An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption

Mohammad Ali Bani Younes 1† and Aman Jantan 2††,

Universiti Sains Malaysia, Computer Science, Penang , Malaysia

Summary
Data encryption is widely 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. 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. In most of the natural 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. In this paper, we introduce a new permutation technique based on the combination of image permutation and a well known encryption algorithm called RijnDael. The original image was divided into 4 pixels × 4 pixels blocks, which were rearranged into a permuted image using a permutation process presented here, and then the generated image was encrypted using the RijnDael algorithm. The results showed that the correlation between image elements was significantly decreased by using the combination technique and higher entropy was achieved.

Key words:
Image Correlation, Image encryption, Image entropy, Image histogram, Permutation.

1. Introduction

The development of information technology and the rapid growth of computer networks allowed large files, such as digital images, to be easily transmitted in open networks such as the internet [1]. Each type of data has its own aspects, and different techniques should be used to protect confidential image data from unauthorized access [2]. Encryption is the process of transforming the information to ensure its security [3]. With the huge growth of computer networks and the latest advances in digital technologies, a huge amount of digital data is being exchanged over various types of networks. It is often true that a large part of this information is either confidential or private demanding different security techniques to be used to provide the required protection [4]. Although data encryption is widely used to ensure security, most of the available encryption algorithms are used for text data. Due to large data size and real time constrains, algorithms that are good for textual data may not be suitable for multimedia data. Even though Triple-DES and IDEA can achieve high security, it may not be suitable for multimedia applications and therefore encryption algorithms such as DES, AES, RSA and IDEA were built for textual data. These algorithms are used perfectly to secure textual data. However, digital images are different from texts in many aspects and thus requiring different encryption algorithms [5]-[10]. In most of the natural 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 [11]-[13]. In order to dissipate the high correlation among pixels and increase the entropy value, we propose a permutation process based on the combination of the image permutation and a well known encryption algorithm called RijnDael. The transformation process will be used to divide the original image into a number of blocks (4 pixels × 4 pixels blocks) that are then shuffled their positions within the image. The generated image is then fed to the RijnDael encryption algorithm. By using the correlation and entropy as a measure of security, the permutation process will be expected to result in a lower correlation and a higher entropy value when compared to using the RijnDael algorithm alone, and thus improving the security level of the encrypted images. A similar or different encryption variable-length secret key is needed in the permutation and encryption processes. The secret key must be known to the sender and the receiver. The rest of this paper is organized as follows. Section 2 gives a background about the current image encryption schemes. In Section 3, the description of the proposed permutation algorithm is presented. Section 4 presents the experimental results and discussion. Finally, section 5 concludes the paper.

2. Background

Cryptography is the science of using mathematics to encrypt and decrypt data, and thus it provides a way to store sensitive information or transmit it across insecure networks such as the internet, so that it cannot be read by anyone except the intended recipient [14],[15]. According to [14] while cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking

Manuscript received April 5, 2008
Manuscript revised April 20, 2008

secure communication. In general, conventional textual cryptography algorithms such as DES, Triple-DES, AES and RSA cannot be used to encrypt images directly. Images are different from texts in many aspects such as high correlation among pixels and high redundancy. Thus, a variety of new image encryption schemes have been proposed [16]. Although we may use the traditional encryption algorithms to encrypt images directly, it is not a good idea for two reasons. The first is the image size is often larger than text. Consequently, the traditional encryption algorithms need longer time to directly encrypt the image data, the second, is the decrypted text must be equal to the original text, but this requirement is not necessary for image data. Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable [8], [17] - [19]. According to [20] image encryption techniques try to convert an image to another one that is hard to understand. On the other side, image decryption retrieves the original image from the encrypted one. There are various image encryption systems to encrypt and decrypt data, and there is no single encryption algorithm satisfies the different image types. In most of the natural 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 [11]-[13].

Most of the algorithms specifically designed to encrypt digital images are proposed in the mid-1990s. There are two major groups of image encryption algorithms: (a) non-chaos selective methods and (b) Chaos-based selective or non-selective methods. Most of these algorithms are designed for a specific image format compressed or uncompressed, and some of them are even format compliant. There are methods that offer light encryption (degradation), while others offer strong form of encryption. Some of the algorithms are scalable and have different modes ranging from degradation to strong encryption [21]. Shujun Li *et al*. [20] have pointed out that all permutation-only image ciphers were insecure against known/chosen-plaintext attacks. In conclusion, they suggested that secret permutations have to be combined with other encryption techniques to design highly secured images. Mitra A *et al*.[2] have proposed a random combinational image encryption approach with bit, pixel and block permutations. Zhi-Hong Guan *et al*. [22] have presented a new image encryption scheme, in which shuffling the positions and changing the grey values of image pixels are combined to confuse the relationship between the cipher image and the plain image. Sinha A. and Singh K. [23] proposed an image encryption by using Fractional Fourier Transform (FRFT) and JigSaw Transform (JST) in image bit planes. Maniccam S.S. and Bourbakis N G. [21] proposed image and video encryption using SCAN patterns. The image encryption is performed by SCAN-based permutation of pixels and a substitution rule which together form an iterated product cipher. Ozturk I. and Sogukpinar I. [19] proposed new schemes which add compression capability to the mirror-like image encryption MIE and Visual Cryptography VC algorithms to improve these algorithms. Maniccam S.S., Nikolaos G. and Bourbakis. [24] have presented a new methodology, which performs both lossless compression and encryption of binary and gray-scale images. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology. Droogenbroeck M.V. and Benedett R. [25] have proposed two methods for the encryption of an image; selective encryption and multiple selective encryption. The proposed process divides the image into number of blocks with predefined maximum and minimum number of pixels (4 pixels× 4 pixels blocks), resulting in a stronger encryption and a decreased correlation.

3. The Proposed Technique

The permutation technique works as follows: The *plain image* can be decomposed into blocks; each one contains a specific number of pixels (4 pixels × 4 pixels blocks). Increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy. The blocks are transformed into new locations. The generated image is then fed to the RijnDael encryption algorithm. In this case, the permutation process refers to the operation of dividing and replacing an arrangement of the original image, and thus the generated one can be viewed as an arrangement of blocks. The intelligible information present in an image is due to the correlation among the image elements in a given arrangement. This perceivable information can be reduced by decreasing the correlation among the image elements using certain permutation techniques. As a result, the correlation will be decreased and thus it becomes difficult to predict the value of any given pixel from the values of its neighbors. Furthermore, this process of dividing and shuffling the positions of image blocks will confuse the relationship between the original image and the generated one. At the receiver, the original image can be reproduced by the inverse permutation of the blocks. A general block diagram of the permutation method is shown in Fig. 1. The permutation algorithm is presented below: it will be used to build a newly permuted image to be used before the RijinDael encryption process.

ALGORITHM CREATE_PERMUTATION_TABLE

```
1: Load the plain Image
```

```
2: Input secret key
3: Get the Width and Height of the image
4:
   4.1: Lower Horizontal Number of Blocks = Integer
        (Image Width / 4)
   4.2: Lower Vertical Number of Blocks = Integer
        (Image Height /4)
5: Number of Blocks = Horizontal Number of Blocks ×
   Vertical Number of Blocks
6: Seed = | Hash value (Key) |
7: Randomize ()
8: For I = 0 to Number of Blocks -1
   8.1: Get the new location of block I from the
        permutation table
   8.2: Set block I in its new location
   END PERFORM_PERMUTATION
   Input: plain Image (BMP image file) and permutation
   table
   Output: permuted Image.
```

The permutation process is based on the combination of image permutation followed by encryption, (i.e. a permutation process followed by the RijnDael algorithm). In this case, the permutation process and the RijnDael encryption algorithm use the original image to produce three output images, (a) a ciphered image using RijnDael, (b) a permuted image and (c) a ciphered image using the combination technique. The overview model of the new technique is shown in Fig.2.

4. Experiments

The method used to evaluate the present technique is described in Fig. 2. The algorithm was applied with a bit mapped (bmp) image that has the size of 300 pixels × 300 pixels with 256 colors. In order to evaluate the impact of the proposed technique on the correlation, histogram and entropy, three different key-lengths were used as shown in Table 1.Each case produces three output images with histograms; (a) a ciphered image using the RijnDael algorithm, (b) a permuted image using the proposed algorithm, and (c) a ciphered image using the proposed algorithm followed by the RijnDael algorithm. For the rest of this paper, we use image A, image B, image C, and image D to refer to the original image, the ciphered image using the RijnDael algorithm, the permuted image, and the ciphered image using the proposed algorithm followed by the RijnDael algorithm respectively. Correlation and entropy are computed for each case according to equation (1) and equation (2). **Case 1**: key length: 8-byte; 64 bits. Fig.3. shows the resulted images with histograms. The correlation and entropy results of this case are summarized in table 2 and fig.4. **Case 2**: key length: 16-byte; 128 bits. Fig.5. shows the resulted images. The correlation and entropy results of this case are summarized in table 3 and fig.6. **Case 3**: key length: 32-byte; 256 bits. Fig.7. shows the resulted images. The correlation and entropy results of this case are summarized in table 4 and fig.8.

5. Conclusion

Image data has strong correlation among adjacent pixels. However, it is very important to disturb the high correlation among image pixels to increase the security level of the encrypted images. In this paper a simple and strong method has been proposed for image security using a combination of image permutation and encryption techniques. The cases showed that the correlation was decreased when the proposed algorithm was applied to them before the RijnDael algorithm. Experimental results showed that the process of dividing and replacing an arrangement of the original image into 4 pixels × 4 pixels blocks reduce the correlation between image elements and then achieved to confuse the relationship between the original image and the generated one. As a result, the combination technique showed that, by using the correlation, entropy, and histogram as a measure of security, this technique enhances the security level of the encrypted images by reducing the correlation among image elements, increasing its entropy value by decreasing the mutual information among the encrypted image variables (i.e. high contrast).

6. Tables, Figures and Equations

6.1 Tables and Figures

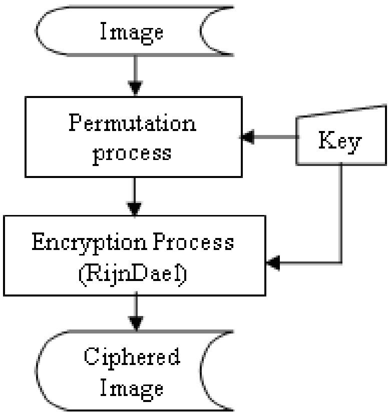


Fig. 1 General block diagram of the permutation technique

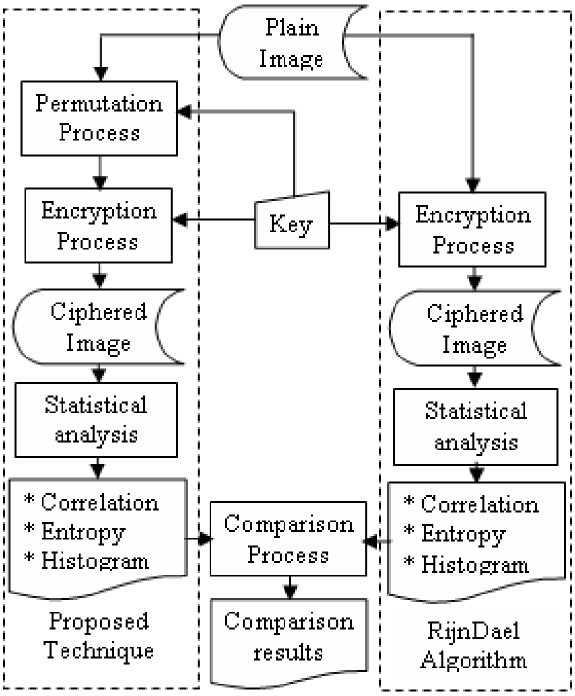
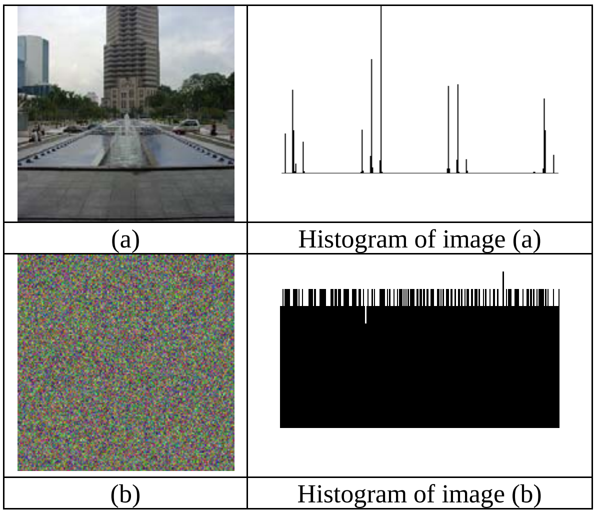


Fig. 2 A block diagram of the proposed technique versus RijnDael algorithm

Table 1 Different Cases to Test the Impact of Block size on the Correlation and Entropy

Case number	*Key length*	*Key*	*Block size*
1	8 bytes	8ualmpur	4 pixels × 4 pixels
2	16 bytes	softhma5ins9ecur	
3	32 bytes	owertyuiopasdfgh jklzxcvbnm123456	



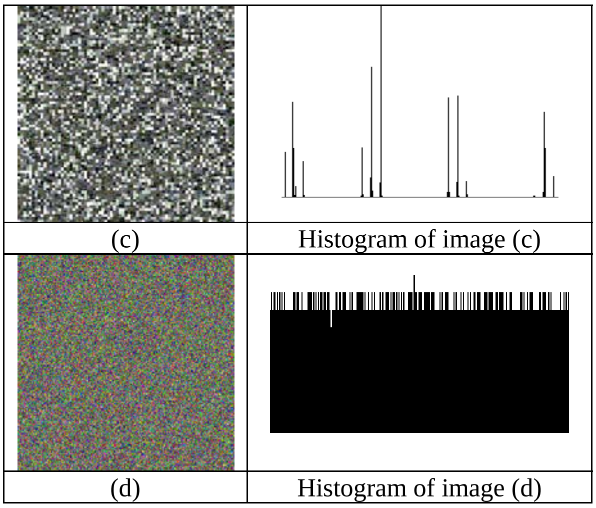


Fig. 3 Results of encryption. (a) Original image. (b) Encrypted image using RijnDael. (c) Permuted image using permutation process. (d) Encrypted image using combination technique.

Table 2 Results of correlation and entropy values of Case 1

Measurement	A	B	C	D
Correlation	0.858	0.0045	0.5714	0.0022
Entropy	2.6463	5.5436	2.6463	5.5436

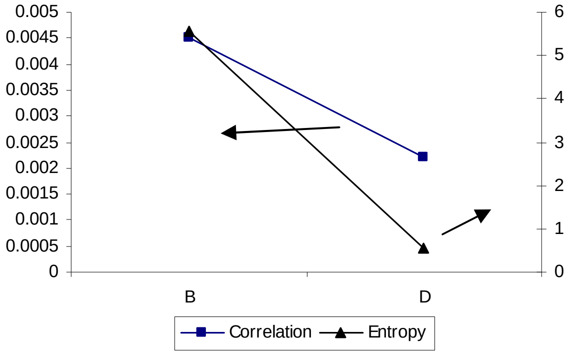
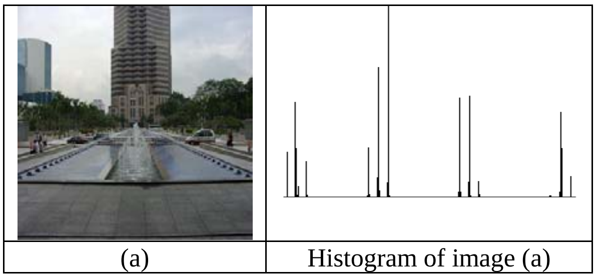
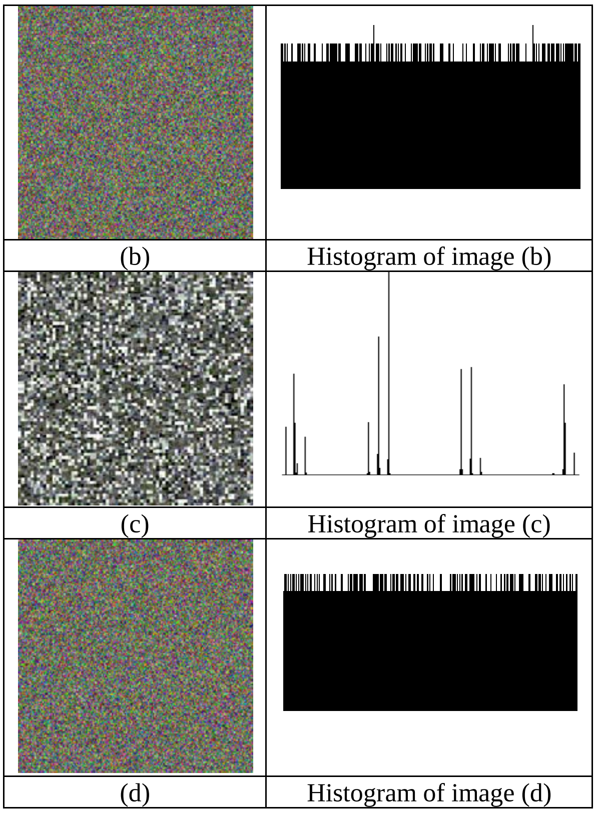


Fig. 4 Correlation and entropy values of case 1 for B and D




(b) Histogram of image (b)

(c) Histogram of image (c)

(d) Histogram of image (d)

Fig. 5 Results of encryption. (a) Original image. (b) Encrypted image using RijnDael. (c) Permuted image. (d) Encrypted image using combination technique.

Table 3 Results of correlation and entropy values of Case 2

measurement	A	B	C	D
Correlation	0.858	0.0043	0.5684	0.0029
Entropy	2.6436	5.5437	2.6463	5.5438

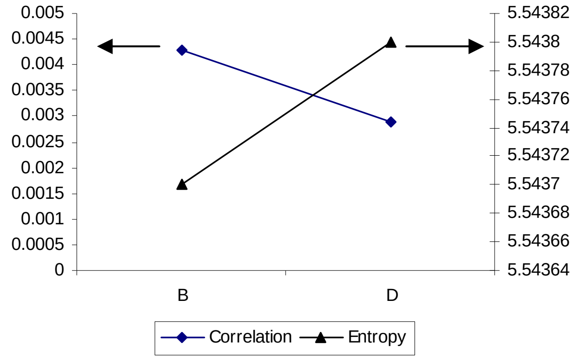
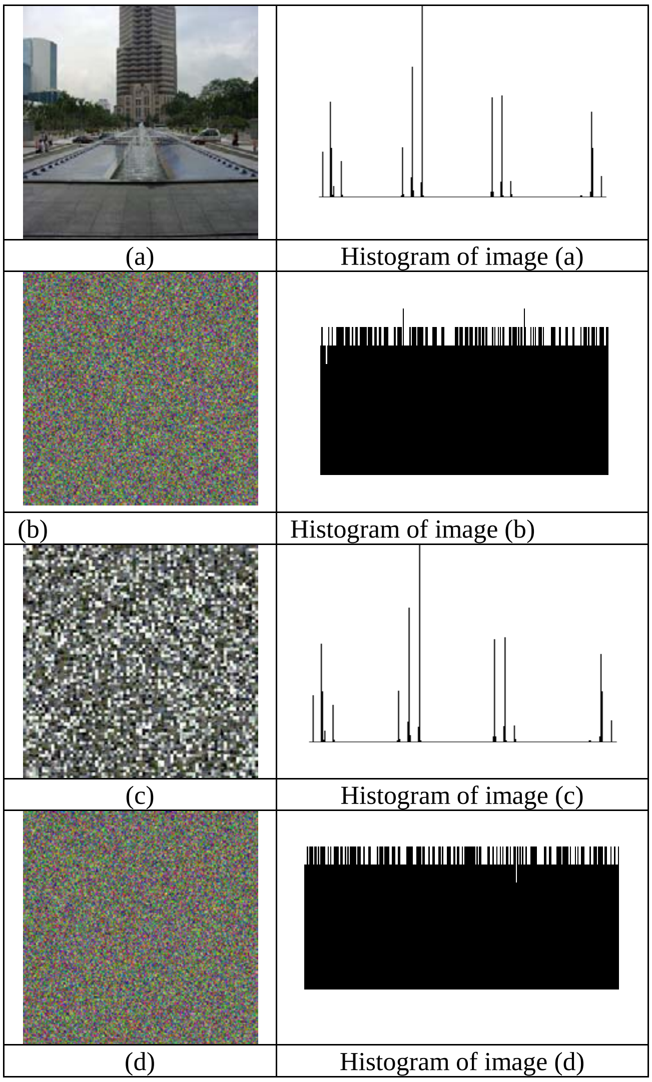


Fig. 6 Correlation and entropy values of case 2 for B and D


(a) Histogram of image (a)

(b) Histogram of image (b)

(c) Histogram of image (c)

(d) Histogram of image (d)

Fig. 7 Results of encryption. (a) Original image. (b) Encrypted image using RijnDael. (c) Permuted image. (d) Encrypted image using combination technique.

Table 4 Results of correlation and entropy values of Case 3

Measurement	A	B	C	D
Correlation	0.858	0.0018	0.6224	0.0012
Entropy	2.6463	5.5435	2.6463	5.5436

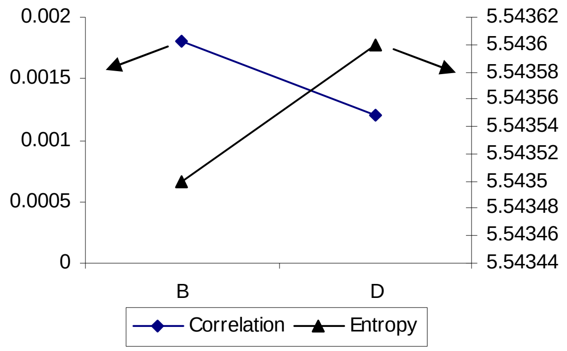


Fig. 8 Correlation and entropy values of case 3 for B and D

6.2 Equations

$$r=\frac{n\sum(xy)-\sum x\sum y}{\sqrt{\left[n\sum(x^2)-(\sum x)^2\right]\left[n\sum(y^2)-(\sum y)^2\right]}} \qquad (1)$$

Where
r: correlation value
n: the number of pairs of data
$\sum xy$: sum of the products of paired data
$\sum x$: sum of *x* data
$\sum y$: sum of *y* data
$\sum x^2$: sum of squared *x* data
$\sum y^2$: sum of squared *y* data

Entropy defined as follows [18], [19].

$$H_e = -\sum_{k=0}^{G-1} P(k)\log_2(P(k)) \qquad (1)$$

Where:
H_e: entropy.
G: gray value of input image (0... 255).
P(k): is the probability of the occurrence of symbol *k*.

References

[1] W. Lee, T. Chen and C. Chieh Lee, "Improvement of an encryption scheme for binary images," Pakistan Journal of Information and Technology. Vol. 2, no. 2, 2003, pp. 191-200, http://www.ansinet.org/

[2] A. Mitra, Y V. Subba Rao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques," Journal of computer Science, vol. 1, no. 1, 2006, p.127, http://www.enformatika.org

[3] 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).

[4] 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.

[5] M. V. Droogenbroech, R. Benedett, "Techniques for a selective encryption of uncompressed and compressed images," In ACIVS'02, Ghent, Belgium. Proceedings of Advanced Concepts for Intelligent Vision Systems, 2002.

[6] S. Fong, P.B. Ray, and S. Singh, "Improving the lightweight video encryption algorithm," proceeding of iasted international conference, single processing, pattern recognition and application, 2002, pp. 25-28.

[7] L.Wei-Bin, C. Tzung-her and L.Chen-Chieh, "Improvement of an Encryption Scheme for Binary Images," Pakistan Journal of Information and Technology. Vol. 2, no. 2, 2003, Pp. 191-200, http://www.ansinet.org/

[8] R. m. Syed, "Anew encryption algorithm for high throughput multimedia," IN: Interactive Multimedia Systems, 2002, p. 269.

[9] Y. Xun, T. H. Chik, K. S. Chee, and R. S. Mahbubur, "Fast encryption for multimedia," Consumer Electronics, IEEE Transactions on Publication Date: Feb 2001 Vol. 47, Issue: 1,2001, pp.101-107

[10] S. Changgui, B. K Bharat, "An efficient MPEG video encryption algorithm," Proceedings of the symposium on reliable distributed systems, IEEE computer society Press, 1998, pp. 381-386.

[11] 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/

[12] c. Ratael, gonzales, e. Richard, and woods, "Digital image processing," 2nd ed, Prentice hall, 2002.

[13] AL. Vitali, A. Borneo, M. Fumagalli and R. Rinaldo, "Video over IP using standard-compatible multiple description coding," Journal of Zhejiang University- Science A, vol. 7, no. 5 ,2006, pp. 668- 676.

[14] C. Harris, "ITN584 Access Control & Smart Cards," research paper, 2001.

[15] G. C. Kessler, "An Overview of Cryptography," published by Auerbach, 1998' (22 Desember 2007). http://www.garykessler.net/

[16] K. Wang , Pei , Z. Liuhua ,S. Aiguo Song, H. Zhenya, "On the security of 3D Cat map based symmetric image encryption scheme," Elsevier, Physics Letters A, Vol. 343, Issue 6, 2005, pp. 432–439.

[17] S. Han, and S. Yang, "An Asymmetric Image Encryption Based on Matrix Transformation," ecti transactions on computer and information technology vol. 1, no. 2, 2005.

[18] D. Salomon, "Data compression, Image compression," Fourth addition, Springer London, 2005, pp. 263-530.

[19] I. Ozturk, and I.Sogukpinar, "Analysis and comparison of image encryption algorithm," International Journal of Information Technology, Vol. 1, no. 2, pp. 64-67. http://www.waset.org/

[20] Li. Shujun, X. Zheng "Cryptanalysis of a chaotic image encryption method," Inst. of Image Process. Xi'an Jiaotong Univ., Shaanxi, This paper appears in: Circuits and Systems, ISCAS 2002. IEEE International Symposium on Publication Date: 2002, Vol. 2, 2002, pp. 708,711.

[21] S.S. Maniccam, N.G. Bourbakis, "Image and video encryption using SCAN patterns," Journal of Pattern Recognition Society, vol. 37, no. 4, pp.725–737, 2004.

[22] G. Zhi-Hong, H. Fangjun, and G.Wenjie, "Chaos-based image encryption algorithm," Department of Electrical and computer Engineering, University of Waterloo, ON N2L 3G1, Canada. Published by: Elsevier, 2005, pp. 153-157.

[23] A. Sinha, K. Singh, "Image encryption by using fractional Fourier transform and Jigsaw transform in image bit planes," Source: optical engineering, spie-int society optical engineering, vol. 44, no. 5 , 2005, pp.15-18

[24] S.S. Maniccam., G.Nikolaos, and Bourbakis, "Lossless image compression and encryption using SCAN," Journal of: Pattern Recognition, vol. 34, no. 6, 2001, pp.1229– 1245.

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

[26] M. Sonka, V. Hlavac. and R. Boyle, "Digital image processing," in: image Processing, Analysis, and Machine Vision, 1998, 2nd ed. http://www.pws.com

[27] D. Feldman, "A brief introduction to: information theory, excess entropy and computational mechanics," college of the atlantic 105 eden street, bar harbor, me 04609, 2002, http://hornacek.coa.edu/

Mohammad Ali Bani Younes received BSc in Computer Science from Yarmouk University in Irbid Jordan, MSc from Sudan University of Science and Technology in 1986 and 2003 respectively and currently enrolled in the PhD program in Computer Science in the Universiti Sains Malaysia.

Dr. Aman Jantan received BSc in Computer Science, Master in AI, PhD in Software Engineering from Universiti Sains Malaysia, Penang in 1993, 1996 and 2002 respectively and currently Lecturer in School of Computer Science in Universiti Sains Malaysia, Penang.