A Hybrid Technique of Combining AES Algorithm with Block Permutation for Image Encryption

Ritu Shaktawat[1], Rajdeep Singh Shaktawat[2], N. Lakshmi[3], Avinash Panwar[4], Arun Vaishnav[5]

•

[1,4,5]Department of Computer Science, Mohanlal Sukhadia University, Udaipur, India
[2]Department of Computer Science, College of Technology and Engineering, MPUAT, Udaipur, India
[3]Department of Physics, Mohanlal Sukhadia University, Udaipur, India

ritushaktawat85@gmail.com, shaktawat.rd@gmail.com, nlakshmi@mlsu.ac.in, avinash@mlsu.ac.in, arun.vaishnav@gmail.com

Abstract

In this paper a hybrid approach for image encryption is proposed by combining AES, a standard cryptography algorithm, along with splitting and block permutation. A standard image (Lena) is taken as an input and to enhance the security, the image is divided into 4*4 matrix followed by block permutation before encryption of the image with AES. Comparison of various parameters with and without block permutation confirms the superiority of the proposed method in terms of better results after using splitting and permutation functions.

Keywords - encryption, decryption, cryptography, AES, symmetric algorithm.

I. Introduction

Since the growth of digital communication using internet is increasing at a rapid rate, security of personal/sensitive or commercially valuable information against unauthorized access, misuse and disclosure poses an ever increasing challenge. Images are used in various fields like e- commerce, medical imaging, multimedia, telemedicine, military etc. and necessarily have very confidential information in most of these applications. Currently various standard algorithms exist which were initially designed for text data but are not very effective when it comes to image data [1, 2]. This is because since images have properties which are different from those of texts, these algorithms cannot be implemented directly over the image data and so a different encryption process needs to be adopted. Encryption is a part of cryptography which converts data into unintelligible form so that the original content cannot be accessed or utilized by an unauthorized person and is a common technique to protect data in the form of text or as images [3]. In particular, there has been a huge increase in the use of images in various applications such as in multimedia systems, internet communication, medical imaging, telemedicine, e-commerce, military communication etc., which, in turn, has generated intense research in the field of image encryption. The present work makes use of a symmetric block cipher algorithm, Advance Encryption Standard (AES) since it is a

widely used and standard algorithm which is also readily available. The popularity of AES for encryption of texts is because it requires relatively less memory for implementation, is fairly robust against attacks and is also fast. However, the direct application of AES to images does not replicate the results as in the case of texts. In order to extend the application of AES to images with enhanced security, in the present work, functions like splitting, rotating and reshuffling of blocks have been performed over the image before implementing AES. To test the efficiency of the algorithm, a standard coloured Lena image of size 256*256 in jpeg format has been used as input image in this work.The encryption and decryption processes have been carried out in JAVA followed by testing and analysis of various parameters using MATLAB. Following the introduction which forms Section 1, the rest of the paper is organized as follows: Section 2 presents the literature review, Section 3 gives details of the AES algorithm, Section 4 presents the proposed approach, Section 5 discusses and analyzes the experimental results and section 6 consists of conclusions.

II. Background

Zeghid et al. [4] have implemented a new, modified version of AES over images. They have added a key stream generator to AES to remove textured zones in existing algorithms. The authors have also compared the scheme with other existing symmetric cryptography algorithms.

Using an AES algorithm, Deshmukh [5] has reconstructed the image without any distortion and concluded that the algorithm is strong enough against most common attacks such as the plaintext attacks, brute force attack and cipher attacks because of its extremely large security key space.

Karwande and Mirza [6] have first split an image into a 3*3 matrix and then applied the AES algorithm over the split image to provide more security. In the decryption process, the reverse order was followed; i.e., the split image was obtained first followed by the original image.

Brindha et al. [7] have carried out image encryption using symmetric block cipher algorithm and have made use of the DES algorithm for this purpose. They have first converted the image into byte array which was then converted into string which was used as an input. Authors have also compared the implemented algorithm with AES algorithm.

In an earlier work, Shaktawat et al. [8] had implemented three symmetric block cipher algorithms AES, DES and Blowfish over a real image and then made a comparative study to show the efficiency of these algorithms over the image data. The results of this study indicated that DES has very good performance followed by Blowfish while AES showed the lowest performance.

III. Advance Encryption Standard (AES) algorithm

Advance Encryption Standard is also known as Rijndael algorithm [1]. AES is a block cipher which was developed by two Belgium cryptographers, Joan Daemen and Vincent Rijmen, in 2000 [2]. Daemen and Vincent submitted their algorithm to NIST for the selection process of AES and it was among five finalist algorithms. The AES algorithm developed by Daemen and Rijmen became effective as a US Federal Government standard on 26th May 2002, after approval by the secretary of commerce [1-3]. It is being used worldwide for text encryption and is a well-known symmetric block cipher algorithm. It supports key sizes of 128, 192 and 256 bit. There are 10, 12and 14 rounds for 128, 192 and 256 bit keys respectively [9]. Figure 1 shows the block diagram of AES.

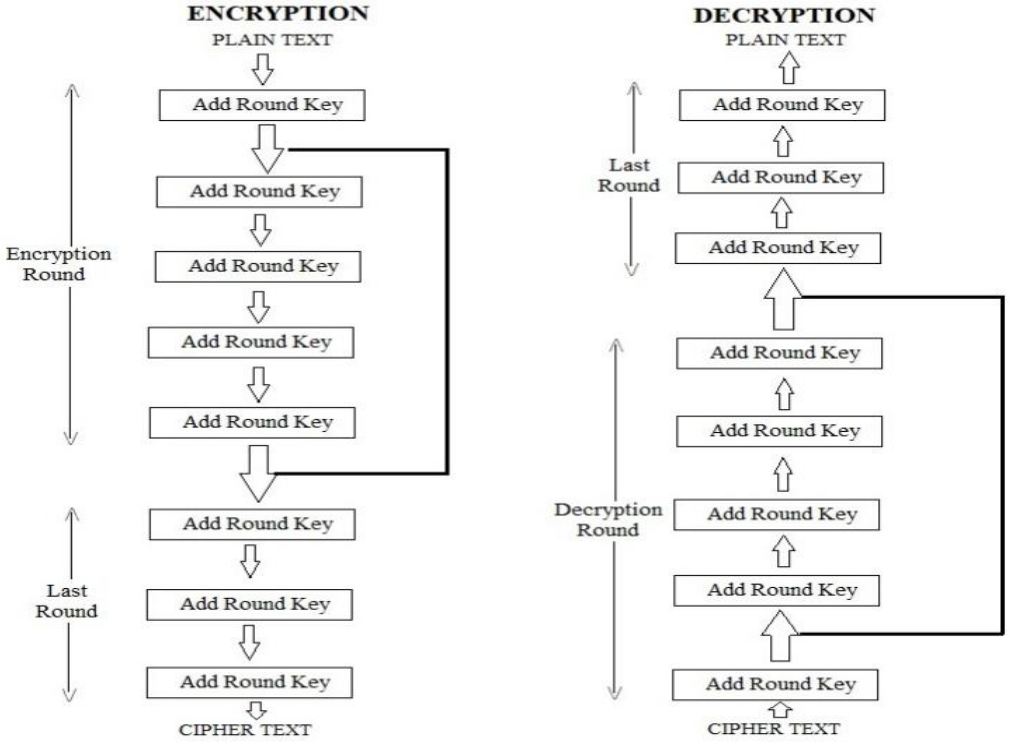

Figure 1: *Encryption and decryption process of AES*

IV. Proposed work

In this section, the proposed approach of implementing AES algorithm using block permutation on an image is presented. Implementation of AES algorithm is done in JAVA and experimental analysis is done using MATLAB. Initially a standard, coloured image (Lena) with size of 256*256 has been taken as an input from GOOGLE. The image is divided into 4*4 matrix which results in 16 blocks. These blocks are then permuted or rotated to change the position of blocks and pixels in the image. A 128 bit key, generated using a random number generator, is used to encrypt the reshuffled image through the AES algorithm. Figures 2 and 3 show the block diagram of proposed encryption and decryption methods respectively.

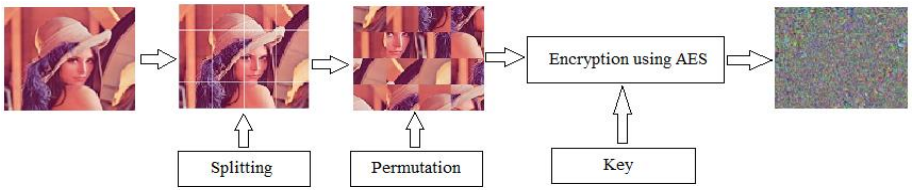

Figure 2: *Block diagram of proposed encryption method*

Figure 3: *Block diagram of proposed decryption method*

In the decryption process, the cipher image is taken as an input and decrypted with AES algorithm using the same key generated for encryption process. The permuted image is obtained after decryption and then reverse permutation operation is applied to the image to obtain the split image which is then combined with all sixteen blocks to get the original image. As shown in figure 3, after decryption the same image with same quality as that of the original is obtained as the original image.

V. Statistical Analysis and Result

i. **Histogram:** A histogram of an image is a graphical representation of the tonal distribution in an image. The entire tonal value can be judged by looking at the histogram since it shows the frequency of similar pixels in an image [10]. The histograms of images encrypted using the proposed method are uniform and are significantly different from the histogram of the original image (Figures 4, 5 and 6). On comparing the histograms of the image which has been encrypted without using permutation (Figure 5) with the one which has been encrypted after permutation (Figure 6), it is evident that the histogram displayed in Figure 6, i.e, of the image which was first split and then permuted followed by encryption is much more uniform. This means that using the proposed hybrid method of combining AES with block permutation operation results in a very low frequency of similar pixels. On comparison of the histograms in Figures 4 and 5 (original and encrypted images respectively) it is also evident that the decrypted image is similar to the original one.

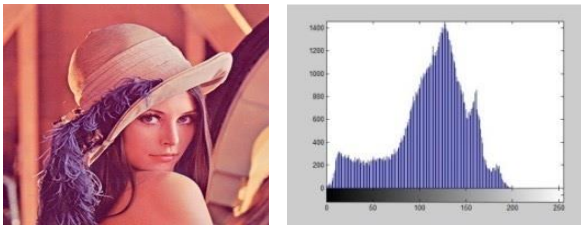

Figure 4: *Original image and Histogram*

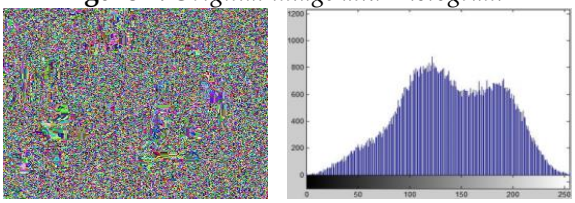

Figure 5: *Encrypted image and Histogram with AES (without block permutation)*

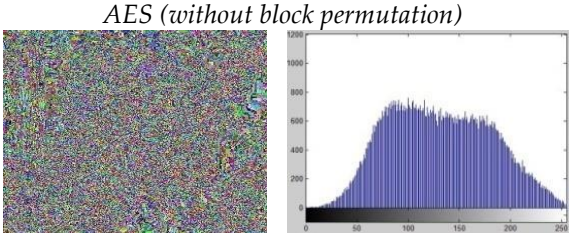

Figure 6: *Encrypted image and Histogram with AES using block permutation*

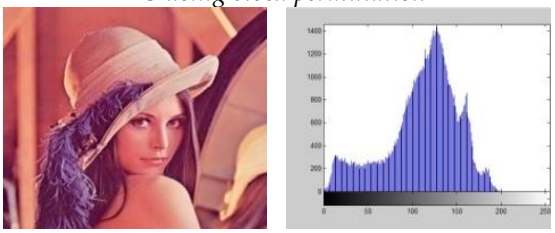

Figure 7: *Decrypted image and Histogram*

ii. **Entropy:** Entropy simply indicates the disorder of the content in an image and is calculated to test the randomness of pixels in an image. The highest value of entropy is 8 [11, 12]. It can be observed from table 1 that a higher level of entropy, with a value close to 8, is obtained with encryption process after using permutation function with AES algorithm.

iii. **PSNR:** PSNR computes the peak signal to noise ratio of an image and is used to measure the quality an encrypted image [13]. A low value of PSNR indicates that the original image and encrypted image are significantly different from each other pointing to the higher security of the encrypted image [14]. From table 1 it is evident that implementing the technique proposed in the present work, which consists of AES with splitting and permutation, yields a lower PSNR ratio than on application of directly implemented AES.

iv. **Correlation:** Correlation indicates any statistical relationship between the pixels of an image. It indicates the dependency of pixels or how the pixels in an image are correlated [15]. The adjacent pixels in an image are always highly correlated and encryption process spreads the pixels in the image. The highest value of correlation is 1. A low value of correlation implies that the adjacent pixels have less dependency and are not easily predictable [16, 17]. From table 1, it is observed that in the approach adopted in the present work, the correlation parameter has very low values, particularly for the horizontal case. This implies that using the proposed method results in a very low correlation among the adjacent pixels, which, in turn indicates stronger security than on direct implementation of AES.

Table 1: *Comparison between AES and AES using block permutation*

Algorithm	Entropy	PSNR	Correlation		
			Vertical	Horizontal	Diagonal
AES	7.5487	11.37	0.0324	0.0010	0.0778
AES using Block Permutation (present work)	7.7926	10.04	0.0205	0.0003	0.0410

VI. Conclusion

In this paper, a standard, coloured image of Lena is taken as an input and the outcome of the implementation of block based symmetric encryption algorithms AES is presented over the image based on some statistical parameters. The superior performance of this standard cryptography algorithm over the image data after the implementation of substitution and transposition approaches by using splitting and permutation functions is amply demonstrated. This is because potential attackers cannot predict that image has first been divided and re-arranged through a random permutation before being encrypted with AES. The study and results of statistical analysis in the case of the hybrid approach adopted in this work shows that the performance is very good with a positive outcome in terms of randomness of the pixels of the encrypted image as it has the higher entropy and PSNR values than the original or direct approach since the histogram and correlation test establishes the reduced dependency and predictability of pixels. This work thus shows how very good results can be achieved by a rather simple modification to a standard AES algorithm which already exists. We are currently in the process of extending this work by exploring the possibility of including other functions for substitution and/or transposition of the image to this standard cryptographic algorithm to improve its performance and hence to make it more versatile in the field of image oriented applications.

References

[1] Stallings W., 2011, *Network Security Essential: Applications and Standards*, 4th edn. Prentice Hall, United States of America.

[2] Kahate A., 2013, *Cryptography and Network Security*, 3rd edn. Tata McGraw Hill, NY, U.S.A.

[3] Gupta B., Agrawal D. P., Yamaguchi S., 2016, *Handbook of research on modern cryptographic solutions for computer and cyber security*, 1st edn. IGI Global, United States of America.

[4] Zeghid, M., Machhout, M., Khriji, L., Baganne, A., & Tourki, R., (2007), "A modified AES based algorithm for image encryption", *International Journal of Computer Science and Engineering*, 1(1), 70-75.

[5] Deshmukh, P., (2016), "An image encryption and decryption using AES algorithm", *International Journal of Scientific & Engineering Research*, 7(2), 210-213.

[6] Karwande, V. S. & Mirza, N., (2014), "Image Encryption using AES Encryption Algorithm", *International Journal & Magazine of Engineering, Technology, Management and Research*. 1(11), 214-218.

[7] Brindha, K., Sharma, R., & Saini, S., (2014), "Use of symmetric algorithm for image encryption", *International Journal of Innovative Research in Computer and Communication Engineering*, 2(5), 4401-4407.

[8] Shaktawat, R., Shaktawat, R. S., Suwalka, I., & Lakshmi, N., (2020), "Implementation of Block-Based Symmetric Algorithms for Real Image Encryption", In *Microservices in Big Data Analytics*, Springer, Singapore, pp. 127-140.

[9] Mulani, A. O., & Mane, P. B., (2019), "High-Speed Area-Efficient Implementation of AES Algorithm on Reconfigurable Platform", In *Computer and Network Security*. IntechOpen.

[10] Mathworks support Homepage, https://in.mathworks.com/help/images/ref/imhist.html, last accessed 2019/09/11.

[11] Mathworks support Homepage,https://in.mathworks.com/help/images/ref/entropy.html, last accessed 2020/01/10.

[12] Sarkar, A., Karforma, S., (2018), "Image Steganography using Password Based Encryption Technique to secure e-Banking Data", *International Journal of Applied Engineering Research*, 13(22), 15477-15483.

[13] Zheng, Q., Wang, X., Khan, M. K., Zhang, W., Gupta, B. B., Guo, W., (2018), "A lightweight authenticated encryption scheme based on chaotic scml for railway cloud service", *IEEE Access*, 6, 711-722.

[14] Mathworks support Homepage, http://in.mathworks.com/help/vision/ref/psnr.html, last accessed 2020/01/05.

[15] Mathworks support Homepage, https://in.mathworks.com/help/images/ref/corr2.html, last accessed 2019/12/05.

[16] Sivakumar, T., Venkatesan, R., (2014), "A novel approach for image encryption using dynamic SCAN pattern", *IAENG International Journal of Computer Science*, 41(2), 91-101.

[17] Tiwari, H., Hamsapriye, N., (2018), "Logistic map based image encryption scheme", *International Journal of Applied Engineering Research*, 13(23), 16573-16577.