A New Image Encryption Approach using The Integration of A Shifting Technique and The Aes Algorithm

Ahmed Bashir Abugharsa
Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka

Abd Samad Bin Hasan Basari
Centre of Advanced Computing Technology, Faculty of Information and Communication Technology, UTeM

Hamida Almangush
Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka

ABSTRACT

In this paper, a new image encryption technique is proposed based on the integration of shifted image blocks and basic AES, where the shifted algorithm technique is used to divide the image into blocks. Each block consists of number of pixels, and these blocks are shuffled by using a shift technique that moves the rows and columns of the original image in such a way to produce a shifted image. This shifted image is then used as an input image to the AES algorithm to encrypt the pixels of the shifted image.

In order to evaluate the performance, the proposed integration technique and AES algorithm were measured through a series of tests. These tests included a histogram analysis, information entropy, correlation analysis, differential analysis. Experimental results showed that the new integration technique has satisfactory security and is more efficient than using the AES algorithm alone without the shifting algorithm which makes it a good technique for the encryption of multimedia data. The results showed that the histogram of an encrypted image produced a uniform distribution, which is very different from the histogram of the plain image, and the correlation among image pixels was significantly decreased by using the integration technique and a higher entropy was achieved.

Keywords: *Image encryption, Shuffling, AES, Shifted Image, Image Entropy, Block Image Encryption, Correlation*.

1. INTRODUCTION

With the continued growth of multimedia applications, security is an important issue in communication and image storage, and encryption is the best way to ensure security. An encryption image technique attempts to convert the original image to another image which is difficult to identify as the original image. The purpose is to keep the image confidential among users, in other words, it is essential that not just anyone can determine the contents of the image without a decryption key (secure key)[1, 2]. In addition, the algorithm can find application where special storage and transmission security and reliability of digital images is necessary such as medical imaging systems, military communications and confidential video conferencing, etc. [1, 3].

In fact, the use of a communication network to exchange data presents certain risks, which requires the existence of appropriate security measures. For example, the transmitted images can be saved and copied during their transmission without loss of image quality. Images can be hacked in time during an exchange of digital information storage and this is of course illegal. It is therefore necessary to develop a tool for effective protection of transferred data against arbitrary interference. Data encryption is very often the only effective way to meet these requirements. In this paper we are interested in the security of image data, which is considered as complex data, in particular, due its size and the information is two-dimensional and redundant in nature. These features of the data make the algorithms developed in the literature unusable in their traditional form due to speed limitations and loss of information that can be caused by conventional encryption algorithms [4].

There are different encryption algorithms used to encrypt and decrypt images. It can be argued that there is no particular encryption algorithm which satisfies the requirements of all image types. Generally, the majority of the existing encryption algorithms are suitable for text data. However, due to the large data size and real time constraints, algorithms that are good for textual data may not be suitable for multimedia data [5, 6]. In most of the images, the values of the neighbouring pixels are strongly correlated. This means that the value of each pixel may be reasonably predicted from the values of its neighbours [7].

In order to decrease the high correlation among pixels and increase the entropy value of an image, we propose a process based on shifting the rows and columns of the image using the following technique. The shifting process will be used to divide the original image into a number of blocks that are then shifted through the rows and the columns within the image based on a shifted table that is generated by another algorithm before the encryption process starts. The generated image is then fed into the AES encryption algorithm. By using a histogram, the correlation, entropy, MAE, NPCR, and UACI as measures of testing the security, the shifting process and the subsequent technique will be expected to result in a different histogram, a lower correlation, a higher entropy value, and thus an improved security level of the encrypted images, i.e., by using analysis of MAE, NPCR and UACR.

2. RELATED WORK

2.1 An Image Encryption Approach using a Combination of a Permutation Technique Followed by Encryption

Mohammad Ali Bani Younes and Aman Jantan [6] further presented another algorithm for image encryption in April 2008, which was a combination of a permutation technique followed by encryption. It introduced a new technique based on the combination of permutation image encryption and a well-known algorithm known as Rijndael. The original image was divided to blocks of 4 pixels by 4 pixels, which were reorganized into a permuted image through a process of random permutation. Then the generated image was encrypted using the Rijndael algorithm. The results showed that the correlation between the elements of the image had been significantly reduced by using the technique of combination and a higher entropy was obtained.

2.2 Image Encryption Using Advanced Hill Cipher Algorithm

Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra and Ganapati Panda [8] proposed an algorithm called Advanced Encryption Hill (AdvHill) that used a matrix of encryption key involution. They took different pictures and encrypted them using the original Hill cipher algorithm and the proposed AdvHill algorithm. It was evident that the original Hill cipher could not properly encrypt the images if the image consists of a large surface covered with the same colour or grayscale. However, the proposed algorithm worked for all grayscale images, and images of different colours.

2.3 A Novel Image Encryption Algorithm Based on a Hash Function

Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchaki [9] proposed a new algorithm for image encryption based on the SHA-512 hash function. The algorithm consisted of two main sections: The first pre-treatment was to mix only half the picture. The second section used the hash function to generate a mask of random numbers. The mask was then XOR'd with the other side of the image that was encrypted.

2.4 New modified version of the Advanced Encryption Standard based algorithm for image encryption

Kamali S.H., Shakerian R., Hedayati M. and Rahmani M., [10] analysed the Advanced Encryption Standard (AES) and presented a modification of the standard (MAES) to reflect a high level of security and improved image encryption. Their results improved the image security to a high level. Their algorithm was also compared with the original AES encryption algorithm.

2.5 Image Encryption Using Affine Transform and XOR Operation

Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar and Partha Pratim Sarkar [11] proposed a two-phase encoding and decoding algorithm based on shuffling the pixels of the image using the affine transformation followed by encryption of the resulting image using the XOR operation. To redistribute the pixel values in the different locations the technique used the affine transformation with four 8-bit keys. The transformed image was split into 2 pixel x 2 pixel blocks and each block was encrypted using the XOR of four 8-bit keys. The total size of the key used in the algorithm was 64 bits. Their results showed that after the affine transformation of the image the correlation between pixel values had been reduced considerably.

2.6 Permutation based Image Encryption Technique

Sesha Pallavi Indrakanti and P.S.Avadhani [12] proposed a new image encryption algorithm based on random permutation pixels with the motivation to maintain image quality. The technique had three distinct phases in the process of encryption. The first phase was the image encryption. The second phase was the phase of key generation. The third phase was the process of identification. This guaranteed confidentiality for colour images with less calculation and the process of permutation was much faster and efficient. The key generation process was unique and was a different process.

2.7 Image Security via Genetic Algorithm,

Rasul Enayatifar, Abdul Hanan Abdullah [13] proposed a new method based on a hybrid model consisting of a genetic algorithm and an encryption based on the chaotic function applied to an image. In their technique, first a number of encrypted images were built using the original image with the help of the chaotic function. In the next step, encrypted images were used as the initial population to start the operation of the genetic algorithm. Then the genetic algorithm was used to optimize the encrypted images as much as possible. Ultimately, a good cipher image was selected as the final image encryption.

3. THE PROPOSED TECHNIQUE

3.1 Description of the Shifting Algorithm

The shifting algorithm is presented below. It creates a shifted table that will be used to build a new shifted image. The technique works as follows:

- To load the *original* image and divide it into a number of blocks with the same number of pixels. The image is decomposed into blocks, each one containing a specific number of pixels. The blocks are shifted into new locations.
- To combine the hash function and secure key to build the shifted table of encryption that will be used to shift the rows and columns of the image. The secret key and hash function of this approach are used to play the main role in building the shifted table, which will be used to generate the encrypted image with a different number of blocks. The shifting process refers to the operation of dividing and shifting an arrangement of the original image.
- The main idea is that an image can be encrypted by shifting the rows and the columns of the original image and not to change the positions of the blocks but by shifting all the rows a number of times depending on the shift table, and then the same number of times for the columns for an arrangement of blocks. For better encryption the block size should be small, because in that way fewer pixels will be similar to their neighbours as otherwise for an image with a high resolution, the content of such an image may be predicted by an unauthorized user who can thus guess the image.
- In this case, the correlation will be decreased and thus it becomes difficult to predict the value of any given pixel from the values of its neighbours.
- The clear information present in an image is due to the relationship (correlation) among the image elements.

This perceivable information can be reduced by decreasing the correlation among the image pixels using the shifting technique or other technique. In other words, decrease the correlation between the blocks of the image so as to provide a good level of the encryption of the image.

- At the receiver side, the original image can be obtained by an inverse of the shift of the blocks. A general block diagram of the shifting method is shown in Figure 1.

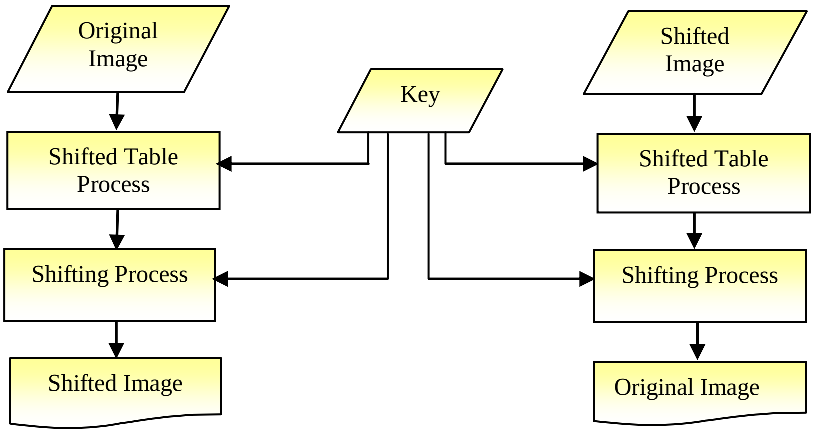


Figure 1 Diagram of the shifting algorithm

The shifting algorithm is presented below. It generates a shifted table that will be used to build a newly encrypted image.

```
ALGORITHM CREATE_SHIFTED_TABLE
1: Load Original Image
2: Input SecureKey
3: Calculate Image Width and Height
4:
    4.1: H_Blocks = Width /3
    4.2: V_Blocks = Height /3
5:
    5.1: V_B_ShiftedTable (Index Of Columns in ShiftedTable ) = 62
    5.2: If (H_Blocks ≥ V_Blocks) then
        H_B_ShiftedTable( Index Of Rows in ShiftedTable ) = H_Blocks
          Else
        H_B_ShiftedTable ( Index Of Columns in ShiftedTable ) = V_Blocks
6:
  For I = 0 to V_B_ShiftedTable -1
        For J = 0 to H_B_ShiftedTable -1
                PositionValue = HashFunction (Index(I),Index(J),SecureKey)
                PositionValue to Assign location I and J in the ShiftedTable
        Next J
  Next I
END CREATE_SHIFTED_TABLE
7: Output: Transformation table
```

```
ALGORITHM CREATE_SHIFTED_IMAGE (Encrypt)
1: Load Original Image
2: Input SecureKey
3: calculate Image Width and Height
4:
    4.1: H_Blocks =ImageWidth /3
    4.2: V_Blocks =ImageHeight /3
5: Divide the original image into (H_Blocks * V_Blocks)
6: L_Key = Length (SecureKey)
7:
  For J = 0 to  L_Key-1
    7.1     (Shift The Rows Of Image)
            IndexOfColumnsInShiftedTable= Int (SecureKey( J ))
        For I = 0 to  H_Blocks-1
              NumberOfShift = ShiftedTable( I , IndexOfColumnsInShiftedTable )
              Shift all the blocks in the row I (NumberOfShift).
        Next I
    7.2     (Shift The Columns Of Image)
            IndexOfColumnsInShiftedTable= Int (SecureKey( J ))
        For I = 0 to  V_Blocks -1
              NumberOfShift = ShiftedTable( I , IndexOfColumnsInShiftedTable )
              Shift all the blocks in the column I (NumberOfShift).
        Next I
  Next J
  END CREATE_SHIFTED_IMAGE
 8:  Output: Shifted Image (Image Encryption)
```

3.2 Description of Integration Technique

The block-based shifting algorithm is based on the integration of image shifting followed by the AES algorithm. The shifting algorithm and the AES algorithm use the original image to generate three encrypted images; (a) a ciphered image using the AES algorithm, (b) a shifted image using a shifting process and (c) a shifted image encrypted using the AES algorithm.

The correlation and entropy of the three images are calculated and evaluated against each other. This technique aims at producing a good security level for the encrypted images by decreasing the correlation among the image pixels and increasing its entropy value.

Image measurements (correlation, entropy and differential analysis) will be carried out on the original image and the encrypted images with and without the shifting algorithm and the results will then be analyzed. The overview of the integration technique is presented in Figure 2.

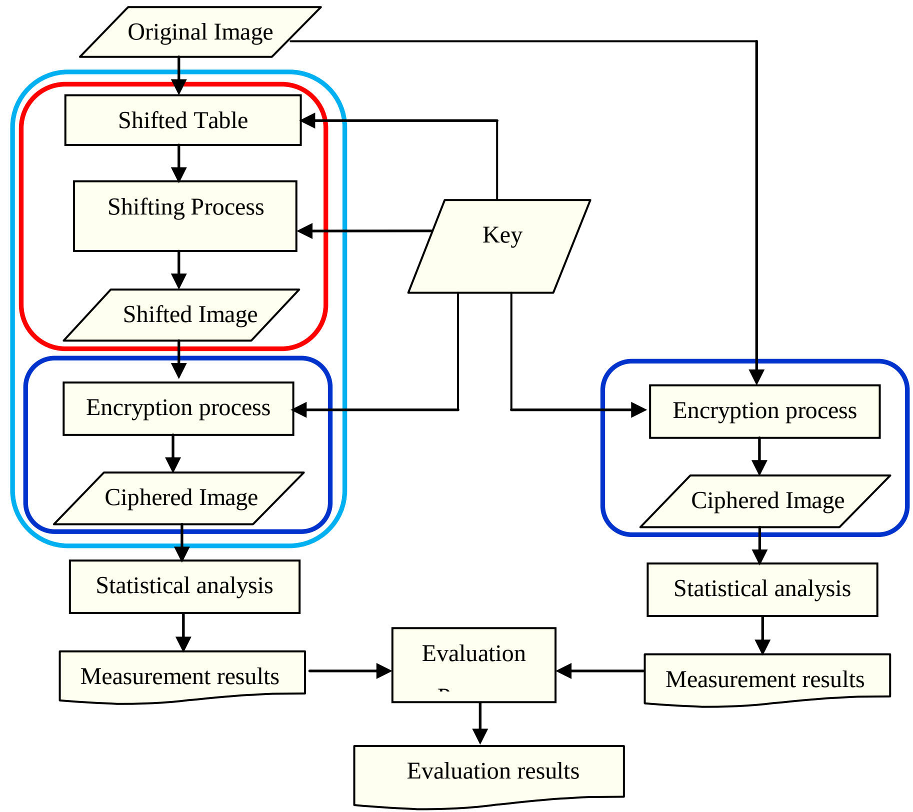


Figure 2. Diagram of the proposed technique

Shifted algorithm, AES algorithm, Proposed technique

4. EXPERIMENTAL DETAILS AND RESULTS

A good quality encryption algorithm should be strong against all types of attacks, including statistical and brute force attacks. Some experiments are given in this section to demonstrate the efficiency of the proposed technique. In this section, a proposed technique is applied on an image that has 300 * 300 pixels and four selected different cases are analyzed in detail to test the performance of the proposed technique. The number of blocks and the block sizes in each case are shown in Table 1.

Table 1 Different cases of number of blocks and the number of pixels

Case number	Number of blocks	Block size
1	150 * 150	2 Pixels * 2 Pixels
2	100 * 100	3 Pixels * 3 Pixels
3	60 * 60	5 Pixels * 5Pixels
4	50 * 50	6 Pixels * 6 Pixels

The shifting algorithm and the AES algorithm are used on the plain image to generate three encrypted images (a) a ciphered image using the AES algorithm, (b) a shifted image using the shifting process and (c) a shifted image encrypted using the AES algorithm. The correlation, entropy and differential analysis of the three images are calculated and evaluated.

4.1 Statistical Analysis

To test the robustness of proposed technique a security analysis is performed. The statistical analysis is presented as the following:

4.1.1 Histogram Analysis

Image histograms may reflect the distribution of image elements. An attacker can examine the histogram of an encrypted image (red, green and blue) using the algorithms of attack and the statistical analysis of the encrypted image to obtain useful information concerning the original image. It is important to ensure that the original image and encrypted image do not have any statistical similarities. The histogram analysis clarifies how the pixels in an image are distributed by plotting the number of pixels at each intensity level.

In the experiments, the original image and its corresponding encrypted image and their histograms for red, blue and green are shown in Figures 3 and 4. The histogram of the original image shows how graphically the distribution of the number of pixels at each grey level. It is clear that the histogram of the encrypted image is almost uniformly distributed and significantly different from the respective histograms of the original image. Thus, the encrypted image does not provide any evidence to use in any statistical attack on the encryption of an image using the proposed technique. The algorithm makes statistical attacks difficult. The histogram of the encrypted image produces an uniform distribution which is very different from the histogram of the plain image.

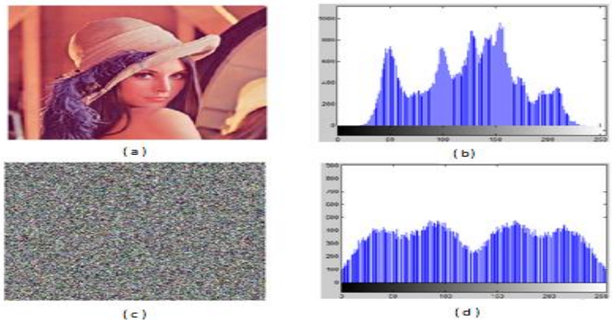


Figure 3: (a) Original Image (b) Histogram of Original Image (c) Encrypted Image (d) Histogram of Encrypted Image

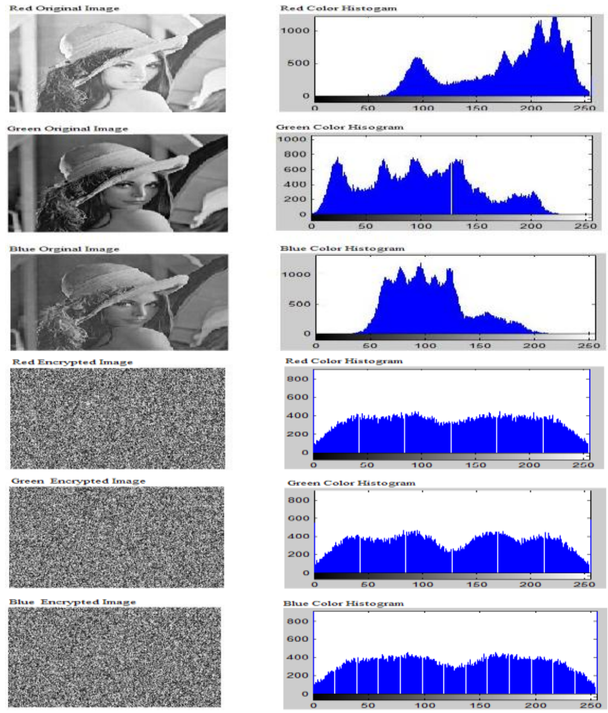


Figure 4: The histograms of red, green and blue channels of the original image, and the histograms of red, green and blue channels of the encrypted image.

4.1.2 Correlation of two adjacent pixels

The correlation between two vertically adjacent pixels, two horizontally adjacent pixels, two diagonally adjacent pixels and two anti-diagonally adjacent pixels in the plain image and the cipher image have been analyzed, in that order.

We randomly chose 5000 pairs of two adjacent pixels. If the correlation of the encrypted image is equal to zero or very near to zero, then the original image and its encrypted image are totally different, i.e., the encrypted image has no features and is highly independent from the original image. If the correlation is equal to -1, this means the encrypted image is a negative of the original image. Figure 5 shows the distribution of two adjacent pixels in the original image and the encrypted image. It is observed that adjacent pixels in the original image have a strong correlation, in other words, there is very good correlation between adjacent pixels in the image elements [2, 14], while there is a weak correlation between adjacent pixels in the encrypted image. Equation (1) is used to study the correlation between two adjacent pixels in the horizontal, vertical, diagonal and anti-diagonal orientations.

$$C_r = \frac{N\sum_{j=1}^{N}(X_j \times Y_j) - \sum_{j=1}^{N} X_j \times \sum_{j=1}^{N} Y_j}{\sqrt{\left(N\sum_{j=1}^{N} X_j^2 - \left(\sum_{j=1}^{N} X_j\right)^2\right) \times \left(N\sum_{j=1}^{N} Y_j^2 - \left(\sum_{j=1}^{N} Y_j\right)^2\right)}} \qquad (1)$$

where x and y are the intensity values of two neighbouring pixels in the image and N is the number of the adjacent pixels selected

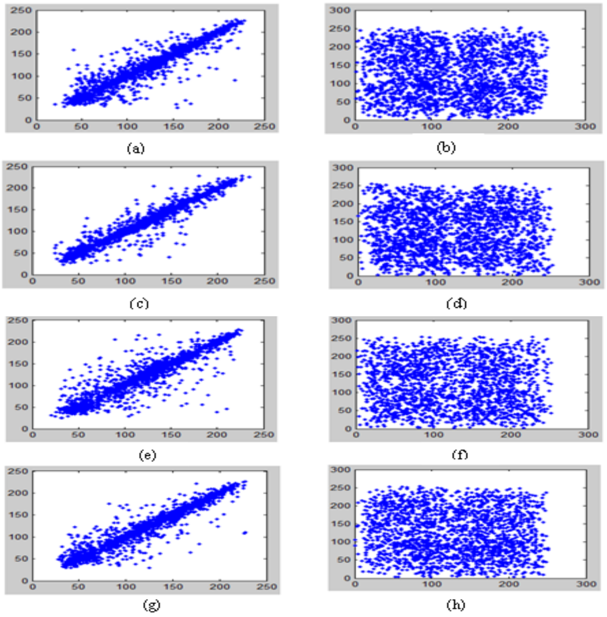


Figure 5: Correlation of two adjacent pixels: (a) distribution of two horizontally adjacent pixels in the original image. (b) distribution of two horizontally adjacent pixels in the encrypted image. (c) distribution of two vertically adjacent pixels in the original image. (d) distribution of two vertically adjacent pixels in the encrypted image. (e) distribution of two diagonally adjacent pixels in the original image. (f) distribution of two diagonally adjacent pixels in the encrypted image. (g) distribution of two anti-diagonally adjacent pixels in the original image. (h) Distribution of two anti-diagonally adjacent pixels in the encrypted image

4.1.3 Information Entropy

Information theory is the mathematical theory of data communication and storage founded in 1949 by Shannon [15]. Information entropy is defined to express the degree of uncertainties in the system. It is well known that the entropy $H(m)$ of a message source m can be calculated as:

$$H(m) = \sum_{i=0}^{2N-1} P(m) \log_2 \frac{1}{P(m_i)} \qquad (2)$$

where $P\ (m_i\ )$ represents the probability of symbol m_i and the entropy is expressed in bits. Let us suppose that the source emits 2^8 symbols with equal probability, i.e., $m = \{m_1, m_2, \ldots, m_{2^8}\}$. Truly random source entropy is equal to 8 [15].Actually, given that a practical information source seldom generates random messages, in general its entropy value is smaller than the ideal one. However, when the image is encrypted, their entropy should ideally be 8. If the output of such a cipher emits symbols with an entropy of less than 8, there exists a certain degree of predictability which threatens its security. Let us consider the cipher-images in Table 2. The number of occurrence of each grey level is recorded and the probability of occurrence is computed. Results for the correlation and the entropy are shown in Tables 2, 3, 4 and 5.

Case 1: The image is divided into 6 pixels * 6 pixels in each block. Figure 6 shows the image cases:

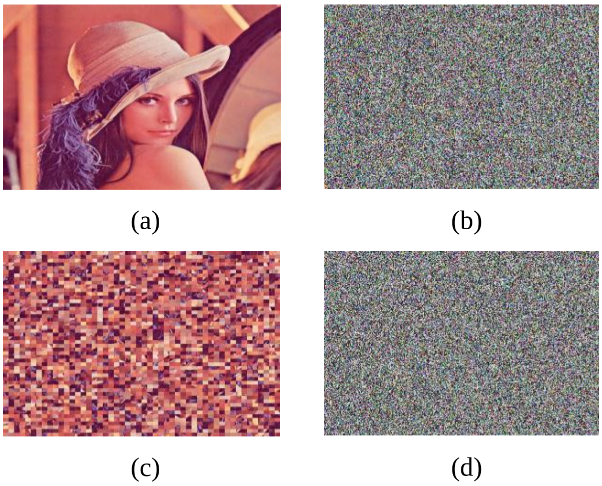

(a) (b)
(c) (d)

Figure 6. (a) Original image. (b) Encrypted image using AES (c) Shifted image. (d) Encrypted image using

integration technique

Table 2. Correlation of Two Pixels and Entropy value

Correlation Analysis					Entropy value
Image	adjacent pixels				
	Horizontal	Vertical	Diagonal	Anti-Diagonal	
A	0.9551	0.9686	0.9364	0.9397	7.4476
B	-0.0212	-0.0290	-0.0387	-0.0293	7.9700
C	0.7660	0.7690	0.5920	0.6089	7.4949
D	-0.0327	-0.0385	-0.0402	-0.0321	7.9924

Case 2: The image is divided into 5 pixels * 5 pixels in each block. Figure 7 shows the image cases:

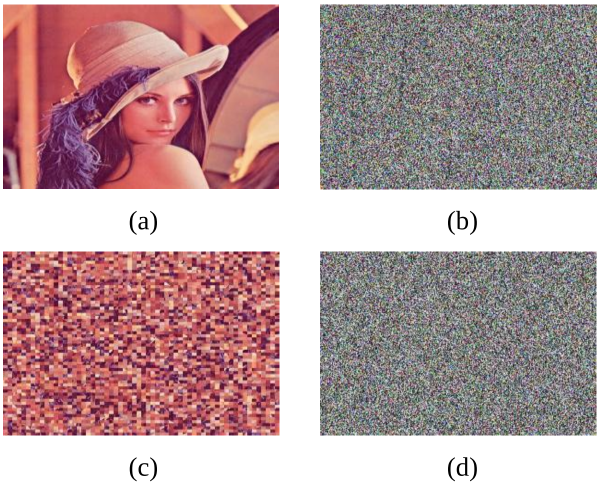

(a) (b)
(c) (d)

Figure 7. (a) Original image. (b) Encrypted image using AES (c) Shifted image. (d) Encrypted image using integration technique.

Table 3. Correlation of Two Pixels and Entropy value

Correlation Analysis					Entropy value
Image	adjacent pixels				
	Horizontal	Vertical	Diagonal	Anti-Diagonal	
A	0.9551	0.9686	0.9364	0.9397	7.4476
B	-0.0212	-0.0290	-0.0387	-0.0293	7.9700
C	0.7169	0.7259	0.5593	0.5770	7.5032
D	-0.0397	-0.0368	-0.0426	-0.0328	7.9837

Case 3: The image is divided into 3 pixels * 3 pixels in each block. Figure 8 shows the image cases:

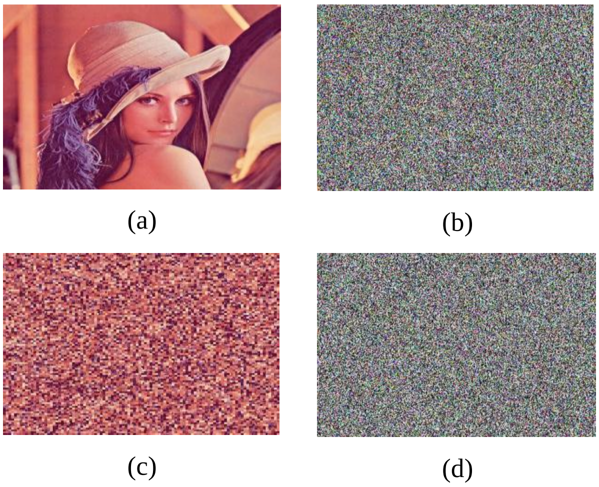
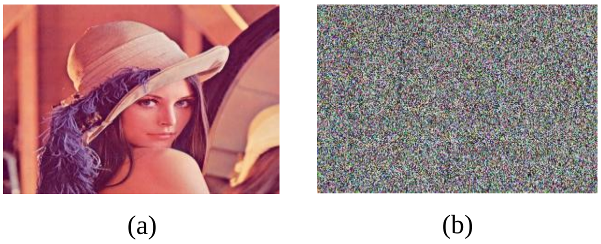

(a) (b)
(c) (d)

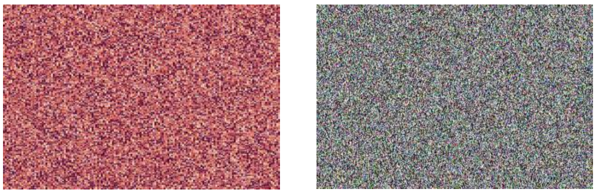
Figure 8. (a) Original image. (b) Encrypted image using AES (c) Shifted image. (d) Encrypted image using integration technique.

Table 4. Correlation of Two Pixels and Entropy value

Correlation Analysis					Entropy value
Image	adjacent pixels				
	Horizontal	Vertical	Diagonal	Anti-Diagonal	
A	0.9551	0.9686	0.9364	0.9397	7.4476
B	-0.0212	-0.0290	-0.0387	-0.0293	7.9700
C	0.6051	0.6103	0.3770	0.3776	7.5112
D	-0.0398	-0.0369	-0.0547	-0.0366	7.9970

Case 4: The image is divided into 2 pixels * 2 pixels in each block. Figure 9 shows the image cases:


(a) (b)



(c) (d)

Figure 9. (a) Original image. (b) Encrypted image using AES (c) Shifted image. (d) Encrypted image using integration technique.

Table 5. Correlation of Two Pixels and Entropy value

Image	Correlation Analysis				Entropy value
	adjacent pixels				
	Horizontal	Vertical	Diagonal	Anti-Diagonal	
A	0.9551	0.9686	0.9364	0.9397	7.4476
B	-0.0212	-0.0290	-0.0387	-0.0293	7.9700
C	0.4221	0.4330	0.1888	0.1970	7.5158
D	-0.0410	-0.0378	-0.0548	-0.0389	7.9985

4.2 Differential analysis

In general, a desirable property for an encrypted image concerns its sensitivity to small changes in the plain-image (e.g., modifying only one pixel). An opponent attempting to crack the encryption can create a small change in the input image to observe changes in the result. By this scheme, a meaningful relationship between the original image and the encrypted image can be simply found. If one small change in the plain image can cause a significant change in the cipher image, with respect to diffusion and confusion, then the differential attack actually loses its efficiency and becomes practically useless. Three common measures have been used for differential analysis: MAE, NPCR and UACI [16-18]. MAE stands for mean absolute error. NPCR is the number of pixel change rate of the ciphered image when one pixel of the plain image is changed. The Unified Average Changing Intensity (UACI) measures the average intensity of the differences between the plain image and the ciphered image. Let *C* (*i*, *j*) and *P* (*i*, *j*) be the grey levels of the pixels at the *i*th row and *j*th column of a *W*×*H* cipher and plain image, respectively. The MAE between these two images is obtained from Equation 3:

$$MAE = \frac{1}{W \times H} \sum_{j=1}^{W} \sum_{i=1}^{H} |C(i,j) - P(i,j)|. \qquad (3)$$

Consider two cipher-images, *C*1 and *C*2, whose corresponding plain images have only one pixel difference. The NPCR of these two images is defined using Equation 4:

$$NPCR = \frac{\sum_{i,j}^{'} D(i,j)}{W \times H} \times 100\,\% \qquad (4)$$

where W and H are the width and height of the image and $D(i, j)$ is defined using Equation 5:

$$D(i,j) = \begin{cases} 0, if\ C_1(i,j) = C_2(i,j) \\ 1, if\ C_1(i,j) \neq C_2(i,j) \end{cases} \qquad (5)$$

Another measure, UACI, is defined using Equation 6:

$$UACI = \frac{1}{W \times H} \sum_{i,j} \left[\frac{|(C_{1(i,j)} - C_{2(i,j)})|}{255} \right] \times 100\,\% \qquad (6)$$

Tests have been performed on the proposed technique on a 256-level grey scale image of size 300×300 pixels. The results are given in Table 6. In order to evaluate the impact of changing one pixel in the plain image on the encrypted image, the NPCR, UACR and MAE are calculated for the proposed technique. The results show that a small change in the original image will result in a significant difference in the cipher (encrypted) image. Therefore, the proposed scheme has a good ability to resist an anti-differential attack

Table 6: Result for differential analysis

Differential analysis between plain image and encrypted image			
Image	**MAE**	**NPCR**	**UACI**
Lena	54.8971	99.6689 %	27.7599 %
Cameraman	48.0368	99.5787 %	26.6995 %
Penguin	49.6552	99.6216 %	29.6995 %

5. CONCLUSION

The proposed algorithm described in this paper has improved image security using an integration of a shifting algorithm and the AES algorithm. It is very important to impact the correlation among image pixels in a plain image to increase the security level of the encrypted image. The proposed technique showed that an inverse relationship exists between the number of blocks and correlation, while there exists a direct relationship between the number of blocks and entropy. The proposed algorithm is expected to show good performance, uniform distribution in a histogram, a low correlation and a high entropy. To quantify the difference between the encrypted image and the corresponding plain-image, three measures were used: MAE, NPCR and UACI. The results show that a small change in the original image will result in a significant difference in the cipher image. Consequently, experimental results show that the proposed algorithm has a high security level. It can withstand against known and chosen plain text, brute force, statistical and differential attacks, and is able to encrypt large data sets efficiently. The proposed method is expected to be useful for real time image encryption.

6. ACKNOWLEDGMENTS

This paper is part of PhD work in the Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM).

7. REFERENCES

[1]. Komal D Patel, S.B., "Image Encryption Using Different Techniques": A Review International Journal of Emerging Technology and Advanced Engineering, 2011. 1(1): p. 30-34.

[2]. H. El-din. H. Ahmed, H.M.K., O. S. Farag Allah, "Encryption quality analysis of the RC5 block cipher algorithm for digital images". Optical Engineering, 2006. 45(10).

[3]. Mohammad Ali Bani Younes, A.J., "Image Encryption Using Block-Based Transformation Algorithm ", IAENG International Journal of Computer Science,, February 2008. 35 , IJCS_35_1_03(1): p. 15-23.

[4]. Belmeguenaï Aïssa, D.N., Redjimi Mohamed, "Image Encryption Using Stream Cipher Algorithm with Nonlinear Filtering Function", in IEEE High Performance Computing and Simulation (HPCS), 2011 International Conference. 2011, IEEE: Istanbul. p. 830 - 835

[5]. M. Van Droogenbroeck , R.B., "Techniques for a selective encryption of uncompressed and compressed images". In ACIVS'02, Ghent, Belgium. Proceedings of Advanced Concepts for Intelligent Vision Systems, 2002(2002).

[6]. Mohammad Ali Bani Younes, A.J., "An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption". IJCSNS International Journal of Computer Science and Network Security, 2008. 8(april 2008): p. 191-197.

[7]. S. P. Nana'Vati, K.P.P., "Wavelets: Applications to Image Compression-I". Scientific and Engineering Computing, 2004. 9 No 3: p. 7.

[8]. B.Acharya, S.K.P., G.Panda, "Image Encryption Using Advanced Hill Cipher Algorithm", 2009 Journal of Recent Trends in Engineering (IJRTE), 2009. 1: p. 663-667.

[9]. Seyedzade, S.M.A., R.E.; Mirzakuchaki, S., "A novel image encryption algorithm based on hash function", in Machine Vision and Image Processing (MVIP), 2010 6th Iranian. 2010, IEEE: Isfahan p. 1 - 6.

[10]. Kamali, S.H.S., R. Hedayati, M. Rahmani, M. , "A new modified version of Advanced Encryption Standard based algorithm for image encryption", in Electronics and Information Engineering (ICEIE), 2010 International 2010, IEEE: Kyoto. p. V1-141 - V1-145.

[11]. Amitava Nag, J.P.S., Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar , Partha Pratim Sarkar, "Image encryption using affine transform and XOR operation", in Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), 2011 International Conference. 2011, IEEE: Thuckafay p. 309 - 312 .

[12]. Sesha Pallavi Indrakanti , P.S.A., "Permutation based Image Encryption Technique". International Journal of Computer Applications, 2011. 28(8): p. 45-47.

[13]. Rasul Enayatifar, A.H.A., "Image Security via Genetic Algorithm", in International Conference on Computer and Software Modeling IPCSIT IACSIT, Editor. 2011, IACSIT Press: Singapore. p. 198-203.

[14]. Ibrahim S I Abuhaiba, M.A.S.H., "Image Encryption Using Differential Evolution Approach In Frequency Domain". Signal & Image Processing : An International Journal(SIPIJ), 2011. 2, No.1: p. 51-69.

[15]. Shannon, C.E., "Communication Theory of Secrecy Systems". Bell Syst Tech J. 1949.

[16]. Xiao Feng, X.T., Shaowei Xia, :A Novel Image Encryption Algorithm Based On Fractional Fourier Transform and Magic Cube Rotation", in IEEE 4th International Congress on Image and Signal Processing. 2011, IEEE: China. p. 1008-1011.

[17]. A.N. Pisarchik, M.Z., "Image Encryption with Chaotically Coupled Chaotic Maps". Physica D., 2008. vol. 237, no. 20: p. 2638-2648.

[18]. G. Chen, Y.M., C. Chui, "A Symmetric Image Encryption Scheme Based on 3d Chaotic Cat Maps". Chaos, Solitons & Fractals, 2004. 12: p. 749-761