American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)
ISSN (Print) 2313-4410, ISSN (Online) 2313-4402

http://asrjetsjournal.org/

Efficient Selective Image Encryption Using Pseudo Random Number Sequences and AES Technique

Ahmed M. Ayoup[a*], Amr H. Hussein[b], Mahmoud A. Attia[c]

[a,b,c] *Electronics and Electrical Communications Engineering Dept., Faculty of Engineering, Tanta University, Tanta 3111, Egypt.*

[a]*Email: Ayoup.2012@hotmail.com*

[b]*Email:amrvips@yahoo.com*

[c]*Email:mahmoudahmedattia@yahoo.com*

Abstract

Selective image encryption has a significant importance in many applications as it offers significant savings in computations, cost, and time. Many attempts are exerted for this purpose as the traditional full image encryption/decryption algorithms may be too massive. In this paper, a new technique for selective image encryption is developed. The algorithm is based on a combination between the pseudo random number sequences, Arnold permutation, and the advanced encryption standard technique. The proposed technique is intended to reduce the execution time of the encryption process and increase the robustness of the encrypted image.

***Keywords*:** Pseudo random number (PRN); Advanced Encryption Standard (AES); Arnold Transformation; Linear Feedback Shift Register (LFSR).

1. Introduction

The selective image encryption has a significant importance in time-critical applications wherein security is also a concern in internet banking transactions , military image database and communication, medical imaging security, satellite image security, pay-TV, confidential video conferencing, corporate communications and military, etc.

---

* Corresponding author.

E-mail address: Ayoup.2012@hotmail.com.

To protect the images from unauthorized access, secure image transfer is required and this can be achieved by using strong encryption techniques like triple Data Encryption Standard (3-DES) and Advanced Encryption Standard (AES) [1]. But the encryption of whole image using these techniques is time consuming.

One way to reduce the implementation time of encryption process, improve the robustness of the encrypted image, and achieve inexpensive security is to use partial encryption (PE) or selective encryption (SE), which is the process of encrypting only carefully selected portions of the original image.

Many attempts are exerted for this purpose. A novel symmetric encryption technique for medical images is presented in [2]. It uses the genetic algorithm which makes it highly adaptive. The images are segmented into a number of regions and the sensitive regions are selected on the basis of pixel intensity and entropy measurements. In addition, it uses several encryption algorithms with variable key lengths to control the execution time required for the encryption process. But, this algorithm provides lower entropy and correlation measurements than the traditional AES. Furthermore, increasing the number of regions should increase the side information which can be considered a main drawback of the algorithm.

A selective encryption technique based on a combination between Arnold's cat map, image hiding, and modified international data encryption algorithm (IDEA) technique was introduced in [3]. The selective encryption is performed by applying the IDEA to the body of the image. In this case, the body of the image is considered as the sensitive area without any rules which is considered the main drawback of this algorithm as the sensitive information may be concentrated in any region rather than the body of the image. In addition, the IDEA has low security compared to 3-DES and AES.

A region based selective image encryption technique was introduced in [4].The image is segmented into a number of regions and the sensitive areas are simply identified by user, not based on any rules. Most existing selective image encryption techniques utilize image compression [5]. The original image is first encoded by a certain kind of encoder. After that, the encoded data are classified into significant part and insignificant part according to their strength of impact or error diffusion in the decoding process. But errors in the significant part will cause substantial change in decoded output or make it unrecognizable.

In this paper, an efficient selective image encryption technique is presented. The proposed technique is based on a combination between the pseudo random number sequences, Arnold permutation, and the advanced encryption standard technique. It combines the randomness and good correlation properities of pseudo random number sequences, speed of arnold permutation, and robustness advantage of AES. So, the proposed technique is intended to reduce the execution time of the encryption process and increase the robustness of the encrypted image. Furthermore, no errors are encountered in the image decryption in contrast to the image compression based selective encryption techniques.

2. Proposed Selective Encryption Technique

In this section, the proposed selective image encryption technique is presented. Figure (1) shows the block diagram of the proposed technique.

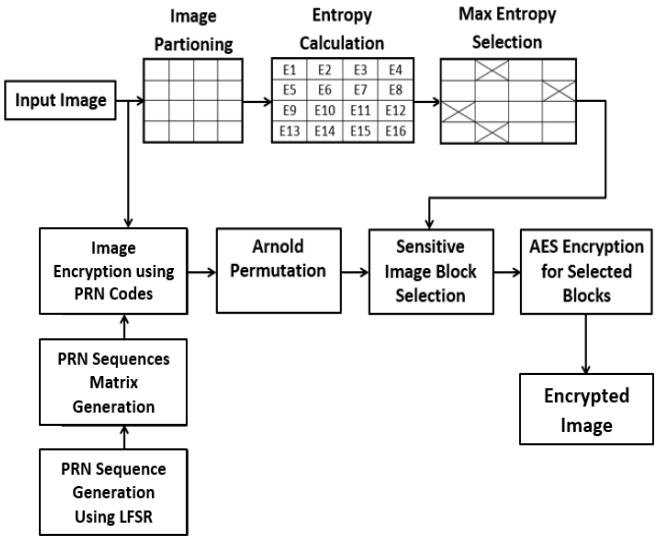


Figure 1: The block diagram of the proposed technique.

The proposed technique follows these steps:

(1) Sensitive Area Selection

The plain image is divided into a number of equal size and non overlapping blocks. Entropy calculation is applied to the individual image blocks to determine the N entropy values $(E_1, E_2, E_3, \ldots\ldots, and\ E_N)$. To recognize the region of interest (ROI) or sensitive area, the blocks having the highest entropy values are selected. For small encryption time and high security the selected blocks should constitute 25% of the size of the plain image.

(2) Pseudo Random Number Matrix Generation

This section presents the pseudo random number generation (PRNG) technique using linear feedback shift register (LFSR). Pseudo random number generators have applications in many areas where producing an unpredictable result is desirable [6]. Random number generators are very useful in developing Monte Carlo method simulations as debugging is facilitated by the ability to run the same sequence of random numbers again by starting from the same random seed. They are also used in various cryptography applications such as data and multimedia encryption keys and bank security communication channels, etc., so long as the seed is secret.

Maximum-length linear feedback shift register produces an m-sequence (i.e. it cycles through all possible $2^n - 1$ states within the shift register). The sequence of numbers generated by this method is random and the period of the sequence is $(2^n - 1)$, where n is the number of shift registers used in the design or the degree of the generator polynomial $P(x)$.

The total number of internal random states generated using the LFSR are $2^n - 1$ and depends on the order of the generator polynomial $P(x)$.

The state of the shift-register at clock pulse i is the finite length vector b_i;

$$b_i = (b_i\,(1\,), b_i\,(2\,), \ldots., b_i\,(n-1\,), b_i\,(n\,)) \tag{1}$$

and the output number c_i at clock pulse i is the concatenation of these states;

$$c_i = (b_i\,(1\,)\&\, b_i\,(2\,)\&\, \ldots.\&b_i\,(n-1\,)\&\, b_i\,(n\,)) \tag{2}$$

where & denotes the concatenation operator.

In this case, a sequence of pseudo random numbers c_i of length M is represented as follows;

$$C_M = (c_1, c_2, c_3, \ldots\ldots., c_M) \tag{3}$$

For $M \times M$ input image, an $M \times M$ matrix of pseudo random numbers $C_{M\times M}$ has to be generated. Considering a sequence of pseudo random numbers C_M of length M, the rows of the coding matrix $C_{M\times M}$ are the L-numbers successive shifted versions of the original sequence C_M where

$$C_{M\times M}(i,:) = circle\ shift\ by\ ((i-1)*L) of\ C_M \tag{4}$$

where i is the row index of the $C_{M\times M}$ matrix, and L is the number of shifts.

The shifted versions of the pseudo random number sequences exhibit low autocorrelation. Such important property plays a significant role in the encryption process of the input images when xored with the $C_{M\times M}$ matrix, as it tends to increase the entropy of the encrypted image, decrease the autocorrelation between the original image and the encrypted image, and provides encrypted image with uniform histogram.

(3) Image Encryption using PRN Sequences

The plain image is initially encrypted using the generated PRN codes. The $M \times M$ plain image is xored with the generated PRN matrix $C_{M\times M}$ to produce a primary PRN encrypted image. This process reduces the correlation between the plain image and encrypted image. It is also secure since it changes the histogram and provides change diffusion.

(4) Image Arnold Transformation

Arnold's cat map scrambling technique [7-9] can be applied in image encryption, and it has more security and better effect. An image (not necessarily a cat) is hit with a transformation that apparently randomizes the original organization of its pixels. However, its period is fixed, the ACM has two main disadvantages:

The original image will be returned to itself if iterating some times, and the histogram of the encrypted image is the same as the histogram of the original image. This is due to the fact that the pixel values themselves didn't change [9]. That is the reason for applying PRN coding for the plain image before Arnold transformation.

(5) AES Encryption

Advanced Encryption Standard (AES) is a cryptographically secure encryption algorithm. A brute force attack requires 2^{128} trials for the 128-bit key size. In addition, the structure of the algorithm and the round functions used in it ensure high immunity to linear and dierential cryptanalysis. Attacks against AES haven't been successful till now and AES is the current encryption standard. The AES design can be used in any application that requires protection of data during transmission through the communication network, including applications such as electronic commerce transactions, ATM machines, and wireless communication. The AES is a universal encryption standard. It can be used for encryption of any type of data, text and other media alike [10].

In the previous section, Arnold cat map is used to shuffle the positions of the primary PRN encrypted image pixels. Selected sensitive image blocks are encrypted using AES to form the final encrypted image.

3. Simulation Results

The proposed SE encryption technique can be applied to any image format. The simulation results was implemented in MATLAB 2014a on an Intel (R), core (TM) i7-2620M, CPU@ 2.7GHz, and 4GB laptop running Windows 7. The 256×256 Lena image is used for simulations.

The simulation follows these steps:

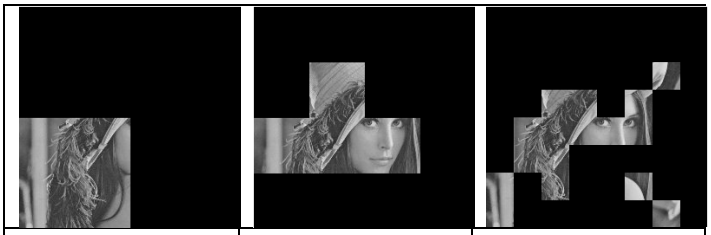
1. The 256×256 Lena image (lena256.jpg) shown in Figure (2) is divided into equal size and non overlapping $N = 2^m$ sub-blocks such that $N = 4, 16, and\ 64$, for $m = 2, 4, and\ 8$, respectively. The resulting sub-bloks are of sizes 128×128, 64×64, and 32×32, respectively.

Figure 2: The 256×256 Lena image (lena256.jpg).

2. Entropy calculation is applied to the individual image sub-blocks.
3. To recognize the region of interest (ROI) or sensitive area, the sub-blocks having the highest entropy values are selected. For small encryption time and high security the selected sub-blocks should constitute 25% of size of input image. The selected entropy values for $N = 4, 16, and\ 64$, caes and the corresponding sensitive sub-blocks are listed in table (1). Figure (3) shows the selected sub-blocks for $N = 4, 16, and\ 64$, cases.

Table 1: Selected entropy values for $N = 4, 16, and\ 64$ caes and the corresponding sensitive sub-blocks.

	Number of image sub- blocks (N)		
	N=4	**N=16**	**N=64**
Selected entropy values	E3= 7.0908	E10=7.0921 E6=7.0611 E11=6.9925 E9=6.9137	E36=7.1335 E43=7.0973 E51=7.0428 E28=7.0142 E38=6.9169 E34=6.8881 E42=6.8782 E35=6.8519 E30=6.8050 E54=6.6925 E27=6.6588 E63=6.6369 E37=6.6242 E49=6.6240 E57=6.5824 E23=6.5006
Selected sensitive blocks	B3	B10 B6 B11 B9	B36 B30 B43 B54 B51 B27 B28 B63 B38 B37 B34 B49 B42 B57 B35 B23



(a) (b) (c)

Figure 3: (a) selected sensitive sub-blocks for $N = 4$ blocks, (b) selected sensitive sub-blocks for $N = 16$ blocks, and (c) selected sensitive sub-blocks for $N = 64$ blocks.

4. Generation of a pseudo random numbers (PRN) sequence C_M using n-stages linear feedback shift register. For 256×256 plain image, it is required to generate a 256 length PRN sequence. In this case, $n = 8$ stages LFSR is used. For maximum length sequence, the the LFSR satisfies the generating polynomial $P(x)$ of Eq. (5). It generates $n = 2^8 - 1 = 255$ internal random states. Figure (4) shows the block diagram of the designed $n = 8$ stages LFSR. The required 256 length sequence C_{256} is composed of the 255 random states plus the first state.

$$P(x) = x\text{^}8 + x\text{^}6 + x\text{^}5 + x\text{^}4 + 1 \quad (5)$$

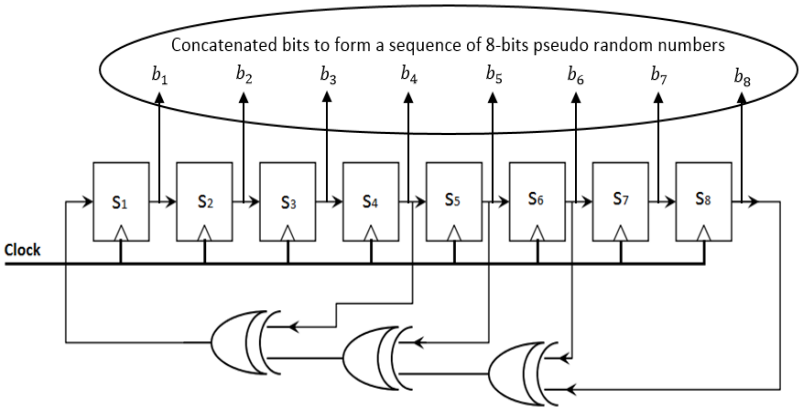


Figure 4: The block diagram of the designed $n = 8$ stages LFSR for generating polynomial $P(x) = x\text{^}8 + x\text{^}6 + x\text{^}5 + x\text{^}4 + 1$.

The main advantage of the PRN sequence is that it exhibits low autocorrelationn properities that enhances the encryption process. Figure (5) shows the autocorrelation between the original PRN sequence and its one number successive shifted versions.

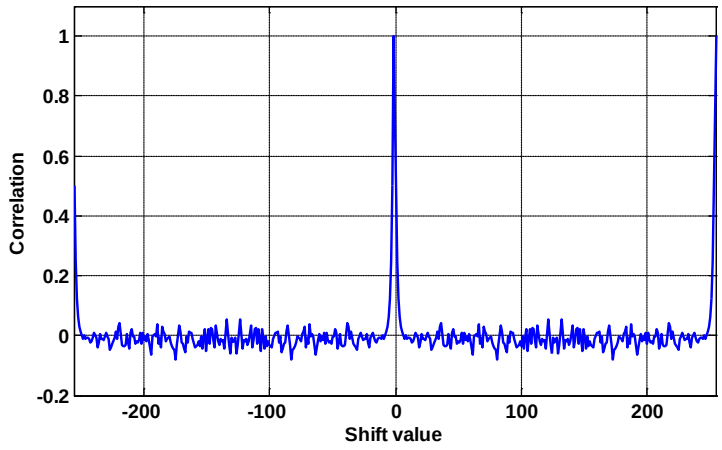


Figure 5: The autocorrelation between the original PRN sequence and its one number successive shifted versions.

5. 256×256 PRN coding matrix formation. The individual rows of the coding matrix $C_{256\times256}$ are the 8-numbers successive shifted versions of the original sequence C_{256}. The shift between any two adjacent PRN sequences in the coding matrix is chosen to be 8 numbers to minimize the correlation between the adjacent pixels in the same column. Figure (6) shows the autocorrelation between the original PRN sequence and its 8-numbers successive shifted versions.

After PRN coding matrix formation, the input plain image is xored with the PRN matrix to generate the primary PRN encrypted image as shown in Figure (7).

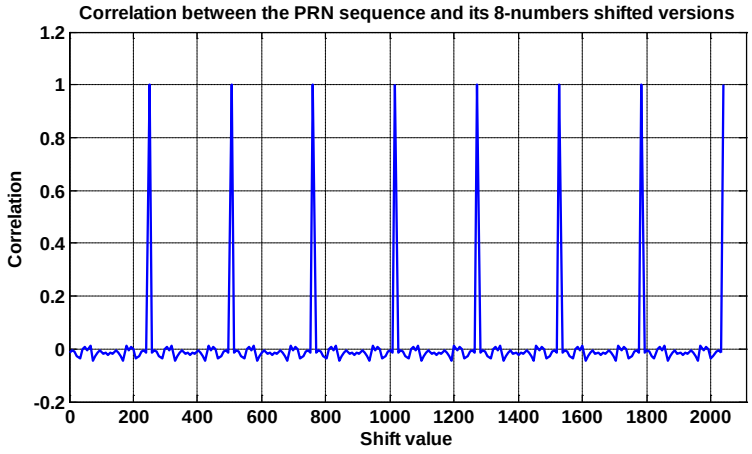


Figure 6: The autocorrelation between the original PRN sequence and its 8-numbers successive shifted versions.

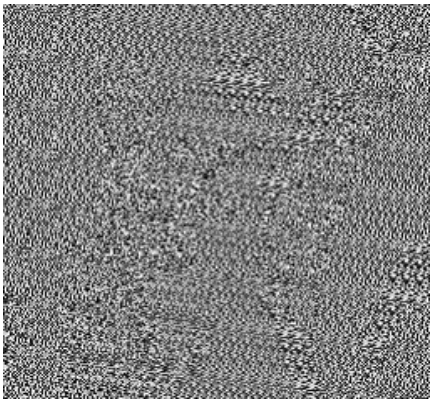


Figure 7: Primary PRN encrypted image.

6. Arnold cat map is used to shuffle the positions of the primary PRN encrypted image pixels, as shown in Figure (8).

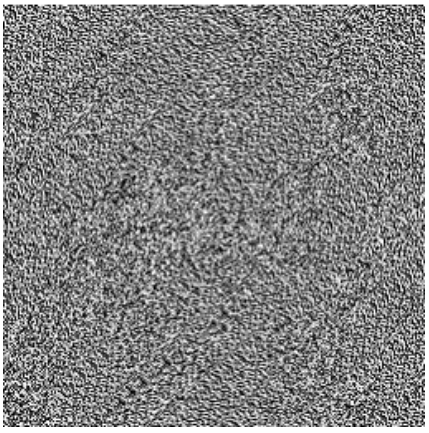
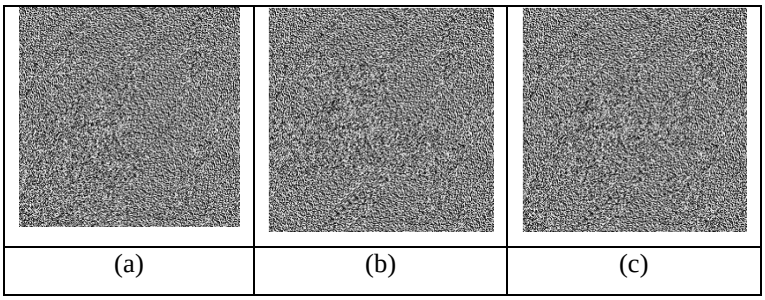


Figure 8: Arnold permutation of the primary PRN encrypted image.

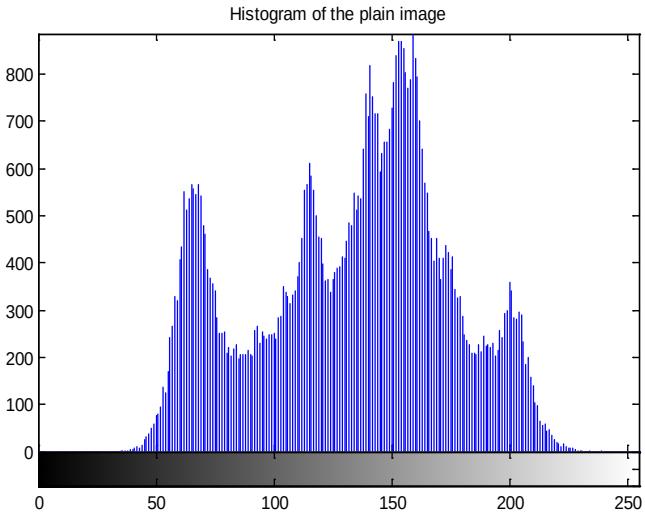
7. Selected sensitive image sub-blocks are encrypted using advanced encryption standard (AES) to form the final encrypted image. The encrypted images for $N = 4, 16, and\ 64$, block caes are shown in Figure (9). The plain image histogram is non-uniform while proposed SE encryption technique results in uniform histogram in all cases, as shown in Figure (10).

The simulation results indicate that the proposed technique provides higher entropy, lower correlation between the plain image and the encrypted image, and reduced encryption time than the AES technique. The encryption times for $N = 4, 16, and\ 64$, block caes are reduced by 72.74%, 72.63%, and 72.3%, respectively compared to full image encryption using AES technique as listed in table (2). Furthermore, the proposed technique provides higher entropy and lower correlation between the plain image and the encrypted image compared to full image encryption using AES technique, as listed in table (2).

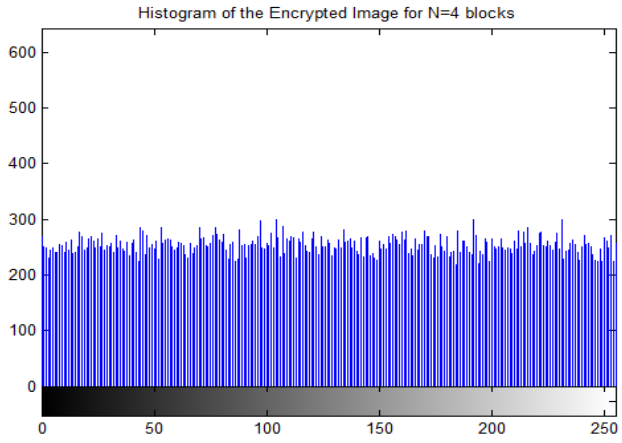


(a) (b) (c)

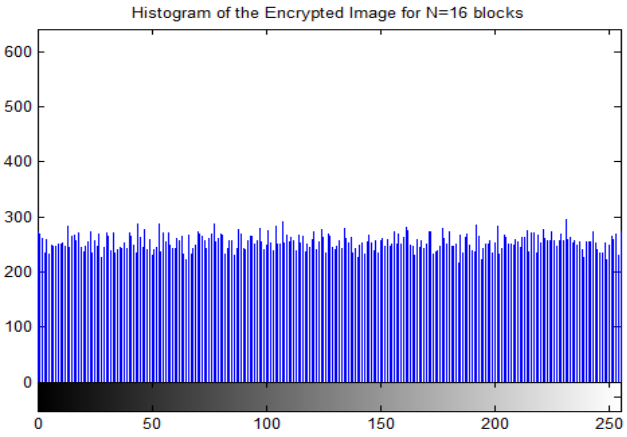
Figure 9: The encrypted images for $N = 4, 16, and\ 64$, blocks caes respectively.



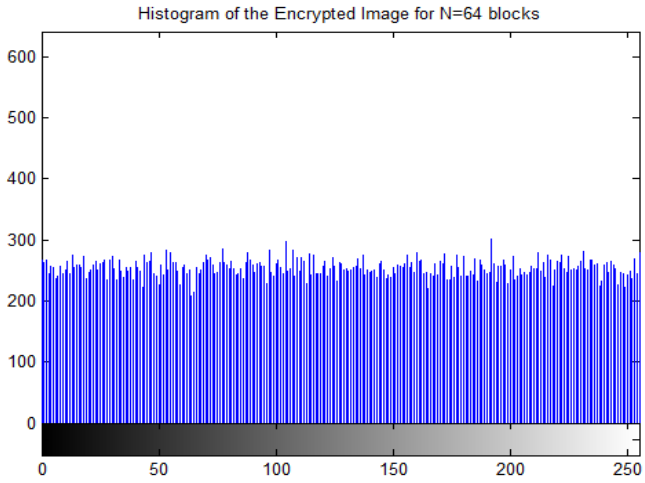
(a)



(b)



(c)



(d)

Figure 10: (a) Histogram of the plain image. (b), (c), and (d) histograms of the encrypted images for $N = 4, 16, and\ 64$ blocks caes respectively.

Table 2: Measured metrics for the proposed SE encryption technique compared to full image encryption using AES technique.

Metrics	Proposed SE Technique			AES
	N=4	N=16	N=64	
Encryption Time (sec)	7.32	7.35	7.44	**26.86**
Time saving (%) compared to AES	72.74%	72.63%	72.3%	----
Entropy	7.9973	7.9977	7.9978	**7.9972**
Correlation between plain image and encrypted image	0.0014	0.0013	0.0015	**0.0019**
ID	0.7221	0.7206	0.7227	**0.7209**
NCPR	99.6292	99.6246	99.6399	**99.6445**
UACI	27.7360	27.7787	27.7672	**27.7907**
MDMF	0.7814	0.7836	0.7872	**0.7891**

4. Conclusion

In this paper, an efficient selective image encryption technique is presented. The algorithm is based on a hyprid combination between the pseudo random number sequences, Arnold permutation, and the advanced encryption standard technique. The proposed technique is intended to reduce the execution time of the encryption process and increase the robustness of the encrypted image. The simulation results indicate that the proposed technique provides higher entropy, lower correlation between the plain image and the encrypted image, and reduced encryption time than the AES technique. The encryption times for $N = 4, 16, and\ 64,$ blocks caes are reduced by 72.74%, 72.63%, and 72.3%, respectively compared to the full image encryption using AES technique. Furthermore, the proposed technique provides higher entropy and lower correlation between the plain image and the encrypted image compared to full image encryption using AES technique.

References

[1] W. Stallings, Cryptography and Network Security Principles and Practice, 5th ed., Prentice Hall, 2011.

[2] A. Mahmood, R. Dony, S. Areibi, "An adaptive encryption based genetic algorithms for medical images", Machine Learning for Signal Processing (MLSP), 2013 IEEE International Workshop, vol., no., pp.1-6, 22-25 Sept. 2013.

[3] A. M. Riad, A. H. Hussein, A. A. El-Azm, "A new selective image encryption approach using hybrid chaos and block cipher," Informatics and Systems (INFOS), 2012 8th International Conference on , vol., no., pp.MM-36,MM-39, 14-16 May 2012.

[4] K. C. Ravishankar, M. G.Venkateshmurthy, "Region based selective image encryption," Computing & Informatics, ICOCI '06. International Conference, pp. 6-8, June, 2006.

[5] S. K. Naveenkumar, H. T. Panduranga, and Kiran, "Partial Image Encryption for Smart Camera," International Conference on Recent Trends in Information Technology (ICRTIT), pp.126-132, 2013.

[6] Schindler, Werner, "Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators", Anwendungshinweise and Interpretation (AIS), pp. 5–11. (Dec., 1999), Retrieved Aug., 2013.

[7] L. Wu, J. Zhang, W. Deng, D. He, "Arnold Transformation Algorithm and Anti-Arnold Transformation Algorithm," Information Science and Engineering (ICISE), 1st International Conference, pp.1164-1167, 26-28 Dec. 2009.

[8] Y. Wang, T. Li, "Study on Image Encryption Algorithm Based on Arnold Transformation and Chaotic System," Intelligent System Design and Engineering Application (ISDEA), 2010 International Conference on , vol.2, pp.449-451, 13-14 Oct. 2010.

[9] S. Lian, Multimedia content Encryption, CRC Press, Taylor & Francis Group, 2009.

[10] Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, Nov. 2001.