International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.3, 2015

RESEARCH ARTICLE

ISSN: 2321-7758

COMPARATIVE STUDY ON BLOCK BASED CODING, DES AND AES IN IMAGE ENCRYPTION TECHNIQUES

RUPALI SRIVASTAVA[1], O. P. SINGH[2]
[1]M.Tech student, Department of ECE, [ASET] Amity University, Lucknow Campus, India
[2]Professor (Dr.), HOD of Department of ECE, [ASET] Amity University, Lucknow Campus, India

Article Received:20/05/2015 | Article Revised on:30/05/2015 | Article Accepted on:10/06/2015

RUPALI SRIVASTAVA

Prof. O.P Singh

ABSTRACT

Digital data exchange with the fast evaluation, security information becomes much important because of various multimedia technologies, more and more data are generated and transmitted and also the internet allows wide distribution of digital media data. Other than, digital documents are also easy to distribute, therefore it will be faced by many threats. It becomes necessary to find appropriate protection as the data may include some sensitive information which should not be accessed by an unauthorized access. It can only be partially exposed to the general users. So in this modern era, security is a prime important issue, and encryption is one of the best ways to ensure security. Moreover, many image encryption schemes have been proposed; each one of them has its own strength and weakness. This paper presents an analysis and comparison of various parameters of block based coding (CBC), DES and AES encryption schemes.

KEYWORDS: Image encryption, Advanced Encryption Standard (AES), Data Encryption Standard (DES), Block Based Coding, Cipher Block Chaining (CBC).

I.INTRODUCTION

Security is an important issue in the digital world and an encryption is one of the methods to ensure security [2]. Encryption is used to securely transmit data in open networks. Every type of data has its own features; therefore different technique should be used to protect confidential image data from unauthorized access. Image encryption has applications in various fields including internet communication, cyberspace communication, military, Tele-medicine, medical imaging and multimedia systems communication. This is one of the best methods for Image encryption for the emerging fields for real-time secure image transformation over the internet and through wireless networks [5]. In this paper, we introduce block-based transformation algorithm based on the combination of image transformation and a well-known encryption and decryption algorithm cipher block chaining (CBC) using key generation [4]. The original image was divided into blocks and they were rearranged into a transformed image using a transformation algorithm, where the transformed image was encrypted using the Block Based algorithm. Image quality can be examining measures, such as the Mean Square Error (MSE), and Peak Signal-to-Noise Ratio (PSNR) [7]. It is computed by averaging the squared intensity differences of distorted and original image pixels with PSNR related quantity.

A. DATA ENCRYPTION STANDARD (DES)

The first encryption standard was Data encryption standard and to be published by National institute of standard and technology (NIST). It was designed by the IBM based on their Lucifer cipher. DES became a standard in 1974 and it was adopted as a national standard in 1997. DES is a 64-bit block cipher. There are many attacks recorded against the weaknesses of DES which makes it insecure block cipher. This standard is public.

B. ADVANCED ENCRYPTION STANDARD (AES)

This algorithm is also called as Rijndael which is also known as Rain Doll algorithm. It was developed by two scientists Joan and Vincent Rijmen in 2000. Rijndael key and block length is 128 bit which performs 9 processing rounds. If the bit of the key is increased processing rounds are incremented automatically. This symmetric block can encrypt data of 128 bits using keys 128, 192 or 256. A well known attack i.e. Brute force attack i.e. Brute force attack is the only attack against this algorithm.

C. CIPHER BLOCK CHAINING (CBC)

mode adds a feedback mechanism to the encryption. In CBC, the plaintext is exclusively-OR ed (XOR ed) with the previous cipher text block prior to encryption. In this mode, the two identical blocks of plaintext never encrypt to same cipher text.

II.PROPOSED TECHNIQUE

A. Algorithm:

Step1: Read the original image of size 256×256 pixels of any kind like jpg, tiff, png.

Step2: Then the original image is divided into RGB plane.

Step3: Then image is divided into number of blocks consist 8 consecutive pixels of the image referred as a single block._Step4: Then on the obtained image apply XOR operation (CBC operation), which is performed among the blocks in order to encrypt the image.

Step5: Encrypted image is obtained (scrambled image).

Step6: On the obtained encrypted image (scrambled image) further XOR operation is performed to obtain the decrypted image along with the correct key (recovered image).

Step7: Decrypted image is obtained (recovered image).

III. TESTING PROCEDURE

Testing procedure include MSE, PSNR values on various images to evaluate the performance of the Algorithm and compare with the values of AES.

A. MSE: Mean Square Error

MSE is the difference between the original image and the encrypted image. This difference must be very high for a better performance. Mathematically it is evaluated as

MSE = (1/MN)*(original image-encrypted image)

For a 256*256 image the value of M=N=256

B. PSNR: Peak Signal to Noise Ratio

PSNR is the ratio of peak signal power to noise power. It is measured for image quality. For a good encrypted image the value of PSNR must be low. Mathematically,

PSNR=10log10(I2max /MSE) dB

I_{max} is the maximum intensity of image

Maximum intensity of 256*256 images is 255(0 to 255)

PSNR = 10log10*(2552/MSE) dB

IV. EXPERIMENTAL RESULT

Comparison Performance Analysis of Mean Square Error (MSE) and Peak signal to noise ratio (PSNR) is depicted from CBC and AES algorithm in Table 1 and Table 2. (Shows the overall time taken by the proposed method to encrypt as well as to decrypt the image).

Table1: for AES algorithm

Original Image	SIZE(KB)	MSE	PSNR
1.Barbara(256*256)	48.3	120.9474	62.784
2.Baboon(256*256)	12.1	114.2402	62.114
3.Mother Teresa(256*256)	7.42	102.4470	64.148
4.Lena(256*256)	8.08	104.3225	61.37

Table2: for CBC Algorithm

Original Image	SIZE(KB)	MSE	PSNR
1.Barbara(256*256)	48.3	110.9474	92.784
2.Baboon (256*256)	12.1	94.2402	102.114
3.Mother Teresa (256*256)	7.42	92.447	104.148

4.Lena (256*256)	8.08	104.3225	111.37

Table 3: Performance Analysis-Speed Performance by AES ALGO

Original Image	Size	Elapsed Time (in sec)
1.Barbara(256*256)	48.3	6.96sec
2.Baboon(256*256)	12.1	13.53sec
3.Mother Teresa(256*256)	7.42	24.42sec
4.Lena(256*256)	8.08	15.78sec

Table 4: Performance Analysis-Speed Performance by CBC ALGO

Original Image	Size	Elapsed Time(in sec)
1.Barbara(256*256)	48.3	3.96sec
2.Baboon(256*256)	12.1	3.53sec
3.Mother Teresa(256*256)	7.42	4.42sec
4.Lena(256*256)	8.08	5.78sec

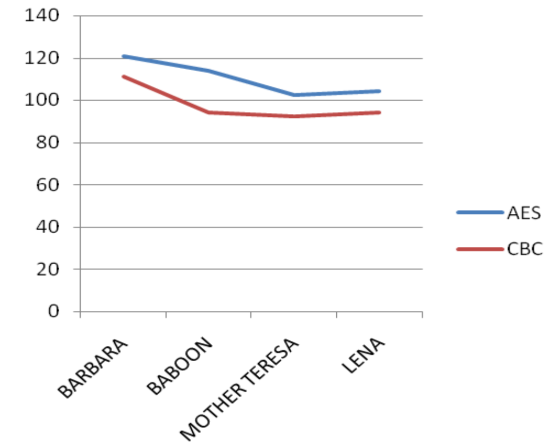

Fig.1Comparison Values of MSE (dB) of AES and CBC

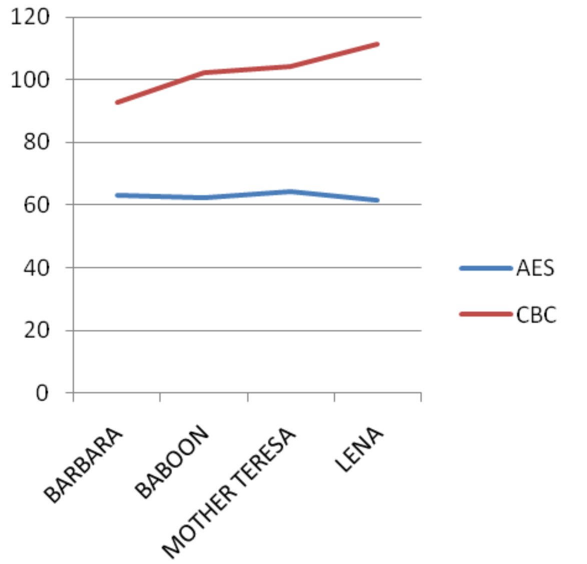

Fig.2 Comparison Values of PSNR (dB) of AES and CBC

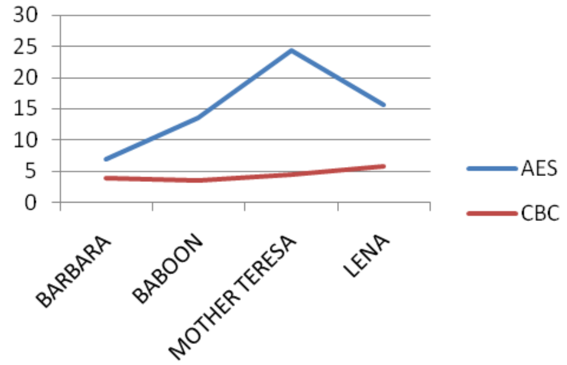

Fig.3 Performance Analysis-Speed Performance of AES and CBC

Table: 5 Experimental Analysis of DES, AES AND CBC

PARAMETERS	DES	AES	CBC
TIME	199.7407	92.3807	4.4225
MSE	8185.4343	8149.8396	100.4892
PSNR	7.6057	7.5523	102.604

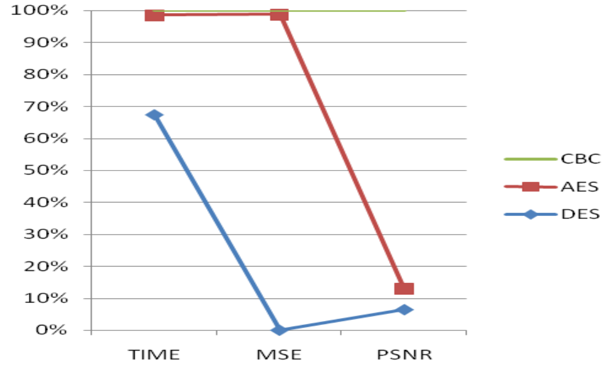

Fig.4 **Experimental Analysis Graph of DES, AES and CBC**

V.SIMULATIONS AND RESULT

The proposed technique is tested on MATLAB R2013a, In this paper effectiveness of the proposed algorithm have been tested with Barbara, Baboon, Mother Teresa and Lena images are taken as input images and then scrambling images have been generated and then finally they decrypted. All images are of in equal dimension and are approximately 7-48 KB in size[1,11]. The obtained images after simulation is listed below as original image, encrypted image and decrypted image with the help of CBC and AES algorithm. [4-10]. Figure.5 from matlab library

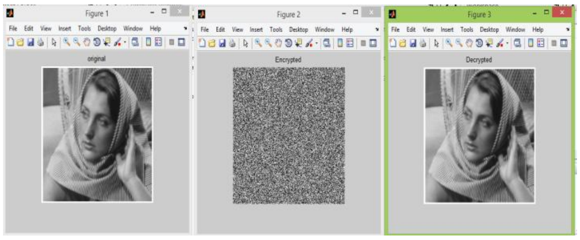

Fig.5 Shows the Image Of Barbara

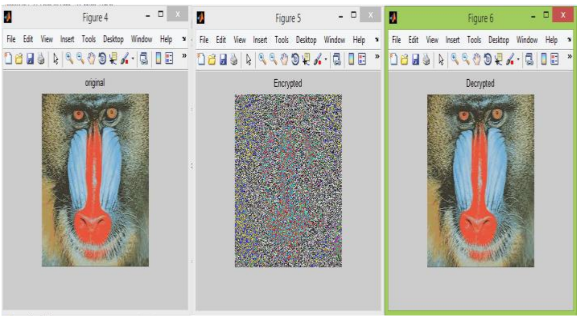

Fig.6 Shows the Image of Baboon

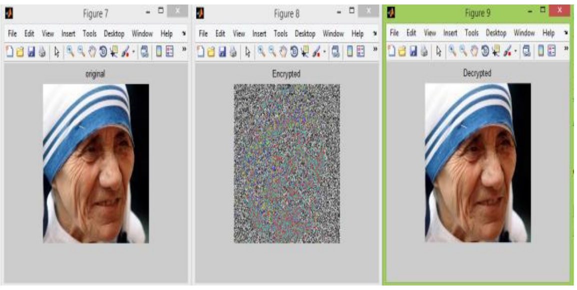

Fig.7 Shows the Image of Mother Teresa

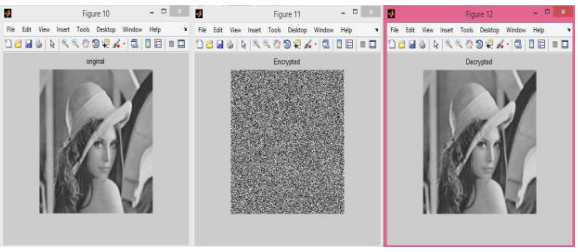

Fig.8 Shows the Image of Lena

VI.CONCLUSIONS

In this paper, better method for encryption has been proposed which provides confidentiality to the images with the less computation work i.e CBC algorithm in comparison to AES and DES. In the proposed method the key generation process is unique(EXOR) and efficient. Hence, block scrambling is much quick and effective which gives the better results and is tested on MATLABR2013a. In this paper encryption with block based matching algorithm is achieved on various imagesand quality parameters such as MSE and PSNR has been calculated, illustrated in tables. From the performance analysis it is found that this technique takes less time for the whole process. This method can be extended in trying to handle multiple images instead of single image.

ACKNOWLEDGEMENTS

The author would like to express their thanks to the department of Electronics and Communication Engineering, Amity School of Engineering and Technology (ASET), Amity University, Lucknow Campus for their supports and encouragements during this work.

REFERENCES

[1]. SeshaPallavi, Indrakanti, P.S.Avadhani “Permutation Based image Encryption technique”, IJCA, Vol.28, No.8, pp.45-47, 2011.

[2]. Yong-Cong Chen and Long-Wen Chang, “A Secure and robust Digital Watermarking Technique By the block cipher RC6 and Secure Hash Algorithm”, IEEE, pp 518-121, 2001.

[3]. Swati Paliwal and Ravindra Gupta, “A Review of Some Popular Encryption Techniques”, IJARCS and Software Engineering Research Paper, Vol. 3, 2277 128X, Issue 2, February 2013

[4]. B. Acharya, S.K.Panigrahy, S.K.Patra, and Ganapati Panda, “Image Encryption Using Advanced Hill Cipher Algorithm”, International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.

[5]. NIST Computer Security Division's (CSD) Security Technology Group (STG) (2013). "Block cipher modes".Cryptographic Toolkit.NIST.Retrieved April 12, 2013.

[6]. Sidra Riaz, Sang-Woong Lee, “Image Authentication and Restoration by Multiple Watermarking Techniques with Advance Encryption Standard in Digital Photography”, ICACT, pp 24-28, 2013.

[7]. Faisal Riaz, Sumira Hameed, Imran Shafi, Rakshanada Kausar And Anil Ahmed , “Enhanced Image Encryption Techniques Using Modified Advanced Encryption Standard”, Springer-Verlag Berlin Heidelberg, pp 385-396, 2012.

[8]. Lian Xiaoqin, Li Wei, Chen Xiuxin, Zhang Xiaoli, Duan Zhengang, “Application of the Advanced Encryption Standard and DM642 in the Image Transmission System”, IEEE The 7th International Conference on Computer science & Education, pp 444-447, 2012.

[9]. Manoj Kumar Ramaiya, Naveen Hemrajani , Anil Kishore Saxena , “Security improvisation in image Steganography using DES”, IEEE 3rd International Advance Computing Conference , pp 1094-1099, 2013.

[10]. R. liu, X. tian “New algorithm for color image encryption using chaotic map and spatial bit level permutation “JTAIT Vol. 43 No.1 2012

[11]. De Wang, Yuan-Biao Zhang, “Image Encryption Algorithm Based On S-Boxes Substitution And Chaos Random Sequence”, IEEE, pp110-113, 2009.

[12]. Ambika Oad, Himanshu Yadav, Anurag Jain, “A Review on Image Encryption Techniques and its Terminologies”, IJEAT, Vol.-3, 2249 – 8958, Issue-4, April 2014

[13]. S.H. Kamali, R. Shakerian “A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption” ICEIE 2010.

[14]. K.C. Ravishankar, M.G. Venkateshmurthy “Region Based Selective Image Encryption” 1-424-0220-4/06 ©2006 IEEE.

[15]. Li, X. Chen, J., Qin, D. , Wan, W., ―Research & realization based on Hybrid Encryption Algorithm of improved AES & ECC , International Conference on Audio Language and Image Processing (ICALIP), 2010.

[16]. Goodwin, J., Wilson, P. R., ―Advanced Encryption Standard (AES) Implementation with Increased DPA Resistance & low overhead , IEEE International Symposium on Circuits and Systems, 2008. ISCAS 2008.

[17]. Li, H., Li., J., ―A New Compact Dual Core Architecture for AES Encryption & Decryption , Canadian Journal of Electrical and Computer Engineering, 2008.

[18]. Islam, Md., N., Mia, Md. M. H., Chowdhury, Md. F.I.C., Matin, M. A., ―Effect of Security Increment to Symmetric Data Encryption through AES Methodology , Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008.

BIOGRAPHY

Rupali Srivastava received his Bachelor of technology degree in Electronics and communication Engineering from the “Uttar Pradesh Technical University”, Lucknow, in 2012 and pursuing Master of technology degree in Electronics and communication from “AMITY UNIVERSITY LUCKNOW” in (2013-2015).

Professor O.P Singh has completed his Phd. degree from IIT BHU. He had a work experience of 16yrs in teaching. Presently he is head of department of electrical and electronics in Amity University Lucknow. He is also a member of Indian society of remote sensing (ISRS) and Material Research Society of India (MRSI). His area of research include digital electronics engineering, microwave and antenna design, control system, pattern recognisation in image compression etc.