ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

Performance Analysis of Image Encryption Using Block Based Technique

Rupali Srivastava[1], O. P. Singh[2]

Professor, Head of Department of ECE, [ASET] Amity University, Lucknow Campus, India

PG student [ECE] Department of ECE, [ASET] Amity University, Lucknow Campus, India

ABSTRACT: In digital communication and multimedia application, security is must for communication and storage of images. Image Encryption is one of the best methods to ensure high security images which are generally used in medical science, military applications. In this paper, an efficient technique is proposed with the help of cipher block chaining (CBC) operation, which is used for image encryption. We test our proposed technique using MATLAB R2013a, it can achieve various image quality parameters such as the mean square error(MSE), peak signal to noise ratio (PSNR) and the overall time taken by the algorithm to perform the process is also computed.

KEYWORDS: Image encryption, Mean Square Error (MSE), Cipher Block Chaining (CBC), Peak- Signal- to- Noise-Ratio (PSNR).

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. Each 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, multimedia systems, medical imaging, Tele- medicine and military communication. Image encryption is one of 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]. In this algorithm the original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm, and then the transformed image was encrypted using the Block Based algorithm. There are many measures for examining image quality, 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, along with the related quantity of the PSNR.

The main idea in this section, the image encryption is to transmit the image secured over the network so that no authorized user can able to decrypt the image. We are going to present the research work of some prominent authors in the same field and then explaining a short description of various techniques that are used for image Encryption.

A. New Modified Version of Advanced Encryption Standard (MAES) Based Algorithm for Image Encryption [5] This technique is proposed by a new encryption scheme as a modification of AES algorithm based on both Shift Row Transformations. In the first row and first column if the value is even, the first and fourth rows are unchanged also each bytes in the second and third rows of the state are cyclically shifted right over different number, as well as the first and third rows are unchanged and each byte of the second and fourth rows of the state are cyclically shifted left over different number of bytes. The result that are experimental shows that the MAES gives better encryption results in terms of security against statistical attacks and increased performance.

B. Digital Image Encryption Algorithm Based on Chaos and Improved DES [15].

This paper is based on the chaotic encryption and Improved DES encryption and a combination of image encryption algorithm is used to find the gaps. By this paper new encryption logistic Map produced pseudo random sequence on RGB image and make double times encryption with improved DES. Combination of Chaos And improved DES makes the final algorithm more secure, faster and more suitable for digital image encryption.

C. A New Chaotic Image Encryption Algorithm [16]

This paper, have proposed a new image encryption scheme based on a chaotic system. It is based on power and tangent function instead of linear function. It uses chaotic sequence generated by NCA map to encrypt image data with different keys for different images .plain-image image can be encrypted by use of XOR operation with the integer sequence.

D. An Efficient Chaos-based Image Encryption Scheme Using Affine Modular Maps [17]

An efficient image encryption scheme based on affine modular maps is proposed in the paper. The proposed scheme can shuffle the plain-image efficiently in the permutation process. An effective two-way diffusion process is also presented to change the gray values of the whole image pixels. All the experimental results show that encryption scheme is secure, its highly sensitivity to the cipher keys and plain-images. It is easy to manipulate and can be applied to any images with unequal width and height.

E. New Algorithm For Color Image Encryption Using Chaotic Map And Spatial Bit Level Permutation [10]

They proposed a new algorithm for color image encryption using chaotic map and spatial bit-level permutation (SBLP).Firstly, use Logistic chaotic sequence to shuffle the positions of image pixels, then transform it into a binary matrix and permute the matrix at bit-level by the scrambling mapping generated by SBLP. Then use another Logistic chaotic sequence to rearrange the position of the current image pixels. Experimental results show that the proposed algorithm can achieve good encryption result and low time complexity. This makes it suitable for securing video surveillance systems, multimedia applications and real-time applications such as mobile phone services.

II.PROPOSED TECHNIQUE

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 proposed Algorithm.

MSE: Mean square error 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

$$\text{MSE} = (1/\text{MN})*(\text{original image-encrypted image})$$

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

PSNR: Peak signal to noise ratio 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,

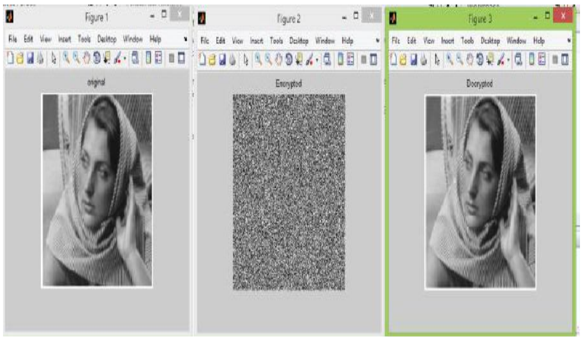
$$PSNR=10\ log10(I2max\ /MSE)\ dB$$

I_{max} is the maximum intensity of image
Maximum intensity of 256*256 images is 255(0 to 255)

$$PSNR = 10log10*(2552/MSE)\ dB$$

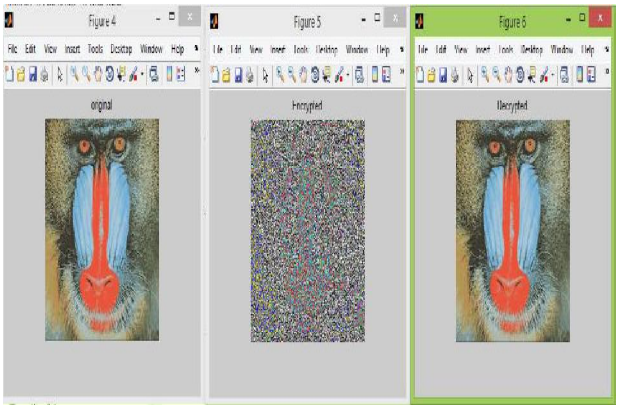
IV. SIMULATIONS AND RESULT

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. [4-10]



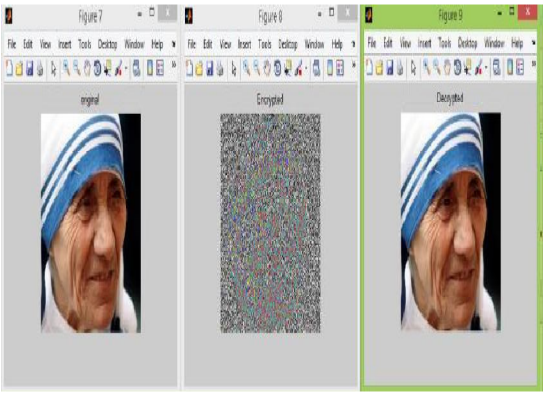
Original Image Encrypted Decrypted

Fig.1 Image of Barbara



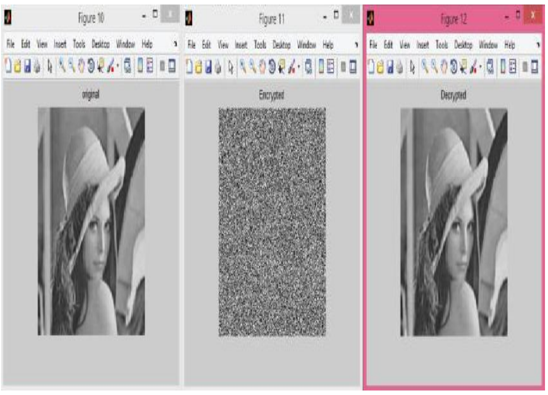
Original Image Encrypted Decrypted

Fig. 2 Image of Baboon



Original Image Encrypted Decrypted

Fig. 3 Image of Mother Teresa



Original Image Encrypted Decrypted

Fig. 4 Image of Lena

V.EXPERIMENTAL RESULT

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

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	114.3225	61.37

Table1 Performance Analysis of MSE & PSNR

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

Table 2 Performance Analysis-Speed Performance

VI. CONCLUSIONS

In this paper, better method for encryption has been proposed which provides confidentiality to the images with the less computation work. 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 MATLAB R2013a. In this paper encryption with block based matching algorithm is achieved on various images and 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] S.H. Kamali, R. Shakerian "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption" 2010 International Conference on Electronics and Information Engineering (ICEIE 2010).

[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] Z.Yun-peng , Z. Zheng-jun " Digital Image Encryption Algorithm Based on Chaos and Improved DES "Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics San Antonio, TX, USA - October 2000.
[16] H.Gao,Y.Zhang, S. Liang, D.Li "A New Chaotic Image Encryption Algorithm "Chaos, Solitons and Fractals 29 (2006) 393–399.
[17] R. Y. H. Zhao "An Efficient Chaos-based Image Encryption Scheme Using Affine Modular Maps" IJCNIS, 2012, 7, 41-50

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.