3rd International Conference on Automation, Control, Engineering and Computer Science (ACECS'16)

Proceedings of Engineering & Technology (PET)
pp. 364-370

Evaluation and a Chaos-Based improvement of a Block Cipher Algorithm

Fatma SBIAA[#*1], Sonia KOTEL[*2], Medien ZEGHID[*3], Rached TOURKI*[4],
Mohsen MACHHOUT[*5], Adel BAGANNE[#6]

[#]*Laboratory of Information Science and Technology Communication and Knowledge (Lab-STICC),*
University of South Brittany,Lorient, France.

[*]*Electronics and Micro-Electronics Laboratory (E. µ. E. L), Faculty of Sciences,*
University of Monastir, Tunisia.

[1]fatma.zayen@univ-ubs.fr
[2]soniakotel@gmail.com

Abstract— **Since the confidentiality of information has become essential in different fields of application, a variety of encryption algorithms have been put forward during the last years. Chaos-based encryption techniques present a new and efficient way for dealing with intractable problem of fast and high security level encryption. In fact, many researchers suggest using the chaos-based encryption in order to overcome the problems and drawbacks of the classical encryption techniques like Simple-DES (Data Encryption Standard), Triple-DES and AES (Advanced Data Encryption). In this paper, a new chaos-based approach for correcting the security level of a block cipher algorithm is proposed. The proposed modifications are based on the exploitation of the chaos theory properties. The experimental results showed that the proposed modifications can be easily implemented as they do not need a high level of consumption or hardware occupation. In addition, the security analysis proved the resistance of the new algorithm to the statistical attacks, the differential attacks, and the initial key sensibility.**

***Keywords*— Symmetric cryptography, block cipher, DES, Security analysis, cryptanalysis, chaos, update functions.**

I. Introduction

With the large-scale development in information technologies, there is a great demand for preserving the secure data storage and transmission. An important tool for providing the security services accounts for the cryptographic algorithms. Thus, many encryption methods have been put forward to cope with various applications [1].

Cryptographic methods can typically be separated into two components. These are the symmetric and the asymmetric encryption. In the symmetric key ciphers, a single key is used for both encryption and decryption process. In fact, this category of algorithms is suggested to be used to encrypt the digital images because it is fast and provides a satisfying security level. The symmetric key algorithms use two different techniques. These are the block and stream cipher encryption [2]. Unfortunately, most of the existing algorithms have been subject to different attacks. In fact, cryptanalysis is the technique of deriving the original message from the cipher text without any prior knowledge of a secret key or derivation of the key from the cipher-text [3]. Thus, a symmetric key cipher is assumed to be secure, if the computation capability required for breaking the cipher by best-known attack is greater than or equal to the exhaustive key search [3][4].

The goal of the modern cryptography is to find sufficiently complex algorithms so that the attacker can not decrypt the cipher-text. However the used functions should not compromise the security level with the hardware performances. Since our main goal is to provide solutions for existing encryption algorithms, we must compromise the perform metrics of the application targets with the perform metrics of the encryption algorithm. These performs include security, implementation parameters and hardware performances.

Many researches relied on the strengths of the block cipher algorithms while adding some improvements. These modifications were used in order to improve the resistance of the algorithm against the new attacks. To specify the appropriate improvements, it is needed to recognize the power of each attack and predict its capability on the algorithm. The designed algorithm should maintain all the advantages presented by the main algorithm while adding solutions to the disadvantages, essentially the security issues. One of the topics of these researches is the chaos theory.

Following the first chaos-based encryption scheme that was proposed in 1989, a big number of cryptography researchers proposed a variety of chaos-based encryption schemes [5-7]. They relied on the chaos-properties such as the sensitive dependence on the initial conditions and the system parameters, the non-periodicity, and the pseudorandom property [5-7].

In this paper, we propose a new encryption scheme as a modification of the DES algorithm using ECB and CTR modes. Our main goal is to provide better security level for these operating modes while proposing update functions which are essentially based on the chaotic theory.

In the first section, we will justify the choice of the algorithm. Then, we will analyse its security level in order to prove the existing weaknesses and propose the appropriate modifications. Finally, we will evaluate the proposed improvements by applying different security analyses on the standard images.

II. Choice of the Algorithm

The present work is a new approach to improve the security level of a block cipher algorithm that presents many security weaknesses. In order to choose the most vulnerable algorithm, we made a comparison between the most known block ciphers.

The main characteristics that identify and differentiate one encryption algorithm from another are its ability to secure the protected data against attacks and its speed and efficiency in doing so. Thus, our evaluation will be based on the study of two main criteria. These are the security level and the implementation performances.

In this section, we will compare the most commonly used algorithms, namely, DES, Triple DES, Blowfish and AES.

A. *The Security Level*

According to the literature, many researches were conducted to discuss the security level of the most known block ciphers. Since this criterion strongly depends on the size of the used key, we observed this parameter then we reported the results presented by the following table:

TABLE I
A Comparison of the Security Level Between the Most Known Block Cipher Algorithms

Properties	**DES**	**Triple-DES**	**AES**	**Blowfish**
Key size	56 bits	168 bits	128, 192 or 256 bits	Between 32 and 448 bits
Block size	64 bits	64 bits	128 bits	64 bits
Round number	16	48	10, 12 or 14	16
Security level	Low	Medium	Medium to high	High

In Ref. 8, H.O.Alanazi argued that AES is considered to be secure while DES is proven inadequate according to nine factors including the algorithms' efficiency, flexibility and security. In fact, DES presents many weaknesses against differential and linear cryptanalysis. In addition, it is vulnerable to exhaustive search. Still, the existence of new attacks which have less complexity than the exhaustive key search is perceived as a lack of security.

B. *The Cost and the Speed*

While designing a new encryption algorithm, the processing speed and the implementation cost present crucial factors. Therefore, many studies were made to evaluate and compare the performance of the most useful block cipher algorithms in terms of the processing time and the microprocessor occupation.

In Ref.9, the authors evaluated the speed of the encryption functions in order to compare DES to Blowfish. They implemented the two algorithms in C language program under Windows XP OS. Then, they estimated their performance for different data size. They concluded that Blowfish runs much faster than DES, yet it consumes a larger memory simultaneously. Although Blowfish is optimized for applications, the large memory requirement makes it infeasible for smart card application.

Observing all the results presented in References 9–12, we conclude the following order (Fig.1):

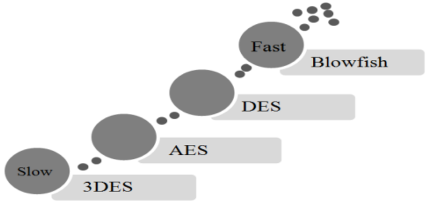

Fig. 1 The comparison of the execution times between DES, 3DES, Blowfish and AES

In order to prove the efficiency of the proposed modifications, we will propose some "up-date functions" to the most vulnerable algorithm. In this work, we chose to use the DES algorithm as it was one of most powerful existing encryption algorithms. Nowadays, DES is considered to be traditional because of some lapses in its resistance against the attacks that are increasingly developing and threatening the security and confidentiality of the information [13] [14]. Although DES is not used the way it was before, many search are still studying and evaluating its performance. For example, in Ref. 15, G.Kumar proposed an approach to provide security in wireless sensor networks. He applied encryption algorithms like DES and Blowfish in CBC mode. The presented approach achieved high data confidentiality and authentication.

In the next section, we will study the DES algorithm in order to highlight its weaknesses.

III. The Data Encryption Standard Analysis

A. *The DES presentation*

DES is a symmetric cryptographic algorithm which was developed by IBM Corporation in 1972. DES mainly contains extension and permutation operations which are easily implemented in hardware. However, its power consumption can be used in the power analysis attack by the statistical methods. The DES algorithm includes 16 rounds of iteration operations. Except from the first and the last rounds, the other operation rounds are similar [16]. The following figure describes the structure of the DES.

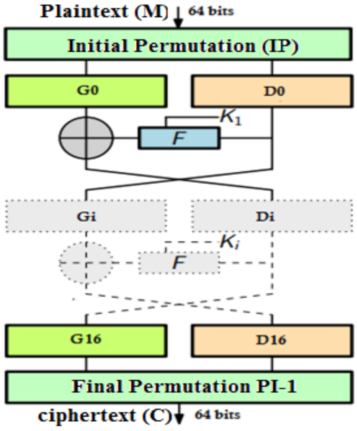

Fig. 1 The DES Structure

Due to its importance, DES has received a great deal of cryptanalytic attention [13][14]. In fact, the DES has several advantages. It is completely specified and user-friendly. Therefore, it is easy to be implemented (software or hardware platform). In addition, it is public, fast and exportable. However, this standard presented many weaknesses especially against differential and linear cryptanalysis. Furthermore, it is vulnerable to exhaustive search. In fact, the weakest point in DES is its short key and the S-BOX structure. It was designed with an effective key length of 56 bits.

Thus, the Triple-DES is a variant of DES that was defined to solve the key size issue. In fact, the used key consists of 168 bits. Since exhaustive search on a 168-bit key is wholly out of reach of the human technology, the differential and the linear cryptanalysis are defeated by the Triple-DES. Yet, it still suffers from the block size issues of the DES. Furthermore, the new algorithm requires too much execution time and hardware consumption.

The Advanced Encryption Standard AES was defined, later, to resist against differential and linear cryptanalysis. The design of the AES benefited from 25 years of insights and research on DES. However, since standardization it has been the subject of extensive cryptanalysis research to improve its robustness [17].

In order to study the security level of the DES algorithm we implemented it in SystemC using 3 different modes (ECB, CBC, and CTR). Then we implemented the security analysis to extract its strengths and weaknesses. We also implemented the Triple-DES and the AES algorithms in order to make a comparison between them. We used four different plain-images which are Lena, Baboon, peppers, and Barbara. The presented values are the average of the four obtained values. In present section, we will describe the different security tests. Then, we will evaluate the security level of the DES in order to propose the appropriate improvements.

B. *Statistical analysis of DES*

The statistical tests include the calculation of the correlation coefficients of the adjacent pixels, the information entropy and the peak signal-to-noise ratio (PSNR).

- The Peak Signal-to-noise ratio (PSNR) is the most widely used metric to estimate image distortion measure. This metric compares the visual quality between the plain image and the ciphered one. The PSNR is based on the Mean Squared Error value (MSE) that provides the error between two images.
- The information entropy is one of the most important feature of randomness. In fact, the source is considered to be truly random if the information entropy of the ciphered image is close to eight.
- The correlation of two adjacent pixels describes the relationship between pixels in the encrypted image. In fact, we have analyzed the correlation between each two vertically, horizontally, and diagonally adjacent pixels in the cipher images. We note that a good ability to resist against statistical attacks is presented by a small correlation values.

The results given in table 2 represent the average of the obtained values which correspond to the four ciphered-images.

TABLE III
THE STATISTICAL ANALYSIS OF THE DES, THE TRIPLE-DES, AND THE AES

	Mode	**NPSR**	**Entropy**	**Vertical Correlation**	**Horizontal Correlation**	**Diagonal Correlation**
DES	ECB	9.125	7,954	0,076	0,082	0,081
	CTR	9.131	7,950	0,069	0,073	0,068
	CBC	9.115	7,954	0.069	0.066	0.076
Triple-DES	ECB	9.279	7,959	0,071	0,071	0,073
	CTR	9.231	7,954	0,073	0,075	0,078
	CBC	9.208	7,954	0.077	0.071	0.077
AES	ECB	9.131	7,999	0,039	0, 042	0,038
	CTR	9.152	7,999	0,033	0,042	0,019
	CBC	9.168	7,999	0.036	0.041	0.019

Therefore, we consider that DES is not vulnerable to the statistical attacks. The CBC mode gives the best result compared to CTR and ECB modes due to its architecture and complexity. We realized also that the AES_128_ECB and the AES_128_CTR present better resistance against statistical attacks compared with the DES and the Triple-DES. Meanwhile, AES_128_CBC mode presents always the best values.

C. *The sensitivity tests*

A good encryption scheme should be sensitive to the data as well as the used keys. In order to evaluate the sensitivity of the cryptographic algorithm to the initial key in process of enciphering, two tests are proposed:

(i) Completely different cipher images should be produced when slightly different keys are used to encrypt the same plain image.

(ii) When an image is decrypted, tiny change of keys can cause the failure of deciphering.

In addition, when we make a slight change in the original image, we should find completely different ciphered images.

To quantitatively describe the sensitivity of the block ciphers, we calculated the NPCR and UACI values of the resulted images [18]. The two parameters given in (1) and (2) can effectively calculate the difference between the images when we change only one pixel in the initial key while decrypting the four test images used before.

$$NPCR = \frac{\sum_{i=1}^{H}\sum_{j=1}^{L} D_{i,j}}{H \times L} \quad with\, D_{i,j} = \begin{cases} 1\, if\; IC1 = IC2 \\ 0 \qquad\quad else \end{cases} \tag{1}$$

$$UACI = \frac{1}{H \times L}\sum_{i=1}^{H}\sum_{j=1}^{L}\frac{IC_{1_{i,j}} - IC_{2_{i,j}}}{2^8 - 1} \times 100\,\% \tag{2}$$

In particular, we have changed one pixel in the plain test images, and we have used the DES, the Triple-DES, and the AES algorithms to encrypt them before and after change. As a next step, we have computed NPCR and UACI using (1) and

(2). The same parameters are calculated when we changed only one bit in the initial key in order to compare the resulted images. The following table represents the obtained results.

TABLE IIIII
THE SENSITIVITY TESTS OF THE DES, THE TRIPLE-DES, AND THE AES

	The Operating Modes	**Sensitivity to the Data**		**Sensitivity to the initial key**	
		NPCR%	**UACI%**	**NPCR%**	**UACI%**
DES	ECB	0.0061	0.023	0.0061	0.023
	CTR	0.0063	0.011	0.0063	0.011
	CBC	99.59	33.43	99.59	33.50
Triple-DES	ECB	0,0156	0,0488	0,0056	0,022
	CTR	0,0061	0,0019	0,0061	0,019
	CBC	99,61	33,38	99,60	33,48
AES	ECB	0.0061	0.0019	99.60	33.39
	CTR	99.60	33.47	99.61	33.49
	CBC	99.61	33.54	99.61	33.58

The results of the DES are well below the expected values. We can see that the security solution offered by DES (ECB mode and CTR mode) does not show extreme sensitivity compared to the slight changes in the initial key and/or data. Consequently, its ability to resist the differential attacks is very low.

IV. THE PROPOSED IMPROVEMENTS

After studying the DES algorithm's architecture, functionality and the various possible modes of operation, we have proved that DES has limits to the different attacks that threaten the security of systems and affect the integrity and confidentiality of information.

To improve the security level of a cryptosystem, there are two approaches that can be followed:

- The first approach is to consider the cryptosystem as a black box, In this case we have to keep the internal architecture of this cryptosystem and add an extra layer of functions to improve security. Despite its advantages in terms of safety, this method has several drawbacks in terms of performance.

- The second approach is to examine the safety of elementary functions of the cryptosystem, locate weaknesses, and suggest correction functions to improve overall security. In this approach, the cryptosystem is seen as a set of functions and the choice of correcting functions is not arbitrary. Our goal is to correct any weaknesses and maintain all the benefits. This approach allows us to have a robust crypto-system and an efficient time.

To take advantage of each of these two approaches, we intend to combine them. In fact, DES can be seen as a set of functions that can be represented by the following model:

FDES= A U B U C U D With { A= the Key Generator, B= the Initial Permutation, C=16 Feistel rounds, D=the reverse Initial Permutation}.

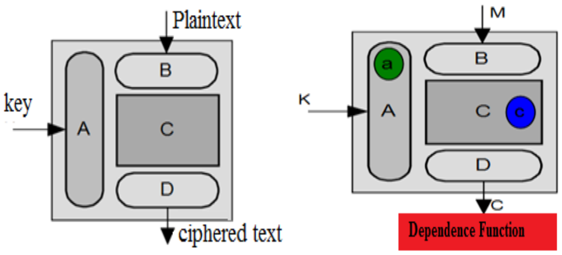

Fig. 3 Proposed approach to improve the security level of DES.

The proposed architecture has several features. In the next section, we will describe each update function and present its advantages.

A. *Chaos to Generate the Initial Key*

Chaotic encryption is a new research direction of cryptography which is characterized by high initial-value sensitivity and good randomness. It is an efficient way to deal with the problem of simple implementation, fast and highly secure encryption [5-7]. The chaos generator is added in order to generate keys.

We have chosen one of the well-known functions having chaotic nature. It is the logistic chaotic map. Its simplicity makes it easy to implement but secure enough to provide good security level. The logistic map is a discrete iteration which can be formulated as follows:

$$x[n+1] = k.x[n].(1-x[n]) \tag{3}$$

k is the parameter of the logistic map that determines the chaotic behavior with x€ [0,1] and k € [3,75;4] for good chaotic properties.

In our crypto-system, we used the logistic chaotic sequence presented previously to generate the initial keys with good randomness while adding little cost. The main idea is to incorporate a complex secret key.

The main advantage of the use of a chaotic generator is the use of a new key for each data. In fact, the use of the same key to encrypt the entire image may lead to the appearance of homogeneous (textured) zones. The non-linearity property of the chaotic function will add the non-linearity to the generated keys.

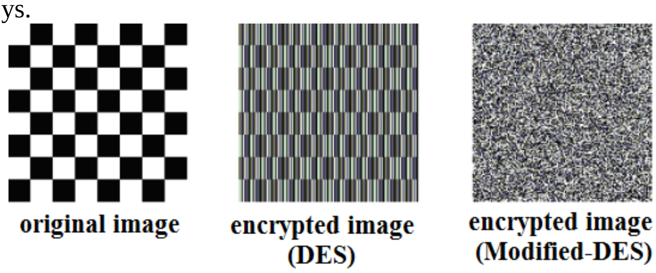
original image
encrypted image (DES)
encrypted image (Modified-DES)

Fig. 4 Homogeneous areas disappear by using a chaotic key generator.

Analyzing the results of encryption, we see that the figure ciphered by the proposed crypto-system is more noisy. So, we can not determine the texture of the images.

B. *Chaos to Improve Differential Analysis*

In ECB encryption and decryption, the forward cipher function is applied directly and independently to each block of the plaintext and the ciphertext. In ECB encryption and ECB decryption, multiple forward cipher functions and inverse cipher functions can be computed in parallel. However, this mode presents a low security level especially to differential attacks.

Our proposed schemas are based on the use of a logistic chaotic sequence to generate data blocks of 128 bits that is combined with the ciphered data. The following figure illustrates the proposed structure.

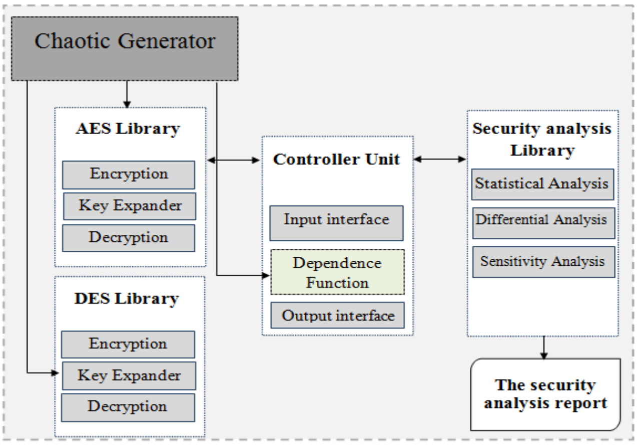

Fig. 5 SystemC design of the proposed environment

We used a chaotic function to generate a counter value in the CTR-mode in order to improve its resistivity to the sensitivity tests. Due to this, used counter become more complex with more random values that highly depends on the initial conditions.

C. *Differential power analysis: active s-box*

In order to protect the algorithm from first-order DPA (Differential Power Analysis) the update function that can be recommended is to use a Boolean masking scheme based on one random byte that is different from one execution to another[19]. In fact, we perform some circular shifts on the S-boxes and the inv-S-Boxes to make it different for each encryption / decryption operation. These shifts are based on the initial key.

Accordingly, with the use of active S-BOX, differential attacks become increasingly difficult.

V. The Experimental results

In order to prove the efficiency of the proposed improvements, we conducted the analysis on four images of BMP type and 128 * 128 pixels size (Lena, Baboon, peppers and Barbara). The results given in all the realized tests are the average of the four obtained values.

A. Statistical analysis

We have analyzed the statistical tests: we observed the entropy values, the PSNR and the correlation between Horizontal, vertical and diagonal adjacent pixels.

TABLE IV
The Values Results of Statistical Analysis

	Modified-DES	
	ECB	CTR
NPSR	9.208	9.236
Entropy	7.959	7.965
Vertical Correlation	0.0765	0.0635
Horizontal Correlation	0.0823	0.0731
Diagonal Correlation	0.0814	0.0685

The various statistical tests illustrate that the obtained results are close to the ideal values which prove the safety, robustness and efficiency of the proposed cryptosystem against this kind of attacks.

B. *Differential analysis*

We modified only one pixel value in the original image and encrypted the modified image using the same key. Then we calculated the NPCR and the UACI values

TABLE V
The Values results of NPCR, UACI

	Modified-DES	
	ECB	CTR
NPCR	99.61	99.61
UACI (%)	33.38	33.42

We note that the proposed cryptosystems results are very close to the expected values of NPCR and UACI. Thus, it shows extreme sensitivity on the plaintext and hence it is not vulnerable to the differential attacks.

D. Sensitivity to the initial key

We used two key that are slightly different to (respectively) encrypt and decrypt the test images. Then we calculated the NPCR and the UACI values.

TABLE VIV
The NPCR and UACI Values while modifying only one bit in the initial key.

	Modified-DES	
	ECB	CTR
NPCR	99.61	99.60
UACI (%)	33.52	33.44

The experimental results of the proposed crypto-system show a good sensitivity to the initial key.

E. Time execution analysis

To analyze the impact of the proposed modifications on the simulation time, we runned the encryption process 100 times and we measured the average of the simulation time using the Linux command time. Before presenting and discussing the results, it is important to note that the error margin of the measurement tool that we employed is not significant and does not affect the results because we need to calculate the time overhead.

The following figure presents the encryption time of the proposed cryptosystems applied on ‘Lena image’ with the size of 128 x 128 pixels.

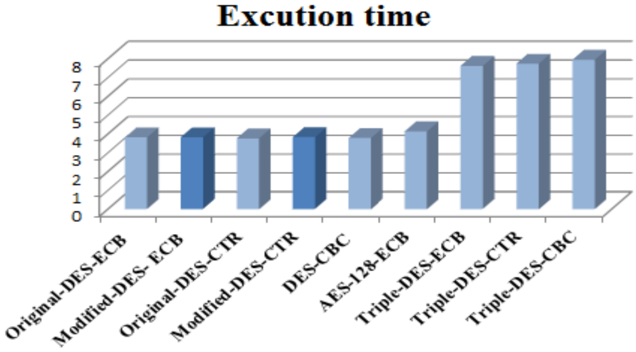

Fig. 6 A comparison of the execution time of the DES, the Triple-DES and the AES algorithms.

While comparing the obteined results, we note that the proposed scheme slightly affects the simulation time of the original design. Thus, the simulation time overhead does not exceed 2.23%.

VI. Conclusions

In this work, we studied and implemented a new encryption algorithm based on DES with a new architecture. The goal was to increase the level of security while improving the resistivity to certain types of attacks. Our modifications were essentially based on the exploitation of the chaos properties. In order to evaluate our contribution, the Modified-DES was compared to the Triple-DES and the AES algorithms. Thus, the security analyses proved the robustness of the proposed modifications; the new crypto-system presents a good efficiency against statistical tests and shows extreme sensitivity to the plaintext as well as the initial key. It presents more complexity, random key-generation and active-S-box.

Moreover, the proposed update functions do not need a high execution time overhead.

References

[1] S. Lian, Multimedia Content Encryption: Techniques and Applications (Taylor & Francis Group, LLC, 2009).

[2] Ayushi, A Symmetric Key Cryptographic Algorithm (International Journal of Computer Applications, V., pp., 2010).

[3] E. Schaefer, An introduction to cryptography and cryptanalysis (pp.94-108,2000).

[4] 6. A. Kaminsky, M. Kurdziel and S. Radziszowski, An Overview of Cryptanalysis Research for the Advanced Encryption Standard (IEEE Military Communications Conference 2010 (MILCOM 2010), pp 1853-1859, San Jose, CA, USA, November 2010).

[5] S. Zhaopin, G. Zhang and J. Jiang, Multimedia Security: A Survey of Chaos-Based Encryption Technology (School of Computer and Information, Hefei University of Technology China).

[6] S. Lian, J. Sun and Z. Wang, A block cipher based on a suitable use of chaotic standard map (Chaos, Solitons & Fractals Vol.26 (No.1): 117–129).

[7] 28. J. Alireza, M. Abdolrasoul, Image Encryption Using Chaos and Block Cipher (Computer and Information Science).

[8] H.O. Alanazi, B.B. Zaidan, A.A. Zaidan, H.A. Jalab, M. Shabbir and Y. Al-Nabhani, New Comparative Study Between DES, 3DES and AES within Nine Factors (JOURNAL OF COMPUTING, VOLUME 2, ISSUE 3, MARCH 2010, pp. 152-157).

[9] *T. Nie and T. Zhang, A Study of DES and Blowfish Encryption Algorithm (2009 IEEE).*

[10] P. Jindal and B. Singh, Analyzing the Security-Performance Tradeoff in Block Ciphers (International Conference on Computing, Communication and Automation “ICCCA2015”).

[11] M. Mathur and A. Kesarwani, Comparison Between DES , 3DES , RC2 , RC6 , Blowfish and AES (Proceedings of National Conference on New Horizons in IT - NCNHIT 2013).

[12] J. Thakur and N. Kumar, DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis (International Journal of Emerging Technology and Advanced Engineering, December 2011).

[13] 13. E. Biham and A. Shamir, Differential Cryptanalysis of the Full 16-Round DES (Advances in Cryptology-CRYPTO '92 Proceedings, Springer-Verlag, 1993, pp. 487- 496).

[14] 15. E. Biham and A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems (Advances in Cryptology “CRYPTO '90”. Springer-Verlag. 2–21, 1990).

[15] G. Kumar, M. Rai and G. Lee, Implementation of Cipher Block Chaining in Wireless Sensor Networks for Security Enhancement (International Journal of Security and Its Applications Vol. 6, No. 1, January, 2012).

[16] FIPS PUB 46-3, Data Encryption Standard (DES), National Institute of Standards and Technology (October 1999).

[17] National Institute of Standards and Technology (NIST), Advanced Encryption Standard (AES), FIPS Publication 197 (2001).

[18] Y. Wu, NPCR and UACI Randomness Tests for Image Encryption (Journal of Selected Areas in Telecommunications (JSAT), April Edition, 2011).

[19] B. Mazumdar, Design for Security of Block Cipher S-Boxes to Resist Differential Power Attacks (International Conference on VLSI Design (VLSID), 2012, pp. 7-11).