DÜMF Mühendislik Dergisi

web: http://dergipark.gov.tr/dumf

Araştırma Makalesi / Research Article

İmge Şifreleme Yöntem ve Algoritmaları

Nur Sena ATALAY*
Fırat Üniversitesi, Adli Bilişim Mühendisliği Bölümü, Elazığ
nursena.atalay@gmail.com ORCID: 0000-0003-2053-7393, Tel: (424) 237 00 00

Şengül DOĞAN, Türker TUNCER, Erhan AKBAL
Fırat Üniversitesi, Adli Bilişim Mühendisliği Bölümü, Elazığ
sdogan@firat.edu.tr , turkertuncer@firat.edu.tr , erhanakbal@firat.edu.tr ORCID: orcid.org/0000-0001-9677-5684, orcid.org/0000-0002-1425-4664, orcid.org/0000-0001-9677-5684

Geliş: 05.11.2018, Revizyon: 05.04.2019, Kabul Tarihi: 28.05.2019

Öz

Teknolojinin gelişimine bağlı olarak, dijital görüntülerin internet üzerinden aktarılması oldukça yaygınlaşmıştır. Kişisel verilerin korunması açısından çeşitli kamu ve resmi alanlarda kullanılan dijital görüntülerin internet üzerinden aktarımını sağlarken yüksek derecede verilerin korunmasını, veri bütünlüğünün ve gizliliğinin sağlanması gerekmektedir. Dijital görüntülerin aktarımının güvenliği ve gizliliğinin sağlanması, genel olarak çeşitli şifreleme algoritmaları ile anahtarlı ve anahtarsız olarak gerçekleşmektedir. Günümüzde, görüntü güvenliği her geçen gün daha da önemli hale gelmektedir. Bunun nedenlerinin başında, gizli görüntülerin kamuya internet üzerinden aktarılıyor olması ve iki kişi arasında yapılan bu aktarıma üçüncü bir şahsın da erişebiliyor olmasıdır. Bu bağlamda, şifreleme, özel bilgilerin güvenliğini sağlamak için etkili ve doğrudan bir teknik olarak kabul edildiğinden, çeşitli görüntü şifreleme sistemleri önerilmiştir. Mimarilere göre, şifrelemeye yönelik yöntemler üç ayrı kategoriye ayrılabilmektedir. Bunlar permütasyon, yer değiştirme, permütasyon ve yer değiştirme olarak kategorize edilmektedir. Bu çalışmada özel bilgilerin güvenliğini sağlamak amacıyla oluşturulan ve yaygın kullanılan bazı imge şifreleme algoritmalarının çalışma yapısı ve mantığı incelendi ve algoritmalar arası performanslar karşılaştırmalı bir şekilde sunuldu. Bu çalışmanın asıl amacı, kişisel bilgilerin güvenliğinin sağlanmasında kullanılan bu imge şifreleme algoritmalarının çalışma yöntemi ve metodolojisini karşılaştırarak, algoritmalar arası farkındalığı ortaya koymaktır.

Anahtar Kelimeler: *İmge şifreleme, Kişisel verilerin gizliliği, İmge şifreleme yöntem ve metodolojisi*

* Yazışmaların yapılacağı yazar

DOI: 10.24012/dumf.478877

Giriş

Günümüzde aklımıza gelebilecek her alan internet kullanımı ile gerçekleşmektedir. İnternet alışverişleri, veri aktarımı, iş yerleri, okullar vb. birçok alanda veri alışverişi internet üzerinden yapılmaktadır. İşlemlerin tamamı kişisel bilgiler, kredi kartı numaraları vb. kullanılarak kişisel bilgilerin paylaşılmaması ve güvenliğinin iyi sağlanması gereken olgular ile gerçekleşmektedir. İnternet kullanıcılarının günden güne artan sayısı ile internet üzerinden iletilen her veri, başka bir kişinin kötü niyetli bir şekilde zarar görmesinden dolayı tehdit altındadır. Sistem ağına gönderilen verilere güvenlik sağlamak için ağ güvenliği yetersiz kalmaktadır. Büyüyen teknoloji ile bilgisayar korsanları, teknolojiyi ve onu ele geçirme yollarını her geçen gün biraz daha farklı teknikler ile gerçekleştirmektedir. Güvenliği sağlamak için tek yol, üçüncü şahısların önemli bilgilerin varlığı hakkında bilgi sahibi olmamasını sağlamaktır. Dijital damgalar, görsel kriptografi, steganografi gibi bilginin korunması amacıyla birçok teknik geliştirilmiştir ve bunun yanı sıra araştırmacılar görüntü verisinin korunması ile ilgili birçok farklı teknik geliştirmişlerdir. 20. yüzyılın sonunda, çeşitli alanlardaki belgeler ve ekipmanların artan kullanımından ötürü, analogdan sayısal analize kadar olağanüstü bir teknik devrime damgasını vurmuştur. Bununla birlikte, dijital devrimin avantajları, dijital multimedya belgelerinin yasadışı kopyalanması ve dağıtılması gibi dezavantajlar olmaksızın gerçekleştirilememiştir. Bu zorluğu gidermek için, araştırmacılar multimedya dokümanlarını yeni ve etkili belge koruma teknikleriyle korumak için daha çok teknik geliştirmeye yönelik çalışmışlardır. Bu bağlamda, şifreleme ve dijital damgalama gibi farklı teknikler üretilmiştir. Bunlardan ilki olan algoritmalar, yasal kullanıcılar dışındaki herkes tarafından okunamaz hale getirmek için geliştirilmiştir. İkincisi, dijital multimedya içeriklerinin sahipliğini ve bütünlüğünü garanti altına almak için dijital filigranları multimedya belgelerine yerleştirmekten ibarettir. Özel anahtar şifreleme standartları (DES ve AES) gibi geleneksel görüntü şifreleme algoritmaları, Rivest Shamir Adleman (RSA) gibi kamu anahtar standartları, eliptik eğri tabanlı şifreleme (ECC) ailesi ve uluslararası veri şifreleme algoritması (IDEA), özellikle hızlı ve gerçek zamanlı iletişim uygulamaları görüntü şifrelemesi için en çok kullanılan algoritmalar arasında yer almaktadır. Kişisel bilgi ve verilerin korunması açısından ve çeşitli özel kamu ve sektör alanlarında kullanılan dijital görüntü ve bilgilerin sanal ortamda aktarımını sağlarken verilerin korunması, veri bütünlüğünün ve gizliliğinin sağlanması gerekmektedir. Son yıllarda, yeni pek çok şifreleme tekniği üzerine çalışılmıştır ve bu şifreleme şemaları, değer dönüşümü, piksel konum permütasyonu, kaotik sistemler, XOR işlemleri gibi farklı kategorilere ayrılmaktadır. Sanal ortamda gerçekleşen bu aktarımda görüntülerin güvenliği ve gizliliğinin sağlanması, genel olarak çeşitli şifreleme algoritmaları ile anahtarlı ve anahtarsız olarak gerçekleşmektedir. Bu çalışmada, sanal ortamda aktarımının sağlandığı dijital görüntülerin gizliliğinin ve bütünlüğünün korunması üzerine kullanılan ulusal ve uluslararası literatür taraması çalışmaları incelenmiştir. Kumari ve arkadaşları tarafından hazırlanan çalışmada, imge şifreleme teknikleri ve bu tekniklerin çalışma mantığı, diferansiyel, istatistiksel ve kantitatif atak analizleri gibi çeşitli performans ölçümleri üzerine bir çalışma sunulmuştur (Kumari vd., 2017). Kumar ve Srivastava tarafından hazırlanan çalışmada, kaotik haritalara dayanan bir dizi görüntü şifreleme algoritması üzerine bir çalışma yapılmıştır (Kumar ve Srivastava, 2014). Parvaz ve Zarebnia çalışmada, kaotik sistemin geliştirilmesi ve analizi üzerine bir çalışma yürütmüştür (Parvaz ve Zarebnia, 2017). Bao ve Zhou tarafından hazırlanan çalışmada, yeni bir görüntü şifreleme sistemi oluşturulmuştur. Simülasyon sonuçları ve güvenlik analizi ile önerilen yöntemin şifreleme performans ölçümlerinin yapıldığı bir çalışma sunulmuştur (Bao ve Zhou, 2015).

Bu çalışmada özel bilgilerin güvenliğini sağlamak amacıyla oluşturulan ve yaygın kullanılan bazı imge şifreleme algoritmalarının çalışma yapısı ve mantığı incelenmiştir. Yapılan çalışma ile ilk olarak imge şifreleme kavramından bahsedilmiş sonraki bölümde imge şifrelemede kullanılan çeşitli algoritma ve

yöntemler açıklanmış ve karşılaştırmaları çeşitli istatistiksel grafikler ile gösterilmiştir. Sonraki bölümlerde görsel şifrelemenin güvenliğinin nasıl sağlandığı ve güvenlik analizi için kullanılan yöntem ve metriklerden bahsedilmiştir.

İmge Şifreleme

Bilgi toplumlar arasında korunması gereken önemli bir unsurdur. Roma imparatoru Sezar'dan günümüze bilginin korunması için geliştirilen birçok teknikler vardır. Her ne kadar bilginin güvenliğini sağlamak için birçok yol geliştirilmiş olsa da bilginin korunmasında ki en büyük yapı taşı bilginin gizlenmesi olmuştur. Bu bilimin adı kriptoloji olarak adlandırılmıştır. Teknolojinin gelişimine bağlı olarak günümüzde kullanılan iletişim ağları, çeşitli bankamatik işlemleri, cep telefonları, bilgisayar, internet ve hatta ulaşım gibi birçok alanda ağ üzerinden veri paylaşımı ve aktarımı yapılmaktadır. Bunlara bağlı olarak bu verilerin gizliliği, güvenliği ve veri bütünlüğünün sağlanması çeşitli şifreleme algoritması ile yapılmaktadır. Bu şifrelemenin kullanıldığı alanlardan biri de imge şifrelemedir. Kriptografik algoritmalar, verileri şifrelemek veya şifresini çözmek için anahtar olarak adlandırılan bir dizi karakter kullanımı gerektirir. Anahtar ve algoritma akışı yardımıyla şifreleme gerçekleştirilebilir. Şifreli metni, kendi içerisinde tekrar şifreleyebilir ve ardından metni tekrar düz metin haline getirebiliriz. Günümüzde bilgi güvenliği, veri depolama ve aktarımında daha önemli hale gelmektedir. Görüntüler farklı farklı süreçlerde yaygın olarak kullanılmaktadır. Bu nedenle, görüntü verilerinin yetkisiz kullanımlardan korunması önemlidir. Görüntü şifreleme, bilgi gizleme alanında önemli bir rol oynar. Bu nedenle, sunucu yöneticileri ve diğerleri dâhil olmak üzere 3. bir şahıs tarafından, internet gibi genel ağlar aracılığıyla orijinal mesaja ya da başka herhangi bir aktarılmış bilgiye erişim sağlayamaz. İmge şifrelemenin çeşitli gereksinimleri bulunmaktadır. Bunlar;

- Orijinal görüntünün piksellerini elde etme yeteneği
- Kolayca saldırıya uğramayacak şekilde güçlü bir şifreleme görüntüsü oluşturma
- Görüntünün şifrelenme süresi
- Şifre çözüldükten sonra resmin orijinalini elde edebilme gibi yeteneklerden oluşmaktadır.

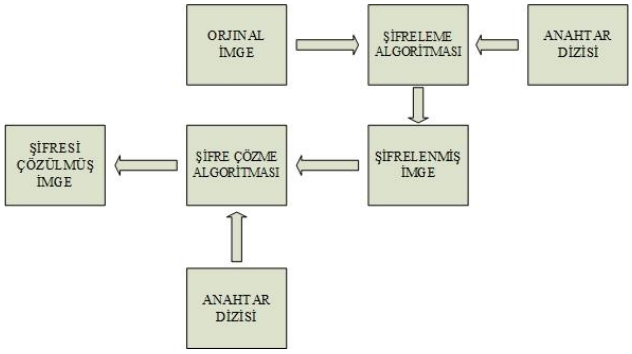
İmge Şifrelemede Kullanılan Algoritmalar

Görüntülerin güvenliği, günümüzde hala genişleyen dijital aktarım alanındaki önemli yönlerden biridir. Güvenliğin sağlanması için görüntülerin şifrelenmesi en çok kullanılan yöntemlerde biridir. İmge şifrelemede asıl amaç dijital görüntülerin güvenliğini arttırmak ve video, tıbbi görüntüleme sistemleri ve askeri görüntü aktarımları gibi çeşitli uygulamalarda güvenliği üst seviyede gerçekleştirebilmektir. Bu tür dijital aktarımlar saldırılara karşı savunmasızdır ve dolayısıyla güvenli veri aktarımı için etkin şifreleme algoritmaları gereklidir. Bugüne kadar literatürde çeşitli teknikler önerilmiş, (Kumari vd., 2017) her bir teknik giderek artan güvenlik ihtiyacına yetişebilmek için yetersiz kalmıştır. Bu teknikler, diferansiyel, istatistiksel ve kantitatif atak analizleri gibi çeşitli performans ölçütlerine dayanarak oluşturulmuştur. Dünya çapında çeşitli görüntü şifreleme teknikleri önerilmiştir fakat tekniklerin çoğu, diferansiyel ve istatistiksel ataklar dâhil olmak üzere ataklara karşı yetersiz kalmıştır. Aşağıda imge şifrelemede kullanılan algoritmalara birkaç örnek verilmiştir.

Vigenere Şifreleme Algoritması

Günümüzde yaygın olarak kullanılmayan geri dönüşümü kolay olan bir şifreleme türüdür (Kester, 2012). Kaydırma ve yerine koyma şifrelemesi gibi şifrelemelerden farkı şifrenin her bir harfe uygulanması yerine, her bir harf bloğuna uygulanması ile gerçekleşmektedir. Vigenere şifresi, şifreleme için bir dizi farklı şifrelerden oluşan bir tür poli-alfabetik şifrelemedir. Vigenere tablosu olarak da bilinen şeküler formda bir dizi eleman kullanılmaktadır. Vigenere tablosunda ki ilk satır, n farklı öğeden

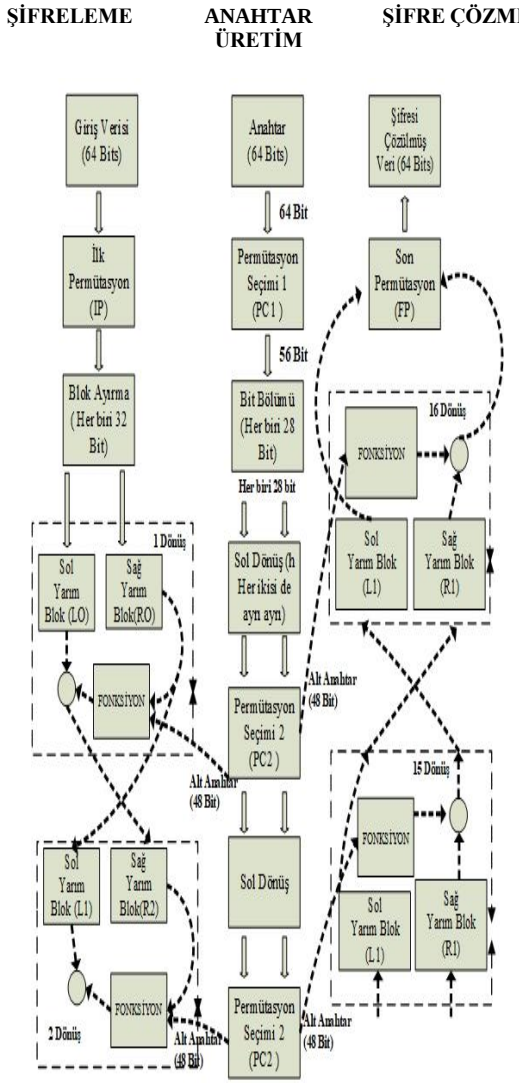
oluşur ve kalan tablo, her devam eden öğe için n-1 sıraya sahiptir. Aynı zamanda Vigenere şifrelemesinde birden fazla alfabe kullanılmaktadır. Şifreleme için bir anahtar seçilmektedir ve bu anahtara göre her harf farklı bir alfabeye göre şifrelenmektedir. Şifre çözme, anahtar elemanına karşılık gelen sıradaki şifreli öğeye bakılarak yapılabilir ve daha sonra sütun, şifresi çözülmüş çıktıyı, yani orijinal harfi temsil edecektir. Geleneksel olarak, Vigenere şifresi, Vigenere tablosunu kullanarak alfabetik metinleri şifrelemek için geliştirilmiştir, ancak son zamanlarda yapılan birçok çalışma, görüntü şifrelemesi için Vigenere`nin şifreleme yöntemini kullanmıştır. Bu teknikler, hem kaotik hem de kaotik olmayan tabanlı olarak kullanılmaktadır. Vigenere imge şifrelemesi için bir giriş görüntüsü alınmaktadır ve ardından Vigenere tablosunu ve anahtarını kullanarak şifreleme işlemi yapılmaktadır. Görüntü piksellerinin tamamı şifrelenene kadar anahtar değeri tekrarlanmaktadır. İmge şifrelemede kullanılan Vigenere algoritması blok diyagramı mantığı aşağıda Şekil1 ile gösterilmiştir.



Şekil 1 Vigenere Şifrelemesi Blok Diyagramı

DES (Data Encryption Standart – Veri Şifreleme Standardı)

Bir çeşit veri şifreleme standardı olan DES, 1970 yıllarında IBM'de geliştirilen ve daha sonra ulusal standartlar bürosu tarafından kabul edilen ve en hızlı blok şifreleme algoritmalarından biri olan şifreleme türüdür (Manjula ve Ravikumar, 2016). Şifrelenecek olan açık metni (Plain Text), parçalara bölerek (Blok) her parçayı birbirinden bağımsız olarak şifreler ve şifrenmiş metni (Cipher Text), açmak için de aynı işlemi bloklar üzerinde yapmaktadır. Bu bloklar 64 bit uzunluğumdadır. DES aynı zamanda 64 bit uzunluğunda bir anahtar almaktadır ancak 8 bit parite için kullanıldığı için bu anahtarın geçerli olan uzunluğu 56 bit olmaktadır. 64 bitlik bir giriş bloğu tek seferde 8 piksel alır ve buna ilk permütasyon (Initial Permutation) işlemi uygulanır. Geçirilen veriler daha sonra iki alt bloğa ayrılmaktadır bunlar L, R bloklarıdır. Bu alt bloklar, farklı 48 bit uzunluğunu kullanılarak on altı yuvarlak işlemden geçtikten sonra şifreli metni elde etme işlemi sonlanmış olur. DES algoritmasında gösterilen fonksiyon bloğu genişleme permütasyonunun (32–48 bit), xoring işlemi ve ardından sübstitüsyonun (48–32 bit) ve son olarak düz permütasyon kutusunun bir kombinasyonudur. İlk anahtar uzunluğu 64 bit olup, bunlardan 8 bit parite kontrolleri için ayrılmıştır. 64 bitten kalan bitler ile PC1 kullanılarak 56 bit kullanılabilir bit sayısı çıkartılmaktadır. Bu 56 bit veri iki yarıya bölünür ve 16 alt anahtar (56 bit anahtar) elde etmek için çeşitli zamanlarda döndürülür. Bu 56 bit alt anahtarlardan, 48 bit anahtarı (PC için yuvarlak anahtarlar için 16 anahtar) ayıklanır. Şifre çözme işleminde, şifreleme işlemine benzer bir yöntem izlemektedir, ancak alt anahtarların sırası tersine çevrilmektedir. Şifreleme ve şifre çözme süreçleri çok sayıda turda ilerlese de, DES güvenlik mekanizması birçok yönden kopabilmektedir. DES, imge şifreleme için piksel değişimleri ile kullanılan bir yöntemdir. İmge şifrelemede kullanılan DES şifreleme standardının blok diyagramı şifreleme mantığı aşağıda Şekil2 ile gösterilmiştir.

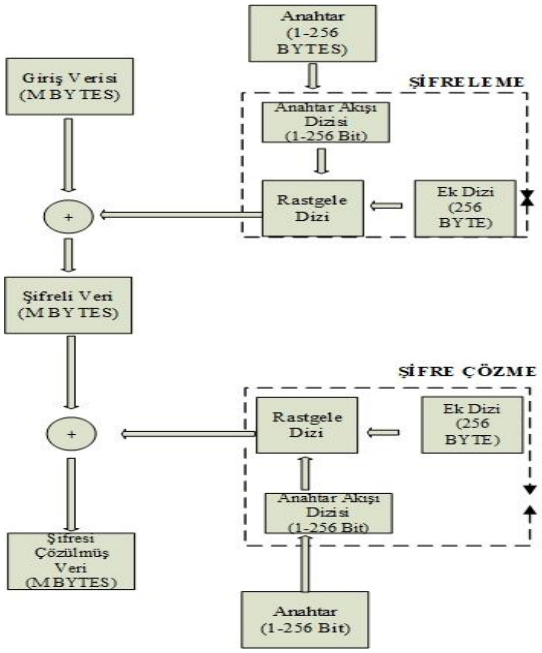


Şekil 2 DES Şifreleme Standardı Blok Diyagramı

RC4 Şifreleme Algoritması

RC4 şifreleme algoritması, oldukça hızlı ve basit bir simetrik anahtar, akış şifreleme türüdür. İlk olarak 1987 yılında ticari olarak tasarlanmıştır. Algoritma olarak, 1 - 256 bayt arasında (genellikle 5 ve 16 bayt arasında) değişen bir anahtar uzunluğu kullanır.

Anahtar değeri 256 baytlık bir anahtar elde etmek için tekrarlanmaktadır. Bu anahtarı, permütasyon işlevini ve rastgele diziyi kullanarak, düz metnin xoring işlemi ile şifrelenmesi için bir rastgele bayt dizesi üretir. Şifre çözme işlemi benzer bir yöntem izlemektedir. Karmaşık olmayan yapısı, hızı ve kolay uygulanabilir olmasına rağmen, algoritma birkaç zafiyete sahip olduğu için sınırlı olarak tanımlanmaktadır. RC4 şifreleme algoritmasının, diğer saldırı türlerine karşı güçlü olması için RC4A, Spritz gibi çeşitli varyantlar geliştirilmiştir. RC4 algoritmasının devamı niteliğinde RC5 VE RC6 şifreleme algoritmaları da bulunmaktadır. İmge şifrelemede kullanılan RC4 yönteminin blok diyagramı şifreleme mantığı aşağıda Şekil3 ile gösterilmiştir.



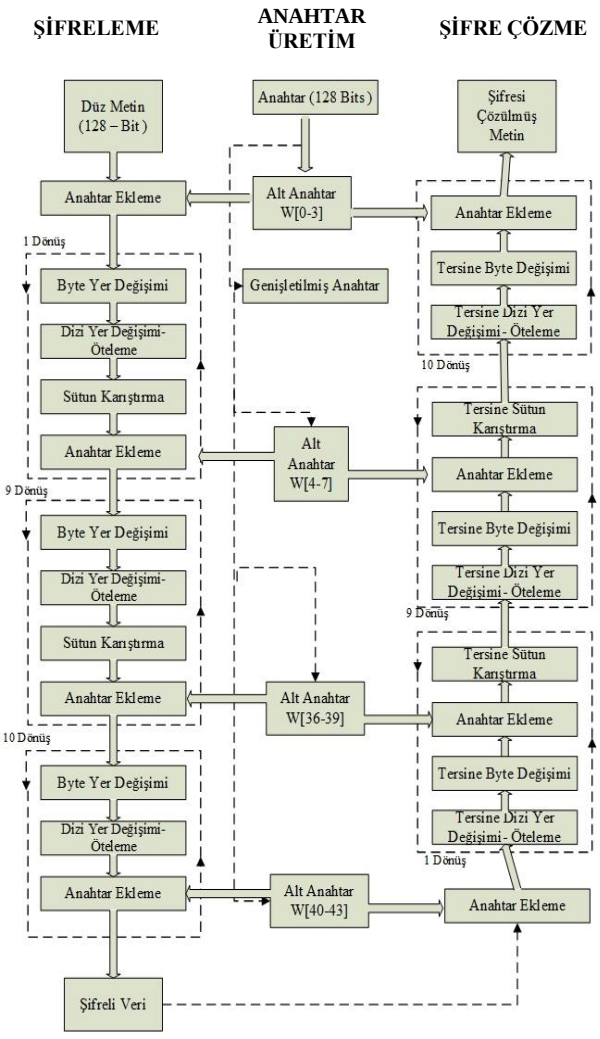
Şekil 3 RC4 Algoritması Blok Diyagramı

AES (Advanced Encryption Standard – Gelişmiş Şifreleme Standardı)

AES, Rijndael Joan Daemen ve Vincent Rijmen tarafından geliştirilen, Rijndeal şifreleme ailesine ait simetrik bir şifreleme algoritmasıdır (Zeghid vd., 2007). AES algoritması, verilerin 128, 192 ve 256 bitlik anahtar boyutunu desteklemektedir ve dört temel işlem bloğuna bölünebilen 128 bit veri uzunluğuna izin vermektedir. Bu bloklar bayt dizisi üzerinde çalışır ve durum olarak adlandırılan 4 × 4 matris olarak düzenlenir. Bloklar, 128-bitlik bir eşit blok boyutuna sahiptir fakat herhangi bir bit artışında güvenlik kuvveti artışını gösteren 128, 192, 256-bit'lik anahtar boyutları vardır.

Boyuttaki bu artış, daha yüksek seviyede bit kullanıldığında tekrarlama döngü sayısındaki

artışın bir sonucudur. Daha önceden yaygın olarak kullanılan DES, Fiestel ağına dayanırken; AES, bir yerleştirme ağı yapısı kullanır. Farklı şifreleme ve şifre çözme işlemleri, benzer bayt yerleşimlerini, değişim sırasını, karıştırma sütununu kullanır ve yuvarlak anahtar adımları ekler. AES algoritmasının üç kabul edilen versiyonunda çok benzer bir anahtar yöntemi vardır ve 128 bit sürümünde, 11 alt grupları gibi çok sayıda alt anahtar kullanılır. Çoğu AES sürümü, 4 9 4 matrisinden yararlanır, bu sayede şifrenin doğrusal olmayan etkisini verir ve boyut kuvvetine katkıda bulunur. Kaba kuvvet saldırısı en hızlı belgelenmiş saldırıdır ve dolayısıyla AES algoritmaları onlara karşı dayanıklı bir yapıya sahiptir. Şekil 4 ile imge şifrelemede kullanılan AES algoritmasının blok diyagramı göstermektedir.



Şekil 4 AES Algoritması Blok Diyagramı

Gizli Görüntülerin Anlamlı Görüntüler Olarak Şifrelenmesi İçin Oluşturulan İmge Şifreleme Algoritması

Son yıllarda, bulut ve internet tabanlı hizmetler dünya çapında çok popüler hale gelmiştir ve pek çok kişi bu hizmetleri bilinçsiz bir şekilde kullanmaktadır. Bu olgu, çevrimiçi verilerin gizliliğini bireyler ve kuruluşlar açısından daha da önemli bir konu haline getirmektedir ve verilerin korunması, önemli bir araştırma alanı haline gelmektedir. Şifreleme ve stenografi dâhil olmak üzere bir dizi veri koruma yaklaşımı vardır. Şifreleme, verilerin şifrelenmesiyle yetkisiz erişimi engellemeyi hedeflerken, stenografinin ana amacı bir host / cover nesnesindeki verileri gizlemektir. Üçlü veri şifreleme standardı (3DES), Gelişmiş Şifreleme Standardı (AES) ve Uluslararası Veri Şifreleme gibi metin için tasarlanan bir dizi geleneksel şifreleme düzeni vardır. Dijital görüntüler ve diğer multimedya formatları, askeri, iş ve sağlık bakımı gibi sayısız hassas uygulamalarda gereklidir. Bu uygulamalar genellikle hassas verilerin depolanmasını ve aktarılmasını gerektirir. Son yıllarda çok sayıda hükümet, iş ve kişisel veri sızıntısı, gelişmiş güvenlik algoritmalarına olan artan ihtiyaçların altını çizmektedir. 3DES, AES ve IDEA gibi geleneksel şifreleme algoritmaları, metin verilerini korumak için tasarlandığından, büyük boyutlarından dolayı dijital multimedya içeriğini koruma konusunda verimsizdirler. Son yıllarda, birtakım kriptanalitik ataklar önerilmiş ve daha önce bahsedilen görüntü şifreleme algoritmalarından bazıları bozulmuş ya da güvenlik kusurlarına sahip olduğu görülmüştür. Kriptanaliz olasılığını azaltmak için, oluşturulan şifreleme görüntüleri rastgele görünmeyen bir şifreleme şemasına ilgi duyulabilir. 2015 yılında, kayıpsız görsel olarak anlamlı imge şifreleme şeması önerilmiştir. Önerilen şema iki aşamadan oluşmaktadır. Birinci aşama, ön işlem ikinci aşama veri gömme olarak tanımlanmaktadır. Ön işleme aşaması, rastgele bir görüntü oluşturmak için gibi mevcut bir düzeni kullanarak giriş düz görüntüsünü şifreler. Bu aşamanın amacı

önerilen planın güvenlik seviyesini arttırmaktır. Böylece, eğer gizli görüntü çok hassas değilse, bu aşama atlanabilir. Bu çalışmanın ana katkısı olan yerleştirme aşaması, frekans alanında gerçekleştirilir. 2D Ayrık Dalgacık Dönüşümü (LWT) kullanarak ana görüntüyü dört alt-bant, yani bir yaklaşım matrisi ve üç detay matrisi halinde ayrıştırır. Daha sonra ön işlem aşamasından kaynaklanan (karıştırılmış) görüntüyü ayrıntı katsayılarına karıştırır. Son olarak, nihai stego-image ters dönüşüm yoluyla üretilir. Simülasyon sonuçları, önerilen planın yüksek kaliteli stego images ürettiğini ve bir dizi güvenlik tehdidine karşı sağlam olduğunu göstermektedir. Bao ve Zhou yöntemi 2015 yılında Bao ve Zhou tarafından önerilmiş (Yang vd., 2017) ve literatürde bilinen ilk VMIES (Visually Meaningful Image Encryption Scheme) metodudur (Bao ve Zhou, 2015). Ön şifreleme ve referans görüntü şifreleme bölümlerinden oluşur. Bu yöntemde, ön şifreleme yönteminin literatürdeki güvenli görüntü şifreleme yöntemlerinden birini kullanabileceği açıkça görülmektedir. Yöntemin özgünlüğü referans görüntü şifrelemesidir. BZ referans görüntü şifreleme yöntemi Tablo 1'de verilmiştir. Şekil 5 ile yeni imge şifreleme konseptine ait akış şeması, Şekil 6 ile yeni imge şifreleme yöntemine ilişkin blog diagramı verilmiştir.

Algoritma 1. BZ referans görüntü şifreleme yöntemi algoritması

Giriş

P: W X H boyutuna sahip önceden şifrelenmiş görüntü.
R: 2W x 2H boyutuna sahip referans görüntü.
K2: Referans görüntü şifreleme anahtarı

Çıkış

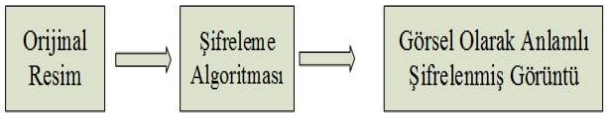
E: 2W x 2H boyutuna sahip son durumda elde edilen şifreli görüntü.

1: Tamsayı 2D DWT uygulanır ve K2 kullanarak LL, LH, HL ve HH alt-bantlarını elde edilir.
2: for i=1 to W do
3: for j=1 to H do
4: $HL_{i,j} = \left\lfloor \frac{P_{i,j}}{10} \right\rfloor$
5: $HH_{i,j} = P_{i,j} \pmod{10}$
6: endfor
7: endfor
8: Ters tamsayı 2D DWT uygulanır ve son durumda şifreli görüntü olan E elde edilir.

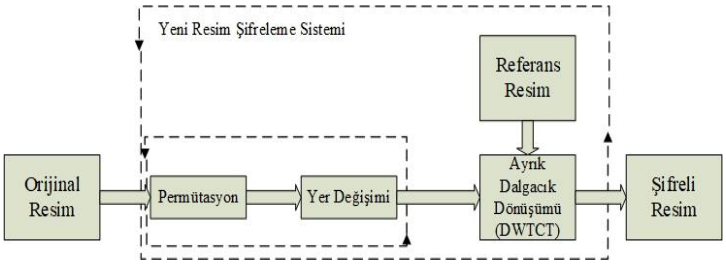
BZ'nin imge şifreleme yöntemine ait referans görüntünün, şifre çözme şemasına işlem akışı 9. ve 10. satır olarak Algoritma 2'de verilmiştir.

Algoritma 2. BZ'nin imge şifreleme yöntemi şifre çözme aşaması algoritması

9- $[LL, LH, HL, HH] = DWT2(R, K_2)$
10- $P = HL \times 10 + HH$



Şekil 5 Yeni İmge Şifreleme Konsepti



Şekil 6 Yeni İmge Şifreleme Yönteminin Blog Diagramı

İmge Şifrelemede Kullanılan Performans Metrikleri

Bir imgenin şifrelenmesinde kullanılan birçok algoritma ve şifreleme yöntemi bulunmaktadır. İmge şifrelemede kullanılan bu şifreleme algoritmalarından elde edilen sonuçların incelenmesi ve bir görsel üzerinde bir değişiklik yapılıp yapılmadığın tespiti için imge şifreleme analizi yapılabilmektedir (Ping vd., 2017) Bu analiz histogram, korelasyon vb. metrikler ile yapılmaktadır.

Histogram Analizi

Bir görüntünün histogramı, bir dijital görüntüde mevcut olan piksel yoğunluğu değerlerinin frekans dağılımının grafiksel bir gösterimidir. İdeal olarak, şifrelenmiş bir resmin histogramı düzgün bir şekilde yayılmalı ve orijinal görüntünün histogramı ile benzerlik göstermemelidir.

AES vb. birçok imge şifreleme tekniği, kriptanaliz riski altındadır bu nedenle şifreleme sonucunda düzenli bir histogram dağılımı gerekmektedir. Histogram analizi ile imge üzerinde herhangi bir değişikliğe gidilip gidilmediğinin de tespiti yapılabilmektedir.

Korelasyon analizi

İmge şifrelemede şifrelenmiş bir görüntü, bitişik pikseller arasında bir korelasyona sahip olmamalıdır. Mevcut herhangi bir korelasyon, yetkisiz bir kullanıcının görüntünün bir kısmını yeniden oluşturması veya orijinal görüntünün kendisini daha kötü hale getirmesi için kullanılabilir. Korelasyon katsayıları – 1 ile + 1 arasında değişmektedir, burada aşırı uçlar sırasıyla mükemmel bir negatif veya pozitif doğrusal ilişkisini göstermektedir. Sıfırın katsayı değeri, bitişik piksel değerleri arasında doğrusal bir ilişkiyi temsil etmemektedir. Bir görüntüde, bitişik pikseller arasındaki yatay, dikey ve çapraz oryantasyon katsayısı matematiksel olarak eşitlik 1 ile 4 arasında ki gibi ifade edilebilir.

$$r_{\alpha\beta}=\frac{cov(\alpha,\beta)}{\sqrt{D(\alpha)}\sqrt{D(\beta)}} \quad (1)$$

$$E(\alpha)=\frac{1}{N}\sum_{i=1}^{N}\alpha_i \quad (2)$$

$$D(\alpha)=\frac{1}{N}\sum_{i=1}^{N}\left(\alpha_{i-E(\alpha)}\right)^2 \quad (3)$$

$$cov(\alpha,\beta)=\frac{1}{N}\sum_{i=1}^{N}(\alpha_i-E(\alpha))\,(\beta_i-E(\beta)) \quad (4)$$

Diferansiyel Saldırı Analizi

Diferansiyel saldırı analizi, pikseldeki en küçük bir değişikliği veya orijinal görüntünün anahtar değeri sağlandıktan sonra şifrelenmiş görüntüdeki değişiklikleri belirlemek için yapılan analiz türüdür. Bu analizi yapmak için, hem orijinal görüntünün hem de değiştirilmiş olan imgenin, aynı şifreleme tekniği kullanılarak şifrelenmesi gerekmektedir. NPCR parametresi, net piksel değişim oranı; UACI, yoğunluktaki birleşik ortalama değişimi oranı olarak tanımlanmaktadır. UACI oranı, kullanıldığı şifreleme tekniğinin çeşitli saldırılara karşı dayanıklılık oranı olarak da tanımlanmaktadır. NPCR oranı, orijinal imge ile piksel değişikliği yapılmış olan imgenin karşılaştırıldığında ki şifreli görüntünün piksel sayısındaki değişim oranını belirtir. C1 parametresi, orijinal imgeyi C2 parametresi, piksel değişimi olmuş olan imgeyi temsil etmektedir. NPCR değeri hesaplaması, eşitlik 5 ile gösterilmektedir.

$$\mathrm{NPCR}=\frac{\sum_{i=1}^{H}\sum_{j=1}^{W}D(i,j)}{W\times H}\times 100\% \quad (5)$$

H ve W parametreleri görüntünün yükseklik ve genişlik değerleridir. D parametresi, C1 ve C2 görüntülerine eşdeğer büyüklükte bir bipolar diziyi temsil etmektedir. Bileşen olarak sadece 0 veya 1 değerleri kullanılmaktadır. D (i, j) değeri hesaplaması, eşitlik 6 ile gösterilmektedir.

$$D(i,j)=\begin{pmatrix}0 & C1(i,j)=C2(i,j),\\ 1 & C1(i,j)\neq C2(i,j)\end{pmatrix} \quad (6)$$

UACI değeri, düz ve şifrelenmiş görüntü arasındaki ortalama yoğunluk farkıdır. UACI değeri hesaplaması, eşitlik 7 ile gösterilmektedir. Hesaplamada ki L parametresi; ilgili kırmızı, yeşil ve mavi kanalları temsil eden bitlerin sayısıdır.

$$\mathrm{UACI}=\frac{1}{W\times H}\left[\sum_{i=1}^{H}\sum_{j=1}^{W}\frac{|C1(i,j)-C2(i,j)|}{2^L-1}\right]100\% \quad (7)$$

Anahtar Uzay (Alan) Analizi

Anahtar alan analizi, bir kaba kuvvet saldırısına karşı dayanıklı bir şifreleme şemasının fizibilitesini tanımlayan önemli bir parametredir. Bunu yapabilmek için, şifrenin anahtar aralığının büyük bir kombinasyonu olmalıdır. Kaos temelli algoritmaların tamamı, kaba kuvvet saldırılarına direnecek kadar büyük bir anahtar alana sahiptir fakat bazı imge şifreleme algoritmaları küçük anahtar alanlara sahip olduğu için temel saldırı türüne karşı savunmasız hale gelmektedir. Tablo 1 ile yaygın olarak kullanılan imge şifreleme

algoritmalarına ait anahtar alan aralığı değerlerini sunmaktadır.

Tablo 1. İmge şifreleme algoritmalarına ait anahtar alan aralığı değerleri

Algoritma	Anahtar Aralığı
Vigenere	2^{128}
DES	2^{56}
IDEA	2^{128}
Blowfish	2^{64}
RC4	2^{256}
RC5	2^{128}
AES	2^{128}

Anahtar Hassasiyet Analizi

Anahtar duyarlılık analizi, imge şifrelemede kullanılan algoritmada ki anahtarda meydana gelen bir değişimi tespit etmek için kullanılan analiz türüdür. Analiz, piksel karşılaştırması ile yapılmaktadır. Şifrelenmiş görüntünün piksel karşılaştırması ve NPCR oranı, anahtar değerinde ki dakika değişikliği (bir bit değişimi) için gözlemlenmektedir. Bir şifreleme şeması, iki koşula göre etkin olarak kabul edilir: İlk koşul, her iki imgenin de şifreli olarak ayrı ayrı şifrelenmiş görüntüler oluşturmak için şifrelerde bağımsız olarak kullanılması durumunda, her iki şifrelenmiş görüntünün de tamamen farklı olması gerektiği belirtilmektedir. İkinci koşul, her iki imgenin de aynı şifrelenmiş görüntünün şifresini çözmek için bağımsız olarak kullanıldığı takdirde, sadece orijinal anahtardan deşifre edildikten sonra, orijinal görüntünün sağlanması, diğerinin ise herhangi bir alakalı sonuç vermemesi gerektiği belirtilmektedir.

Zaman Karmaşıklığı Analizi

Zaman karmaşıklığı analizi, yürütme talimatı tarafından hesaplanan zaman miktarıdır. Manuel yaklaşımı, temel işlemlerin kendileriyle ilişkili sabit bir zamana sahip olmasından dolayı sette bulunan toplam temel yürütme işlemleri kullanılarak yapılabilir. Burada, hesaplanan zaman miktarı, resmin şifreleme ve şifre çözme süresini temsil eder ve yerleşik işlemler tarafından hesaplanır. Zaman karmaşıklığı, sistem konfigürasyonu ve kullanılan görüntü gibi çeşitli faktörlere bağlı olarak değişiklik göstermektedir.

İmge Şifrelemede Kullanılan Algoritmaların Performans Metriklerinin Karşılaştırılması

Tablo 2. İmge şifrelemede kullanılan algoritmaların performans metriklerinin karşılaştırılması

Şifreleme Algoritması	İmge Şifreleme	Histogram Dağılımı	Piksel Duyarlılığı	Anahtar Duyarlılığı	Entropi Değeri
DES	Orta	Artan	Orta	Yüksek	Yüksek
RC4	Yüksek	Tek Düze	En Düşük	Yüksek	Yüksek
RC5	Orta	Artan	Orta	Yüksek	Yüksek
TDES	Orta	Artan	Orta	Yüksek	Yüksek
AES	Orta	Artan	Orta	Yüksek	Yüksek
Vigenere	En az	Artan	En Düşük	Düşük	Yüksek
IDEA	Orta	Artan	Orta	Yüksek	Yüksek

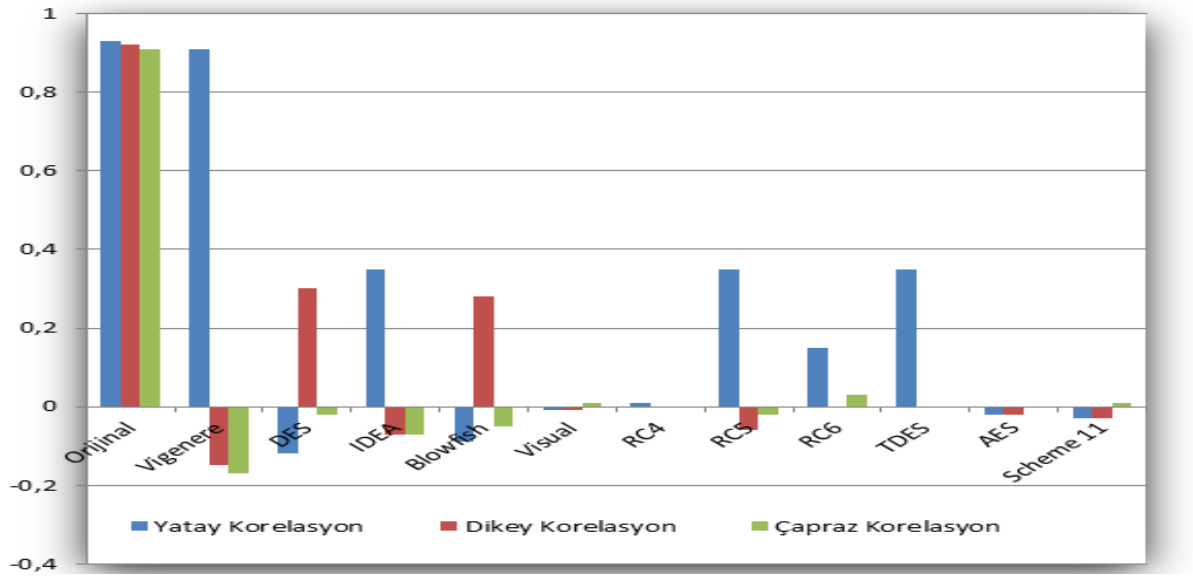
İmge Şifrelemede Kullanılan Algoritmalarında Piksel Değerindeki Bir bitlik Değişiklik İçin NPCR ve UACI Değerleri Karşılaştırılması

Tablo 3. İmge şifrelemede kullanılan algoritmalarda piksel değerindeki bir bitlik değişiklik için NPCR ve UACI değerleri sonuçları

Boyut	128 x 128		192 x 192		256 x 256	
	NPCR	UACI	NPCR	UACI	NPCR	UACI
DES	4.88×10^{-4}	1.17×10^{-4}	2.17×10^{-4}	5.12×10^{-5}	1.22×10^{-4}	5.43×10^{-5}
RC4	6.10×10^{-5}	2.87×10^{-6}	2.71×10^{-5}	1.28×10^{-6}	1.53×10^{-5}	7.18×10^{-7}
AES	9.77×10^{-4}	3.21×10^{-4}	4.34×10^{-4}	1.42×10^{-4}	2.44×10^{-4}	6.21×10^{-5}
Vigenere	6.10×10^{-5}	4.79×10^{-6}	2.71×10^{-5}	2.13×10^{-6}	1.53×10^{-5}	1.20×10^{-6}
IDEA	4.88×10^{-4}	1.25×10^{-4}	2.17×10^{-4}	8.83×10^{-5}	1.22×10^{-4}	4.09×10^{-5}
TDES	4.88×10^{-4}	1.57×10^{-4}	2.17×10^{-4}	6.45×10^{-5}	1.22×10^{-4}	4.97×10^{-5}
Visual	6.10×10^{-5}	2.39×10^{-7}	2.71×10^{-5}	1.06×10^{-7}	1.53×10^{-5}	5.98×10^{-8}

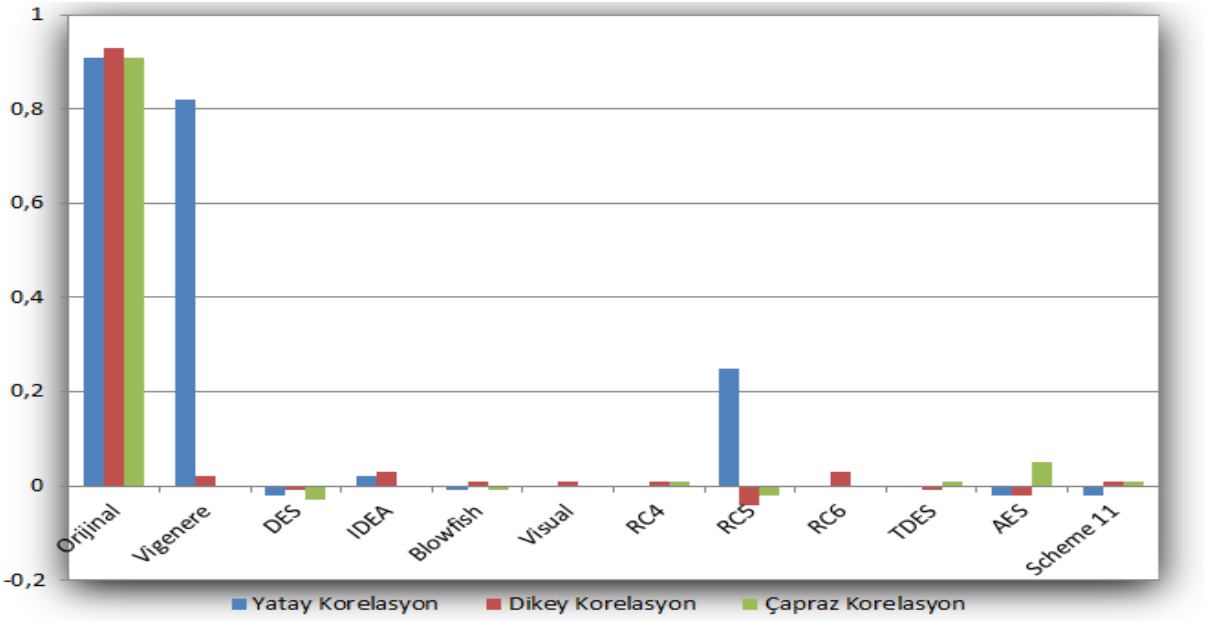
İmge Şifrelemede Kullanılan Algoritmaların Korelasyon Analizi

Özel bilgilerin güvenliğini sağlamak amacıyla oluşturulan ve yaygın olarak kullanılan imge şifreleme algoritmaları ile farklı boyuttaki görsellere uygulanan korelasyon analizi istatistiksel sonuçları aşağıda grafiksel olarak görselleştirilmiştir. Korelasyon analizi sonucunda, üzerinde çalışılan her imge şifreleme algoritması için yatay, dikey ve çapraz korelasyon analizi matematiksel hesaplama sonuçları karşılaştırılmıştır. 128 × 128 boyutundaki görüntüde kullanılan şifreleme tekniği için korelasyon analizi karşılaştırma sonuçları, Şekil 7 ile gösterilmiştir.



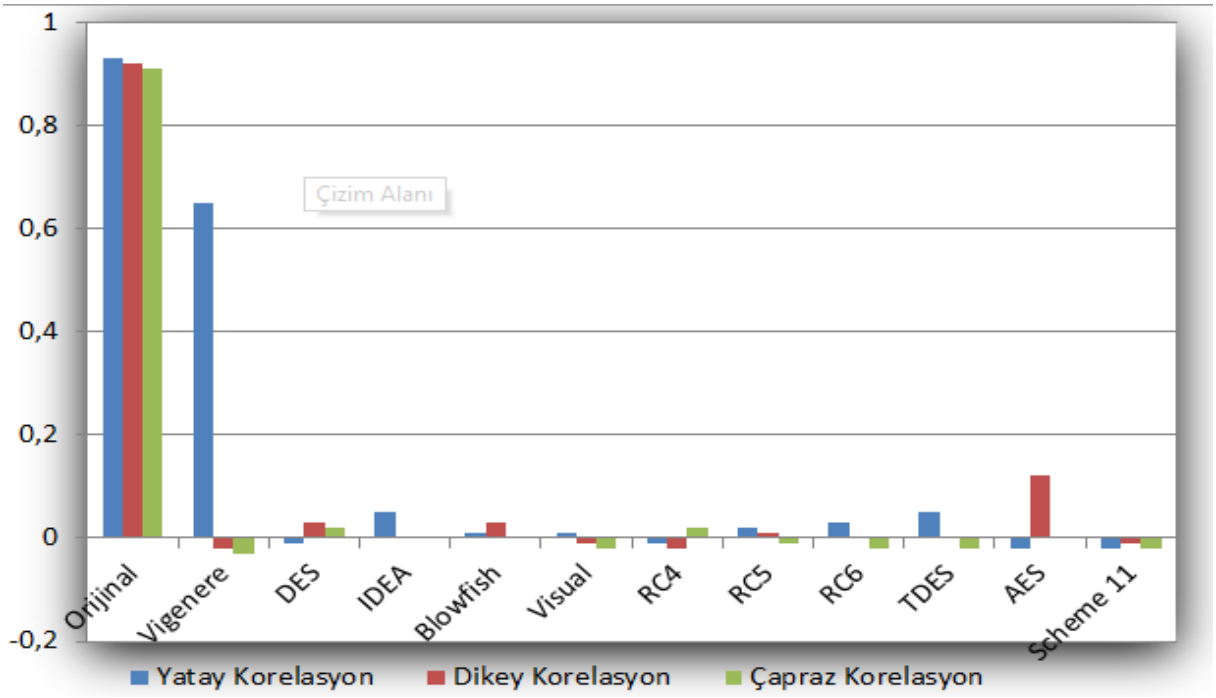
Şekil 7 128 × 128 Boyutunda Görüntüde Kullanılan Şifreleme Tekniğinin Korelasyon Analizi

192 × 192 boyutunda görüntüde kullanılan şifreleme tekniği için korelasyon analizi karşılaştırma sonuçları, Şekil 8 ile gösterilmiştir.



Şekil 8 192 × 192 Boyutunda Görüntüde Kullanılan Şifreleme Tekniğinin Korelasyon Analizi

Şekil 9, 256 x 256 boyutunda görüntüde kullanılan şifreleme tekniği için korelasyon analizi karşılaştırma sonuçlarını göstermektedir.



Şekil 9 256 × 256 Boyutunda Görüntüde Kullanılan Şifreleme Tekniğinin Korelasyon Analizi

İmge Şifrelemede Güvenlik Analizi

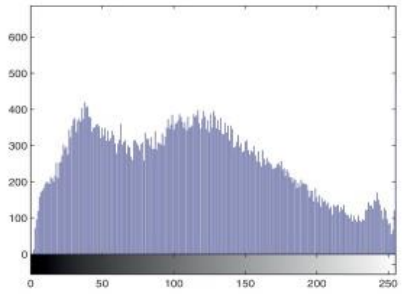
Dijital ortamda kullanılan güvenlik kavramı, kriptografi için çok önemli bir unsurdur. İyi bir görüntü şifreleme şeması; bilinen düz metin saldırısı, şifreli metin saldırısı, istatistiksel analiz saldırısı ve kaba kuvvet saldırıları gibi çeşitli saldırılara karşı dayanıklı olmalıdır. Bir şifreleme algoritmasını kripto analize ederken genel varsayım, kripto analist'in anahtar dışındaki algoritmanın tüm ayrıntılarını bilmesidir. Kripto analiz, şifrelenmiş verileri çözümlemeyi ve anahtarı kullanmadan şifresini kırmaya çalışmaktır. Kripto analizde, düz metine (plaintext), şifrelere veya kripto sistemin diğer yönlerine ne kadar eriştiğine bağlı olarak kripto analizi gerçekleştirebilecek çok sayıda teknik bulunmaktadır. En yaygın saldırı türlerine örnek olarak şifreli metin saldırısı, seçilmiş düz metin saldırısı, seçilmiş şifreli saldırı, bilinen düz metin saldırısı verilebilir. Şifreli metin saldırında, kriptanalist bazı şifreleme algoritmasına yada şifreleme anahtarına dair bazı parçalara sahiptir. Muhtemelen en çok kullanılan kriptanaliz tipidir. Seçilmiş düz metin saldırısında ise kiptanalist şifreleme algoritmasına sahiptir. Bu nedenle, herhangi bir düz metin (plaintext) seçebilir ve karşılık gelen şifreleri elde edebilir. Bir sonraki saldırı, en çok kullanılan saldırılardan olan seçilmiş şifreli saldırısıdır. Bu saldırıda, kriptanalist şifre çözme algoritmasına sahiptir. Bu nedenle herhangi bir şifreleme metni seçebilir ve karşılık gelen düz metinleri(plaintext) elde edebilir. Son olarak; bilinen düz metin saldırısı, kriptanalist, şifreleme algoritmasına dair bazı düz metinlere (plaintext) ve karşılık gelen şifreleme halkalarına sahiptir. Bu dört saldırının her birinde, amaç anahtarı belirlemektir. Anahtar yukarıda bahsedilen saldırılardan biriyle öğrenildiği takdirde, kriptosistem güvensiz kabul edilir. Şifreleme kalitesini kanıtlamak için şifreleme algoritmasına güvenlik analizleri gereklidir. Şifreleme algoritmalarının analizi için;

1. Histogram Analizi
2. Korelasyon Katsayısı,
3. Doğrusal ve Diferansiyel Saldırı (NPCR)
4. Bilgi Entropisi Analizi
5. Şifreleme Kalitesi
6. Anahtar Alan Analizi
7. Şifreli anahtarlama

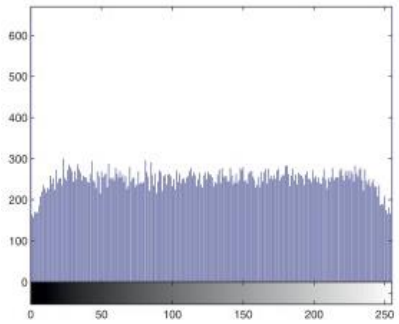
gibi görüntünün güvenliğini ölçmek amacıyla çeşitli güvenlik analizleri gerçekleştirilmektedir.

İmge Şifreleme Güvenlik Analizinde Histogram Dağılımı Kullanımı

İmge histogramı, bir görüntünün istatistiksel bir özelliğidir ve piksellerin her bir gri düzeyindeki piksel sayısını çizerek görüntüye ne şekilde dağıldığını gösterir. Bir şifre görüntüsündeki oldukça eşit sayıda gri düzey, gri seviyenin düzgün dağılımını ve dolayısıyla iyi bir rasgelelik düzeyini gösterir. Histogram analizi, bir görüntüdeki piksel değerlerinin ağırlığının grafiksel bir gösterimidir. Histogram grafiğini inceleyerek, görüntünün tonu hakkında bilgi edinebilirsiniz. Dağıtım değerleri eşit veya en azından yakınsa, histogram dağılımın iyi olduğu anlamına gelmektedir. Orijinal görüntünün histogram dağılım grafiğinin incelenmesi, dengesiz bir dağılıma sahip olduğunu ortaya koymaktadır. Test edilen tüm şifreleme algoritmaları dengeli ve yakın bir dağıtıma sahiptir. Sonuç olarak, şifreleme algoritması dengeli ve iyi bir histogram dağılımı sağlar ve bunun sonucunda bir imgenin histogram analizine bakılarak şifrelimi yoksa şifresiz mi olduğu histogram dağılımına göre anlaşılabilmektedir. Örnek bir dağılımı ait histogram sonuçları Şekil 10 ile verilmiştir. Şekil 10 (a) görseli ile orjinal görüntünün histogram sonucu, Şekil 10 (b) görseli ile şifreli imgenin histogram sonucu grafiksel olarak sunulmuştur.



(a)

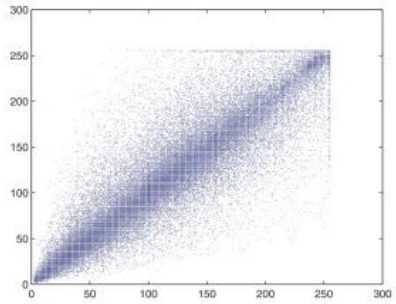


(b)

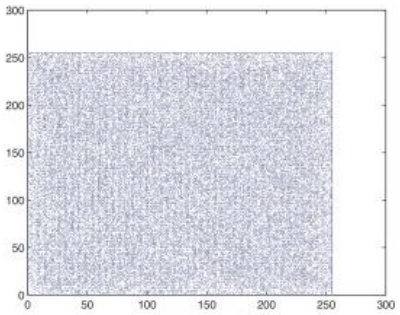
Şekil 10 Histogram Sonuçları (a) Orjinal görüntünün histogram sonucu (b) Şifreli görüntünün histogram sonucu

İmge Şifreleme Güvenlik Analizinde Korelasyon Katsayısı Kullanımı

Korelasyon katsayısı analizi, iki rastgele değişken arasındaki korelasyona dayanarak, bu ilişkinin bağımsız olduğunu simgelemektedir. Korelasyon doğrusal ise, korelasyon dağılımının iyi olmadığı anlamına gelmektedir. Diğer taraftan, korelasyon doğrusal değilse, şifrelemenin iyi olduğu anlamına gelmektedir. Örnek bir dağılımı ait korelasyon sonuçları Şekil 11 ile verilmiştir. Şekil 11 (a) görseli ile orijinal görüntünün korelasyon analizi sonucu, Şekil 11 (b) görseli ile, şifreli görüntünün korelasyon analizi sonucu grafiksel olarak sunulmuştur.



(a)



(b)

Şekil 11 Komşu Pixellerin Korelasyon Sonuçları (a) Orijinal görüntünün korelasyon analizi (b) Şifreli görüntünün korelasyon analizi

İmge Şifreleme Güvenlik Analizinde Doğrusal ve Diferansiyel Saldırı (NPCR – UACI Analizi)

NPCR (Piksel Değişim Oranı Sayısı) ve UACI (Birleştirilmiş Ortalama Değişim Şiddeti) , farklı ataklara karşı imge şifreleme algoritmasının dayanıklılığına uygun olarak dirençli şifreleme algoritmasını bulmak için kullanılan bir kriptanaliz yöntemidir. Orijinal görüntülerde küçük değişikliklerin şifrelemeyi nasıl etkilediğini tespit etmek için de kullanılır. Bu yöntem, şifrelenmiş bitler ve orijinal görüntüden seçilen rastgele bitlerle yapılan şifreleme değişikliklerini kullanır ve bu şekilde şifrelenmiş görüntünün şifresini çözmeye çalışır. Orijinal görüntüdeki değişikliklerin bir sonucu olarak şifrelemede büyük değişiklikler meydana gelirse, saldırıya dayanıklı şifreleme elde edilir. Şifreleme algoritmalarının güvenlik ve performans karşılaştırma tablosu Tablo 4 ile verilmiştir.

Tablo 4. Algoritmalar arası kriter karşılaştırma sonuçları

	Kaos Algoritması	AES Algoritması	Önerilen Algoritma
NPCR	99.60672	99.63245	99.62987
UACI	31.24768	31.87236	31.83459
Bilgi Entropisi	7.95454	7.95912	7.95667
Şifreleme Kalitesi	29.67574	35.84217	35.87899
Şifreleme Süresi(sn.)	1.21468	27.36952a	1.67342
Şifre Çözme Süresi(sn.)	1.16734	29.21683	1.30321
Toplam Süre(sn.)	2.38202	56.58635	2.97663

İmge Şifreleme Güvenlik Analizinde Bilgi Entropisi Analizi Kullanımı

Bilgi entropi analizi, şifrelenmiş verilerin karmaşıklığını ölçmek için kullanılan bir yöntemdir. Şifrelenmiş verilerin karmaşıklık oranı arttıkça orijinal veriler hakkında bilgi elde etmekte bir o kadar zorlaşmaktadır. Şifreleme için optimum bilgi entropi değeri 8 olarak tanımlanmaktadır. Hesaplanan değer, 8 tamsayı değerine yaklaştıkça, şifreleme kalitesi artmaktadır. Aşağıda eşitlik 8 simgesinde yer alan matematiksel denklem ile karmaşıklık değeri hesaplanabilmektedir.

$$\mathrm{ShanEn}(x) = -\sum_{i=1}^{N} \left(P_i(x)\right)\left(\log_2 P_i(x)\right) \qquad (8)$$

İmge Şifreleme Güvenlik Analizinde Şifreleme Kalitesi Kullanımı

Şifreleme kalitesi, şifreli ve orijinal görüntülerin piksel değerlerini karşılaştırarak elde edilen bir değerdir. Piksel değerindeki değişim ne kadar büyük olursa, daha yüksek şifreleme kalitesine sahip olduğu anlamına gelmektedir. İmge şifreleme kalitesi değer hesaplama matematiksel fonksiyonu eşitlik 9 ile gösterilmektedir.

Şifreleme kalitesi değeri, iki görüntü arasındaki sapma olarak ifade edilmektedir. P değeri; orijinal görüntüyü, C değeri; şifrelenmiş görüntüyü ifade etmektedir.

$$\text{Şifreleme Kalitesi} = \frac{\sum_{L=0}^{255} |H_L(C) - H_L(P)|}{256} \qquad (9)$$

İmge Şifreleme Güvenlik Analizinde Anahtar Alan Analizi Kullanımı

Boyut olarak geniş anahtar alanlı bir şifreleme algoritması, güçlü saldırılara karşı oldukça dayanıklıdır. Bunun nedeni, anahtar alanın geniş olmasından dolayı, saldırganların anahtarı bulmasının zor olmasıdır. Kaos tabanlı şifrelemede, kaotik sistemin boyutu ve sistem parametrelerinin sayısı arttıkça, sistem anahtar alanı genişler ve sistem daha karmaşık hale gelir. Ancak, sistem daha karmaşık hale geldiği için süreç yükünü artırdığı için dengeli bir yapıya ihtiyaç vardır. AES algoritması 128 bit şifreleme için 2 üzeri 128 bit anahtar alana sahiptir. Kaotik sistem ve AES algoritması anahtar alanı karşılaştırıldığında, kaotik sistem anahtar alanı değerinin çok daha fazla olduğu görülmektedir. Anahtar boyutu alanı ne kadar geniş olursa şifrenin aşılması bir o kadar güç olacaktır ve güvenlik seviyesi yüksek olacaktır.

İmge Şifreleme Güvenlik Analizinde Şifreli Anahtarlama Kullanımı

Kaotik sistemlerin en önemli özelliklerinden biri, başlangıç koşullarına ve sistem parametrelerine çok hassas bir şekilde bağlı olmalarıdır. Başlangıç koşullarında veya sistem parametrelerinde küçük bir değişiklik bile tamamen farklı bir yörüngeye ve değerlere yol açacaktır. Güvenli bir şifreleme sisteminde, anahtardaki küçük bir değişiklik şifreli verilerin şifresini çözmeyi engelleyebilmelidir. Bu noktada kaotik sistemlerin ilk koşullara ve sistem parametrelerine çok hassas bir şekilde bağlı olması, güvenli bir şifreleme için büyük önem taşımaktadır ve bu özellikler bu gereksinimi karşılamaktadır. Örneğin, rasgele sayı üretimi için kullanılan RC4 algoritmasının girişi, önceki adımdan geldiğinden, küçük bir değişiklik bile tüm sistemi etkiler. Bu nedenle tasarlanan

şifreleme sisteminin anahtar hassasiyetinin yüksek olduğu söylenebilir.

Tartışmalar

Bu makalede imge şifreleme yöntemlerinden söz edilmiştir. Vigenere, DES, AES, RC4 ve BZ'nin yönteminden bahsedilmiştir. Vigenere klasik bir şifreleme algoritmasıdır ve frekans analizi saldırısına karşı dayanıksızdır. Bu sebepten dolayı modern şifreleme algoritması olarak kullanılmamaktadır. DES 2000'li yıllara kadara blok şifreleme standardı olarak kullanılan bir algoritmadır ancak bu sisteminde diferansiyel atağa karşı dayanıksız olduğu bilinmektedir. AES günümüzde kullanılan blok şifreleme standardıdır. AES'in en büyük problemi ise yüksek maliyetli olması ve ECB modunun imge şifreleme için yetersiz olmasıdır. Yüksek maliyet problemini çözebilmek için akan şifreleme yöntemleri kullanılmaktadır. RC4 gibi sistemler hızlıdır, iyi istatistiksel özelliklere sahiptir ancak bu tür sistemleri de kırabilmek için başarılı ataklar mevcuttur. BZ'nin algoritması kaotik yapılar ve steganografiyi bir arada kullanan bir algoritmadır. Burada temel amaç kaotik yapıların sahip olduğu problemleri gidermek için steganografi kullanmak ve çok seviyeli bir güvenlik sistemi önermektir. Bu sistemde görülen en önemli problem ise yüksek gürültü oranına sahip olmasıdır.

Sonuç ve Öneriler

Günümüzde, büyüyen teknolojiye bağlı olarak bilgisayar korsanları, teknolojiyi ve onu ele geçirme yollarını her geçen gün biraz daha farklı teknikler ile gerçekleştirmektedir. Veri aktarımı, kurumsal alanlar, sanal ortam alışverişleri vb. birçok alanda veri aktarımı internet üzerinden gerçekleşmektedir. Dijital ortamda gerçekleşen bu veri aktarımında, kişisel ve özel bilgilerin güvenliğinin iyi sağlanması gerekmektedir. Bilim insanları ve araştırmacılar görüntü verisinin korunması ile ilgili birçok teknikler geliştirmişlerdir. Bu çalışmada, dijital ortamda aktarımının yapıldığı özel ve kişisel verilerin güvenliğini sağlamak amacıyla oluşturulan ve yaygın olarak kullanılan bazı imge şifreleme algoritmalarının çalışma yapısı ve mantığı incelenerek çeşitli literatür taramaları yapılmıştır. İncelenen algoritmalar arası performans ve metrik karşılaştırmaları yapılmış ve istatistiksel veriler elde edilmiştir. Elde edilen veriler grafik ve tablolar ile görselleştirilmiştir. Çalışmanın son aşamasında imge şifrelemenin güvenliğinin nasıl sağlandığı ve güvenli analizi için kullanılan yöntemlerden bahsedilmiştir.

Kaynaklar

Aphetsi Kester, A cryptosystem based on Vigenère cipher with varying key, ISSN: 2278 – 1323 International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 10, December 2012

LongBao,YicongZhou, Image encryption: Generating visually meaningful encrypted images, Department of Computer and Information Science, University of Macau, Macau, China

Manju Kumari . Shailender Gupta . Pranshul Sardana, A Survey of Image Encryption Algorithms , DOI 10.1007/s13319-017-0148-5, 3D Research Center, Kwangwoon University and Springer-Verlag GmbH Germany, part of Springer Nature 2017

Manjula K G, Color Image Encryption and Decryption Using DES Algorithm, M.Tech (EC) (4th SEM), Dept. of ECE , Malnad College of Engineering , Hassan, India, Volume: 03 Issue: 07 | July-2016, e-ISSN: 2395 -0056 p-ISSN: 2395-0072

M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, A Modified AES Based Algorithm for Image Encryption, International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:1, No:3, 2007

Ping Ping, Designing permutation substitution image encryption networks with Henon map, College of Computer and

Information, Hohai University, Nanjing 210098, China

R. Parvaz, A combination chaotic system and application in color image encryption, Department of Mathematics, University of Mohaghegh Ardabili, 56199-11367 Ardabil, Iran

Sanjay Kumar, Image Encryption using Simplified Data Encryption Standard (S-DES), International Journal of Computer Applications (0975 – 8887) Volume 104 – No.2, October 2014

Yu-Guang Yang, Eliminating the texture features in visually meaningful cipher images, College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China

N.K.Pareeka, Vinod Patidara, K.K.Sud, Image encryption using chaotic logistic map, Volume 24, Issue 9, 1 September 2006, Pages 926-934, Department of Physics, College of Science Campus, M.L.S. University, Udaipur 313002, Rajasthan, India

Shi Liu, Changliang Guo, John T. Sheridan, A review of optical image encryption techniques, Volume 57, April 2014, Pages 327-342, School of Electrical, Electronic and Communication Engineering, College of Engineering and Architecture, University College Dublin, Belfield, Dublin 4, Ireland

Aloka Sinha, Kehar Singh, A technique for image encryption using digital signature, Volume 218, Issues 4–6, 1 April 2003, Pages 229-234, Photonics Group, Department of Physics, Indian Institute of Technology Delhi, New Delhi 110016, India

Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, A new encryption algorithm for image cryptosystems, Volume 58, Issue 2, 1 September 2001, Pages 83-91, Department of Computer Science and Information Engineering, National Chung Cheng University, Chaiyi, Taiwan, ROC

S.Behnia, A. Akhshani, H. Mahmodi, A. Akhavan, A novel algorithm for image encryption based on mixture of chaotic maps, Volume 35, Issue 2, January 2008, Pages 408-419, Department of Physics, IAU, Urmia, Iran

Rinki Pakshwar, Vijay Kumar Trivedi, Vineet Richhariya, A Survey On Different Image Encryption and Decryption Techniques, Rinki Pakshwar et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (1) , 2013, 113 – 116, Dept. of Computer Science Lakshmi Narain College of Technology, Bhopal(India)

Majid Khan, Tariq Shah, A Literature Review on Image Encryption Techniques, 22 October 2014, Quaid-i-Azam University, Islamabad, Pakistan

Image Encryption Methods and Algorithms

Extended Abstract

Depending on the development of technology, the transfer of digital images over the Internet has become widespread. In the transmission of digital images used in various public and official places over the internet, data protection, data integrity and confidentiality should be ensured. The safety and confidentiality of the transmission of digital images provide keyed and keyless with various encryption algorithms. Today, image security is becoming more and more important. One of the reasons for this is that confidential images are transmitted to the public over the internet and a third person can access this transfer between two people. Therefore, encryption was considered an effective and direct technique to ensure the security of private information. According to architects, methods for encryption can be divided into three categories. They are categorized as permutations, displacements, permutations and displacements. In this article, various literature surveys have been done the working structure and logic of some commonly used image encryption algorithms, which are used to ensure the security of private and personal data that is transmitted in digital environment. The data obtained are visualized by graphs and tables. Explained the methods used for the security and secure analysis of image encryption in the final stage of the article. The main purpose of this article is to compare the methodology of some image encryption algorithms used to ensure the security of personal information to introduce awareness among algorithms. First of all, image encryption is explained in this article. Algorithms used in Image Encryption according to the flow of the article were examined. The structure and logic are examined encryption algorithms are

1. *Vigenere Encryption Algorithm*
2. *DES (Data Encryption Standart)*
3. *RC4 Encryption Algorithm*
4. *AES (Advanced Encryption Standard)*
5. *An algorithm for encryption of secret images into meaningful images(Bao ve Zhou encryption method).*

Immediately after the algorithm analysis, Performance Metrics Used in Image Encryption were examined. The metrics reviewed are

1. *Histogram Analysis*
2. *Correlation analysis*
3. *Differential Attack Analysis*
4. *Key Space Analysis*
5. *Key Accuracy Analysis*
6. *Time Complexity Analysis.*

After metric inspection , security was reviewed analysis in image encryption. Security analysis under the topic title,

1. *Histogram Distribution in Image Encryption Security Analysis*
2. *Correlation Coefficient in Image Encryption Security Analysis*
3. *Linear and Differential Attack in Image Encryption Security Analysis (NPCR - UACI Analysis)*
4. *Knowledge Entropy Analysis in Image Encryption Security Analysis*
5. *Encryption Quality in Image Encryption Security Analysis*
6. *Key Space Analysis in Image Encryption Security Analysis*
7. *Encrypted Switching in Image Encryption Security Analysis was examined.*

Comparison of the image encryption algorithms, metrics and security analyzes' results were graphically visualized.

Keywords: *image encryption, privacy of personal data, image encryption process and methodology*