Engineering Sciences
ISSN: 1308 7231 (NWSAENS)
ID: 2016.11.4.1A0367

Status : Original Study
Received: June 2016
Accepted: October 2016

Zainab Obaid
Arkan Sabonchi
Bahriye Akay
Erciyes University, zainabark@yahoo.com, arkankhaleel@gmail.com, bahriye@erciyes.edu.tr, Kayseri-Turkey

http://dx.doi.org/10.12739/NWSA.2016.11.4.1A0367

KLASİK KRİPTOLOJİ YÖNTEMLERİNİN KARŞILAŞTIRILMASI

ÖZ

Kriptoloji, bilgilerin şifrelenmesi ve şifrelenmiş bilgilerin çözümlenmesi için kullanılan metotlarla ilgilenir. Kriptoloji yöntemleri klasik ve modern yöntemler olmak üzere ikiye ayrılmaktadır. Bu çalışmada klasik algoritmalardan yaygın olarak kullanılan Sezar, Vigenere, Vernam, Hill, Playfair algoritmalarının genel yapısı hakkında bilgi verilerek sözü geçen algoritmaların metinler ve Base64 tabanlı görüntü üzerindeki karşılaştırılmaları yapılmıştır. Metin ya da görüntüler şifreleme algoritmalarına girdi olarak verilerek anahtar ile şifrelenmiş metin elde edilmiştir ve algoritmalar çalışma zamanı (şifrelenme zamanı+şifre çözülme zamanı), zaman karmaşıklığı, işlemci karmaşıklığı, hafıza karmaşıklığı, kurulacak sisteme uygunluk, esneklik, güven oranı bakımından kıyaslanarak avantaj ve dezavantajları belirlenmiştir.

Anahtar Kelimeler: Şifreleme Algoritmaları, Performans Analizi, Kriptoloji, Bilgi Güvenliği, Görüntü Şifreleme

COMPARISON OF CLASSICAL CRYPTOGRAPHY METHODS

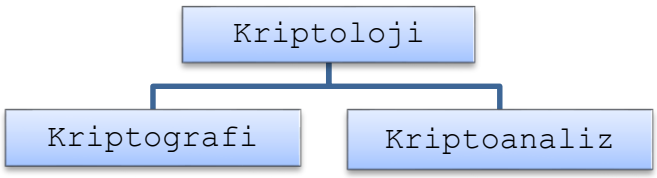
ABSTRACT

Cryptography is the science which deals with methods and theories of encryption and decryption. Cryptography is divided into two parts: Modern and classic methods. In this study, we employed some common classical encryption algorithms including Caesar, Vigenere, Vernam, Hill, Playfair algorithms. The overall structure of these algorithms have been explained and an analysis have been performed on the images encoded with Base64. Images and text data are passed to the algorithms and encrypted data is obtained using crypto key. The performances of the algorithms were analyzed based on time consumption for encryption/decryption, the memory consumption, the processor consumption, time complexity, and space complexity, adaption to the system, flexibility and confidence rate. Once the performance of the algorithms obtained, the advantages and disadvantages of these algorithms were evaluated.

Keywords: Cryptography, Cryptography Algorithms, Performance Analysis, Information Security, Image Cryptography

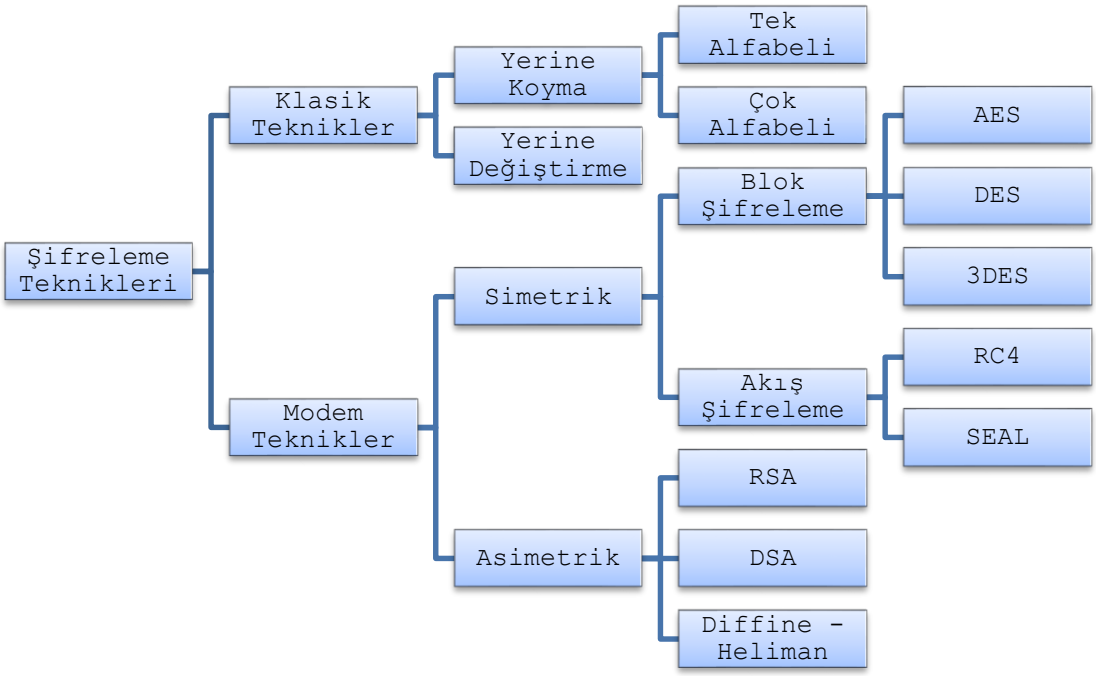
1. GİRİŞ (INTRODUCTION)

Teknolojinin gelişmesi ile veri aktarımında gizlilik ve güvenlik önem kazanmıştır. Dijital ortamlarda metnin yanı sıra ses, resim ve diğer çoklu ortam bilgileri de giderek artmaktadır. Günlük hayatımızda görüntü çok yaygın olarak kullanıldığından güvenliğini sağlamak da çok büyük önem kazanmıştır. Bu nedenle çok çeşitli şifreleme yöntemleri geliştirilmiştir. Bilgisayarların gücünün ve kapasitesinin artması ile bilgiler hızlı bir şekilde şifrelenerek iletilebilmektedir. Kullanılan şifreleme algoritmalarının güvenirliğinin test edilmesi de önemli bir konudur. Şekil 1'de görüldüğü gibi şifre bilimi yani Kriptoloji Kriptografi ve Kripoanaliz olmak üzere iki alt bilim dalına ayrılmaktadır. Kriptografi, herkese görünebilen verileri algılanmaz biçime getirmek için kullanılan bir bilimdir. Kriptoanaliz ise şifrelenmiş bir metnin analiz aşamalarını konu alır ve metni açık hale getirmek için kullanılabilecek metotları kapsar [1].



Şekil 1. Kriptoloji bilimi alt bilim dalları [1]
(Figure 1. Subfields of cryptography science)

Gelişen teknoloji ile şifreleme için uygulanan yöntemler de değişkenlik göstermiştir. Kriptografi algoritmaları Şekil 2'de görüldüğü gibi klasik ve modern olmak üzere iki ana kategoriye ayrılmıştır [2 ve 3].



Şekil 2. Şifreleme algoritmalarının sınıflandırılması [3]
(Figure 2. Classification of encryption algorithms)

Geçmişte sadece askeri ve bazı ileri akademik alanlarda kullanılan klasik şifreleme yöntemleri algoritması gizli olan şifreleme

yöntemlerini kapsamaktadır ve genellikle basit işlemlerle hesaplanabilecek algoritmalardan oluşmaktadır [4]. İlk klasik yöntemlerden biri olarak ENIGMA İkinci Dünya Savaşı döneminde kullanılmıştır [5]. Sezar, Vigenére, Vernam, Playfair, Hill sistemleri klasik yöntemlerden bazılarıdır. Metin şifrelenirken kullanılan dildeki harf sayısına göre şifreleme işlemi yapılır. Görüntü şifrelemede ise büyük/küçük harfler, nümerik rakamlar ve bazı operatörlerden oluşan 64 karakterlik bir alfabe (Base64) kullanılmaktadır (A-Z, a-z) (0-9)(+/). Görüntüler Base64 vasıtasıyla bir karakter dizisine dönüştürülür ve algoritmaya düz metin girdisi olarak verilir. Daha sonra şifreleme anahtarı ile girdi üzerinde algoritma çalıştırılır ve şifrelenmiş görüntüye karşılık gelen çıktı elde edilir. Bu çalışmada, mevcut klasik şifreleme algoritmalarının genel yapısı ve performansları hakkında bilgi verilerek sonuçlar analiz edilmiştir. Algoritmalar işlem zamanı, bellek kullanımı ve işlemci kullanımı [6, 7 ve 8] gibi kriterlere dayanılarak kıyaslanmıştır. Çalışmanın ikinci bölümünde kullanılan algoritmalar kısaca özetlenmiş, üçüncü bölümde yapılan deneysel çalışma anlatılmış, dördüncü bölümde analizlerden elde edilen bulgular tartışılmış ve beşinci bölümde ise sonuçlar verilmiştir.

2. ÇALIŞMANIN ÖNEMİ (RESEARCH SIGNIFICANCE)

Bu çalışmada klasik algoritmalardan yaygın olarak kullanılan Sezar, Vigenere, Vernam, Hill, Playfair algoritmalarının genel yapısı hakkında bilgi verilerek sözü geçen algoritmaların metinler ve Base64 tabanlı görüntü üzerindeki karşılaştırılmaları yapılmıştır. Metin ya da görüntüler şifreleme algoritmalarına girdi olarak verilerek anahtar ile şifrelenmiş metin elde edilmiştir ve algoritmalar çalışma zamanı (şifrelenme zamanı+şifre çözülme zamanı), zaman karmaşıklığı, işlemci karmaşıklığı, hafıza karmaşıklığı, kurulacak sisteme uygunluk, esneklik, güven oranı bakımından kıyaslanarak avantaj ve dezavantajları belirlenmiştir.

3. ÇALIŞMADA KULLANILAN KLASİK ALGORİTMALAR (CLASSICAL ALGORİTHMS USED IN THE STUDY)

3.1. Sezar Şifreleme (Caesar Cipher)

Tek alfabeli şifreleme yöntemidir. Bu yöntem öteleme şifrelemesi olarak da tanınmaktadır [11, 12 ve 13]. Matematiksel ifadesi Eşitlik 1 ile verilir:

$$E_k(m) = (m + k) \bmod N \quad (1)$$

m, açık metindeki o anki harfin sıra numarası, k, harfleri öteleme ölçüsüdür. N alfabedeki karakter sayısıdır. Şifreleme işlemi başlatıldıktan sonra orijinal görüntünün Base64 kod çıktısının her karakteri girilen anahtar sayısına göre ötelenerek Base64 tablosunda denk gelen sayının karşısındaki karakter alınır. Eşitlik 2 ile orijinal görüntü tekrar elde edilir.

$$E_k(m) = (m-k) \bmod 64 \quad (2)$$

3.2. Vigenere Şifreleme (Vigenere Cipher)

Bu yöntemde şifrelenmemiş metindeki her bir harf başka bir alfabeyle şifrelenir. Alfabenin seçimine anahtar kelimeye göre karar verilir. Anahtar kelimenin farklı seçilmesi, şifrelenmemiş metinde aynı kelimeler için farklı şifreli metinler oluşmasını sağlar. Vigenére şifreleme için alfabedeki harflerin yer aldığı bir tablo kullanılır. Bu tablo şifreleme ve şifre çözme eylemlerinde sabit olarak kullanılır [11, 12, 13, 14 ve 15].

Anahtar kelime= (a_1 , a_2, ……a_i) ve Düz metin = (d_1, d_2, ….., d_i) olmak üzere

$$fi(d) = (d+a_i) \bmod 64 \quad (3)$$

fi(d), şifreli metin, d, düz metin ve a, kullanılan anahtarı göstermektedir. Base64 kodundan ilk karakter alınıp onun tablodaki denk geldiği sıra numarası ile anahtardaki ilk karakterin sıra numarası toplanıp mod64 işlemi yapılarak şifreleme işlemi gerçekleştirilmiş olur.

Şifrelenmiş görüntüyü çözmek için de Eşitlik 4 kullanılır:

$$fi(d) = (d-a_i) \bmod 64 \quad (4)$$

3.3. Vernam Şifreleme (Vernam Cipher)

Bu yöntem Vigenére yöntemine benzemektedir. Farkı ikili sayı sistemine yer vermesi ve şifrelenmemiş metnin XOR (exclusive-or) işlemine tabi tutulmasıdır. Veri rastgele belirlenmiş ve kendisini tekrarlatmayan anahtarlar vasıtasıyla şifrelenir. Şifreleme işleminde ikili sistemde kodlanmış ASCII tablosu kullanılır. Rastgele belirlenen anahtar dizisinin her bir karakterine karşılık gelen ASCII koduna, şifrelenmemiş metinin her bir karakterinin ASCII kodu eklenerek (XOR) yeni şifreli karakter dizisi elde edilir [11, 12, 13, 14 ve 15]. Şifrelenmemiş M_1M_2…, anahtar dizi K_1K_2…, ve şifreli metin C1C2… ile temsil edildiğinde, şifreli görüntü Eşitlik 5 ile elde edilir:

$$C_i = (M_i \text{ XOR } K_i) \quad (5)$$

Şifreleme işleminde kullanılan anahtar karakterleri ve şifrelenmiş Base64 kodu üzerinde Eşitlik 6 kullanılarak orijinal Base64 kodu ve orijinal görüntü elde edilir

$$P_i = (C_i \text{ XOR } K_i) \quad (6)$$

3.4. Hill Şifreleme (Hill Cipher)

Bu yöntem, şifrelenmemiş metni bitişik ve aynı uzunluktaki bloklara bölerek şifreleyen ve bu şifreli blokları şifreli metin çıktısı olarak gruplara ayıran bir blok şifreleme algoritmasıdır. Hill şifrelemede şifreleme anahtarı olarak bir katsayılar matrisi (K) kullanılır. Katsayılar matrisinin elamanları ile şifrelenmemiş metindeki karakterlerin sayısal karşılıklarından oluşturulan matrisin elamanları çarpılır [11, 12, 13, 14 ve 15]. Şifrelenmemiş P, anahtar K, ve şifreli metin C, ile temsil edildiğinde, şifreli görüntü Eşitlik 7 ile elde edilir:

$$C = K * P \bmod 64 \quad (7)$$

Şifreleme işleminde kullanılan anahtarın tersi alınır ve Eşitlik (8)kullanılarak görüntü deşifre edilmiş olur:

$$P = K_{-1} * C \bmod 64 \quad (8)$$

3.5. Playfair Şifreleme (Playfair Cipher)

Bu yöntem yerine koyma yönteminin bir türüdür. 5X5'lik matris düzeni ile şifreleme işlemini gerçekleştirir [11, 12, 13, 14, 15 ve 16]. Orijinal görüntünün Base64 kodunu ikili gruplara ayırarak aynı grupta benzer harfler yan yana geldiğinde X ile ayrılır. Orijinal görüntünün Base64 kod karakter sayısı tek sayı ise sonuna X eklenir. Daha önceden ikili gruba ayrılan karakterler şifreleme tablosunu kullanarak başka karakterlerle değiştirilerek şifreleme işi gerçekleştirilmiş olur. 1. İkili grup aynı satırda ise her karakter bir hane sağ tarafa ötelenir. 2.İkili grup aynı sütunda ise her karakter bir hane aşağı kısma doğru ötelenir. 3.İkili grup farklı satır ve sütunda yer alırsa köşeleri alınır.

4. DENEYSEL ÇALIŞMA (EXPERIMENTAL STUDY)

Bu çalışmada şifrelemede kullanılan klasik yöntemlerin performanslarının görüntü şifreleme üzerinde kıyaslanması

hedeflenmektedir. Şifreleme algoritmalarının performans analizi genel olarak aşağıda belirtilen kriterler üzerinden yapılır [17 ve 18]:

- Şifreleme sistemin kırılabilme süresinin uzunluğu.
- Şifreleme ve çözme işlemlerine harcanan zaman(Zaman Karmaşıklığı).
- Şifreleme ve çözme işleminde ihtiyaç duyulan bellek miktarı
- Bu algoritmaya dayalı şifreleme uygulamalarının esnekliği.
- Bu uygulamaların dağıtımındaki kolaylık ya da algoritmaların standarthale getirilebilmesi.
- Algoritmanın kurulacak sisteme uygunluğu.

Çalışma kapsamında algoritmaların şifreleme ve şifre çözme için harcadıkları zaman, işlemci tüketimi ve hafıza tüketimi, sisteme uygunluk, esneklik, güven oranını metrikleri incelenmiştir. Metrikler üzerinden algoritmaların avantaj ve dezavantajlarının tespit edilmesi amaçlanmıştır. İyi bir şifreleme algoritması hem hızlı olmalı hem de bellek tüketimi az olmalıdır [19]. Geliştirilen uygulamaların kaynak tüketim değerleri Diagnostic tools aracılığıyla elde edilmiştir. "CPU Sampling" seçeneği ile CPU üzerindeki işlem yükü belirlenmiştir. "Instrumentation" seçeneği ile harcanan zaman ve çağrılan fonksiyon sayısı belirlenmiştir. "NET Memory Allocation" seçeneği ile bellek kullanımı belirlenmiştir. Çalışmada gerçekleştirilen testlerde farklı boyutta ve renklerde 4 görüntü kullanılmıştır. Bu görüntülerin seçilmesinde herhangi bir özel durum söz konusu değildir. Çalışmada kullanılan görüntüler Şekil 3'de verilmektedir.

Şekil 3. Çalışmada kullanılan görüntüler
(Figure 3. Images used in the study)

Tüm testler için aynı anahtar kullanılmakla birlikte Vernem algoritması anahtarını otomatik üretmektedir. Deneysel çalışmalar ve performans analizleri Windows 8.1 işletim sistemine sahip AMD E- 350 Processor 1.60 GHz dizüstü bilgisayar kullanılarak yapılmıştır. Algoritmaların gerçekleştirimleri Microsoft Visual Studio 2015 C# ile kodlanmıştır.

5. BULGULAR VE TARTIŞMA (FINDINGS AND DISCUSSIONS)

Beş farklı algoritmanın şifreleme ve çözme işlemlerinde performans analizi için aynı yöntemler kullanılmıştır.

Tablo 1-4'te kullanılan algoritmanın görüntüler üzerinde yapılmış şifreleme ve çözme işlemlerine ait elde edilen değerler görülmektedir. Tablolar da yer alan işlem zamanına ait değerler milisaniye, işlemci

kullanımına (CPU) ait değerler yüzde(%), hafıza kullanımına (RAM) ait değerler ise (Byte) türünden ifade edilmiştir.

Tablo 1. 2.5KB'lık görüntü (Erciyes Logo) üzerinde algoritmaların performans analiz değerleri
(Table 1. Performance Comparison of the algorithms on 2.5 KB image (Erciyes logo))

Algoritma	İşlem Zamanı (MS)		RAM Kullanımı (Byte)		CPU Kullanımı (%)	
	Şifreleme	Çözme	Şifreleme	Çözme	Şifreleme	Çözme
Sezar	22.36	25.59	127.94	127.76	90.75	92.99
Vigenere	24.68	26.52	241.46	241.20	88.91	91.15
Vernam	22.23	23.44	128.96	126.63	87.81	91.15
Hill	205.81	186.84	227.62	227.38	0.36	0.12
Playfair	160.84	139.43	194.45	194.43	0.53	0.37

Tablo 2. 1.83 KB'lık görüntü (Cameraman)için şifreleme ve çözme işlemeleri için algoritmaların performans analiz değerleri.
(Table 2. Performance Comparison of the algorithms on 1.83 KB image (Cameraman))

Algoritma	İşlem Zamanı (MS)		RAM Kullanımı (Byte)		CPU Kullanımı (%)	
	Şifreleme	Çözme	Şifreleme	Çözme	Şifreleme	Çözme
Sezar	124.3	84.38	515.0	2.032	15.93	16.60
Vigenere	89.79	99.95	1.020	2.537	17.17	16.92
Vernam	87.48	95.09	517.0	2.034	15.93	16.81
Hill	1.371	1.266	808.8	808.7	0.03	0.04
Playfair	771.8	1.041	814.0	814.0	0.10	0.11

Tablo 3. 1.10KB'lıkgörüntü (Lenna) için şifreleme ve çözme işlemeleri içinalgoritmaların performans analiz değerleri.
(Table 3. Performance Comparison of the algorithms on 1.10 KB image (Lenna))

Algoritma	İşlem Zamanı (MS)		RAM Kullanımı (Byte)		CPU Kullanımı (%)	
	Şifreleme	Çözme	Şifreleme	Çözme	Şifreleme	Çözme
Sezar	62.51	59.89	345.0	1.432	46.80	51.06
Vigenere	56.09	61.29	706.9	1.793	47.10	51.70
Vernam	54.78	67.96	346.6	1.433	46.51	51.78
Hill	770.0	766.0	529.8	829.6	0.03	0.36
Playfair	525.9	556.3	534.0	1.621	0.07	0.57

Tablo 4. 1.19 KB'lıkgörüntü (Peppers) için şifreleme ve çözme işlemeleri için algoritmaların performans analiz değerleri
(Table 4. Performance Comparison of the algorithms on 1.19 KB image (Peppers))

Algoritma	İşlem Zamanı (MS)		RAM Kullanımı (Byte)		CPU Kullanımı (%)	
	Şifreleme	Çözme	Şifreleme	Çözme	Şifreleme	Çözme
Sezar	95.53	118.5	505.4	1.998	17.45	18.67
Vigenere	91.60	105.3	1.002	2.495	18.94	19.36
Vernam	83.63	101.4	507.3	2.000	16.01	8.79
Hill	1.301	1.280	792.5	792.4	0.05	0.04
layfair	1.058	733.7	797.7	797.6	0.19	0.11

Performans değerlerinin karşılaştırılmasında doğru sonuçları elde edebilmek için, her algoritma dört farklı görüntü için çalıştırılmıştır. Farklı görüntüler için farklı sonuçlar elde edilmektedir. Görüntüdeki renklere göre Base64 Kodunda karakter sayıları değiştiği için her

algoritma 2.5KB'lık, 1.83KB'lık, 1.19KB'lık ve 1.10KB'lık farklı görüntüler üzerinde çalıştırılmıştır. Performans analizi çalışmalarında elde edilen sonuçlar anahtara göre de değişkenlik gösterdiği için anahtar bütün testlerde sabit 3 olarak belirlenmiştir. Anahtarın 3 olarak belirlenmesinde herhangi özel bir durum olmamakla birlikte Vernem Algoritması kendi anahtarını otomatik olarak üretmektedir. Algoritmaların beşi de aynı bilgisayarda ve aynı yazılım ortamında test edilmiştir.

Tablo 1, Tablo 2, Tablo 3 ve Tablo 4 incelendiği zaman değerler farklık göstermektedirler. Bunun nedeni farklı boyuttaki görüntüler üzerinde çalışılmasıdır. İşlem zamanı bakımından Vigenere algoritması Sezar ve Vernam Algoritmalarından daha fazla zaman harcayan ancak Hill ve Playfair Algoritmalarına göre daha avantajlı bir algoritmadır. Vernam Algoritmasının şifreleme ve çözme işlemlerinde diğer algoritmalara göre daha hızlı olduğu görülmektedir. Bu durum Vernam algoritmasının bitler üzerinde çalışmasından kaynaklanmaktadır. Bit düzeyinde çalışması Vernam Algoritması için işlem zamanı anlamında kazanç sağlamakta ve geçen sürenin azaltılmasında katkı sağlamaktadır. Karşılaştırma sonuçlarına işlem zamanı açısından bakıldığında Vernam algoritması performans sıralamasında birinci, Sezar Algoritması ikinci, Vigenere üçüncü, Playfair dördüncü ve Hill Algoritması beşinci sırada yer almaktadır.

Tablo 1, Tablo 2, Tablo 3 ve Tablo 4'te RAM kullanım sütunundan görüldüğü üzere bellek kullanımı açısından en düşük çıkan algoritma Sezar Algoritmasıdır. Bellek kullanımı açısından performans sıralamasına bakıldığında, Sezar birinci, Vernam ikinci, Playfair üçüncü, Hill dördüncü ve en son da Vigenere beşinci sıradadır. Sezar Algoritmasının ilk sırada olma sebebi verilerin tek bir dizide tutulması ve yer değişim işlemlerinin yapılmamasıdır. Diğer algoritmalarda ise veri birden fazla dizide tutulmakta, birden fazla işlem yapılmakta ve öteleme ile yer değişim işlemleri uygulanmaktadır.

Tablo 1, Tablo 2, Tablo 3 ve Tablo 4'teki CPU sütunundan görüldüğü üzere Sezar Algoritması CPU kullanımı açısından en yüksek değere sahiptir. Performansı en iyi olandan en kötü olana doğru sıralama yapıldığında Hill Şifreleme Algoritması birinci, Playfair Şifreleme Algoritması ikinci, Vernam Şifreleme Algoritması üçüncü, Vigenere Şifreleme Algoritması dördüncü ve Sezar Şifreleme Algoritması beşince sıradadır. Daha çok matematiksel işlem kullanan ve gruplar şeklinde işleyen algoritmaların daha az CPU kullandığı gözlemlenmiş; tüm dizini birden şifreleyen öteleme, yer değiştirme, harf değiştirme işlemlerine dayanan algoritmaların ise yüksek CPU tüketim değerlerine sahip olduğu görülmüştür. Bellek kullanım oranları ve CPU kullanım oranları arasında ters ilişki ortaya çıkmıştır. CPU kullanımı en yüksek olan Sezar Algoritmasının bellek kullanımı en düşüktür. Bu durumun sebebi ise algoritmaların kaynak kodlarındaki adım ve işlem sayısı olabilmektedir. Daha az kod satırı ile daha çok iş yapılması bu durumun temel nedeni olabilir. Genelde kullanılan algoritmalar gücü ve hızı düşük algoritmalardır. Sezar, Vigenere ve Playfair Algoritmalarının görüntü şifrelemek için esnek ve kolay algoritmalar olduğu görülmüştür. Ancak Vernam ve Hill Algoritmalarında bu esneklik bulunmamaktadır. Bunun sebebi Vernam Algoritması için çök uzun bir anahtar kullanılmasının gerekli oluşudur. Özellikle görüntü şifrelemede, görüntüye denk gelen Base 64 Kodu karakter sayısı 3436 olan (Erciyes Logo) görüntüsü için, 3436 karaktere sahip olan bir anahtar kullanmak zorundayız. Hill Algoritmasında bazen kullanılan anahtar için ters değer bulunamamaktadır. Orijinal görüntünün şifrelenmesi ve çözerken de orijinal görüntünün tekrardan elde edilmesi, oranı olan güven oranı(%),verilmektedir. Sezar,Vigenere ve Hill Algoritmaları için %100 olduğu tespit edilmiş, ancak Vernam %99 ve Playfair için %97 tespit

edilmiştir. Ayrıca algoritmalarda görüntü şifreleme ve çözme işlemlerinde verilerin sonuna eklenti gerekebildiğinden veri artışı da bulunabilmektedir.

6. SONUÇ VE ÖNERİLER (CONCLUSION AND RECOMMENDATIONS)

Güvenlik, iletişimde ve görüntü depolamada önemli bir unsurdur. Kriptoloji bu güvenliği sağlayan yöntemler bilimidir. İnternet, tıbbi görüntüler, multimedya ve askeri iletişimlerde şifreleme kullanılmaktadır. Klasik şifreleme algoritmalarından en yaygın olan Sezar, Vigenere, Vernam, Hill, Playfair Algoritmaları yapısı hakkında bilgi vererek farklı boyuttaki görüntüler üzerinde uygulama ve performans analizi yapılıp sonuçları karşılaştırılmıştır. Bu çalışmada sık kullanılan klasik algoritmaların uygulamaları gerçekleştirilmiştir ve zaman karmaşıklığı, islemci karmaşıklığı, hafıza karmaşıklığı bakımından kıyaslamaları yapılmıştır. Performans analizi incelemelerinde farklı boyuttaki görüntüler için CPU iş yükü, bellek kullanımı ve işlem sürelerinin değişken olduğu görülmüştür. Bu nedenle çalışmada sabit bir anahtar kullanılmıştır. CPU üzerindeki iş yükü açısından Hill Algoritması birinci, Playfair Algoritması ikinci, Vernam üçüncü, Vigenere dördüncü ve Sezar Algoritması beşinci olarak tespit edilmiştir. Bellek tüketimi açısından birinci Sezar Algoritması, ikinci Vernam, üçüncü Playfair, dördüncü Hill ve beşince Vigenere Algoritması olarak tespit edilmiştir.

İşlem zamanı açısından karşılaştırma yapılırsa en ideal algoritmanın Vernam olduğu görülmüştür. İkinci Sezar, üçüncü Vigenere, dördüncü Playfair ve beşinci Hill Algoritması olarak tespit edilmiştir. Klasik şifreleme sistemleri görüntüler için kullanılabilse de, iki nedenden dolayı sıkıntı çıkabilmektedir. Birincisi, görüntüler metin verilerine göre çok daha büyüktür. Bu nedenle klasik algoritmalar görüntüleri şifrelemek için yavaş kalmaktadırlar. Yazı verisinin şifresi çözüldüğünde orijinal yazının geri gelmesi gerekli iken, görüntü dosyalarında böyle bir zorunluluk yoktur. Şifresi çözülmüş bir görüntüde fark edilemeyecek kadar farklılıklar olabilmektedir ancak insan doğası nedeniyle bu değişiklikler fark edilemeyecek derecede azdır. Bu çalışma ve incelemeler sadece görüntüler üzerinde yapılmıştır. Dosya, ses ve video için de geliştirilebilir ve amaçlara yönelik metotlarla işlem zamanının indirgenebilir veya daha az bellek tüketmesi sağlanabilir.

NOT (NOTE)

Bu çalışma, 1-4 Eylül 2016 tarihleri arasında İstanbul-Büyükada'da yapılan International Science Symposium (ISS2016)' da sözlü bildiri olarak sunulduktan sonra genişletilmiş ve yeniden yapılandırılmıştır.

TEŞEKKÜR (ACKNOWLEDGMENT)

Bu çalışmanın gerçekleştirilmesi için gereken desteğinden dolayı Erciyes Üniversitesi Bilimsel Araştırma Projeleri Birimi'ne teşekkür ederiz (FYL-16-6463).

KAYNAKLAR (REFERENCES)

1. Sağıroğlu, Ş. ve Alkan, M., (2005). Bilgi Güvenliği Bilimi (Kriptoloji), Her Yönüyle Elektronik İmza, Grafiker Yayınları, Ankara.
2. Dalkılıç, G. ve Akın, O., (2005). Anahtar Tabanlı Gelişmiş Rotor Makinesi, Akademik Bilişim Konferansı, Gaziantep.
3. Bayar, E., (2012). Modern Kriptosistemlerle Şifrelemenin Modellenmesi İle VeriGüvenliğinin Sağlanması, Yüksek Lisans Tezi. İstanbul: Marmara Üniversitesi Fen Bilimleri Enstitüsü.

4. Buluş, H.N., (2006). Temel Şifreleme Algoritmaları ve Kripto analizlerinin İncelenmesi, Yüksek Lisans Tezi. Edirne: Trakya Üniversitesi Fen BilimleriEnstitüsü.
5. Yılmaz, R., (2010). Kriptolojik Uygulamalarda Bazı İstatistik Testler, YüksekLisans Tezi. Konya: Selçuk Üniversitesi Fen Bilimleri Enstitüsü.
6. Ülker, Ü., (2014). Klasik Teknikler Kullanılarak Bir Kriptografi Algoritması Geliştirilmesi ve Des Algoritması İle Performans Analizlerinin Karşılaştırılması, Yüksek Lisans Tezi. Ankara: Gazi Üniversitesi Bilişim Enstitüsü.
7. OBAID, Z., (2016). Kriptoloji Yöntemlerinin Karşılaştırılması, Yüksek Lisans Tezi. Kayseri: Erciyes Üniversitesi Fen Bilimleri Enstitüsü.
8. Günden, Ü., (2010). Şifreleme Algoritmalarının Performans Analizi, YüksekLisans Tezi. Sakarya: Sakarya Üniversitesi Fen Bilimleri Enstitüsü.
9. Kodaz, H. ve Botsalı, F.M., (2010). Simetrik ve Asimetrik Şifreleme Algoritmalarının Karşılaştırılması, Selçuk Üniversitesi Teknik Bilimler MeslekYüksekokulu Teknik-Online Dergi. Konya, 9(1):10-23.
10. What is base64 encoding and how can we benefit from ithttp://inchoo.net/magento/what-is-base64-encoding-and-how(Date accessed: November2015).
11. Stallings, W., (2003). Cryptography and Network Security, Third Edition. New Jersey.
12. Henk, C.A. van Tilborg (2016). Fundamentals Of Cryptology, A Professional Reference and Interactive Tutorial, London, Boston,Dordrecht. Eindhoven University of Technology The Netherlands, Kluwer Academic Publishers (Erişim Tarihi:20.06.2016).
13. Kenneth, H.R., (2007). An Introduction To Cryptography, Second Edition, Discrete Mathematics And Its Applications.
14. Canbek, G. ve Sağıroğlu, Ş., (2006). Bilgi ve Bilgisayar Güvenliği Casus Yazılımlarve Korunma Yöntemleri, Ankara. Grafiker Yayınları.
15. Çeşmeci, M.Ü., (2009). Kriptoloji Tarihi, UEKAE Dergisi,1.
16. Denning, R.D.E., (1982). Encyption Algorithms, Cryptography and Data Security, America, United States.Addison-Wesley Publishing.
17. Yerlikaya, T., (2006). Yeni Şifreleme Algoritmalarının Analizi, Doktora Tezi. Edirne: Trakya Üniversitesi Fen Bilimleri Enstitüsü.
18. Yerlikaya, T., Buluş, E. ve Buluş, N., (2006). Asimetrik Şifreleme Algoritmalarında Anahtar Değişim Sistemleri, Akademik Bilişim Konferansı, Denizli.
19. Bahçetepe, H., (2006). Modüler Çarpma Algoritmalarının İncelenmesi veKriptolojide Uygulanması, Yüksek Lisans Tezi. İstanbul: İstanbul Üniversitesi FenBilimleri Enstitüsü.