T.C.
İSTANBUL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

TIBBİ GÖRÜNTÜ VERİLERİNİN İLETİMİNDE KULLANILAN ŞİFRELEME ALGORİTMALARININ ANALİZİ

Çetin ŞAHİN

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği Programı

DANIŞMAN
Prof. Dr. Ahmet SERTBAŞ

Haziran, 2017

İSTANBUL

Bu çalışma, 8.06.2017 tarihinde aşağıdaki jüri tarafından Bilgisayar Mühendisliği Anabilim Dalı, Bilgisayar Mühendisliği Programında Yüksek Lisans tezi olarak kabul edilmiştir.

Tez Jürisi

Prof. Dr. Ahmet SERTBAŞI(Danışman)
İstanbul Üniversitesi
Mühendislik Fakültesi

Doç. Dr. Rüya ŞAMLI
İstanbul Üniversitesi
Mühendislik Fakültesi

Yrd. Doç. Dr. Muhammed Ali AYDIN
İstanbul Üniversitesi
Mühendislik Fakültesi

Prof. Dr. Fırat KAÇAR
İstanbul Üniversitesi
Mühendislik Fakültesi

Yrd. Doç. Dr. Akhan AKBULUT
İstanbul Kültür Üniversitesi
Mühendislik Fakültesi

20.04.2016 tarihli resmi gazetede yayımlanan Lisansüstü Eğitim ve Öğretim Yönetmeliğinin 9/2 ve 22/2 maddeleri gereğince; Bu Lisansüstü teze, İstanbul Üniversitesi'nin abonesi olduğu intihal yazılım programı kullanılarak Fen Bilimleri Enstitüsü'nün belirlemiş olduğu ölçütlere uygun rapor alınmıştır.

ÖNSÖZ

Bu tez çalışmamda tıp alanındaki görüntüleme teknolojilerinin ürettikleri verilerin (MR, Tomografi, Ultrasonografi, Röntgen Filmi, EMG gibi) iletiminde, kurumlar arasında paylaşımında kullanılan SİEK, HL7, DICOM gibi standartların görüntü iletimindeki güvenlik eksiklikleri ve optimizasyonu ile ilgili çalışmalar yapılmıştır. Aynı zamanda verilerin güvenliğini sağlamak için bilgisayar ortamında C# programlama dili ile yazılmış program üzerinde veriler test edilmiş ve analizi yapılmıştır.

Çalışmalarımda bana yardımcı olan İstanbul İl Sağlık Müdürlüğü Sağlık Bilgi Sistemleri Şube Müdürlüğü'ne,

Danışman hocalarım Prof. Dr. Ahmet SERTBAŞ ve Yrd. Doç. Dr. Muhammed Ali AYDIN'a

İstanbul Çekmece Kamu Hastane Birliği çalışanlarından Bilgisayar Mühendisi Musa AYKAÇ ve Elektronik Mühendisi Murat KONUK'a,

Tez çalışmamda planlanmasında, araştırılmasında, yürütülmesinde ve oluşumunda ilgi ve desteklerini esirgemeyen, engin bilgi ve tecrübelerinden yararlandığım, İstanbul İl Sağlık Müdürlüğü Sağlık Bilgi Sistemleri Şube Müdürlüğü çalışanları, Elektronik Haberleşme Yüksek Mühendisi Bilal TÜTÜNCÜ ve Bilgi İşlem Birimi Destek Personeli Şenol YAHŞİ'ye,

Çalışmalarım boyunca maddi manevi destekleriyle beni hiçbir zaman yalnız bırakmayan, tercihlerimde yanımda olan, amaçlarım peşinde giderken beni destekleyen ve yüreklendiren, aileme sonsuz teşekkürler ederim.

Haziran 2017 Çetin ŞAHİN

İÇİNDEKİLER

Sayfa No

ŞEKİL LİSTESİ

Sayfa No

TABLO LİSTESİ

Sayfa No

SİMGE VE KISALTMA LİSTESİ

Kısaltmalar	Açıklama
3DES	**:** Triple Data Encryption Standart
AES	**:** Advanced Encryption Standard
ATNA	**:** The Audit Trail and Node Authentication
CR	**:** Computed Radiography
DICOM	**:** Digital Imaging and Communications in Medicine
DX	**:** Digital Radiography
ECG-EKG	**:** Electrocardiography
HBYS	**:** Hastane Bilgi Yönetim Sistemi
HL7	**:** Health Level Seven
IO	**:** Intra-oral Radiography
MG	**:** Mammography
MR	**:** Magnetic Resonance
NM	**:** Nuclear Medicine
PT	**:** Positron emission tomography
PX	**:** Panoramic X-Ray
RBS	**:** Radyoloji Bilgi Sistemi
RF	**:** Radiofluoroscopy
RSA	**:** Ron Rivest, Adi Shamir, and Leonard Adleman şifreleme algoritması
SHA-1	**:** Secure Hashing Algorithm 1
SİE	**:** Sağlık İşletmelerinin Entegrasyonu
UEÜB	**:** Ulusal Elektrik Üreticileri Birliği
US	**:** Ultrasound
XA	**:** X-Ray Angiography
XC	**:** External-camera Photography
XDS	**:** Cross-Enterprise Document Sharing

ÖZET

YÜKSEK LİSANS TEZİ

TIBBİ GÖRÜNTÜ VERİLERİNİN İLETİMİNDE KULLANILAN ŞİFRELEME ALGORİTMALARININ ANALİZİ

Çetin ŞAHİN

İstanbul Üniversitesi

Fen Bilimleri Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

Danışman : Prof. Dr. Ahmet SERTBAŞ

Tıp alanındaki görüntüleme teknolojilerinin gelişimi ve çeşitlenmesi, tedavi kurumlarındaki iş süreçlerinin önemli bir bölümünü oluşturan tıbbi görüntülerin arşivlenmesi ve kullanılmak üzere arşivden geri çağrılmasından doğan gereksinim nedeniyle bu işlemlerin de elektronik ortama taşınmaya başlaması standardizasyon, maliyet vb. birçok amaçla bu alanda bir düzenleme yapılması zorunluluğu doğurmaktadır. Bilgi üretimi, iletimi ve paylaşımı için ortak bir dilin kullanılması zorunludur. Bu amaca hizmet eden bazı ulusal ve uluslararası kodlama ve sınıflandırma sistemleri mevcuttur. Bu kapsamda tıp alanındaki görüntüleme teknolojilerinin ürettikleri verilerin (MR, Tomografi, Ultrasonografi, Röntgen Filmi, EMG gibi) güvenliği ve bu verilere yetkisiz kişilerin ulaşmaması için gerekli çalışmaların yapılması hedeflenmektedir.

Bu tezde tıp alanındaki görüntüleme teknolojilerinin ürettikleri verilerin (MR, Tomografi, Ultrasonografi, Röntgen, EKG gibi) iletiminde ve kurumlar arasında paylaşılmasında kullanılan HL7, DICOM gibi standartların görüntü iletimindeki güvenlik eksikliklerinin giderilmesi ve optimizasyonu için geliştirmeler yapılmıştır. Bu amaçla, tıbbi görüntüleme sistemlerinde kullanılan standart DICOM'un hem dosya alanına hem de DICOM formatının görüntü ve veri kısımlarını ayırarak hasta mahremiyetini oluşturan veri kısmının güvenliği için etiket alanına şifreleme ve şifre çözme yöntemleri uygulanmıştır ve birbiriyle karşılaştırılmıştır. Çalışmada 3DES, AES ve RSA ile etiket şifreleme ve şifre çözme yöntemleri tercih edilmiştir. Verilerin güvenliğini DICOM şifreleme ile sağlama maliyetinin örneklenen küçük, orta ve büyük ölçekli hastane işleyişi üzerinden etkileri gösterilmiştir.

Haziran 2017, 94 sayfa.

Anahtar kelimeler: Tıbbi Görüntü veri güvenliği performans analizi, DICOM veri güvenliği performans analizi, Etiket veri güvenlik performans analiz

SUMMARY

M.Sc. THESIS

AN ANALYSIS OF ENCRYPTION ALGORITHMS USED FOR MEDICAL IMAGE DATA TRANSFER

Çetin ŞAHİN

İstanbul University

Institute of Graduate Studies inScience and Engineering

Department of Computer Engineering

Supervisor : Prof. Dr.Ahmet SERTBAŞ

The development and diversification in the field of medical imaging technologies, is an important part of medical treatment institutions and business processes, and archiving the images back to the archive to be used in the electronic media because of the need arising from invoked of these operations, the cost to relocate to the standardization of the starting in this area, and so on for the purpose of the obligation to edit. For this purpose thereare some of national and international coding and classification systems.

In this dissertation, the standartslike HL7 and DICOM which used for transmitting and sharingdatas (MR, tomography, ultrasonografi, rontgen, ecgetc.) with institutions beingproducedby medical visulasition technologies has been improved in respect of security deficiencies of image transmitting and optimization. Encryption and decryptionmethods has been applied and compared to standart DICOM format used medical visualisation systems for both file field and metatag field which provides privacyof patient by distinguishing image and data of DICOM format. Inaddition to 3DES, AES, RSA also metatag encrypting and decryptingmethods has been preferred in the dissertation. The effects of data security bymeans of DICOM encryption cost has been manifestedthroughoperation of sampledsmall, medium and largehospitals.

June 2017,94 pages.

Keywords: Medical image data security performance analysis, DICOM data security performance analysis, Metatag data security performance analysis

1. GİRİŞ

Bilgisayar teknolojilerindeki gelişmeler daima Sağlık Sektörüne yansımakta, tedavi hizmetlerinin kalite ve performansında ciddi değişimlere neden olmaktadır. Son yıllarda ülkemizdeki tedavi kurumlarında ivme kazanmış olan bilgisayarlaşma sürecinde tıbbi kayıtların elde edilmesi, saklanması, iletimi, paylaşılması ve kullanılması bakımından ileri adımların atılması gereklidir.

Türkiye'de ki tüm tedavi kurumları, finansal çevirimin tamamını kapsayan ve diğer bazı bilgi sistemleri ile bütünleşmiş uygulamalara sahiptir. Bu kurumlarımızın önemli bir bölümünde de tıbbi kayıtların tutulmasının önemi kavranmış olup bu doğrultuda çalışmalar olanca hızıyla sürdürülmektedir.

Bu kapsamda tıp alanındaki görüntüleme teknolojilerinin ürettikleri verilerin (MR, Tomografi, Ultrasonografi, Röntgen Filmi, EMG gibi);

• Radyolog iş yükünü sanal ortam aracılığıyla radyologlara eşit olarak dağıtılması,

• Radyologların vakalar üzerinde çevrimiçi (online) konsültasyon yapabileceği platformu oluşturmak,

• Hastanın radyoloji hizmetini aynı kurumdan alması,

• Hastanelerde görev alan uzman radyologların bağlı oldukları kurumların dışında, başka kurumların hastalarına ait görüntülerin raporlamasının sağlanması,

• Radyolojik tetkiklerin raporlama süresinin kısaltılması,

gibi sebeplerle gerek hastane içerisinde gerekse hastaneler arası tıbbi görüntü verilerinin paylaşılması söz konusu olmuştur.

Gerek özel hayatın mahremiyeti gerekse de hasta mahremiyeti hukuki anlamda teminat altına alınmıştır. Dolayısı ile yasal düzenlemeler ilgili diğer kişilere(hekim, sağlık çalışanı ve diğerleri) bir diğerinin özel hayatına ve sağlığı ile ilgili hayatına saygı gösterme,

mahremiyetlerini koruma zorunluluğu getirmektedir. Bu zorunluluk hukuki anlamda sır saklama yükümlülüğü olarak tanımlanmaktadır.

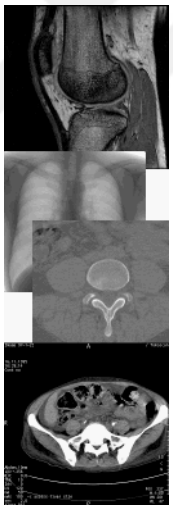
Sır saklama yükümlülüğü yasal dayanağını Anayasa, Türk Medeni Kanunu, Borçlar Kanunu, Hasta Hakları Yönetmeliği, Yataklı Tedavi Kurumları İşletme Yönetmeliği, Türk Deontoloji Nizamnamesi, Hekimlik Mesleği ve Etik Kuralları, Hipokrat Andı maddelerinden almaktadır. Anayasa'nın 20. Maddesi, Türk Ceza Kanunu'nun 135.136.137. Maddeleri, Borçlar Kanunu'nun 386.390. Maddeleri, Hasta Hakları Yönetmeliği 20.21.23. Maddeleri, Yataklı Tedavi Kurumları İşletme Yönetmeliği 7. Maddesi, Türk Deontoloji Nizamnamesi 4. Maddesi, Hekimlik Mesleği ve Etik Kuralları 9. Maddesi ve Hipokrat Andı hekimler ve sağlık çalışanları ve diğer kişiler için sır saklama yükümlülüğü ile ilgili maddeleri içermektedir.

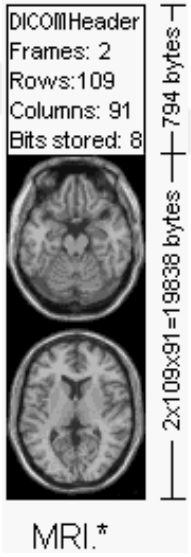
Yukarıda sayılan sebeplerden dolayı; tıbbi görüntü verilerinin yetkisiz kişilerin eline geçmesinin önlenmesi ve yetkisiz kişiler elde etse bile bu verilerin kullanılmasının engellenmesi önem kazanmaktadır.

Bu çalışmada; tıbbi görüntü verilerinin taşınması ve paylaşımında kullanılan DICOM (Digital Imaging and Communications in Medicine) standardının veri güvenliğinin analizi, tıbbi verilerin taşınması saklanması için protokol belirleyen Sağlık İşletmelerinin Entegrasyonu kurumunun (IHE-Integrating the Healthcare Enterprise) DICOM ve HL7 (Health Level Seven) güvenliği için kullandığı ATNA Profili'nin (The Audit Trail and Node Authentication) (SİEK North America Connectathon and Demonstration Handbook, 2006) analizi ve son olarak mevcut yapıların güvenliğini performansı etkilemeyecek şekilde geliştirme yapılabilmesi için yazılmış program verilerinin analizi incelenmektedir.

2. GENEL KISIMLAR

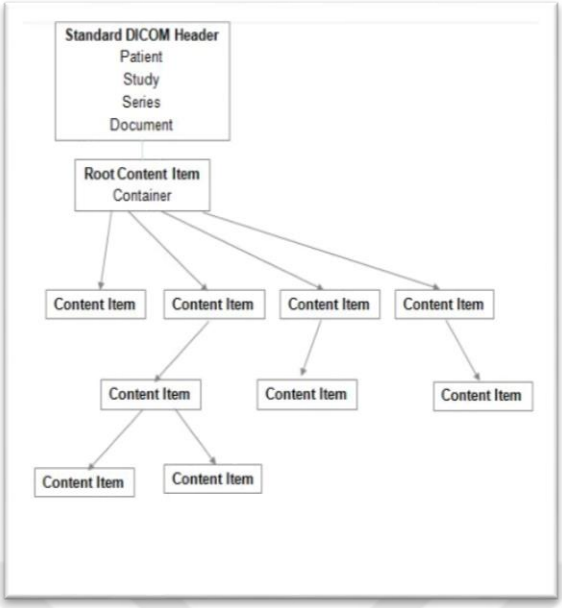
DICOM (Digital Imaging and Communications in Medicine) tıbbi görüntülerin dijital olarak saklanması ve taşınması konusundaki standart olarak kabul edilen görüntü formatıdır. Bu formatın önemli özelliği tıbbi görüntüler için standardize edilmiş, tüm tıbbi yazılımların kullandığı format olmasının yanında, görüntünün dışında hasta ile ilgili bilgileri ve yapılan tetkike ait parametre ve bilgileri taşımasıdır (Şekil 2.1 ve 2.2). Bu standart Amerikan Radyoloji Koleji(American College of Radiology-ACR) ve Ulusal Elektrik Üreticileri Birliği(National Electrical Manufacturers Association-NEMA) tarafından geliştirilmiştir. (Sağlık Bilişim Derneği Çalışma Grupları, 2008)

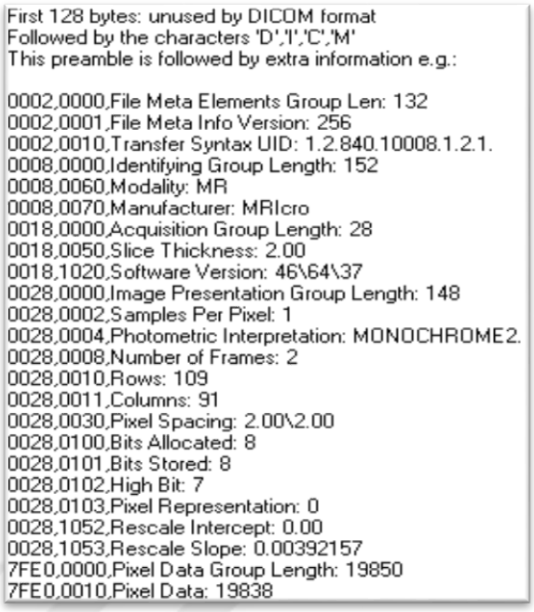




Şekil 2.1: DICOM görüntü örnekleri. **Şekil 2.2:** DICOM genel yapısı.

DICOM görüntü formatında veriler DICOM'un başlık(header) kısmında etiketler (metatag) halinde tutulur (Şekil 2.4). Bu etiket DICOM dosyasında Şekil 2.3'te gösterildiği gibi ağaç(tree) mantığı ile yerleştirilir (Gorthi ve diğ., 2009). Bu etiketler uygulamalara göre ve modelite (Örn: MR, CT, CR vb..) bazında değişiklik gösterebilir. Ancak DICOM 3.0 standardında standart tanımlanması gereken etiketler tanımlanmıştır.





Şekil 2.3: DICOM başlık yapısı . **Şekil 2.4:** DICOM etiket yapısı.

DICOM ile ilgili standartları geliştiren Ulusal Elektrik Üreticileri Birliği (NEMA, 2003), DICOM nesnesinin farklı modalitelerin aktarılmasında kullanılmasını esas almıştır. Bu modaliteler Şekil 2.5'te ayrıntılı olarak listelenmiştir.

Coding Scheme Designator	**Code Value**	**Code Meaning**
DCM	EPS	Cardiac Electrophysiology
DCM	CR	Computed Radiography
DCM	CT	Computed Tomography
DCM	DX	Digital Radiography
DCM	ECG	Electrocardiography
DCM	ES	Endoscopy
DCM	XC	External-camera Photography
DCM	GM	General Microscopy
DCM	HD	Hemodynamic Waveform
DCM	IO	Intra-oral Radiography
DCM	IVUS	Intravascular Ultrasound
DCM	MR	Magnetic Resonance
DCM	MG	Mammography
DCM	NM	Nuclear Medicine
DCM	PX	Panoramic X-Ray

Şekil 2.5: Dicom modalite tipi (nemavers. 20030108, 2003).

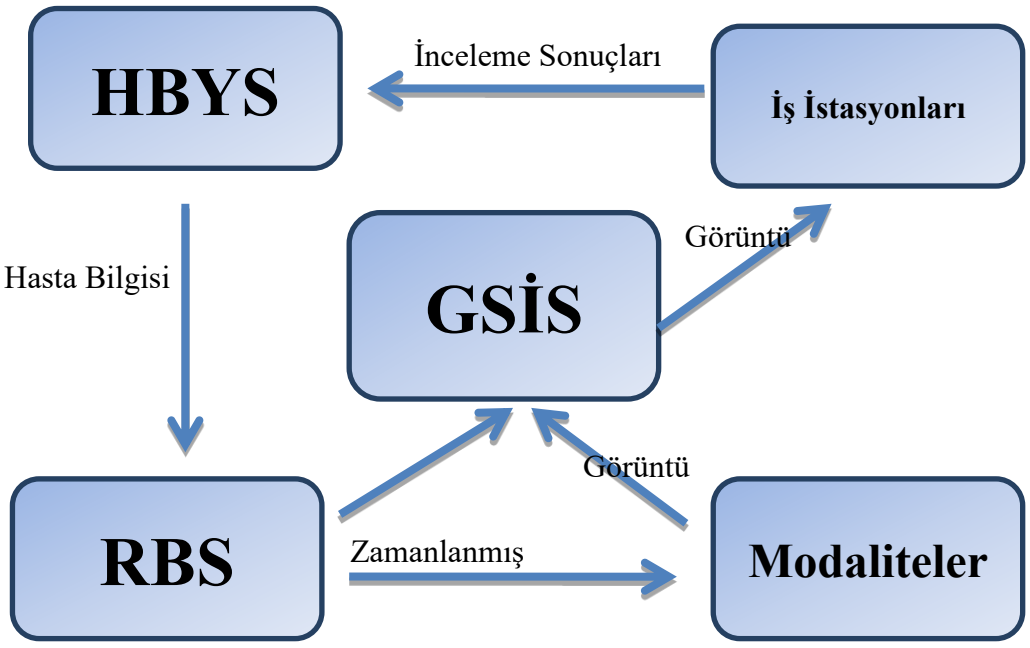
Coding Scheme Designator	Code Value	Code Meaning
DCM	PT	Positron emission tomography
DCM	RF	Radiofluoroscopy
DCM	RG	Radiographic imaging
DCM	RTIMAGE	Radiotherapy Image
DCM	SM	Slide Microscopy
DCM	US	Ultrasound
DCM	XA	X-Ray Angiography

Şekil 2.5 (devam): Dicom modalite tipi (nemavers. 20030108, 2003).

2.1. TIBBI GÖRÜNTÜLERİN SAĞLIK TESİSİNDEKİ TOPOLOJİSİ

Türkiye'de genellikle DICOM 3.0 (DICOM standart Ulusal Elektrik Üreticileri Birliği, 2004) da tanımlanan etiket hasta id (patient id) tekilliği (unique) sağlamak amacıyla T.C. kimlik no olarak kullanılmaktadır.

Şekil 2.6'da SİEK standartlarına uygun Türkiye genelindeki hastanelerdeki HBYS (Hastane Bilgi Yönetim Sistemi), RBS (Radyoloji Bilgi Sistemi), GSİS (Görüntü Saklama ve İletişim Sistemleri) ve iş istasyonlarının çalışma yapısı verilmiştir.



Şekil 2.6: SİE standartlarına uygun bir bilgi sistemi yapısı.

2.2. TIBBI GÖRÜNTÜLERİN (DICOM) YAPISINA AİT GÜVENLİK ÇALIŞMALARI

Türkiye'de kullanılan GSİS yazılımları hasta mahremiyetini korumak için hastanın verisini çalışma dosyası oluştururken anonimleştirmekte ve bu verinin sağlığı geliştirme çalışmaları için dahi kullanılması durumunda hastanın mahremiyetini korumaktadır.

2.2.1. DICOM 3.0 standardı modeli Dijital imza, Veri Bütünlüğü, Veri Gizliliği, Kimlik doğrulama, Anahtar yönetimi metotları

DICOM 3.0 standardı Güvenlik mimarisinde referans modeli Dijital imza, Veri Bütünlüğü, Veri Gizliliği, Kimlik doğrulama, Anahtar yönetimi metotları ifade edilmiştir.

Medikal görüntü veri bütünlüğü ve doğrulamadan bahsetmek için iki esas önemlidir (Kobayashi ve diğ., 2009).

Veri güvenliliğini sağlamak adına görüntü ve etiket ilişkisinin bozulması (görüntünün kime ait olduğu ve çekim tarihi gibi önemli bilgiler) veriyi anlamsız hale getirecektir. Bu sebeple; görüntü ve üst verinin ilişkisel yapısını bozulmaması veri güvenliği çalışmalarında önem arz etmektedir.

Veri güvenliliğini sağlamak adına görüntü işleme yöntemleri kullanılarak verinin anahtar değer (key Value) -örneğin bir kist gibi- önemli piksellerindeki kayıplar veriyi anlamsız hale getirecektir. Bu sebeple; görüntü kalitesinin bozulmaması, veri güvenliği çalışmalarında önem arz etmektedir.

Kobayashi ve diğ. (2009) makalesinde; bu iki sorun için Medikal görüntü (DICOM) veri bütünlüğü ve doğrulamayı iki değişik yaklaşım ile incelemiştir.

Üst Veri Kullanma Yöntemi; Bu yaklaşımda dijital imza DICOM başlık içinde saklanır. Görüntü Kalitesinin Bozulmaması; Dijital imzalama görüntü verisine uygulanarak sağlanır.

Mevcut yaklaşımların zayıf noktaları;

a. Üst Veri Kullanma Yöntemi

Bu yaklaşım üst veri ile görüntü verisinin ilişkisinin sabit tutacağını garanti edemiyor.

b. Damgalama (Watermarking)

Görüntünün dijital imza kısmı olan ilgili alan (region of interest -ROI)'i resmin ihtiyaç olan kısmına göre manuel seçilmesi uygulanabilir olmaması ve otomatik seçilmesi algoritmaya ağır iş yükü getiriyor. Unutulmamalıdır ki Damgalama yöntemi DICOM standardı olarak şu anda kabul görmemektedir.

Görüntü verisini şifrelemek için 16-bitlik piksel değerini iki eşit barçaya bölüp 8-bitlik 2 adet piksel verisi haline getirerek quaternion algoritmaları kullanılarak şifrelenmesi ve şifre çözme işlemi gerçekleştirilebilir. Bu durumda AES-ECB yöntemine göre toplam süre ile kıyaslandığından daha performanslı olduğu söylenebilir (Mariusz Dzwonkowski ve diğ. , 2015).

DICOM yapısı tek kesitli (frame) olduğu gibi; çok kesitli X-ray angiography (XA) intravascular ultrasound (IVUS) modeliteleri gibi veriler de olabilir.

Bu yapıda olan DICOM'lar için her kesit için aynı key kullanımı saldırıya açık bir durum oluşturur. Bu yüzden her kesit için farklı anahtar kullanmak gerekir. Simetrik şifreleme ardışık bir şekilde DICOM etiketlerini kullanarak yapılabilir. Gizli Anahtar(Private key) üretmek için başlangıç değerini her DICOM için tekil etiket olan DICOM standardında tanımlı SOP Instance UID kullanabilir ve devamında bundan üreteceğimiz anahtar ile bir sonraki kesit ardışık olarak şifrelemiş olur. İşlemleri tersten işleyerek verilerin değişmemesi koşulu ile şifre çözme yapılmış olur (Kobayashi ve Furuie, 2009).

Kobayashive Furuie'nin (2009) bu çalışmasından farklı olarak DICOM etiketlerinden üretilmiş AES-GCE ile şifreli etiketler hash'lenerek oluşan 512-bithash çıktısı orijinal görüntü verisinin AES-GCE ile şifrelenmesinde başlangıç (initial) vektör ve anahtar olarak kullanılabilir. Bu sayede; DICOM veri güvenliği artırılmış ve şifreleme ve şifre çözme performansı da artırılmış olur (Ali Al-Haj, 2015).

DICOM etiket verisi ile görüntü verisi ayrı ayrı şifrelenerek tekrar bir DICOM içerisinde şifreli bir şekilde tutulabilir. P.Subhasri, Dr. A. Padmapriya (2015) deki çalışmasında; DICOM etiketinin ASCII karşılıklarının Vigenere tablosu ile şifreleme yapılmıştır. DICOM görüntü verisinin ise RGB (Red, Green, Blue) piksel verisi, Vigenere tablosu ile şifreleme yapılmıştır. Ancak bu yaklaşım veri bütünlüğünü garanti edememekle birlikte

görüntü verisinin de bozulmamasını garanti edememektedir. Ayrıca Vigenere tablosu ile şifreleme yerine daha performanslı şifreleme yöntemleri tercih edilmesi uygun olacaktır.

DICOM hasta üst verisinin DICOM'un içinde tutulması veri güvenliğini azalttığı düşünülerek üst verinin, üst veri ile görüntü verisinin ilişkisel yapısını bozmadan ayrı bir veritabanında tutulması sağlanabilir (McEvoy, Svalastoga, 2007).

Bununla birlikte DICOM veri güvenliği için yapılacak herhangi bir güvenlik algoritması DICOM verisi üzerinde performansa dayalı aksaklıklara neden olmamalıdır. Çünkü gerek hastane içerisinde gerek hastaneler arası DICOM paylaşımı çekim sayıları fazla olduğu için ciddi network tıkanmalarına neden olmaktadır.

Kuzey Amerika Radyoloji Topluluğu 2003'un network ve sistem üzerine getirdiği yükü DICOM modalite bazında yapmış olduğu çalışma aşağıdaki listede ayrıntılı bir şekilde verilmiştir.

Tablo 2.1: Modalite bazında ağ trafiği ve sistem üzerinde DICOM yükü.

Incomingtrafficreport							
Modality	**Studies**	**Volume (mb)**	**Im/Stady**	**ImgSize (kb)**	**Rate (kb/s)**	**Acc Time**	**Total Time**
CR	6149	102,168.3	2.3	7,123.2	2,433.5	2.9	4.7
CT	1646	101,657,3	118.8	520.0	1,488.2	0.3	3.7
DS	79	5,422.2	33.4	2,053.8	345.8	5.9	153.7
MG	92	6,831.6	8.7	8,560,9	2,731.0	3.1	3.3
MR	525	19,726.5	202.6	185.4	645.4	0.3	57.8
OT	1	20.7	23.0	900.7	1,484.0	0.6	14.0
US	658	20,603.2	35.3	885.8	1,348.2	0.7	23.0
CR	9362	168,958.2	3.7	4,920.7	3,423.3	1.4	3.0
CT	1956	138,940,1	133.9	530.6	2,632.8	0.2	2.7
DS	118	10,927.4	47.3	1,956.6	3,590.9	0.5	14.4
DX	253	9,097.4	19.7	1,827,1	2,140.7	0.9	5.3
MG	83	2,556.6	3.8	8,142,1	216.2	37.7	15.8
MR	613	25,112.7	212.0	193.2	1,029.3	0.2	31.0
Outgoingtrafficreport							

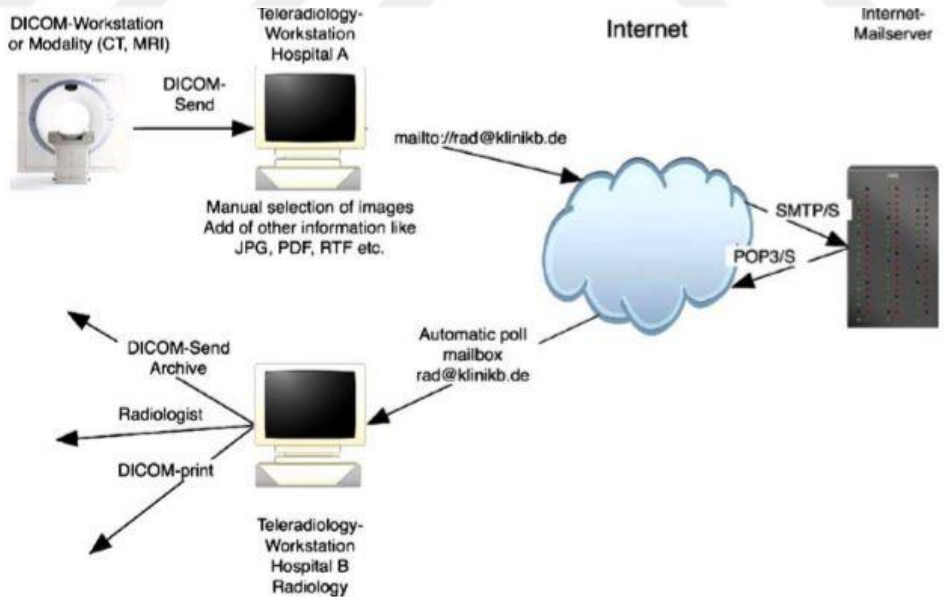
Tablo 2.1 (devam): Modalite bazında ağ trafiği ve sistem üzerinde DICOM yükü.

Modality	Studies	Volume (mb)	Im/Stady	ImgSize (kb)	Rate (kb/s)	Acc Time	Total Time
NM	1	1.0	1.0	1,025,6	1,924.2	0.5	0.5
OT	2	21.0	12.0	873,9	2,211.3	0.4	4.7
Unknown	53	3,894.1	30.9	2,377.3	3,553.4	0.7	0.8
US	1109	118,916.6	113.0	948.8	3,996.1	0.2	11.2

2.3. TIBBI GÖRÜNTÜLERİN (DICOM) SAĞLIK TESİSİNE GÖNDERİMİNDE KULLANILAN YÖNTEMLER

2.3.1 E-Posta ile Gönderme Yöntemi

DICOM veri transferi için PACS sunucu yazılımlarını kullanmamız şart değildir. Mesela;G. Weisser ve diğ. (2007) çalışmasında DICOM verisini e-posta protokolleri kullanarak transfer etmiştir. Burada DICOM iş istasyonu DICOM'u e-postaya ekleyip (attach) talep eden tarafa e-posta olarak gönderme yöntemi uygulanmıştır (Şekil 2.7).



Şekil 2.7: DICOM e-posta ile teleradyoloji uygulamaları.

Bu yöntemde;

a. DICOM gibi büyük hacimli verilerin e-posta içerisinde gönderen ve alanlarda tekrarlı bir şekilde tutulması veri tekrarına sebep olabilir ve disk problemleri oluşturabilir.

b. Veri güvenliğini sağlamak konusunda sadece e-posta güvenlik protokollerinin yeterli güvenliği sağlayamaması güvenlik açıklarına sebep olabilir.

c. DICOM veri transferinin fazla olduğu durumlarda, DICOM eklenmiş (attached e-mail) e-postaların posta sunucuları tarafından istenmeyen e-posta(spam) olarak algılanıp posta listesinden silinmesi gibi durumlara sebep olabilir.

2.3.2. Görüntü Saklama ve İletişim Sistemleri (PACS - Picture Archiving Communication Systems) ile gönderme yöntemi

DICOM verisinin toplanması ve yayınında GSİS sunucu yazılımı ile web ortamında iletilmesi sağlanması durumunda, 3 temel güvenlik aşaması söz konusu olmaktadır. (Vazquez-Naya ve diğ.,2002) (Sağlık İşletmelerinin Entegrasyonu Kurumu (IHE) DICOM 3.0 standardı)

2.3.2.1. İletim katmanındaki güvenlik

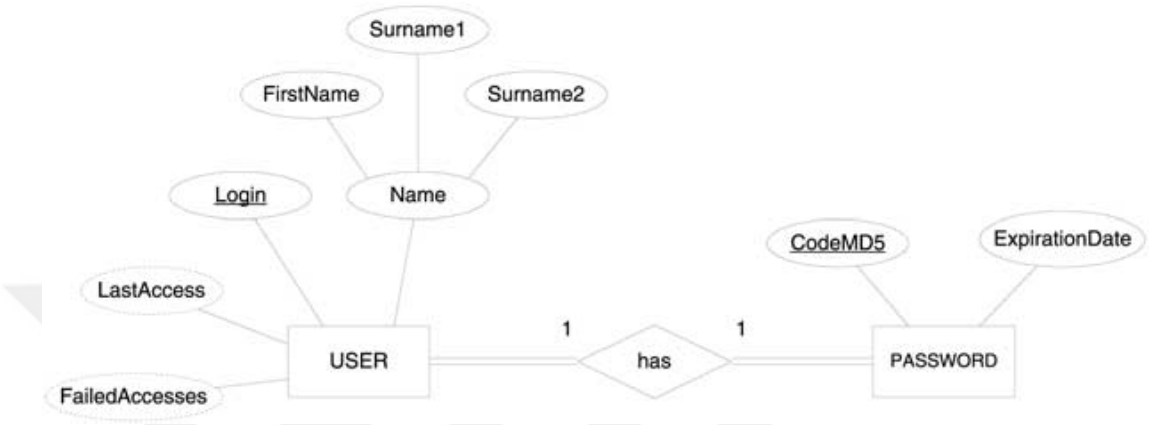
Bu katmanda TCP/IP üzerinde iletişim güvenliği ve mesaj bütünlüğü için tasarlanmış kriptografik bir protokol olan SSL(Secure Socket Layer) protokolü ve sertifikası güvenliği, istemciler ve sunucular arasındaki güvenin sağlanması, kimlik denetimi ve iletişimin şifrelenmesi sayesinde sağlamaktadır. Bu güvenlik yöntemleri esas alındığında yerel kısıtlamalar olmadığı sürece DICOM verisine Bulut(cloud) üzerinden Mobil ve PC ortamlarından erişim mümkün olacaktır (Patel ve diğ.,2012).

Standart TCP/IP haricinde DICOM için; DICOM sağlayıcı ve DICOM'u talep edici arasında farklı bir el sıkışma (Handshake) yöntemi ve belirli bir porttan erişim sağlanabilir.(Stites, S. Pianykh, 2016).El sıkışma başarılı olmaması durumunda ilgili bağlantı reddedilerek yetkisiz kişilerin erişimi engellenmiş olur. Standart 3'ü el sıkışma yöntemi ve varsayılan (default) port kullanımında DICOM Ping benzeri uygulamalar ile ağa erişime açık DICOM'lar taranarak yetkisiz kişiler tarafından ele geçirebilir.

2.3.2.2. Kimlik denetimi ve doğrulama

Bu aşamada Kullanıcı adı ve şifre kullanılır. İstemci tarafından girilmiş kullanıcı adı ve şifre SSL protokolü tarafından şifrelenerek güvenli bir şekilde sunucu tarafına yönlendirilir. İstemci kullanıcı adı şifreyi sunucuya gönderirken tek taraflı şifreleme algoritması MD5 veya geliştirilen Hash yöntemleri ile şifreler. Sunucu tarafında

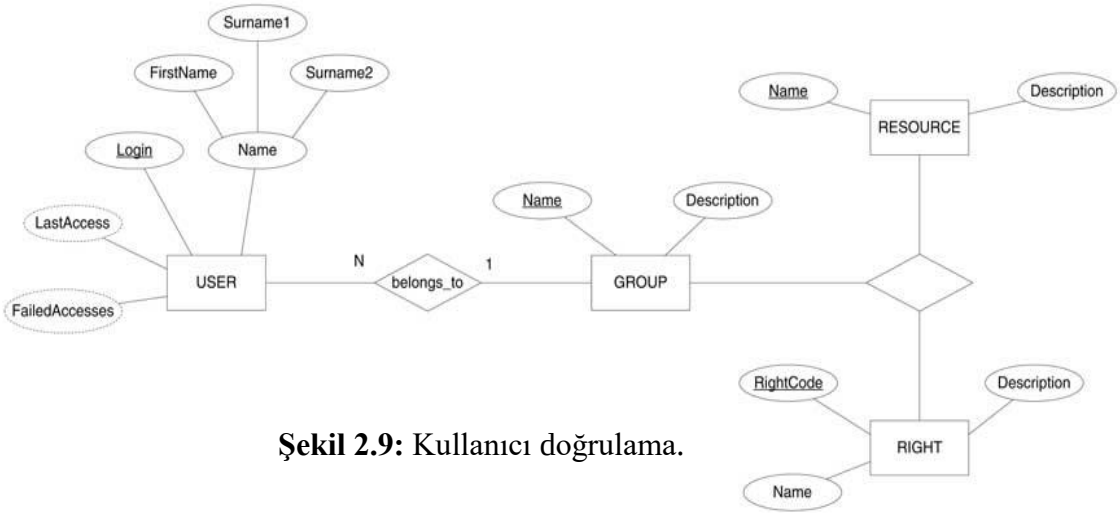
veritabanında MD5 veya geliştirilen Hash hali tutulan kullanıcı adı ve şifre gönderilen kullanıcı adı ve şifre ile karşılaştırılır ve eşleşme sağlanırsa kimlik denetimi yapılmış olur. Bu sayede veritabanı elde edilse dahi veritabanında tek taraflı şifrelenmiş MD5 veya geliştirilen Hash şifreleri olduğu için kullanıcı adı ve şifre yetkisiz kişilerin erişimine karşı korunmuş olur (Şekil 2.8).



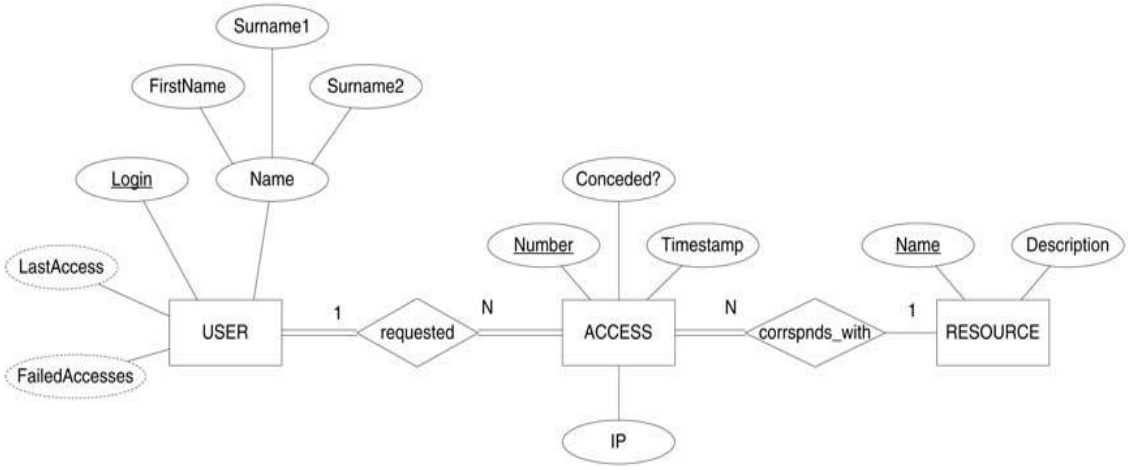
Şekil 2.8: Kullanıcı kimlik denetimi.

2.3.2.3. Veri erişimi kontrolü

Kullanıcı adı ve şifresi doğrulanan kullanıcılar yetki düzeylerine göre yetkilendirilmeleri sağlanmalıdır. Bu da kullanıcı profilleri oluşturularak kullanıcı bazında ve kullanıcı profili bazında yetkilendirme ile erişim kısıtlaması ile yapılabilir (Şekil 2.9, Şekil 2.10).



Şekil 2.9: Kullanıcı doğrulama.



Şekil 2.10: Veri erişimi kontrolü.

2.4. SİEK DICOM 3.0 STANDARDI VE KARŞILIKLI DOKÜMAN PAYLAŞIM SİSTEMİ (XDS CROSS-ENTERPRİSE DOCUMENT SHARİNG) YAPISI

Hastane ortamında paylaşılan veriler sadece DICOM verileri değildir. Bu verilerin hasta mahremiyeti kapsamında tamamı mahrem veri olduğu için bütün bu verilere yetkisiz kişiler tarafından erişimin kısıtlanması gerekmektedir.

Bu veriler; Hasta Kişi bilgileri, Tıbbi geçmiş, DICOM, EKG, Laboratuvar sonuçları Raporlar ve Mali veriler olarak özetlenebilir.

DICOM verilerini de kapsayan bu veri kümelerinin SİEK tarafından taşınması ve paylaşımının yapılması için XDS tanımlanmıştır. XDS'nin genel yapısı, HBYS (Hastane Bilgi Yönetim Sistemi), dokümanların tutulduğu depo (Repository) ve bu dokümanların indekslerinin tutulduğu kayıt defterin (Registry)'den oluşmaktadır.

XDS yapısında medikal dokümanların üst verisini ve dokümanın aslının tutulduğu yerin bilgisini içerir. XDS medikal verilerin paylaşılması için minimum veri kümelerinin kullanır. Bu sayede, entegrasyon ve iyileştirmelerin kolay yapılması mümkün kılınır.

2.4.1. XDS Veri Erişim Yapısı

XDS mantığını analizini doğru yapabilmek için KİM, NEYİ, NE ZAMAN ve NERDE sorularına cevap aranmalıdır (Parisot, 2005).

Neyi ve Nerde sorusuna; XDS'de ilgili doküman verisi XDS depoda ve bu verinin adresi ve üst bilgisi kayıt defterinde ilişkili olarak tutularak cevap verilir.

XDS SİEK'nin tanımladığı hasta numarası(Patient ID) profiline uygun yapıda olduğu için ilgili doküman her aşamada KİM'e ait olduğu bilinmektedir.

XDS yapılan bütün işlemleri zaman sunucusunda saklar. Bu şekilde yapılan işlemlerin NE ZAMAN yapıldığı kayıt altına alınmış olur.

2.4.2. Denetim İzi ve Düğüm Kimlik Doğrulaması (DİDKD ATNA-Audit Trail and Node Authentication) Profili.

XDS'de veriye erişimin yetkilendirilmesini ve doğrulanmasını DİDKD profili sağlar.

DİDKD'da sistemde dosyalara oluşturma, erişme, değiştirme ve silme işlemlerini yapabilecek Güvenli düğüm (Secure node) tanımlaması yapılmalıdır (Tsai ve diğerleri,2009).

Bu işlemlerin ne kadarını hangi kullanıcı yapacağını kısıtlama yetkisi SİEK aktor olarak tanımlanan üst düzey kullanıcılarda mevcuttur. Her Güvenli düğüm aynı zamanda zaman sunucusuyla senkronize çalışarak yapılan işlemlerin zaman kütüklerini oluşturur.

Güvenli düğümler diğer güvenli düğümlerle, zaman sunucusu ile SİEK Aktor'le kütük defteri ve depo ile yaptığı bütün bağlantılar sertifika ile sertifikalandırılmalıdır.
Ayrıca hasta verisine sadece ilgili hasta doktoru veya danışmanı yetkilendirilmeli, sistemdeki diğer kullanıcılardan bu bilgiler saklanmalıdır.

Bütün bunlar DİDKD profilinin güvenliği sağlamaktaki kolaylıkları olsa da, hastanelerin acil bölümlerinde acil gelen hastaların kimlik bilgileri ilk giriş sırasında alınamayabilir. Burada güvenlik ve verilerin doğru gönderilmesi insan hayatından sonra geleceği için göz ardı edilebilir. Bunun içinde ayrı bir çalışma yapılması gerekir.

Güvenli düğümlerin yaptıkları her erişim ve olayları (events) denetim (audit) mesajları olarak tutulur. Denetim mesaj yapısı Tablo 2.2'de belirtilmiştir.

Tablo 2.2: DİDKD'da tanımlı denetim mesajları.

Özellik	Tanımlamalar
Durum	Yapılan işlemin durumu (Sonlandı, Hata, Askıda)
Başlangıç Zamanı	İşlemin başlangıç tarih ve saati
Bitiş Zamanı	İşlemin bitiş tarih ve saati
Mesaj	İşlemin içeriği ilgili bütün veriler
Kütük seviyesi	Bilgi, Hata, Uyarı

3. MALZEME VE YÖNTEM

3.1. KULLANILAN PLATFORM VE ŞİFRELEME ALGORİTMALARI

Hasta verisini okumak ve gerekli olan verileri belirlemek içinVisual studio 2010 (Microsoft Corporation) platformu kullanıldı. Bu platform Visual basic ve C# dillerinin desteklemektedir. C# daha güçlü bir dil olması sebebiyle bu program için C# dili tercih edilmiştir.

Bu çalışmada geliştirilen program Windows 10 Pro işletim sistemi , Intel i7 64 bit 8 çekirdekli işlemci ve 8 GB RAM olan PC ortamında çalıştırılmıştır.

DICOM görüntüleyici (Açık kaynak kod - Open Source) Harsha T, Amarnath S, S Mahesh Reddy tarafından 2011 tarihinde yazılan C# kütüphanesi kullanılmıştır.

İlgili verilerin depolanmasında MSSQL SERVER 2014 Veritabanı Yönetim Sistemi kullanılmıştır. Veri tabanı işlemlerini yapabilmek için kodlamada Veri tabanı Erişim katmanı (Data Access Layer) olarak katmanı olarak LinQtoSQL iskelet (Framework)'i kullanılmıştır.

İlgili verileri uygun görsellerde gösterimi için Sunum katmanında Telerik iskeletinin Grafik bileşenleri kullanılmıştır. Şifreleme işlemleri için 3DES, AES, RSA şifreleme ve şifre çözme algoritmaları kullanılmıştır.

3.1.1. Çizgi Grafik (Line Chart) Bileşenleri

Telerik iskeletinin Çizgi grafikleri ile kıyaslama yapılabilmesi kolaylaştırılmıştır. Bu çalışmada geçen yöntemler adedince Çizgi serileri oluşturulmuş. Elde edilen veriler oluşan bu serilerde aynı çizgi üzerinde gösterilerek kıyaslama yapılmıştır.

3.1.2. Sütun Grafik (Bar Chart) Bileşenleri

Elde edilen veriler Telerik iskeletinin Grafik ile Bar serileri oluşturarak gruplar halinde sütun grafikler çizilmiş ve kıyaslamaya yardımcı olacak görsel grafikler oluşturulmuştur.

3.1.3. Pasta Grafik(Pie Chart) Bileşenleri

Elde edilen veriler Telerik iskeletinin Grafik ile pasta serileri oluşturarak ortalama değerler üzerinden yüzdelik oranlar çıkarılmış ve kıyaslamaya yardımcı olacak görsel grafikler oluşturulmuştur.
Tüm sürelerin ölçümünde .net iskeletinin System.Diagnostics.Stopwatch kütüphanesi içindeki sayaç kullanılarak ilgili sayacın Elapsed Milliseconds özelliğinden geçen süreler milisaniye cinsinden kaydedilmiştir.

3.1.4. 3DES Algoritması

3DES (Üçlü DES), 1978 yılında IBM tarafından geliştirilmiş olan bir şifreleme algoritmasıdır. Brute Force saldırılara karşı koymakta zorlanan DES (Data Encryption Standard - Veri Şifreleme Standardı) algoritmasının üzerine geliştirilmiştir. (link:http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/08/3des-algoritması).

Özellikleri:

Çift yönlü çalışır. Şifrelenmiş veri geri çözülebilir.

DES şifrelemesinin 3 kere art arda yapılması şeklinde çalışır.

DES şifreleme yöntemine göre 3 kat daha yavaş çalışır.

Şifreleme yapmak için uzunluğu 24 bayt olan bir anahtar kullanılır. Her bayt için 1 eşlik biti vardır. Dolayısıyla anahtarın uzunluğu 168 bittir.

Veri, 3DES anahtarının ilk 8 baytı ile şifrelenir. Sonra veri anahtarın ortadaki 8 baytı ile çözülür. Son olarak anahtarın son 8 baytı ile şifrelenerek 8 bayt bir blok elde edilir.

Avantajları:

Çift yönlü çalıştığından şifreli bir şekilde veriler saklanabilir, istenildiği zaman geri çağrılarak şifresi çözülebilir.

Bilgisayarın donanımsal açıklarını kapatır (örnek: VPN, veri haberleşme ağları).

Dezavantajları:

Güvenlik tamamen kullanılan anahtara dayanmaktadır. Anahtarın zayıflığı, şifrenin çözülmesini kolaylaştırır.

Daha gelişmiş bir algoritmaya sahip olan AES (Advanced Encryption Standard-Gelişmiş Şifreleme Standardı) şifreleme yöntemine göre daha yavaş çalışır.

Kullanıldığı Yerler:

Bankacılık sistemi

Ciddi güvenlik programları

Elektronik ödeme sistemi (kredi kartıyla internetten alışveriş yapma)

3DES, yavaş yavaş ortadan kalkmaktadır. 3DES'in yerini AES (Gelişmiş Şifreleme Standardı) almaktadır.

.NET teknolojisi ile yazılım geliştirenler, herhangi bir veride şifreleme yapmak için, NET iskeleti içerisinde yer alan System.Security.Cryptography kütüphanesini kullanmaktadırlar. Bu kütüphane içerisinde yer alan fonksiyonlar sayesinde, yazılımcı istediği platformda güvenli bir şekilde veri şifreleme ve şifre çözümleme yapabilmektedir. Yazılım geliştiricinin 3DES algoritmasını kullanarak şifreleme yapabilmesi için TripleDESCryptoServiceProvider sınıfını kullanması gerekmektedir.

3.1.5. AES (Advanced Encrytion Standard - Gelişmiş Şifreleme Standartı)

3DES'e göre daha güvenli bir sistemdir. Çeşitli bilim adamları tarafından 3DES'in kırılması üzerine 2001 yılında geliştirilmiştir. Belçikalı Vincent Rijmen ve Joan Daemen tarafından bulunmuş, 3DES'in ve zayıf yönlerini tamamen düzelterek, matematikle oluşturulmuş bir blok şifreleme algoritmasıdır. 128 bit, 192 bit ve 256 bit olmak üzere üç farklı anahtar uzunluğuna sahip olabilir. AES'in3DES'in aksine donanımda ve yazılımda hızlı olması, daha kolay uygulanabilir olması ve çok daha az hafızaya gerek duyması güçlü yönleri olarak söylenebilir. Günümüzde bilinen tüm akademik, pratik ve doğrudan (bruteforce) saldırılara karşı dayanıklı olduğu düşünülmektedir. En yaygın olarak kullanılan simetrik şifreleme algoritmasıdır.

(link:http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/şifreleme-yöntemleri, 2013)

3.1.6. RSA (Rivest-Shamir-Adleman)

1977 yılında R. Rivest, A. Shamir ve L. Adleman isminde üç bilim adamının oluşturduğu yeni asimetrik şifreleme algoritması RSA, anahtar dağıtımının yanında şifreleme ve şifre çözme işlemlerini de gerçekleştirmektedir. RSA, güvenilirliği çok büyük tam sayılarla işlem yapmanın zorluğuna dayanan bir şifreleme tekniğidir. Bir genel anahtarlı şifreleme tekniği olan RSA, çok büyük tamsayıları oluşturma ve bu sayıları işleminin zorluğu üzerine düşünülmüştür. Anahtar oluşturma işlemi için asal sayılar kullanılarak daha güvenli bir yapı oluşturulmuştur. Genel olarak RSA hem mesaj şifreleme hem de elektronik imza amacıyla kullanılan daha çok ticari uygulamalarda tercih edilen tam sayılar üzerinden iyileştirme yapılarak oluşturulan değerlerden anahtarların üretildiği bir şifreleme teknolojisidir. RSA algoritmasında sistemin güvenilirliğinin yanı sıra hızının da yüksek olması için, kullanılacak anahtarın sayısal büyüklüğü önemlidir. Yeterli güvenilirlik derecesine ulaşmak için gerekli büyüklük Eliptik Eğri Şifreleme (ECC) Algoritması kullanılarak belirlenmektedir. RSA ile günümüzde 1024 bitlik bir anahtar (yaklaşık 300 basamaklı bir sayı) basit uygulamalar için yeterli bir şifreleme tekniği olarak kullanılabilir. RSA algoritması, bir şifreleme algoritması için oldukça basit bir algoritmadır. Buna karşın sürekli çok büyük asal sayı oluşturmak oldukça zor bir işlemdir.

RSA şifreleme sistemin oluşturulmasıyla birlikte asimetrik şifreleme algoritmalarının günümüzde daha yaygın olarak kullanılması sağlanmıştır.

3.1.7. Kullanılan Test Verileri

Bu çalışmada; Test amaçlı 95 adet CR (Computed Radiography), CT (Computed Tomography), DX(Dijital Radiography), EK (Electrocardiography), IO (Intra-oral Radiography), MR (Magnetic Resonance), US (Ultrasound), MG (Mammography) ve OT (Other Modality - retired) DICOM verileri kullanılmış ve modalite bazında Tablo 3.1'de gösterilmiştir.

Tablo 3.1: Modalite bazında DICOM verileri.

Modalite	Toplam Boyut(byte)	Sayı
US	93064	1
MR	140650	4
MR	140652	4
MR	140654	16
CT	527834	45
CT	533354	1
CT	578980	1
US	922612	1
IO	1155414	1
IO	1155416	2
IO	1155418	1
IO	1155540	1
IO	1155544	2
IO	1155546	1
IO	1157072	3
IO	1157074	1
IO	1157484	1
IO	1157488	1
EK	2922616	1
CR	7534548	1
MG	8788800	1
OT	10556710	1
CR	11800510	2
DX	13273880	1
DX	15505792	1
Toplam	85022652	95

3.2. YÖNTEM

Bu çalışmada anlatılan yöntemlere ek olarak yapılan çalışmada DICOM nesnesinin İletim Katmanı Güvenliği (TLS - Transport Layer Security) ve kullanıcı temelli ve denetim kütüklerinin tutulması (DİDKD profili) gibi yöntemlere rağmen saldırıların ve güvenlik açıklarının çoğunluğunun iç güvenlik açıklarından kaynaklanması göz önünde bulundurulduğunda; DICOM nesnesinin bir şekilde kötü niyetli kişiler tarafından ele geçirilmesi durumunda bile hasta mahremiyetini sağlamak amacıyla DICOM'un tamamını şifrelenmesi ve etiketlerinin şifrelenerek asıl büyüklüğü sağlayan görüntü

verisinin şifrelenmeden DICOM'un anonimleştirilmesi yapılarak; iki yöntem arasındaki performans farklarının ve surelerinin analizi yapılmıştır.

DICOM nesnesinin ele geçirilmesi durumunda; DICOM içerisinde hasta verileri (TC kimlik no, hasta no, hasta adı vb..) açık bir şekilde bulunması standart DICOM görüntüleyicilerle kolayca okunabilmesi hasta mahremiyeti ihlali oluşturmaktadır. Bu durumu engellemek için DICOM nesnesini iki farklı yöntem ile şifrelemesi bu çalışmada uygulanmıştır.

3.2.1. DICOM'u Dosya Olarak Tamamının Şifrelenmesi

DICOM dosyası standart dosya şifre yöntemleri ile şifrelenerek yetkisiz kişilerin erişmesi durumunda hasta verilerine DICOM etiketlerine ve DICOM'un görüntü kısmına erişimin engellenmesi sağlanabilir.

3.2.1.1 Avantajları

- DICOM dosyasının tamamı şifreleneceğinden yetkisiz kişiler tarafından görüntü verisine de erişilememesi,

- Etiket ve görüntü ayrıştırılmayacağından ayrışma işlemi sırasında doğabilecek hatalar durumunda veri bütünlüğünün ve etiketlerin bozulmasının engellenmesi,

- DICOM'un orjinal yapısının bozulmaması görüntünün ayrışması sırasında bozulmaların önüne geçmesinin sağlanması şeklinde sıralanabilir.

3.2.1.2. Dezavantajları

- DICOM dosyalarının boyut olarak büyük kısmını görüntü verileri oluşturduğundan dosya olarak şifreleme durumunda verinin tamamımın şifrelenmesinin performans sorunları oluşturacağı,

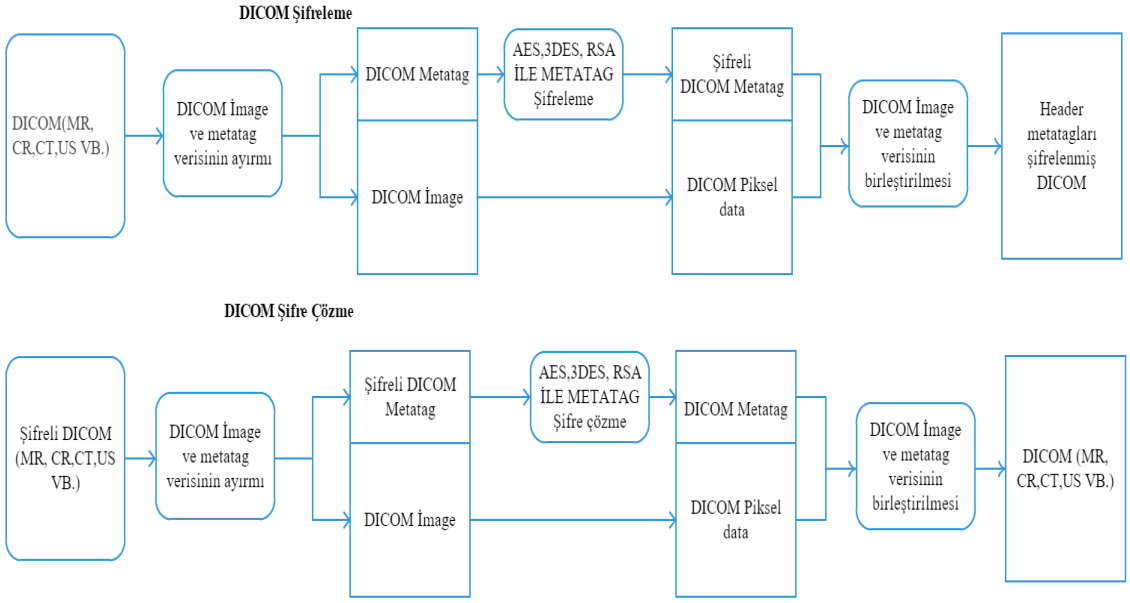
- Şifreleme ve şifre çözme sırasında çıkabilecek sorunlarda DICOM dosyasının tamamının erişilemez olması,

- Şifreleme ve şifre çözme sırasında çıkabilecek sorunlarda DICOM'un görüntü kısmında deformasyon olması durumunda klinik karar vermede malpraktis oluşturabilmesi şeklinde sıralanabilir.

3.2.2. DICOM Dosyasının Sadece Etiket Kısmının Şifrelenmesi

DICOM'un görüntü verisinin başlangıç bitine kadar olan kısım kesilip bütün etiketleri özyinelemeli (recursive) bir şekilde alınarak standart metin şifreleme algoritmaları ile şifrelenmesidir. Şekil 3.1'de DICOM dosyasının sadece etiket kısmının şifreleme (encryption) ve şifre çözme (decryption) yöntemi diyagram olarak gösterilmiştir.

Bu çalışmada simetrik şifreleme yöntemleri 3DES, AES ve asimetrik şifreleme yöntemi RSA seçilmiştir. Burada yöntemlerin şifreleme ve şifre çözme performansının DICOM üzerindeki etkilerinin analizi çıkarılmaktadır.



Şekil 3.1: Çalışmada önerilen etiket şifreleme ve şifre çözme yöntemi.

3.2.2.1. Avantajları

- DICOM dosyalarının boyut olarak büyük kısmını görüntü verileri oluşturduğundan sadece etiketlerin şifrelenmesi performans yönünden avantaj sağlaması,

- Şifreleme ve şifre çözme sırasında çıkabilecek sorunlarda DICOM'un görüntü kısmının bozulmaması ve erişilemez hale gelmemesi,

- Dosya bazında şifreleme yerine metin bazlı şifreleme kullanıldığından şifreleme süresinin kısa olması,

- Şifreleme ve şifre çözme sırasında çıkabilecek sorunlarda DICOM'un görüntü kısmında deformasyon olmayacağından klinik karar vermede malpraktisin önlenmesi şeklinde sıralanabilir.

3.2.2.2. Dezavantajları

- DICOM dosyasının tamamı şifrelenmediğinden yetkisiz kişiler tarafından görüntü verisine erişilebilir olması,

- Etiket ve görüntü ayrıştırılacağından ayrışma işlemi sırasında doğabilecek hatalar durumunda veri bütünlüğü ve etiketlerin bozulması şeklinde sıralanabilir.

3.3. DICOM'DAKİ HASTA VERİSİNİN OKUNMASI VE ŞİFRELENMESİ

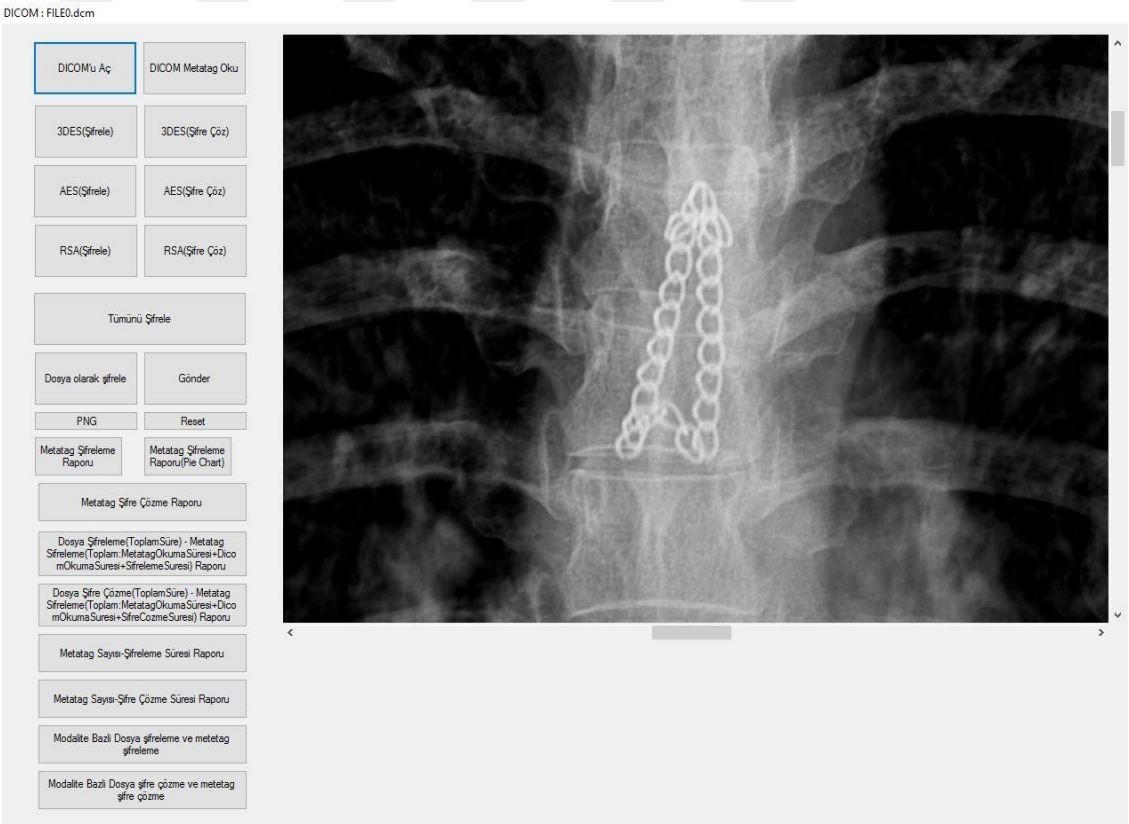
3.3.1. DICOM'un Okunması

Eğer seçilen dosya büyüklüğü 0 byte'tan büyükse ve seçilen dosya DICOM formatında yani (.dcm) uzantılı bir dosya ise seçilen bu dosya DicomDecoder.cs sınıfından bir nesne oluşturularak bu nesneye atılıp, DICOM dosyasının etiketleri, DicomDictionary.cs sınıfından bir nesne oluşturulduktan sonra bu nesneye atıldı.

DicomDecoder sınıfında görüntünün başladığı bit belirlendi ve bu şekilde görüntü ve etiket verilerinin dosyanın hangi bitinden itibaren başladığı tespit edilmiş oldu.

Belirlenmiş olan bit aralığındaki görüntü verisi DICOM içindeki görüntü verisinin gösterilmesini sağlayan Image Panel Control componentine piksel piksel gönderilerek Şekil 3.2'de görüldüğü gibi ekranda gösterimi sağlandı.

Performans kıyaslaması yapabilmek için işlem zamanını ölçülmesi gerekmektedir. Bu yüzden System.Diagnostics.Stopwatch kütüphanesi kullanılarak oluşturulan diff nesnesi işlemin başlangıç zamanında Start() foksiyonu ile başlatılıp işlemin bitiş zamanında Stop() fonksiyonu ile sonlandırılarak aradaki zaman farkı mili saniye cinsinden Elapsed time (geçen süre) olarak belirlendi.

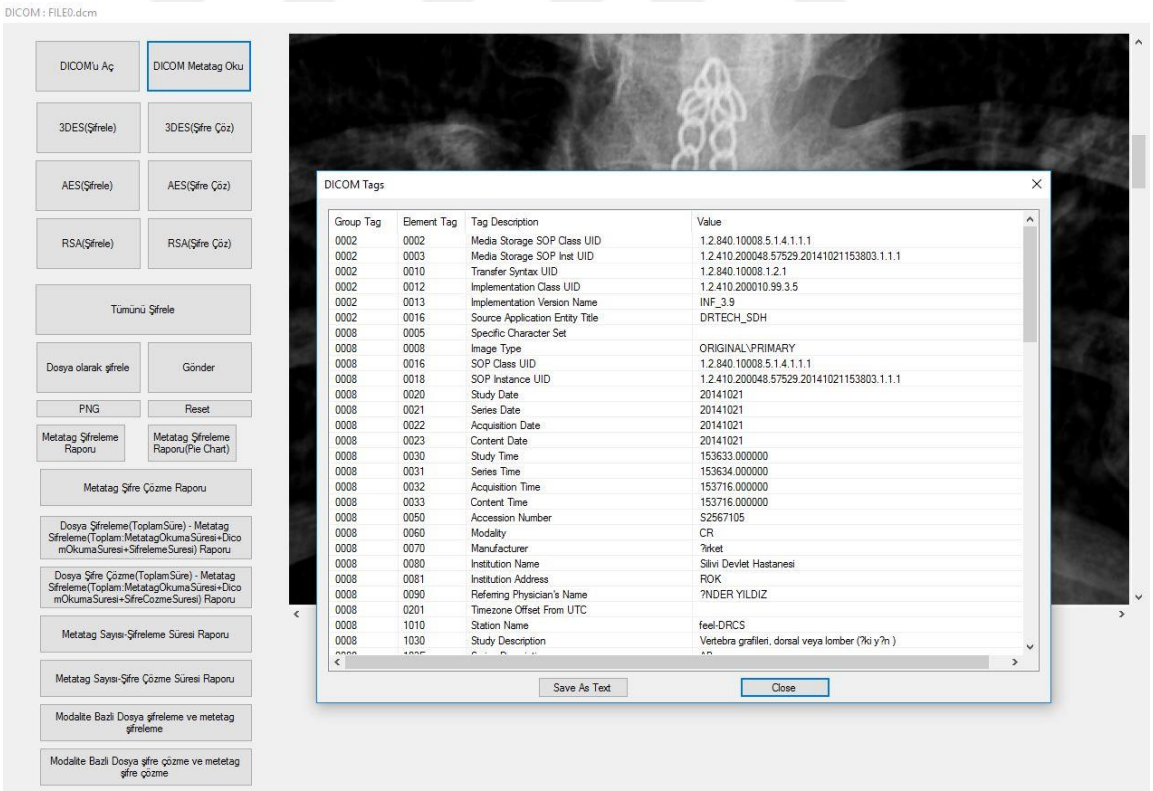


Şekil 3.2: Okunan DICOM gösterimi.

3.3.2. Açılan DICOM etiketlerini Okuma

Açılan DICOM'un görüntü verisi ve etiketlerinin başladığı bitler okunma sırasında tespit edildiği için etiketlerin başladığı bitlerden etiket verisi okunmaya başlandı.
Etiket verisi Grup etiketi, Element etiketi, Etiket Açıklaması ve etiket Değeri olarak dört kısımdan oluşur. DICOM'un etiketlerinin başladığı bitten, görüntü verisinin başladığı bite kadar bir döngü içinde Grup etiketi, Element etiketi, Etiket Açıklaması ve etiket Değeri sırasıyla okunması sağlandı. Okunan veriler metinlerden oluşan bir listeye atılarak Şekil 3.3'de görüldüğü gibi ekrana yazdırıldı.

Performans kıyaslaması yapabilmek için işlem zamanını ölçülmesi gerekmektedir. Bu yüzden System.Diagnostics.Stopwatch kütüphanesi kullanılarak oluşturulan diff nesnesi işlemin başlangıç zamanında Start() foksiyonu ile başlatılıp işlemin bitiş zamanında Stop() fonksiyonu ile sonlandırılarak aradaki zaman farkı mili saniye cinsinden Elapsed time olarak belirlendi.

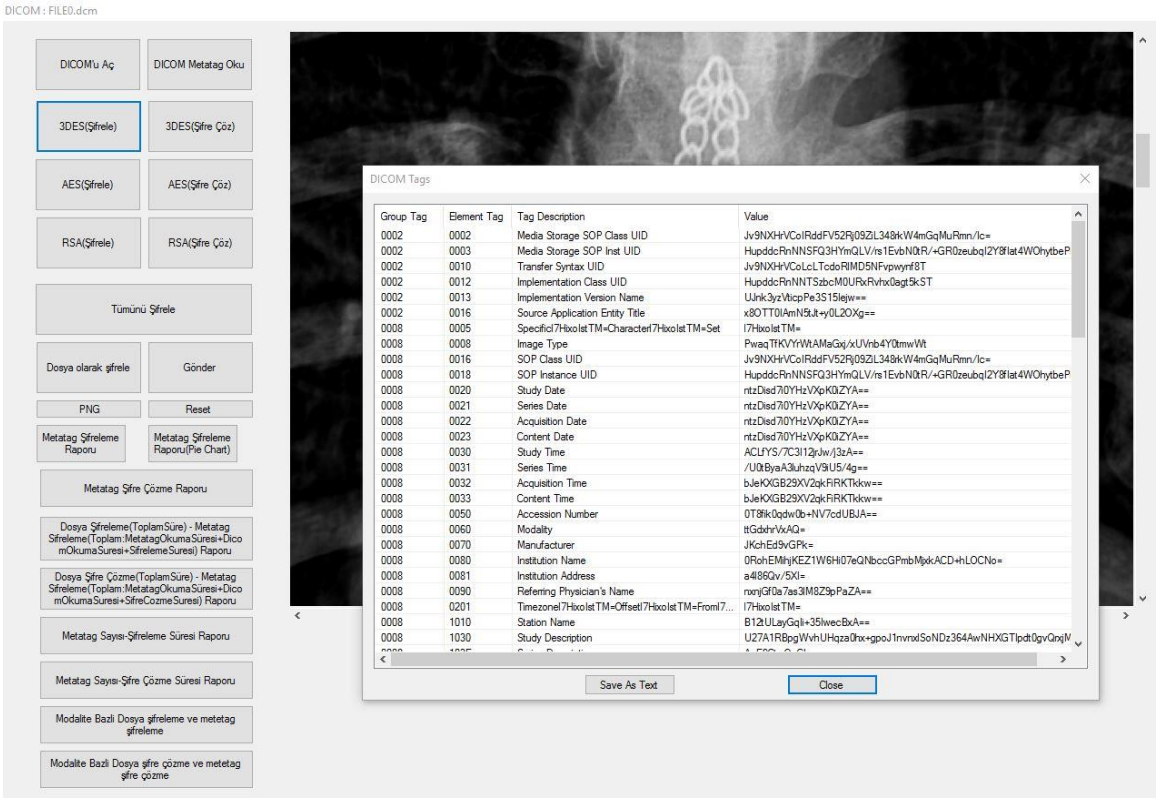


Şekil 3.3: Okunan DICOM etiket gösterimi.

3.3.3. Okunan DICOM etiketlerini 3DES İle Şifreleme

Okunan ve metinlerden oluşan bir listede tutulan DICOM etiketlerin değeri, anahtar değeri "NYYObMInlTtentKODigMiSE/NSp/4JQv" ve başlangıç vektör değeri "PenS8UCVF7s=" ile 3DES şifreleme ile bir döngü içinde şifrelenerek DICOM'a kaydedildi ve Şekil 3.4'de görüldüğü gibi ekrana yazdırıldı.

Performans kıyaslaması yapabilmek için işlem zamanını ölçülmesi gerekmektedir. Bu yüzden System.Diagnostics.Stopwatch kütüphanesi kullanılarak oluşturulan diff nesnesi işlemin başlangıç zamanında Start() foksiyonu ile başlatılıp işlemin bitiş zamanında Stop() fonksiyonu ile sonlandırılarak aradaki zaman farkı mili saniye cinsinden Elapsed time olarak belirlendi.

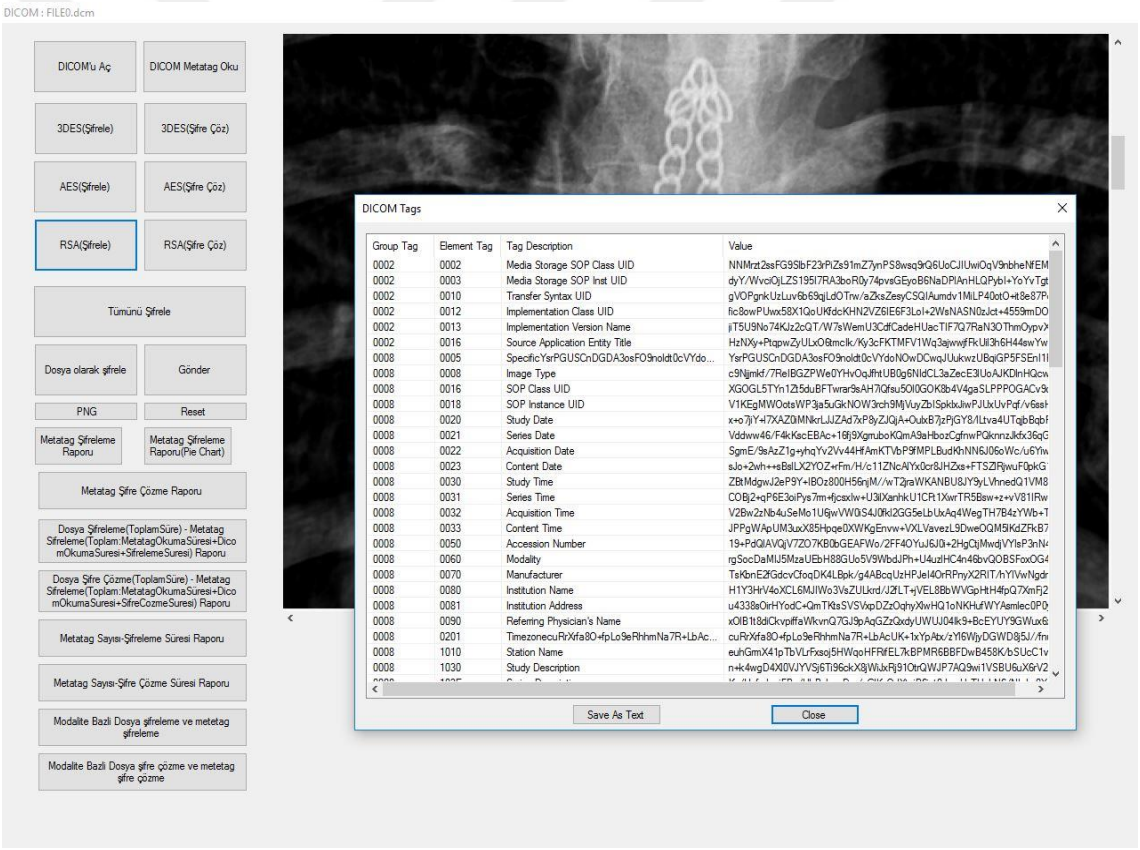


Şekil 3.4: Okunan DICOM 3DES ile şifrenmiş etiket gösterimi.

3.3.4. Okunan DICOM etiketlerini RSA İle Şifreleme

Okunan ve metinlerden oluşan bir listede tutulan DICOM etiketlerin Değeri, .net kütüphanesinde bulunan RSACryptoServiceProvider sınıfından türetilen ve RSA şifrelemesi için üretilen parametrelerle RSA ile bir döngü içinde şifrelenip DICOM'a kaydedilerek, Şekil 3.5'te görüldüğü gibi ekrana yazdırıldı.

Performans kıyaslaması yapabilmek için işlem zamanını ölçülmesi gerekmektedir. Bu yüzden System.Diagnostics.Stopwatch kütüphanesi kullanılarak oluşturulan diff nesnesi işlemin başlangıç zamanında Start() foksiyonu ile başlatılıp işlemin bitiş zamanında Stop() fonksiyonu ile sonlandırılarak aradaki zaman farkı mili saniye cinsinden Elapsed time olarak belirlendi.



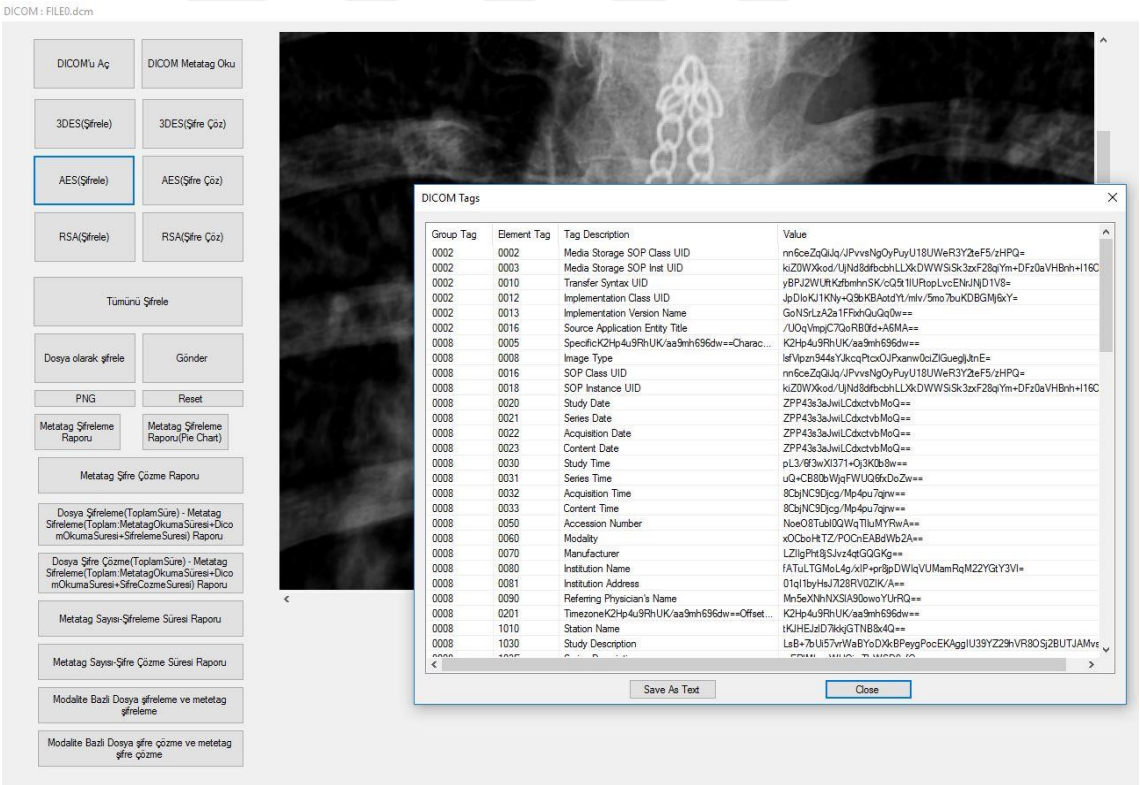
Şekil 3.5: Okunan DICOM RSA ile şifrenmiş etiket gösterimi.

3.3.5. Okunan DICOM Etiketlerini AES İle Şifreleme

Okunan ve metinlerden oluşan bir listede tutulan DICOM etiketleri,

- Anahtar “12345678” ,
- Hash Algoritması SHA1,
- Başlangıç vektörü “OFRna73m*aze01xY”,
- Şifre tekrarlanması 2 (key iteration) ,
- Anahtar size 256 bit ve
- Salt Kosher değerleri kullanılarak AES şifreleme ile bir döngü içinde şifrelenerek DICOM’a kaydedildi ve Şekil 3.6’de görüldüğü gibi ekrana yazdırıldı.

Performans kıyaslaması yapabilmek için işlem zamanını ölçülmesi gerekmektedir. Bu yüzden System.Diagnostics.Stopwatch kütüphanesi kullanılarak oluşturulan diff nesnesi işlemin başlangıç zamanında Start() fonksiyonu ile başlatılıp işlemin bitiş zamanında Stop() fonksiyonu ile sonlandırılarak aradaki zaman farkı mili saniye cinsinden Elapsed time olarak belirlendi.



Şekil 3.6: Okunan DICOM AES ile şifrenmiş etiket gösterimi.

Bu çalışmada; DICOM verisini okumak ve hastane içerisinde paylaşımını sağlamak için yazılmış lisanslı Görüntü Saklama ve İletişim Sistemleri (GSİS) yazılımları DICOM üzerinde performansı etkileyecek farklı parametreler ve uygulamalar kullandığı için Açık kaynak kodlu (Open Source) bir yazılım tercih edilmiştir.

Performans kıyaslaması yapabilmek için işlem zamanını ölçülmesi gerekmektedir. Bu yüzden System.Diagnostics.Stopwatch kütüphanesi kullanılarak oluşturulan diff nesnesi işlemin başlangıç zamanında Start() fonksiyonu ile başlatılıp işlemin bitiş zamanında Stop() fonksiyonu ile sonlandırılarak aradaki zaman farkı mili saniye cinsinden Elapsed time olarak belirlendi.

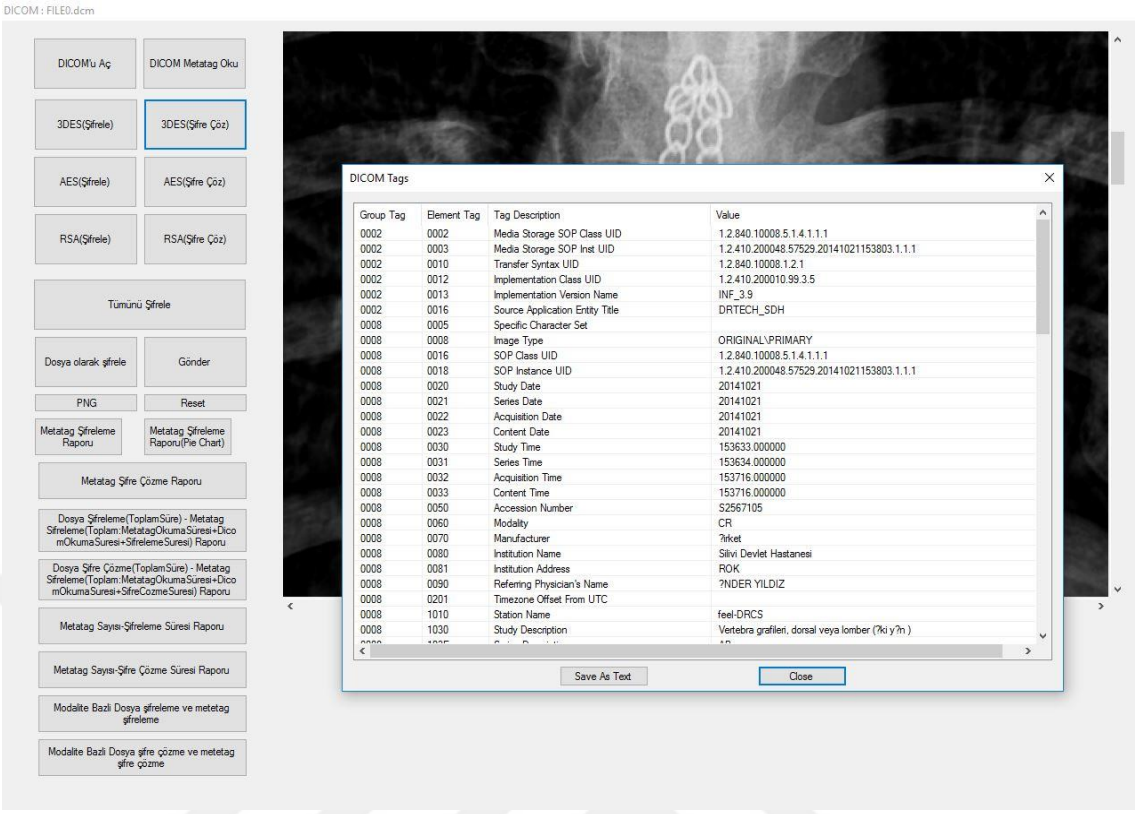
3.4. ETİKETLERİ ŞİFRELİ DICOM ŞİFRESİNİ ÇÖZME İŞLEMLERİ

Bu çalışmada belirtilen 3.3.1 ve 3.3.2 maddelerindeki yöntemlerle DICOM verisi ve etiketleri publicList<string>dicomInfo objesine atıldı.

3.4.1. DICOM etiketlerinin 3DES İle Şifre Çözme İşlemi

Okunan ve metinlerden oluşan bir listede tutulan DICOM etiketlerinin değeri, anahtar değeri “NYYObMInlTtentKODigMiSE/NSp/4JQv” ve başlangıç vektör değeri “PenS8UCVF7s=” ile 3DES şifre çözme ile bir döngü içinde şifre çözme işlemi ile DICOM’a kaydedildi ve Şekil 3.7’de görüldüğü gibi ekrana yazdırıldı.

Performans kıyaslaması yapabilmek için işlem zamanını ölçülmesi gerekmektedir. Bu yüzden System.Diagnostics.Stopwatch kütüphanesi kullanılarak oluşturulan diff nesnesi işlemin başlangıç zamanında Start() fonksiyonu ile başlatılıp işlemin bitiş zamanında Stop() fonksiyonu ile sonlandırılarak aradaki zaman farkı mili saniye cinsinden Elapsed time olarak belirlendi.



Şekil 3.7: Okunan DICOM 3DES ile şifresi çözülmüş etiket gösterimi.

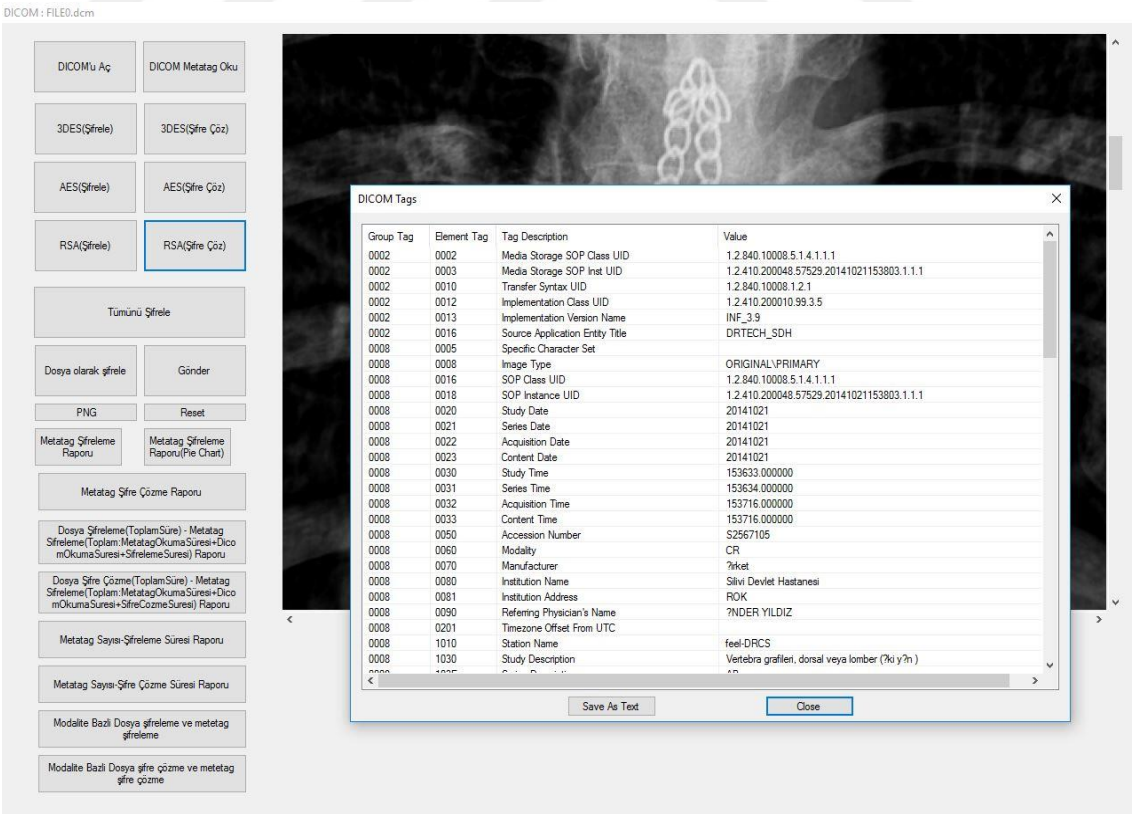
3.4.2. DICOM etiketlerini RSA İle Şifre Çözme İşlemi

Okunan ve metinlerden oluşan bir listede tutulan DICOM etiketlerin Değeri, .net kütüphanesinde bulunan RSACryptoServiceProvider sınıfından türetilen ve RSA şifre çözme için üretilen parametrelerle RSA ile bir döngü içinde şifre çözme işlemi (Decryption) ile DICOM'a kaydedilerek, Şekil 3.9'da görüldüğü gibi ekrana yazdırıldı. RSA için aşağıdaki Şekil 3.8 deki gizli anahtar kullanılmıştır.

"<RSAKeyValue><Modulus>21wEnTU+mcD2w0Lfo1Gv4rtcSWsQJQTNa6gio05AOkV/Er
9w3Y13Ddo5wGtjJ19402S71HUeN0vbKILLJdRSES5MHSdJPSVrOqdrll/vLXxDxWs/U0U
T1c8u6k/Ogx9hTtZxYwoeYqdhDblof3E75d9n2F0Zvf6iTb4cI7j6fMs=</Modulus><Expone
nt>AQAB</Exponent><P>/aULPE6jd5IkwtWXmReyMUhmI/nfwfkQSyl7tsg2PKdpcxk4mp
PZUdEQhHQLvE84w2DhTyYkPHCtq/mMKE3MHw==</P><Q>3WV46X9Arg2l9cxb67K
VlNVXyCqc/w+LWt/tbhLJvV2xCF/0rWKPsBJ9MC6cquaqNPxWWEav8RAVbmmGrJt51Q
==</Q><DP>8TuZFgBMpBoQcGUoS2goB4st6aVq1FcG0hVgHhUI0GMAfYFNPmbDV3c
Y2IBt8Oj/uYJYhyhlaj5YTqmGTYbATQ==</DP><DQ>FIoVbZQgrAUYIHWVEYi/187zFd
7eMct/Yi7kGBImJStMATrluDAspGkStCWe4zwDDmdam1XzfKnBUzz3AYxrAQ==</DQ>
<InverseQ>QPU3Tmt8nznSgYZ+5jUo9E0SfjiTu435ihANiHqqjasaUNvOHKumqzuBZ8NRt
kUhS6dsOEb8A2ODvy7KswUxyA==</InverseQ><D>cgoRoAUpSVfHMdYXW9nA3dfX7
5dIamZnwPtFHq80ttagbIe4ToYYCcyUz5NElhiNQSESgS5uCgNWqWXt5PnPu4XmCXx6ut
co1UVH8HGLahzbAnSy6Cj3iUIQ7Gj+9gQ7PkC434HTtHazmxVgIR5156ZjoQ8yGNCPZns
dYEmhJWk=</D></RSAKeyValue>";

Şekil 3.8: RSA gizli anahtar.

Performans kıyaslaması yapabilmek için işlem zamanını ölçülmesi gerekmektedir. Bu yüzden System.Diagnostics.Stopwatch kütüphanesi kullanılarak oluşturulan diff nesnesi işlemin başlangıç zamanında Start() fonksiyonu ile başlatılıp işlemin bitiş zamanında Stop() fonksiyonu ile sonlandırılarak aradaki zaman farkı mili saniye cinsinden Elapsed time olarak belirlendi.



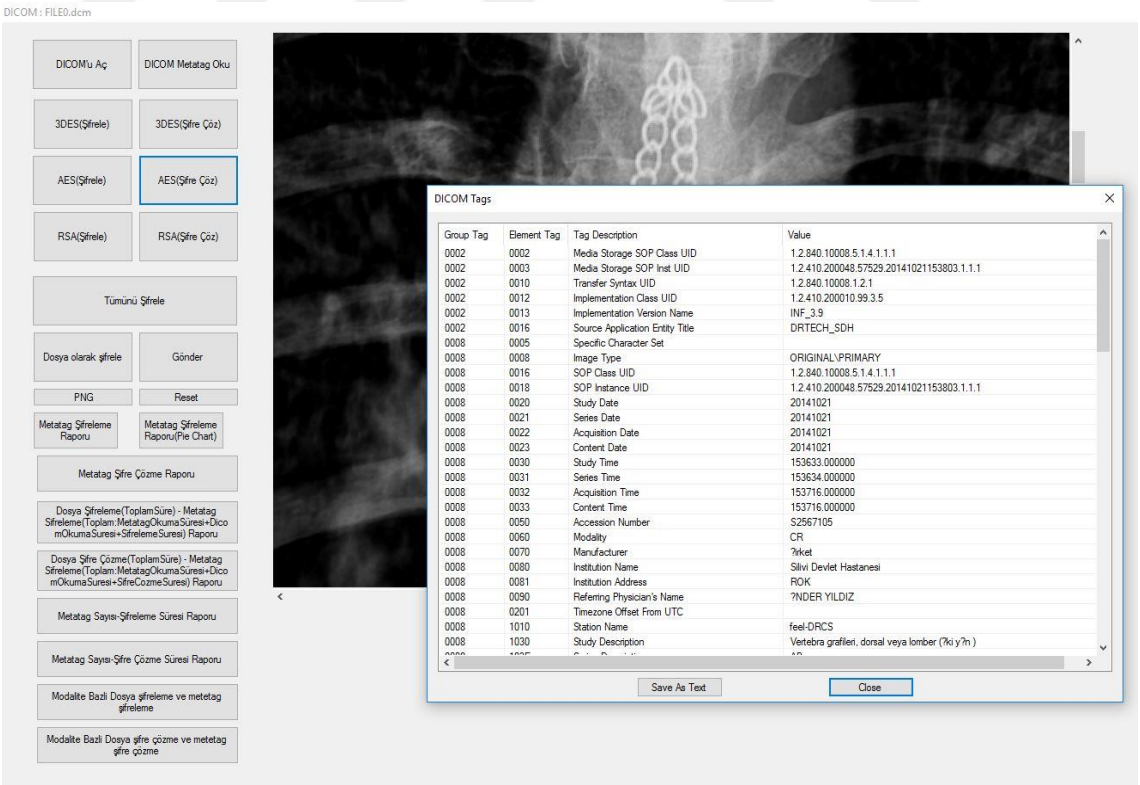
Şekil 3.9: Okunan DICOM RSA ile şifresi çözülmüş etiket gösterimi.

3.4.3. DICOM etiketlerini AES İle Şifre Çözme İşlemi

Okunan ve metinlerden oluşan bir listede tutulan DICOM etiketleri,

- Anahtar“12345678” ,
- Hash Algoritması SHA1,
- Başlangıç vektorü“OFRna73m*aze01xY”,
- Şifre tekrarlanması 2 (key iteration),
- Anahtar size 256 bit
- Salt Kosher değerleri kullanılarak AES ile bir döngü içinde şifre çözme işlemi ile DICOM’a kaydedildi ve Şekil 3.10’de görüldüğü gibi ekrana yazdırıldı.

Performans kıyaslaması yapabilmek için işlem zamanını ölçülmesi gerekmektedir. Bu yüzden System.Diagnostics.Stopwatch kütüphanesi kullanılarak oluşturulan diff nesnesi işlemin başlangıç zamanında Start() fonksiyonu ile başlatılıp işlemin bitiş zamanında Stop() fonksiyonu ile sonlandırılarak aradaki zaman farkı mili saniye cinsinden Elapsed time olarak belirlendi.



Şekil 3.10: Okunan DICOM AES ile şifresi çözülmüş etiket gösterimi.

3.5. DICOM VERİSİNİN BİR DOSYA OLARAK ETİKETLERİNİ AYIRMADAN ŞİFRELEME YÖNTEMİ

3.5.1. DICOM'u Dosya Olarak Şifreleme İşlemi

Nathan Blomquist (link: https://www.codeproject.com/Articles/8633/File-Encryption-Decryption-with-Hash-Verification, 2004) belirtilen yöntemlerle dosya bazlı şifreleme yapılmıştır.

Burada esas olarak .net Framework'unun System.Security.Cryptography kütüphanesi kullanılmıştır.

Dosya öncelikli olarak byte stream haline çevrildi. Sonra IV and Salt değerler rastgele olarak byte stream halinde belirlendi. Belirlenen şifre ve Salt değerleri sma.KeySize = 256 sma.Key = pdb.GetBytes(32); sma.Padding = PaddingMode.PKCS7 değerleri ve AES (Rijndael) algoritması ile türetilerek Filestream olarak alınan dosyanın başından itibaren yazıldı.

SHA256 ile hashing bir stream oluşturulduktan sonra oluşturulan Filesteram'deki dosyanın en sonuna eklenerek belirlenen uzantıda belirlenen konuma kaydedildi.

3.5.2. Şifrelenmiş DICOM'u Dosya Olarak Şifre Çözme İşlemi

Şifrelenmiş dosyadaki IV and Salt değerleri ve hash'lenmiş Hashing stream ile kıyaslanıp eğer değerler eşitse belirlenen password ve salt değerleri sma. Key Size = 256 sma. Key = pdb.GetBytes(32); sma.Padding = Padding Mode.PKCS7 değerleri ve AES (Rijndael) algoritması ile dosya şifre çözmeye başlandı. Şifresi çözülmüş halde byte stream olarak belirlenen stream belirlenen konuma dcm formatında kaydedildi.

4. BULGULAR

Bu çalışmada; mevcut yapıların güvenliğini performansı etkilemeyecek şekilde geliştirme yapılabilmesi için yazılmış program verilerinin analizi incelenmektedir.

Test amaçlı 95 adet CR (Computed Radiography), CT (Computed Tomography), DX (Dijital Radiography), EK (Electrocardiography), IO (Intra-oral Radiography), MR (Magnetic Resonance), US (Ultrasound), MG (Mammography) ve OT (Other Modality - retired) DICOM verilerinin sırasıyla; DICOM okunma süreleri, DICOM etiket okuma süreleri, etiketlerin 3DES şifreleme süreleri, etiketlerin AES şifreleme süreleri, etiketlerin RSA şifreleme süreleri, Ham DICOM verisini dosya olarak şifreleme süreleri, AES, RSA ve 3DES şifrelerinin çözme süreleri, Dosya olarak şifrelenmiş DICOM şifre çözme süreleri tablolar halinde verilmiş ve analiz sonuçları bu kısımda listelenmiştir.

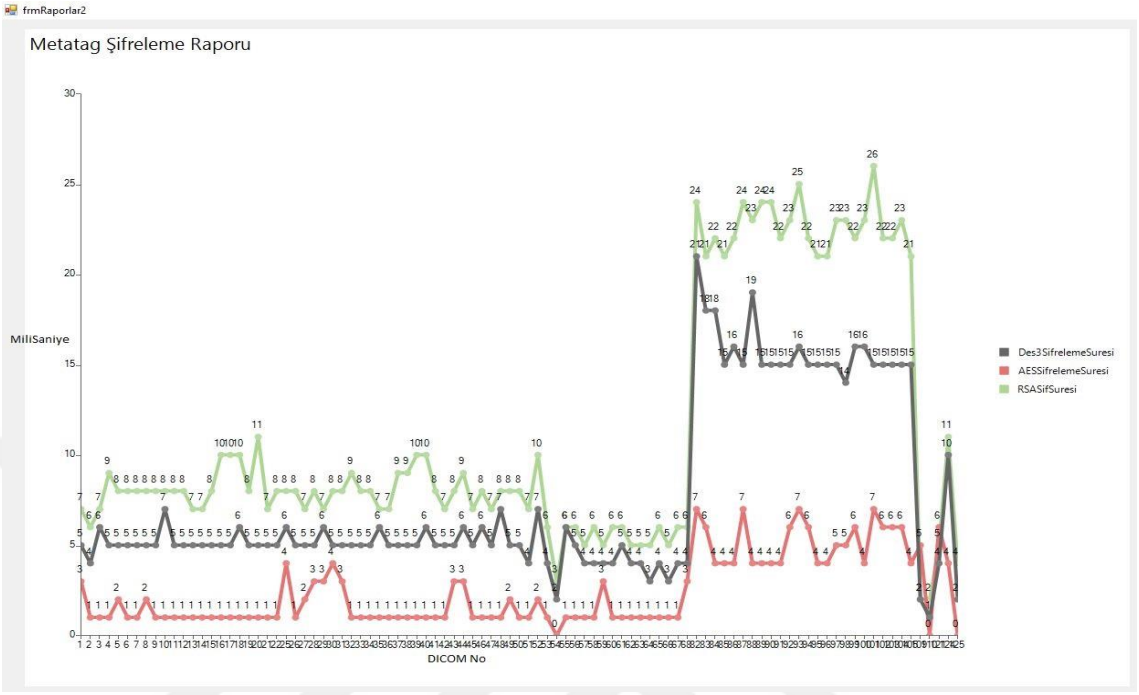
4.1. SADECE ETİKET ŞİFRELEME SÜRELERİ ANALİZLERİ

Test amaçlı 95 adet DICOM verisi için etiketlerin şifreleme süreleri analiz raporu Şekil 4.1 de belirtilmiştir. İlgili analiz raporu iki aşamada incelendiğinde; ilk 68 test DICOM'un süreleri (Şekil 4.2) AES ile etiketlerin şifrelemesi için ortalama 1 milisaniye, 3DES ile etiketlerin şifrelemesi için ortalama 5 milisaniye ve RSA ile etiketlerin şifrelemesi için ortalama 8 milisaniye olarak görülmektedir.

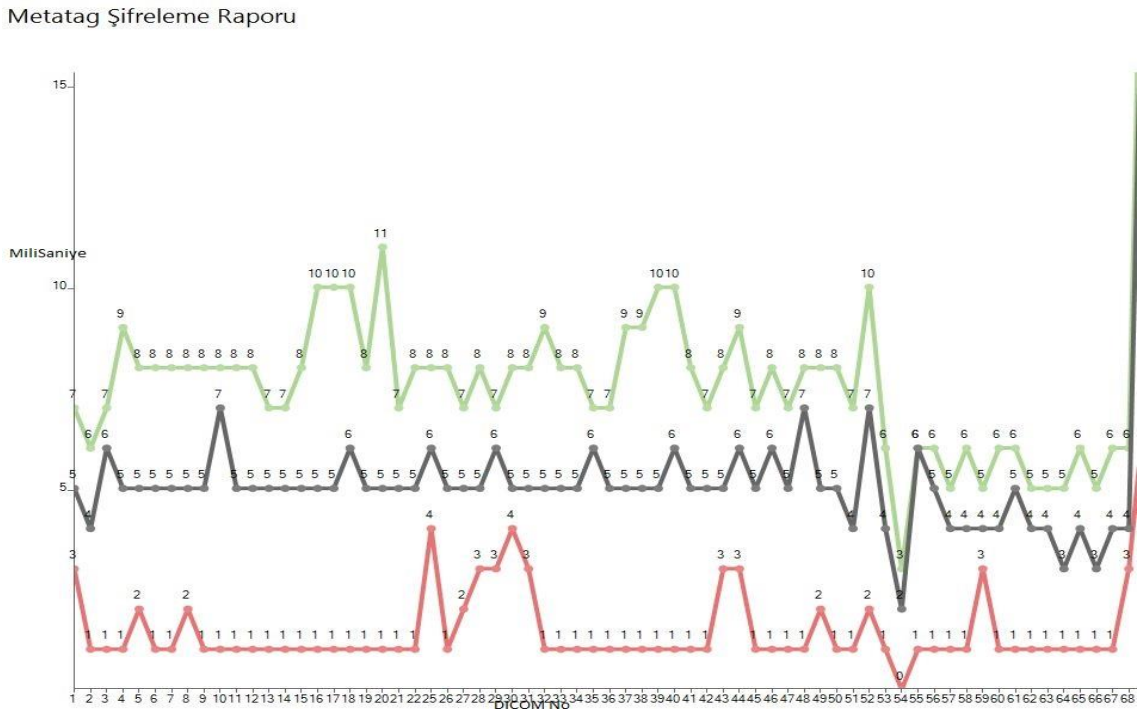
3DES ile etiketlerin şifrelemesi RSA ile etiketlerin şifrelemesi ile kıyaslandığında milisaniye cinsinden küçük bir fark görülmektedir. Ancak AES ile etiketlerin şifrelemesinin; 3DES ile etiketlerin şifreleme ve RSA ile etiketlerin şifreleme yöntemlerinden belirgin farkla kısa sürelerde şifrelendiği görülmektedir.

Test verilerinde Şekil 4.3 68. DICOM'dan sonraki AES ile etiketlerin şifrelemesi için ortalama 5 milisaniye, 3DES ile etiketlerin şifrelemesi için ortalama 15 milisaniye ve RSA ile etiketlerin şifrelemesi için ortalama 22 milisaniye olarak görülmektedir. Süreler

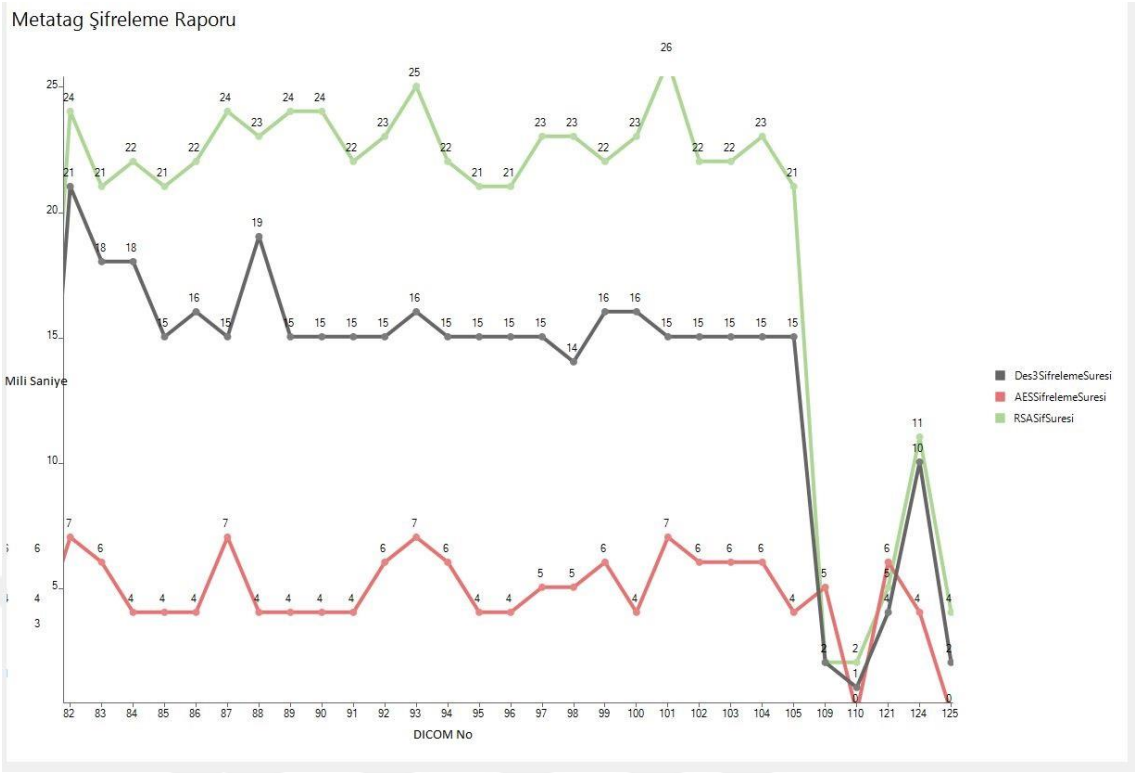
artmasına rağmen şifreleme yöntemlerini kıyaslarsak ilk 68 veri ile benzer sonuçlar gözlemlenmektedir.



Şekil 4.1: Etiket şifreleme grafiği (milisaniye).



Şekil 4.2: Etiket şifreleme grafiği (68. dicom'a kadar).



Şekil 4.3: Etiket şifreleme grafiği (68-125 Arası DICOM).

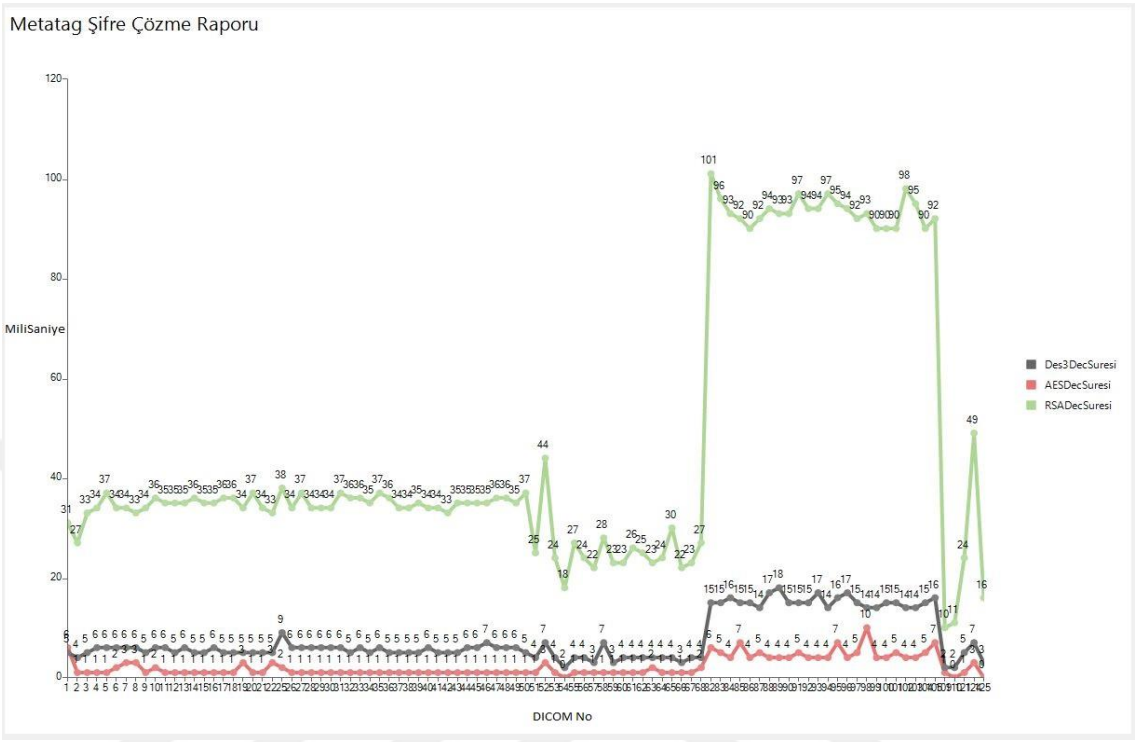
4.2. SADECE ETİKET ŞİFRE ÇÖZME ANALİZİ

Test amaçlı 95 adet DICOM verisi için etiketlerin şifre çözme süreleri analiz raporu Şekil 4.4 de belirtilmiştir. İlgili analiz raporu 2 aşamada inceleyebiliriz. İlk 68 test DICOM'un süreleri (Şekil 4.5) AES ile etiketlerin şifre çözme için ortalama 1 milisaniye, 3DES ile etiketlerin şifre çözme için ortalama 5 milisaniye ve RSA ile etiketlerin şifre çözme için ortalama 33 milisaniye olarak görülmektedir. Şifrelemeden farklı olarak AES ve 3DES şifre çözmenin değerleri benzerlik gösterirken; RSA şifre çözme süresinin arttığı görülmektedir.

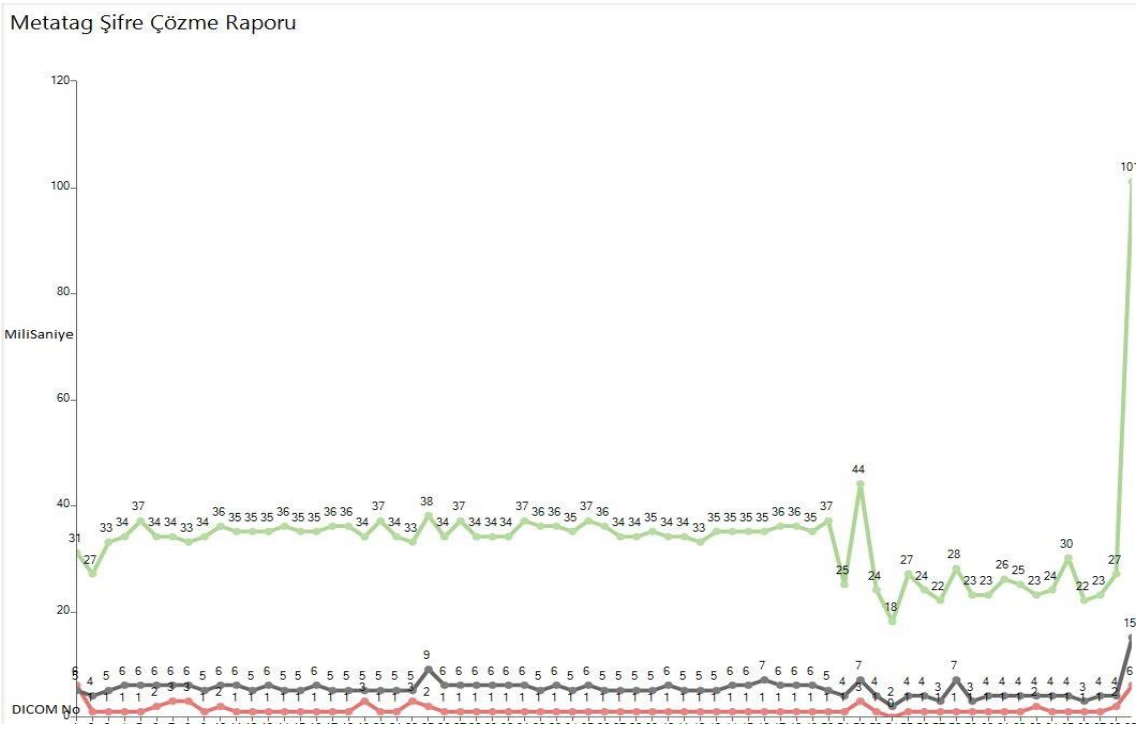
Şifrelemenin aksine 3DES ile etiketlerin şifre çözme RSA ile etiketlerin şifre çözme ile kıyaslandığında milisaniye cinsinden farkın belirgin olduğu görülmektedir.

AES ile etiketlerin şifre çözme işleminin; 3DES ile etiketlerin şifre çözme ve RSA ile etiketlerin şifre çözme yöntemlerinden belirgin sürelerdeki farkla şifre çözme yaptığı görülmektedir. AES ile etiketlerin şifre çözme daha kısa sürede şifre çözdüğü gözlemlenmiştir.

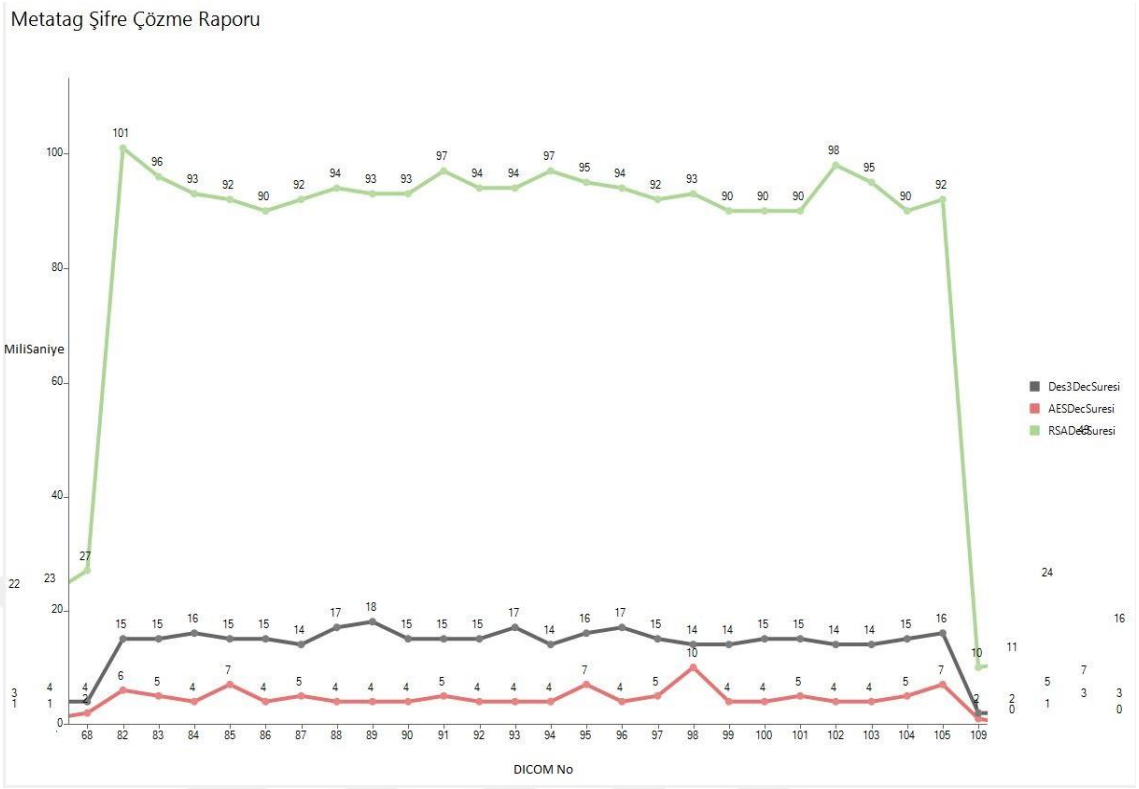
Test verilerinde Şekil 4.6'daki 68. DICOM'dan sonraki süreler artmasına rağmen şifre çözme yöntemlerini kıyaslarsak ilk 68 veri ile benzer sonuçlar gözlemlenmektedir.



Şekil 4.4: Etiket şifre çözme grafiği.



Şekil 4.5: Etiket şifre çözme grafiği (ilk 68 DICOM'akadar).



Şekil 4.6: Etiket şifre çözme grafiği (68– 109 DICOM'a kadar).

4.3. GENEL ŞİFRELEME ANALİZİ DOSYA ŞİFRELEME VE ETİKET ŞİFRELEME RAPORU

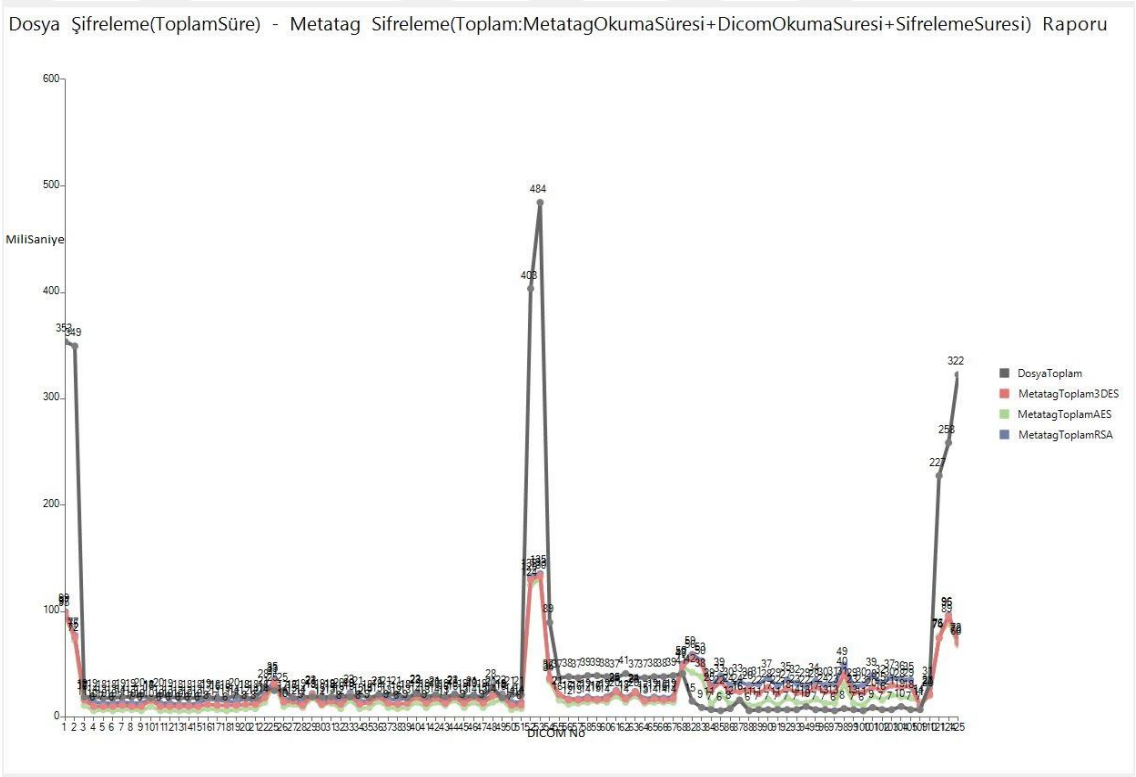
DICOM şifreleme yöntemlerinden dosya olarak şifrelemede DICOM'u okuma ve etiketlerin okuma süreleri olmadığından doğrudan dosya şifreleme süresi alınmıştır. Etiket şifrelemede (3DES, AES, RSA) ise; DICOM'u şifrelemek için toplam harcanan süre DICOM Okuma Süresi, Etiket Okuma Süresi ve Şifreleme sürelerinin toplamından oluşmaktadır.

Şekil 4.7 de Dosya Şifreleme(Toplam Geçen Süre–milisaniye) ve Etiket Şifreleme (Toplam: Etiket Okuma Süresi + Dicom Okuma Süresi + Şifreleme Süresi) genel raporu gösterilmiştir.

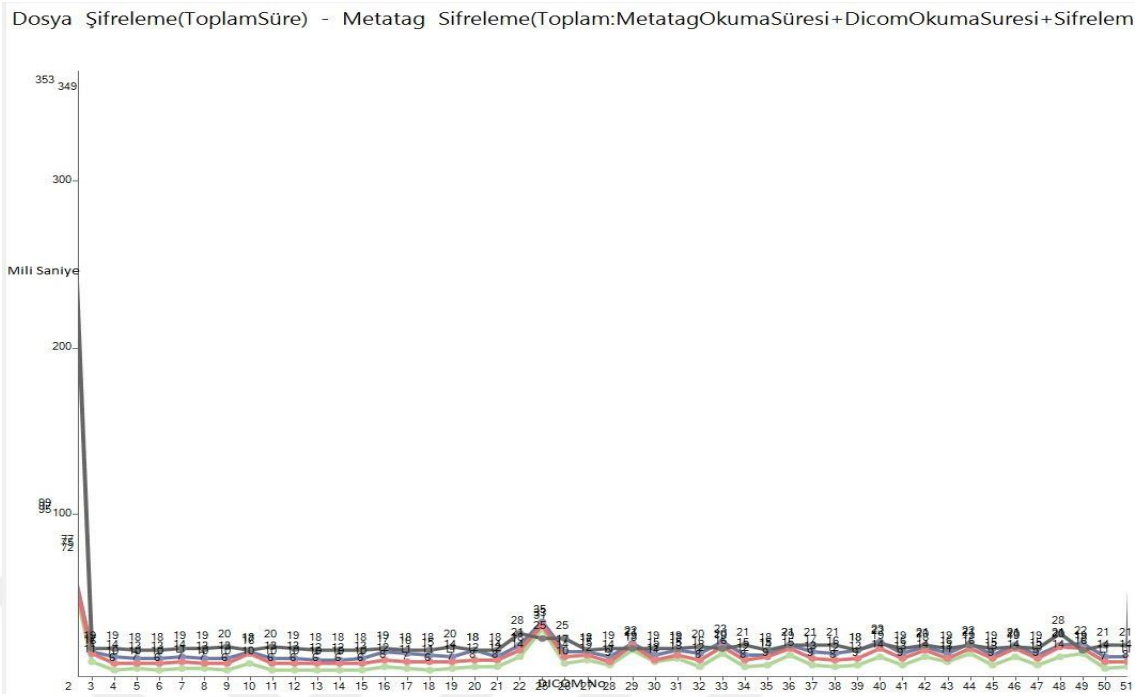
Şekil 4.7 incelendiğinde; 1, 2, 3 ve 52, 53 numaralı verilerde dosyalama süresinin ciddi farkla Etiket şifrelemeden daha uzun sürdüğü gözlemlenmektedir. Bu veriler incelendiğinde CR ve DX modalitelerinin olduğu görülmüştür. Modalite bazlı şifreleme ve şifre çözme grafiğinde ayrıntılı incelenmiştir.

Ancak Şekil 4.8'deki 3–51 arasındaki verilerde; AES Etiket şifreleme ile toplam süre; diğer Etiket şifreleme yöntemlerinde harcanan toplam süre ve Dosya olarak şifreleme ile harcanan süreye kıyaslandığında; AES ile Etiket şifreleme yönteminin daha kısa sürede şifrelediği gözlemlenmiştir. Dosya olarak şifreleme genel olarak Etiket şifreleme yöntemlerine göre daha yavaş olduğu görülmektedir.

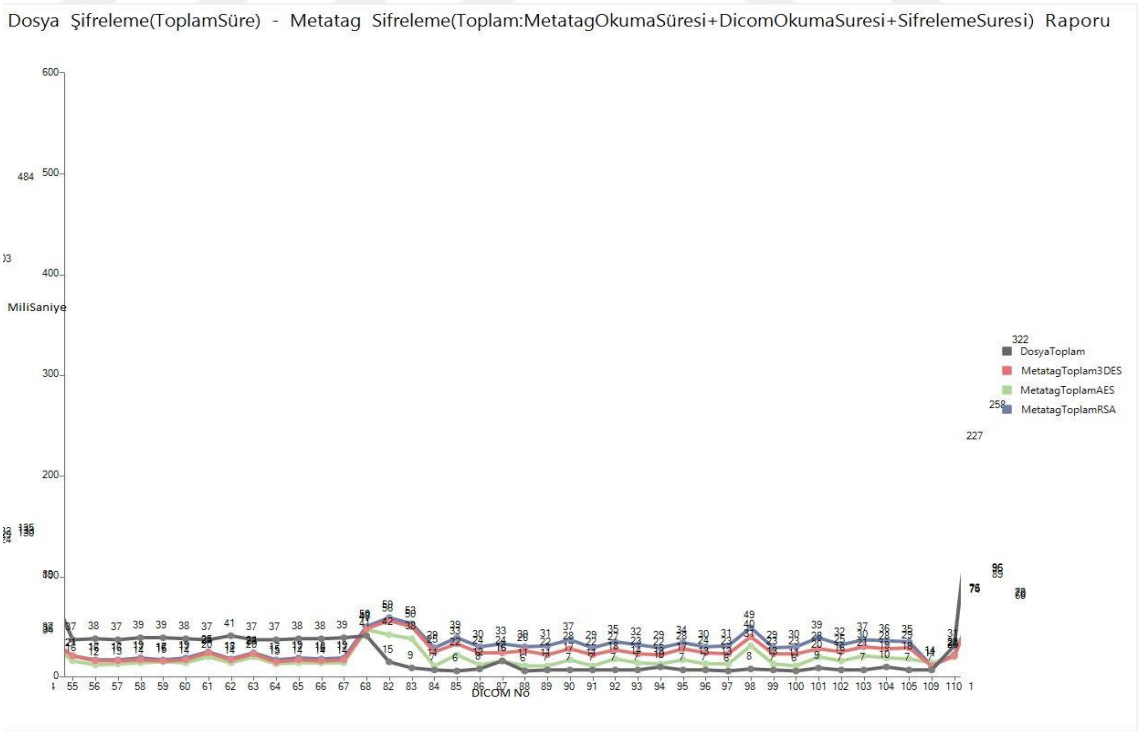
Ancak Şekil 4.9 incelendiğinde; 68. veriye kadar Şekil 4.8 deki grafiğe benzer grafik görülmektedir. 82'den 110 numaralı DICOM'a kadar grafikteki genel yapının aksine dosya şifreleme süreleri diğer tüm şifreleme yöntemlerine göre daha hızlı sürelerde şifrelediği gözlemlenmiştir. 82 ve 110 arasındaki verilerin MR, US verilerinden oluştuğu görülmüştür. Modalite bazlı şifreleme ve şifre çözme grafiğinde ayrıntılı incelenmiştir.



Şekil 4.7: Dosya şifreleme (toplam geçen süre - milisaniye) ve Etiket şifreleme (toplam: Etiket okuma süresi + dicom okuma süresi + şifreleme süresi) genel raporu.



Şekil 4.8: Dosya şifreleme (toplam geçen süre - milisaniye) ve Etiket şifreleme (toplam: Etiket okuma süresi + dicom okuma süresi + şifreleme süresi) 3–51 arasındaki veriler.



Şekil 4.9: 55'den 110 numaralı DICOM'a kadar grafik.

4.4. GENEL ŞİFRE ÇÖZME ANALİZİ DOSYA ŞİFRE ÇÖZME VE ETİKETŞİFRE RAPORU

DICOM şifre çözme yöntemlerinden dosya olarak şifre çözmede; DICOM'u okuma ve etiketlerin okuma süreleri olmadığından, doğrudan dosya şifre çözme süresi alınmıştır. Etiket şifre çözme (3DES, AES, RSA) ise; DICOM'u şifrelemek için toplam harcanan süre DICOM okuma suresi, Etiket okuma süresi ve şifre çözme sürelerinin toplamından oluşmaktadır.

Şekil 4.10'da dosya şifre çözme (toplam geçen süre-milisaniye) ve Etiket şifre çözme (toplam: Etiket okuma süresi + dicom okuma süresi + şifre çözme süresi) genel raporu gösterilmiştir.

Şekil 4.11 incelendiğinde; 1, 2, 3 ve 52, 53 numaralı verilerde dosyalama süresinin ciddi farkla Etiket şifre çözmeden daha uzun sürdüğü gözlemlenmektedir. Bu veriler incelendiğinde CR ve DX modalitelerinin olduğu görülmüştür. Modalite bazlı şifreleme ve şifre çözme grafiğinde ayrıntılı incelenmiştir.

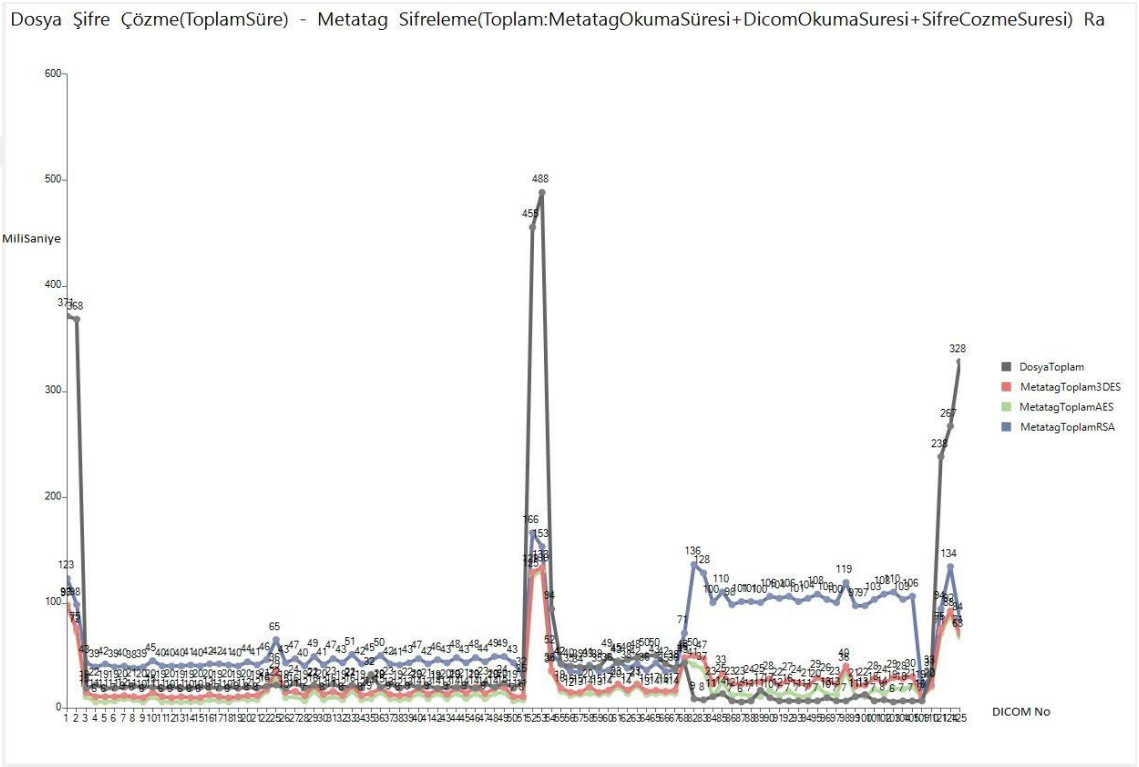
Ancak Şekil 4.11'deki 3-51 arasındaki verilerde; AES Etiket şifreleme ile toplam süre diğer Etiket şifreleme yöntemlerinde harcanan toplam süre ve Dosya olarak şifreleme ile harcanan süreye kıyaslandığında; AES ile Etiket şifreleme yönteminin daha kısa sürede şifrelediği gözlemlenmiştir.

Şifrelemenin aksine 3-51 arasındaki verilerde; Dosya olarak şifre çözme, AES ve 3DES şifrelemeden daha yavaş görülmekte ancak RSA şifre çözmeden daha hızlı olduğu görülmektedir.

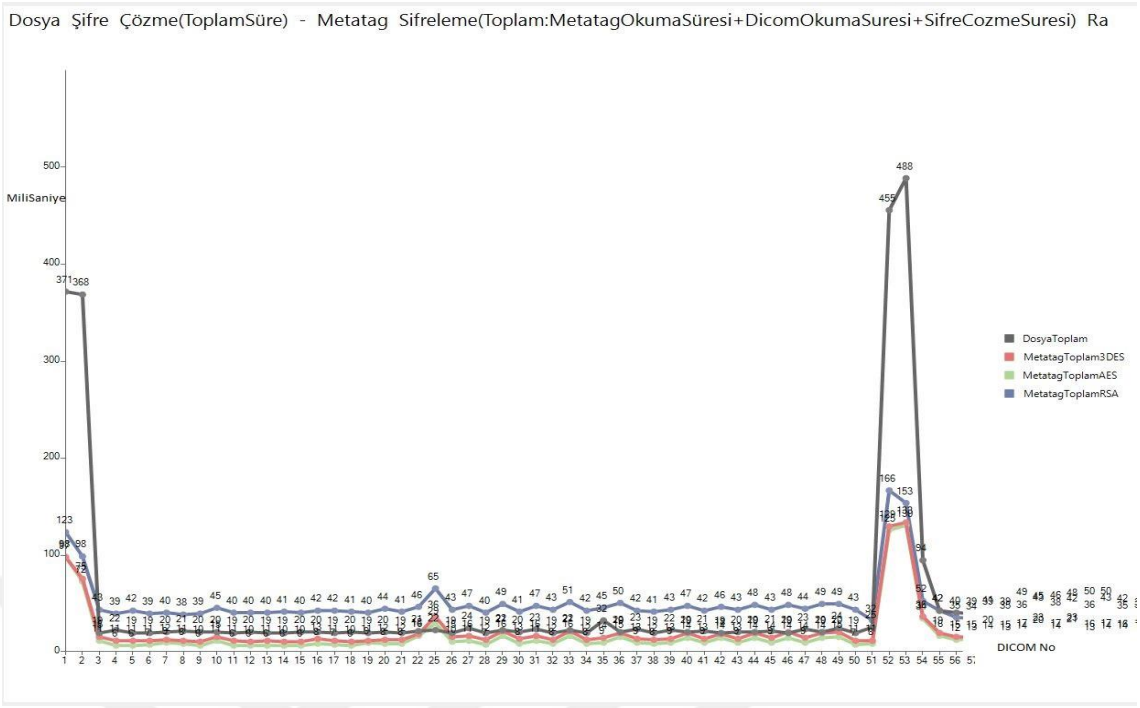
Ancak Şekil 4.12 incelendiğinde; 54-68. veriye kadar verilerde 3DES ve AES ile Etiket şifre çözme performansları Şekil 4.11'deki grafiğe benzer olmasına rağmen; RSA şifre çözme dosya şifre çözmeden Şekil 4.11'e göre daha hızlı olduğu görülmektedir.

Şekil 4.13'te 68 nolu DICOM'dan 110 numaralı DICOM'a kadar grafikteki genel yapının aksine dosya şifre çözme süreleri diğer tüm şifreleme yöntemlerine göre daha hızlı sürelerde şifre çözdüğü gözlemlenmiştir. 82 ve 110 arasındaki verilerin MR, US verilerinden oluştuğu görülmüştür. Modalite bazlı şifreleme ve şifre çözme grafiğinde ayrıntılı incelenmiştir.

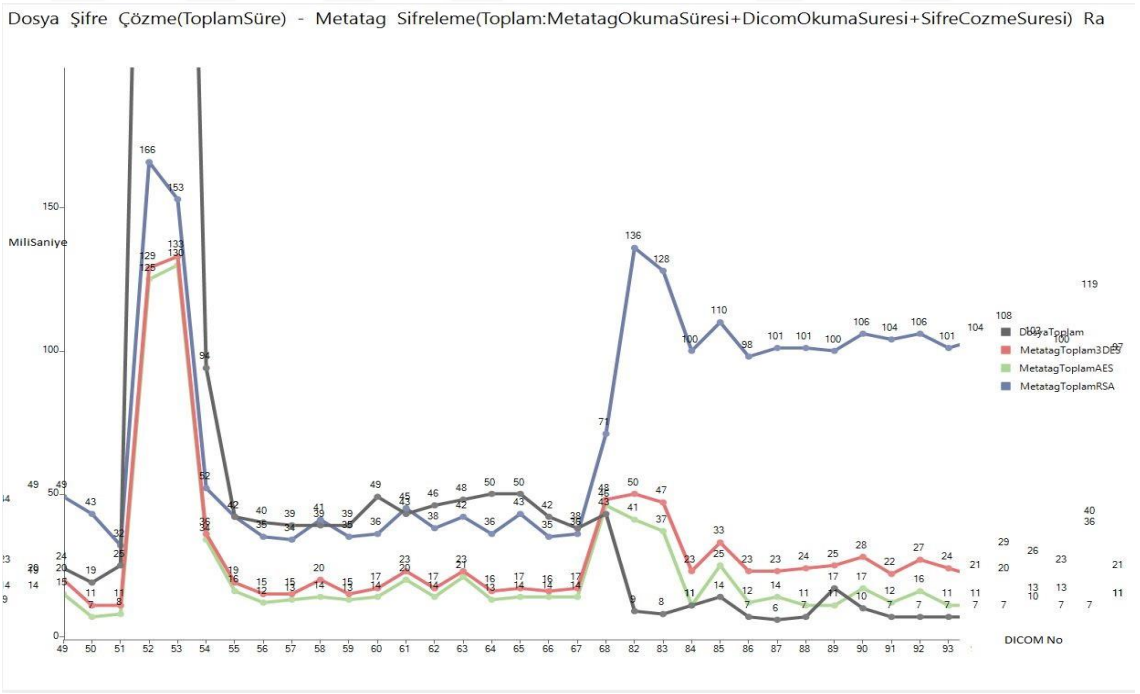
Şekil 4.14'te ise 121 numaralı DICOM'dan 125 numaralı DICOM verisine kadar veriler incelendiğinde 1, 2, 3 ve 52, 53 numaralı verilerdeki benzer grafiğin oluştuğu ve dosyalama süresinin ciddi farkla etiket şifre çözmeden daha uzun sürdüğü gözlemlenmektedir. İlgili verilerin modaliteleri CR, MG, OT gibi birbirine benzer modaliteler olduğu gözlemlenmiştir. Modalite bazlı şifreleme ve şifre çözme grafiğinde ayrıntılı incelenmiştir.



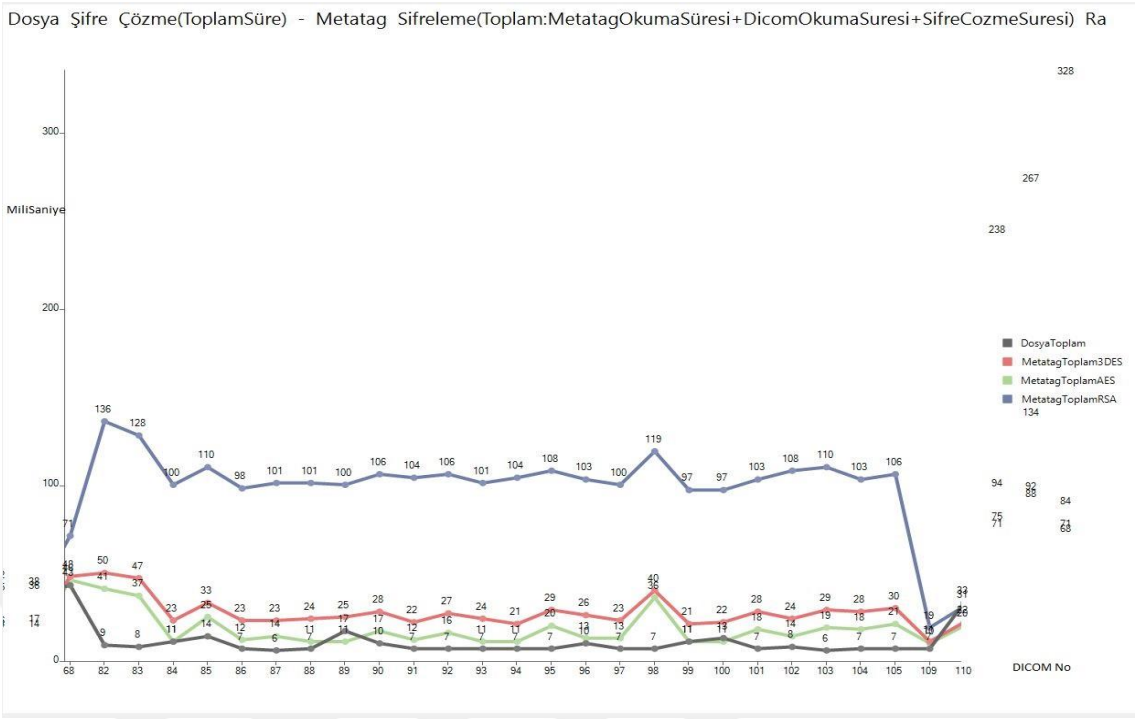
Şekil 4.10: Dosya şifre çözme (toplam geçen süre - milisaniye) ve Etiket şifre çözme (toplam: Etiket okuma süresi + dicom okuma süresi + şifre çözme süresi) genel grafik.



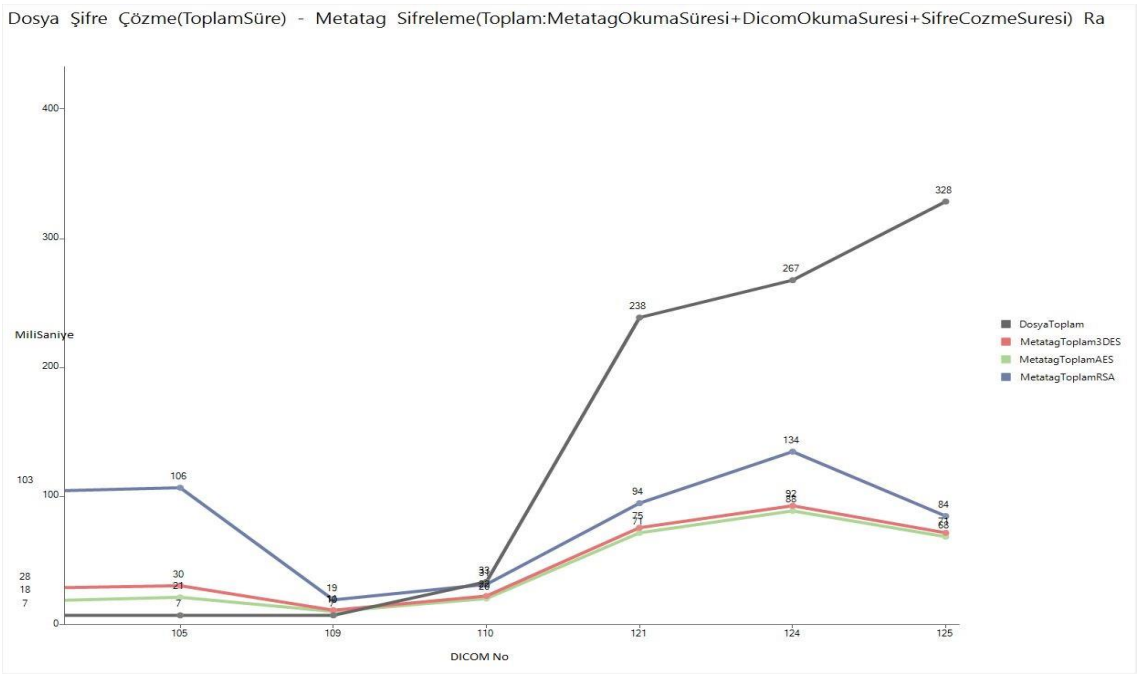
Şekil 4.11: Dosya şifre çözme (toplam geçen süre - milisaniye) ve Etiket şifre çözme (toplam: Etiket okuma süresi + dicom okuma süresi + şifre çözme süresi) 3–51 arası.



Şekil 4.12: Dosya şifre çözme (toplam geçen süre - milisaniye) ve Etiket şifre çözme (toplam: Etiket okuma süresi + dicom okuma süresi + şifre çözme süresi) 53–93 arası.



Şekil 4.13: Dosya şifre çözme (toplam geçen süre - milisaniye) ve Etiket şifre çözme (toplam: Etiket okuma süresi + dicom okuma süresi + şifre çözme süresi) 68–109 arası.



Şekil 4.14: Dosya şifre çözme (toplam geçen süre - milisaniye) ve Etiket şifre çözme (toplam: Etiket okuma süresi + dicom okuma süresi + şifre çözme süresi) 109–125.

4.5. ETİKET ŞİFRELEMEYİ OLUŞTURAN ETKENLERİN ANALİZİ

Bu çalışmada; dosya olarak şifrelemeye alternatif olarak önerilen etiketlerin şifrelenmesi metodunda toplam süreye Etiket okuma süresi, DICOM okuma suresi, şifreleme surelerinin etkilerinin belirlenmesi için Pasta (Pie Chart) grafiği yöntemi ile tüm Test verilerinin ortalama değerleri alınarak gösterimi sağlanmıştır.

3DES şifreleme yönteminin toplam süre üzerindeki etki grafiği Şekil 4.15'te, AES şifreleme yönteminin toplam süre üzerindeki etki grafiği Şekil 4.16'da, RSA şifreleme yönteminin toplam süre üzerindeki etki grafiği Şekil 4.17'de gösterilmiştir.

Şekil 4.15'te görüldüğü gibi; 3DES ile şifreleme yönteminde DICOM okuma süresi %70, Etiketlerin 3DES ile şifrelenmesi %30, Etiket okunma süresi neredeyse %0'a yakın olduğundan ihmal edilebilir düzeyde çıkmıştır.

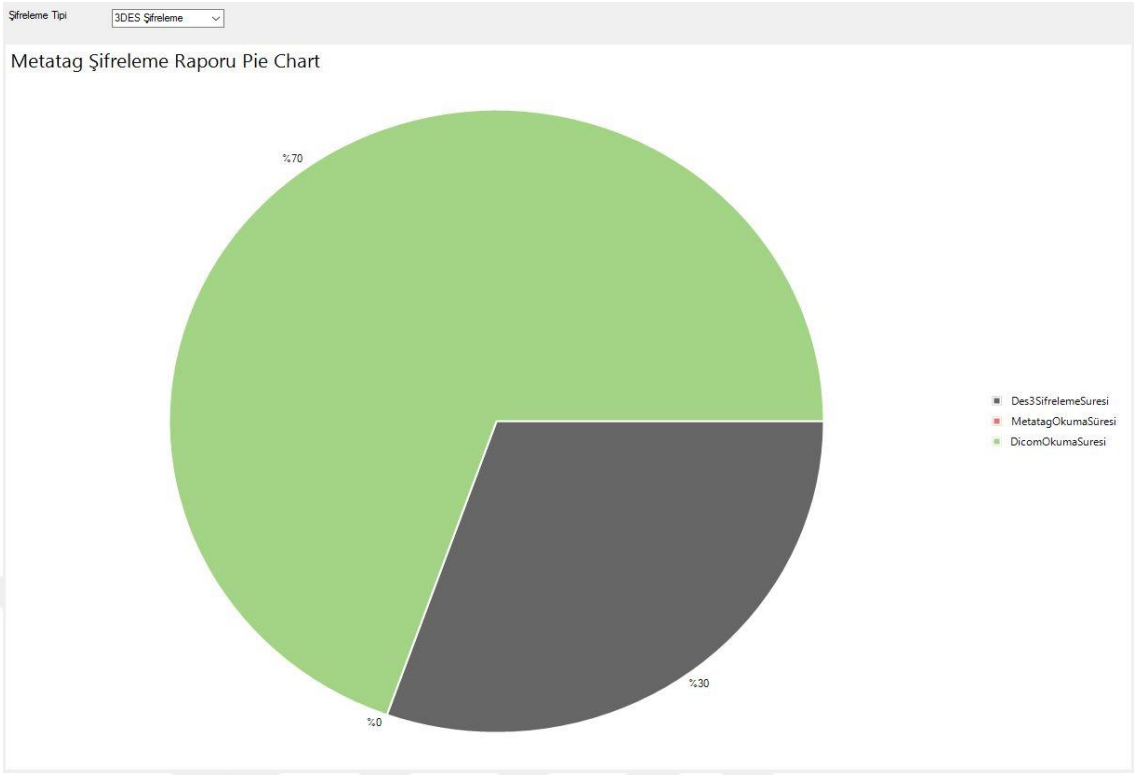
Buradan 3DES ile şifrelemenin toplam sürede DICOM okuma süresi belirleyici olmuştur.

Şekil 4.16'da görüldüğü gibi; AES ile şifreleme yönteminde DICOM okuma süresi %89, Etiketlerin AES ile şifrelenmesi %11, Etiket okunma süresi neredeyse %0'a yakın olduğundan ihmal edilebilir düzeyde çıkmıştır.

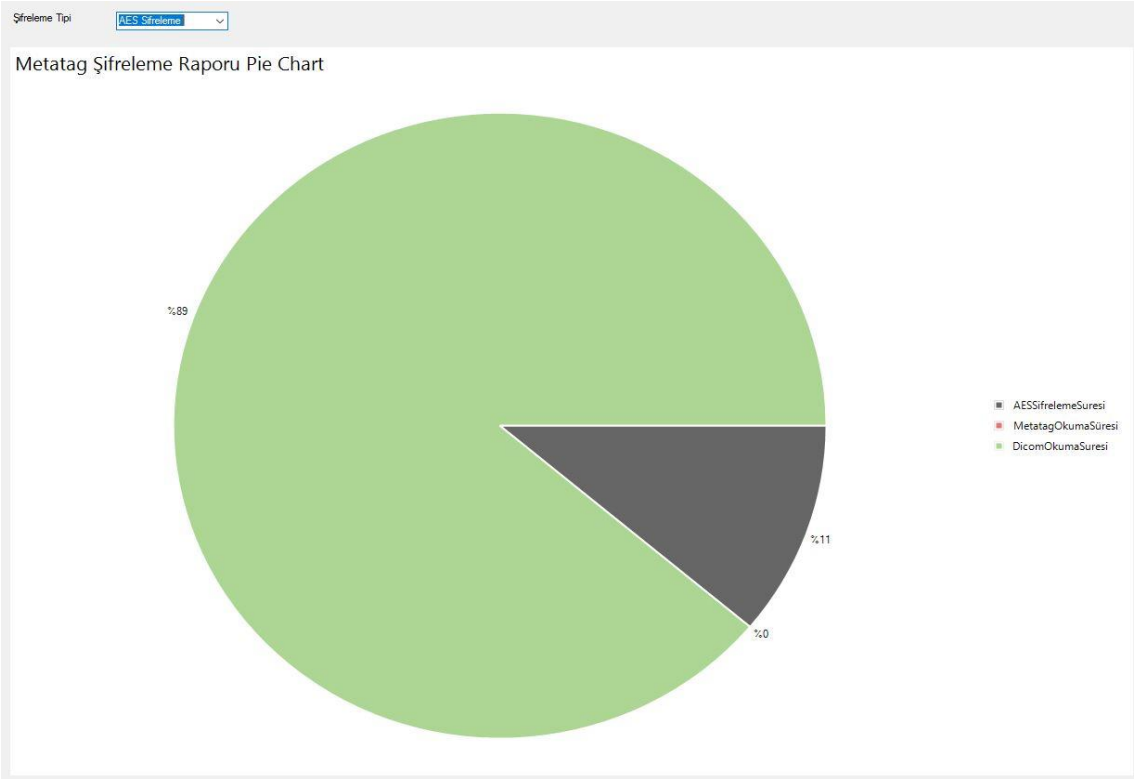
Buradan AES ile şifrelemenin toplam sürede; DICOM okuma süresi belirleyici olmuştur. AES şifreleme 3DES şifrelemeye göre daha hızlı olduğundan DICOM okuma süresinin genel toplamda yüzdelik etkisini artırdığı söylenebilir.

Şekil 4.17'de görüldüğü gibi; RSA ile şifreleme yönteminde DICOM okuma süresi %59, Etiketlerin RSA ile şifrelenmesi %41, Etiket okunma süresi neredeyse %0'a yakın olduğundan ihmal edilebilir düzeyde çıkmıştır.

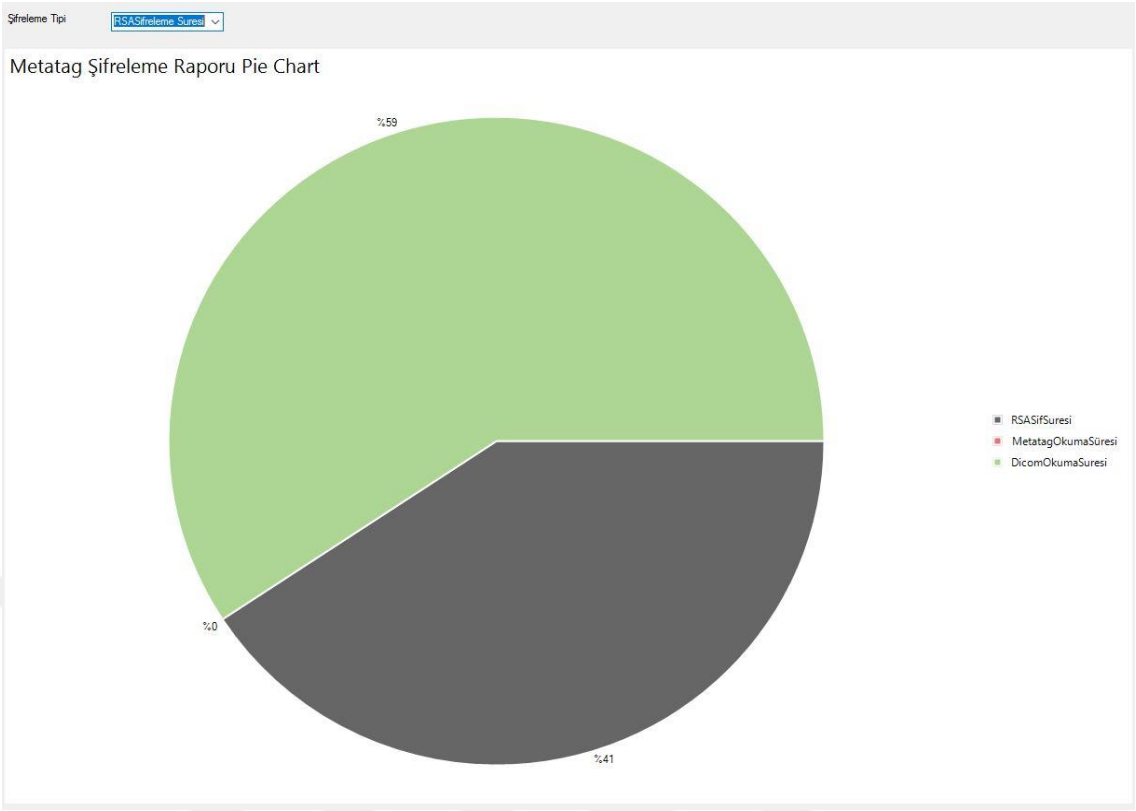
Buradan RSA ile şifrelemenin toplam sürede DICOM okuma süresi belirleyici olmuştur. RSA şifreleme 3DES,AES şifrelemeye göre daha yavaş olduğundan DICOM okuma süresinin genel toplamda yüzdelik etkisini azaltarak; DICOM okuma süresi ile ortalama yakın yüzdeliklerde olduğu gözlemlenmiştir.



Şekil 4.15: 3DES şifreleme yönteminin toplam süre üzerindeki etki grafiği.



Şekil 4.16: AES şifreleme yönteminin toplam süre üzerindeki etki grafiği.



Şekil 4.17: RSA şifreleme yönteminin toplam süre üzerindeki etki grafiği.

4.6. ETİKET ŞİFRE ÇÖZMEYİOLUŞTURAN ETKENLERİN ANALİZİ

Bu çalışmada; dosya olarak şifre çözmeye alternatif olarak önerilen etiketlerin şifre çözme metodunda toplam süreye Etiket okuma süresi, DICOM okuma suresi, şifre çözme sürelerinin etkilerinin belirlenmesi için Pasta (Pie Chart) grafiği yöntemi ile tüm test verilerinin ortalama değerleri alınarak gösterimi sağlanmıştır.

3DES ile şifre çözme yönteminin toplam süre üzerindeki etki grafiği Şekil 4.18'de, AES şifre çözme yönteminin toplam süre üzerindeki etki grafiği Şekil 4.19'da, RSA şifre çözme yönteminin toplam süre üzerindeki etki grafiği Şekil 4.20'de gösterilmiştir.

Şekil 4.18'de görüldüğü gibi; 3DES ile şifre çözme yönteminde DICOM okuma süresi %70, Etiketlerin 3DES ile şifre çözme %30, Etiketlerin okunma süresi neredeyse %0'a yakın olduğundan ihmal edilebilir düzeyde çıkmıştır.

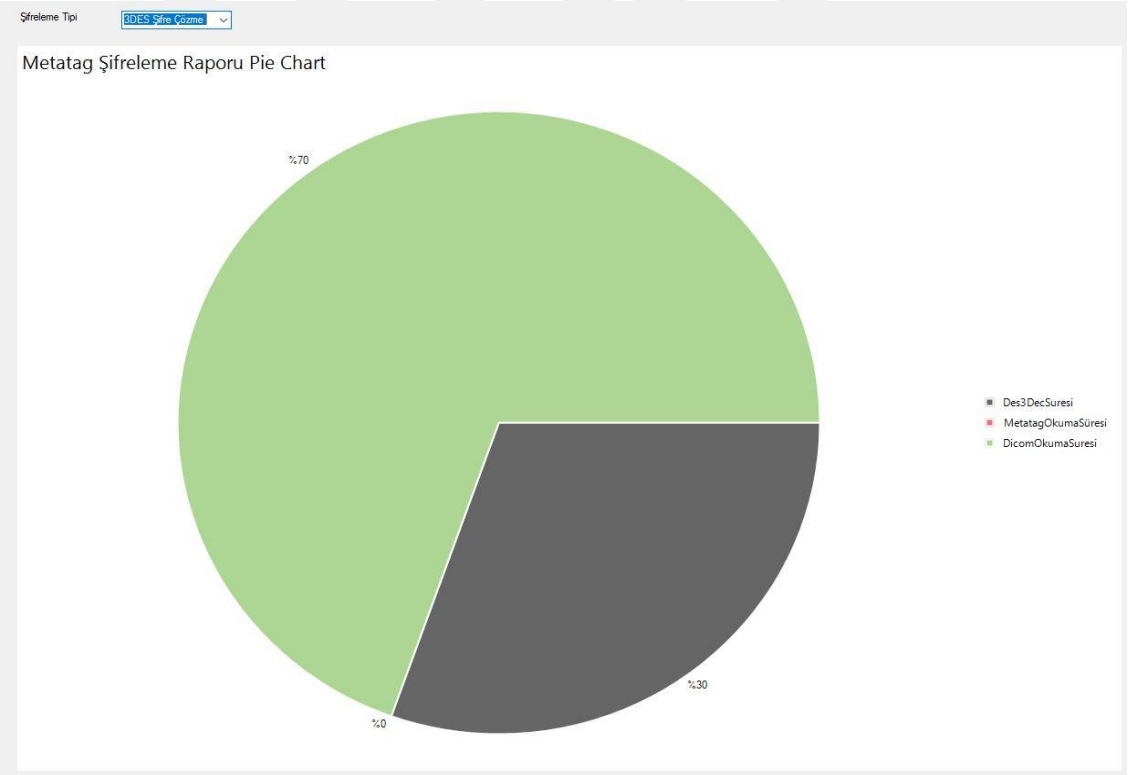
Buradan 3DES ile şifre çözmenin toplam sürede DICOM okuma süresi belirleyici olmuştur.

Şekil 4.19'da görüldüğü gibi; AES ile şifre çözme yönteminde DICOM Okuma Suresi %89, Etiketlerin AES ile şifre çözmesi %11, Etiketlerin okunma süresi neredeyse %0'a yakın olduğundan ihmal edilebilir düzeyde çıkmıştır.

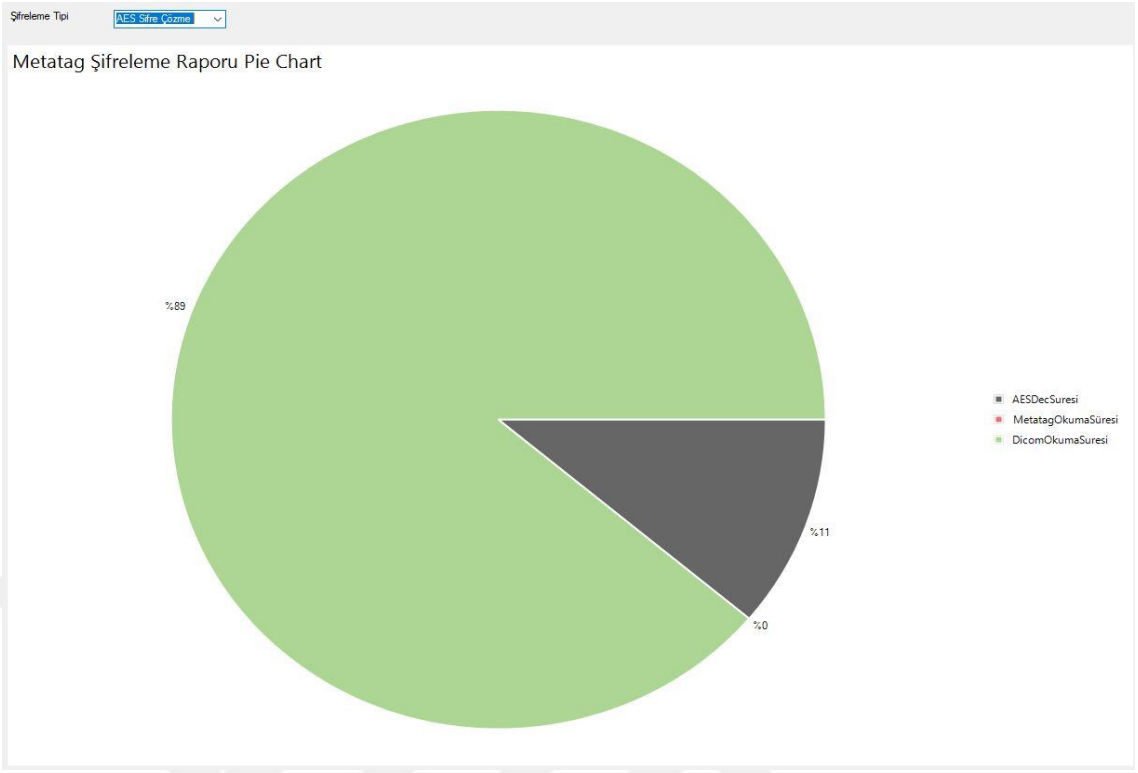
Buradan AES ile şifre çözme; toplam sürede DICOM okuma süresi belirleyici olmuştur. AES şifre çözme 3DES şifre çözmeye göre daha hızlı olduğundan DICOM okuma süresinin genel toplamda yüzdelik etkisini artırdığı söylenebilir.

Şekil 4.20'te görüldüğü gibi; RSA ile şifre çözme yönteminde DICOM okuma süresi %25, Etiketlerin RSA ile şifre çözme %75, Etiket okunma süresi neredeyse %0'a yakın olduğundan ihmal edilebilir düzeyde çıkmıştır.

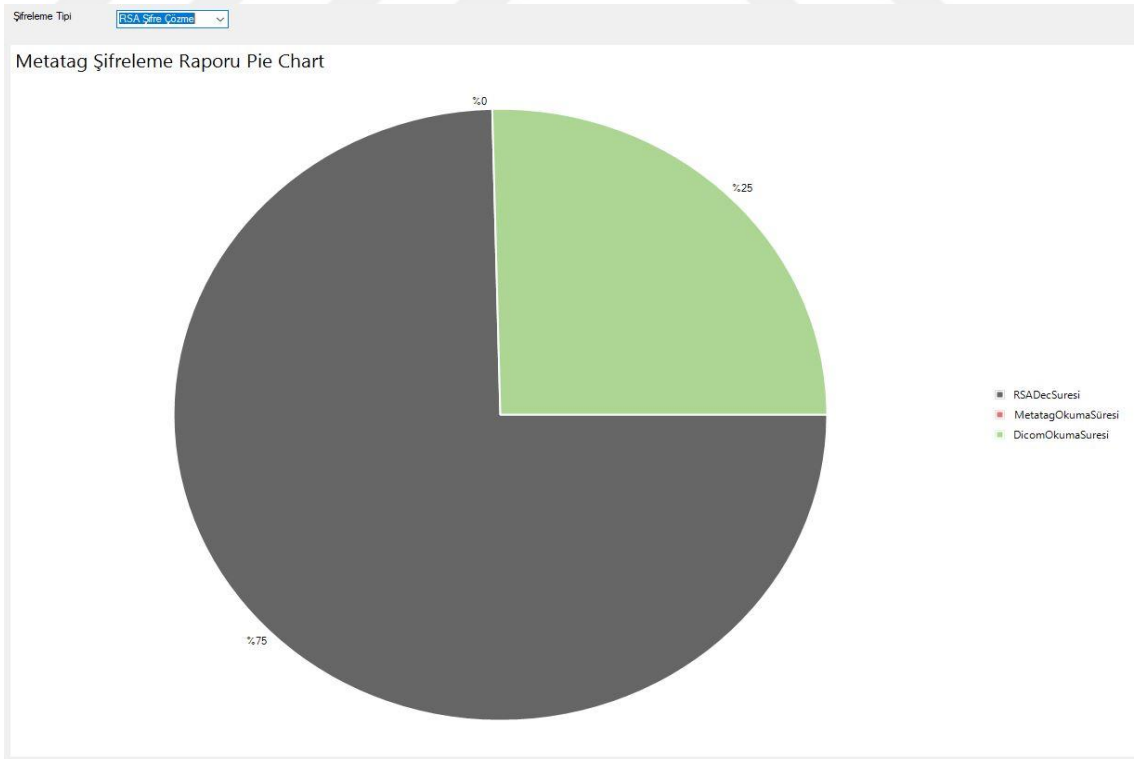
Buradan RSA ile şifre çözmenin toplam sürede; RSA şifre çözme süresi belirleyici olmuştur. RSA şifre çözme 3DES,AES şifre çözmeye göre daha yavaş olduğundan DICOM okuma süresinin genel toplamda yüzdelik etkisini azaltarak; DICOM okuma süresinin 3 katı sürede olduğu gözlemlenmiştir.



Şekil 4.18: 3DES şifre çözme yönteminin toplam süre üzerindeki etki grafiği.



Şekil 4.19: AES şifre çözme yönteminin toplam süre üzerindeki etki grafiği.



Şekil 4.20: RSA şifre çözme yönteminin toplam süre üzerindeki etki grafiği.

4.7. DICOM ETİKET SAYISININ ETİKET ŞİFRELEME İŞLEMİNE ETKİLERİNİN ANALİZİ

DICOM verisi içerisinde modaliteye göre ve Tıbbi cihazın özelliklerine göre değişen sayılarda dinamik etiket eklenebilmektedir. Bu durumda; etiket sayısı DICOM'a göre farklılık gösterebilmektedir.

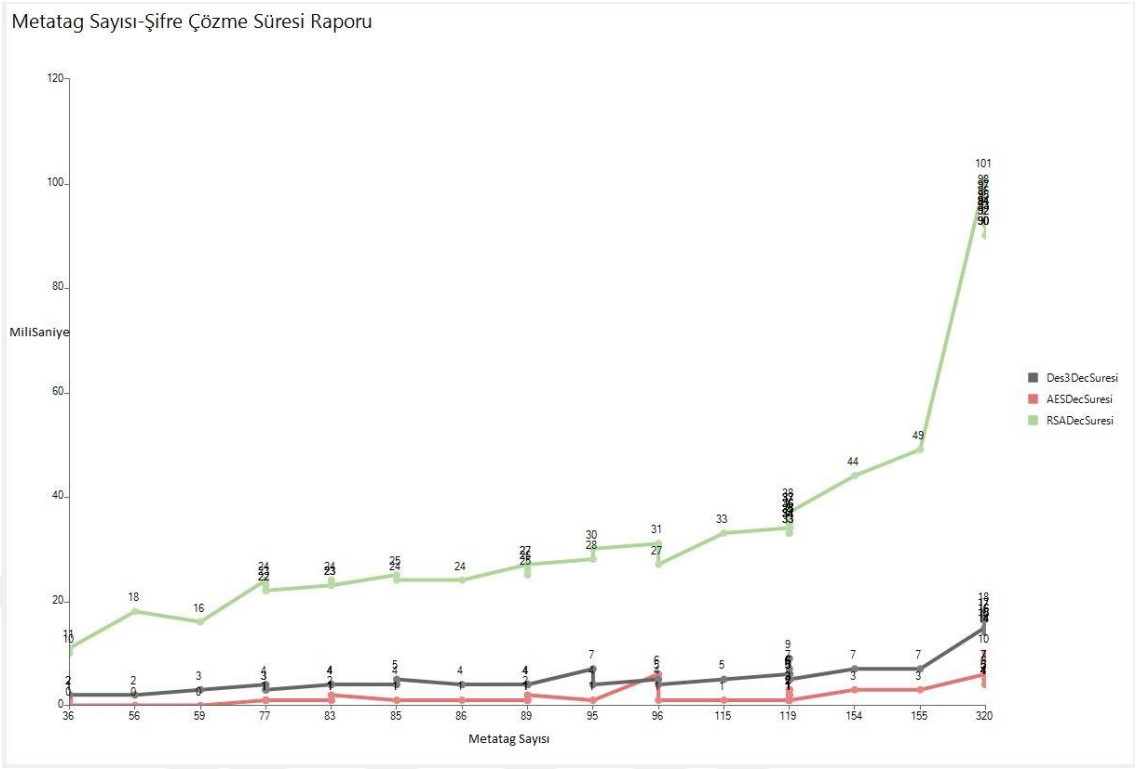
Etiket sayıları azdan çoğa sıralandığında 3DES, AES, RSA şifreleme sürelerinde etkileri Şekil 4.21 'de gösterilmiştir. Etiket şifreleme için kullanılan 3DES, AES, RSA 3 yöntemde de DICOM'daki etiket sayısının artışı etiket şifreleme sürelerini artırdığı görülmüştür.

3DES şifrelemede; etiket sayısı 36'dan 119'a kadar olan DICOM örneklerindeki sürelerde 0 milisaniye ile 6milisaniye aralığında az farklılıklarla olduğu görülmüştür. Ancak etiket sayısı 119–320 aralığındaki DICOM örneklerinde bu farklılığın artarak 4 milisaniye ile 21 milisaniye aralığında değiştiği gözlemlenmiştir.

AES şifrelemede; etiket sayısı 36'dan 119'a kadar olan DICOM örneklerindeki sürelerde 0 milisaniye ile 5 milisaniye aralığında az farklılıklarla olduğu görülmüştür. Etiket sayısı 119–320 aralığındaki DICOM örneklerinde bu farklılığın benzer oranlarda arttığı 1 milisaniye ile 7 milisaniye aralığında değiştiği gözlemlenmiştir.

Ancak RSA ile etiket şifrelemedeki durum 3DES ve AES etiket şifrelemedeki durumdan farklılık göstermektedir. Etiket sayısı 36'dan 155'a kadar olan DICOM örneklerinde sürelerde 1 milisaniye ile 11 milisaniye aralığında artan değer görülmüştür. Bu artış süreleri 3DES ve AES etiket şifreleme yöntemine göre daha fazla aralıkta olduğu ve etiket sayısı arttıkça doğrusala yakın artış gösterdiği gözlemlenmiştir.

Ayrıca RSA ile etiket şifrelemedeki etiket sayısı 155–320 aralığındaki DICOM örneklerinde bu farklılığın hızlı bir şekilde artarak 11 milisaniye ile 26 milisaniye aralığında değiştiği gözlemlenmiştir.



Şekil 4.21: Etiket sayıları azdan çoğa sıralandığında 3DES, AES, RSA şifreleme sürelerinde etkileri.

4.8. DICOM ETİKET SAYISININ ETİKET ŞİFRE ÇÖZMEDE ETKİLERİNİN ANALİZİ

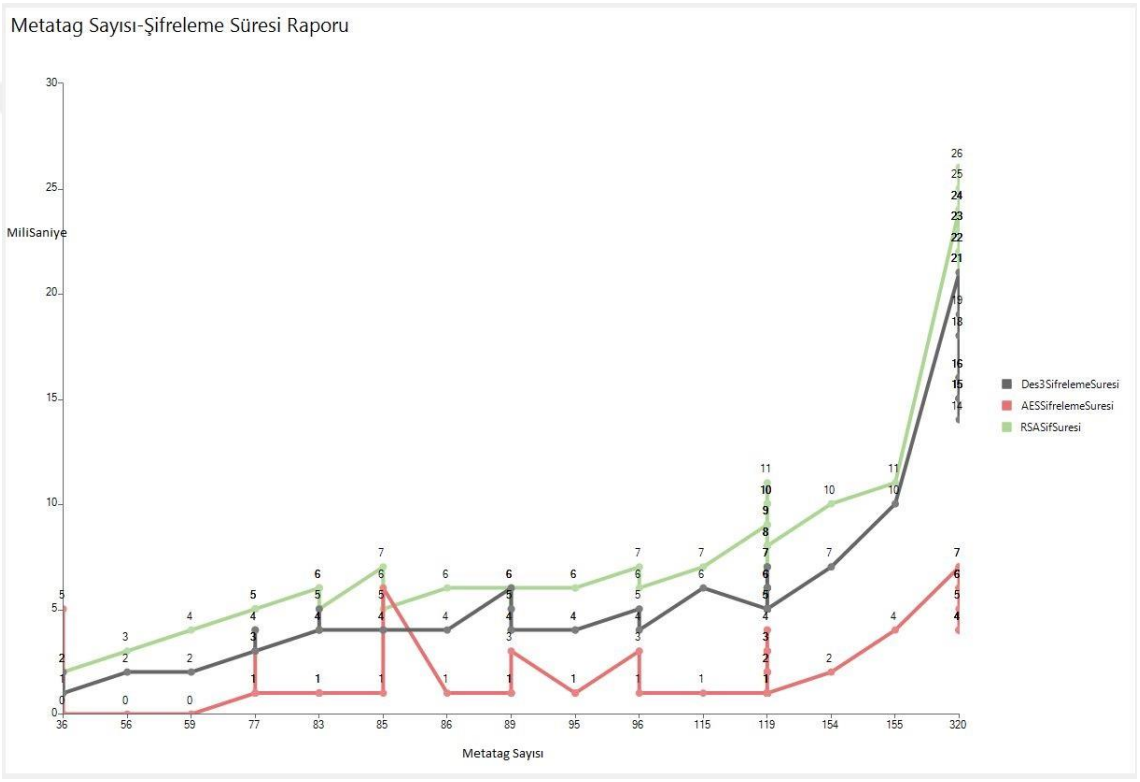
DICOM verisi içerisinde modaliteye göre ve Tıbbi cihazın özelliklerine göre değişen sayılarda dinamik etiket eklenebilmektedir. Bu durumda; etiket sayısı DICOM'a göre farklılık gösterebilmektedir.

Etiket sayıları azdan çoğa sıralandığında 3DES, AES, RSA şifre çözme sürelerinde etkileri Şekil 4.22 'de gösterilmiştir. Etiket şifre çözme için kullanılan 3DES, AES, RSA 3 yöntemde de DICOM'daki etiket sayısının artışı etiket şifre çözme sürelerini artırdığı görülmüştür.

3DES ve AES etiket şifre çözmede; etiket sayısı 36'dan 119'a kadar olan DICOM örneklerinde sürelerde 2 milisaniye ile 7 milisaniye aralığında az farklılıklarla olduğu görülmüştür. Ancak etiket sayısı 119–320 aralığındaki DICOM örneklerinde bu farklılığın artarak 3 milisaniye ile 18 milisaniye aralığında değiştiği gözlemlenmiştir.

Ancak RSA ile etiket şifre çözmedeki durum 3DES ve AES etiket şifre çözmedeki durumdan farklılık göstermektedir. Etiket sayısı 36'dan 155'a kadar olan DICOM örneklerinde sürelerde 10 milisaniye ile 49 milisaniye aralığında artan değer görülmüştür. Bu artış süreleri 3DES ve AES etiket şifre çözme yöntemine göre daha fazla aralıkta olduğu ve etiket sayısı arttıkça doğrusala yakın artış gösterdiği gözlemlenmiştir.

Ayrıca RSA ile etiket şifre çözmedeki etiket sayısı 155–320 aralığındaki DICOM örneklerinde bu farklılığın hızlı bir şekilde artarak 49 milisaniye ile 101 milisaniye aralığında değiştiği gözlemlenmiştir.



Şekil 4.22: Etiket sayıları azdan çoğa sıralandığında 3DES, AES, RSA şifre çözme sürelerinde etkileri.

4.9. MODALİTEYE GÖRE DOSYA ŞİFRELEME VE ETİKET ŞİFRELEME RAPORU

Sağlık alanında DICOM formatı farklı modalitelerde kullanılmakta ve modaliteye göre DICOM yapısı değişiklik gösterebilmektedir.

Modaliteye göre Dosya şifreleme (toplam geçen süre-milisaniye) – Etiket şifreleme (toplam: Etiket okuma süresi + DICOM okuma süresi + şifreleme süresi) Raporu Şekil 4.23'de gösterilmiştir.

Bu çalışmada kullanılan DICOM örneklerinde CR (Computed Radiography), CT (Computed Tomography), DX (Dijital Radiography), EK (Electrocardiography), IO (Intra-oral Radiography), MR (Magnetic Resonance), US (Ultrasound), MG (Mammography) ve OT (Other Modality-retired) DICOM modaliteleri kullanılmıştır.

Modalitesi CR olan DICOM örneklerinde; Şekil 4.24'te görüldüğü gibi; 3DES, AES, RSA etiket şifrelemede geçen toplam süre (toplam: etiket okuma süresi + DICOM okuma süresi + şifreleme süresi) AES ile etiket şifreleme en performanslı olsa da; 3 şifreleme yönteminde de birbirine yakın sürelerde olduğu görülmüştür.

Ancak 3DES, AES, RSA etiket şifrelemede geçen toplam süre (toplam: etiket okuma süresi + DICOM okuma süresi + şifreleme süresi) Dosya şifreleme (Toplam Geçen süre)'ye kıyaslandığında; 2 veya 3 katı oranında daha hızlı olduğu gözlemlenmiştir.

Modalitesi CT olan DICOM örneklerinde; Şekil 4.25'te görüldüğü gibi; 3DES, AES, RSA etiket şifrelemede geçen toplam süre (toplam: etiket okuma süresi + DICOM okuma süresi + şifreleme süresi) AES ile etiket şifreleme en performanslı olsa da; 3 şifreleme yönteminde de birbirine yakın sürelerde olduğu görülmüştür.

Modalitesi CT olan DICOM örneklerinden faklı olarak 3DES, AES, RSA etiket şifrelemede geçen toplam süre (toplam: etiket okuma süresi + DICOM okuma süresi + şifreleme süresi) dosya şifreleme (Toplam Geçen Süre)'ye kıyaslandığında; etiket şifreleme yöntemleri ile dosya şifrelemede geçen sürelerin birbirine yakın değerler olduğu gözlemlenmiştir.

Modalitesi DX olan DICOM örneklerinde; Şekil 4.26'da görüldüğü gibi; modalitesi CR olan DICOM örneklerine benzer bir şekilde 3DES, AES, RSA etiket şifrelemede geçen toplam süre (toplam: etiket okuma süresi + DICOM okuma süresi + şifreleme süresi) AES ile etiket şifreleme en performanslı olsa da; 3 şifreleme yönteminde de birbirine yakın sürelerde olduğu görülmüştür.

Ancak 3DES, AES, RSA etiket şifrelemede geçen toplam süre (toplam: etiket okuma süresi + DICOM okuma süresi + şifreleme süresi) dosya şifreleme (Toplam Geçen Süre)'ye kıyaslandığında; yaklaşık 3 katı oranında daha hızlı olduğu gözlemlenmiştir.

Modalitesi IO olan DICOM örneklerinde; Şekil 4.27'de görüldüğü gibi; modalitesi CR ve DX olan DICOM örneklerine benzer bir şekilde 3DES, AES, RSA etiket şifrelemede geçen toplam süre (toplam: etiket okuma süresi + DICOM okuma süresi + şifreleme süresi) AES ile etiket şifreleme en performanslı olsa da; 3 şifreleme yönteminde de birbirine yakın sürelerde olduğu görülmüştür.

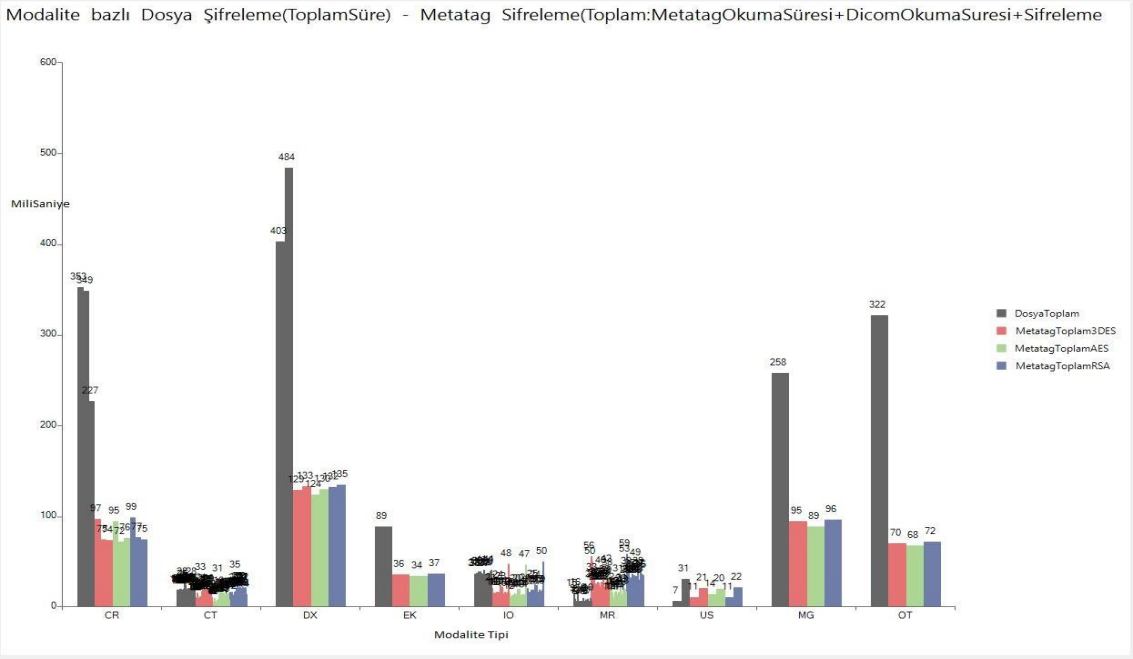
Ancak 3DES, AES, RSA etiket şifrelemede geçen toplam süre (toplam: etiket okuma süresi + DICOM okuma süresi + şifreleme süresi) dosya şifreleme (Toplam Geçen Süre)'ye kıyaslandığında; yaklaşık 2 katı oranında daha hızlı olduğu gözlemlenmiştir. Burada Modalitesi CR ve DX olan DICOM örneklerinden farklı olarak bazı DICOM örneklerinde dosya şifreleme yöntemi; etiket şifrelemedeki 3 yönteme göre daha performanslı olduğu gözlemlenmiştir.

Modalitesi MR olan DICOM örneklerinde; Şekil 4.28'de görüldüğü gibi; diğer modalite türlerinden farklı olarak dosya şifreleme yöntemi ile geçen süre (Toplam Geçen Süre); 3DES, AES, RSA etiket şifreleme yöntemi ile geçen toplam süreye (toplam: etiket okuma süresi + DICOM okuma süresi + şifreleme süresi) göre; yaklaşık 3 katı oranında daha hızlı olduğu gözlemlenmiştir.

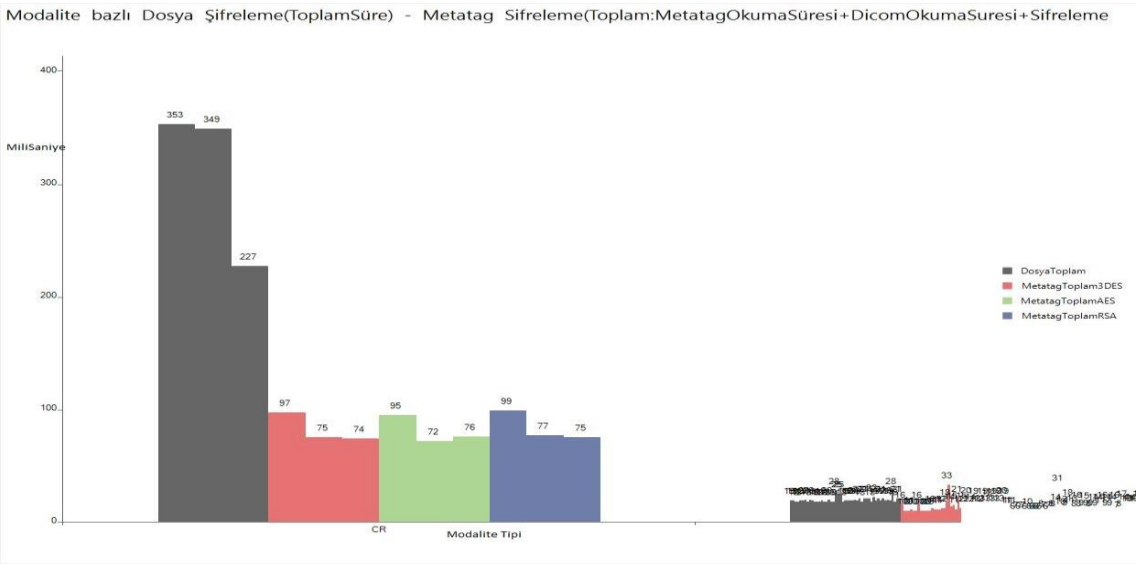
Ancak 3DES, AES, RSA etiket şifrelemede geçen toplam süre (toplam: etiket okuma süresi + DICOM okuma süresi + şifreleme süresi) AES ile etiket şifreleme en performanslı olsa da; 3 şifreleme yönteminde de birbirine yakın sürelerde olduğu görülmüştür.

Modalitesi US, MG ve OT ve EK olan DICOM örneklerinde örnek sayısı az olsa bile Şekil 4.29'te görüldüğü gibi; modalitesi CR ve DX olan DICOM örneklerine benzer bir şekilde 3DES, AES, RSA etiket şifrelemede geçen toplam süre (toplam: etiket okuma süresi + DICOM okuma süresi + şifreleme süresi) AES ile etiket şifreleme en performanslı olsa da; 3 şifreleme yönteminde de birbirine yakın sürelerde olduğu görülmüştür.

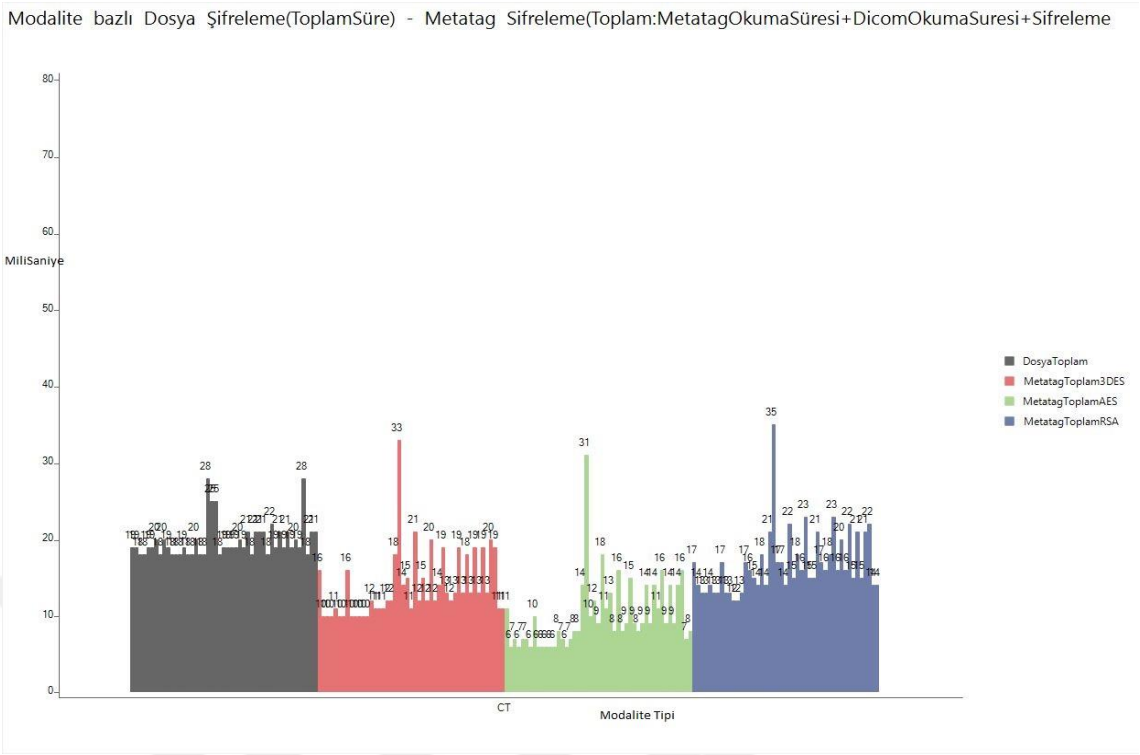
Ancak 3DES, AES, RSA etiket şifrelemede geçen toplam süre (toplam: etiket okuma süresi + DICOM okuma süresi + şifreleme süresi) dosya şifreleme (Toplam Geçen Süre)'ye kıyaslandığında; yaklaşık 2 veya 3 katı oranında daha hızlı olduğu gözlemlenmiştir.



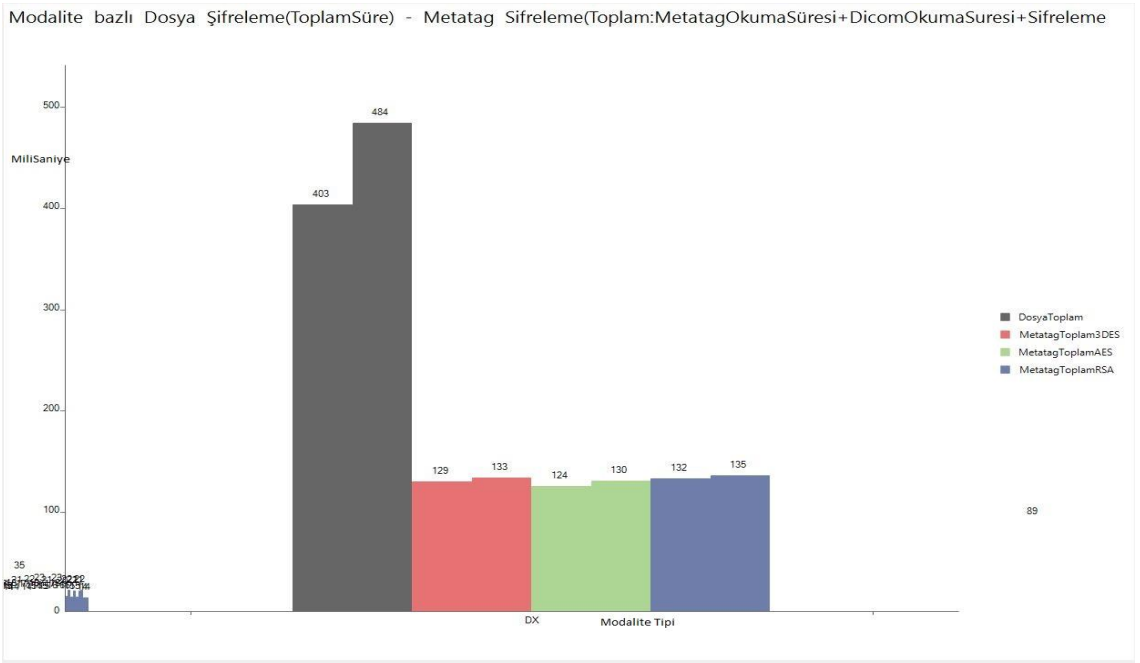
Şekil 4.23: Modaliteye göre dosya şifreleme (toplam geçen süre - milisaniye) – etiket şifreleme (toplam: etiket okuma süresi + DICOM okuma süresi + şifreleme süresi) raporu.



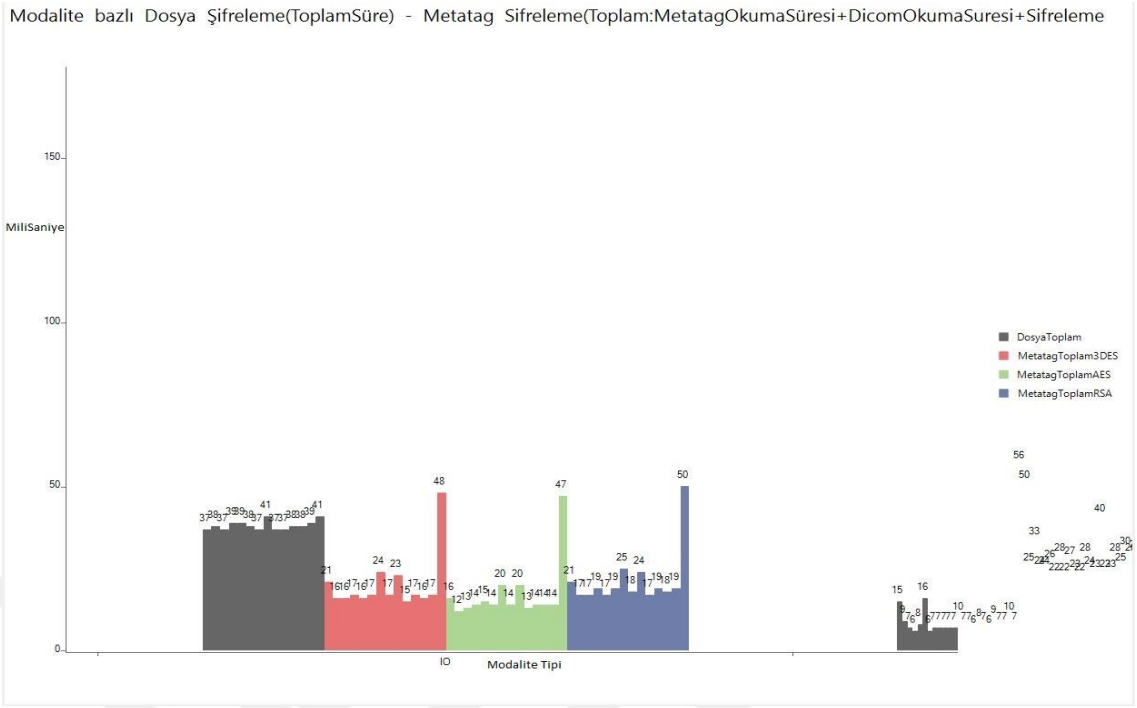
Şekil 4.24: CR dosya şifreleme (toplam geçen süre-milisaniye) – etiket şifreleme (toplam: etiket okuma süresi + DICOM okuma süresi + şifreleme süresi) raporu.



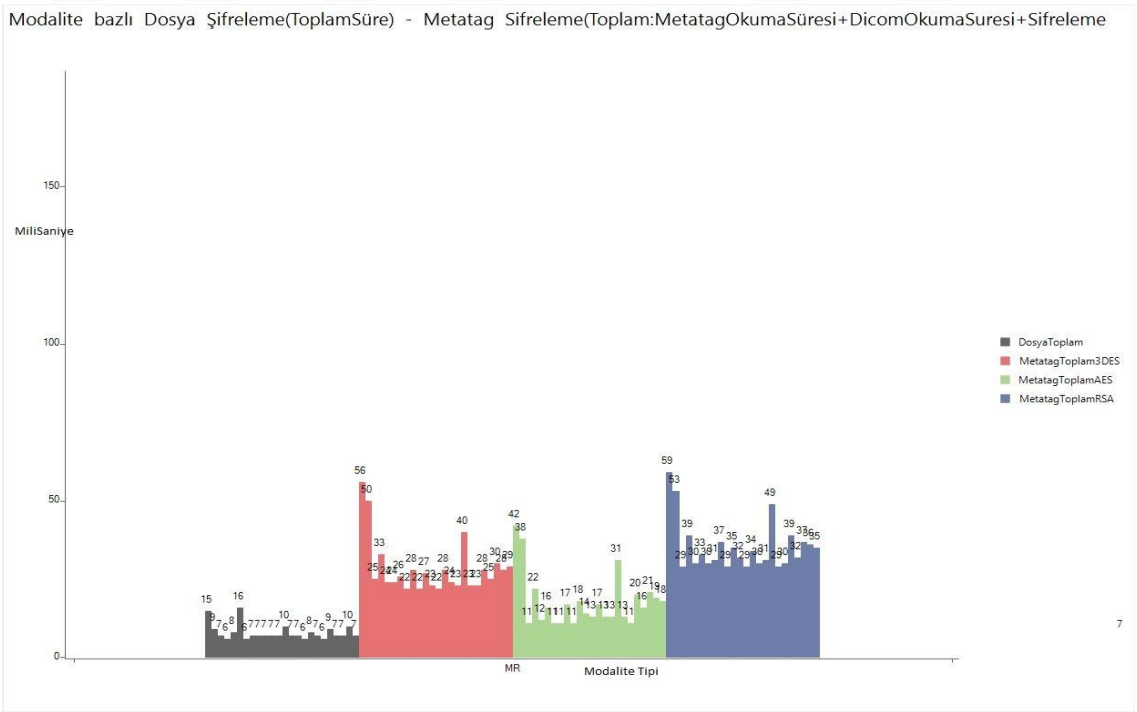
Şekil 4.25: CT dosya şifreleme (toplam geçen süre - milisaniye) – etiket şifreleme (toplam: etiket okuma süresi + DICOM okuma süresi + şifreleme süresi) raporu.



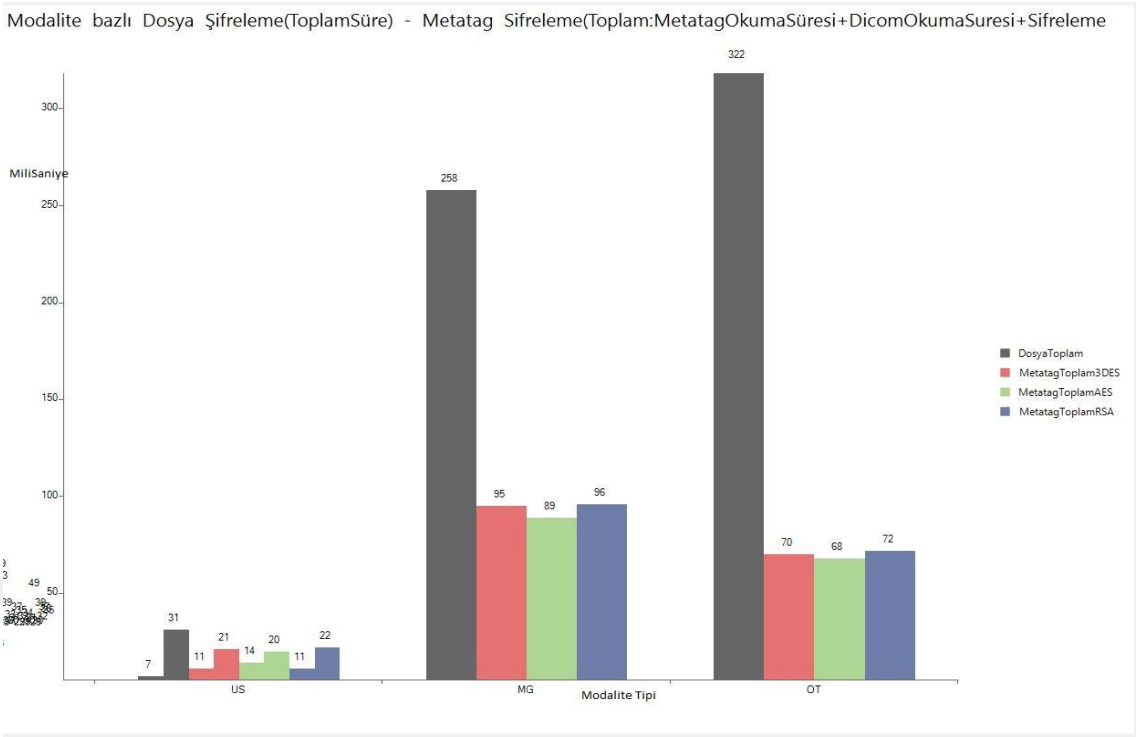
Şekil 4.26: DX dosya şifreleme (toplam geçen süre - milisaniye) – etiket şifreleme (toplam: etiket okuma süresi + DICOM okuma süresi + şifreleme süresi) raporu.



Şekil 4.27: IO dosya şifreleme (toplam geçen süre - milisaniye) – etiket şifreleme (toplam: etiket okuma süresi + DICOM okuma süresi + şifreleme süresi) raporu.



Şekil 4.28: MR dosya şifreleme (toplam geçen süre - milisaniye) – etiket şifreleme (toplam: etiket okuma süresi + DICOM okuma süresi + şifreleme süresi) raporu.



Şekil 4.29: US, MG ve OT dosya şifreleme (toplam geçen süre - milisaniye) – etiket şifreleme (toplam: etiket okuma süresi + DICOM okuma süresi + şifreleme süresi) raporu.

4.10. MODALİTEYE GÖRE DOSYA ŞİFRE ÇÖZMEVE ETİKET ŞİFRE ÇÖZME RAPORU

Sağlık alanında DICOM formatı farklı modalitelerde kullanılmakta ve modaliteye göre DICOM yapısı değişiklik gösterebilmektedir.

Modaliteye göre dosya şifre çözme (toplam geçen süre - milisaniye) – etiket şifre çözme (toplam:etiket okuma süresi + DICOM okuma süresi + şifre çözme süresi) raporu Şekil 4.30'da gösterilmiştir.

Bu çalışmada kullanılan DICOM örneklerinde CR, CT, DX, EK, IO, MR, US, MG ve OT DICOM modaliteleri kullanılmıştır.

Modalitesi CR olan DICOM örneklerinde; Şekil 4.31'de görüldüğü gibi; 3DES, AES, RSA etiket şifre çözmede geçen toplam süre (toplam: etiket okuma süresi + DICOM okuma süresi + şifre çözme süresi) AES ile etiket şifre çözme en performanslı olsa da; üç şifre çözme yönteminde de birbirine yakın sürelerde olduğu görülmüştür.

Ancak 3DES, AES, RSA etiket şifre çözmede geçen toplam süre (toplam: etiket okuma süresi + DICOM okuma süresi + şifre çözme süresi) dosya şifre çözme (toplam geçen süre)'ye kıyaslandığında; 3 veya 4 katı oranında daha hızlı olduğu gözlemlenmiştir. Burada modalitesi CR (Computed Radiography) olan DICOM örneklerindeki şifre çözme işlemlerindeki kıyaslamalarda; şifreleme yöntemlerindeki kıyaslamalara göre sürelerdeki farkın arttığı görülmüştür.

Modalitesi CT olan DICOM örneklerinde; Şekil 4.32'de görüldüğü gibi; AES ile etiket şifre çözme, 3DES ile etiket şifre çözme, RSA ile etiket şifre çözme ve Dosya şifre çözme sürelerine göre kıyaslandığında;

1. AES ile etiket şifre çözme,
2. 3DES ile etiket şifre çözme,
3. Dosya şifre çözme,
4. RSA ile etiket şifre çözme

Şeklinde sıralandığı görülmüştür.

Şifreleme sürelerinden faklı olarak; dosya şifre çözme işlemi, RSA ile etiket şifre çözme geçen toplam süreden (toplam: etiket okuma süresi + DICOM okuma süresi + şifre çözme süresi) daha performanslı olarak görülmüştür.

Modalitesi DX olan DICOM örneklerinde; Şekil 4.33'te görüldüğü gibi; modalitesi CR olan DICOM örneklerine farklı olarak 3DES, AES, RSA etiket şifre çözme geçen toplam süre (toplam: etiket okuma süresi + DICOM okuma süresi + şifre çözme süresi) AES ile etiket şifre çözme en performanslı olsa da; 3 şifre çözme yönteminde de birbirine yakın sürelerde olduğu görülmüştür.

Ancak 3DES, AES, RSA etiket şifre çözmede geçen toplam süre (toplam: etiket okuma süresi + DICOM okuma süresi + şifre çözme süresi) Dosya şifre çözme (toplam geçen süre)'ye kıyaslandığında; yaklaşık 3 veya 4 katı oranında daha hızlı olduğu gözlemlenmiştir. Burada Modalitesi DX (Dijital Radiography) olan DICOM örneklerindeki şifre çözme işlemlerindeki kıyaslamalarda; şifre çözme yöntemlerindeki kıyaslamalara göre sürelerdeki farkın arttığı görülmüştür.

Modalitesi IO olan DICOM örneklerinde; Şekil 4.34'te görüldüğü gibi; AES ile etiket şifre çözme, 3DES ile etiket şifre çözme, RSA ile etiket şifre çözme süreleri ile dosya şifre çözme sürelerine göre kıyaslandığında;

1.AES ile etiket şifre çözme,
2.RSA ile etiket şifre çözme
3.Dosya şifre çözme,
4.RSA ile etiket şifre çözme
Şeklinde sıralandığı görülmüştür.

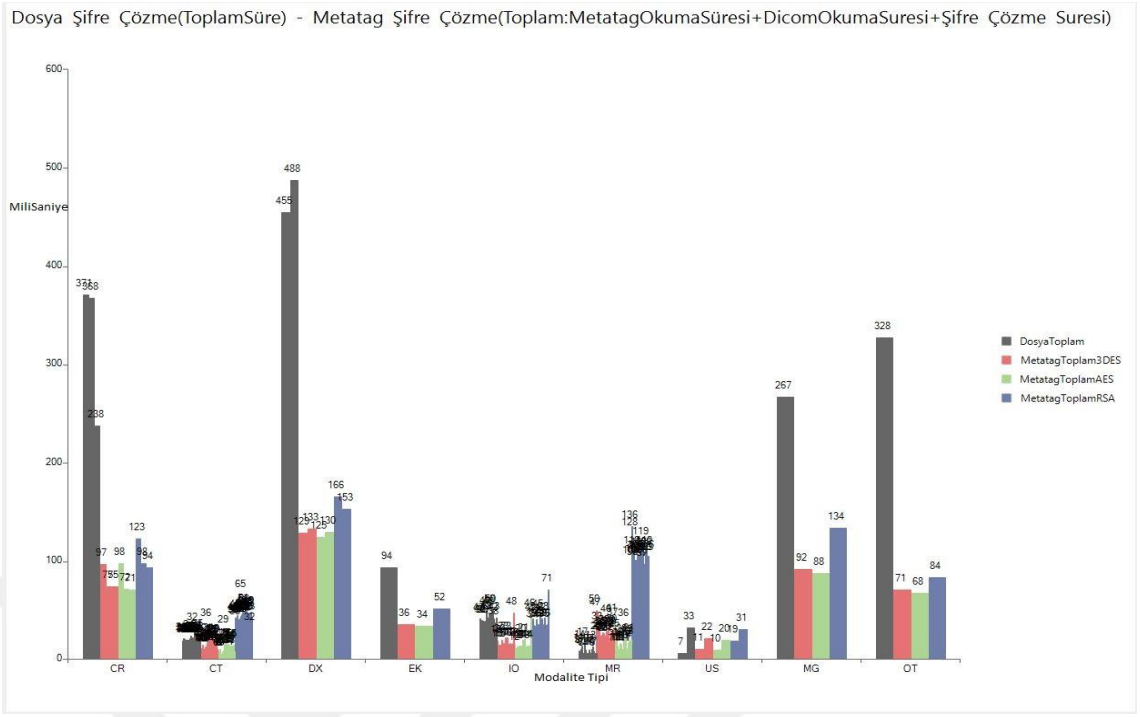
Şifreleme sürelerinden faklı olarak; AES ile etiket şifre çözme en iyi performansa sahip olmasına rağmen 3DES ile etiket şifre çözme ile yakın sürelerde şifre çözme yaptığı, RSA ile etiket şifre çözme ile dosya şifre çözme süreleri yakın olduğu görülmüştür.

Modalitesi MR olan DICOM örneklerinde; Şekil 4.35'te görüldüğü gibi; diğer modalite türlerinden farklı olarak dosya şifre çözme yöntemi ile geçen süre (toplam geçen süre); 3DES, AES, RSA etiket şifre çözme yöntemi ile geçen toplam süreye (toplam: etiket okuma süresi + DICOM okuma süresi + şifre çözme süresi) göre; yaklaşık 3 katı oranında daha hızlı olduğu gözlemlenmiştir.

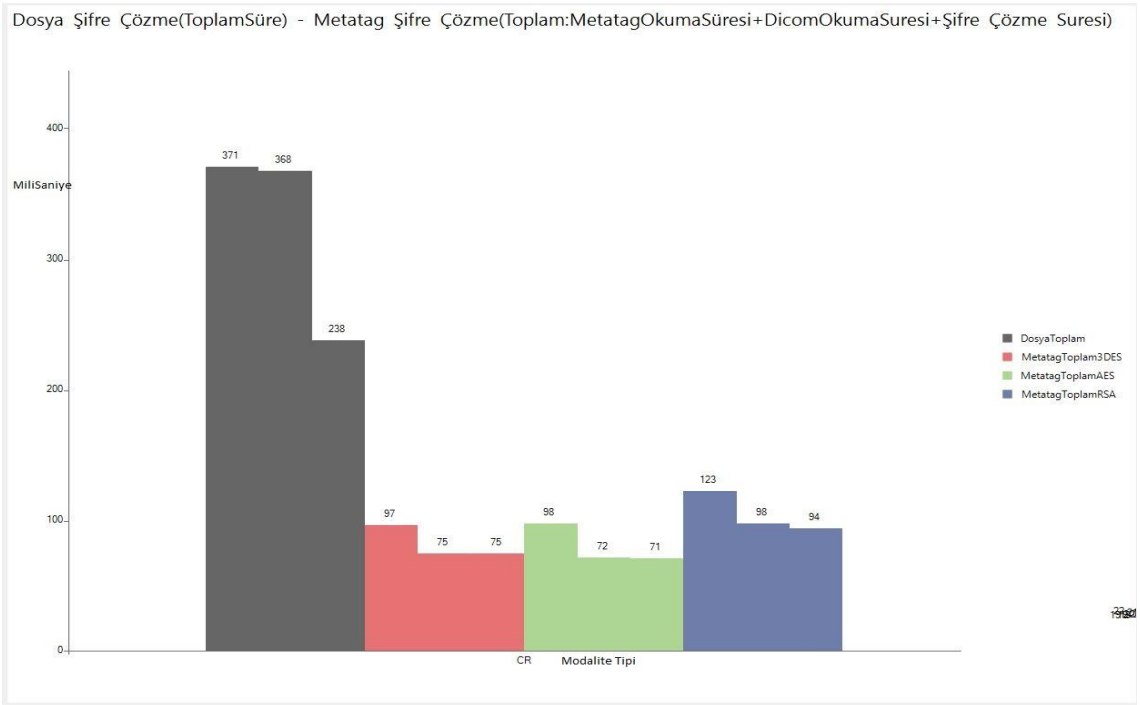
Ancak 3DES, AES, RSA etiket şifre çözmede geçen toplam süre (toplam: etiket okuma süresi + DICOM okuma süresi + şifre çözme süresi) AES ile etiket şifre çözme, 3DES ile etiket şifre çözme, RSA ile etiket şifre çözme şeklinde sıralandığı görülmüştür. RSA ile etiket şifre çözme işleminin diğer modalitelerdeki sürelerden farklı olarak daha uzun sürdüğü görülmüştür.

Modalitesi US, MG ve OT ve EK olan DICOM örneklerinde örnek sayısı az olsa bile Şekil 4.36'da görüldüğü gibi; 3DES, AES, RSA etiket şifre çözme geçen toplam süre (toplam: etiket okuma süresi + DICOM okuma süresi + şifre çözme süresi) AES ile etiket şifre çözme ile 3DES ile etiket şifre çözme yöntemlerinin birbirine yakın değerlerde olduğu; RSA ile etiket şifre çözme yönteminin diğer etiket şifre çözme yöntemlerinden ayrılarak daha yavaş olduğu görülmüştür.

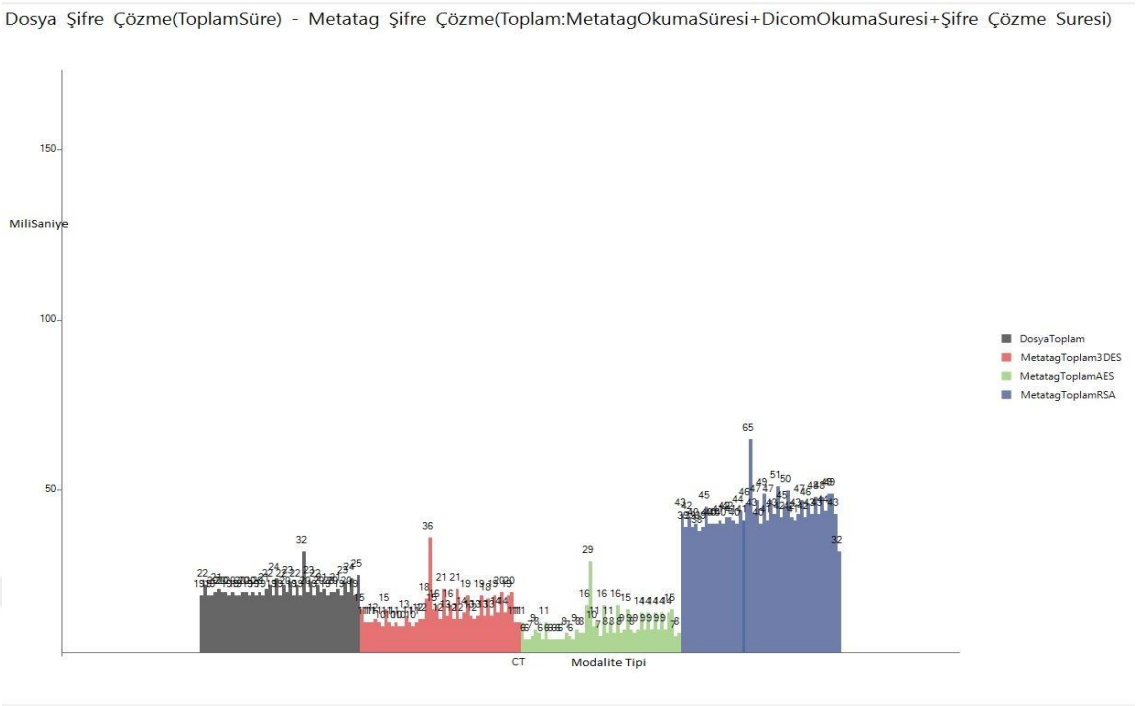
Ancak 3DES, AES, RSA etiket şifre çözmede geçen toplam süre (toplam: etiket okuma süresi + DICOM okuma süresi + şifre çözme süresi) Dosya şifre çözme (toplam geçen süre)'ye kıyaslandığında; yaklaşık 3 veya 4 katı oranında daha hızlı olduğu gözlemlenmiştir. Buradaki DICOM örneklerindeki şifre çözme işlemlerindeki kıyaslamalarda; şifreleme yöntemlerindeki kıyaslamalara göre sürelerdeki farkın arttığı görülmüştür.



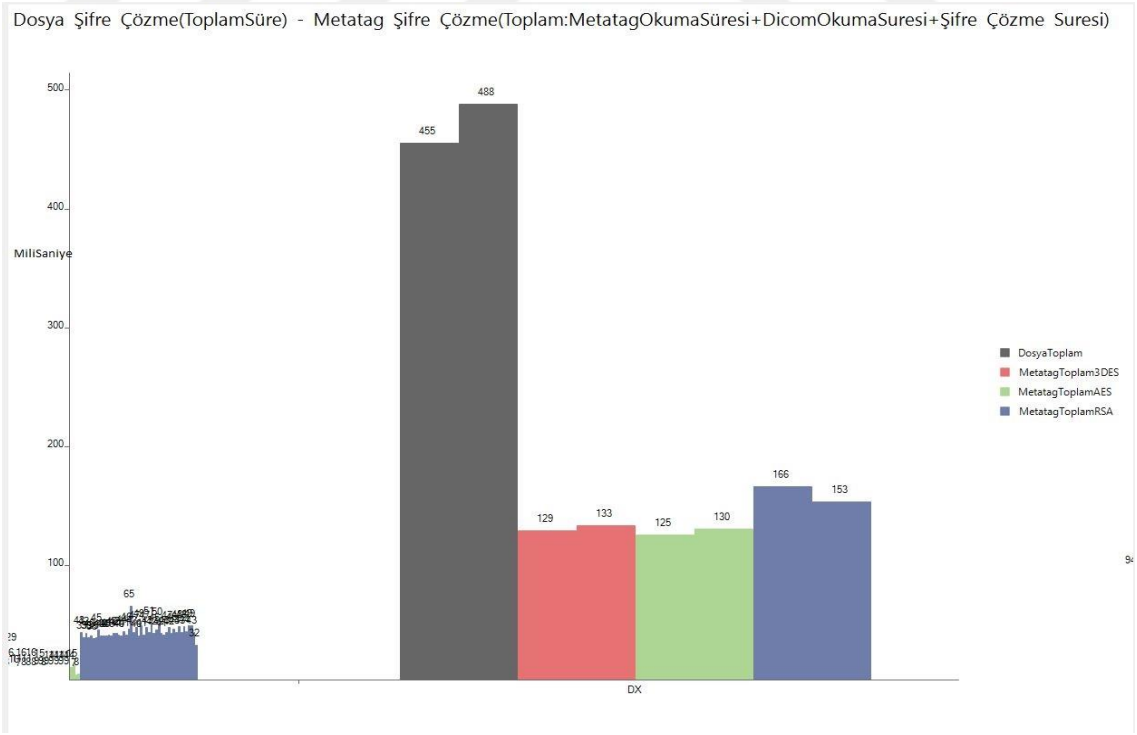
Şekil 4.30: Modaliteye göre dosya şifre çözme (toplam geçen süre - milisaniye) – etiket şifre çözme (toplam: etiket okuma süresi + dicom okuma süresi + şifre çözme süresi) raporu.



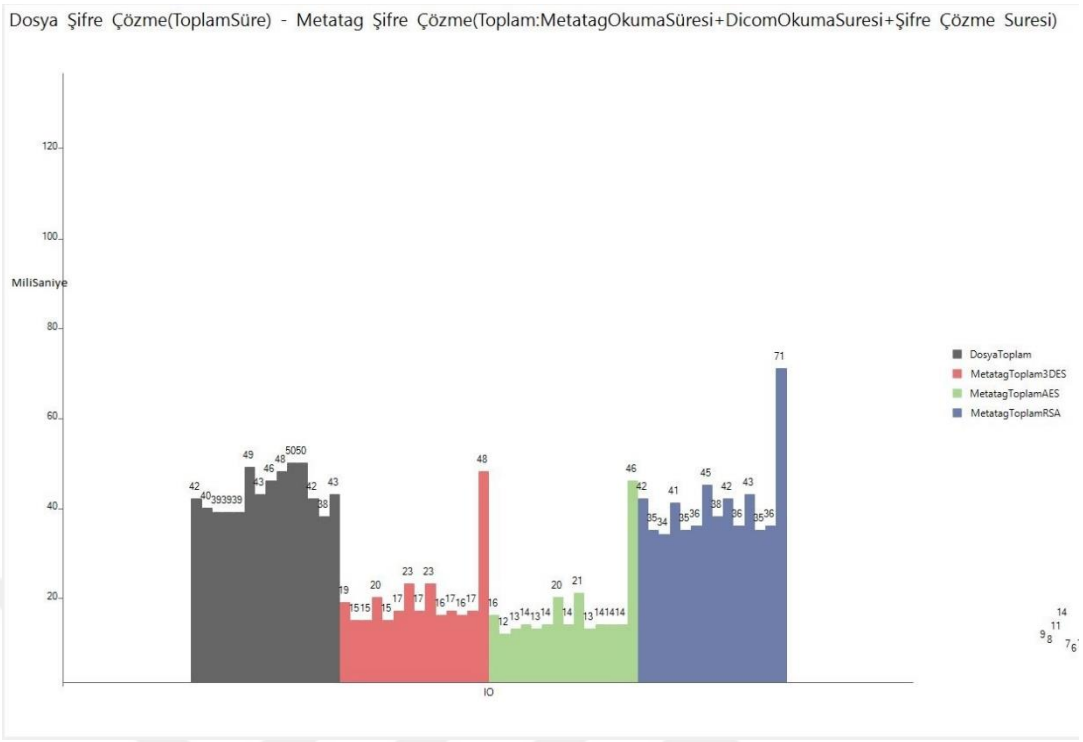
Şekil 4.31: CR dosya şifre çözme (toplam geçen süre - milisaniye) – etiket şifre çözme (toplam: etiket okuma süresi + DICOM okuma süresi + şifre çözme süresi) raporu.



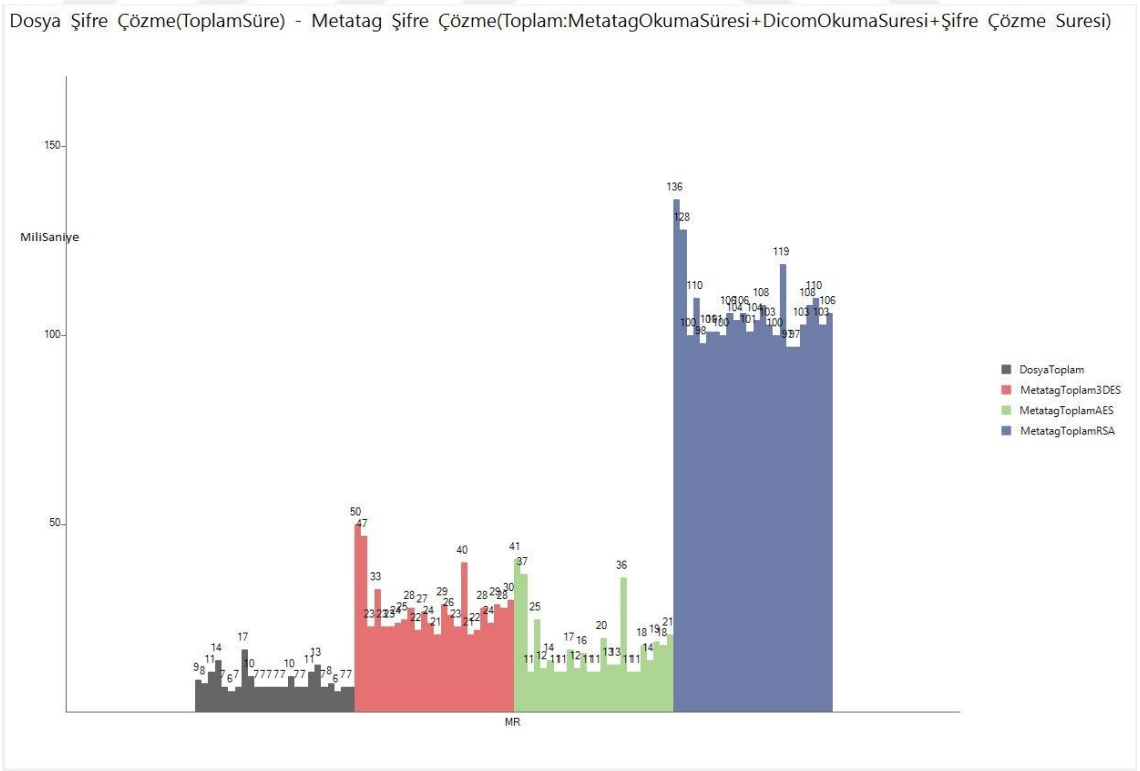
Şekil 4.32: CT dosya şifre çözme (toplam geçen süre-milisaniye) – etiket şifre çözme (toplam: etiket okuma süresi + DICOM okuma süresi + şifre çözme süresi) raporu.



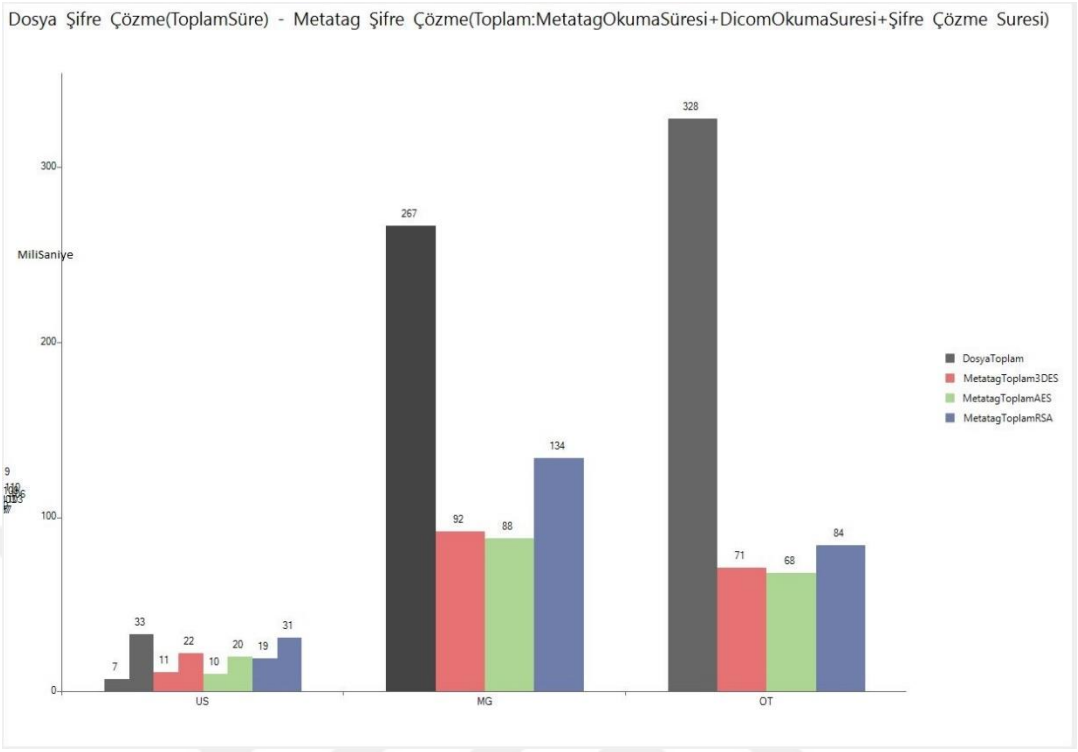
Şekil 4.33: DX dosya şifre çözme (toplam geçen süre - milisaniye) – etiket şifre çözme (toplam: etiket okuma süresi + DICOM okuma süresi + şifre çözme süresi) raporu.



Şekil 4.34: IO dosya şifre çözme (toplam geçen süre - milisaniye) – etiket şifre çözme (toplam: etiket okuma süresi + DICOM okuma süresi + şifre çözme süresi) raporu.



Şekil 4.35: Modalitesi MR dosya şifre çözme (toplam geçen süre - milisaniye) – etiket şifre çözme raporu.



Şekil 4.36: US, MG ve OT dosya şifre çözme (toplam geçen süre - milisaniye) – etiket şifre çözme raporu.

4.11. DOSYA BOYUTUNUN ŞİFRELEME ÜZERİNDEKİ ETKİLERİ

Sağlık Ekosisteminde modaliteye göre ve Tıbbi cihazın özelliklerine göre değişen boyutlarda DICOM verisi üretilmektedir. Bu durumda; dosya boyutu DICOM modalitesine göre farklılık gösterebilmektedir.

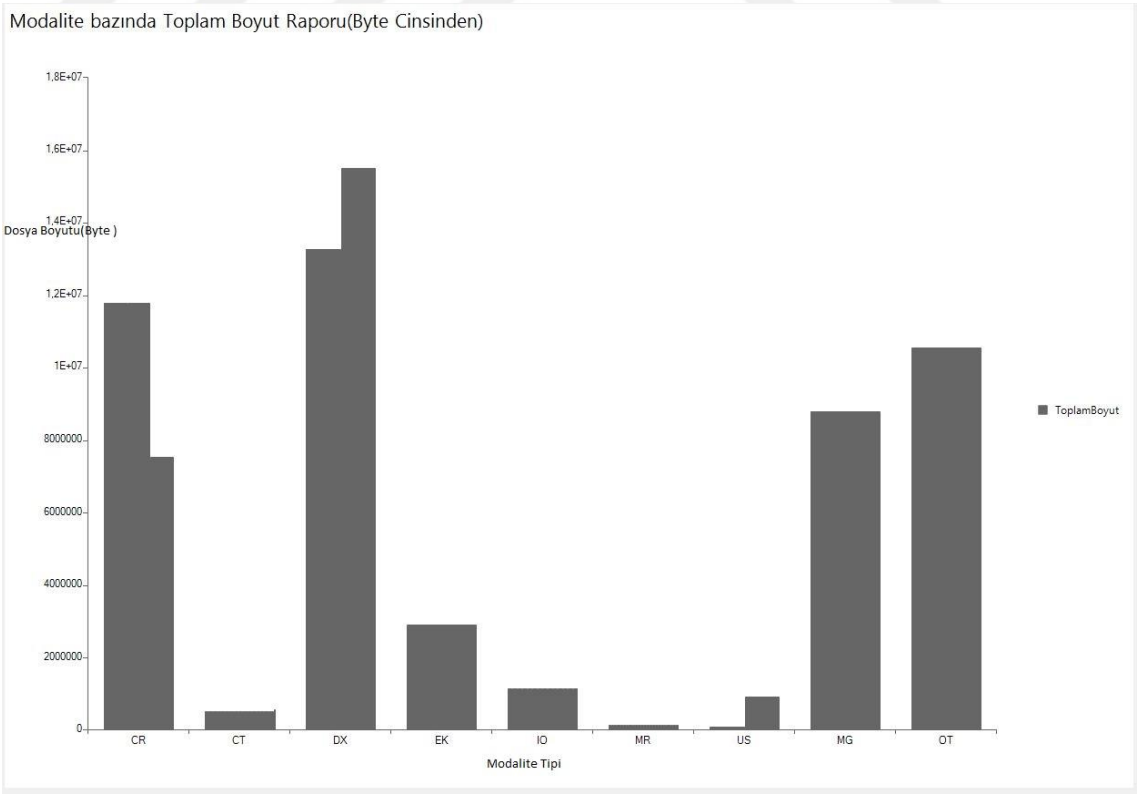
Bu çalışmada kullanılan test verilerinde; Şekil 4.37 de görüldüğü gibi farklı modalitelerden farklı boyutlarda örnekler alınmıştır. Bu örnekler incelendiğinde; MR verilerinin diğer modalitelere göre dosya boyutunun belirgin seviyede küçük olduğu görülmektedir.

DICOM dosya boyutu azdan çoğa sıralandığında dosya olarak şifreleme, 3DES, AES, RSA şifreleme sürelerinde etkileri Şekil 4.38 ‘de gösterilmiştir. Şifreleme için kullanılan dosya olarak şifreleme ve 3DES, AES, RSA ile etiket şifreleme yöntemlerinde; genel

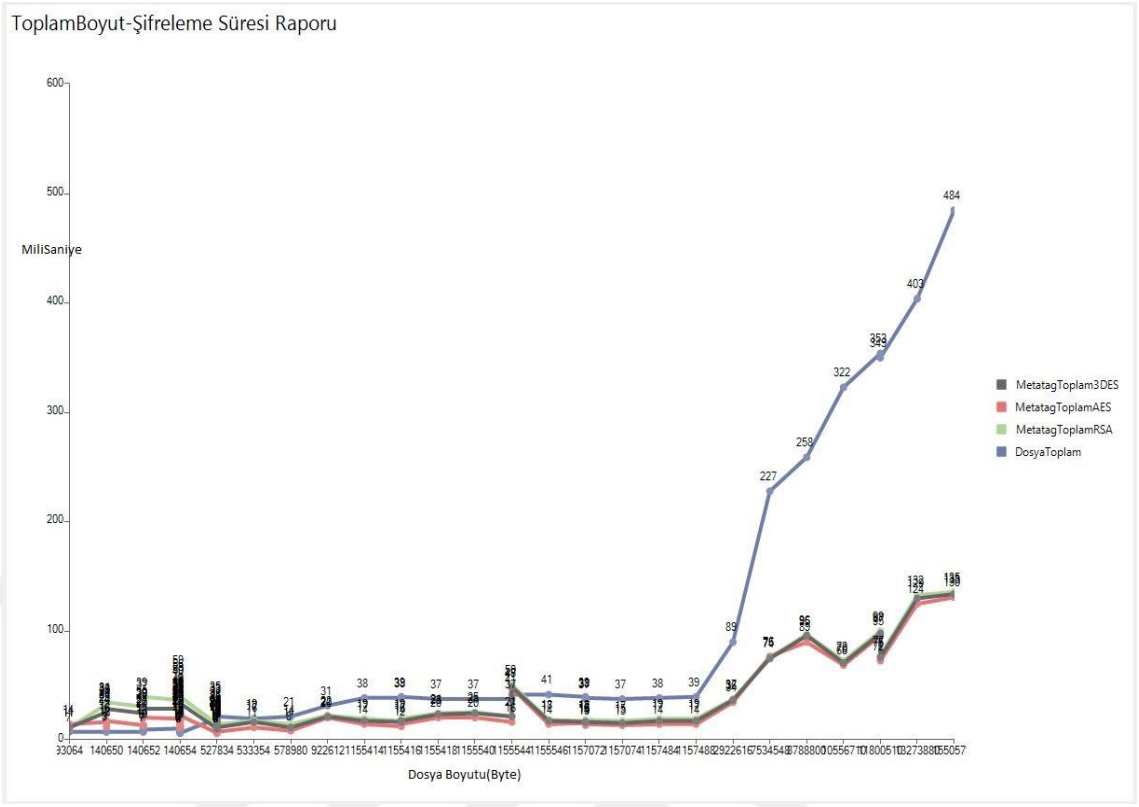
olarak dosya boyutunun artması şifreleme sürelerinin artmasına sebep olduğu gözlemlenmiştir.

Şekil 4.39'da MR DICOM verilerinde dosya boyutunun şifreleme yöntemlerindeki etkileri gösterilmiştir. Buna göre; dosya boyutu 527834 byte'a kadar olan veriler için; dosya olarak şifreleme yöntemleri etiket şifreleme yöntemlerine göre daha hızlı olduğu gözlemlenmiştir. Ancak 527834 byte'tan büyük dosyalar için dosya olarak şifreleme etiket şifrelemenin en yavaşı olan RSA ile etiket şifrelemeden bile daha yavaş olduğu görülmektedir. Dosya boyutu 527834 byte'a kadar olan verilerin MR modaliteye ait olduğu görülmüştür.

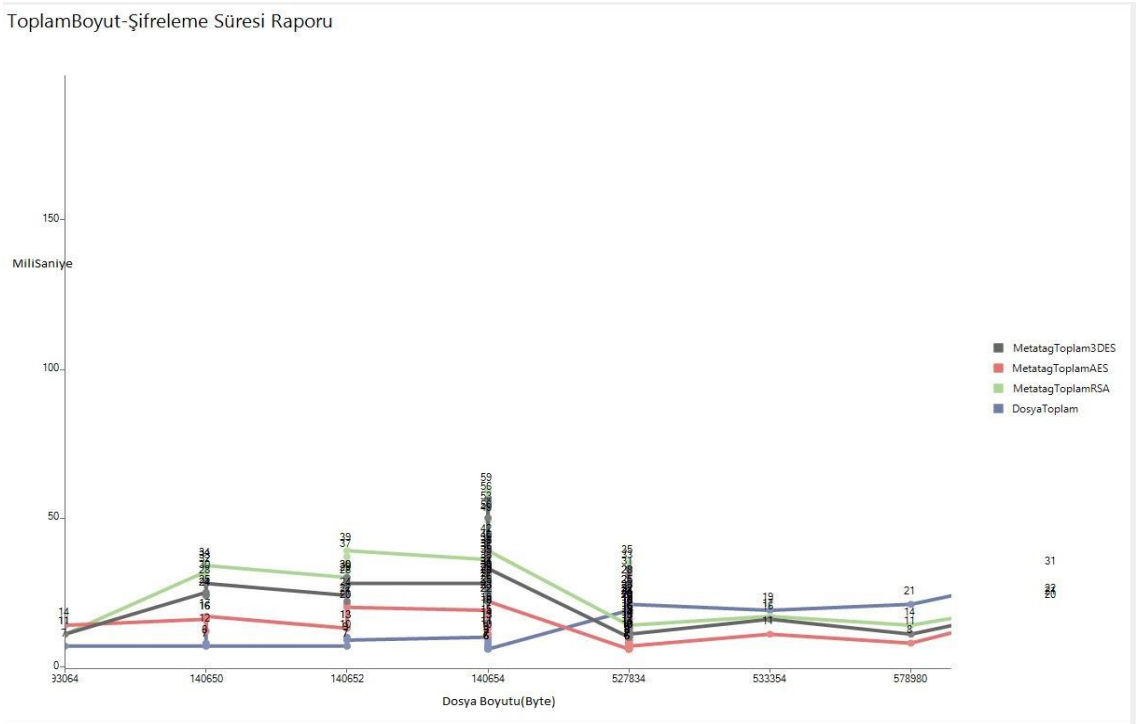
Şekil 4.40 da dosya boyutu 1157484 byte'tan büyük verilerde şifreleme yöntemlerindeki etkileri gösterilmiştir. Buna göre; dosya boyutunun artması etiket ile şifreleme yöntemlerindeki sürelerde küçük farklarda artışlara sebep olurken; dosya olarak şifreleme sürelerinde; özellikle 2922616 byte'tan sonraki verilerde yüksek oranlarda artışların olduğu görülmüştür.



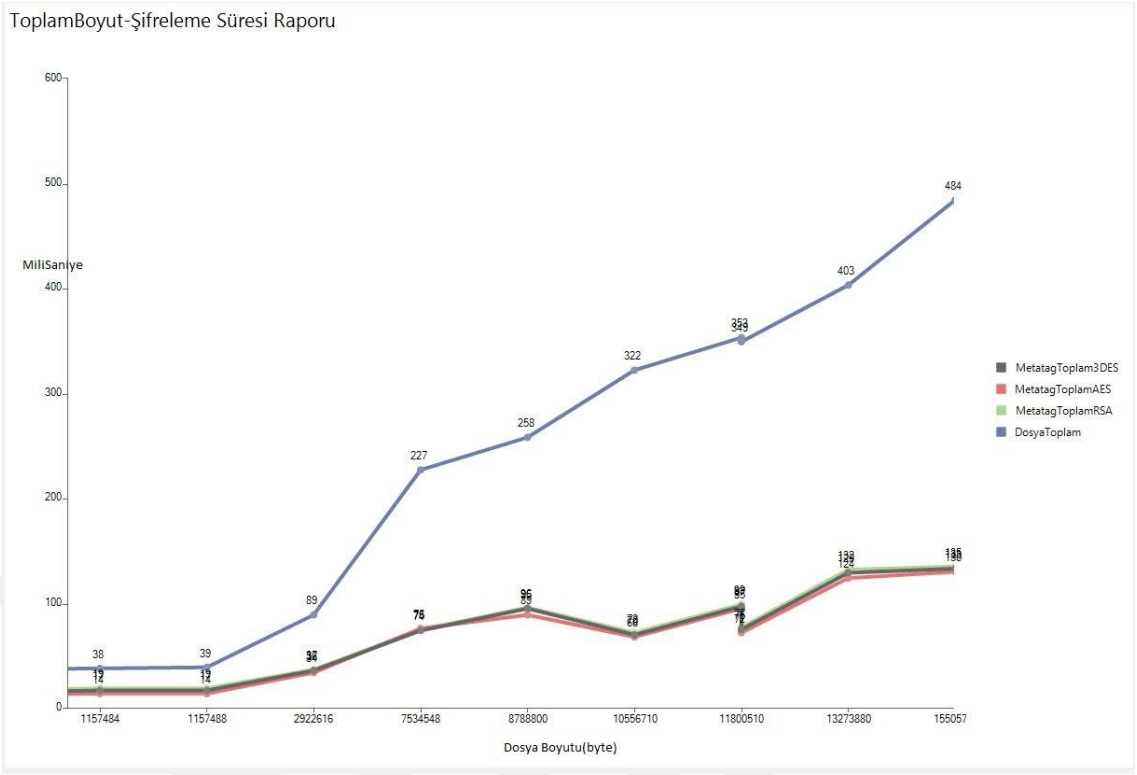
Şekil 4.37: Modalite bazında Dosya Boyutu.



Şekil 4.38: Dosya boyutunun şifreleme yöntemlerinde etkileri.



Şekil 4.39: Dosya Boyutunun şifreleme yöntemlerindeki etkileri (MR DICOM verilerinde).



Şekil 4.40: Dosya Boyutunun şifreleme yöntemlerindeki etkileri (dosya boyutu 1157484 byte'tan büyük verilerde).

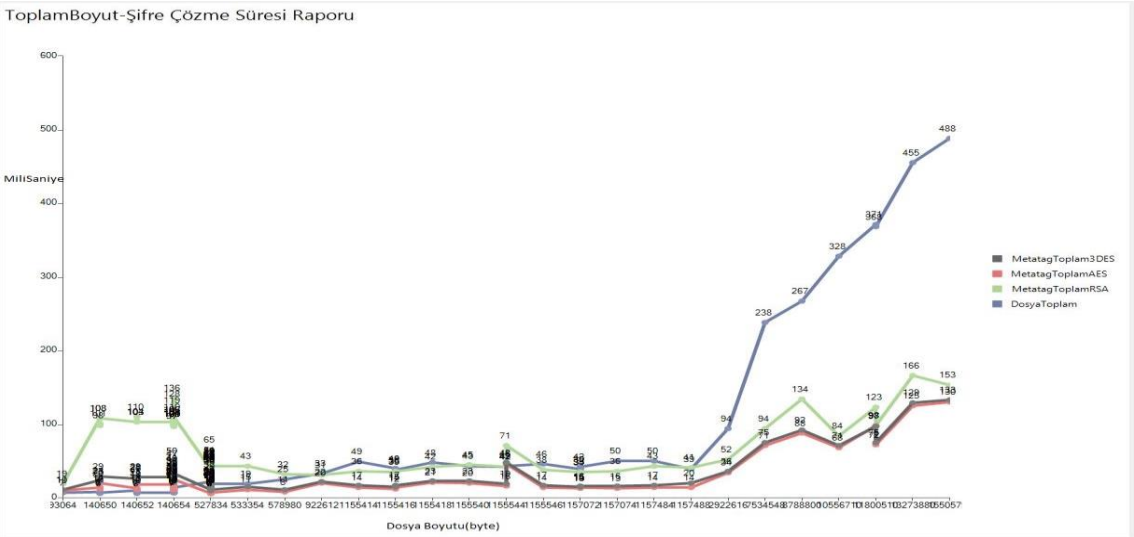
4.12. DOSYA BOYUTUNUN ŞİFRE ÇÖZME ÜZERİNDEKİ ETKİLERİ

DICOM dosya boyutu azdan çoğa sıralandığında dosya olarak şifre çözme, 3DES,AES, RSA şifre çözme sürelerinde etkileri Şekil 4.41 'de gösterilmiştir. Şifre çözme için kullanılan dosya olarak şifre çözme ve 3DES, AES, RSA ile etiket şifre çözme yöntemlerinde; genel olarak dosya boyutunun artması şifre çözme sürelerinin artmasına sebep olduğu gözlemlenmiştir.

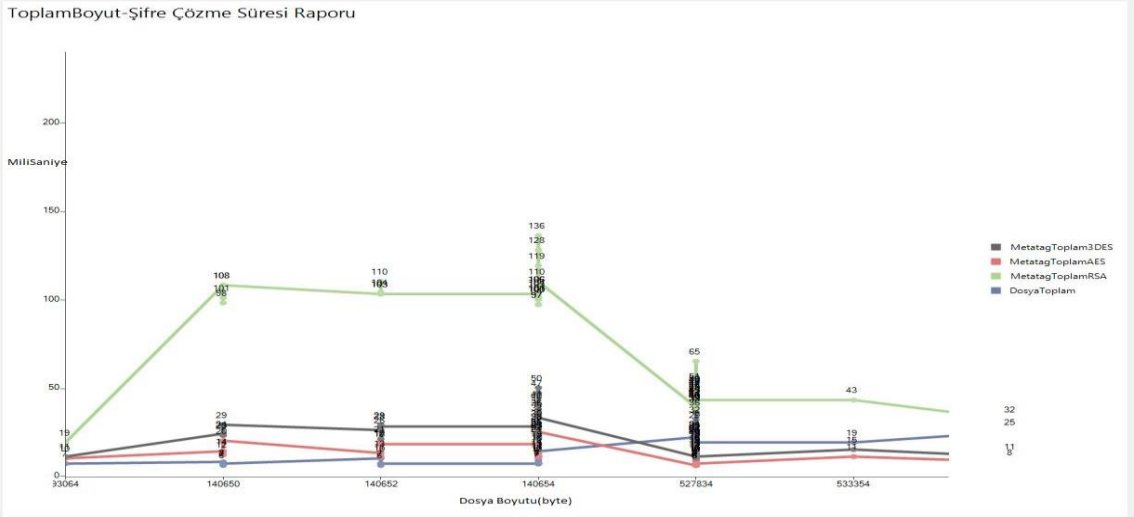
Şekil 4.42'de MR DICOM verilerinde dosya boyutunun şifre çözme yöntemlerindeki etkileri gösterilmiştir. Buna göre; dosya boyutu 527834 byte'a kadar olan veriler için; dosya olarak şifre çözme yöntemleri etiket şifre çözme yöntemlerine göre daha hızlı olduğu gözlemlenmiştir. Ancak 527834 byte'tan büyük dosyalar için; dosya olarak şifre çözme 3DES ve AES etiket şifre çözmeden daha yavaş olduğu görülmektedir. Şifrelemeden farklı olarak RSA ile etiket şifre çözme dosya boyutu 922612 byte'tan

büyük olan verilerde dosya şifre çözmeden daha hızlı olduğu görülmüştür. Dosya boyutu 527834 byte'a kadar olan verilerin MR modaliteye ait olduğu görülmüştür.

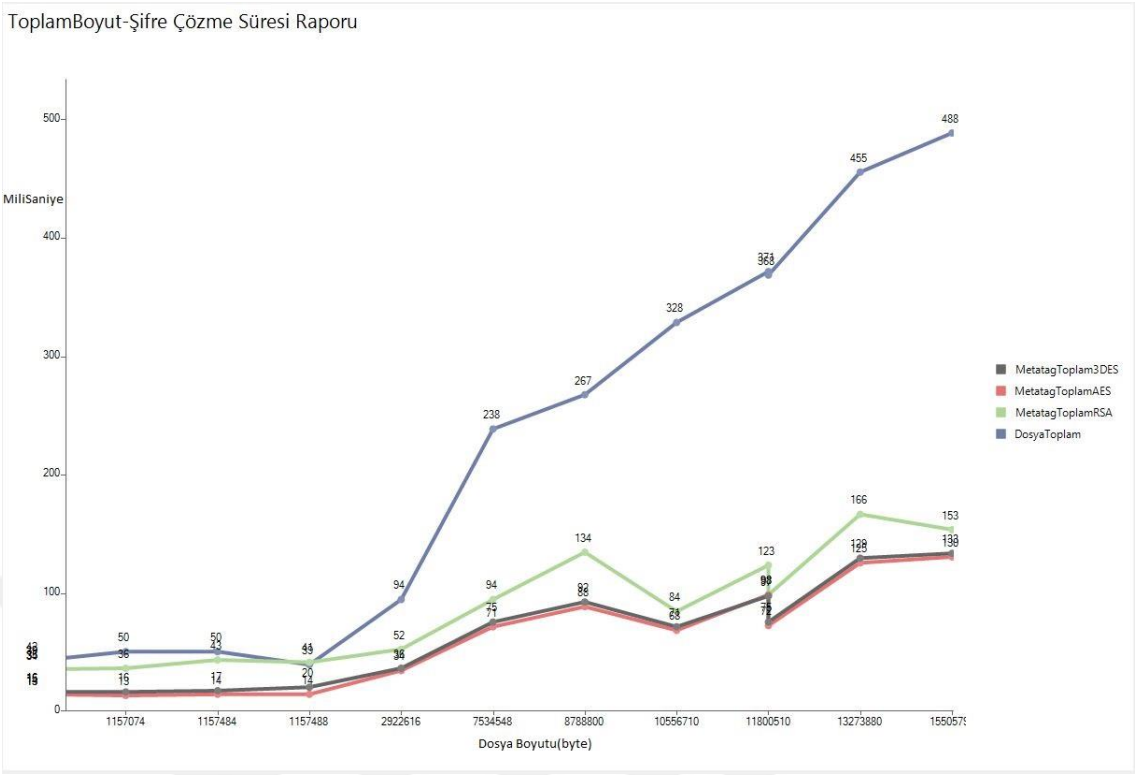
Şekil 4.43'te dosya boyutu 1157484 byte'tan büyük verilerde şifre çözme yöntemlerindeki etkileri gösterilmiştir. Buna göre; dosya boyutunun artması etiket ile şifre çözme yöntemlerindeki sürelerde küçük farklarda artışlara sebep olurken; dosya olarak şifreleme sürelerinde; özellikle 2922616 byte'tan sonraki verilerde yüksek oranlarda artışların olduğu görülmüştür.



Şekil 4.41: Dosya boyutunun şifre çözme yöntemlerinde etkileri.



Şekil 4.42: Dosya Boyutunun şifre çözme yöntemlerindeki etkileri (MR DICOM verilerinde).



Şekil 4.43: Dosya boyutunun şifre çözme yöntemlerindeki etkileri (dosya boyutu 1157484 byte'tan büyük verilerde).

4.13. DICOM ŞİFRELEME PERFORMANS ANALİZİ

Tez çalışmasının etkinliğini göstermek için, hastane işleyişi içinde yapılan birçok tetkikler sonucu elde edilen modaliteler üzerinde DICOM şifrelemenin etkisi incelenmiştir. Bilindiği gibi, DICOM dosyasının şifrelenerek saklanması hastane işleyişlerinde performans kayıplarına neden olmaktadır. Bu kayıpların belirlenmesi için bu çalışmada; kullanılan şifreleme yöntemlerinin küçük, orta ve büyük ölçekli hastane ortamlarındaki yıllık modalite bazında yaklaşık tetkik sayısı ile şifreleme sürelerinin çarpımları hesaplanarak performans analizi yapılmıştır. Tablo 4.1'de modalite bazında şifreleme ve şifre çözmede harcanan ortalama süreleri (milisaniye cinsinden); Tablo 4.2'de küçük, orta, büyük ölçekli hastane ortamlarındaki yıllık modalite bazında yaklaşık tetkik sayıları; Tablo 4.3'te DICOM Dosya Şifreleme Süresinin yıllık bazda Hastane etkisi (dk cinsinden); Tablo 4.4'te DICOM 3DES Şifreleme Süresinin yıllık bazda Hastane etkisi (dk cinsinden); Tablo 4.5'te DICOM AES Şifreleme Süresinin yıllık bazda

Hastane etkisi (dk cinsinden) ve Tablo 4.6'da DICOM RSA Şifreleme Süresinin yıllık bazda Hastane etkisi (dk cinsinden) gösterilmiştir.

Tablo 4.1: Modalite bazında şifreleme ve şifre çözmede harcanan ortalama süre (ms)

Modalite	CR	CT	DX	EK	IO	MG	MR	OT	US
Dosya Olarak Şifreleme Süresi	634	39	914	183	81	525	16	650	39
3DES Şifreleme Süresi	164	27	262	72	39	187	55	141	32
AES Şifreleme Süresi	163	24	258	70	36	181	44	139	33
RSA Şifreleme Süresi	188	59	292	89	61	230	141	156	41

Tablo 4.2: Küçük, orta, büyük ölçekli hastane ortamlarındaki yıllık modalite bazında yaklaşık tetkik sayısı

Hastane	Yatak S.	CR	CT	DX	EK	IO	MG	MR	OT	USG	TOPLAM
BÜYÜK ÖLÇEKLİ HASTANE	377	201.920	84.228	217.024	60.000	16.000	18.096	80.748	6.000	153.144	837.537
ORTA ÖLÇEKLİ HASTANE	175	148.224	23.304	50.000	20.000	7.000	9.600	22.176	2.300	19.080	301.859
KÜÇÜK ÖLÇEKLİ HASTANE	100	87.672	20.000	100.000	7.000	3.000	2.904	12.840	700	35.196	269.412

Tablo 4.3: DICOM dosya şifreleme süresinin yıllık bazda Hastane etkisi (dk cinsinden)

Hastane	Yatak S.	CR	CT	DX	EK	IO	MG	MR	OT	USG	T. DK
BÜYÜK ÖLÇEKLİ HASTANE	377	2.134	55	3.306	183	22	158	22	65	100	6.043
ORTA ÖLÇEKLİ HASTANE	175	1.566	15	762	61	9	84	6	25	12	2.541
KÜÇÜK ÖLÇEKLİ HASTANE	100	926	13	1.523	21	4	25	3	8	23	2.547

Tablo 4.4: DICOM 3DES şifreleme süresinin yıllık bazda Hastane etkisi (dk cinsinden)

Hastane	Yatak S.	CR	CT	DX	EK	IO	MG	MR	OT	USG	TOPLAM
BÜYÜK ÖLÇEKLİ HASTANE	377	552	38	948	72	10	56	74	14	82	1.846
ORTA ÖLÇEKLİ HASTANE	175	405	10	218	24	5	30	20	5	10	728
KÜÇÜK ÖLÇEKLİ HASTANE	100	240	9	437	8	2	9	12	2	19	737

Tablo 4.5: DICOM AES şifreleme süresinin yıllık bazda Hastane etkisi (dk cinsinden)

Hastane	Yatak S.	CR	CT	DX	EK	IO	MG	MR	OT	USG	TOPLAM
BÜYÜK ÖLÇEKLİ HASTANE	377	549	34	933	70	10	55	59	14	84	1.807
ORTA ÖLÇEKLİ HASTANE	175	403	9	215	23	4	29	16	5	10	716
KÜÇÜK ÖLÇEKLİ HASTANE	100	238	8	430	8	2	9	9	2	19	725

Tablo 4.6: DICOM RSA şifreleme süresinin yıllık bazda Hastane etkisi (dk cinsinden)

Hastane	Yatak S.	CR	CT	DX	EK	IO	MG	MR	OT	USG	TOPLAM
BÜYÜK ÖLÇEKLİ HASTANE	377	633	83	1.056	89	16	69	190	16	105	2.256
ORTA ÖLÇEKLİ HASTANE	175	464	23	243	30	7	37	52	6	13	875
KÜÇÜK ÖLÇEKLİ HASTANE	100	275	20	487	10	3	11	30	2	24	862

5. TARTIŞMA VE SONUÇ

Bu çalışmada; tıbbi görüntüleme sistemlerinde kullanılan DICOM formatının saklanmasında uygulanan yöntemler incelenmiştir. Bu yöntemlere ek olarak DICOM'un dosya olarak şifreleme ve şifre çözme yöntemi ile DICOM formatının image ve veri kısımlarını ayırarak hasta mahremiyetini oluşturan veri kısmı güvenliği etiket şifreleme ve şifre çözme yöntemleri kıyaslanmıştır. Etiket şifrelemede ise; 3DES ile etiket şifreleme ve şifre çözme yöntemi, AES ile etiket şifreleme ve şifre çözme yöntemi ve RSA ile etiket şifreleme ve şifre çözme yöntemi tercih edilmiştir.

Bu kıyaslamalar bulgular kısmında görüldüğü gibi;

Test verilerinde Şekil 4.3 incelendiğinde; Etiket şifreleme yöntemlerinde AES ile etiket şifreleme yöntemi 3DES ve RSA ile etiket şifreleme yöntemine göre daha performanslı olduğu söylenebilir.

Etiket Şifrelemeye benzer bir şekilde; etiket şifre çözme yöntemlerinde de AES ile etiket şifre çözme yöntemi 3DES ve RSA ile etiket şifre çözme yöntemine göre daha performanslı olduğu söylenebilir.

Bu çalışmada; DICOM formatının tamamının şifrelenmesi ile ilgili çalışma yapıldığından; dosya şifreleme yöntemi ile etiket şifreleme yöntemlerinde geçen toplam süre hesap edilmelidir. DICOM şifreleme yöntemlerinden dosya olarak şifrelemede DICOM'u okuma ve etiketlerini okuma süreleri olmadığından doğrudan dosya şifreleme süresi alınmıştır. Etiket şifreleme 3DES, AES, RSA da ise DICOM'u şifrelemek için toplam harcanan süre, DICOM okuma süresi, etiket okuma süresi ve şifreleme sürelerinin toplamından oluşmaktadır.

Şekil 4.7 incelendiğinde; dosya olarak şifreleme yöntemi RSA ile etiket şifreleme yöntemine yakın olmasına rağmen; genel olarak en yavaş etiket şifreleme yönteminin bile dosya olarak şifrelemeden daha hızlı olduğu sonucuna varılabilir.

Şifre çözme içinde dosya şifreleme yöntemi ile etiket şifreleme yöntemlerinde geçen toplam süre hesap edilmiştir. Buna göre Şekil 4.10 incelendiğinde; şifrelemeden farklı olarak; test verilerinin genelinde dosya olarak şifre çözme; RSA ile etiket şifre çözmeden hızlı olmasına rağmen; 3DES ve AES ile etiket şifre çözmeden daha yavaş olduğu sonucuna varılabilir.

Dosya olarak şifrelemeye alternatif olarak önerilen etiket şifreleme yöntemlerinde ise; toplam sürelerde etkili olan etiket okuma süresi, DICOM okuma süresi, şifreleme sürelerinin etkilerinin incelendiğinde;

Şekil 4.15'te 3DES ile etiket şifreleme yönteminde DICOM okuma süresinin ortalama olarak şifrelemenin toplam süresinin belirlenmesinde etkili olduğu sonucuna varılabilir. Etiket okunma süresi, DICOM okuma süresi ve etiket şifreleme süreleri ile yüzdelik dilime kıyaslandığında %0'a yakın olduğundan ihmal edilebilir seviyelerde olduğu söylenebilir.

Şekil 4.16'da AES ile etiket şifreleme yönteminde ise; AES ile etiket şifreleme diğer şifreleme yöntemlerine göre daha hızlı olduğundan; etiket şifreleme süresinin yüzdelik dilimini düşürmüştür. Bu yüzden DICOM okuma süresinin -ortalama olarak- şifrelemenin toplam süresinin belirlenmesinde, 3DES ile etiket şifrelemeye göre etkisini artırdığı sonucuna varılabilir. Etiket okunma süresi; DICOM okuma süresi ve etiket şifreleme süreleri ile yüzdelik dilime kıyaslandığında; %0'a yakın olduğundan ihmal edilebilir seviyelerde olduğu sonucuna varılmıştır.

Şekil 4.17 de ise; Etiket şifreleme yöntemlerinden en yavaşı olan; RSA ile şifreleme yönteminde ise DICOM okuma yüzdesine yaklaştığı görülmektedir. Ancak halen DICOM okuma süresinin yüzdeliği yüksek olduğu; genel toplamda 3DES ile etiket şifreleme ve AES ile etiket şifrelemedeki gibi DICOM okuma süresinin belirleyici olduğu sonucuna varılabilir.

Etiket şifre çözme yöntemlerinde toplam şifre çözme süresinde etkili olan adımı, tespit etmek için Şekil 4.18 incelendiğinde; 3DES ile şifre çözme yönteminde; şifrelemede olduğu gibi toplam süreyi, DICOM okuma süresinin baskın bir şekilde etkilediği sonucuna varılabilir.

Şekil 4.19 incelendiğinde; etiket şifrelemede diğer yöntemlere göre hızlı olan AES ile şifre çözme yönteminde şifrelemede olduğu gibi şifre çözme işlemi genel toplam üzerindeki etkisi azalarak DICOM okuma süresinin genel toplamda etkisinin arttığı sonucuna varılabilir.

Şekil 4.20 incelendiğinde RSA ile şifre çözme yönteminin şifrelemeden farklı olarak DICOM okuma süresinden3 kat fazla yüzdelikte olması, toplam sürede etiketlerin RSA ile şifre çözme süresinin etkili olduğu sonucunu ortaya çıkarmıştır.

DICOM verisi içerisinde modalite sayısına göre Şekil 4.21 incelendiğinde; Etiket sayısı 119'a kadar olan DICOM'lar için etiket şifrelemenin 3DES ile yapılması durumunda süre artışları tolere edilebilecek düzeylerde olduğu sonucuna varılabilir.

Etiket sayısının AES ile şifreleme yapılması durumunda; 3DES'e göre şifreleme sürelerinde daha az etkili olduğu sonucuna varılabilir. Etiket sayısı artması durumunda bile şifreleme sürelerinde artışın ihmal edilebilecek düzeylerde olduğu sonucuna varılabilir.

RSA ile etiket şifrelemede; etiket sayısının şifreleme süresi üzerinde doğrusal artışa yakın bir artışa sebep olduğu sonucuna varılabilir. RSA ile etiket şifrelemede etiket sayısının artması toplam süreyi doğrudan etkilediği sonucuna varılabilir.

DICOM verisi içerisinde modalite sayısına göre Şekil 4.22 incelendiğinde; Etiket sayısı 119'a kadar olan DICOM'lar için etiket şifre çözmenin AES ve 3DES ile yapılması durumunda süre artışları tolere edilebilecek düzeylerde olduğu sonucuna varılabilir. Ayrıca RSA ile etiket şifre çözmede etiket sayısının şifre çözme süresi üzerinde doğrusala yakın bir artışa sebep olduğu sonucuna varılabilir.

Modalite tiplerine göre dosya şifreleme ve etiket şifreleme yöntemlerinin toplam sürelerdeki etkilerini gösteren Şekil 4.23 incelendiğinde; Modalitesi CR, DX, US, MG, OT ve EK olan DICOM örneklerinden dosya şifrelemenin etiket şifreleme yöntemine göre daha uzun sürelerde olduğu; etiket şifrelemede ise; AES ile etiket şifrelemenin 3DES ve RSA ile etiket şifrelemeye göre az da olsa kısa sürelerde yapıldığı sonucuna varılabilir.

Şekil 4.32 ile Modalitesi CT, IO olan DICOM örnekleri ayrıntılı incelendiğinde; RSA ile etiket şifreleme süresi Dosya ile şifreleme süresine göre daha uzun süreler olmasına

rağmen AES ile etiket şifreleme tüm yöntemlerden daha kısa sürelerde olduğu sonucuna varılabilir.

Ancak diğer modalitelerden farklı olarak; modalitesi MRolan DICOM örneklerinde; Dosya şifreleme süresi tüm etiket şifrelemelerinden daha performanslı olduğu sonucuna varılabilir.

Çalışılan test verilerinde MR verilerinin dosya boyutu 527834 byte'tan küçük veriler olduğu görülmüştür. Buna göre Şekil 4.38 ve 4.39'dan anlaşılacağı gibi; dosya olarak şifreleme yöntemi 527834 byte' a kadar olan verilerde(örneğin MR verileri) etiket şifreleme yöntemlerinden daha performanslı olduğu sonucuna varılabilir.

Modaliteye göre şifre çözme yöntemlerinde de RSA ile etiket şifre çözme süreleri artmasına rağmen; modalitesi MR olan DICOM örnekleri haricinde; etiket ile şifre çözme yöntemi olan AES ile şifre çözme yönteminin daha performanslı olduğu sonucuna varılabilir. Şifrelemeye benzer bir şekilde; dosya olarak şifre çözme yöntemi 527834 byte' a kadar olan verilerde (örneğin MR verileri) etiket şifre çözme yöntemlerinden daha performanslı olduğu sonucuna varılabilir.

Bu çalışmada; esas olarak DICOM'u dosya olarak şifreleme ve şifre çözme ile etiket ile şifre çözme performansları kıyaslandığından şifre çözme algoritmaları üzerinden genel bir kıyaslamaya gidilmemiştir.

Metin şifreleme algoritmalarının kıyaslamaları sadece süre üzerinden yapılması uygun olmayacaktır. Ancak simetrik ve asimetrik şifreleme algoritmalarından örnek algoritmalar tercih edilmiştir.

Bu çalışmada multi kesit birbiriyle ilişkili DICOM nesneleri tek tek DICOM olarak alındığından; Multi kesit DICOM'lar için farklı performans testleri de yapılabilir. Modalitesi MR olan DICOM'lar haricinde DICOM güvenliği için etiket şifreleme kullanılabilir olarak görülmektedir. Her ne kadar etiket sayısı şifreleme algoritmalarının sürelerini etkilese de etiket şifreleme efektif çözüm olarak önümüze çıkmaktadır.

Bu çalışmada şifre çözme işleminde 95 DICOM verisi içerisinde herhangi bir bozulma görülmemiş olsa da; şifre çözmelerdeki bozulmalar etiket şifreleme yönteminin riski olarak görülebilir.

DICOM image verisi üzerinde herhangi bir işlem yapılmadığından image verisini de şifreleyen dosya şifreleme yöntemlerine göre image verisindeki veri kayıplarının önüne geçilebilir.

Ayrıca image verisinde literatürde yapılan çalışmalardaki gibi görüntü kayıplarının yaşanması tıbbi müdahale sürecine doğrudan etkileyeceğinden Malpraktis'e [(Malpractice) "bilgisizlik, deneyimsizlik ya da ilgisizlik nedeni ile bir hastanın zarar görmesi, hekimliğin kötü uygulanmasıdır" (Türk Tabipleri Birliği Hekimlik Meslek Etiği Kuralları, md.13)] sebebiyet verebileceğinden veri güvenliğini daha az kritik olarak görülmesine sebebiyet vermektedir.

Ayrıca anahtar(Key) paylaşımı ile şifrelenmiş DICOM verisinin gönderim ve yayınlama yöntemlerinin tamamına uygun olarak etiket şifreleme yöntemi kullanılabilir.

DICOM şifrelemenin hastane işleyişine etkisi bulguları incelendiğinde; bu çalışmada kullanılan tüm şifreleme yöntemlerinde; yıllık bazda hastane tetkik sayıları ile dakikalar seviyelerinde gecikmelere neden olduğu görülmektedir. Ancak burada yöntemlerin avantajları dezavantajları da değerlendirildiğinde; görüntü verisindeki bozulmaları ciddi geri dönüşü olmayan sonuçlar doğurabileceğinden etiket şifreleme yöntemi tercih edilebilir. Etiket şifrelemede en performanslı olan AES şifreleme olsa da yıllık bazda diğer yöntemlerin de dakikalar cinsinden etkileri düşünüldüğünde; 3DES ve RSA şifreleme de tercih edilebilir.

KAYNAKLAR

ACC/HIMSS/RSNA/IHE, 2006, *North America Connectathon and Demonstration Handbook*, IHE North America.

Al-Haj A., 2015, ProvidingIntegrity, Authenticity, and Confidentiality for Header and Pixel Data of DICOM Images, *Society for Imaging Informatics in Medicine*, 28:179–187.

Blomquist N., 2004, *File Encryption/Decryptionwith Hash Verification in C#*, https://www.codeproject.com/Articles/8633/File-Encryption-Decryption-with-Hash-Verification , [Ziyaret tarihi: 4 Ekim 2014].

Dzwonkowski M., Papaj M., and Rykaczewski R, 2015, A New Quaternion-Based Encryption Method for DICOM Images, IEEE Transactions On Image Processing, VOL. 24, NO. 11.

Gorthi, S.,Cuadra, M.B. and Thiran, J.P, 2009, Exporting Contours to DICOM-RT Structure Set, Signal Processing Laboratory (LTS5), *The Insight Journal* , .

Harsha T, Amarnath S, S Mahesh Reddy, 2011, *DICOM Image Viewer (Open Source)*, www.codeproject.com/script/Articles/ArticleVersion.aspx?aid=36014&av=209773, [Ziyaret tarihi: 4 Kasım 2015].

Kobayashi, L.O.M, Furuie, S.S and Barreto, P.S.L.M, 2009 , ProvidingIntegrity and Authenticity in DICOM Images: A NovelApproach, *IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE*, VOL. 13, NO. 4.

Kobayashi, L.O.M, Furuie, S.S, 2009, Proposal for DICOM Multiframe Medical Image Integrity and Authenticity, *Journal of Digital Imaging*, Vol 22, No 1.

Larsen, G.P. and Toubro Limited, 2012, DICOM Medical Image Management the Challenges and Solutions: Cloud as a Service (CaaS), *Computing Communication & Networking Technologies (ICCCNT)*, 26-28 July 2012 Coimbatore India, Mysore.

McEvoy F.J. and Svalastoga E., 2007, Security of Patient and Study Data Associatedwith DICOM ImageswhenTransferred Using Compact Disc Media, *Journal of Digital Imaging(IHE)*, Vol 22, No 1.

National Electrical Manufacturers Association, 2004, *Part 3: Information Object Definitions*, Digital Imaging and Communications in Medicine, Rosslyn, Virginia 22209 USA, National Electrical Manufacturers Association, PS 3.3.

Parisot C., 2005, *Leveraging IHE to build RHIO Interoperability*, http://ihe.univ-rennes1.fr/data/editable/organization/PCC_WS_2005/Interoperability_Workshop_IHEforRHIO-3.ppt, [Ziyaret Tarihi: 10 Eylül 2014]

Stites M., Pianykh O.S., 2016, How Secure Is Your Radiology Department? Mapping Digital Radiology Adoption and Security Worldwide, *AJR Am J Roentgenol*, 206(4):797-804.

Subhasri P., Dr. Padmapriya A., 2015, Enhancing the Securıty of DICOM content using modified VigenereCipher, *International Journal of Applied Engineering Research*, Vol. 10 No.55.

Tsai T.L., Pan M.L., Liou D.M., 2009, Implementation of an IHE ATNA-Based Electronic Health Record System, *Biomedical Informatics* , Sep. 2010 Institute of Public Health National Yang-Ming University No.155, Sec. 2, Linong St., BeitouDistrict Taipei City 112 Taiwan (R.O.C.).

Vazquez-Naya J. M., Loureiro J.P., de la Calle J.D., Vidal J.T. and Sierra A.P., 2002, Necessary Security Mechanisms in a PACS DICOM Access System with Web Technology,*Journal of Digital Imaging(IHE),* Vol 15 pp 107-111.

Weisser G., Engelmann U., Ruggiero S., Runa A., Schröter A., Baur S., Walz M., 2007, Teleradiologyapplicationswith DICOM-e-mail, *EurRadiol Computer Applications*, Vol 17: 1331–1340.

ÖZGEÇMİŞ

Kişisel Bilgiler	
Adı Soyadı	Çetin ŞAHİN
Doğum Yeri	ISPARTA/MERKEZ
Doğum Tarihi	10.03.1984
Uyruğu	☑ T.C. ❒ Diğer:
Telefon	0505 548 8404
E-Posta Adresi	cetins32@gmail.com
Web Adresi	https://www.linkedin.com/in/cetinsahin34/

Eğitim Bilgileri	
Lisans	
Üniversite	İstanbul Üniversitesi
Fakülte	Mühendislik Fakültesi
Bölümü	Bilgisayar Mühendisliği
Mezuniyet Yılı	13.07.2007

Yüksek Lisans	
Üniversite	İstanbul Üniversitesi
Enstitü Adı	Fen Bilimleri Enstitüsü
Anabilim Dalı	Bilgisayar Mühendisliği Ana Bilim Dalı
Programı	Bilgisayar Mühendisliği
Mezuniyet Tarihi	08.06.2017