Australian Journal of Basic and Applied Sciences, 7(7): 570-579, 2013
ISSN 1991-8178

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

[1]Ahmed Bashir Abugharsa, [2]Abd Samad Bin Hasan Basari, [3]Hamida Almangush

[1]Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka.
[2]Centre of Advanced Computing Technology, Faculty of Information and Communication Technology, UteM.
[3]Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka.

Abstract: Image scrambling is a useful approach to secure the image data by scrambling the image into an unintelligible format. This paper proposes a new scramble algorithm which can be produced by a series of shifting the rows and the columns. The first part of the algorithm aims to build a shifted table using hash function within scramble phase and descramble phase to generate an scrambled (shifted) image and the retrieved image. The second part of the algorithm uses the shifted table resulted from the first part of the algorithm to generate newly shifted image (Scrambled) in which the rows and the columns of the original image are shifted. This makes the scrambled images difficult to decode thus providing a high level of security protection for the images. The results show that the correlation between image elements has been significantly decreased using the proposed technique, and higher entropy has been achieved. Furthermore, implies a high similarity and a good quality of the retrieved image compared to the original image. The algorithm can be applied in the real-time applications since it is a straightforward process and easily implemented.

Key words: Block Image encryption; Scramble Image; Image Entropy; Block Image Scramble; Image Correlation.

INTRODUCTION

The security of images is of particular interest in this paper. Traditional data encryption algorithms such as the private key encryption standard (DES), public key standards such as Rivest Shamir Adleman (RSA), and the family of elliptic-curve-based encryption (ECC), as well as the international data encryption algorithm (IDEA), may not be suitable for image encryption, especially for real-time applications. In recent years, a number of encryption algorithms have been proposed to protect images. These encryption algorithms can be classified into several categories such as value transformation(Guo, Liu *et al*. 2010; R. Tao, X. Y. Meng *et al*. 2010; Liu, Chen *et al*. 2011; Liu, Xu *et al*. 2011), pixel position permutation (Zunino 1998; Zhao and Gang 2002; Zhang and Liu 2011; Zhu, Zhang *et al*. 2011), and chaotic systems (Wang, Zou *et al*. 2005; Huang and Nien 2009; Wang, Yang *et al*. 2010; Wang, Wong *et al*. 2011; Loukhaoukha, Chouinard *et al*. 2012).

In the first group, Liu *et al*. (Liu, Xu *et al*. 2011) proposed an image encryption algorithm based on an iterative random phase encoding in gyrator transform domains. Two-dimensional chaotic mapping is used to create much random data for iterative random stage encoding. In (Guo, Liu *et al*. 2010), a colour image encryption method using a discrete fractional random transform (DFRNT) and the Arnold transform (AT) in the intensity-hue-saturation (IHS) colour space has been suggested. Each colour space component is then encrypted separately by different approaches. In (Liu, Chen *et al*. 2011), an image encryption algorithm based on the Arnold transform and the gyrator transform has been presented. The amplitude and stage of the gyrator transform are divided into a number of sub-images, which are shuffled using the Arnold transform. The parameters of the gyrator transforms and the separation algorithm provide the key for the encryption process.

Tao *et al*. (R. Tao, X. Y. Meng *et al*. 2010) proposed an image encryption algorithm based on the fractional Fourier transform (FRFT) which can be applied to double or more image encryptions. The encrypted image is achieved by the summation of different orders of inverse discrete fractional Fourier transforms (IDFRFT) of the interpolated sub-images. The complete transform orders of the employed FRFT are used as the secret keys for the decryption of each sub-image.

In the second group, Zunino (Zunino 1998) used Peano-Hilbert curves to provide pixel position permutations (transformation) to destroy the spatial autocorrelation of an image. Zhang and Liu (Zhang and Liu 2011) proposed an image encryption algorithm based on a permutation-diffusion construction and a skew tent map system. In their proposed algorithm, the P-box is chosen as the size of the plain image, which totally scrambles the pixels. To enhance the security, the key stream in the diffusion step depends on both the key and the plain image. Zhao and Chen (Zhao and Gang 2002) proposed to used ergodic matrixes for the shuffling and encryption of images. The authors analyzed the isomorphism relationship between ergodic matrices and

Corresponding Author: Ahmed Bashir Abugharsa, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka.
E-mail: abugharsa@student.utem.edu.my

permutations. Zhu *et al*. (Zhu, Zhang *et al*. 2011) proposed an innovative permutation method to confuse and diffuse the grey-scale image at the bit level, which changes the position of each pixel and changes its value. This algorithm also utilizes the Arnold cat map to permute the bits and a logistic map to additionally encrypt the permutated image.

In the third category, Huang and Nien (Huang and Nien 2009) proposed a new pixel shuffling scheme for colour image encryption which used chaotic sequences created by chaotic systems as encryption codes. In (Wang, Zou *et al*. 2005), a two-dimensional chaotic cat map was generalized to three-dimensions which was then utilized to design a rapid and secure symmetric image encryption algorithm. This algorithm uses the 3D cat map to scramble the locations and the values of the image pixels. Wang *et al*. (Wang, Yang *et al*. 2010) proposed an image encryption algorithm based on a simple perceptron network and used a high-dimensional chaotic system in order to produce three sets of pseudorandom sequences. The weight of each neuron of the perceptron is created in addition to a set of input signals, by use of a nonlinear strategy. Recently, a new image encryption algorithm combining permutation and diffusion has been proposed by Wang *et al*. (Wang, Wong *et al*. 2011). The original image is divided into blocks and a spatiotemporal chaotic system is then employed to create the pseudorandom sequences that are used for diffusing and scrambling these blocks.

This paper proposes a process based on the shifted rows and columns of the image using the shifted. 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 then scrambled the blocks image into original image through shift the rows and the columns within the image based on the shifted table that is generated by another algorithm before scramble process starts.

MATERIALS AND METHODS

The shifting technique works as follows:

- 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.
- Combine the hash function and secure key to build the shifting 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 shifting table, which will be used to generate the shifted 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 Scrambled 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 shifting 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.
- 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. 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.

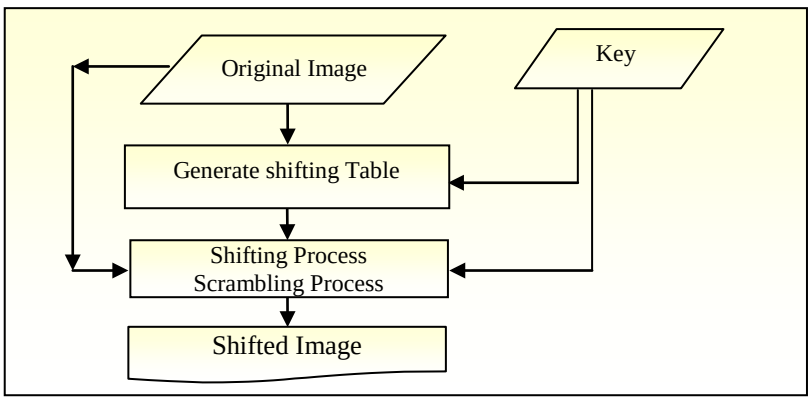

Fig. 1: Diagram of the shifted algorithm at sender side.

The algorithm of the shifting technique will be described and presented in this thesis as following:
Firstly, algorithm is described to generate the shifting table.

```
ALGORITHM CREATE_SHIFTED _TABLE
1: Load Image
2: Input SecureKey
3: Get ImageWidth and ImageHeight
4:
    4.1: HorizontalNoBlocks = Int(ImageWidth /3)
    4.2: VerticalNoBlocks = Int(ImageHeight /3)
5:
    5.1: V_N_B_Of_ShiftedTable (Index Of
         Columns in  ShiftedTable  ) = 62
    5.2: If (HorizontalNoBlocks  ≥
                    VerticalNoBlocks) then
           H_N_B_Of_ShiftedTable( Index Of Rows
           in  ShiftedTable  )  =  HorizontalNoBlocks
         Else
           H_N_B_OfShiftedTable( Index Of Columns
           in  ShiftedTable  ) = VerticalNoBlocks
6:
  For I = 0 to VerticalNoBlocksOfShiftedTable -1
    For J = 0 to HorizontalNoBlocksOfShiftedTable -1
          PositionValue = HashFunction
         (Index(I),Index(J),SecureKey)
          PositionValue  to Assign location I and J
          ShiftedTable
     Next J
  Next I
END CREATE_SHIFTED_TABLE
Output: shifted  table
```

The shifting process uses the original image, the shifting table and secure key to build the newly shifting image with a different arrangement.
Secondly, algorithm describes the generation of the shifted image.

```
ALGORITHM CREATE_SHIFTED_IMAGE
    _AND_FOLOWED_TECHNIQUE (Encrypt)

1: Load Image
2: Input SecureKey
3: Get ImageWidth and ImageHeight
4:
    4.1: HorizontalNoBlocks = Int(ImageHeight / 3)
    4.2: VerticalNoBlocks = Int(ImageWidth /3)
5: Divide the original image  to
      (HorizontalNoBlocks * 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
    Next J
      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_FOLOWED_TECHNIQUE (Scrambled Image)
Output: Scrambled Image
```

Experimental Details and Results:

A good quality encryption algorithm should be strong against all types of attack, including statistical and brute force attacks. Some experiments are given in this section to demonstrate the efficiency of the proposed technique. In this section, the 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	30 * 30	10 Pixels * 10 Pixels
2	50 * 50	6 Pixels * 6 Pixels
3	60 * 60	5 Pixels * 5 Pixels
4	100 * 100	3 Pixels * 3 Pixels
5	150 * 150	2 Pixels * 2 Pixels
6	300 * 300	1 Pixels * 1 Pixels

In this research, an original image is selected as shown in Figure 2 for use in this experiment.

Original image	**Measurements**	
	Correlation	**Entropy**
	0.9714	7.3667

Fig. 2: The original images used in the experiment.

Correlation of Two Adjacent Pixels:

A correlation is a statistical measure of security that expresses a degree of relationship between two adjacent pixels in an image or a degree of association between two adjacent pixels in an image. The aim of correlation measures is to keep the amount of redundant information available in the encrypted image as low as possible(Burger and Burge 2008).

In general, if the correlation coefficient equals zero or is very near to zero, then the original image and its encrypted version are totally different. It can be inferred that the encrypted image has no features and is highly independent of the original image. If the correlation coefficient is equal to -1, that means the encrypted image is a negative of the original image. Equation (1) is used to study the correlation between two adjacent pixels in horizontal, vertical, diagonal and anti-diagonal orientations(El-din., Ahmed *et al*. 2006).

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

Where *x* and *y* are the intensity values of two neighbouring pixels in the image and *N* is the number of adjacent pixels selected from the image to calculate the correlation.

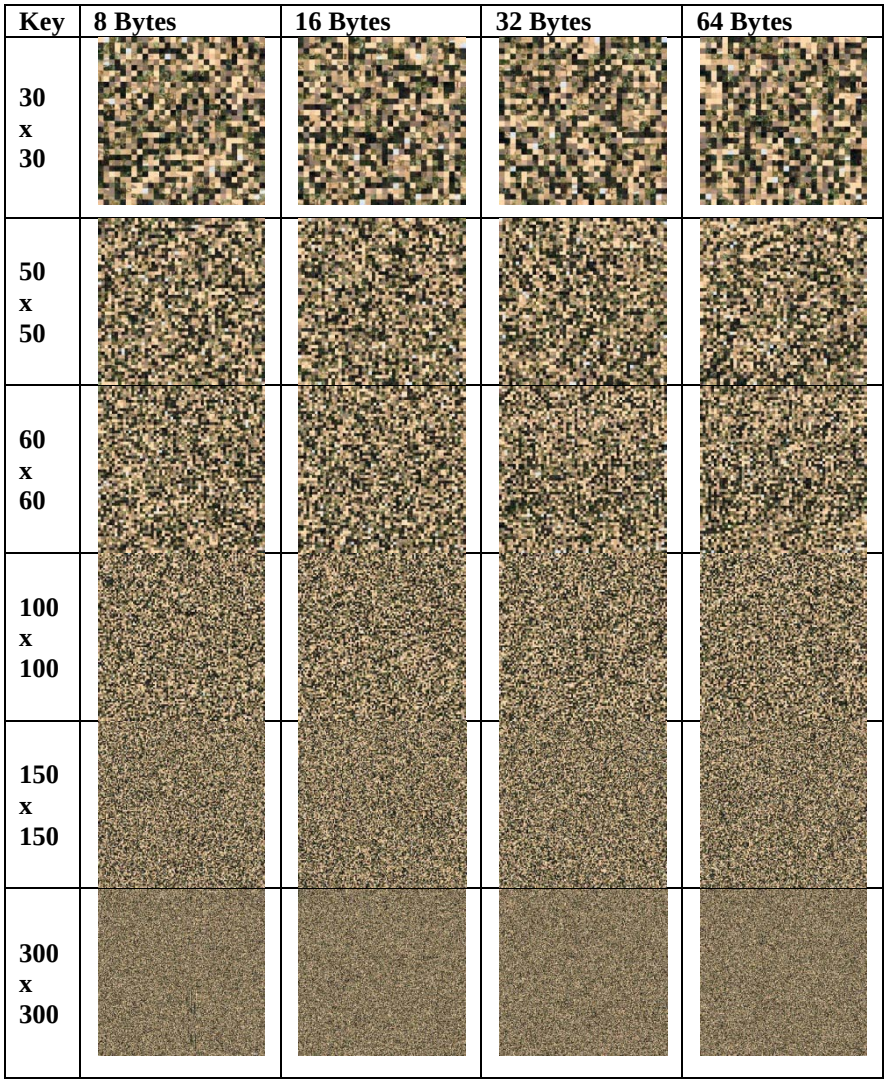

Fig. 3: Result of shifted image for all the cases by using an 8 byte key, 16 byte key, 32 byte key and a 64 byte key.

Impact of Number of Blocks on Correlation of Shifted Image:

In order to evaluate the effect of the number of blocks on the correlation of the images, a different number of block sizes and key lengths have been used for each of these cases. Figure 2 illustrate the results of the shifted image for all the cases by using 8 byte, 16 byte, 32 byte and 64 byte keys respectively. Results for the correlation coefficients of two adjacent pixels are shown in Table 2.

Table 2 and Figure 4 show that there is an inverse relationship between the number of blocks and the correlation. This means that increasing the number of blocks resulted in a lower correlation for all the cases by using the shifting algorithm. The process of dividing and shuffling the positions of the image blocks will confuse the relationship between the original image and the shifted image. Also, it minimizes the relationship among image elements, Therefore, the perceivable information in the shifted image is reduced by decreasing the correlation among the image pixels using the shifting technique.

Table 2: Correlation value results of the shifted image for all cases.

Case	Number of blocks	Key length	Correlation of shifted image
1	30 x 30	8 Bytes	0.828099053
2	50 x 50		0.744299619
3	60 x 60		0.702773236
4	100 x 100		0.540789385
5	150 x 150		0.364913292
6	300 x 300		0.000308951
7	30 x 30	16 Bytes	0.827422901
8	50 x 50		0.743325145
9	60 x 60		0.702399117
10	100 x 100		0.537428801
11	150 x 150		0.36078483
12	300 x 300		-0.000200930
13	30 x 30	32 Bytes	0.826593844
14	50 x 50		0.742806416
15	60 x 60		0.700076349
16	100 x 100		0.535259502
17	150 x 150		0.359747300
18	300 x 300		-0.000214984
19	30 x 30	64 Bytes	0.826318844
20	50 x 50		0.74177068
21	60 x 60		0.696131122
22	100 x 100		0.534117742
23	150 x 150		0.359258962
24	300 x 300		-0.000276434

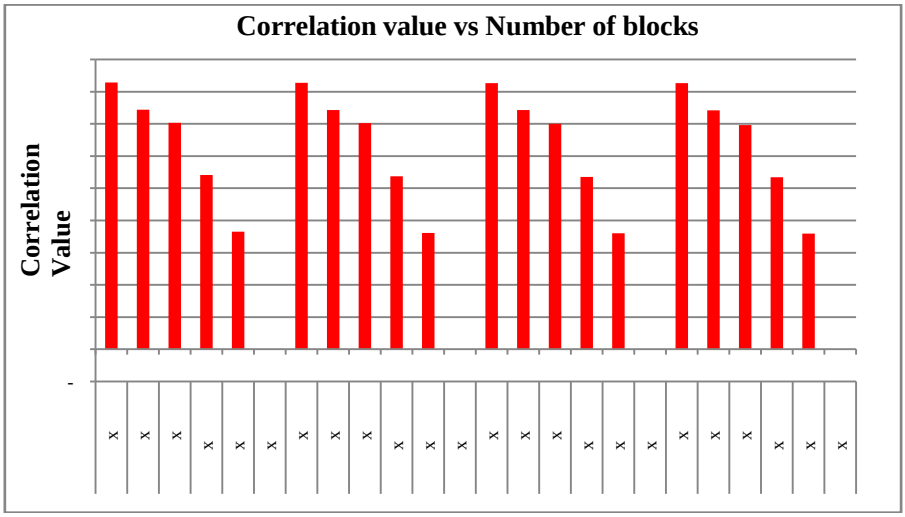

Fig. 4: Correlation value against number of blocks of shifted image.

Impact of Number of Blocks on Correlation of the Encrypted Image:

Table 3 shows the results of the correlation value of encrypted image using the AES algorithmand the combination of the Shifted image and AES algorithm respectively for all the cases. Figure 4 illustrate the correlation of the encrypted image that is encrypted by the AES algorithm alone and the encrypted image that is encrypted by using the combination of the Shifted image and AES algorithm image against the number of blocks by using different key lengths for all cases.

Table 3 and Figure 5 show that increasing the number of blocks by using smaller block sizes results in a lower correlation as well as for the encrypted image by using the combination of the shifted and AES algorithm which resulted in a lower correlation than the encrypted image by using the AES algorithm alone.

Information Entropy:

Information theory is the mathematical theory of data communication and storage founded in 1949 by Shannon (Shannon 1949). 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:

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

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 2^8 symbols with equal probability, i.e., $1\ 2\ 2^8$ $m = \{m, m, ..., m\}$. 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. In order to test and evaluate the effect of the number of blocks and the key lengths of all the cases on the entropy value, different numbers of block sizes and key lengths have been used for these image cases.

Table 3: Correlation value results of the encrypted image for all cases.

Case	Number of blocks	Key length	Correlation of Image AES algorithm	Correlation of image (Shifted image and AES algorithm)
1	30 x 30	8 Bytes	0.00797	-0.00175
2	50 x 50		0.00797	-0.00193
3	60 x 60		0.00797	-0.00211
4	100 x 100		0.00797	-0.00232
5	150 x 150		0.00797	-0.00246
6	300 x 300		0.00797	-0.00325
7	30 x 30	16 Bytes	0.00497	-0.00193
8	50 x 50		0.00497	-0.00239
9	60 x 60		0.00497	-0.00245
10	100 x 100		0.00497	-0.00252
11	150 x 150		0.00497	-0.00258
12	300 x 300		0.00497	-0.00354
13	30 x 30	32 Bytes	0.001725	-0.00221
14	50 x 50		0.001725	-0.00248
15	60 x 60		0.001725	-0.00261
16	100 x 100		0.001725	-0.00269
17	150 x 150		0.001725	-0.00275
18	300 x 300		0.001725	-0.00393
19	30 x 30	64 Bytes	-0.0012	-0.00226
20	50 x 50		-0.0012	-0.00263
21	60 x 60		-0.0012	-0.00275
22	100 x 100		-0.0012	-0.00289
23	150 x 150		-0.0012	-0.00316
24	300 x 300		-0.0012	-0.00441

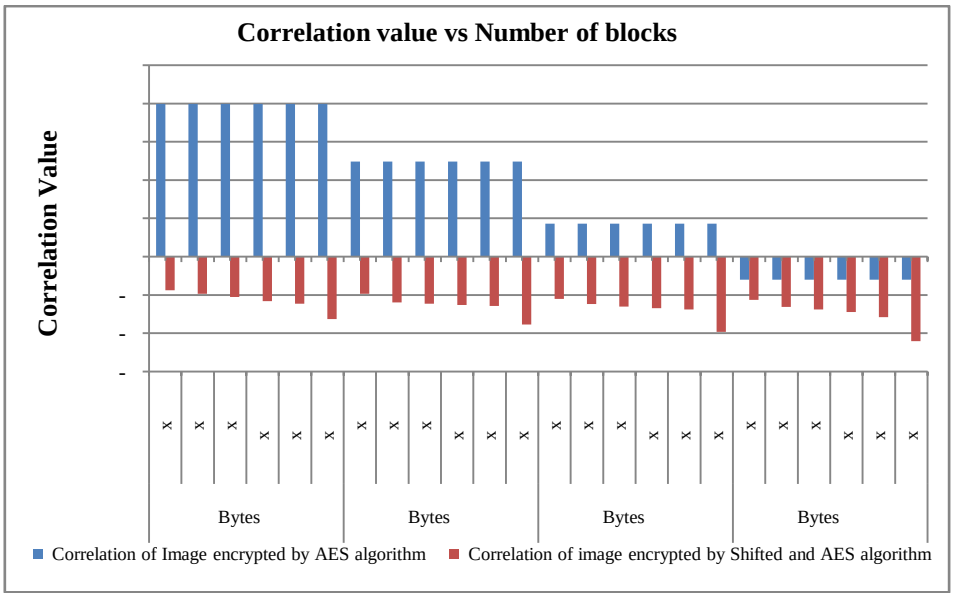

Fig. 5: Correlation value against blocks number of the encrypted image.

Impact of Number of Blocks on Entropy of Shifted Image:

Table 4 and Figure 6 summarize the entropy value results of the shifted image for all cases by using a different number of blocks with different key lengths.

Table 4: Entropy value results of the shifted image for all cases.

Case	Number of blocks	Key length	Entropy of shifted image
1	30 x 30	8 Bytes	7.575176
2	50 x 50		7.679820
3	60 x 60		7.715556
4	100 x 100		7.776080
5	150 x 150		7.820931
6	300 x 300		7.852980
7	30 x 30	16 Bytes	7.575195
8	50 x 50		7.679972
9	60 x 60		7.716901
10	100 x 100		7.776218
11	150 x 150		7.819383
12	300 x 300		7.853466
13	30 x 30	32 Bytes	7.575246
14	50 x 50		7.679980
15	60 x 60		7.718851
16	100 x 100		7.777164
17	150 x 150		7.820140
18	300 x 300		7.854018
19	30 x 30	64 Bytes	7.575260
20	50 x 50		7.680065
21	60 x 60		7.719246
22	100 x 100		7.779339
23	150 x 150		7.821069
24	300 x 300		7.854961

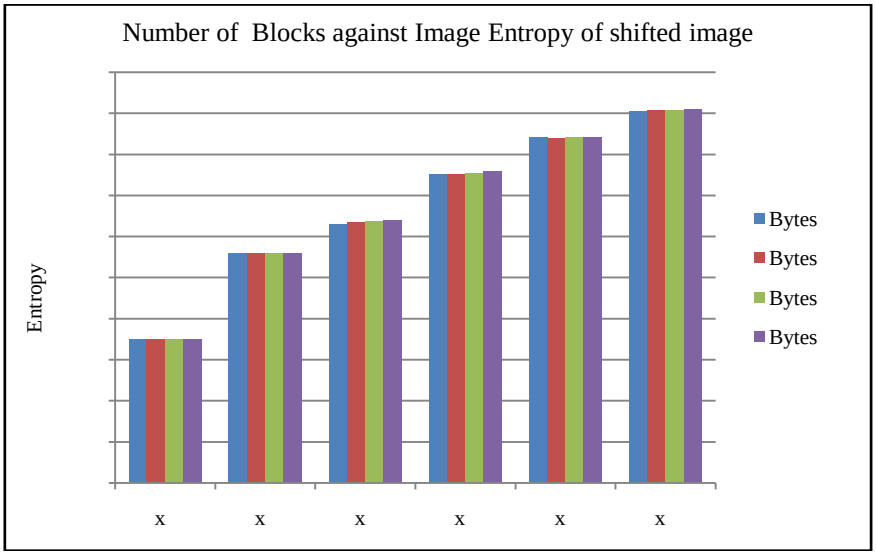

Fig. 6: Entropy value against number of blocks of shifted image.

Table 4 and Figure 6 indicate that there is a direct relationship between the number blocks and the entropy value. This means that increasing the number of blocks resulted in a higher entropy value for all the cases by using the shifting algorithm. The process of the dividing and shuffling of the positions of the image blocks will confuse the relationship between the original image and the shifted image.

Impact of Number of Blocks on Entropy of Encrypted Image:

Table 5 shows the results of entropy value of the encrypted image using the AES algorithm, the combination of the Shifted image and AES algorithm respectively for all the cases. Figure 7 illustrate the entropy value of the encrypted image that is encrypted by the AES algorithm alone and the encrypted image that is encrypted by the combination of the shifted and AES algorithm against the number of blocks by using different key length for all cases.

The results show that a direct relationship exists between the number blocks and the entropy in all the image cases. By increasing the number of blocks using smaller block sizes results in higher entropy value as well as the entropy value of the encrypted image by using the combination of Shifted image and AES algorithm resulting in higher entropy than the encrypted image by using the AES algorithm alone.

Table 5: Entropy value results of the encrypted image for all cases.

Case	Number of blocks	Key length	Entropy of Image AES algorithm	Entropy of image (Shifted image and AES algorithm)
1	30 x 30	8 Bytes	7.92022	7.930618
2	50 x 50		7.92022	7.945864
3	60 x 60		7.92022	7.950186
4	100 x 100		7.92022	7.960366
5	150 x 150		7.92022	7.965666
6	300 x 300		7.92022	7.976624
7	30 x 30	16 Bytes	7.93429	7.936639
8	50 x 50		7.93429	7.948673
9	60 x 60		7.93429	7.952969
10	100 x 100		7.93429	7.96464
11	150 x 150		7.93429	7.967423
12	300 x 300		7.93429	7.978975
13	30 x 30	32 Bytes	7.936571	7.9390971
14	50 x 50		7.936571	7.949958
15	60 x 60		7.936571	7.956703
16	100 x 100		7.936571	7.966677
17	150 x 150		7.936571	7.969678
18	300 x 300		7.936571	7.981002
19	30 x 30	64 Bytes	7.941972	7.9434772
20	50 x 50		7.941972	7.951171
21	60 x 60		7.941972	7.959999
22	100 x 100		7.941972	7.969904
23	150 x 150		7.941972	7.972399
24	300 x 300		7.941972	7.984245

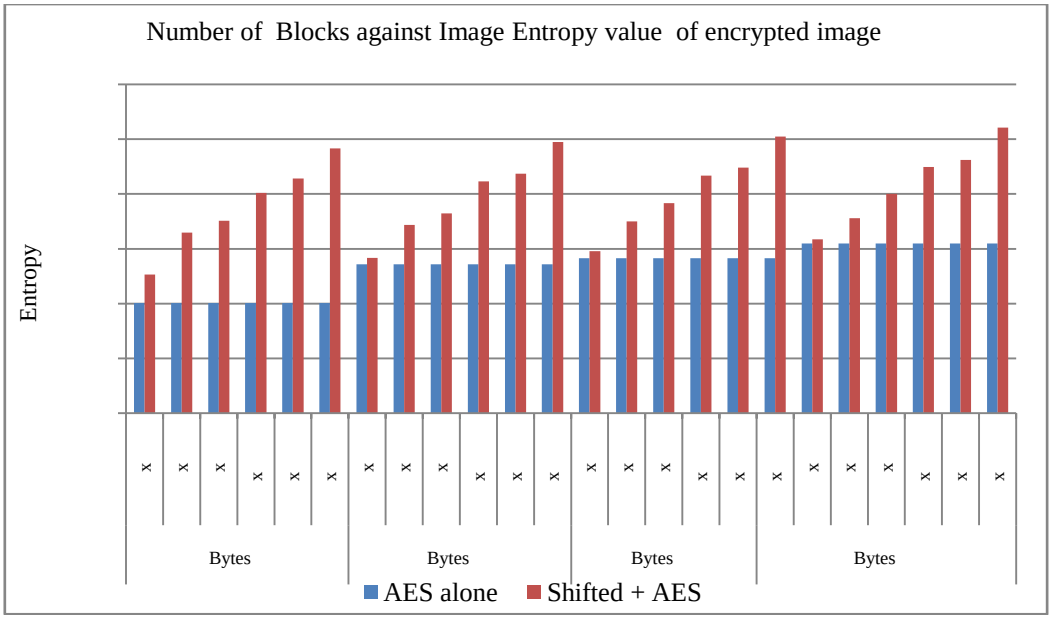

Fig. 7: Entropy results against key length for all the cases of encrypted image.

Discussion:

The shifting technique have been implemented and tested to achieve the objectives of the research. This technique is used as pre-encryption. The correlation measure has been used to test and evaluate the impact of the number of blocks by using a shifting technique. Experimental results of the shifting technique showed an inverse relationship exists between the number of blocks and correlation for all cases. It has also been illustrated that there is a direct relationship between the number blocks and the entropy value. This means that increasing the number of blocks results in a higher entropy value for all the cases.

As a result, the process of dividing and shuffling the positions of the image blocks confuses the relationship between the original image and the shifted image. Moreover, the perceivable information in the shifted image has been reduced by decreasing the correlation among the image elements. Furthermore, the process of dividing and shuffling the positions of the image blocks decreases the mutual information among the shifted image variables. As a consequence, the entropy value is increased.

The combination of the shifting technique and AES algorithm showed that the security level of the encrypted images was enhanced by reducing the correlation (relationship) among the image elements, increasing

the entropy value by decreasing the mutual information among the encrypted image variables (high contrast), Furthermore, the entropy value of the encrypted image by using the combination of the shifting image and AES algorithm results in a higher entropy than for the images encrypted by using the AES algorithm alone. This means that as the number of blocks increases, the entropy increases.

Conclusion:

Simple and strong technique has been proposed for image security using a block based on shifted algorithm (scrambled algorithm). The original image is divided into blocks which are transformed into a shifted rearranged by using a shifting table. The security measurements of the original images have highly correlated elements. This means there is a good relationship between the elements of the original images, which also have a low entropy value and a large standard deviation. The correlation between the image elements is significantly decreased and the entropy value is significantly increased by using the proposed techniques (shifting technique). The proposed technique showed that an inverse relationship exists between number of blocks and correlation, while there is a direct relationship between number of blocks and entropy. The proposed algorithm is expected to show good performance, low correlation and high entropy.

ACKNOWLEDGMENT

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

REFERENCES

Burger, W. and M. Burge, 2008. Digital image processing: an algorithmic introduction using Java, Springer-Verlag New York Inc.

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

Guo, Q., Z. Liu and S. Liu, 2010. "Color image encryption by using Arnold and discrete fractional random transforms in IHS space." Optics and Lasers in Engineering, 48(12): 1174-1181.

Huang, C. and H. Nien, 2009. "Multi chaotic systems based pixel shuffle for image encryption." Optics Communications, 282(11): 2123-2127.

Liu, Z., H. Chen, T. Liu, P. Li, L. Xu, J. Dai and S. Liu, 2011. "Image encryption by using gyrator transform and Arnold transform." Journal of Electronic Imaging, 20: 013020.

Liu, Z., L. Xu, C. Lin, J. Dai and S. Liu, 2011. "Image encryption scheme by using iterative random phase encoding in gyrator transform domains." Optics and Lasers in Engineering, 49(4): 542-546.

Loukhaoukha, K., J.Y. Chouinard and A. Berdai, 2012. "A Secure Image Encryption Algorithm Based on Rubik&# 39; s Cube Principle." Journal of Electrical and Computer Engineering 2012.

R. Tao, X.Y. Meng and Y. Wang, 2010. Image encryptionwithmultiorders of fractional fourier transforms. Information Forensics and Security, IEEE Transactions on Image Processing.

Shannon, C.E., 1949. "Communication theory of secrecy systems." Bell system technical journal, 28(4): 656-715.

Wang, K., L. Zou, A. Song and Z. He, 2005. "On the security of 3D Cat map based symmetric image encryption scheme." Physics Letters A., 343(6): 432-439.

Wang, X.Y., L. Yang, R. Liu and A. Kadir, 2010. "A chaotic image encryption algorithm based on perceptron model." Nonlinear Dynamics, 62(3): 615-621.

Wang, Y., K.W. Wong, X. Liao and G. Chen, 2011. "A new chaos-based fast image encryption algorithm." Applied Soft Computing, 11(1): 514-522.

Zhang, G. and Q. Liu, 2011. "A novel image encryption method based on total shuffling scheme." Optics Communications.

Zhao, X. and C. Gang, 2002. Ergodic matrix in image encryption.

Zhu, Z., W. Zhang, K. Wong and H. Yu, 2011. "A chaos-based symmetric image encryption scheme using a bit-level permutation." Information Sciences, 181(6): 1171-1186.

Zunino, R., 1998. "Fractal circuit layout for spatial decorrelation of images." Electronics Letters, 34(20): 1929-1930.