SAKARYA UNIVERSITY JOURNAL OF COMPUTER AND INFORMATION SCIENCES
VOL. 2, NO. 3, DECEMBER 2019
DOI: 10.35377/saucis.02.03.648493

The Performance Comparison of Lightweight Encryption Algorithms

Ünal ÇAVUŞOĞLU[1], Hussein AL-SANABANI[2]
[1]Corresponding Author; Bilgisayar Mühendisliği, Sakarya Üniversitesi; unalc@sakarya.edu.tr; https://orcid.org/0000-0002-5794-6919; 0264 295 65 40
[2]Fen Bilimleri Enstitüsü, Sakarya Üniversitesi; hussein.sanabani@ogr.sakarya.edu.tr; https://orcid.org/0000-0001-6580-4470

Received 19 November 2019; Revised 16 December 2019; Accepted 23 December 2019; Published online 31 December 2019

Abstract

In recent years, security has become more critical, especially with the introduction of the Internet in all areas of our lives and developments in the Internet of Things (IoT) platform. He studies on security algorithm designs to be used in these platforms are increasing day by day. In order to use these algorithms safely, they must have sufficient security levels. In this study, cryptography algorithms are used to perform performance and security analysis of lightweight encryption algorithms. In the security and performance analyzes, histogram, correlation, NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity), entropy, encryption quality and time analyzes of the encryption processes are performed. Using the obtained results, evaluation of the security and performance levels of the algorithms is presented.

Keywords: lightweight algorithm, image encryption, performance comparison

Hafif Sıklet Şifreleme Algoritmalarının Performans Karşılaştırması

Öz

Son yıllarda özellikle internetin hayatımızın her alanına girmesi ve nesnelerin interneti (IoT) platformundaki gelişmeler ile birlikte güvenlik daha kritik bir duruma gelmiştir. Bu platformlarda kullanılacak olan güvenlik algoritma tasarımları üzerinde çalışmalar günden güne artış göstermektedir. Bu algoritmaların güvenli bir şekilde kullanılabilmesi için yeterli güvenlik seviyelerine sahip olmaları gerekmektedir. Bu çalışmada, hafif sıklet kriptoloji algoritmalarının performans ve güvenlik analizlerini gerçekleştirmek için farklı resim dosyaları üzerinde şifreleme işlemleri yapılmıştır. Güvenlik ve performans analizlerinde şifreleme işlemlerine ait histogram, korelasyon, NPCR (Number of Pixels Change Rate) ve UACI (Unified Average Changing Intensity), entropi, şifreleme kalite ve zaman analizleri gerçekleştirilmiştir. Elde edilen sonuçlar kullanılarak algoritmaların güvenlik ve performans seviyeleri hakkında değerlendirme sunulmuştur.

Anahtar Kelimeler: Hafif sıklet şifreleme algoritmaları, resim şifreleme, performans karşılaştırması

1. Giriş

Hafif sıklet şifreleme algoritmaları sınırlı kaynaklara sahip cihazlar üzerinde güvenli bir haberleşme sağlanması için tasarlanan hafif işlem yüküne sahip tasarımlardır. Özellikle Nesnelerin interneti gibi kavramların gelişmesi ile hayatımızın her alanında internete bağlı çok fazla sayıda cihaz kullanılmaya başlanmıştır. Bu durum güvenlik ve kişisel mahremiyetin korunmasını çok daha önemli bir duruma getirmiştir. IoT ağında kullanılan cihazlar genellikle düşük işlem gücüne, hafızaya ve enerji kaynağına sahip cihazlardan oluşmaktadır. Bu sebeple bu cihazlar üzerinde çalışacak olan program ve algoritmaların daha az işlem yükü ve bellek gereksinimine sahip, daha az enerji tüketecek şekilde tasarlanması gerekmektedir. Bununla birlikte kullanılacak olan algoritmaların güvenlik seviyesinden ödün vermemeleri istenmektedir. Geleneksel standart olarak kabul edilen algoritmaların bu platformda kullanılması durumunda aşırı işlem yükünden dolayı gecikmeler, fazla enerji tüketimi ve bellek gereksinimlerinin yetersiz kaldığı görülmektedir. Hafif sıklet kriptoloji güvenlik zafiyetine sebep olmadan, düşük maliyetli ve performanslı şifreleme gerçekleştirmeyi amaçlamaktadır. Hafif sıklet

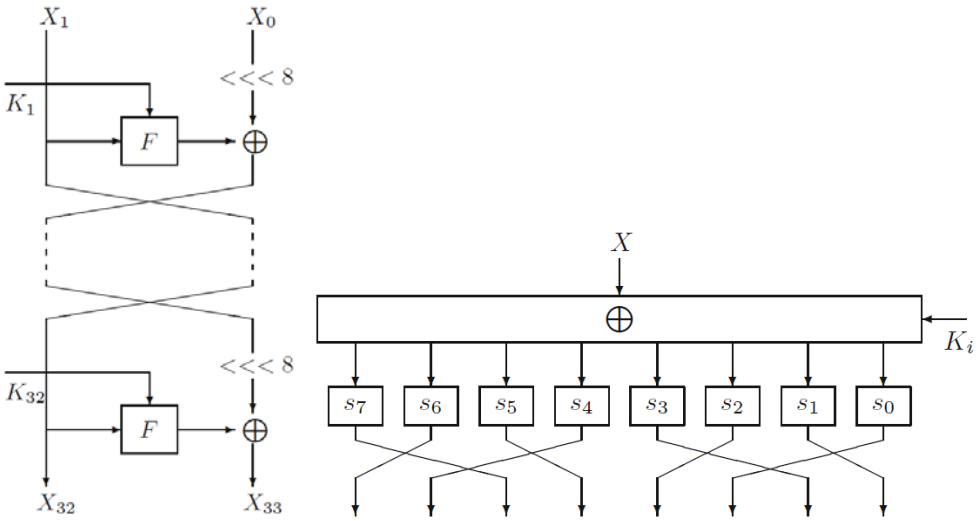
şifreleme algoritmalarının çok farklı kullanım alanları bulunmaktadır. Örneğin kablosuz vücut alan (WBAN) [1-2], Smart cards[3-4], Nesnelerin İnterneti [5-9], Kablosuz algılayıcı ağlar (WSN) [10-12].Bu çalışmanın amacı hafif sıklet kriptoloji algoritmalarının performans ve güvenlik analizini gerçekleştirmektir. Bu amaçla literatürdeki hafif sıklet kriptoloji algoritmalarının resim şifreleme üzerindeki performans ve güvenlik analizleri yapılmıştır. Hafif sıklet şifreleme algoritmalarından bazıları seçilerek AES algoritması ile karşılaştırması gerçekleştirilmiştir. Şifreleme işlemlerinde kullanılan algoritmalar tanıtılmış, ardından farklı resim dosyaları üzerinde şifreleme işlemleri gerçekleştirilmiş ve sonuçları sunulmuştur. Şifreleme işlemlerine ait korelasyon, histogram, NPCR (Number of Pixels Change Rate) ve UACI (Unified Average Changing Intensity), bilgi entropi, şifreleme kalitesi ve zaman analizleri gerçekleştirilmiştir. Bu analizler kullanılarak algoritmaların güvenlik/performans değerlendirmesi sunulmuştur. Makalenin planı şu şekildedir: giriş bölümünün ardından şifreleme algoritmaları hakkında bilgi verilmiş, ardından 3. Bölümde resim şifreleme işlemi gerçekleştirilmiş ve performans analizleri yapılmıştır. Son bölümde ise elde edilen sonuçlar kullanılarak değerlendirme yapılmıştır.

2. Hafif Sıklet Şifreleme Algoritmaları

Literatürde çok sayıda hafif sıklet şifreleme algoritması tasarımı bulunmaktadır. Literatürdeki algoritmalar incelendiğinde, anahtar uzunlukları, şifre blok boyutları, mimarileri ve döngü sayısı gibi özellikler açısından bir birinden oldukça farklı oldukları görülmektedir. Bu bölümde resim şifreleme işlemlerinde kullanılan LBLock, Klein, AES ve S-AES şifreleme algoritmalarının tanıtımı yapılmış ve kısaca mimarileri açıklanmıştır. Tablo 1'de bazı şifreleme algoritmalarına ait özellikler verilmiştir.

Tablo 1 Şifreleme algoritmaları

Algoritma	Anahtar uzunluğu	Mimarisi	Blok boyutu	Döngü sayısı
AES [13]	128/192/256	SPN	128	10/12/14
S-AES [14]	128	SPN	128	2
DES [15]	54	Feistel	64	16
3DES [16]	56/112/168	Feistel	64	48
Hight [17]	128	Feistel	64	32
Kasumi [18]	128	Feistel	64	8
LBlock [19]	80	Feistel	64	32
Klein [20]	64/80/96	SPN	64	12/16/20
Present [21]	80/128	SPN	64	31
RC6 [22]	128/192/256	Feistel	128	20
Ktantan [23]	80	Stream	32/48/64	254



Şekil 1 LBlock algoritması blok diyagramı ve F fonksiyonun içeriği [19]

2.1 LBlock algoritması

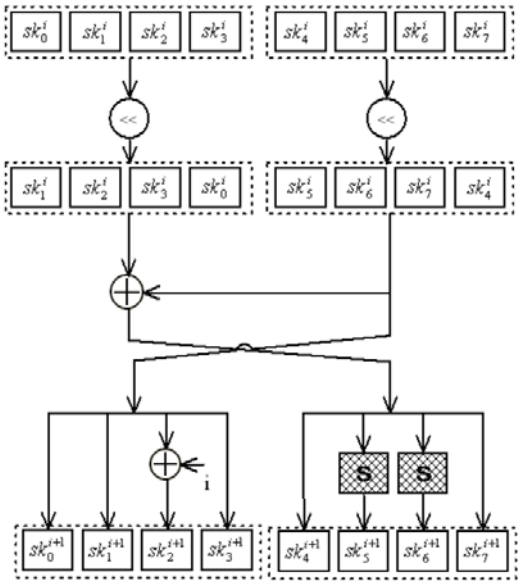
LBlock algoritması Feistel ağ yapısına sahip 64 bit blok boyutuna sahip, anahtar uzunluğu 80 bit ve32 döngüden oluşan bir şifreleme algoritmasıdır. 2011 yılında Wu ve Lei tarafından tasarımı gerçekleştirilmiştir. Her bir çevrim anahtar ekleme, S-kutusu katmanı ve kelimelerin permütasyonundan oluşur. Kendine özgü bir anahtar şeması olan L-Block, 80 bitlik ana anahtardan her bir çevrim için 32 bit çevrim anahtarı üretir. Literatürde yapılan kriptanaliz çalışmalarında L-Block algoritmasının güvenlik seviyesi açısından kabul edilebilir olduğu gösterilmiştir ve algoritma üzerinde analiz çalışmaları devam etmektedir. [24-25].

2.2 Klein algoritması

Klein algoritması 2012 yılında Gong ve arkadaşları tarafından tasarlanmış bir şifreleme algoritmasıdır. Farklı anahtar boyutu ve döngü sayılarına sahiptir. Anahtar uzunluğunun boyutuna göre döngü sayısı değişiklik göstermektedir. SPN mimarisine sahip bir algoritmadır. Şifrelenecek olan veri blokları bölünmeden tamamı döngüye girmektedir. 64/80/96 olmak üzere 3 farklı anahtar boyutunda şifreleme gerçekleştirilebilir. Blok boyutu ise 64 bit olarak tasarlanmıştır. Döngü sayısı ise anahtar boyutuna bağlı olarak 12/16/20 olarak değişmektedir. Şekil 2'de Klein algoritmasına ait sözde kod görülmektedir. Bir döngüde sırasıyla Addrounkey, SubNibbles, RotateNibbles ve MixNibbles işlemleri gerçekleştirilmektedir. Ayrıca Şekil 3'te algoritmanın anahtar üretim sürecine ait blok diyagram verilmiştir.

$sk^1 \leftarrow \text{KEY};$
STATE $\leftarrow$ PLAINTEXT;
for $i = 1$ *to* N_R do
  $AddRoundKey(\text{STATE}, sk^i);$
  $SubNibbles(\text{STATE});$
  $RotateNibbles(\text{STATE});$
  $MixNibbles(\text{STATE});$
  $sk^{i+1} = KeySchedule(sk^i, i);$
end for
CIPHERTEXT $\leftarrow AddRoundKey(\text{STATE}, sk^{N_R+1});$

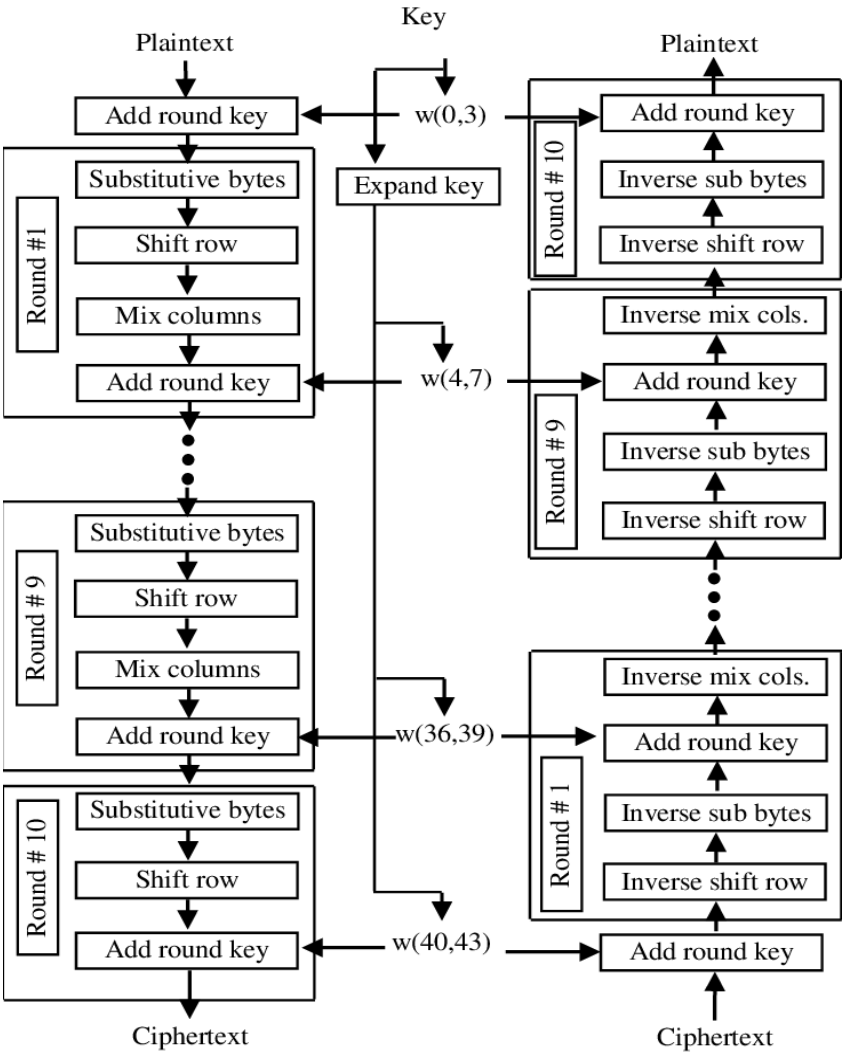
Şekil 2 Klein algoritması sözde kodu[20]



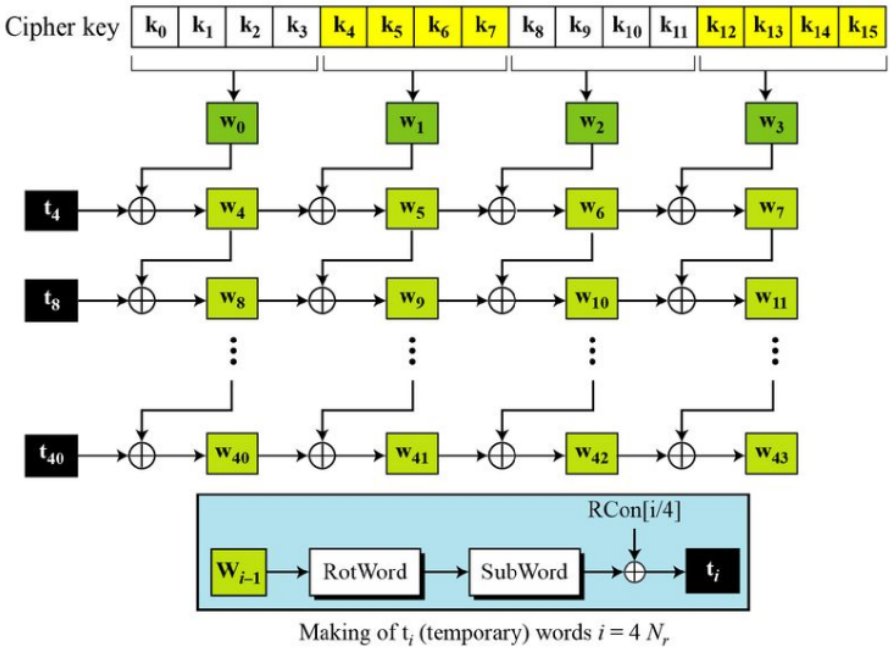
Şekil 3 Klein algoritması anahtar üretimi[20]

2.3 AES/S-AES algoritması

AES algoritması J.Daemen ve V. Rijmen tarafından geliştirilmiş, block iterasyon işlemleri ile gerçekleştirilen, substituion-permutation network(SPN) olarak bilinen simetrik blok şifreleme algoritmasıdır. AES şifreleme algoritmasının kullanılan birçok versiyonu bulunmaktadır. AES algoritması key uzunluğu 128, 192, 256 bit olmak üzere farklı boyutlarda gerçekleştirebilmektedir. AES-128 10, AES-192 12 ve AES-256 14 döngüde şifreleme işlemlerini gerçekleştirir. AES algoritmasının anahtar uzunluğu algoritmayı kaba kuvvet saldırılarına karşı dayanıklı hale getirmektedir. S-AES algoritması ise daha az işlem gücü ve kaynak kullanımı maksadıyla AES algoritmasının basitleştirilmiş versiyonudur. S-AES algoritmasında toplamda 2 döngüde daha az işlem gücü ve kaynak kullanımı ile şifreleme işlemi gerçekleştirilmektedir. AES algoritmasının bir döngüsünde bayt değişimi, satır kaydırma, sütun karıştırma ve döngü anahtarının eklenmesi olmak üzere 4 adım bulunmaktadır. Son döngüde sütunları karıştırma işlemi gerçekleştirilmez. Diğer tüm döngülerde bu 4 adım sırasıyla gerçekleştirilmektedir. AES blok şifreleme işlemleri 128 bit şifreleme için durum adı verilen 16 bayt 4x4 durum matrisi üzerinde gerçekleşmektedir. Şifre çözme sürecinde ise, şifreleme işleminde gerçekleştirilen işlemlerin tersi gerçekleştirilerek, orjinal veri elde edilmektedir. Şifreleme işlemine başlamadan önce 16 bayt uzunluğundaki şifrelenecek olan veri durum matrisi diye ifade edilen 4x4 lük bir matris şekline getirilmektedir. Algoritmada her döngüde kullanılmak üzere oluşturulacak anahtarlar, anahtar genişletme algoritması kullanılarak üretilmektedir. Şekil 4'te AES algoritması blok diyagramı ve Şekil 5'te anahtar üretim işlemine ait blok diyagram görülmektedir.



Şekil 4 AES algoritması blok diyagramı [26]



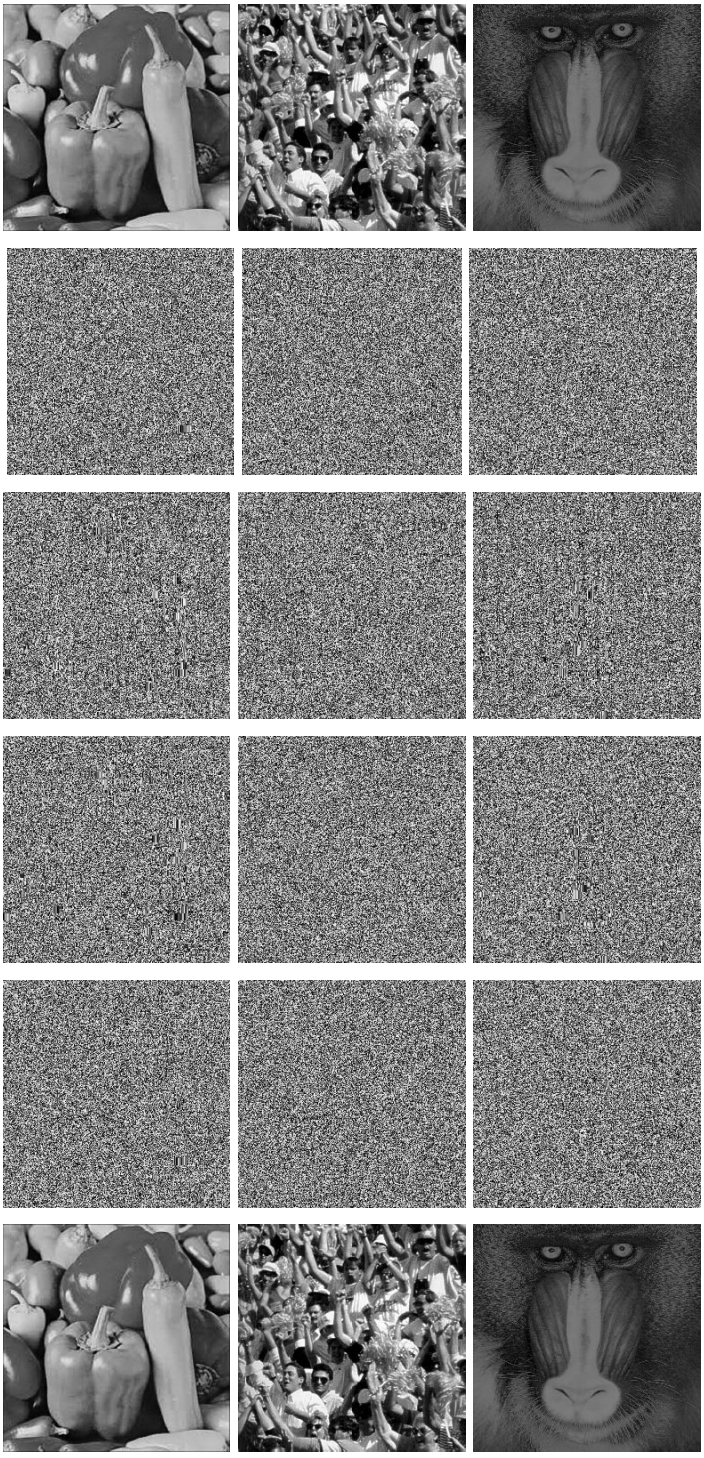
Şekil 5 AES algoritması anahtar üretim algoritması [27]

3. Resim Şifreleme Uygulaması ve Güvenlik/Performans Testleri

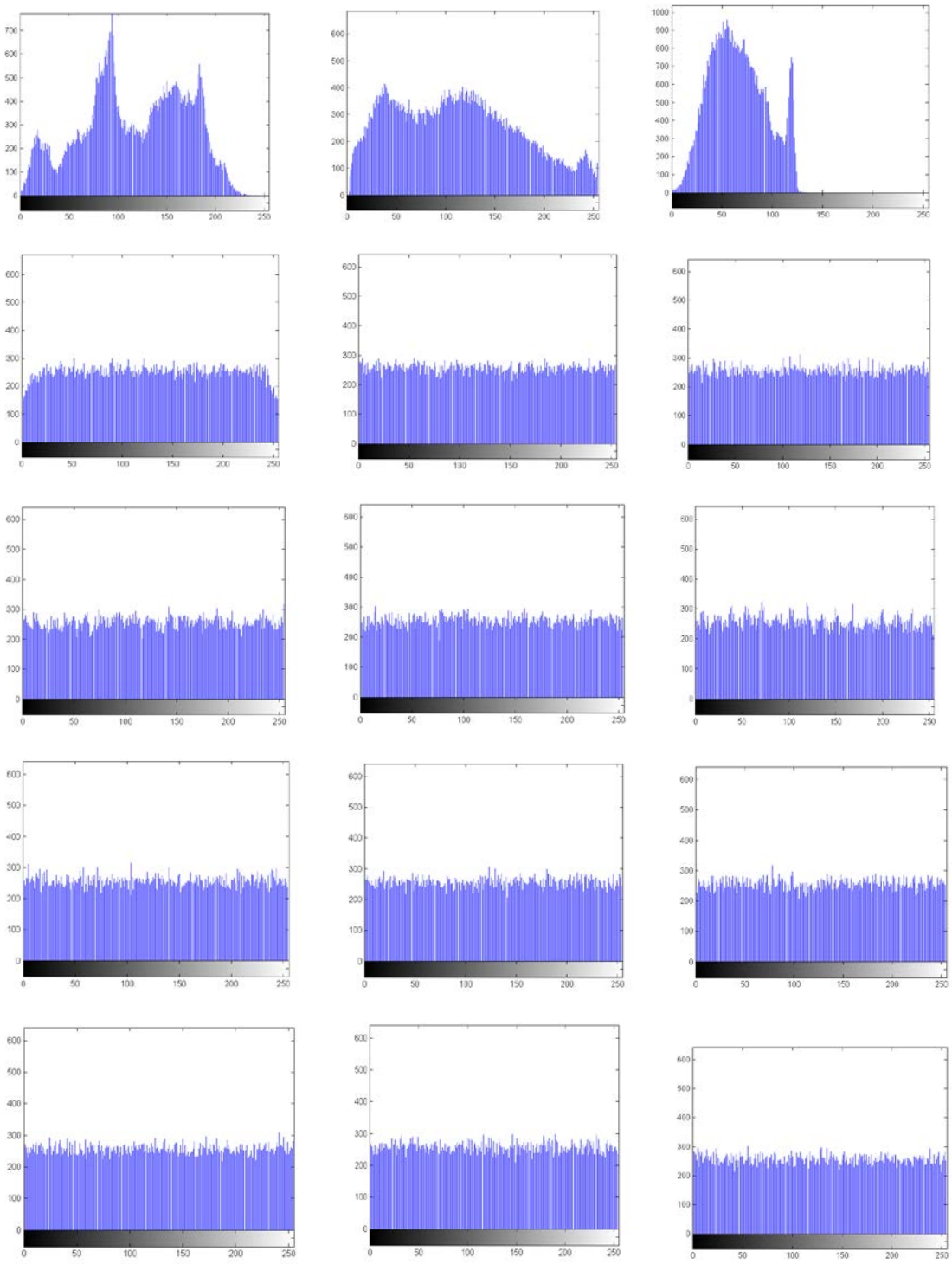
3.1 Resim Şifreleme Uygulaması

Hafif sıklet şifreleme algoritmalarının güvenlik ve performans ölçümlerini gerçekleştirmek için 256x256 boyutundaki farklı resim dosyaları üzerinde şifreleme ve çözme işlemleri gerçekleştirilmiştir. Şifreleme işleminde 256*256 boyutundaki pepper.png / crowd.png / baboon.png resim dosyaları kullanılmıştır. Şekil 6'de orijinal resim dosyaları ve sırasıyla LBlock, Klein, AES ve S-AES algoritmaları ile şifreleme sonucu elde edilen çıktılar verilmiştir. Şekil 6'da en son satırda ise şifre çözme işlemi sonucu elde edilen çözülmüş resim dosyaları görülmektedir. Çözülmüş resim dosyaları ile orijinal dosyalar kıyaslandığında işlemin başarılı bir şekilde gerçekleştirildiği görülmektedir.

Korelasyon analizi [28], iki rassal değişken arasında ilişkinin hesaplanması temeline dayanır. Kovaryans, iki rasgele değişkenin birlikte değişim değerini hesaplamaktadır. Korelasyon analizinde korelasyon katsayısı tespit edilmektedir. Korelasyon katsayısı bu iki değişken arasındaki ilişkinin, bağımsızlık durumunu göstermektedir. Rasgele herhangi bir sayıdaki çift yakın piksel, resimden alınarak, Denklemde verilen formül yardımıyla her çiftin korelasyon katsayısı hesaplanabilir [29]. Denklem 1'de x ve y resimdeki bitişik iki pikselin değerleri ve N seçilen piksel çiftinin sayısını göstermektedir. Şekil 8'de original resimlere ve şifreleme sonucu elde edilen resimlere ait korelasyon grafikleri sırasıyla verilmiştir. Tablo 2'de ise hesaplanan korelasyon katsayıları görülmektedir. Sonuçlar değerlendirildiğinde algoritmaların tamamının iyi bir seviyede dağılım gerçekleştirdiği tespit edilmiştir.



Şekil 6 Resim şifreleme uygulaması sonuçları



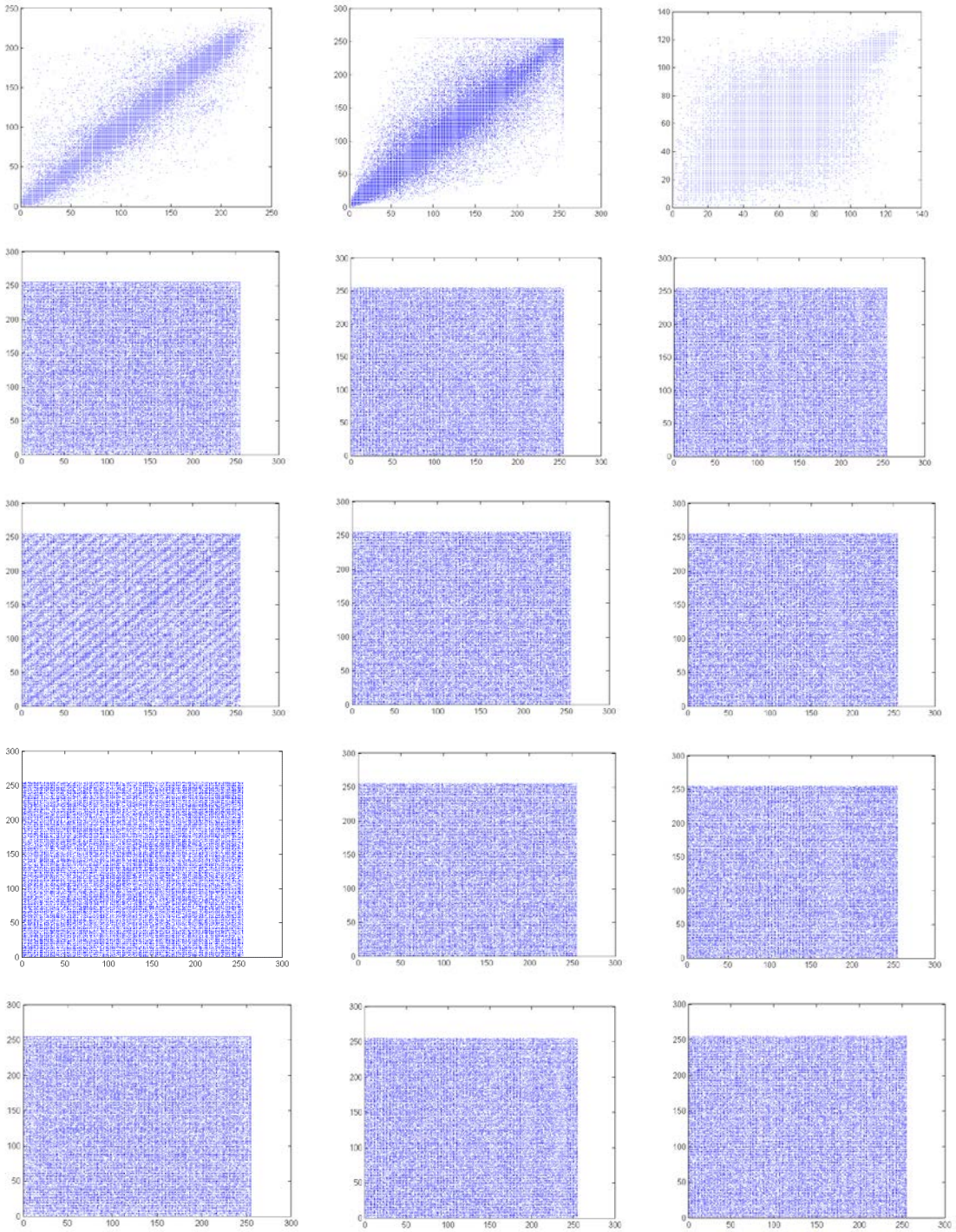
Şekil 7. Histogram Analizi Sonuçları

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2$$

$$\mathrm{cov}(x, y) = \frac{1}{N}(\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y))) \quad (1)$$

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)D(y)}}$$



Şekil 8 Korelasyon Analizi Sonuçları

NPCR (Number of Pixels Change Rate) ve UACI (Unified Average Changing Intensity), analizleri Biham ve Shamir [30] tarafından geliştirilen diferansiyel kriptoanaliz, orijinal resim üzerindeki küçük değişimlerin şifreli resimler üzerinde nasıl bir etki meydana getirdiğini incelemektedir. Rasgele seçilmiş orijinal resim ve değiştirilmiş pikselinin aynı anahtar kullanılarak gerçekleştirilen şifreleme sonuçları karşılaştırmakta, bu değişimlerden elde ettiği bilgiyi kullanarak şifreyi çözmeyi denemektedir. Orijinal resimdeki küçük değişimler, şifreli resim üzerinde büyük değişimlere yol açıyor ise, şifrelemenin diferansiyel atak saldırılarına karşı dirençli olduğunu göstermektedir. NPCR ve UACI değerlerinin en uygun değerleri şu şekildedir: $NPCR_{opt}$ = 99.61% ve $UACI_{opt}$ =33.46% [31]. Tablo 2'de şifreleme işlemlerine ait sonuçlar görülmektedir. İki resim arasındaki ilişkiyi belirleyen NPCR değeri denklem 2'de verildiği gibi hesaplanmaktadır.

$$NPCR(A,B) = (\sum_{(i,j)} \frac{D(i,j)}{N}) * 100\%$$

$$D(i,j) = \begin{cases} 1 \leftarrow if \cdots A(i,j) \neq B(i,j) \\ 0 \leftarrow if \cdots A(i,j) = B(i,j) \end{cases} \quad (2)$$

İki resim arasındaki ortalama yoğunluğu ifade eden UACI değerinin hesaplanması için kullanılan formül Denklem 3'te verilmiştir. Denklemde verilen A(i,j) ve B(i,j) değerleri önceki ve sonraki pikselleri ifade ederken, L değeri ise resmin pikselini ifade eden bit sayısıdır. N değeri ise NPCR' de olduğu gibi toplam piksel sayısını ifade etmektedir. Tablo 2'de şifreleme işlemlerine ait NPCR ve UACI değerleri görülmektedir. Analiz sonuçlarına göre, geliştirilen şifreleme algoritması saldırılara dayanıklı bir şifreleme gerçekleştirmiştir.

$$UACI(A,B) = \frac{1}{N} (\frac{\sum_{(i,j)} (|A(i,j) - B(i,j)|)}{(2^L - 1)}) * 100\% \quad (3)$$

Bilgi entropi analizi [32] şifreli verinin karmaşıklığını ölçmek için kullanılan metotlardan birisidir. Çalışmada bu analiz için Shannon Entropi metodu kullanılmıştır. Denklem 4'de Shanon bilgi entropi formülü verilmiştir. Formülde N olasılık kütle fonksiyonun değerlerinin sayısı, $p_i(x)$ i. sıradaki olasılık kütle fonksiyonu değeridir. 256x256 resim dosyaları için ideal entropi değerinin 8 olması beklenmektedir. Şifrelenen verinin entropi değeri 8'e ne kadar yakınsa şifreleme işlemi o kadar iyi bir entropi değerine sahiptir. Tablo 2'de verilen sonuçlara göre şifreleme işlemlerinde optimal değere yakın sonuçlar elde edildiği görülmektedir.

$$ShanEn(x) = -\sum_{i=1}^{N} (p_i(x))^2 (\log_2 p_i(x))^2 \quad (4)$$

Şifreleme kalitesi analizinde [33], şifreleme işleminden önceki ve sonraki piksel değişim değerleri karşılaştırılarak, şifreleme kalitesi ölçülmektedir. Şifreleme işleminin ardından hemen hemen bütün piksellerde değişim gerçekleşmektedir. Piksel değişim değerleri ne kadar fazlaysa, şifreleme kalitesi artmaktadır. Denklemde görüldüğü üzere, orijinal resim ve şifreli resim arasındaki sapma şifreleme kalite değerini belirlemektedir. Tablo 2'de şifreleme işlemlerine ait şifreleme kalitesi değerleri görülmektedir.

$$Enc.Quality = \frac{\sum_{L=0}^{255} |H_L(C) - H_L(P)|}{256} \quad (5)$$

Tablo 2 Performans Testleri Sonuçları

	Algorithms	**Correlation**	**NPCR**	**UACI**	**Entropy**	**Enc. Quality**	**Time**
Bipper.png	AES	-0.0018	0.9963	0.2965	7.9972	31.2109	61.564
	LBlock	0.0556	0.9959	0.2924	7.9958	28.234	3.1416
	Klein	0.043	0.9957	0.2968	7.9966	28.623	70.345

	S-AES	0.00151	0.9963	0.2954	7.9973	28.652	8.7452
Fan.png	AES	0.0009617	0.9962	0.3162	7.9975	34.9492	61.918
	LBlock	0.001443	0.9956	0.3151	7.9966	35.0429	3.1012
	Klein	-0.00767	0.9956	0.3162	7.9971	35.138	71.5888
	S-AES	-0.00289	0.9961	0.3161	7.9970	34.6522	8.8098
Baboon.png	AES	0.0008293	0.9962	0.3196	7.9970	60.8865	61.9247
	LBlock	0.0028922	0.9954	0.3142	7.9947	60.3433	3.12906
	Klein	0.002239	0.9957	0.32012	7.9967	61.9648	71.6887
	S-AES	0.0001799	0.9960	0.3198	7.9970	61.3962	8.6532

4. Sonuçlar

Hafif sıklet şifreleme algoritmaları hafif işlem yükleri, düşük kaynak ve enerji tüketim değerlerine sahip olduklarından dolayı özellikle kısıtlı kaynaklara sahip cihazlarda güvenli iletişim için yaygın olarak kullanılmaktadır. Fakat azaltılmış işlem hacimlerinden dolayı güvenlik noktasında zafiyete sebep vermemeleri gerekmektedir. Bu makalede hafif sıklet şifreleme algoritmalarının performans analizleri gerçekleştirilmiştir. İlk olarak seçilen hafif sıklet şifreleme algoritmalarının çalışma prensipleri açıklanmıştır. Ardından farklı resim dosyaları kullanılarak, şifreleme işlemleri gerçekleştirilmiştir. Tablo 2'de şifreleme işlemlerine ait analiz sonuçları toplu olarak görülmektedir. Genel olarak değerlendirildiğinde AES, LBlock, Klein ve S-AES algoritmaları ile yapılan farklı şifreleme işlemlerinde tüm algoritmaların iyi analiz sonuçlarına sahip oldukları görülmektedir. LBlock algoritmasının mimarisi ve hafif işlem yükünden dolayı iyi bir güvenlik seviyesine sahip olmasının yanında karşılaştırma yapılan diğer algoritmalarından çok daha kısa bir zamanda işlem gerçekleştirmiştir. LBlock algoritması ile birlikte AES algoritmasının döngü azaltılmış versiyonu S-AES algoritması da LBlock algoritmasından sonra şifreleme işlemlerini oldukça kısa sürede tamamladığı görülmektedir. Uzun yıllar standart olarak kullanılan AES algoritması ve Klein algoritmasının ise süre olarak LBlock ve S-AES algoritmasından kat kat uzun sürelerde işlem gerçekleştirdiği tespit edilmiştir. Sonuç olarak LBlock ve S-AES algoritmalarının hem yeterli güvenliği sağladığı hem de hızlı ve dolayısıyla daha az kaynak tüketen hafif sıklet algoritmalar olduğu ve kısıtlı kaynaklara sahip platformlarda güvenli iletişim için kullanılabileceği gösterilmiştir.

Referanslar

[1] C. Min et al. "Body area networks: A survey." *Mobile networks and applications*, vol. 16, no.2, pp. 171-193, 2011.

[2] Z. G. He, C. C.Y. Poon, and Y. T. Zhang. "A review on body area networks security for healthcare." *ISRN Communications and Networking*, 2011.

[3] B. Soumi and A. Patil. "ECC Based Encryption Algorithm for Lightweight Cryptography." *International Conference on Intelligent Systems Design and Applications. Springer, Cham*, 2018.

[4] R. Carsten, et al. "Ultra-lightweight implementations for smart devices–security for 1000 gate equivalents." *International Conference on Smart Card Research and Advanced Applications. Springer, Berlin, Heidelberg*, 2008.

[5] H. M. Asif et al. "Speeding Up the Internet of Things: LEAIoT: A Lightweight Encryption Algorithm Toward Low-Latency Communication for the Internet of Things." *IEEE Consumer Electronics Magazine*, vol7, no.6, pp. 31-37, 2018.

[6] M. Khan et al. "Secure surveillance framework for IoT systems using probabilistic image encryption." *IEEE Transactions on Industrial Informatics*, vol14, no.8, pp.3679-3689,2018.

[7] K. Masanobu and S. Moriai. "Lightweight cryptography for the internet of things." *Sony Corporation*, pp.7-10, 2008.

[8] S. Ankit and M. Engineer. "A survey of lightweight cryptographic algorithms for iot-based applications." *Smart Innovations in Communication and Computational Sciences. Springer, Singapore*, pp.283-293, 2019.

[9] S. Vijay, A.Vithalkar, and M. Hashmi. "Lightweight security protocol for chipless RFID in Internet of Things (IoT) applications." *2018 10th International Conference on Communication Systems & Networks (COMSNETS). IEEE*, 2018.

[10] W. Yawen and Y. Guan. "Lightweight location verification algorithms for wireless sensor networks." *IEEE Transactions on Parallel and Distributed Systems*,vol. 24, no.5, pp.938-950, 2012.

[11] K. Shankar and M. Elhoseny. "Multiple Share Creation with Optimal Hash Function for Image Security in WSN Aid of OGWO." *Secure Image Transmission in Wireless Sensor Network (WSN) Applications. Springer, Cham*, pp.131-146, 2019.

[12] M. Vandana, Y. Singh, and R. Bhatt. "A Review on Lightweight Node Authentication Algorithms in Wireless Sensor Networks." *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC). IEEE*, 2018.

[13] J. Daemen and V. Rijmen. "AES proposal: Rijndael.", 1999.

[14] A. M. Mohammad, F. Schaefer, and S. Wedig. "A simplified AES algorithm and its linear and differential cryptanalyses." *Cryptologia*, vol. 27,no.2, pp.148-177, 2003.

[15] Standard, Data Encryption. "Federal information processing standards publication 46." *National Bureau of Standards, US Department of Commerce*, vol. 23, 1977.

[16] A. Ross and M. Kuhn. "Low cost attacks on tamper resistant devices." *International Workshop on Security Protocols. Springer, Berlin, Heidelberg*, 1997.

[17] H. Deukjo et al. "HIGHT: A new block cipher suitable for low-resource device." *International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg*, 2006.

[18] B. Eli, O. Dunkelman, and N. Keller. "A related-key rectangle attack on the full KASUMI." *International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg*, 2005.

[19] W. Wenling and L. Zhang. "LBlock: a lightweight block cipher." *International Conference on Applied Cryptography and Network Security. Springer, Berlin, Heidelberg*, 2011.

[20] G. Zheng, S. Nikova, and Y. Wei Law. "KLEIN: a new family of lightweight block ciphers." *International Workshop on Radio Frequency Identification: Security and Privacy Issues. Springer, Berlin, Heidelberg*, 2011.

[21] B. Andrey et al. "PRESENT: An ultra-lightweight block cipher." *International workshop on cryptographic hardware and embedded systems. Springer, Berlin, Heidelberg*, 2007.

[22] L. Rivest, Ronald, et al. "RC6 as the AES." *AES Candidate Conference*, 2000.

[23] D. Canniere, O. Dunkelman, and M. Knežević. "KATAN and KTANTAN—a family of small and efficient hardware-oriented block ciphers." *International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg*, 2009.

[24] Y. Liu, D. Gu, Z. Liu, and W. Li, "Impossible Differential Attacks on Reduced-Round LBlock", *In ISPEC 2012*, pp. 97-108, 2012.

[25] L. Wen, M. Wang, and J. Zhao,"Related-Key Impossible Diferential Attack on Reduced-Round LBlock", J. *Comput. Sci. Technol.*, vol.29,no.1, pp.165-176, 2014.

[26] G. Wadday, M. Ahmed Salim and Hayder J. Mohammed Ali A. Abdullah. "Study of WiMAX Based Communication Channel Effects on the Ciphered Image Using MAES Algorithm." *International Journal of Applied Engineering Research*,vol.13, no.8, pp.6009-6018, 2018.

[27] A. Forouzan, Behrouz, "*Cryptography & network security*", *McGraw-Hill, Inc*., 2007.

[28] J. Cohen, *Statistical Power Analysis for the Behavioral Sciences*. New York: Academic Press, 1977.

[29] N. K. Pareek, V. Patidar, K. K.Sud, "Image encryption using chaotic logistic map", *Image and Vision Computing*, vol.24, no.9, pp. 926–934, 2006.

[30] E. Biham, A. Shamir, "Differential cryptanalysis of DES-like cryptosystems", *Journal of Cryptology*, vol.4, no.1, pp. 3–72, 1991.

[31] Y. Wang, K. Wong, X. Liao,T. Xiang,G. Chen, "A chaos-based image encryption algorithm with variable control parameters", *Chaos, Solitons and Fractals*, vol.41,no.4, pp.1773–1783, 2009.

[32] CE. Shannon, "Communication theory of secrecy system", *Bell Syst. Tech. J.*, vol.28, pp. 656–715, 1949.

[33] A. Jolfaei, A. Mirghadri, "A New Approach to Measure Quality of Image Encryption", *International Journal of Computer and Network Security*, vol. 2,no. 8, pp. 38–43, 2010.