A Comprehensive Layer Based Encryption Method for Visual Data

Reza Moradi Rad, Abdolrahman Attar and Reza Ebrahimi Atani

Department of Computer Engineering, University of Guilan, Rasht, Iran
reza.moradirad@gmail.com, a.attar.q@gmail.com, rebrahimi@guilan.ac.ir

Abstract

Data encryption is a vital application to ensure security in open networks like internet. Image is widely used for various purposes and one of the most popular formats of data on the web. Different image encryption algorithms are proposed so far to generate encrypted image so that it is so difficult make prediction of pixels value by attackers. This paper proposes a new framework for image encryption, a layer based method combining some most efficient image encryption algorithms. It is tried to take all encryption concerns into consider, achieve highest possible level of security while cost is already acceptable. The proposed method provides different security level to blocks of varied significance in image to consume less computational resources. Various analysis and experiments such as histogram, correlation coefficient, entropy, and computational time revealed that significant promotion in security has been achieved without compromising on the computational time.

Keywords: *Visual cryptography, Image Encryption, Ciphering, Security Analysis*

1. Introduction

Nowadays multimedia is one of the most popular formats in data storage and transmission areas. Due to the vital role of multimedia data in digital world, the security of multimedia data is becoming more and more important. Every day huge amount of multimedia data is transmitted through the World Wide Web which poses some real security issues, such as unauthorized access. Data encryption comes to field to overcome these issues and improve the security level of digital world. Each kind of data has its own features. Different representations of information like text, voice, video and image can be individually considered for encryption using appropriate techniques basis on their inherent specific features. Text encryption has longer story than image encryption and there already exist several traditional methods for text encryption such as DES, AES, RSA and IDEA. Please note that they are not suitable for images [1, 3, 10, 13, and 16] due to some inherent differences between image and text in many aspects which listed in the rest:

- The larger size of images against texts;
- In case of image, exact reconstruction is not necessary and output of decryption is acceptable within tolerance range;
- The pixels of image are strongly correlated.

Different image encryption algorithms are proposed so far to generate encrypted image so that it is so difficult make prediction of pixels value by attackers. There are various image encryption systems to encrypt and decrypt data, and there is no single encryption algorithm satisfies the different image types. Furthermore some encryption schemas have embedded facilities into their own techniques such as compression; region based selective, independent

encryption and so on. In this paper, a novel encryption system based on some layers is proposed to enhance the encryption proficiency. It was tried to consider all concerns about visual cryptography.

Different regions of image carry different importance, for instance edge area in image has more perceivable information in comparison with smooth area in that image. Providing similar security level to data with varied significance imposes more computational cost [7]. In this paper region based selective is exploited to provide different security level for blocks of varied significance in image. Region based selective image encryption has lots of usages in time-critical applications wherein security is also a concern such as, internet banking transactions, military image database and communication and medical imaging systems [1]. The image is decomposed into unfix but predefined blocks, and then they will be classified as significant or in significant using edge detection methodology. Each of these two block groups are treated separately in encryption phase.

This paper is organized into six sections. Section 2 classifies image encryption algorithms, section 3 describes the proposed method, section 4 presents security analysis, section 5 concludes the search work, and section 6 lists references which are used to do the work.

2. Image Encryption Algorithms

To address data confidentiality, lots of approaches has been proposed so far using affine transformation, space filling curves, SCAN methodology, quad tree structure, etc. There is no single encryption algorithm satisfies users for any application and treat all different image types as well some. The papers [1, 5, 11, 13] classify all these approaches into three major groups namely, transposition techniques (position permutation), substitution techniques (value transformation), and combination of both.

Transposition techniques (position permutation): Some of the encryption methods have exploited transposition techniques to visual encryption. Transposition techniques basically rearrange individual pixels of an image so that the original concept is not visible. The chaotic based image encryption [15] proposed by Yen and Guo and also the paper [16] proposed by Mitra et al. which uses random combinational of bit, pixel, and block permutations are categorized in this class.

Substitution techniques (value transformation): Some other encryption methods have exploited substitution techniques to visual encryption. Substitution maps each element in the original (plain) image into another element. A new chaotic neural signal security system proposed by Yen and Guo [17] which changes the pixel values of the original image is categorized in this class. This algorithm depends on a one-dimensional chaotic map for generating a pseudo-random key sequence.

Combination of both: Some other approaches have combined and used both position permutation and value transformation techniques. For example, the Space Filling Algorithm is categorized in this class. It uses space-filling curves in order to pixel permutation and large period pseudo random number generators for pixel value substitution. The work [18] proposed a method that is based on permutation of pixels and substitution of the pixel values. SCAN methodology is used for permutation and a simple substitution rule, which adds confusion and diffusion properties, is used to value transformation.

3. Proposed Method

In this section a novel layer based image encryption method is proposed, it is tried to take all encryption concerns into consider. Concerns and facilities that the authors have treated are mention in the following:

- Exploit previous author's experiences to achieve lower correlation and higher entropy
- Embed region selective encryption
- Embed block independent encryption
- Propose a new permutation algorithm called PP algorithm and define BBE measure
- Provide different security level according to the block significance
- Achieve to both less processing time and more secure encryption

The proposed layer based image encryption can be decomposed into four layers, segmentation, localization, permutation, and encryption. Each of the layers is separately described in the rest.

3.1 Segmentation

This step deals with dividing the whole image into N_b number of non-overlapping blocks with variable size. Each block (region) is represented using a square matrix containing a specific number of pixels for each block size. This representative matrix is used for performing the operations on regions, each region is considered separately for encryption. Different block sizes are considered for region segmentation, block sizes defines as $B_s = 2^q$, where corresponding block is consisted of $2^q \times 2^q$ pixels where $1<q<6$. In this work four various sizes are considered for blocks of images including 4×4, 8×8, 16×16, and 32×32. Input images are predefined as a 512×512 dimensions and all four block sizes contribute same (128×128 of 512×512) to decomposition of input image. So, system will have four set of blocks, comprise of *32 blocks of 4×4, 16 blocks of 8×8, 8 blocks of 16×16,* and *4 blocks of 32×32*. The work [3] use random number of blocks while here, system will have fixed number of blocks for each image so that one of the four different sizes assigned to each block. Just as variable block size is more secure than fixed block size, having some large blocks reduce the encryption time.

3.2 Localization

Image file has distinct regions which belong to different level of importance. Recently researchers exploit this feature of image file and develop a new approach which refers as partial encryption or selective encryption. Selective Encryption makes it possible to encrypt only some regions of the image. The concept of partial or selective image encryption finds use in applications such as, internet banking transactions, military image database and communication and medical imaging systems [1]. The main advantages of selective encryption is reduction of the overhead involved in data transmission over secure channels.
Providing same security level to whole of image data which have varied significance consumes more computational resources and seems unnecessary. First we should search the image to extract the features and identify important regions of image, the work [1] just let user to mark some region as important, while the work [3] do this automatically using prewitt edge detector. In this paper, two ways considered for identification of significant regions, Firs, it can be done automatically by system, and second, manually by user.

The Edge property of an image plays a critical role its representation concept. An efficient encryption technique should be able to perturb edges shape and location to stand firm against various attacks. We decide to use Prewitt edge detection technique as in [3], for three reasons, first it is accurate, second it has easily implemented, and third it imposes low computational costs.

3.3 Permutation

Region permutation deals with interweaving the blocks of the image to build a newly transformed image. The perceivable information of an image is highly depended on the correlation among the image elements in a given arrangement. Decreasing the correlation among the image elements using certain permutation techniques can makes it so hard to understand. Furthermore, the process of dividing and shuffling the positions of image blocks will makes difficult to predict the value of any given pixel from the values of its neighbors in other hand, it confuses the relationship between the original image and the generated one. Various permutation algorithms are exploited by [1] including, RC Permutation, Z-Permutation, Random Sequence, and Chaotic Reordering. The work [19] have pointed out that all permutation-only image encryption are vulnerable to attacks. As a conclusion, they suggested that permutations have to be combined with other encryption techniques to design strongly secured images. In this paper, a new simple and efficient algorithm is designed by the authors to permutation of image blocks. We called it perspicacious permutation (PP) here, because this simple algorithm has a strategy exactly knowing where the current block should replace in. This algorithm calculates a measure value for each block. The PP algorithm efficiently permutes blocks with the help of Block Background Estimation (BBE) measure. BBE is the average of pixel intensity value for all pixels of the block. This algorithm simply acts in such way that minimizes the correlation in permuted image. For instance if BBE of the current block got 46, it will substitute with a block BBE most near as possible to 209 (255-46). Figure 4 shows how PP algorithm affects on the image.

3.4 Encryption

As mentioned before in the second layer (localization), blocks are classified into insignificant or significant category. Binary significant vector of size $1 \times N_b$ is generated, so that element '0' indicate the corresponding block is insignificant, and '1' indicate the corresponding block is significant. Two procedures are designed to treat with blocks according to whether it is classified as insignificant or significant. Each insignificant block which is included less important information will encrypt using rescanning; a less complex methodology which introduced in [5, 9, 12]. Each significant block which has high potential to include critical information will encrypt using one of the algorithms in golden set. This is also illustrated with the help of a block diagram in Figure 1.

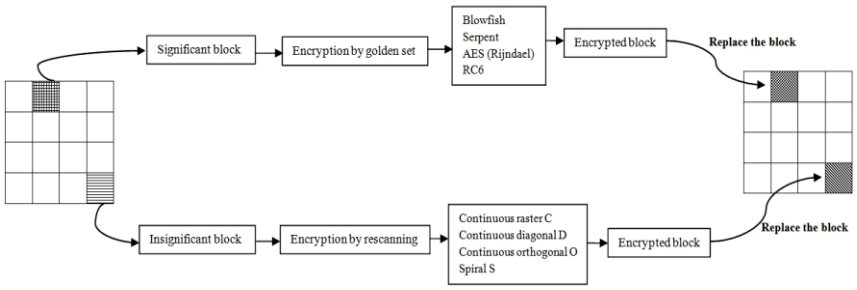

Figure 1. Block Diagram for Encryption Process

3.4.1 Procedure One, Rescan

The SCAN is a language based two dimensional spatial accessing methodology which can efficiently specify and generate a wide range of scanning paths. Scan based image encryption is based on rearrangement of the pixels of the image. Scanning path of an image is simply an order to access sequentially or process the n×n pixels of the image exactly once, an n×n array has (n×n)! scanning paths. Some kinds of scan based methods are described so far [5, 9, and 12]. In this method each block of images is rearranged by various scan patterns that generated by the SCAN methodology.

SCAN language uses four basic scan patterns, in this paper these four patterns are exploited to encrypt insignificant blocks, including continuous raster C, continuous diagonal D, continuous orthogonal O, and spiral S, as shown in Figure 2 respectively from left to right.

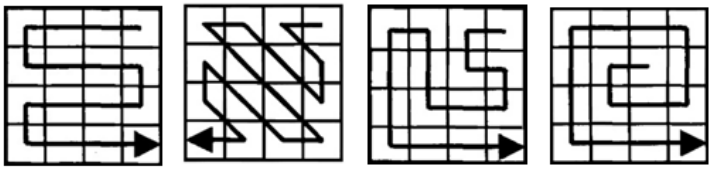

Figure 2. Four Basic Patterns for Rescanning

3.4.2 Procedure Two, Golden Set

In order to transmit secret images to other people, a variety of encryption schemes have been proposed. The majority of the encryption algorithms in use today are block algorithms, which operate on one block, stream and hash are some other kinds of encryption algorithms. Among all the algorithms addressed image encryption, there are some more efficient ones mainly used in the papers [1, 3, 4, 10, and 11]. In this paper these four various methods such as Blowfish, Serpent, AES (Rijndael), and RC6 comprise our golden set to encrypt significant blocks. AES (Rijndael), Serpent, and RC6 also ranked in four best encryption algorithms for AES nomination. The golden set methods work in combination to provide the most possible security for significant blocks.

Blowfish: Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms [20]. It is gradually recognized as a strong encryption algorithm. Blowfish combines a Feistel network, key-dependent S-Boxes, and a non-invertible F function to create what is perhaps one of the most secure algorithms so far. The only known attacks against Blowfish are based on its weak key classes.

Rijndael (AES): The block cipher Rijndael was designed by Joan Daemen and Vincent Rijmen [22]. The cipher has a variable block and key length and it is very secure and has no known weaknesses. According to The Rijndael web page, name of the algorithm is a combination of the names of its two creators, 'Daemen' and 'Rijmen'". The algorithm can be implemented very efficiently on a wide range of processors and in hardware. The National Institute of Standards and Technology (http://www.nist.gov) has recently selected the algorithm as an Advanced Encryption Standard (AES).

RC6: RC6 block cipher was designed by Ron Rivest in collaboration with Matt Robshaw, Ray Sidney, and Yiqun Lisa Yin from RSA Laboratories [23]. It can accept variable length keys. It is very similar to RC5, incorporating the results of various studies on RC5 to improve the algorithm. The studies of RC5 found that not all bits of data are used to determine the

rotation amount (rotation is used extensively in RC5); RC6 uses multiplication to determine the rotation amount and uses all bits of input data to determine the rotation amount, strengthening the avalanche effect.

Serpent: Serpent was designed by Ross Anderson, Eli Biham and Lars Knudsen [21], Serpent is faster than DES and more secure than Triple DES. Its authors combined the design principles of DES with the recent development of bit-slicing techniques to create a very secure and very fast algorithm. Serpent used bit-slicing to encrypt multiple blocks in parallel and also can work with different combinations of key lengths. The algorithm's designers limited themselves to well understood cryptography mechanisms, so that they could rely on the wide experience and proven techniques of block cipher cryptanalysis. Figure 3 depicts the proposed method layers relationship and functions at a glance.

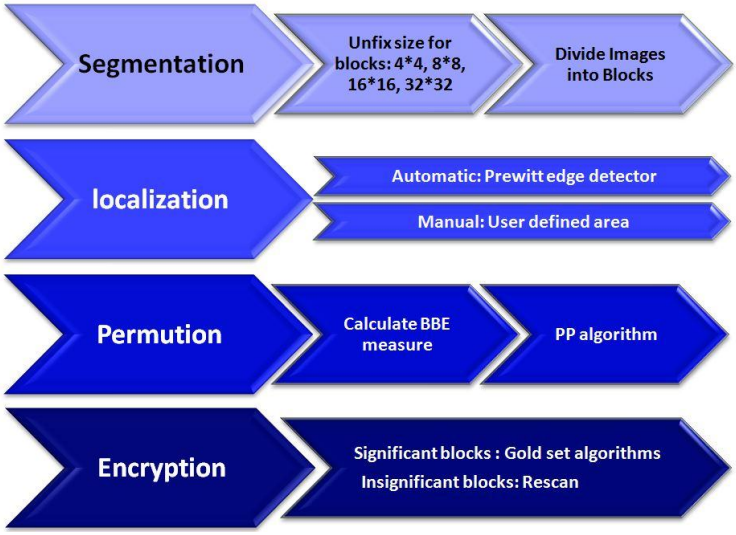

Figure 3. Proposed Method from the Point of View of Layers

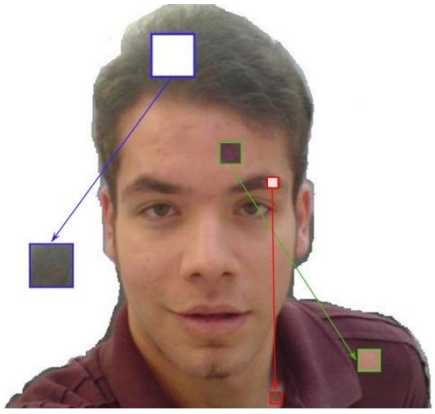

Figure 4. Proposed Method

4. Security Analysis

An efficient encryption procedure should be unbeatable against all kinds of cryptanalytic, brute-force and statistical attacks. In this work, several tests have done to check the proficiency of the proposed method.

4.1 Histogram Analysis

Image histogram is one of the most important features in an image and one of the most well-known tests on image encryption area. From Figure 5 it is obvious that the histograms of the encrypted image are fairly uniform and significantly different from the respective histograms of the original image. Hence it does not provide any clue to employ any statistical analysis attack on the encryption image. In the original image (*i.e.*, plain image), some gray-scale values in the range [0, 255] are still not existed, but every gray-scale values in the range [0, 255] are existed and uniformly distributed in the encrypted image.

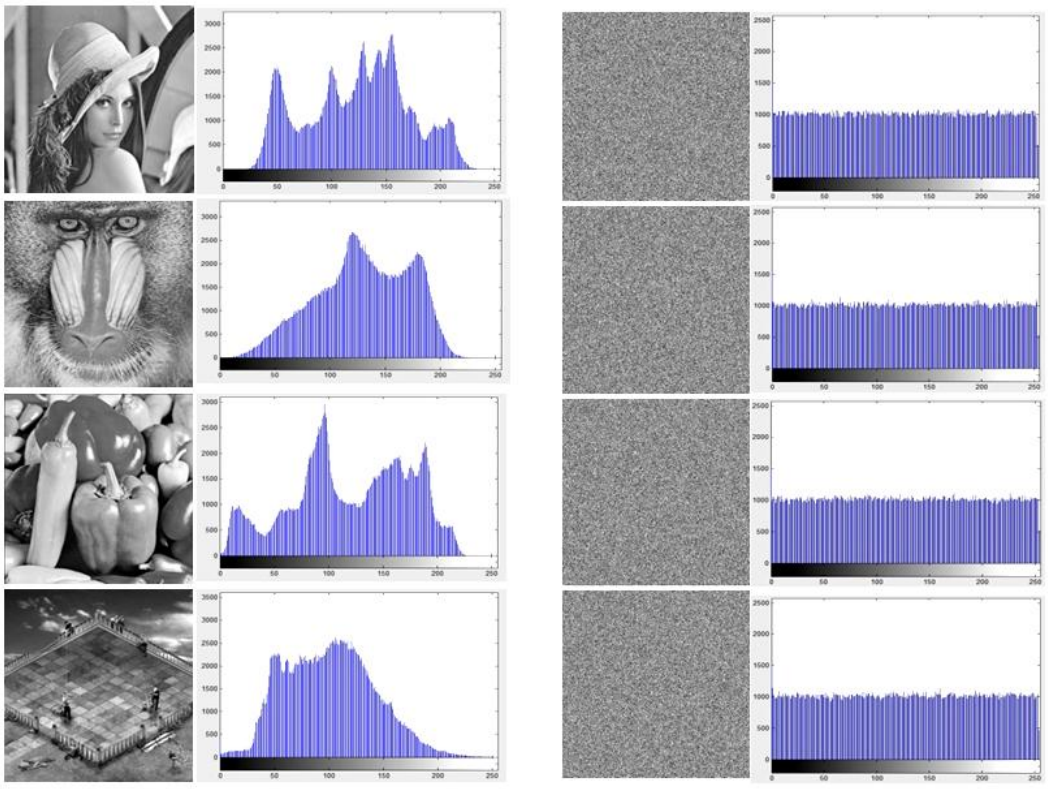

Figure 5. Histogram Analysis for Original and Encrypted Images

4.2 Correlation Coefficient

Correlation is a measure of the relationship between two adjacent pixels. In the case of original image (plain message), pixels are strongly correlated, while in encrypted one, it is tried to keep correlation among pixels at minimum level. We have analyzed the correlation between two vertically adjacent pixels, two horizontally adjacent pixels, and two diagonally

adjacent pixels in an image. 1500 pairs of two adjacent (in vertical, horizontal, and diagonal direction) pixels from original image and encrypted image were randomly selected and the correlation coefficients were calculated by using the following equations:

$$r_{xy} = \frac{Cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{1}$$

Where x, y are grey scale values of two adjacent pixels in the image. In numerical computation, the following formulas were used:

$$E(x) = \frac{1}{n}\sum_{i=1}^{n} x_i\,, \qquad D(x) = \frac{1}{n}\sum_{i=1}^{n}(x_i - E(x))^2 \tag{2}$$

$$Cov(x,y) = \frac{1}{n}\sum_{i=1}^{n}(x_i - E(x))(y_i - D(x)) \tag{3}$$

The obtained correlation coefficient for the original image and its encrypted counterpart are shown in Table 1. Low correlation coefficient value and distributed correlation plot (Figure 6) for an encrypted image has been obtained as opposed to high correlation value and concentrated correlation plot of original image. This ascertains no information leakage from the encrypted image.

Table 1. Correlation Coefficient for Two Adjacent Pixels in Various Directions

Sample Image		Horizontal	Vertical	Diagonal
Lena	Original	0.9281	0.9115	0.8847
	Encrypted	-0.0138	-0.0029	0.0017
Baboon	Original	0.8714	0.8921	0.8754
	Encrypted	0.0021	0.0023	0.0097
Pepper	Original	0.9458	0.9621	0.9415
	Encrypted	-0.0139	0.0207	-0.0233
Escher painting	Original	0.8454	0.7548	0.8121
	Encrypted	0.0055	0.0062	0.0027

If the correlation coefficient equals one, that indicates the original image is same as its encryption. If the correlation coefficient equals zero, that means the encrypted image is completely different from the original which is best scenario in encryption. If the correlation coefficient equals minus one that means the encrypted image is the negative of the original image.

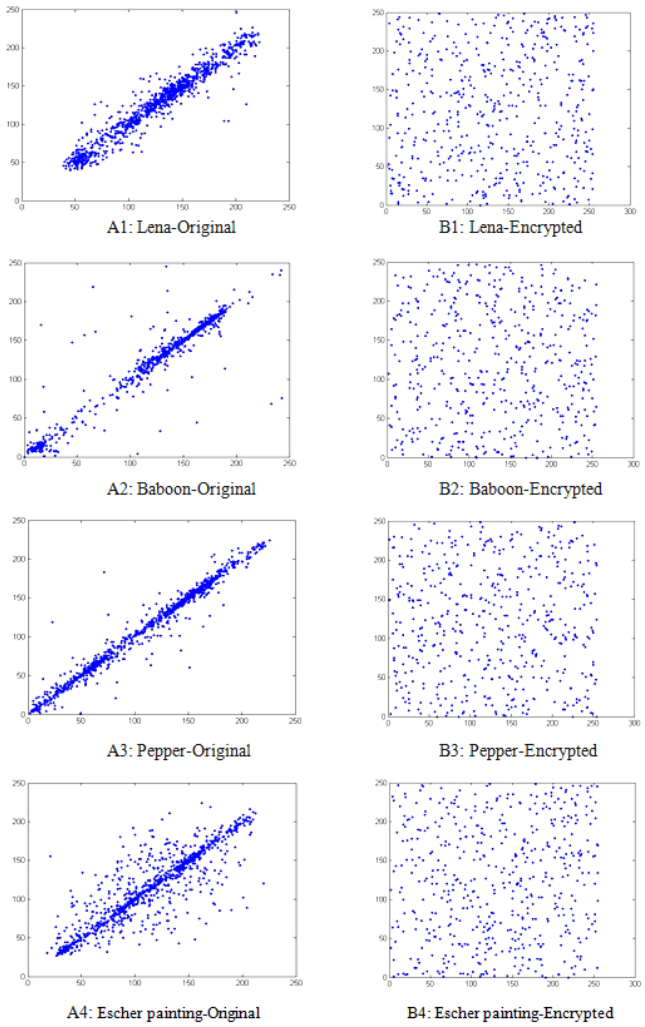

Figure 6. Correlation Analyses for A) Original and B) Encrypted Images

4.3 Image Entropy

It is well known that entropy is a quantity measure which is used to describe the `business' of an image. As for grayscale image in Block Based Image Encryption decreases the mutual information among encrypted image variables and consequently increases the entropy value. A secure encryption should provide a situation which the encrypted image is not provide any information about the original image. On the other hand, high entropy images such as an image of heavily cratered areas on the moon have a great deal of contrast from one pixel to the next and consequently cannot be compressed as much as low entropy images. Entropy H= 8 indicates that each symbol has an equal probability. The information entropy is calculated using equation 4 and is depicted in Table 2.

$$H = -\sum_{i=1}^{n} p_i \times log_2 p_i \quad (4)$$

H: Entropy of image
N: Gray level of an input image (0-255)
Pi: Probability of the occurrence of symbol i

Table 2. Entropy Analysis for Original and Encrypted Images

Sample Image		Type/Size	Entropy Value
Lena	Original	Jpeg/512×512	7.4853
	Encrypted	Jpeg/512×512	7.9522
Baboon	Original	Jpeg/512×512	7.5894
	Encrypted	Jpeg/512×512	7.9751
Pepper	Original	Jpeg/512×512	7.4541
	Encrypted	Jpeg/512×512	7.9689
Escher painting	Original	Jpeg/512×512	7.6674
	Encrypted	Jpeg/512×512	7.9886

4.4 Time Analysis

As the last test to prove proficiency of the proposed algorithm, in this section time performance simulation of the proposed encryption algorithm is provided. The time performance simulation is done by computer system with following specifications: MATLAB 8.0 under Microsoft Windows 7 Home Premium version 2009 on, Intel(R) Core(TM) i7 CPU 1.73GHz, 4 GB of RAM, and 300 GB hard-disk capacity (Laptop computer). The test is applied on four selected jpeg images; each image is 512 × 512 pixels in size. The main interest lies in the 24 bit uncompressed RGB color mode, and 8 bits per pixel (bpp), or 256 intensity levels. The time analysis details are shown in Table 3.

Table 3. Time Analysis for Original and Encrypted Images

Sample Image	**Type/Size**	**Encryption Time**	**Decryption Time**
Lena	Jpeg/512×512	0.1954 sec	0.1819 sec
Baboon	Jpeg/512×512	0.2089 sec	0.2014 sec
Pepper	Jpeg/512×512	0.1521 sec	0.1497 sec
Escher painting	Jpeg/512×512	0.2367 sec	0.2372 sec

5. Conclusion

This paper proposed a new framework for image encryption, a layer based method combining some most efficient image encryption algorithms. This layer based method is comprised of four layers, segmentation, localization, permutation, and encryption. Author's innovations are applied in all the layers. In localization all blocks briefly are processed and identified as significant and in significant. In permutation layer which PP algorithm is designed to shuffle blocks using BBE measure. In encryption layer various security levels is provided according to importance of the block using combination strategy. It is tried to take all encryption concerns into consider. The proposed method provides different security level to blocks of varied significance in image to consume less computational resources. Various analysis and experiments such as histogram, correlation coefficient, entropy, and computational time revealed that significant promotion in security has been achieved without compromising on the computational time.

References

[1] K. C. Ravishankar and M. G. Venkateshmurthy, "Region based selective image encryption Region based selective image encryption", International Conference on Computing and Informatic (ICOCI'06), Kuala Lumpur, Malaysia, **(2006)** June.
[2] S. F. El-Zoghdy, Y. A. Nada and A. A. Abdo "How Good Is The DES Algorithm In Image Ciphering?", International Journal of Advanced Networking and Applications, vol. 1, Issue 7, **(2011)**.
[3] M. A. B. Younes and A. Jantan, "Image Encryption Using Block-Based Transformation Algorithm", IAENG, International Journal of Computer Science, vol. 35, no. 1, **(2008)** February.
[4] A. Gautam, M. Panwar and P. R. Gupta, "A New Image Encryption Approach Using Block Based Transformation Algorithm", IJAEST, International Journal of Advanced Engineering Sciences and Technologies, **(2011)**.
[5] C. S. Chen and R. J. Chen, "Image Encryption and Decryption Using SCAN Methodology", Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06), Taipei, Taiwan, **(2006)** December.
[6] M. S. Azzaz, C. Tanougast, S. Sadoudi and A. Dandache, "Robust chaotic key stream generator for real-time images encryption", Real-Time Image Processing Journal, **(2010)** August.
[7] N. Taneja, B. Raman and I. Gupta, "Combinational domain encryption for still visual data", Journal of Multimedia Tools and Applications, **(2011)** March.
[8] R. Pfarrhofer and A. Uhl, "Selective Image Encryption Using JBIG", Conference on Communications and Multimedia Security, **(2005)**, pp. 98-107.
[9] S. S. Maniccam and N. G. Bourbakis, "SCAN Based Lossless Image Compression and Encryption", International Conference on Information Intelligence and Systems, **(1999)**.
[10] M. A. B. Younes and A. Jantan, "An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption", IJCSNS International Journal of Computer Science and Network Security, vol. 8, no. 4, **(2008)** April.
[11] M. A. El-Wahed, S. Mesbah and A. Shoukry, "Efficiency and Security of Some Image Encryption Algorithms", World Congress on Engineering 2008, vol. 1, WCE 2008, London, UK, **(2008)** July.
[12] N. Bourbakis, "Image Data Compression Encryption using G-SCAN Patterns", IEEE Conference on SMC, Orlando, Florida, USA, **(1997)** October, pp. 1117–1120.
[13] I. Ozturk and A. Sogukpinar, "Analysis and Comparison of Image Encryption Algorithms", World Academy of Science, Engineering and Technology, **(2005)**.
[14] M. A. Bani Younes and A. Jantan, "A New Steganography Approach for Image Encryption Exchange by Using the Least Significant Bit Insertion", IJCSNS International Journal of Computer Science and Network Security, vol. 8, no. 6, **(2008)** June.
[15] J. -C. Yen and J. -I. Guo, "A New Chaotic Image Encryption Algorithm", IEEE International Conference Circuits and Systems, vol. 4, **(2000)**, pp. 49-52.
[16] A. Mitra, Y. V. Subba Rao and S. R. M. Prasanna, "A new image encryption approach using combinational permutation techniques", International Journal of Computer Science, vol. 1, no. 2 , **(2006)**, pp. 1306-4428.
[17] C. Yen and I. Guo, "The Design and Realization of a Chaotic Neural Signal Security System", Pattern Recognition and Image Analysis, vol. 12, no. 1, **(2002)**, pp. 70-79.
[18] S. S. Maniccama and N. G. Bourbakisa, "Image and video encryption using SCAN patterns", Pattern Recognition, vol. 37, **(2004)**, pp. 725 – 737.
[19] S. Li, C. Li, G. Chen, N. G. Bourbakis and K. T. Lo, "A general cryptanalysis of permutation-only multimedia encryption algorithms", Cryptology ePrint Archive, Report 2004/374, **(2004)**, http://eprint.iacr.org/2004/374.
[20] B. Schneier, "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)", Cambridge Security Workshop on Fast Software Encryption, Cambridge, UK, **(1993)** December, pp. 191-204.
[21] R. J. Anderson, E. Biham and L. R. Knudsen, "Serpent: A Proposal for the Advanced Encryption Standard", submitted to NIST as an AES candidate. A short version of the paper appeared at the AES conference, **(1998)** August, http://www.cl.cam.ac.uk/~rja14/serpent.html.
[22] J. Daemen and V. Rijmen, "The Design of Rijndael, AES - The Advanced Encryption Standard", Springer-Verlag, **(2002)**.
[23] R. Rivest, M. Robshaw, R. Sidney and Y. Yin, "ThenRC6[TM] Block Cipher", NIST AES Proposal, **(1998)** June, http://csrc.nist.gov/encryption/aes/round2/AESAlgs/RC6/cipher.pdf.
[24] A. Pommer and A. Uhl, "Selective Encryption of Waveletpacket Encoded Image Data: Efficiency and Security", Multimedia Systems, vol. 9, no. 3, **(2003)**, pp. 279–287.
[25] D. Socek, H. Kalva, S. S. Magliveras, O. Marques, D. Culibrk and B. Furht, "New Approaches to Encryption and Steganography for Digital Videos", Springer ACM Multimedia Systems Journal, vol. 13, no. 3, **(2007)**, pp. 191-204.

Authors

Reza Moradi Rad

He was born in Rasht, Iran. He began his journey through life on September 12, 1989. He graduated from Kharazmi high school of Rasht and awarded the diploma in Mathematics and Physics in 2006. In 2007, he started to study computer engineering in University of Guilan, the largest and most prestige university in north of Iran. Currently he is in his last semester of B.Sc. studies and throughout his final research project, he is working on image processing, machine vision, and pattern recognition. He has published more than 12 journal and conference papers so far.

Abdolrahman Attar Qazaani

He was born in Tehran, Iran. He began his journey through life on September 16, 1989. He graduated from Kharazmi high school of Rasht and awarded the diploma in Mathematics and Physics in 2006. In 2007, he started to study computer engineering in University of Guilan, the largest and most prestige university in north of Iran. Currently he is in his last semester of B.Sc. studies and throughout his final research project, he is working on image processing, machine vision, and pattern recognition. He has published more than 12 journal and conference papers so far.

Reza Ebrahimi Atani

He was born in 1980. He received the B.S. degree in electrical engineering from the University of Guilan in 2002 and the M.Sc and PhD degrees in electronics from Iran University of Science and Technology in 2004 and 2010 respectively. He has been a faculty member of the Computer Engineering Department at the University of Guilan, Rasht, since 2010. His current research interests include the design and implementation of cryptographic algorithms, Image Processing and design of VLSI circuits. Dr. Atani is a member of IEEE and IACR and a Chartered Engineer (Email: rebrahimi@guilan.ac.ir).