100   -0.3100
   -0.7100   -1.0100
```

```
OzVektorler =
    0.6779   -0.7352
    0.7352    0.6779

OzDegerler =
    1.2840    0.0491

tranSonVeri =
    0.8280
   -1.7776
    0.9922
    0.2742
    1.6758
    0.9129
   -0.0991
   -1.1446
   -0.4380
   -1.2238
```

EK - C : Temel Bileşenler Analizi İle İlgili Basit Bir Uygulama

Bu bölümde Temel Bileşenler Analizi' ni basit bir şekilde uygulaması anlatılmaktadır. Temel Bileşenler Analizi' ni uygulayabilmek için bazı adımlardan geçmek gerekir. Bu adımlar aşağıdaki gibidir.

Adım 1 : Biraz veri al

Öncelikle bir veri kümesine ihtiyacımız var. Aşağıdaki örnekte de görüldüğü gibi örnek verimizi 2 boyutludur. Verimizin 2 boyutlu olmasının nedeni, PCA analizinin her adımında neler olduğunu grafiksel olarak gösterebilmektir. Kullanılan veri aşağıdaki tablo ve şekilde gösterilmektedir.

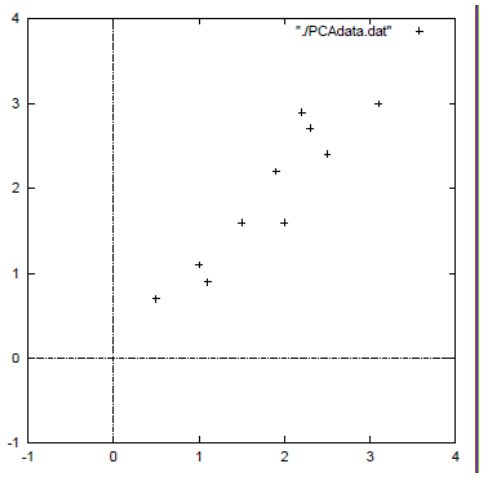
Tablo C1: PCA örnek verisi

Veri =

x	*y*
2.5	2.4
0.5	0.7
2.2	2.9
1.9	2.2
3.1	3.0
2.3	2.7
2	1.6
1	1.1
1.5	1.6
1.1	0.9

Düzeltilmiş Veri =

x	*y*
0.69	0.49
-1.31	-1.21
0.39	0.99
0.09	0.29
1.29	1.09
0.49	0.79
0.19	-0.31
-0.81	-0.81
-0.31	-0.31
-0.71	-1.01



Şekil C1: Orijinal verinin grafiksel olarak gösterimi

Adım 2 : Ortalamayı Çıkar

PCA' yı tam olarak çalıştırabilmek için öncelikle her boyuttaki veriler o boyuttaki ortalama değerden çıkartılması gerekmektedir. Bu işlem sonucu ortalaması sıfır olan bir veri kümesi elde edilir.

Adım 3 : Kovaryans Matrisini Hesapla

Bundan sonraki aşamada kovaryans matrisi hesaplanır. Elimizdeki örnek veri 2 boyutlu olduğundan kovaryans matrisimiz 2 x 2 ebatlarında olacaktır. Hesaplanan kovaryans matrisinin değeri aşağıdaki gibidir.

$$\text{cov} = \begin{pmatrix} .616555556 & .615444444 \\ .615444444 & .716555556 \end{pmatrix} \quad \text{(C.1)}$$

Kovaryans matrisinin köşegeninde yer almayan elemanlar pozitif olduğundan, x ve y değişkenlerinin aynı anda beraber artış gösterdikleri söylenebilir.

Adım 4 : Kovaryans matrisinin öz vektörlerini ve öz değerlerini hesapla

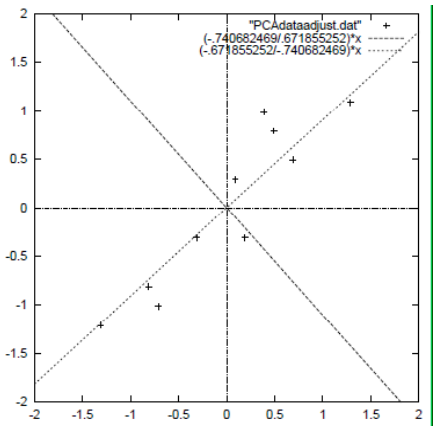
Kovaryans matrisi kare olduğundan bizler bu matrisin öz vektörlerini ve öz değerlerini hesaplayabiliriz. Bunlar bize veri hakkında oldukça önemli bilgiler verdiklerinden dolayı büyük öneme sahiptirler. Hesaplanan öz vektörler ve öz değerler aşağıdaki gibidir.

$$\text{ozdegerler} = \begin{pmatrix} .0490833989 \\ 1.28402771 \end{pmatrix} \quad \text{(C.2)}$$

$$\text{ozvektorler} = \begin{pmatrix} -.735178656 & -.677873399 \\ .677873399 & -.735178656 \end{pmatrix} \quad \text{(C.3)}$$

Buradaki öz vektörler birim öz vektörüdür (unit eigenvector) ve onların uzunluğu 1 birimdir. Bu PCA için çok önemlidir, çoğu matematik program paketlerinde öz vektör bulunması istenildiği zaman program çalıştıktan sonra geri birim öz vektör değerini dönerler.

Şekil C2' de yer alan verinin grafiğine bakıldığında verinin ne kadar güçlü bir örüntüye sahip olduğu görülebilir. Kovaryans matrisinden de anlaşılacağı üzere gerçekten 2 değişkende beraber artıyor. Grafiğin üst kısmında her iki öz vektörde görülmektedir.



Şekil C2: Öz vektörler ile normalleştirilmiş verilerin çizim grafiği

Buradaki grafikte öz vektölerden birisi noktaların ortasından geçtiği görülmektedir. Sanki en uygun çizgi çizilmiş gibi gözüküyor. Buradaki öz vektör bize veri kümesinin birbiri ile nasıl ilişkili olduğunu göstermektedir. Diğer öz vektör de bize daha az önemde, ana çizgideki noktalar ile beraber akan, fakat ana çizgiden belirli mesafede uzak olan verinin örüntüsü hakkında bilgi verir.

Kovaryans matrisindeki öz vektörlerin bulunması işlemi sonucunda bizler veriyi karakterize eden hatları ortaya çıkartabiliriz. Sonraki adımlarda verinin dönüşümü işlemleri gerçekleşir.

Adım 5 : Bileşenlerin seçilmesi ve özellik vektörünün oluşturulması

Bu adımda veri sıkıştırma ve boyut indirgemesi gerçekleşir. Öz vektörler oldukça farklı değerlerdir. Gerçekte en yüksek öz değere sahip öz vektör veri kümesinin temel bileşeni (principle components) olarak kabul edilir. Örneğimizde en büyük öz değere sahip öz vektör verinin ortasını işaret etmektedir. O veri boyutları arasındaki en belirgin ilişkidir.

Genel olarak kovaryans matrisinden öz vektör bulunduktan sonra öz değerler, en yüksekten en düşüğe doğru sıralanır. Bu bize bileşenlerin önemine göre sıralanmış halini verir. İstenirse daha az öneme sahip olan bazı bileşenler dikkate alınmayabilir. Bu durumda bazı bilgiler kaybedilebilir. Fakat eğer öz değerler küçük ise çok fazla bilgi kaybedilmez. Eğer bazı bileşenler hariç tutulursa, son veri kümesinde orjinalde

var olan boyutlardan daha az boyut elde edilir. Daha dikatli olmak gerekirse, orjinal verimizde n boyut var ise n adet öz vektör ve öz değer hesaplanır. Bunlardan sadece ilk p boyutundaki öz vektörler seçilir ve veri kümemiz p boyutunda olmuş olur.

Şu aşamada bizim özellik vektörümüzü (feature vector) oluşturmamız gerekiyor. Kullanılmak istenen öz vektörler, öz vektör listesinden seçilerek özellik vektörü oluşturulur.

$$\text{OzellikVektoru} = (eig_1\ eig_2\ eig_3\ \ldots\ eig_n) \tag{C.4}$$

Verilen örnek veri kümesinde, gerçekte biz 2 öz vektöre sahibiz ve 2 seçeneğimiz var. Öz vektörlerin her ikisini de kullanarak özellik vektörünü oluşturabiliriz.

$$\begin{pmatrix} -.677873399 & -.735178656 \\ -.735178656 & .677873399 \end{pmatrix} \tag{C.5}$$

Yada küçük olan ve daha az öneme sahip bileşeni atmayı seçersek tek kolonlu bir özellik vektörü elde ederiz.

$$\begin{pmatrix} -.677873399 \\ -.735178656 \end{pmatrix} \tag{C.6}$$

Adım 6 : Yeni veri kümesinin çıkarılması

Bu Temel Bileşenler Analizinde (PCA) en son ve en kolay adımdır. Bir kere verimizde tutmak istediğimiz öz vektörleri seçtiğimiz ve özellik vektörünü oluşturduğumuz zaman, basit bir şekilde vektörün transpozunu alır ve orjinal veri kümesinin solundan transpozu alınmış vektör çarpılır.

$$SonVeri = SatirOzellikVektoru \ x \ SatirDuzeltilmisVerisi, \tag{C.7}$$

Buradaki eşitlikte yer alan SatirOzellikVektoru adlı vektör, transpozu alınmış kolonların öz vektörlerin matrisidir. Böyece öz vektörler satırlarda, en önemli öz vektör de en üstte olacak şekilde yer alır. SatirDuzeltilmisVerisi adlı değişken ise ortalaması ayarlanmış verinin transpozudur (her kolonda veri öğeleri yer alması ile

her satırda ayrı boyutların tutulması gibi). SonVeri, kolonlarda veri öğelerinin ve satırlarda boyutların yer aldığı son veri kümesidir.

Bu işlem sonucunda sadece seçtiğimiz vektörlerin orjinal verisini elde edeceğiz. Bizim orjinal verimiz x ve y olmak üzere 2 eksene sahiptir, bu yüzden verimizde onlar ile aynı şartlardadır. İstediğimiz koşullarda herhangi 2 eksende veriyi ifade etmek mümkündür. Eğer bu eksenler birbirine dik ise o zaman ifadeler daha fazla etkili olur. Bu da öz vektörlerin birbirlerine her zaman dik olmasının nedenini açıklar. X ve Y eksenlerinde yer alan verimiz şu anda 2 öz vektör şekline dönüştü. Veri kümesinin boyutunun azaldığı durumlarda bazı öz vektorleri dikkate almadık. Yeni verimiz sadece tutmak istediğimiz vektörlerden oluştu.

Bunu verimizde göstermek için mümkün olan tüm özellik vektörlerinin son dönüşümü yapılır. Her adımdaki sonuçların transpozu alınarak verinin tablo şeklinde daha anlaşılır olması yapılır. Bileşenlerin birbirleri ile nasıl bir ilişkiye sahip olduğu da göstermek için son noktaların grafiği çizilmiştir.

Dönüşümde her iki öz vektörün tutulduğu durumu dikkate alırsak Şekil 2.34' teki çizim elde edilmiş olur. Bu çizim temel olarak orjinal veridir, döndürülmüştür, böylece öz vektörler eksenleri oluşturmaktadır. Sıkıştırma işleminden sonra geri dönüşümü yaptığımız zaman hiç bir bilgiyi kaybetmediğimiz anlaşılabilir.

Yapabileceğimiz bir diğer dönüşümde en büyük öz değere sahip olan, öz vektörün alınması ile yapabiliriz. Buna göre işlem yaptığımızda oluşan verinin çizimi Tablo C1' de gösterilmiştir. Beklendiği gibi sadece tek bir boyuta sahiptir. Eğer bu veri kümesi, her iki öz vektörün kullanıldığı sonuçlar ile karşılaştırılırsa, diğerindeki birinci sütün ile tam olarak aynı olduğu görülebilir. Böylece bu veriyi çizdiğiniz zaman tek boyut oluşur. Bu da Şekil C3' teki çizimde gösterilen x' in noktalarına karşılık gelir. Diğer öz vektörün yer aldığı ekseni etkili bir şekilde atmış olduk.

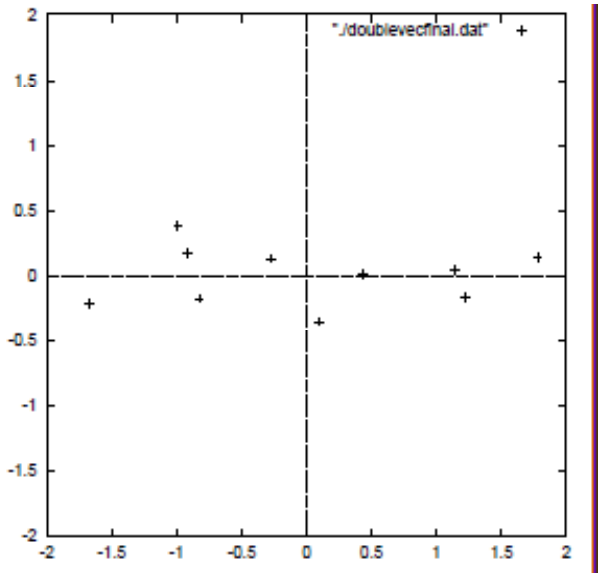
Bu adımda temel olarak verimizin dönüşümünü aldık, böylece onlar arasındaki örüntüler ile ifade edilmiş oldu. Burada örüntüler çizgi şeklindedir ve bunlar daha çok birbiri ile ilişkili olan verileri gösterir. Satırların herbirinin katılımının birleşimi

ile verimizdeki noktaları sınıflandırmış olunması yararlıdır. Başlangıçta x ve y eksenlerimiz vardı. Bu güzel, fakat her veri noktasındaki x ve y değerleri geri kalan noktalarla nasıl bir ilişkinin olduğunu bize söylememektedir. Veri noktalarının değerleri, akış çizgilerinin ne tarafa doğru olduğunu bize söyler. Her iki öz vektörün kullanıldığı dönüşüm durumunda, basit bir şekilde veriyi değiştirdik. Böylece genel eksenler yerine buradaki öz vektörler şeklinde ifade edilmiş oldu. Fakat tek öz vektörün kullanıldığı geri dönüşümde katılım en düşük öz vektörden dolayı silinmiş oldu.

Tablo C2: PCA yöntemi ile dönüştürülmüş veri

Dönüştürülmüş Veri =

x	*y*
-0.827970186	-0.175115307
1.77758033	0.142857227
-0.992197494	0.384374989
-0.274210416	0.130417207
-1.67580142	-0.209498461
-0.912949103	0.175282444
0.0991094375	-0.349824698
1.14457216	0.0464172582
0.438046137	0.0177646297
1.22382056	-0.162675287



Şekil C3: PCA analizi uygulanmış verinin tablosu ve yeni veri noktalarının çizimi

Tablo C3: Sadece en önemli öz vektor kullanılarak dönüşümü yapılmış veri

x
-0.827970186
1.77758033
-0.992197494
-0.274210416
-1.67580142
-0.912949103
0.0991094375
1.14457216
0.438046137

Adım 7 : Eski verinin geri alınması

PCA dönüşümü veri sıkıştırmak için kullanılmış ise orjinal verinin geri alınması büyük bir iştir. Şimdi geri dönüşüm işinin nasıl yapıldığına bakalım. Öncelikle dönüşümümüzde eğer tüm öz vektörler kullanılmış ise orjinal verimizi elde edebiliriz. Eğer son dönüşümde öz vektörlerin sayısını azaltmış isek geri dönüşümde bazı bilgileri kaybetmiş olarak alırız.

Son dönüşüm aşağıdaki gibiydi.

$$\text{SonVeri} = \text{SatirOzellikVektoru} \times \text{SatirDuzeltilmisVerisi} \quad \text{(C.8)}$$

Orjinal veriyi almak için yukarıdaki denklemi aşağıdaki denklem haline getirebiliriz.

$$\text{SatirDuzeltilmisVerisi} = \text{SatirOzellikVektoru}^{-1} \times \text{SonVeri} \quad \text{(C.9)}$$

$\text{SatirOzellikVektoru}^{-1}$ ifadesi SatirOzellikVektoru' nün tersidir. Bununla beraber özellik vektörümüzdeki tüm öz vektörleri aldığımız zaman, özellik vektörümüzün tersi özellik vektörümüzün tanspozesine eşittir. Bu sadece matrisin elemanlarının hepsi birim öz vektör olduğu durum için doğrudur. Bu bize dönen parçayı verimizi için daha kolay yapar çünkü denklem aşağıdaki gibi olur.

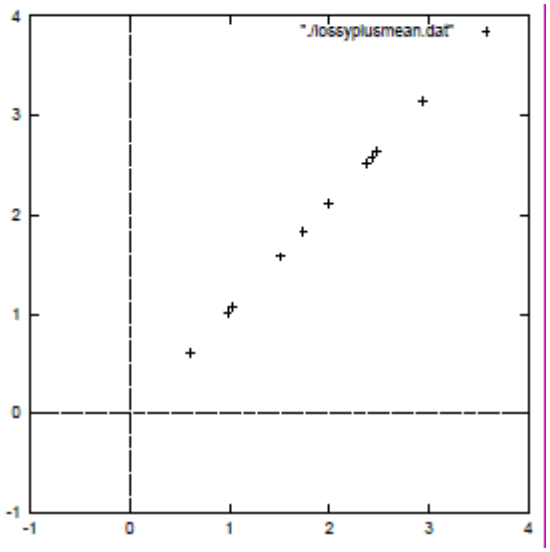
$$\text{SatirDuzeltilmisVerisi} = \text{SatirOzellikVektoru}^{T} \times \text{SonVeri} \quad \text{(C.10)}$$

Fakat orjinal veriyi geri alabilmek için bu orjinal verinin ortalamasına ekleme yapmamız gerekmektedir. Bu yüzden bütünlük için;

$$SatirOrjinalVerisi = (SatirOzellikVektoru^{T} \times SonVeri) + OrjinalOrtalama \quad (C.11)$$

Bu formul özellik vektöründeki bütün öz vektörler kullanılmadığı zaman da da uygulanabilir. Hatta bazı öz vektörler hariç tutulduğunda yukarıdaki denklem doğru dönüşümü yapacaktır.

Tam özellik vektörü ile geri dönüşümde aynı değerler elde edilirken Şekil C4 te görüldüğü gibi azaltılmış özellik vektörü bize bilgilerin nasıl kaybedildiğini gösteriyor.



Şekil C4: Tek öz vektör kullanılarak türetilen verinin yeniden oluşturulması

Şekil C1' de yer alan orjinal çizim ile karşılaştırıldığında temel öz vektörler arasındaki değişim tutulurken, diğer bileşenler arasındaki değişim kaybolur.

EK - D : Dalgacık Tabanlı Dönüşüm İle Görüntü Sıkıştırma

Dalgacık tabanlı dönüşüm için orijinal görüntü ile işleme başlayacağız. Orjinal görüntüde, her pikselde yer alan renk değeleri matrisin bir bileşeni gibi gösterilir. Bu matristeki en düşük değer siyahı, en yüksek değer ise beyazı ifade eder. Ortalama ve

fark alma diye adlandırılan yöntemi kullanarak aynı matrisi daha az bir şekilde yeni bir matris ile ifade edeceğiz. Daha sonra bu görüntüyü sıkıştırmak için gereksiz bazı bilgileri eleyip orijinal görüntüye benzeyen bir duruma varacağız [45].

EK - D.1. Ortalama Ve Fark Alma

Ortalama ve fark alma işlemini daha basit anlatabilmek için 8x8' lik matrisin sadece ilk satırını alıyoruz. Bu satır aşağıda gösterilmiştir. Matrisimiz 8x8 ebatlarında olduğundan dönüşüm işlemi 3 adımda ($2^3 = 8$) gerçekleşecektir.

$$[3 \quad 5 \quad 4 \quad 8 \quad 13 \quad 7 \quad 5 \quad 3] \tag{D.1}$$

Adım 1 : İlk adımda yukarıdaki satırdaki elemanları çifter çifter gruplara ayırıp ortalamalarını alıyoruz. Ortalamasını aldığımız değerler yeni ifadenin ilk dört sayısını meydana getirecektir. Kalan dört sayıda her çiftin ilk elemanının o çiftin ortalamasından çıkarılması ile bulunur (3 - 4 = -1, 4 – 6 = -2 vb gibi). Bu değerler detay katsayıları diye adlandırılır. İlk adımdan sonra oluşan değerlerden ilk dört tanesi ortalamayı, kalan dört taneside detay katsayılarını (koyu ifade ile yazılan elemanlar) aşağıdaki gibi gösterir.

$$[4 \quad 6 \quad 10 \quad 4 \quad -1 \quad -2 \quad 3 \quad 1] \tag{D.2}$$

Adım 2 : Yukarıda sekiz elaman için uyguladığımız yöntemin aynısını yeni satırdaki ilk dört eleman için uygulayacağız. Ve sonuç olarak elde ettiğimiz ifadenin ilk iki eleman ortalamaları, sonraki iki elemanda onların uygun detay katsayılarını ifade eder. Sonraki dört adet detay katsayısıda önceki adımda bulduğumuz değerlerden alınır. Ve ikinci adımda oluşan ifade aşağıdaki gibi olur.

$$[5 \quad 7 \quad \mathbf{-1} \quad \mathbf{3} \quad -1 \quad -2 \quad 3 \quad 1] \tag{D.3}$$

Adım 3 : Aynı ortalama ve fark alma yöntemini kalan çift içinde gerçeklenirse üçüncü adım tamamlanmış olur. Son altı eleman daha önce yaptığımız gibi önceki

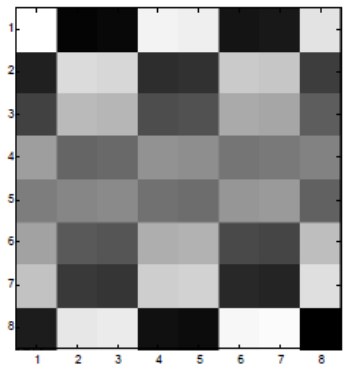
adımda üretilen değerlerden taşınır. Şimdi aşağıda da gösterildiği gibi yeni ifademize sahibiz. Buradaki satırdaki ilk eleman ortalamayı kalan yedi elemanda detay katsayılarını belirtir.

$$[\,6 \quad \mathbf{-1} \quad -1 \quad 3 \quad -1 \quad -2 \quad 3 \quad 1\,] \tag{D.4}$$

EK - D.2. Görüntünün Temsili

Şimdi aynı ortalama ve fark alma adımlarını tüm matrisimize uygulayabiliriz. Aşağıdaki A matrisi, Şekil D1' deki görüntüyü ifade eder. Dikkat edilirse matriste yer alan büyük bileşenler, gri renk tonundaki daha açık olan renkleri gösteriyor.

$$A = \begin{bmatrix} 64 & 2 & 3 & 61 & 60 & 6 & 7 & 57 \\ 9 & 55 & 54 & 12 & 13 & 51 & 50 & 16 \\ 17 & 47 & 46 & 20 & 21 & 43 & 42 & 24 \\ 40 & 26 & 27 & 37 & 36 & 30 & 31 & 33 \\ 32 & 34 & 35 & 29 & 28 & 38 & 39 & 25 \\ 41 & 23 & 22 & 44 & 45 & 19 & 18 & 48 \\ 49 & 15 & 14 & 52 & 53 & 11 & 10 & 56 \\ 8 & 58 & 59 & 5 & 4 & 62 & 63 & 1 \end{bmatrix} \tag{D.5}$$



Şekil D1: Yakınlaştırılmış bir görüntü

Eğer her satıra ortalama ve fark almayı uygularsak elde ettiğimiz matristeki ilk kolonda satır ortalamaları ve kalan bileşenlerde o satırın detay katsayılarını belirtir.

$$\begin{bmatrix} 32.5 & 0 & .5 & .5 & 31 & -29 & 27 & -25 \\ 32.5 & 0 & -.5 & -.5 & -23 & 21 & -19 & 17 \\ 32.5 & 0 & -.5 & -.5 & -15 & 13 & -11 & 9 \\ 32.5 & 0 & .5 & .5 & 7 & -5 & 3 & -1 \\ 32.5 & 0 & .5 & .5 & -1 & 3 & -5 & 7 \\ 32.5 & 0 & -.5 & -.5 & 9 & -11 & 13 & -15 \\ 32.5 & 0 & -.5 & -.5 & 17 & -19 & 21 & -23 \\ 32.5 & 0 & .5 & .5 & -25 & 27 & -29 & 31 \end{bmatrix} \quad \text{(D.6)}$$

Ortalama ve fark alma yöntemlerini eğer kolonlara uygular isek aşağıdaki matrisi elde ederiz.

$$\begin{bmatrix} 32.5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & -4 & 4 & -4 \\ 0 & 0 & 0 & 0 & 4 & -4 & 4 & -4 \\ 0 & 0 & .5 & .5 & 27 & -25 & 23 & -21 \\ 0 & 0 & -.5 & -.5 & -11 & 9 & -7 & 5 \\ 0 & 0 & .5 & .5 & -5 & 7 & -9 & 11 \\ 0 & 0 & -.5 & -.5 & 21 & -23 & 25 & -27 \end{bmatrix} \quad \text{(D.7)}$$

Şimdi elde ettiğimiz matris, görüntümüzü daha kısa bir şekilde ifade eder. Burada genel ortalama matrisin üst sol köşesinde yer alır. Geri kalan bileşenler, görüntünün belirtilen bölgesindeki tüm detayların detay katsayılarını ifade eder. Bunları bildiğimizden dolayı, matrisimizdeki bazı bilgileri eleyebilir ve elememize rağmen orijinal matrisimize yakın iyi bir değer elde edebiliriz. Bunu yapmak için biz bir sayı seçeriz (δ) ve burada seçtiğimiz δ sayısının ağırlığından daha az olan elemanları sıfıra eşitleriz.

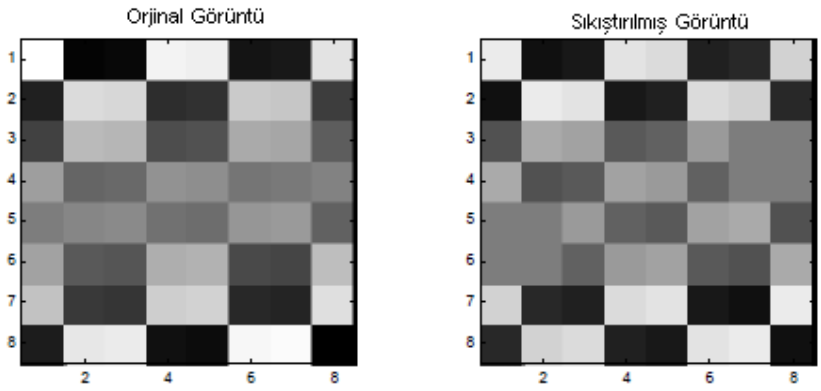
$\delta = 5$ olarak seçilmesi detay katsayılarından (koyu) 18 tanesinin elenmesine neden olur.

$$\begin{bmatrix} 32.5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 27 & -25 & 23 & -21 \\ 0 & 0 & 0 & 0 & -11 & 9 & -7 & 0 \\ 0 & 0 & 0 & 0 & 0 & 7 & -9 & 11 \\ 0 & 0 & 0 & 0 & 21 & -23 & 25 & -27 \end{bmatrix} \quad \text{(D.8)}$$

Orijinal matrisimize yakın bir değere ulaşmak için ortalama ve fark alma işlemlerinin tersini uygularız.

$$\begin{bmatrix} 59.5 & 5.5 & 7.5 & 57.5 & 55.5 & 9.5 & 11.5 & 53.5 \\ 5.5 & 59.5 & 57.5 & 7.5 & 9.5 & 55.5 & 53.5 & 11.5 \\ 21.5 & 43.5 & 41.5 & 23.5 & 25.5 & 39.5 & 32.5 & 32.5 \\ 43.5 & 21.5 & 23.5 & 41.5 & 39.5 & 25.5 & 32.5 & 32.5 \\ 32.5 & 32.5 & 39.5 & 25.5 & 23.5 & 41.5 & 21.5 & 21.5 \\ 32.5 & 32.5 & 25.5 & 39.5 & 41.5 & 23.5 & 43.5 & 43.5 \\ 53.5 & 11.5 & 9.5 & 55.5 & 57.5 & 7.5 & 5.5 & 59.5 \\ 11.5 & 53.5 & 55.5 & 9.5 & 7.5 & 57.5 & 59.5 & 5.5 \end{bmatrix} \quad \text{(D.9)}$$

Şekil D2' deki sıkıştırılmış görüntüde görüldüğü gibi bu işlemi kullanarak orijinal görüntüye yakın bir değer elde ederiz. Görüntüdeki detayların bazılarını kaybettik, fakat kaybedilen değerler çoğu durumda fark edilmeyecek kadar düşük seviyededir.



Şekil D2: Orjinal ve sıkıştırılmış görüntü

EK - D.3. Lineer Cebir Yönteminin Kullanılması

Ortalama ve fark alma yöntemlerini lineer cebir kullaranarak uygulanabilir. Bunun için ortalama ve fark alma işlemlerinin uç adımını da gerçekleyen üç adet matrisi (A_1, A_2, A_3) kullanırız.

Adım 1 : İfademizi ilk matris ile çarptığımız zaman, elde edilen değerde ilk dört sütün her çiftin ortalamasını ve son dört sütünda uygun farkları verir.

$$\begin{bmatrix} 3 & 5 & 4 & 8 & 13 & 7 & 5 & 3 \end{bmatrix} \begin{bmatrix} 1/2 & 0 & 0 & 0 & 1/2 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 0 & -1/2 & 0 & 0 & 0 \\ 0 & 1/2 & 0 & 0 & 0 & 1/2 & 0 & 0 \\ 0 & 1/2 & 0 & 0 & 0 & -1/2 & 0 & 0 \\ 0 & 0 & 1/2 & 0 & 0 & 0 & 1/2 & 0 \\ 0 & 0 & 1/2 & 0 & 0 & 0 & -1/2 & 0 \\ 0 & 0 & 0 & 1/2 & 0 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 1/2 & 0 & 0 & 0 & -1/2 \end{bmatrix}$$

$$= \begin{bmatrix} 4 & 6 & 10 & 4 & -1 & -2 & 3 & 1 \end{bmatrix} \quad \text{(D.10)}$$

Adım 2 : İkinci matriste oldukça benzer bir yöntemle çalışır. İlk dört sütün, şimdi ortalama ve fark alma işlemlerini kalan çiftler için gerçekler. Benzer matrisin son dört kolonu birinci adımdan detay katsayılarından alınır.

$$\begin{bmatrix} 4 & 6 & 10 & 4 & -1 & -2 & 3 & 1 \end{bmatrix} \begin{bmatrix} 1/2 & 0 & 1/2 & 0 & 0 & 0 & 0 & 0 \\ 1/2 & 0 & -1/2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1/2 & 0 & 1/2 & 0 & 0 & 0 & 0 \\ 0 & 1/2 & 0 & -1/2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 5 & 7 & -1 & 3 & -1 & -2 & 3 & 1 \end{bmatrix} \quad \text{(D.11)}$$

Adım 3 : Son adıma benzer olarak ortalama ve fark alma işlemi matrisin ilk iki kolonu için gerçeklenir. Sonra benzer matris detay katsayılarını ikinci adımdan buraya taşır.

$$\begin{bmatrix} 5 & 7 & -1 & 3 & -1 & -2 & 3 & 1 \end{bmatrix} \begin{bmatrix} 1/2 & 1/2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1/2 & -1/2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 6 & -1 & -1 & 3 & -1 & -2 & 3 & 1 \end{bmatrix} \quad \text{(D.12)}$$

Bu süreci basitleştirmek için bu üç matrisi birbiri ile çarpıp tek bir dönüşüm matrisi ($W = A_1A_2A_3$) elde edebiliriz. A_1, A_2 ve A_3 matrislerini birbirleri ile çarptığımızda elde edilen dönüşüm matrisi (W) aşağıdaki gibidir.

$$W = A_1A_2A_3 = \begin{bmatrix} 1/8 & 1/8 & 1/4 & 0 & 1/2 & 0 & 0 & 0 \\ 1/8 & 1/8 & 1/4 & 0 & -1/2 & 0 & 0 & 0 \\ 1/8 & 1/8 & -1/4 & 0 & 0 & 1/2 & 0 & 0 \\ 1/8 & 1/8 & -1/4 & 0 & 0 & -1/2 & 0 & 0 \\ 1/8 & -1/8 & 0 & 1/4 & 0 & 0 & 1/2 & 0 \\ 1/8 & -1/8 & 0 & 1/4 & 0 & 0 & -1/2 & 0 \\ 1/8 & -1/8 & 0 & -1/4 & 0 & 0 & 0 & 1/2 \\ 1/8 & -1/8 & 0 & -1/4 & 0 & 0 & 0 & -1/2 \end{bmatrix} \quad \text{(D.13)}$$

Orijinal ifademizi sadece dönüşüm matrisi ile çarptığımızda, direkt olarak orijinal ifademizden üçüncü adımdaki sonucu elde ederiz.

$$[3\ \ 5\ \ 4\ \ 8\ \ 13\ \ 7\ \ 5\ \ 3] \begin{bmatrix} 1/8 & 1/8 & 1/4 & 0 & 1/2 & 0 & 0 & 0 \\ 1/8 & 1/8 & 1/4 & 0 & -1/2 & 0 & 0 & 0 \\ 1/8 & 1/8 & -1/4 & 0 & 0 & 1/2 & 0 & 0 \\ 1/8 & 1/8 & -1/4 & 0 & 0 & -1/2 & 0 & 0 \\ 1/8 & -1/8 & 0 & 1/4 & 0 & 0 & 1/2 & 0 \\ 1/8 & -1/8 & 0 & 1/4 & 0 & 0 & -1/2 & 0 \\ 1/8 & -1/8 & 0 & -1/4 & 0 & 0 & 0 & 1/2 \\ 1/8 & -1/8 & 0 & -1/4 & 0 & 0 & 0 & -1/2 \end{bmatrix}$$

$$= [6\ \ -1\ \ -1\ \ 3\ \ -1\ \ -2\ \ 3\ \ 1] \quad \text{(D.14)}$$

Aşağıdaki denklemler ile bizler bu süreci matris çarpımları şeklinde basitleştiriyoruz. Buradaki birinci denklem ortalama ve fark almayı belirtirken, ikinci denklem buradaki işlemlerin tersini alır.

1. $T = ((AW)^T W)^T$ (D.15)

   $T = (W^T A^T W)^T$ (D.16)

   $T = W^T (A^T)^T (W^T)^T$ (D.17)

   $T = W^T A W$ (D.18)

2. $(W^{'})^{-1}\ TW^{-1} = A$ (D.19)

   $(W^{-1})^{'}\ TW^{-1} = A$ (D.20)

EK - D.4. Dalgacık Tabanlı Yöntemde Görüntü Sıkıştırma

Daha büyük ölçeklerde bu dönüşümün nasıl çalıştığını anlamak için buradaki görüntüleri farklı derecelerde sıkıştırdık. İlk baştaki orjinal görüntüyü, ondan sonrakiler de sıra ile daha iyi durumda olan benzerini belirtir.

Şekil D4' deki görüntü, en büyük ölçeğe göre ortalama ve fark alma adımları gerçeklendikten sonra, delta' nın oldukça büyük değeri seçilerek sıkıştırıldı. Bu dönüşüm matrisinden az sayıda bileşeni elimine etti. Bu dönüşüm matrisi orjinal matristeki 65,536 değere karşın sadece 631 adet sıfır olmayan elemana sahiptir. Sıkıştırma oranı yaklaşık olarak 103' e 1 oranındadır. Matriste sadece sıfır olmayan sayılar ve bu sayıların konumlarının kullanılması ile matrisin saklanması için daha az

yer gerekecek ve iletim daha hızlı gerçekleşecektir. Görüntünün sıkıştırılması ile gereksiz yere kullanılabilinecek yeri göstermiş olduk. Fakat Şekil D3' de gösterildiği gibi detayın büyük bir bölümü kayıp ve onun kullanışsızlığı sorgulanabilir.

Daha küçük delta değerinin seçildiği Şekil D5' de gösterildiği gibi orta seviyedeki daha uygun değere ulaşılır. Burada dönüşüm matrisi 1,411 değer için sıfır değildir ve sıkıştırma oranı yaklaşık 46' ya 1 oranındadır. Görüntüde arşivelenen detay yükarıda belirtildiği gibi kabul edilebilir. Yine de biz yüksek sıkıştırma oranı elde etmiş olduk.

Son görüntü en az sıkıştırılmıştır. Orjinal matrsite 65,536 giriş var iken dönüşüm matrisinde 9,060 tane sıfır olmayan giriş değerine sahiptir. Bu da bize 7' ye 1 oranında bir sıkıştırma sağlar. Burada biz orjinal görüntü için daha iyi bir sıkıştırma oranına sahipiz.



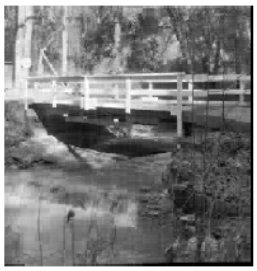
Şekil D3: Orjinal görüntü



Şekil D4: 103'e 1 oranında sıkıştırılmış görüntü



Şekil D5: 46'ya 1 oranında sıkıştırılmış görüntü



Şekil D6: 7'ye 1 oranında sıkıştırılmış görüntü

Yukarıdaki görüntüler bir görüntü için mümkün olan birkaç ihtimali gösterir. Buradaki yaklaşımların her biri farklı durumlar için uygun olabilir. Örneğin Şekil D5' de yer alan görüntü İnternet üzerinden orjinal görüntüye göre daha hızlı iletilebilir. Burada kullanıcıya tüm görüntünün yüklenmesi için beklemek isteyip istemediği seçeneği sorulabilir yada basit bir şekilde görüntü gönderilebilir. Benzerlikler daha iyi oldukça, görüntülerde gitgide daha kullanışlı olurlar. Örneğin Şekil D6' daki görüntü orjinal görüntüye çok benzer olduğundan orjinal resim kadar kullanışlı olabilir.

EK - E : Şifreleme Yöntemleri

Dalgacık tabanlı dönüşüm için orijinal görüntü ile işleme başlayacağız. Orjinal görüntüde, her pikselde yer alan renk değeleri matrisin bir bileşeni gibi gösterilir. Bu matristeki en düşük değer siyahı, en yüksek değer ise beyazı ifade eder. Ortalama ve fark alma diye adlandırılan yöntemi kullanarak aynı matrisi daha az bir şekilde yeni bir matris ile ifade edeceğiz. Daha sonra bu görüntüyü sıkıştırmak için gereksiz bazı bilgileri eleyip orijinal görüntüye benzeyen bir duruma varacağız [33].

EK - E.1. Basit Şifreleme Yöntemleri

Basit şifreleme yöntemleri genellikle kağıt kalem kullanarak gerçekleştirilebilen, çok karışık matematik temellere dayanmayan sistemlerdir. En gelişmiş örnekleri mekanik cihazlar olan basit şifreleme yöntemleri, elektronik cihazların kullanılmaya başlanmasıyla beraber ortadan kalkmıştır [2].

MÖ 5. yüzyılda Ispartalıların geliştirdiği cihaz ile tarihin ilk yer değiştirme sistemini uygulamışlardır. Bu cihaz Şekil E1' de gösterildiği gibi belli kalınlıkta bir tahta silindirden ve silindirin etrafına eğik biçimde sarılmış papirüs ya da ince, deri bir şeritten oluşuyordu. Gizli mesaj silindir boyunca silindire sarılı şerit üzerine yazılıyor, daha sonra şerit silindirden çözülüyordu. Birbirinden ayrılan harfler yeniden aynı kalınlıkta bir tahta silindire sarılmadıkça hiçbir anlam ifade etmiyordu.



Şekil E1**:** Ispartalıların kullandığı kripto cihazı [46]

En çok bilinen basit şifreleme yöntemi "Mono Alfabetik Şifreleme" yöntemidir. Bu yönteme göre harfler kendisinden birkaç harf sonra gelecek harf ile yer değiştirme yapılır. Şifrelenecek metindeki harfler alfabede 3 harf kaydırılarak değiştirilir. Bu şifreleme yönteminin diğer bir adı da Sezar Şifreleme algoritmasıdır.

Sezar Şifresi : ci = E(pi) = pi+3
Açık Mesaj : Gizli Bilgi
Şifreli Mesaj : Ilcol Dloıl

Bu yöntemin biraz daha gelişmişi olan tablo yönteminde ise alfabedeki her harf başka bir harfle yer değiştirir ama bu bir kurala bağlı olmadan karışık bir şekilde yapılır.

ABCÇDEFGĞHIİJKLMNOÖPRSŞTUÜVYZ



CÇAVYJŞÜZKÖTUENOİPFGILĞHRMBDS

Şekil E2: Tablo yöntemi ile harf değiştirme

Mono alfabetik şifreleme yöntemleri bilgisayar yardımıyla çok kısa sürede kırılabilir. Bu yöntemler kullanılan dildeki harflerin yerini değiştirir ama harflerin kullanım sıklığını (frekansını) değiştirmez. Örneğin Türkçe'de en çok kullanılan harf olan "a" harfi tablo yöntemi kullanılarak "c" harfi ile yer değiştirilirse elde edilecek şifreli metinde en çok tekrar eden harfin "c" olduğu görülür ve bunun "a" harfi olabileceği tahmin edilerek şifre çözülmeye başlanabilir. Bir diğer basit şifreleme yöntemi "Poli Alfabetik Şifreleme" dir. Bu tip şifrelemede, mono alfabetik yöntemlerden farklı olarak bir harf değiştirilince her seferinde aynı harfe dönüşmez. Bu yöntemlere güzel bir örnek Şekil E3' de gösterilen Vigenere tablosudur.

	0					5					10					15		
	A	**B**	**C**	**Ç**	**D**	**E**	**F**	**G**	**Ğ**	**H**	**I**	**İ**	**J**	**K**	**L**	**M**	**N**	**O**
A	a	b	c	ç	d	e	f	g	ğ	h	ı	i	j	k	l	m	n	o
B	b	c	ç	d	e	f	g	ğ	h	ı	i	j	k	l	m	n	o	ö
C	c	ç	d	e	f	g	ğ	h	ı	i	j	k	l	m	n	o	ö	p
Ç	ç	d	e	f	g	ğ	h	ı	i	j	k	l	m	n	o	ö	p	r
D	d	e	f	g	ğ	h	ı	i	j	k	l	m	n	o	ö	p	r	s
E	e	f	g	ğ	h	ı	i	j	k	l	m	n	o	ö	p	r	s	ş
F	f	g	ğ	h	ı	i	j	k	l	m	n	o	ö	p	r	s	ş	t
G	g	ğ	h	ı	i	j	k	l	m	n	o	ö	p	r	s	ş	t	u
Ğ	ğ	h	ı	i	j	k	l	m	n	o	ö	p	r	s	ş	t	u	ü
H	h	ı	i	j	k	l	m	n	o	ö	p	r	s	ş	t	u	ü	v
I	ı	i	j	k	l	m	n	o	ö	p	r	s	ş	t	u	ü	v	y
İ	i	j	k	l	m	n	o	ö	p	r	s	ş	t	u	ü	v	y	z
J	j	k	l	m	n	o	ö	p	r	s	ş	t	u	ü	v	y	z	a
K	k	l	m	n	o	ö	p	r	s	ş	t	u	ü	v	y	z	a	b
L	l	m	n	o	ö	p	r	s	ş	t	u	ü	v	y	z	a	b	c
M	m	n	o	ö	p	r	s	ş	t	u	ü	v	y	z	a	b	c	ç

Şekil E3: Vignere tablosu [46]

Bu yöntemde oluşturulan tablo ve bir anahtar kelime kullanılarak şifreleme yapılır.

Şifreleme

Açık Mesaj (sütun) : BULUŞ MAYER İANKA RA

Anahtar Kelime (satır) : KALEM KALEM KALEM KALEM ...

Şifreli Mesaj : LUZAĞ ZAJIF UABÖM DA...

Şifre Çözme

Şifreli Mesaj (tablo) : LUZAĞ ZAJIF UABÖM DA...

Anahtar Kelime (satır) : KALEM KALEM KALEM KALEM ...

Açık Mesaj (sütun) : BULUŞ MAYER İANKA RA

Poli alfabetik şifreleme yöntemleri de bilgisayar yardımıyla ve frekans sayımı ile çok kolay ve çabuk çözülebilmektedir.

Başka bir basit şifreleme tekniği de "Tek Kullanımlık Karakter Dizisi (One-time Pad)" yöntemidir. Bu yöntemde rastgele üretilen bir karakter (harf veya rakam) dizisi kullanılarak şifreleme yapılır. Açık mesaj içinde yer alan her karakter, üretilen dizide karşısına denk gelen karakterle işleme sokularak (Örneğin modüler toplama işlemi) şifreli mesaj elde edilir. Mesajı çözmek için rastgele dizinin bilinmesi gereklidir. Bu yönteme Vernam şifreleme yöntemi denir.

Açık Mesaj : BULUSMAYERIANKARA

Rastgele Dizi : DEFRYPLCNMLJKHFGH

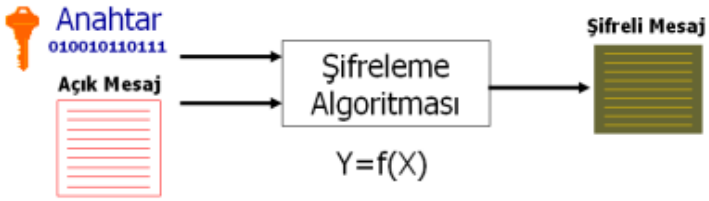
Şifreli Mesaj : RLDYDOY....

Bu yöntemin güvenliği rastgele üretilen diziye bağlıdır. Bu dizi gerçekten rastgele üretilmelidir, eğer bir kurala bağlı olarak üretilirse ve bu kural saldırgan tarafından bilinirse sistem kırılabilir. Bu tehdit dışında sistem mükemmel bir şifreleme sistemidir ve ilk olarak 1917'de bulunup "teletype" makinelerinde kullanılmıştır.

EK - E.2. Güvenli Şifreleme Yöntemleri

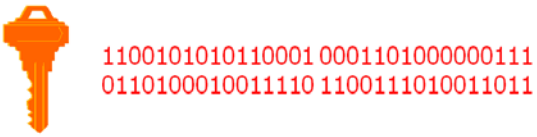
Güvenli şifreleme yöntemleri klasik şifreleme yöntemlerinin zayıf yönlerini ortadan kaldıran ve kriptoanalize karşı dirençli olan algoritmalarla gerçeklenir. Bu yöntemler

elektronik sistemlerde (bilgisayar, telekomünikasyon vb) kullanılır ve ikili düzende saklanan ve taşınan bilgi üzerinde uygulanır. Bu nedenle anahtar olarak bit dizileri kullanılır [2].



Şekil E4: Güvenli şifreleme yöntemi

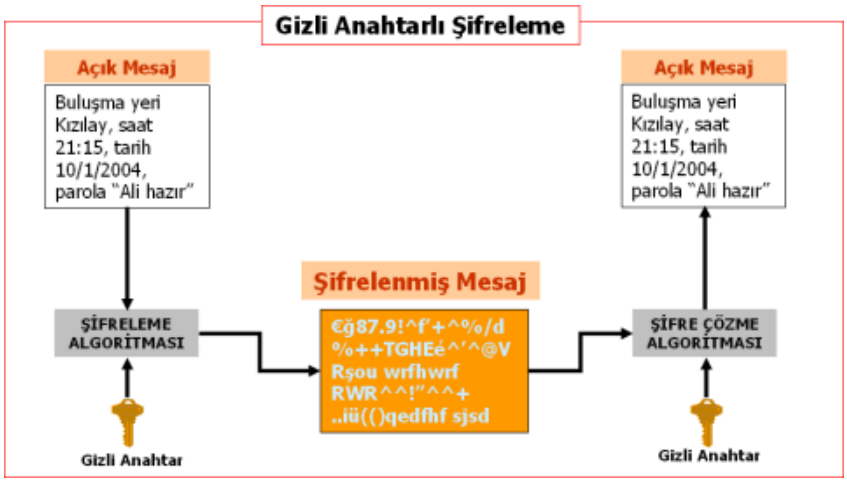
Bir şifreleme algoritmasının güvenliği belirleyen en önemli değişkenlerden birisi anahtar uzunluğudur. Örneğin Şekil E5' de gösterilen 64 bitlik bir anahtarı kullanan şifreleme algoritması için toplam anahtar sayısı 2^{63} = 9.223.372.036.854.775.808 adettir. Şifrelemede bu anahtarlardan herhangi birisi kullanılabileceği için bu anahtarı tahmin yoluyla elde etme olasılığı ($1/2^{63} \sim= 1/10^{19}$) çok düşüktür.



Şekil E5: 64 bitlik şifreleme anahtarı

Simetrik Şifreleme : Bu yöntemde, şifreleme ve şifre açma işlemi aynı anahtar ile yapılır. Simetrik şifrelemede bu anahtar gizli tutulmalıdır. Bu nedenle, bu tip sistemlere gizli anahtarlı şifreleme sistemi adı da verilmektedir. Bu sistemde haberleşen taraflar aynı şifreleme algoritmasını ve aynı anahtarı Şekil E6' da gösterildiği gibi kullanırlar [2].

.



Şekil E6**:** Simetrik Şifreleme Yöntemi

Simetrik şifreleme algoritmaları hızlıdır ve "gizlilik" güvenlik hizmetini yerine getirir. Fakat simetrik şifreleme ölçeklenebilir değildir, emniyetli anahtar dağıtımı ve yönetimi zordur. Bütünlük, Kimlik Doğrulama ve İnkar Edememe güvenlik hizmetlerini gerçeklemiyor

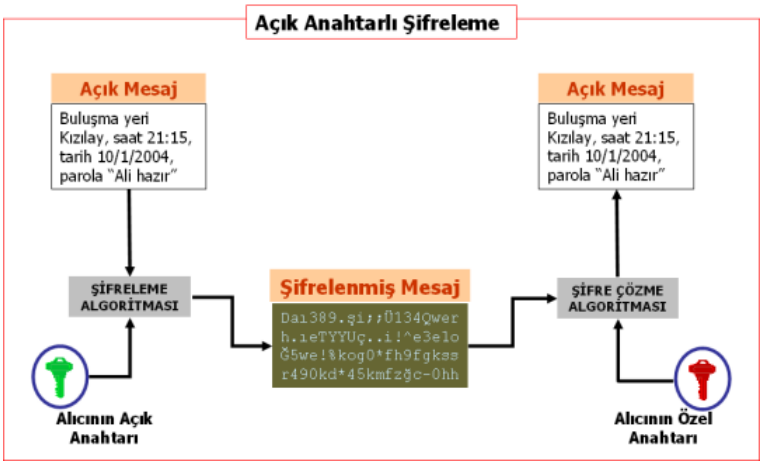
Simetrik şifrelemenin en önemli öğesi anahtar gizliliği olduğu için birden fazla kişinin haberleştiği bir ortamda anahtar yönetimi büyük dikkat gerektirmektedir. Bu yöntem sistemdeki kişi sayısına bağlı olarak çok fazla anahtar üretimini gerektirdiği için çok kullanışlı değildir. Anahtar sayısının kullanıcı sayısına bağlı olarak artışı aşağıdaki tabloda görülebilir.

Tablo E1: Simetrik şifrelemede anahtar sayısı

Kullanıcı Sayısı	Anahtar Sayısı
3	3
4	6
10	45
100	4,950
1,000	499,500
10,000	49,995,000
n	n*(n-1) /2

Asimetrik Şifreleme : Asimetrik şifreleme tekniğinde, şifreleme ve şifre çözme işlemi farklı anahtarlar ile yapılır. Bu anahtar çiftini oluşturan anahtarlara açık ve özel anahtar adı verilir. Bu şifreleme yönteminde özel anahtar gizli tutulmalıdır fakat

açık anahtar gerekli kişilere verilebilir ve başka kişilerle paylaşılabilir. Bu özelliğinden dolayı asimetrik şifreleme, açık anahtarlı şifreleme adıyla da anılır. Bu sistemi kullanarak haberleşen taraflar, Şekil E7' de gösterildiği gibi aynı şifreleme algoritmasını kullanır ve gerekli anahtarlara erişebilirler [2].



Şekil E7: Asimetrik Şifreleme Yöntemi

Asimetrik şifrelemenin birçok avantajı vardır. Buna göre; anahtar yönetimi asimetrik şifrelemede ölçeklenebilirdir. Kripto-analize karşı dirençlidir yani kırılması zordur. Bütünlük, kimlik doğrulama ve inkâr edememezlik güvenlik hizmetleri sağlanabilir.

Asimetrik şifrelemenin başlıca dezavantajları şunlardır; Algoritmalar genel olarak yavaş çalışırlar. Simetrik kriptografi algoritmalarına göre yaklaşık 1500 kat daha yavaştırlar.Anahtar uzunluğu bazı durumlar için kullanışlı değildir. Mobil cihazlar için klasik algoritma anahtar uzunlukları sorunlu olabilir.

Asimetrik kriptografi için anahtar yönetimi çok önemlidir. Buna göre, açık anahtarlar kontrollü olarak bir otorite tarafından yayınlanmalı ve değiştirilmeleri önlenmelidir. Anahtar çiftleri merkezi bir otorite tarafından üretilebilir veya her kullanıcı kendi anahtar çiftini üretebilir. Şifreleme ve imzalama için ayrı ayrı anahtar çiftleri olmalıdır. Çok özel durumlar için imzalama ve şifreleme anahtar çiftlerinin aynı olmasına izin verilebilir. Anahtar iptalleri kontrollü bir şekilde yapılmalı ve duyurulmalıdır.

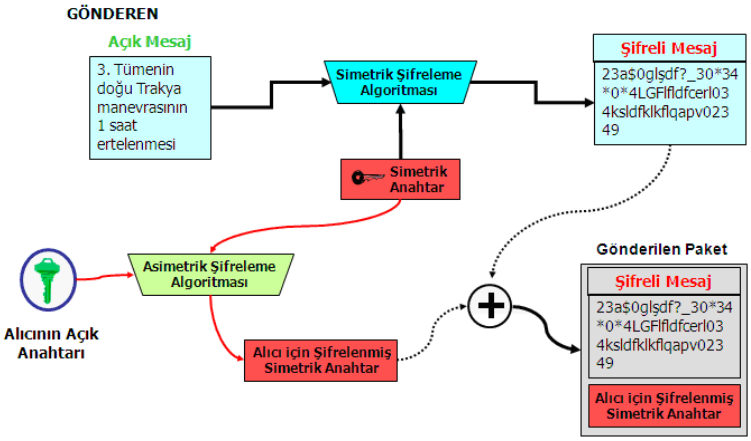
Asimetrik şifreleme için anahtar yönetimi simetrik şifrelemeye göre daha kolaydır çünkü bir kullanıcıyla şifreli haberleşmek isteyen kişi karşı tarafın açık anahtarına ihtiyaç duyar. Bu açık anahtar kamuya açık olarak yayınlandığı için sisteme giren bir kişi için sadece bir anahtar çifti üretmek yeterli olmaktadır [2].

Tablo E2: Asimetrik şifrelemede anahtar sayısı

Kullanıcı Sayısı	Anahtar Sayısı
3	3
4	4
10	10
100	100
1,000	1,000
10,000	10,000
n	N

Şifreli Mesaj Oluşturma ve Çözme Örneği :

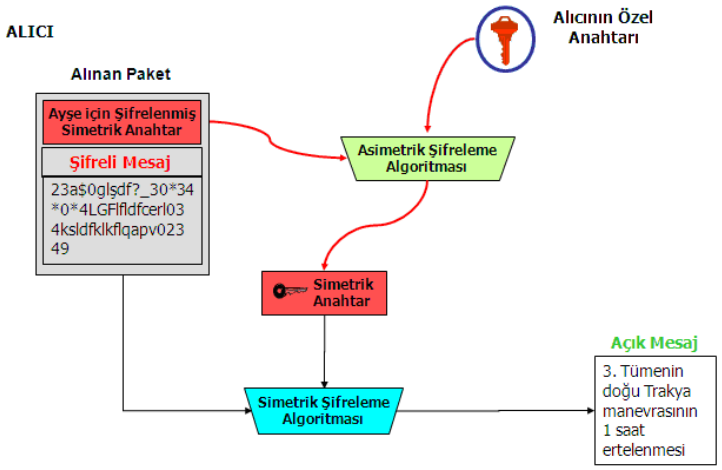
Şekil E7' de gönderici tarafından şifreli bir mesajın oluşturulması anlatılmaktadır. Burada mesajın şifrelenmesinde daha hızlı çalıştığı için simetrik anahtar kullanılıyor. Daha sonra bu simetrik anahtarın şifrelenmesi gerekiyor. Bu anahtarı şifrelemek için alıcının açık anahtarı kullanılır ve şifrelenen simetrik anahtar şifreli mesajın sonuna eklenip paketlenerek alıcıya gönderilir.



Şekil E8: Şifreli mesaj oluşturma

Şekil E8' de gösterildiği gibi alıcı tarafından alınan şifreli mesaj ve şifrelenmiş simetrik anahtarın çözülmesi gerekmektedir. Öncelikle alıcı şifrelenmiş simetrik

anahtarı kendi özel anahtarını kullanarak çözer. Daha sonra elde ettiği bu simetrik anahtar ile şifrelenmiş mesajı hızlı bir şekilde çözmektedir [2].



Şekil E9: Şifreli mesaj çözme

EK - F : Sayısal Sertifikalar

Sertifikalar, nüfüs cüzdanı, ehliyet belgesi veya diğer kimlik belgeleri gibi kişinin internet üzerinde kimliğini ispatlaması için kullanılan elektronik dosyalardır. Başka bir deyişle kimliğin sayısal ispatıdır.

Sertifikalar çift anahtarlı kriptografi (asimetrik şifreleme) teknolojisine dayanır ve herkese açıktır. Asimetrik şifrelemede özel ve açık anahtar olmak üzere iki adet anahtar üretilir. Açık anahtar, o açık anahtarın sahibiyle haberleşmek isteyen herkes tarafından görülebilir ve kullanılabilir. Bu açık anahtarın isteyen kişilerce kullanımını kolaylaştırmak için değişik şekillerde yayınlanması ve isteyenlerin erişimine açılması mümkündür. Bu yayınlama şekline sertifika adı verilmektedir. Sertifika kişilere ait olabildiği gibi kurumların ve web sunucuların da sertifikaları olabilir. Sertifikalar, sahibinin kişisel bilgilerini ve bu kişisel bilgilere ait açık anahtar bilgisini taşır. Açık anahtar bilgisinin belirtilen kişi veya kuruma ait olduğu anlaşılabilir. Kişisel, sunucu ve kök sertifikası olmak üzere 3 çeşit sertifika vardır.

Kişisel Sertifikalar : Kişisel sertifikalar şahısların kimlik bilgilerini ve açık anahtarını taşıyan elektronik dosyalardır. Nüfus cüzdanı veya ehliyet belgesi gibi kişisel

sertifikalar da internet üzerinde kimliğin ıspatlanması amacıyla kullanılırlar. Şahısların internet üzerindeki güvenli ve gizli iletişim yeteneklerinden faydalanabilmesi için öncelikle bir sertifikaya sahip olmaları gerekmektedir.

Sertifika X.509 standartına uygun olarak üretilir ve bu standartla uyumlu olan web tarayıcılarına yüklenerek kişisel bilgisayarlarda tutulur. Bununla birlikte sertifikanın akıllı kartta veya diskette taşınıp kullanılması da mümkündür.

Sunucu Sertifikası : Sunucu sertifikası, web sitesinin kimlik bilgilerini ve açık anahtarını taşıyan ve web sitesine bağlanan kullanıcılara sunulan elektronik dosyalardır. Örneğin bir internet tarayıcı kullanıcısı bir web sunucuya gizli bir bilgi göndermek istediğinde, tarayıcı sunucunun göndermiş olduğu sunucu sertifikasını alır. İçinde web sunucusunun açık anahtarını bulunduran sunucu sertifikası, tarayıcı tarafından web sunucunun kimliğinin doğrulanması ve sunucuya gönderilecek olan bilginin SSL teknolojisi kullanılarak şifreli gönderilmesi için kullanılır.

Gönderilecek olan bilgi sunucu sertifikanın içindeki açık anahtar ile şifrelenir. Bu şifreli bilgiyi çözecek gizli anahtar sadece sunucuda bulunduğundan başka birisinin şifreyi çözmesi mümkün değildir. Böylece şifreli bilginin internet üzerinden gönderiminde güvenlik sağlanmış olur.

Kök Sertifika : Kök sertifika sertifika hizmet sağlayıcısının kimlik bilgilerini ve açık anahtarını taşıyan elektronik dosyadır. Kök sertifikayı diğer sertifikalardan ayıran tek özellik, üzerinde kendi imzasını taşıyor olmasıdır. Yayınladıkları diğer sertifikalara güvenilirlik onayının verilebilmesi için kök kimliklerin kullanıcı tarafında mevcut olmaları gereklidir. Örneğin bir web sunucusunun sertifikasını alan internet tarayıcısı bu kimliğe güvenip güvenmeyeceğine karar verebilmesi için sunucuya sertifikayı veren sertifika hizmet sağlayıcısının sertifikasına ihtiyaç duyar. Eğer söz konusu kök sertifika internet tarayıcısında tanımlı değilse, tarayıcı bu sitenin güvenilir olmadığını kullanıcıya bildirir. Bazı sertifika hizmet sağlayıcısı sertifikaları, Netscape ve Internet explorer gibi popüler olan tarayıcılarda önceden tanımlanmıştır yani kök sertifikalar tarayıcıya yüklenmiş durumdadır. Diğer sertifika hizmet sağlayıcılarının

da tarayıcıya tanımlanabilmesi için kök sertifikalarının tarayıcıya yüklenmesi gerekmektedir.

Sertifika yayımlayan kurumlar tarafından sertifika ile ilgili çeşitli kurallar tanımlanır. Bu kurallar genel olarak bir sertifikanın hangi uygulamalarda kullanılabileceğini ve hangi durumlarda güvenilir kabul edilebileceğini belirler. Günlük hayatta bunun benzeri kuralları bankaların kredi kartlarında görebiliriz. Örneğin Silver, Gold, Platinum gibi değişik kart sahiplerinin değişik harcama limitleri ve değişik kullanım kuralları bulunur. Bazı kartlar sadece o sisteme üye mağazalarda geçerli kabul edilir. Elektronik sertifikalarda bulunan alanlar, sertifikaların (ve ilgili özel anahtarların) e-posta imzalama ya da sözleşme onaylama gibi değişik amaçlarla kullanılabileceğini gösteren özel değerler taşıyabilirler.

Sertifikaların taklit edilemiyor olmaları gereklidir. Bunu sağlamanın yolu sertifikaların güvenilir kurumlar tarafından dağıtılmasıdır. Sertifikaların doğruluğu kontrol edilirken her zaman sertifikayı imzalayan makamın elektronik imzasının doğruluğu kontrol edilir. Bu kontrol işlemi birbirine bağlı olarak bir veya daha fazla sertifikadan oluşan bir zincirin, yolun takibini ve doğrulamasını gerektirebilir.



Şekil F1: Sertifikasyon işlemleri [2]

Bu amaçla geliştirilen değişik sertifikasyon yolu çözümleri aşağıdaki özellikleri taşır:

- Ölçeklenebilir bir sistem kurulmaya çalışılır.
- Sertifika yöntemi hiç tanımadığımız kişilere güvenilir bir kurum aracılığıyla güvenmemizi sağlıyor.

- Haberleştiğimiz bir kişi herhangi bir yayıncı kuruluştan sertifika almış olabilir.
- Kişi/kurum e-posta koruması, sözleşme onaylama, web güvenliği sertifikalarını ayrı ayrı yayıncılardan alabilir
- Güvenilen tüm sertifika yayıncılarını bir listede tutabilir.
- Bir sertifika yayıncısı diğer yayıncıların güvenilirliğini gösteren sertifikalar yayınlayarak bir sertifikasyon zinciri ya da hiyerarşisi yaratabilir.
- İki sertifika yayıncısı birbirlerine güvendiklerini gösteren sertifikalar yayınlayarak çapraz sertifikasyon yapabilirler.

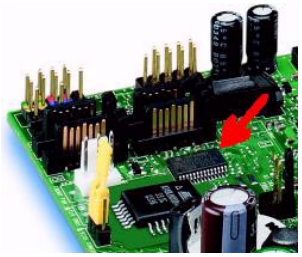
Açık anahtar sertifikasının içeriğinin güncel olup olmadığı sorusuna cevap vermek gerekmektedir çünkü sertifika sahibinin erişim bilgileri değişmiş olabilir yada sertifika sahibi özel anahtarını kaybettiği için yeni bir açık anahtar kullanmaya başlamış olabilir. Sertifika sahibi sertifikasını kullanmak isteyen kişilere dağıttıktan sonra geri toplayamaz. Ayrıca sertifika sahibinin kendisi ile ilgili değişiklikleri duyurması çok zordur. Bu nedenle sertifika iptal listeleri (SİL) kullanılır. Sertifika iptal listeleri sayısaldır ve sık aralıklarla elektronik ortamda (örneğin internette) yayınlanır. Sertifika iptal listelerinde, artık güvenilemeyecek olan ve kullanım süresi dolmamış sertifikaların seri numaralarını, yayın tarihini, son kullanım tarihini, yayınlayan kuruluşun adını ve sayısal imzasını içerir.

Sertifikaların birçok kullanım amacı vardır. Genel anlamda sertifikaların kullanım amaçları aşağıdaki gibi özetlenebilir:

- Web üzerinde kullanıcı ile sunucu arasındaki güvenli iletişim kanallarında şifreleme
- Kullanıcının ve sunucunun kimliklerinin doğrulanması
- Güvenli internet e-posta iletişimi için mesajların şifrelenmesi
- E-posta mesajlarında gönderenin kimliğinin doğrulanması
- Web üzerinden yüklenebilen, imzalı, çalışabilir programların bütünlüğünün (değiştirilmediğinin) ve kaynağının (programı imzalayan kurum veya kişinin kimliğinin) doğrulanması

EK - G : Güvenilir Platform Modülü (TPM)

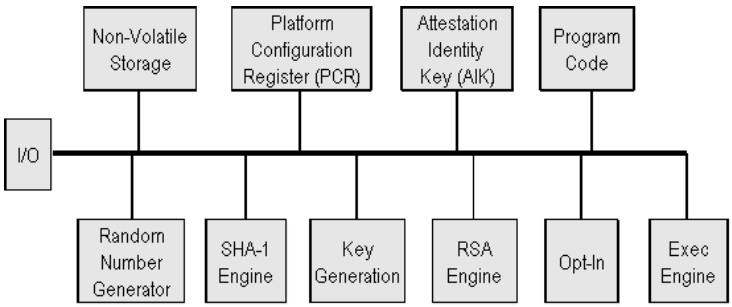
TPM, TCG tarafından tanımlanan, güvenlikle ilişkili özellikleri çalıştırabilen donanım seviyesinde bir yongadır. Günümüzde artık birçok bilgisayarlar modelinde ana kart üzerinde Şekil G1' de gösterildiği gibi yer almaktadır. TPM bilgisayarlar, cep telefonları ve gömülü sistemler gibi her ortama entegre edilebilir. Fiziksel saldırılara karşı koruması vardır ve var olan sistemlerde güvenin kaynağı olarak kullanılabilir.



Şekil G1: Ana kart üzerinde yer alan TPM yongası [47]

Yazılım ve donanım üreticileri kripto grafik özelliklerin TPM içersinden çalıştırılmasını sağlar. TPM yongasının bazı kripto grafik yetenekleri rasgele sayı üreteci, özetleme, asimetrik anahtar üretimi ve asimetrik şifreleme / şifre çözmedir.

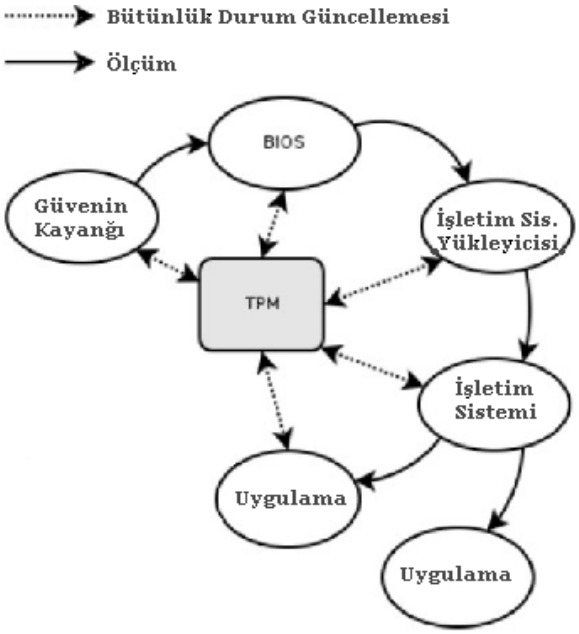
TPM' in ana bileşenleri Şekil G2' de gösterilmiştir.



Şekil G2: TPM' in ana bileşenleri [47]

Bu şekilde yer alan bileşenlerden olan I/O, iletişim veri yolunda bilgi akışını sağlar. Non-volatile dediğimiz kısımda Endorsement Key (EK), Storage Root Key (SRK), sahip onaylama verisi ve kalıcı bayraklar yer alır. Attestation Identity Key (AIK)

sadece TPM içerisinde üretilebilen 2048 bit RSA anahtar çiftini bilgilerin imzalanması için kullanır. Özel AIK, TPM' in dışarısına asla çıkarılmaz. Program code kısmı platform sürücülerinin ölçülmesinde kullanılabilir. TPM, rastgele sayı üretmek için gerçek zamanlı bit üretecini içerir. Güvenli özetleme algoritma (SHA1) motoru imzaların hesaplanmasında, anahtar parçacıklarının oluşturulmasında ve genel bazı işler için kullanılır. RSA anahtar üretme motoru imzalama (signing) ve yükleme (storage) anahtarlarını oluşturmak için kullanılır. RSA motoru imza anahtarları ile imzalama işlerinde, yükleme anahtarları ile şifreleme ve şifre çözme işlemlerinde, EK ile de şifre çözme işlemlerinde kullanılır. "Opt-in" kısmı kalıcı ve geçici işaretlerin (flags) durumlarını kontrol etmek için kullanılır. Burada anlamsal ilişkiler işaretlerin içerisine konulur. "Execute Engine" kısmı işlemciden gelen TPM komutlarını çalıştırır.



Şekil G3: TPM kullanılarak sistemin güvenli bir şekilde açılması

Şekil G3' de gösterilen sistemin açılışı esnasında TPM en alt seviyeden en üst seviyeye kadar bütün güvenlik kontrollerini yapmak için kullanılabilir. Her bileşen (BIOS, işletim sistemi yükleyicisi ve işletim sistemi) için bir öz (hash) değer oluşturulur ve sistem açılırken TPM' e aktarılır. Bu değerler TPM içerisinde yer alan korumalı alanda PCR (Platform Configurator Registers) kayıtçıları içerisinde saklanırlar. Daha sonra o an hesaplanan öz değerlerinin TPM içerisindeki öz

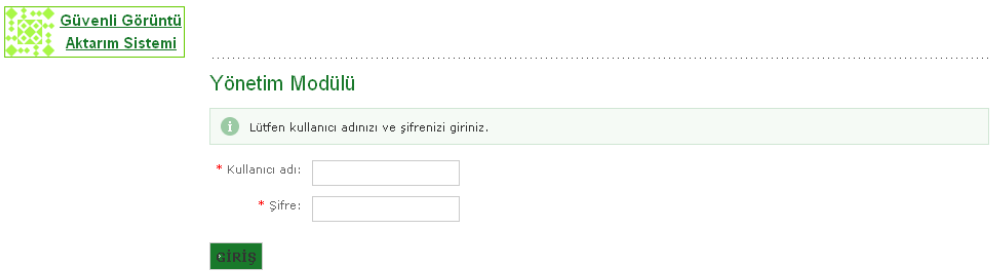
değerleri ile aynı olup olmadığı kontrol edilir. Buradan kullanıcı bilgisayarındaki verilerin yada bileşenlerin değiştirilip değiştirilmediğini anlamak mümkün olabilir [48]. Bununla beraber yazılım ve donanımların doğrulanması kontrol sertifikaları aracılığı ile yapılabilir.

EK - H : Güvenilir Görüntü Aktarımı Yazılımı Ekranları

Güvenli görüntü aktarım sistemi yönetim ve kullanıcı işlemlerinin gerçekleştiği iki ayrı modülden meydana gelmektedir. Yönetim modülünde kullanıcıların indirebileceği görüntüler sisteme yüklenmekte ve sistemi kullanacak olan kullanıcılar tanımlanmaktadır. Kullanıcı modülünde ise yönetim modülünde tanımlanan kullanıcıların görüntüleri indirebilmeleri sağlanmaktadır.

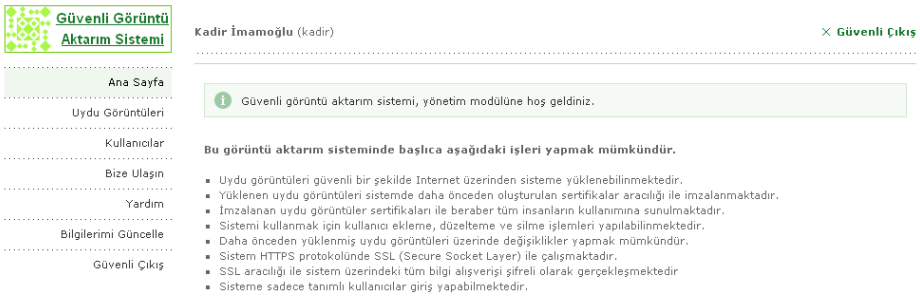
EK - H.1. Güvenli Görüntü Aktarım Yazılımı Yönetim Ekranları

Yönetim modülü yardımı ile sistem yöneticisi yeni uydu görüntüsünü sisteme yükleyebilir ve bu görüntülere erişim hakkı olacak olan kullanıcılar sertifikaları ile beraber tanımlar. Bu ekranda tanımlanan kullanıcı sertifikaları güvenli yollardan sahiplerine iletilir. GGAS' ne giriş yapabilmek için Şekil H1' de gösterildiği gibi kullanıcı adı ve şifre bilgilerinin girilmesi gerekmektedir.



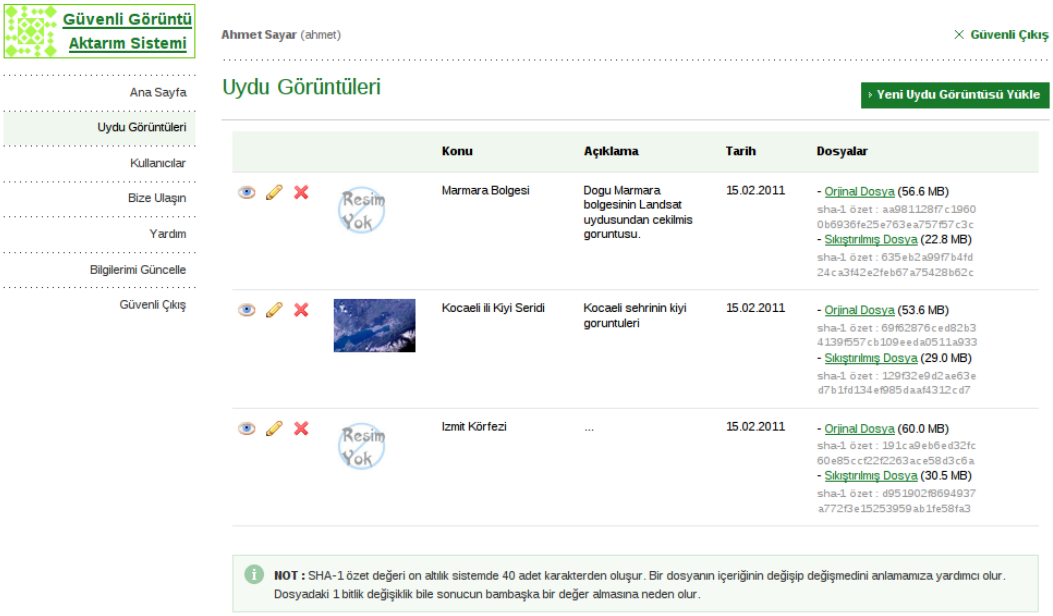
Şekil H1: Yönetim modülü giriş erkranı

Yönetim ekranı modülüne Şekil H1.' deki ekran kullanılarak giriş yapıldıktan sonra sistem yöneticisinin karşısına Şekil H2' de gösterilen ana ekran gelecektir.



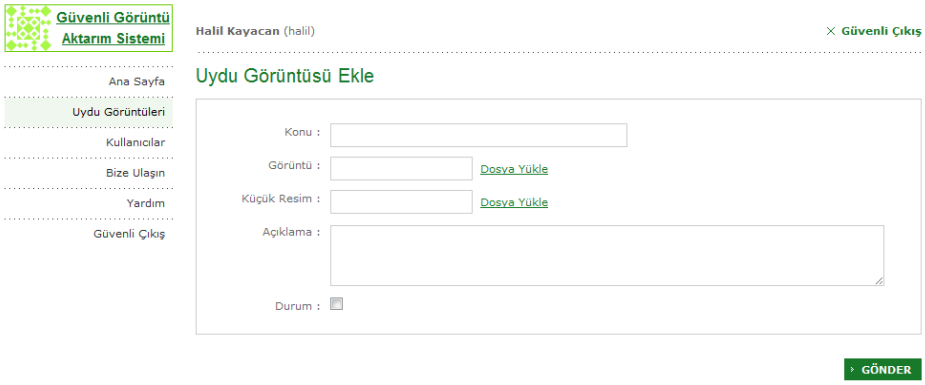
Şekil H2: Yönetim Modülü ana sayfa ekranı

Sıkıştırılan uydu görüntüleri sisteme yönetim panelindeki Uydu Görüntüleri menüsü üzerinden yüklenir. Şekil H3' te gösterildiği gibi once sistemde yüklü olan tüm uydu görüntüleri listelenir. Bu görüntüler üzerinde slime yada düzeltme yapmak için sol kısımda yer alan kalem ve çarpım işareti şeklindeki ikonlara tıklatmak gerekiyor.



Şekil H3: Yönetim modülü uydu görüntüleri listeleme ekranı

Sisteme yeni bir uydu görüntüsü Şekil H-4' de gösterilen ekran üzerinden yapılmaktadır. Bu ekranda bir uydu görüntüsü için konu, uydu görüntüsü, küçük resim, açıklama ve durum gibi alanlara giriş yapmak gerekiyor.

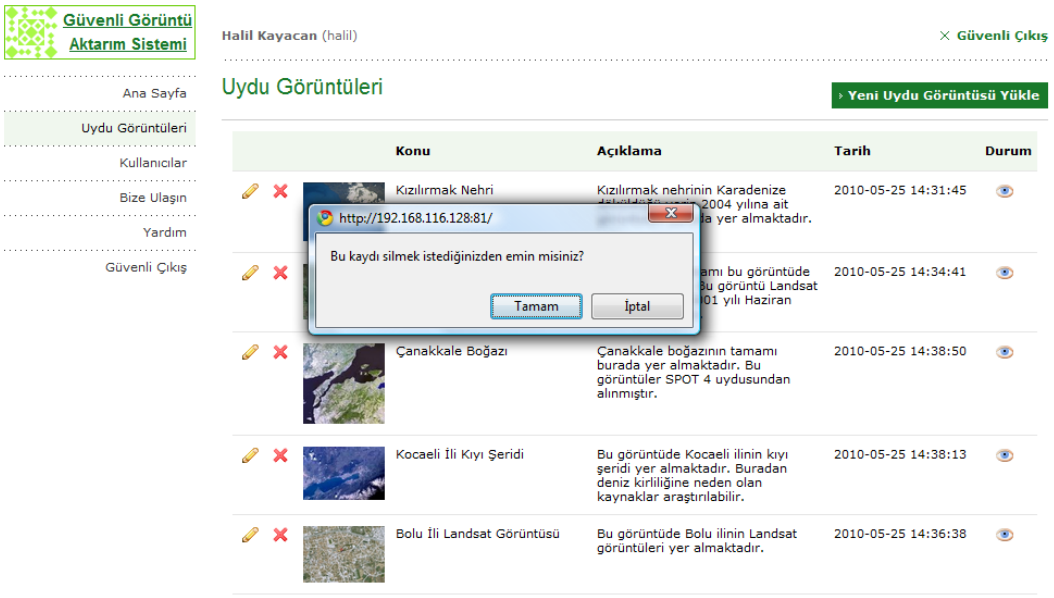


Şekil H4: Yönetim modülü uydu görüntüsü ekleme ekranı

Yüklenen görüntüleri düzenlemek için Şekil H5' te gösterilen ekran kullanılmaktadır. Bu ekranda uydu görüntüsü ile ilgili daha önceden girilen tüm bilgiler kutular içerisinde dolu olarak gelir. Uydu görüntüsü üzerinde gerekli değişiklikler yapıldıktan sonra Güncelle buttonuna basılarak güncelleme işlemi yapılır.

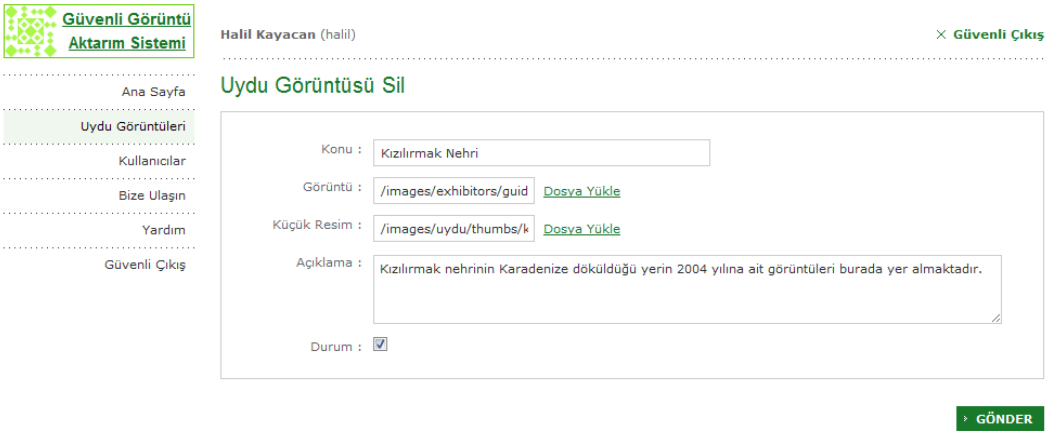


Şekil H5: Yönetim modülü uydu görüntüsü güncelleme ekranı



Şekil H6: Yönetim modülü uydu görüntüsü silme onay ekranı

Uydu görüntüsü silmek için Şekil H6 ve Şekil H7' deki ekranlar kullanılmaktadır. Yukarıdaki şekilde silme işlemine başlamadan önce kullanıcıdan bir küçük pencere ile onay alınmaktadır.



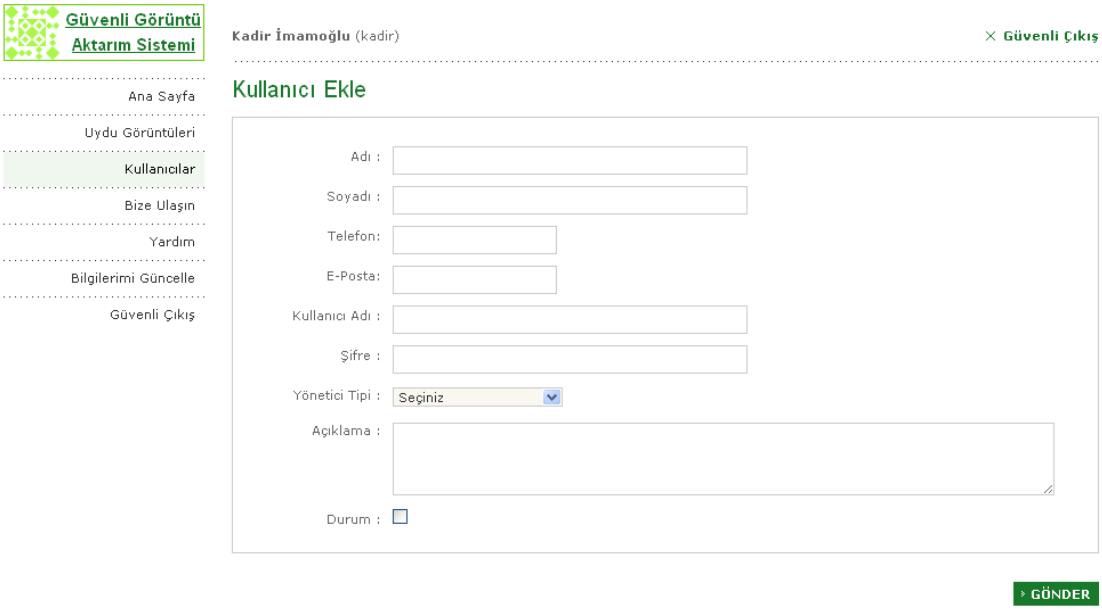
Şekil H7: Yönetim modülü uydu görüntüsü silme ekranı

Sistemde tanımlı olan kullanıcılar Şekil H8' de gösterilen ekranda listelenir. Bu ekran üzerinden kullanıcı ile ilgili ekleme, silme ve düzeltme gibi diğer işlemlerin ekranlarına gidilebilir.



Şekil H8: Yönetim modülü kullanıcılar listesi ekranı

Sisteme yeni bir kullanıcı Şekil H9.' da gösterilen ekran üzerinden eklenir. Eklenen kullanıcı için ad, soyad, telefon, e-posta, kullanıcı adı, şifre, açıklama ve durum gibi alanlara giriş yapmak gerekecektir.



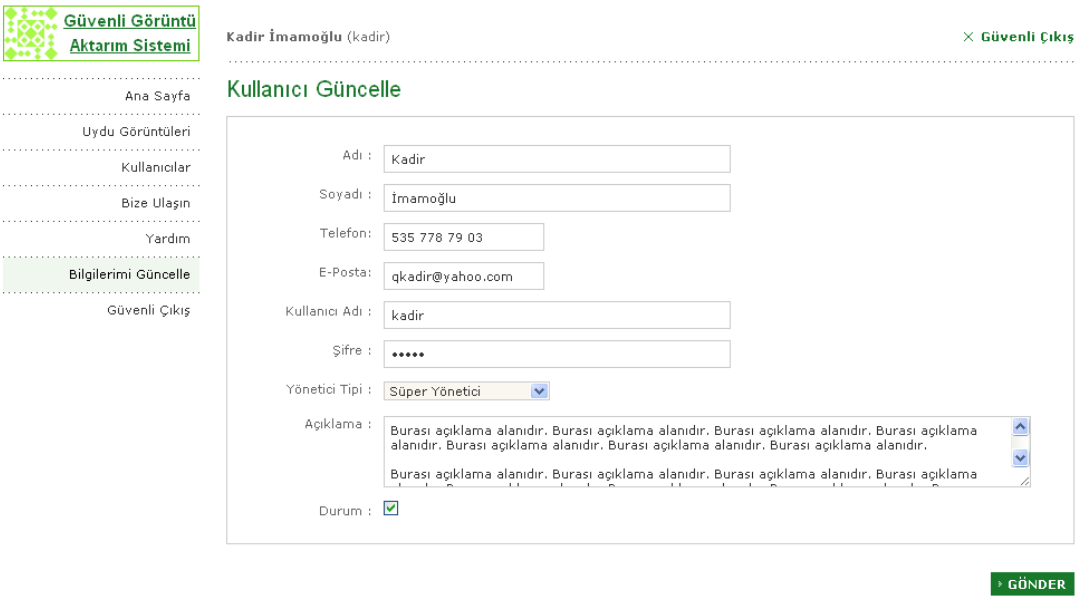
Şekil H9: Yönetim modülü kullanıcı ekleme ekranı

Burada bazı alanlar girilmeyip boş bırakıldığında sistem yöneticisine boş bırakılan alan ile ilgili gerekli uyarılar kırmızı renkte Şekil H10' da gösterildiği gibi yapılmaktadır.

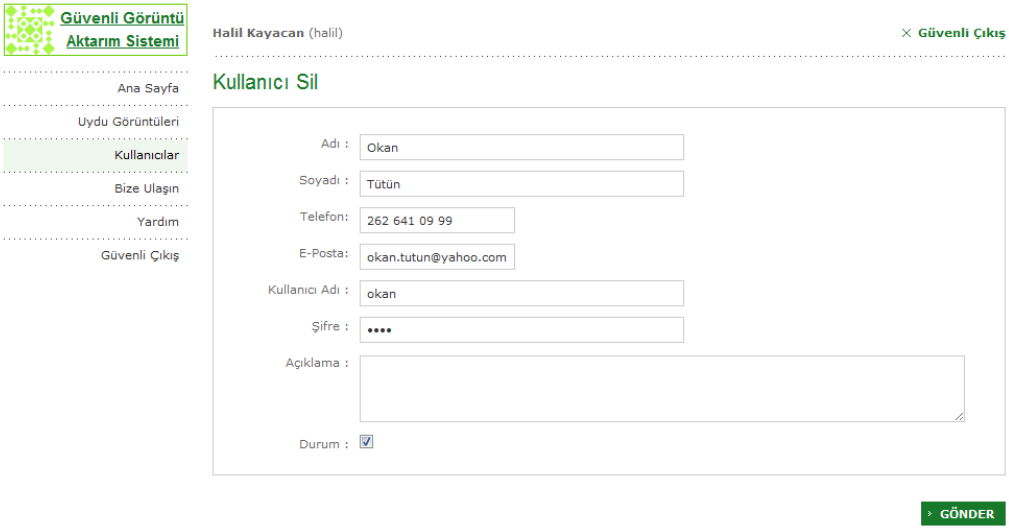


Şekil H10: Yönetim modülü kullanıcı ekleme hata ekranı

Kullanıcı bilgilerinin güncellenmesi ekranı aynı kullanıcı ekleme ekranındaki gibidir. Sadece burada ekrandaki alanlar daha önce girilen değerler ile dolu olarak gelir. Kullanıcı güncelleme sayfası Şekil H11' de gösterilmiştir.



Şekil H11: Yönetim modülü kullanıcı güncelleme ekranı



Şekil H12: Yönetim modülü kullanıcı silme ekranı

Kullanıcı silme ekranı Şekil H12.' de gösterildiği gibidir. Kullanıcı silme işleminden sonra kullanıcı sisteme bir daha giriş yapamıyacaktır.



Şekil H13: Yönetim modülü bize ulaşın mesajları ekranı

Kullanıcılar tarafından sisteme yöneticisine gönderilen mesajlara Şekil H13 ve Şekil H14' de gösterilen ekranlar üzerinden bakılabilir.



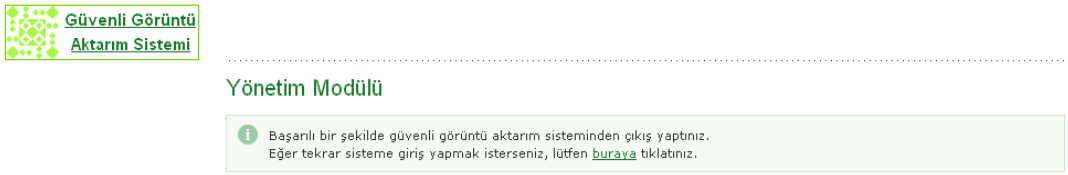
Şekil H14: Yönetim modülü bize ulaşın mesajları detay ekranı

Şekil H15' de yönetim modülünde yer alan yardım ekranı yer alır. Burada sistemin kullanımı ile ilgili bazı soruların cevapları yer alır. Sistem yöneticisi için bir yardım sayfasıdır denilebilir.



Şekil H15: Yönetim modülü bize yardım ekranı

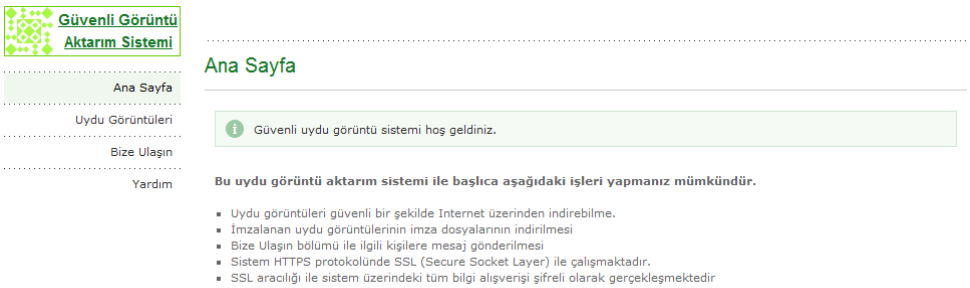
Yönetim modülünde yer alan sol menüdeki Güvenli Çıkış bağlantısına tıklatılınca sistem yöneticisi yönetim ekranından güvenli bir şekilde çıkmış olur. Ve kullanıcının karşısına Şekil H16' daki gösterilen ekran gelir.



Şekil H16: Yönetim modülü güvenli çıkış ekranı

EK - H.2. Güvenli Görüntü Aktarım Yazılımı Kullanıcı Ekranları

Bu ekranlar yardımı ile system yöneticisi tarafından tanımlanan kullanıcılar sertifikalarını internet tarayıcılarına tanıtarak sisteme girebileceklerdir. Sertifikalar yardımı ile kullanıcıların kimlik doğrulaması yapılmış olunacaktır.



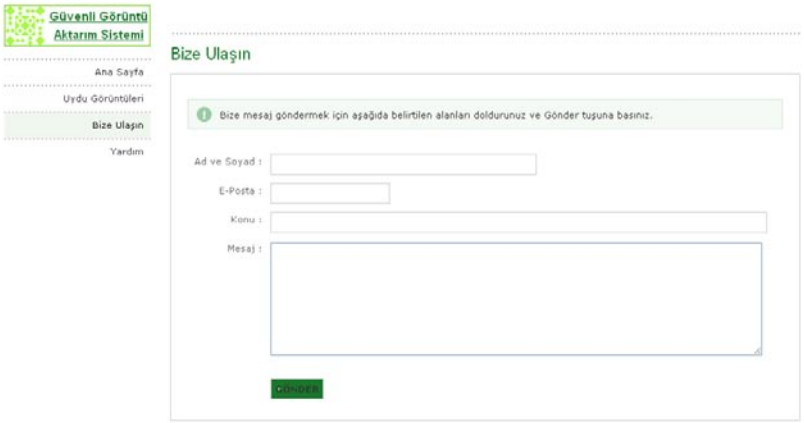
Şekil H17: Kullanıcı modülü kullanıcı ana sayfası ekranı

Internet taraycısı üzerinden sisteme giriş yapan kullanıcı Şekil H17’ de gösterilen ana sayfa ile karşılaşacaktır. Bu ekranda kullanıcıların bu sistemde yapabileceği işler maddeler halinde sıralanmıştır.



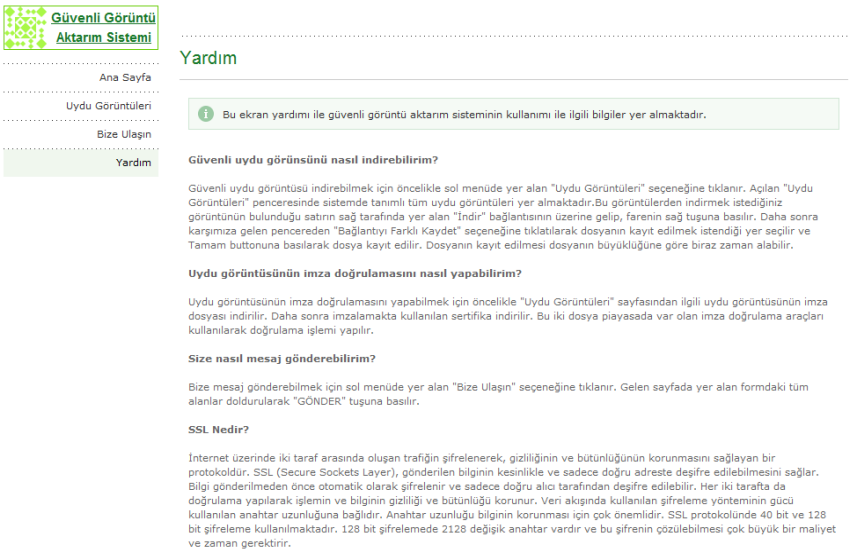
Şekil H18: Kullanıcı modülü uydu görüntüleri ekranı

Sistemde yüklü olan uydü görüntülerine sol menüde yer alan Uydu Görüntüleri bağlantısına tıklatılarak gidilebilir. Şekil H18.' de gösterilen bu ekran üzerinden kullanıcı istediği uydu görüntüsünü bilgisayarına indirebilir.



Şekil H19 : Kullanıcı modülü bize ulaşın mesaj formu

Şekil H19' te kullanıcılar "Güvenli Görüntü Aktarım Sistemi" ile ilgili sistem yöneticisine mesajlar gönderebilmektedir. Kullanıcılar sistemin kullanımı ile ilgili Şekil H20.' de gösterilen yardım ekranından yararlanabilirler.



Şekil H20 : Kullanıcı modülü yardım ekranı

ÖZGEÇMİŞ

1978 yılında Kırcali' de doğdu. İlkokulu Bulgaristan' da, orta ve lise öğrenimini KOCAELİ ilinin Gebze ilçesinde tamamladı. 1995 yılında girdiği Kocaeli Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği bölümünden 1999 yılında Bilgisayar Mühendisi olarak mezun oldu. 2001-2004 yılları arasında Gebze Yüksek Teknoloji Enstitüsü Fen Bilimleri Enstitüsü, Jeodezi ve Fotogrametri Mühendisliği Anabilim Dalı' nda Yüksek Lisans eğitimini tamamladı. 2008 yılından beri Kocaeli Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı'nda yüksek lisans eğitimine devam etmekte olup evli ve bir çoçuk babasıdır.