

A New Image Encryption Approach using Block-Based on Shifted Algorithm

Ahmed Bashir Abugharsa[†], Abd Samad Bin HasanBasari^{††} and Hamida Almangush^{†††}

[†]Misurata University Faculty IT

^{††}Universiti Teknikal Malaysia Melaka (UTeM)

^{†††}Misurata University Faculty IT

Summary

Security is the main concern in today's world. It is important to secure data from unauthorized access. Data encryption is often used to ensure security in open networks such as the internet. Each type of data has its own features; therefore, different techniques should be used to protect confidential image data from unauthorized access. This paper proposes a new algorithm. The first part of the algorithm aims to build a shifted table using hash function within encryption phase and decryption phase to generate an encrypted (shifted) image and the original image. The second part of the algorithm uses the shifted table resulted from the first part of the algorithm to generate newly shifted image (Encrypted) in which the rows and the columns of the original image are shifted and followed by encryption technique to increase the security of the image encryption. This implies a high similarity and a good quality of the retrieved image compared to the original image. The results show that the correlation between image elements has been significantly decreased using the proposed technique, and higher entropy has been achieved. By using differential analysis, i.e., MAE, NPCR and UACR, a small change in the original image has resulted in a significant difference in the cipher-image. Therefore, the proposed scheme has a high capability to resist anti differential attacks.

Key words:

Image encryption; Shifted Image; Image Entropy; Block Image Encryption; Correlation.

1. Introduction

Many digital services require reliable security in storage and transmission of digital images. Due to the fast growth of the internet in the digital world today, the security of digital images has become more important and been given more attention. Encryption techniques of digital images are very important and should be used to frustrate antagonist attacks from unauthorized access [1], [2]. Visual encryption is important in transferring image through the network to secure it against reading, alteration of its content, adding false information or deleting part of its content [3].

As the number of the Internet users increase exponentially, the need to protect the data and the multimedia on the Internet has become a high priority. Most of the processes in government, military, financial institution, hospitals,

and private businesses greatly deal with data that are in the form of image.

Most of the today's encryption algorithms are based on textual data. These encryption algorithms may not be suitable for encrypting image data types and might not give proper attention to the sensitivity of image types. Digital images are exchanged over various types of networks. It is often true that a large part of this information is either confidential or private. Encryption is the preferred technique for protecting the transmitted data [4]. There are various encryption systems to encrypt and decrypt image data, however, it can be argued that there is no single encryption algorithm which satisfies the different image types [1].

In general, most of the available encryption algorithms are used for text data. However, due to large data size and real time constrains, algorithms that are good for textual data may not be suitable for multimedia data [5]. Even though triple-data encryption standard (T-DES) and international data encryption algorithm (IDEA) can achieve high security, they may not be suitable for multimedia applications. Therefore, encryption algorithms such as data encryption standard (DES), advanced encryption standard (AES), and international data encryption algorithm (IDEA) have been developed for textual data.

In most of the images, the values of the neighboring pixels are strongly correlated. This means that the value of any given pixel can be reasonably predicted from the values of its neighbors [6]. In order to decrease the high correlation among pixels and increase the entropy value of the image, we propose a process based on the shifted 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 (3 pixels by 3 pixels blocks) that are then shifted through the rows and the columns within the image based on the shifted table that is generated by another algorithm before encryption process starts. The generated image is then fed into the following encryption algorithm. By using the histogram, the correlation, entropy, MAE, NPCR, and UACI as the measures of security, the shifted process and its following technique will be expected to result in a different histogram, a lower correlation, a higher entropy value, and thus improved

security level of the encrypted images, i.e., by using analysis of MAE, NPCR and UACR. The secret key must be known to the sender and the receiver.

2. Related Work

2.1 A New Approach for Fast Color Image Encryption Using Chaotic Map

Kamlesh Gupta, and Sanjay Silakari presented a new technique in October 2011 that replaces the conventional pretreatment complex system and uses basic operations such as confusion, and diffusion, which provide the same or even better encryption using the 3D cat map and standard 3D. they generate diffusion models using the standard 3D map rotation of the image using vertical and horizontal planes (red and green) of the input image. They shuffle red, green and blue by using the card and 3D Cat Map. Finally, the image is encrypted by performing XOR operation on the shuffled image and the diffusion model. The theoretical analysis and computer simulations are based on the analysis of the space key, statistical analysis, histogram analysis, analysis of information entropy, correlation analysis and analysis differential. These confirm that the new algorithm minimizes the possibility of a brute-force attack to decrypt and is very fast to encrypt concrete images. Theoretical analysis and experimental tests have been carried out, both confirming that the new cipher possesses high security and fast encryption speed. Therefore, the new cipher indeed has excellent potential for practical image encryption applications [7].

2.2 Image Encryption using Block-Based Transformation Algorithm

Mohammad Ali, Bani Younes, and Aman Jantan presented an image encryption approach in February 2008 from combination of image transformation and the well known encryption and decryption algorithm called Blowfish. The original image was divided into blocks of variable sizes, which were rearranged into a transformed image using a transformation algorithm presented here, and then the transformed image was encrypted using the Blowfish algorithm. The results showed that the correlation between image elements was significantly decreased using the proposed technique. The results also showed that increasing the number of blocks by using smaller block sizes resulted into a lower correlation and higher entropy [8].

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

Mohammad Ali Bani Younes, and Aman Jantan presented an image encryption algorithm in April 2008 which was the combination of permutation technique followed by encryption. They introduced a new permutation technique based on the combination of image permutation and the well known encryption algorithm called Rijndael. The original Image was divided into 4 pixels by 4 pixels blocks, which were rearranged into a permuted image using a permutation random process, and then the generated image was encrypted using the Rijndael algorithm. The results showed that the correlation between the image elements was significantly decreased by using the combination technique and higher entropy was achieved [9].

2.4 Image Encryption Using Chaos and Block Cipher

Alireza Jolfaei and Abdolrasoul Mirghadri proposed a new image encryption scheme presented in January 2011 based on the combination of pixels and new brewing amended to simplify AES. The Baker map is used to generate a permutation matrix, which is in turn used to generate the S-box in the AES-S. All parts of the proposed chaotic encryption system were simulated using the computer code. Pixel patch extends the property distribution and correlation dissipates vertical, horizontal and diagonal of two adjacent pixels. The number of occurrences of each gray level in the image is not changed after pixel shuffling. Then shuffled image histogram is the same as the image of the histogram plain. The theoretical and experimental results indicate that the distribution histogram of the image encryption system is proposed as well as the entropy measured is almost equal to the ideal value. The uniform histogram was justified by the chi-square [10].

2.5 Secure Image Data by Double Encryption

Bhola Nath Kushwaha and Jayant Roy proposed a scheme on August 10, 2010 to encrypt data for secure image using a combination of double encryption process based on the combination of encryption by pixel position (x,y) and another encryption for blocks. We are using the public key cryptography which is a universal encryption algorithm with known range. The transformation process we have used is meant to divide the original image into a number of blocks, which are then encrypted by their position with another pixel in the image. The resulted image then becomes the input of the algorithm for public key encryption. By transferring the correlation and the entropy as the security setting, encryption process is performed using their pixel position (x, y), and the AES encryption

algorithm encrypts each block using the recipient's public key. The result shows that the correlation between neighboring pixels of the image is reduced and the entropy is obtained using this technique [11].

3. Proposed Approach

3.1 The proposed approach diagram

A general block diagram of the shifted method is shown in Figure 1.

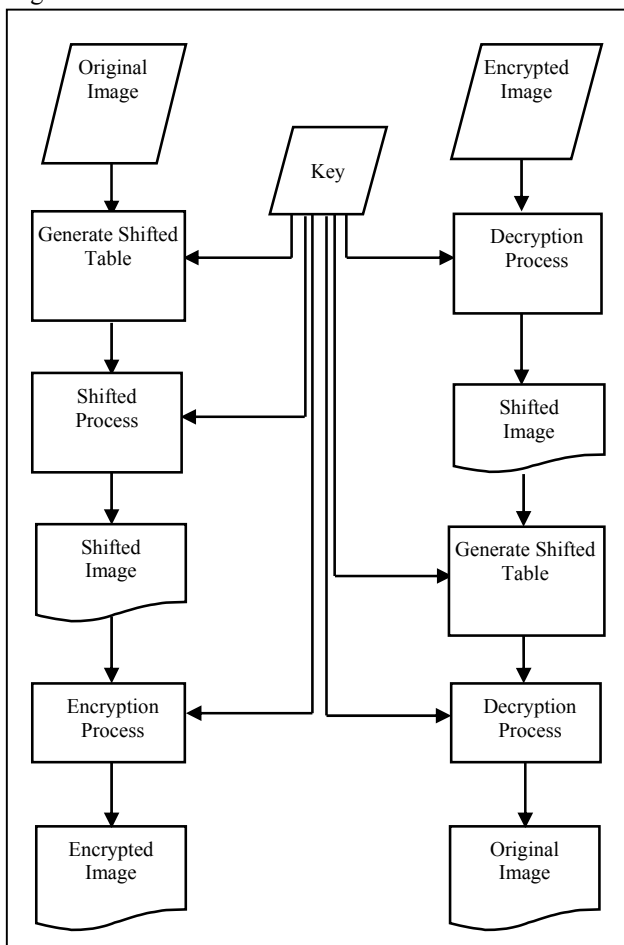


Figure 1 Diagram of the shifted algorithm and its following technique

3.2 ALGORITHM CREATE_SHIFTED_TABLE

- 1: Load Image
- 2: Input SecureKey
- 3: Get ImageWidth and ImageHeight
- 4:
 - 4.1: $\text{HorizontalNoBlocks} = \text{Int}(\text{ImageWidth} / 3)$
 - 4.2: $\text{VerticalNoBlocks} = \text{Int}(\text{ImageHeight} / 3)$
- 5:

- 5.1: $V_N_B_Of_ShiftedTable(\text{Index Of Columns in ShiftedTable}) = 62$
- 5.2: If ($\text{HorizontalNoBlocks} \geq \text{VerticalNoBlocks}$) then
 - $H_N_B_Of_ShiftedTable(\text{Index Of Rows in ShiftedTable}) = \text{HorizontalNoBlocks}$
 - Else
 - $H_N_B_OfShiftedTable(\text{Index Of Columns in ShiftedTable}) = \text{VerticalNoBlocks}$

- 6:
 - For I = 0 to $\text{VerticalNoBlocksOfShiftedTable} - 1$
 - For J = 0 to $\text{HorizontalNoBlocksOfShiftedTable} - 1$
 - PositionValue = HashFunction($\text{Index}(I), \text{Index}(J), \text{SecureKey}$)
 - PositionValue to Assign location I and J ShiftedTable
 - Next J
 - Next I
- END CREATE_SHIFTED_TABLE
- Output: shifted table

3.3 ALGORITHM CREATE_SHIFTED_IMAGE_AND_FOLOVED_TECHNIQUE (Encrypt)

- 1: Load Image
- 2: Input SecureKey
- 3: Get ImageWidth and ImageHeight
- 4:
 - 4.1: $\text{HorizontalNoBlocks} = \text{Int}(\text{ImageHeight} / 3)$
 - 4.2: $\text{VerticalNoBlocks} = \text{Int}(\text{ImageWidth} / 3)$
- 5: Divide the original image to ($\text{HorizontalNoBlocks} * \text{VerticalNoBlocks}$)
- 6: LengthOfKey = Length (SecureKey)
- 7: For J = 0 to LengthOfKey-1
 - 7.1 (Shift The Rows Of Image)
 - IndexOfColumnsInShiftedTable= Int (SecureKey(J))
 - For I = 0 to HorizontalNoBlocks-1
 - NumberOfShift = ShiftedTable(I , IndexOfColumnsInShiftedTable)
 - Shift all the blocks in the row I (NumberOfShift) positions.
 - Next I
 - 7.2 (Shift The Columns Of Image)
 - IndexOfColumnsInShiftedTable= Int (SecureKey(J))
 - For I = 0 to VerticalNoBlocks -1
 - NumberOfShift = ShiftedTable(I , IndexOfColumnsInShiftedTable)
 - Shift all the blocks in the column I (NumberOfShift) positions.
 - Next I
- 8:output the shifted image

```

9: For N = 0 to LengthOfKey-1
  For I = 0 to ImageHeight -1
    For J = 0 to ImageWidth -1
      9.1 Encrypt image each pixel using
        their neighbor pixel & the SecureKey
      Next J
    Next I
  Next N
END
CREATE_SHIFTED_IMAGE_AND_FOLOVED_TECH
NIQUE (Encrypt)
Output: Cipher Image

```

3.4 ALGORITHM DECRYPT_SHIFTED_IMAGE AND_FOLOVED_TECHNIQUE (Decrypt)

```

1: Load Encrypted_Image
2: Input SecureKey
3: LengthOfKey = Length (SecureKey)
  4: Get ImageWidth and ImageHeight
  5: For N = 0 to LengthOfKey-1
    For I = 0 to ImageHeight -1
      For J = 0 to ImageWidth -1
        5.1 Decrypt image each pixel using their
          neighbor pixel and the SecureKey
        Next J
      Next I
    Next N
6: output the shifted image
7:
  7.1: HorizontalNoBlocks = Int(ImageWidth /3)
  7.2: VerticalNoBlocks = Int(ImageHeight /3)
8: Divide the shifted image (Encrypted image) to
  (HorizontalNoBlocks * VerticalNoBlocks )
9:
  For J = LengthOfKey-1 to 0
    9.1 (Shift The Rows Of Shifted Image)
      IndexOfColumnsInShiftedTable= Int
      (SecureKey( J ))
      For I = 0 to HorizontalNoBlocks-1
        NumberOfShift = ShiftedTable( I ,
        IndexOfColumnsInShiftedTable )
        Shift all the blocks in the row I
        (NumberOfShift) position.
      Next I
    9.2 (Shift the Columns Of Shifted Image)
      IndexOfColumnsInShiftedTable= Int
      (SecureKey( J ))
      For I = 0 to VerticalNoBlocks -1
        NumberOfShift = ShiftedTable( I ,
        IndexOfColumnsInShiftedTable )
        Shift all the blocks in the column I
        (NumberOfShift) position.

```

```

      Next I
    Next J
  END CREATE_SHIFTED_IMAGE
  _AND_ORIGINAL Image (Decrypt)
  Output: Original Image (Image decryption)

```

4. Experimental Results

A high-quality encryption algorithm should be strong against all kinds of attacks, statistical and brute force attacks. Some experimental results are given in this section to demonstrate the efficiency of our algorithm. All the experiments are performed on a PC with Intel Core 2 Duo CPU, 4G RAM with Windows Vista. The compiling environment is MATLAB 7.8 (2009a).

4.1. Statistical Analysis

In order to resist the statistical attacks, which are quite common nowadays, the encrypted images should possess certain random properties. To prove the robustness of the proposed scheme, we have performed statistical analysis by calculating the histograms, the entropy, the correlations and differential analysis for the plain image and cipher image. Different images have been tested, and we have found that the intensity values are good.

4.2 Histogram Analysis

Histograms may reflect the distribution information of the pixel values of an image. An attacker can analyze the histograms of an encrypted image (Red, Green and Blue) by using some attacking algorithms and statistical analysis on the encrypted image to get some useful information of the original image. It is important to ensure that encrypted and original images do not have any statistical similarities. The histogram analysis clarifies how 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 of red, blue and green channels are shown in Fig 2 and 3. The histogram of the original images illustrates how the pixels are distributed by graphing the number of pixels in every gray level. It is clear that the histogram of the encrypted image is nearly uniformly distributed, and significantly different from the respective histograms of the original image. Therefore, the encrypted image does not provide any trace to utilize any statistical attack on the proposed encryption of an image procedure, which makes statistical attacks difficult. The encrypted image histogram approximated uniform distribution, hence it is very different from the plain image histogram.

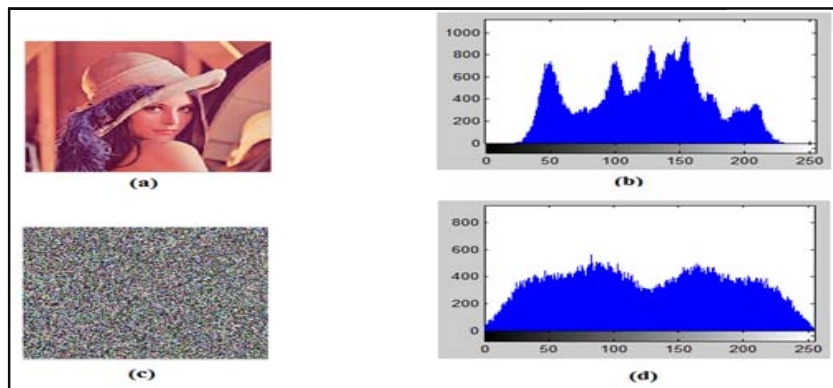


Figure 2: (a) Original Image (b) Histograms of Original Image (c) Encrypted Image (d) Histograms of Encrypted Image

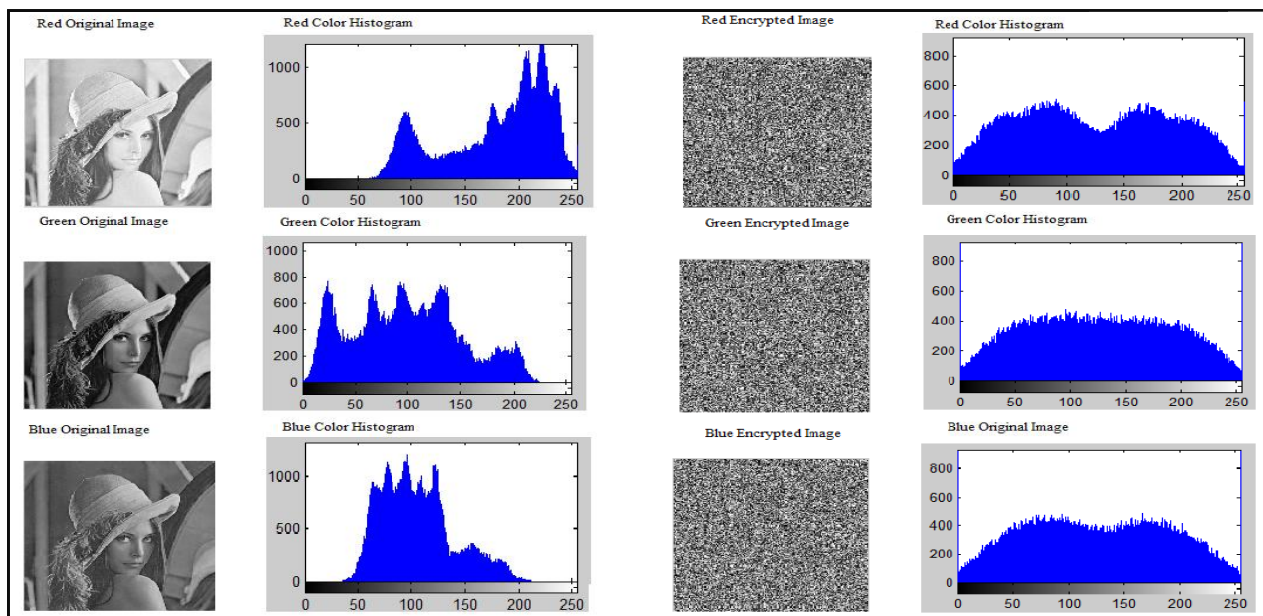


Figure 3: The histograms of red, green and blue channels of the original image, and the histograms of red, green and blue channels of the encrypted image.

4.3 Correlation of two adjacent pixels

In addition to the histogram analysis, we have also analyzed the correlation between two vertically adjacent pixels, two horizontally adjacent pixels, two diagonally adjacent pixels and two anti-diagonally adjacent pixels in plain image and cipher image, respectively.

We randomly select 2000 pairs of two adjacent pixels. If the correlation coefficient equals zero or very near to zero, then the original image and its encryption are totally different, i.e., the encryption image has no features and highly independent from the original image. If the correlation coefficient is equal to -1, this means encrypted

image is a negative of the original image. Figures 4(a),4(b) shows the distribution of two adjacent pixels in the original image and encrypted-image. It is observed that adjacent pixels in the original image (i.e., plain-image) are correlated too much, in other word, there is very good correlation between adjacent pixels in the image data [4], while there is a small correlation between adjacent pixels in the encrypted image. Equation (1) is used to study the correlation between two adjacent pixels in horizontal, vertical, diagonal and anti-diagonal orientations.

$$C_r = \frac{N \sum_{i=1}^N (X_i \times Y_i) - \sum_{i=1}^N X_i \times \sum_{i=1}^N Y_i}{\sqrt{(N \sum_{i=1}^N X_i^2 - (\sum_{i=1}^N X_i)^2) \times (N \sum_{i=1}^N Y_i^2 - (\sum_{i=1}^N Y_i)^2)}} \quad (1)$$

where x and y are intensity values of two neighboring pixels in the image and N is the number of the adjacent pixels selected from the image to calculate the correlation. Result for correlation coefficients of two adjacent pixels is shown in table 1

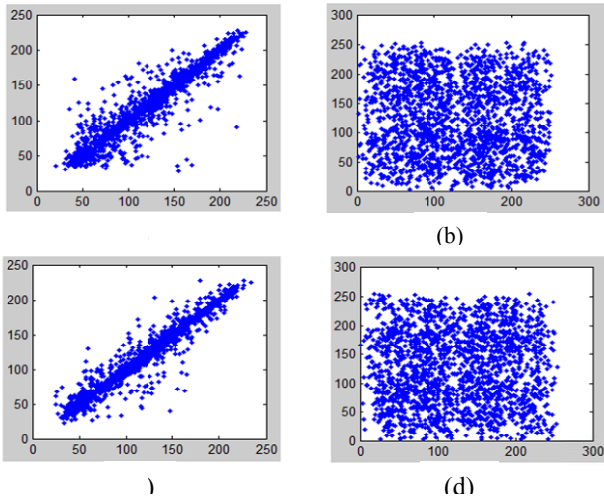


Figure 4(a): Correlation of two adjacent pixels: (a) distribution of two horizontally adjacent pixels in the original image, (b) distribution of two horizontally adjacent pixels in the encrypted-image (i.e., cipher image); (c) distribution of two vertically adjacent pixels in the original image, (d) distribution of two vertically adjacent pixels in the cipher-image.

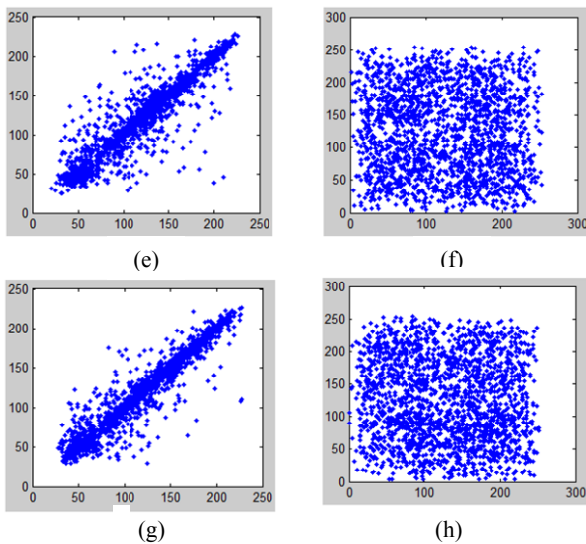


Figure 4(b): Correlation of two adjacent pixels: (e) distribution of two diagonally adjacent pixels in the original image, (f) distribution of two diagonally adjacent pixels in the encrypted-image (i.e., cipher image). (g) distribution of two anti-diagonally adjacent pixels in the original image, (h) distribution of two anti-diagonally adjacent pixels in the cipher-image.

Table 1: Correlation of Two Pixels

Image	Correlation Analysis			
	adjacent pixels			
	Horizontal	Vertical	Diagonal	Anti-Diagonal
Lena Original Image (Plain Image)	0.9799	0.9486	0.9350	0.9523
Encrypted Image (Cipher Image)	-0.0078	-0.0555	-0.0446	-0.0580



4.4 Information Entropy



Information theory is the mathematical theory of data communication and storage founded in 1949 by Shannon [12]. 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:

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

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 28 symbols with equal probability, i.e., $1/28$. Truly random source entropy is equal to 8. 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 messages are encrypted, their entropy should ideally be 8. If the output of such a cipher emits symbols with entropy less than 8, there exists certain degree of predictability which threatens its security. Let us consider the cipher-images in Table 2. The number of occurrence of each gray level is recorded and the probability of occurrence is computed. Results for the entropy are shown in Table 2.

Table 2: Result for the Entropy

Entropy Analysis		
Image		Entropy value
	Original Image (Plain Image)	7.7614
	Encrypted Image (Cipher Image)	7.9926

	Original Image (Plain Image)	7.8308
	Encrypted Image (Cipher Image)	7.9906

4.5 Differential analysis

In general, a desirable property for an encrypted image is about its sensitivity to small changes in plain-image (e.g., modifying only one pixel). Opponent can create a small change in the input image to observe changes in the result. By this scheme, the meaningful relationship between original image and 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 [13, 14]. MAE stands for mean absolute error. NPCR is the number of pixels change rate of ciphered image while one pixel of plain image is changed. 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 gray levels of the pixels at the i th row and j th column of a $W \times H$ cipher and plain image, respectively. The MAE between these two images is obtained from Equation (3):

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

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):

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

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

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





Another measure, UACI, is defined using Equation (6):

$$UACI = \frac{1}{W \times H} \sum_{i,j} \left[\frac{|(C_1(i, j) - C_2(i, j))|}{255} \right] \times 100 \% \quad (6)$$

Tests have been performed on the proposed scheme on a 256-level gray scale image of size 300×300 . The results are shown in Table 3. In order to assess the impact of

changing a single pixel in the original image on the encrypted image, NPCR, UACR and MAE are computed in the proposed scheme. The results show that a small change in the original image will result in a significant difference in the cipher image. Therefore, the proposed scheme has a high capability to resist anti-differential attack

Table 3: Result for differential analysis

Differential analysis between plain image and encrypted image			
Image	MAE	NPCR	UACI
 Original Image (Plain Image)	40.8971	99.5689 %	15.7599 %
 Encrypted Image (Cipher Image)			
 Original Image (Plain Image)	40.0368	99.5467 %	15.6995 %
 Encrypted Image (Cipher Image)			

5. Conclusion

The proposed algorithm of this paper has improved image security using a combination of shifted algorithm and encryption techniques. It is very important to disturb the high correlation among image pixels to increase the security level of the encrypted images. The proposed technique showed that an inverse relationship exists between number of blocks and correlation, while there exists a direct relationship between number of blocks and

entropy. The proposed algorithm is expected to show good performance, low correlation and high entropy. NPCR, UACR and MAE are computed in the proposed scheme. The results show that a small change in the original image will result in a significant difference in the cipher image. Experimental results show that the proposed scheme 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.

References

- [1] Shujun Li and Xuan Zheng. "Cryptanalysis of a chaotic image encryption method", in Proc. IEEE Int. Symposium on Circuits and Systems (ISCAS'2002), 2, 708-711, 2002.
- [2] W. Lee, T. Chen and C. Chieh Lee. "Improvement of an encryption scheme for binary images", Pakistan Journal of Information and Technology, 2(2), 191- 200, 2003, retrieved from <http://www.ansinet.org/>.
- [3] Nawal El-Fishawy¹ and Osama M. Abu Zaid², Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms, International Journal of Network Security, Vol.5, No.3, PP.241–251, Nov. 2007.
- [4] H. El-din H. Ahmed, M. K Hamdy, and O. S. Farag Allah, "Encryption quality analysis of the RC5 block cipher algorithm for digital images," Optical Engineering, Vol. 45, Issue 10107003, 2006, (7 pages).
- [5] M. Van Droogenbroeck and R. Benedett, "Techniques for a Selective Encryption of Uncompressed and Compressed Images," in Proceedings of Advanced Concepts for Intelligent Vision Systems (ACIVS) 2002, Ghent, Belgium, Sept. 2002.
- [6] S. P. Nana'Vati and K. P. Prasanta, "Wavelets: Applications to Image Compression-I," Joined of the Scientific and Engineering Computing. Vol. 9, No.3: 2004, PP. 4-10 <http://www.ias.ac.in/>.
- [7] Kamlesh Gupta, Sanjay Silakari, " New Approach for Fast Color Image Encryption Using Chaotic Map " *Journal of Information Security*, 2011, 2, PP 139-150 doi:10.4236/jis.2011.24014 October 2011 (<http://www.SciRP.org/journal/jis>).
- [8] B. Y. Mohammad Ali and J. Aman, "Image Encryption Using Block-Based Transformation Algorithm," IAENG International Journal of Computer Science, Vol. 35, Issue. 1, 2008, pp. 15-23.
- [9] Mohammad Ali Bani Younes and Aman Jantan, "An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption" International Journal of Computer Science IJCSNS, VOL.8 No.4, PP 191-197, April 2008.
- [10] Jolfaei and Abdolrasoul Mirghadri "Image Encryption Using Chaos and Block Cipher " International Journal of Computer and Information Science, Vol. 4, No. 1, PP 172-185; January 2011.
- [11] Bhola Nath Kushwaha and Jayant Roy, "Secure Image Data by Double Encryption ", *International Journal of Computer Applications (0975 – 8887) Volume 5– No.10, PP 28-32, August 2010.*
- [12] Shannon, C.E. (1949). "Communication Theory of Secrecy Systems". Bell Syst Tech J, 28, 656-715.
- [13] A.N. Pisarchik and M. Zanin, "Image Encryption with Chaotically Coupled Chaotic Maps," *Physica D*, vol. 237, no. 20, 2008, PP. 2638–2648.
- [14] G. Chen, Y. Mao, and C. Chui, "A Symmetric Image Encryption Scheme Based on 3d Chaotic Cat Maps" *Chaos, Solitons & Fractals*, vol. 12, 2004, pp. 749–761.



Ahmed Bashir Abugharsa received BSc in Computer Science from Misurata University in Misurata, Libya, MSc from Universiti Tun Abd Razak, Faculty of Information Technology in January 2011 in Kuala Lumpur, Malaysia and currently enrolled in the PhD program in Computer Science in the Universiti Teknikal Malaysia Melaka (UTeM) in Malaka, Malaysia



Dr. ABD. SAMAD BIN HASAN BASARI received BSc in Mathematics from Universiti Kebangsaan Malaysia in 1998, Master in IT-Education from Universiti Teknologi Malaysia in 2002, PhD in ICT from Universiti Teknikal Malaysia Melaka in 2009 and currently SENIOR Department of Industrial Computing Faculty of Information and



Hamida Mohamed Almagush received BSc in Computer Science from Misurata University in Misurata, Libya, MSc from Universiti Tun Abd Razak, Faculty of Information Technology in January 2011 in Kuala Lumpur, Malaysia and currently enrolled in the PhD program in Computer Science in the Universiti Teknikal Malaysia Melaka (UTeM) in Malaka, Malaysia.