Analysis of Pixel Merging for Multi Image Integration for Security Enhancement

A. D. Senthil Kumar
Department of Instrumentation Engg
Annamalai University
Chidambaram, India

T. S. Anandhi
Department of Instrumentation Engg
Annamalai University
Chidambaram, India

Ranganath Muthu
Department of EEE
SSN College of Engineering
Kalavakkam (near Chennai), India

ABSTRACT

This paper focus on image security based on compressing the image with encryption and pixel integration. This process involves applying Joint Photographic Experts Group compression for RGB layers, encrypting the images with Elliptic Curve Encryption Algorithm and block based interleaving followed by pixel based integration technique. With the key specifically generated for the image, the original image is decrypted from multiple images. This method is useful when access permissions needs to be restricted to certain viewers. The proposed method provides a high-level security in the fields of aerospace, national security, military, financial and economic, and so on. Performance is evaluated by calculating the correlation coefficient and entropy values.

Keywords

Encryption; Pixel Integration; Elliptic Curve Encryption Algorithm; Digital Communication; Image Interleaving; Image Processing

1. INTRODUCTION

Digital image is a description of a real-world natural or a visual scene, which sampled temporally and spatially, whereas video coding is compression and decompression process. Image or video transmission requires compression to decrease the quantity of data for fast and secure transmission and encryption is used to protect the use of data against unauthorized access.

With the advancement in multimedia technology many defense sectors across the globe are using images and videos to train newly recruited troops. Such confidential data must be secured in transmission or storage. One possible way to protect multimedia information is to restrict unauthorized access, with this approach cannot make sure that the multimedia information is physically secure. Another easy security approach is to encrypt the complete data with a cryptographic algorithm, such as Advanced Encryption Standard or Data Encryption Standard. Generally, multimedia possesses a large volume of data and require real-time operations. With the enhancement in wireless mobile systems and limited processing power, memory, and bandwidth, and is rarely able to handle the heavy encryption processing load. Therefore, taking into consideration the specific characteristics for resource-limited systems, new encryption algorithms need to be developed.

For real- world applications, an encryption algorithm must consider various parameters like security, computational efficiency, compression efficiency and so on. Different types of applications require different levels of security. For example, for military purposes or financial information, high level of security is required to completely prevent unauthorized access., whereas for video on demand, low security will be fine. Computational efficiency means that the encryption or decryption process should not cause too much time delay, so that the requirements of real-time applications are met. Compression is employed to reduce the storage space and save bandwidth, so that the encryption process should have the least impact on the compression efficiency. Overall, a well-designed encryption algorithm should provide sufficient security, high computational efficiency imposes little impact on the compression efficiency.

Advanced digital technologies and growth of computer networks, a huge amount of digital data is being transferred over various types of networks. A large part digital data of this information is either private or confidential. Most of the security algorithms specifically designed to encrypt digital data are proposed in the mid-1990s. Different algorithms can do encryption and decryption of images. There are two groups of cryptography [16] image encryption algorithms: (a) Non-chaos selective methods and (b) Chaos-based [5], [19] selective or non-selective methods. It can be admitting, no encryption algorithm which satisfies all image type requirements [6]. An Encryption Algorithm should be strong against all types of attacks, including statistical and brute force attacks. Different security algorithms [3] have been used to provide the required protection and many encryption algorithms have been proposed to enhance the image security.

The process of image encryption [1], [2] is to convert an image to another format that is hard to understand. The reverse process is on other hand that retrieves original image is by decryption. The transformation of information in secure manner is based on encryption.

In this paper, we presented, image integration method to enhance security. In our proposed method, nine input images with an image size of m*m pixels are taken for integration with block size of 4*4 is applied to test the performance. The JPEG Compression, Interleaving with Pixel based Integration and the Elliptic Curve Cryptography [12] algorithm is used on the number of images to generate encrypted image, decryption process is done by selection of the key. The entropy and correlation of the encrypted images are calculated and evaluated.

To increase the image entropy value and to decrease the high correlation among pixels, and thus an improved security level of the encrypted images. We propose JPEG compression which done to all input images in RGB layers format individually and applying ECC encryption algorithm. Then interleaving the columns and rows of the image using the pixel based technique for image merging. The interleaving process will be used to split (divide) the original image into several blocks that are then shifted through the columns and the rows within the image before the process starts. Finally, Multi Image integrated image is generated.

2. RELATED WORK

Ahmed Bashir Abugharsa et al. [8] proposed an encryption algorithm based on the rotation of the faces of a Magic Cube. This process involves dividing the original image into six sub-images and further these sub images are divided into small blocks and attached to the faces of magic cubes.

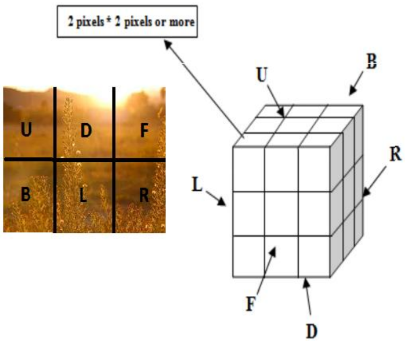


Fig. 1. Six sub-images on the magic cube faces using Mapping

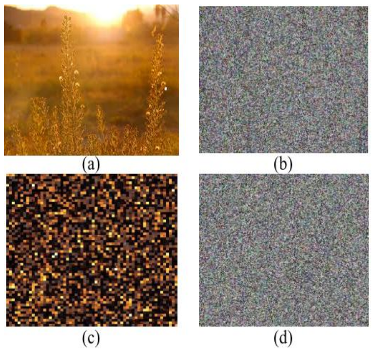


Fig. 2. (a) Input Original Image. (b) AES Encrypted image (c) Rotation image. (d) Integration Technique Encrypted Image

Table I Entropy and Correlation Value of Two Pixels for Image Divide into 3*3 Pixels

Correlation Analysis				Entropy Value
Horizontal	***Vertical***	***Diagonal***	***Anti-Diagonal***	
0.9951	0.99355	0.9917	0.9914	7.0443
-0.0444	-0.0476	-0.0208	-0.0317	7.9256
0.5220	0.5887	0.3820	0.3898	7.1766
-0.0449	-0.0520	-0.0433	-0.0388	7.9448

Mitra A et al. [9] have proposed image encryption using a combination of different permutation techniques.

Guiliang Zhu et al. [11] proposed image encryption algorithm based on pixels by applying ECC. Scrambling the image pixels, through the method of watermark. Camouflaged image to vision or the pixels of the true image, getting the final encryption image.

Laiphrakpam Dolendro Singh et al. [12] proposed an image encryption using Elliptic Curve Cryptography based on pixel grouping to reduce the number of computation. The group of pixels are transformed into big integer, these big integer values are paired and given as input in ECC operation. This operation helps us to ignore the mapping operation and the need to share mapping table between sender and receiver.

Sinha A et al. [14] proposed a new technique for image encryption and decryption in which the image is broken up into bit planes by approaching a method to jigsaw the image in which every block is trans-located to a different location of the three-dimensional cube. This increases the robustness of the encryption system by several orders of magnitude.

Zhi-Hong Guan et al. [19] proposed encryption scheme based on position shuffling and changing the image pixel grey values are combined to confuse the relationship between the plain-image and the cipher-image.

Rogelio Hasimoto Beltran et al. [13] proposed interleaving scheme where the de-correlation process is applied to co-efficient or pixel level in the compressed domain.

Frank Dellaert et al. [15] proposed image-based tracking algorithm, which relies on the selective integration of a small subset of pixels that contain a lot of information about the state variables to be estimated.

3. PROPOSED METHOD

3.1 JPEG Compression

JPEG image frame consists of three 2-D patterns of pixels, one for luminance and two for chrominance. Because high-frequency color information is less sensitive to human eye, JPEG calls for the coding of chrominance (color) information at a reduced resolution compared to the luminance (brightness) information.

The input images are layered as RGB.JPEG compression is applied to all image layers individually for better performance. The JPEG image compression technique consists of 5 functional stages.

1. RGB image is converted to YCC color space,

2. A spatial subsampling of the chrominance channels in YCC space,

3. Using discrete cosine transform(DCT) transformation of a blocked representation of the YCC spatial image data to a frequency domain representation.

4.Quantization of the blocked frequency domain data per a user-defined quality factor, and finally

5. Huffman coding for storage of frequency domain data.

3.2 Eliptic Curve Cryptograpy

Elliptical curve cryptography (ECC) [3] function is based on public key encryption technique based on elliptic curve theory that can be used to create efficient cryptographic keys which is smaller and faster. Key generated through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers.

3.2.1 Image Encryption

The encryption procedure is based on encrypting the image intensity and thus converting it into a new intensity. This new intensity is decrypted to obtain the original intensity.

1. Read the image and find the intensity I from the image intensity matrix.
2. Convert the intensity of the image I into an elliptic curve point E using Mapping-1.

3. Elliptic curve point from Mapping-1 Encrypted to a new point(E').
4. The new point (E') is converted to a corresponding integer M, using Mapping-2.
5. This integer M is used to calculate the new encrypted intensity I.

3.2.2 Image Decryption

1. The decryption is done by reverse process of encryption.
2. The encrypted image intensity I' is read from the received files.
3. The intensity I parameter is to calculate the integer M.
4. Integer M is converted to encrypted elliptic curve point E', using reverse mapping-2.
5. The encrypted elliptic curve point E' is decrypted to get the original point E.
6. By reverse mapping-1, the original intensity I is obtained.

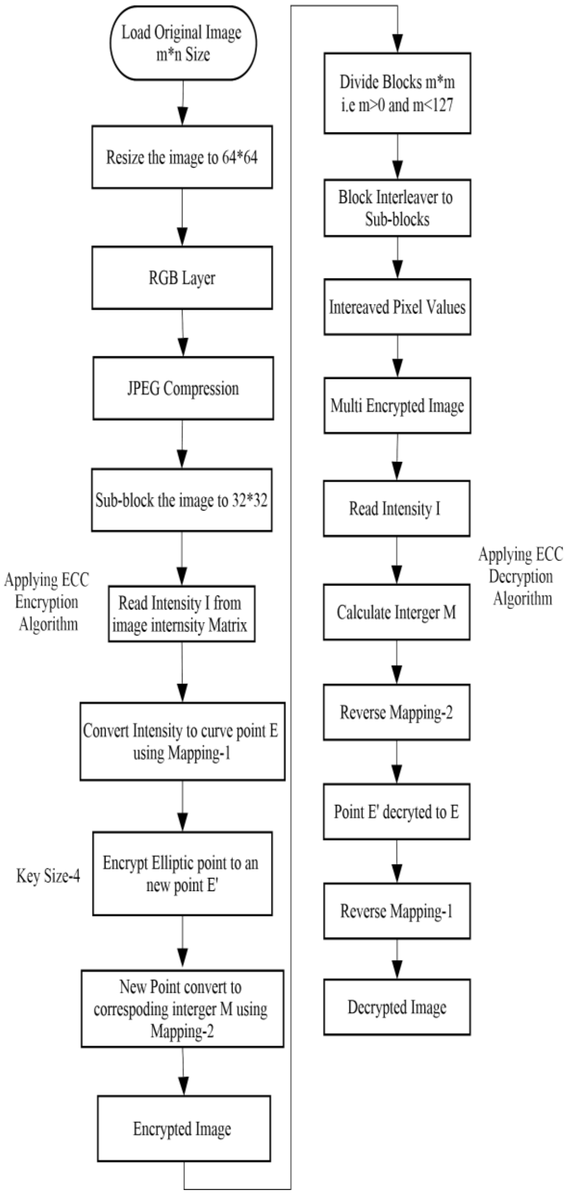

Load Original Image m*n Size
Resize the image to 64*64
RGB Layer
JPEG Compression
Sub-block the image to 32*32
Applying ECC Encryption Algorithm
Read Intensity I from image internsity Matrix
Convert Intensity to curve point E using Mapping-1
Key Size-4
Encrypt Elliptic point to an new point E'
New Point convert to correspoding interger M using Mapping-2
Encrypted Image
Divide Blocks m*m i.e m>0 and m<127
Block Interleaver to Sub-blocks
Intereaved Pixel Values
Multi Encrypted Image
Read Intensity I
Applying ECC Decryption Algorithm
Calculate Interger M
Reverse Mapping-2
Point E' decryted to E
Reverse Mapping-1
Decrypted Image

Fig. 3. Design Flow

3.3 Interleaved Image Signal Processing

For better encryption, the input images are divided small blocks [7], [8] as 4*4. These sub-block images are interleaved column wise. The number of sub-block pixel values in each block is fixed for a given interleaver [10]. The interleaver operation on a set of image pixel values is independent of its operation on all other sets of symbols Applying block based interleaving by selecting the initial location randomly.

Firstly, we divide the interleaving scheme into column-wise interleaving and row-wise interleaving randomly. Secondly, we assign the value of seed as column-wise seed and row-wise seed to column-wise interleaver and row-wise respectively. Therefore, the location of bits after interleaving will be as follows.

Row-wise	**Column-wise**
1-1	1-1
2-$(1+p_{row})$ mod n_r	2-$(1+p_{col})$ mod n_c
3-$(1+2p_{row})$ mod n_r	3-$(1+2p_{col})$ mod n_c
n_r-$(1+(n_r-1)\ p_{row})$	nc-$(1+(n_c-1)\ p_{col})$

Where p_{row} and p_{col} are row-wise and column-wise seeds. After we get the new location of bits after interleaving on both row-wise and column-wise, the new locations are mapped back into 2D interleaver to get the resulted interleaved bits in 2D.

A1	A2	B1	B2
A3	A4	B3	B4
C1	C2	D1	D2
C3	C4	D3	D4

(a)

A1	C1	A2	C2
D1	B1	D2	B2
A3	C3	A4	C4
D3	B3	D4	B4

(b)

Fig. 4. (a)Input Sequence block interleaver (b) Arrangements of proposed block interleaver

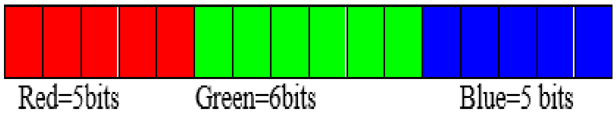


Fig. 5. 16-bit Color Representation

3.4 Color Representation

16-bit Colour is represented as pixel[3] using 16 bits or 2 bytes. The bits are divided as red, blue and green each having values i.e. 5-bits for red, 6-bits for green, and 5-bits for blue.

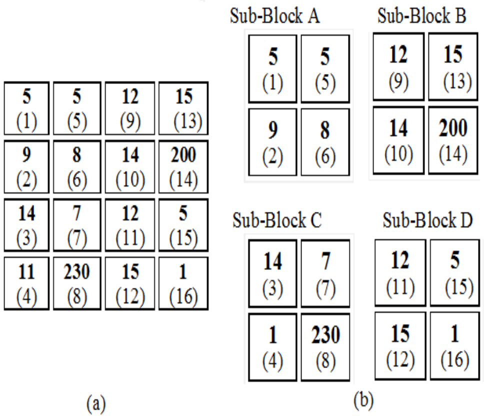
3.5 Pixel Based Integration Technique

Pixel values ranging from 0-255 are represented for input images. Forming pixel integration table row wise and column wise, assigning pixel values in the column wise with starting value as 1 to ending value 266 and the input images are taken as row wise. We consider the color depth of image as 16-bit, choosing the sub-blocks as 4x4 as shown in fig.6.

Considering an image with size of 64x64 and dividing into 4x4 blocks will produce 16 blocks i.e Sub-Block A, Sub-Block B, Sub-Block C, and Sub-Block D. First sub-block A is represented as A(i,j),where i is pixel value and j is index location of pixel. As shown in fig.7, pixel integration table is created. Assigning the pixel index to the corresponding pixel value for the first block of all input images and then second block of every image. This process is continued for all blocks of input images.

16-bit color representation is used in case of multiple indices with the same pixel value in a block. The value is calculated by representing them in the 16-bit color RGB palette as shown in fig.8, and finding their corresponding value.

This process is repeated for all the blocks of the image. By summing all the pixel indices value for each pixel value for all the images, Image Integration is done.



5 (1)	5 (5)	12 (9)	15 (13)
9 (2)	8 (6)	14 (10)	200 (14)
14 (3)	7 (7)	12 (11)	5 (15)
11 (4)	230 (8)	15 (12)	1 (16)

Sub-Block A

5 (1)	5 (5)
9 (2)	8 (6)

Sub-Block B

12 (9)	15 (13)
14 (10)	200 (14)

Sub-Block C

14 (3)	7 (7)
1 (4)	230 (8)

Sub-Block D

12 (11)	5 (15)
15 (12)	1 (16)

Fig. 6. (a) Image Pixel value for 4*4 Image Size (b)Sub-blocks image pixel value for (a)

Image/Pixel	1	2	3..	10
1	4,16			
2	9			
3				
4				
5	1,5,15			
6				
7	7			
8	6			
9	2			
10				
11				
12	9,11			
13				
14	10,3			
15	13,12			
.				
.				
200	14			
230	8			
256				

Fig. 7. Pixel Integration values

1	0	0	0	1	0	0	0	0	0	0	1	0	1	1	0
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Fig.8. RGB values for multiple values in location

4. EXPERIMENTAL DETAILS AND RESULTS

The proposed method has been implemented in MatLab 8.6 in windows environment with a system configuration of I7 Intel Pentium VI Generation processor with 16 GB RAM. The proposed algorithm has been tested with various images. A good quality encryption algorithm should be strong against all types of attack. Another important factor that evaluates the efficiency of algorithms is measuring the amount of time required for overall process. Some experiments are given in this section to demonstrate the efficiency of the proposed technique.

4.1 Correlation Co-Efficient

The correlation [17] is analyzed between input image and encrypted image, which ranges from -1 to +1. If the encrypted image correlation value is equal to zero or very near to zero, then the encrypted image and original image are different, i.e., the original image has no features and is highly independent from the encrypted image. The encrypted image is a negative of the original image, if the correlation is equal to -1. Correlation coefficients were calculated by using the equation (1), (2) and (3),

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

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

Where x, y is input image and encrypted image values of two adjacent pixels in the image. In numerical computation, the following formulas were used

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

The obtained correlation coefficient for encrypted image is shown in Table II and IV.

4.2 Information Entropy

Information entropy [18] is defined to express the degree of uncertainties in the system. Higher entropy images such as an image of heavily cratered on the moon have a great deal of contrast from one pixel to the next and consequently pixel cannot be compressed as much as low entropy images. Entropy H indicated that each symbol has an equal probability. The information entropy for encrypted image is calculated using equation (4),

$$H = -\sum_{i=1}^{n} P_i \text{ x } log_2 P_i \qquad (4)$$

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

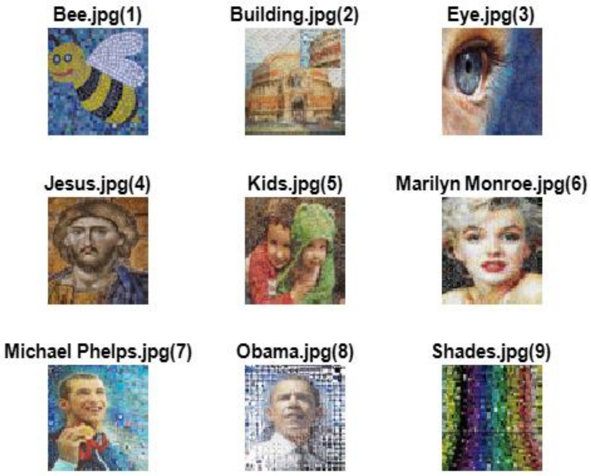


Fig. 9. Mosaic Input Image

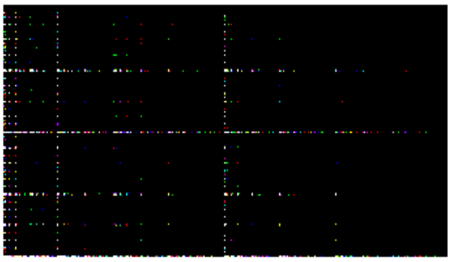


Fig. 10. Encrypted Image

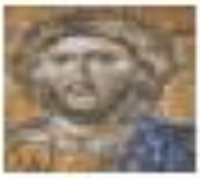


Fig.11. Decrypted Image with Key No.4

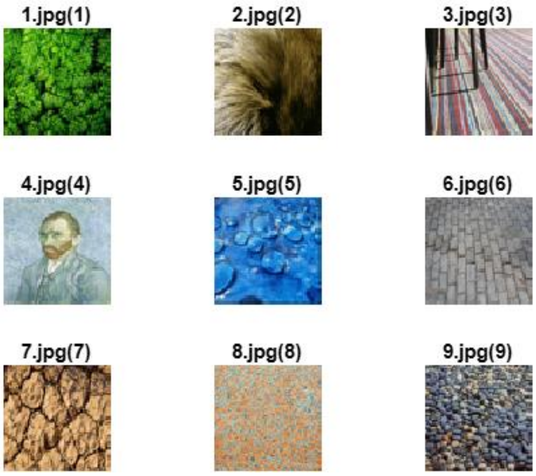


Fig. 12 Texture Input Image

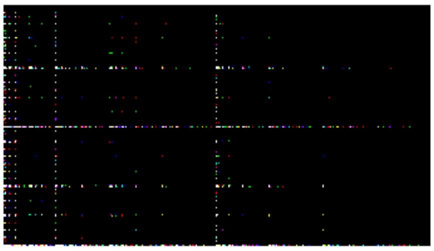


Fig. 13. Encrypted Image

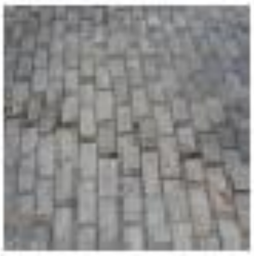


Fig.14. Decrypted Image with Key

A. Result Analaysis

High entropy value and low correlation values provides good encryption. The time taken for encrypting and decrypting mosaic image with key is 687.2435 seconds and texture image with key is 545.8217 seconds.

Results for the correlation and the entropy values are shown in Tables II, III, IV and V.

Table II Entropy and correlation value

IMAGE NAME	ENTROPY	CORRELATION
Bee	1.7015	0.0347
Building	1.7744	0.0522
Eye	1.8929	0.0546
Jesus	1.8898	0.0506
Kids	1.8752	0.0438
Marilyn Monroe	1.8648	0.0470
Michael Phelps	1.7461	0.0470
Obama	1.5968	0.0493
Shades	1.6002	0.0442

Table III Compression ratio

IMAGE NO	R LAYER	G LAYER	B LAYER
1	0.6921	0.6206	0.8538
2	0.7756	0.7861	0.8176
3	0.7031	0.6938	0.6975
4	0.7803	0.8032	0.7788
5	0.7297	0.7141	0.7070
6	0.7642	0.7471	0.7271
7	0.5728	0.6021	0.6653
8	0.6548	0.7673	0.6433
9	0.6021	0.5959	0.5969

Table IV Entropy and correlation value

IMAGE NO	ENTROPY	CORRELATION
1	1.7952	0.0488
2	1.9038	0.0602
3	1.7054	0.0522
4	1.9261	0.0483
5	1.8471	0.0492
6	1.8707	0.0618
7	1.5836	0.0344
8	1.7598	0.0380
9	1.5322	0.0387

Table V Compression ratio

IMAGE NAME	R LAYER	G LAYER	B LAYER
Bee	0.6807	0.6746	0.6624
Building	0.7263	0.7307	0.7246
Eye	0.7795	0.7764	0.7737
Jesus	0.7295	0.7427	0.7471
Kids	0.7209	0.7234	0.7314
Marilyn Monroe	0.7283	0.7244	0.6985
Michael Phelps	0.6816	0.6917	0.6924
Obama	0.6204	0.6208	0.6406
Shades	0.6282	0.6208	0.6489

5. CONCLUSION AND FUTURE WORK

Digital image security has become highly important since the communication by transmitting of digital products over the network occur very frequently. The image encryption algorithm is proposed, based on pixels interleaving with image integration in this paper. First, interleaving the image pixels, then through the method of pixel integration increasing the difficulty of decoded. At last, a camouflaged image for all the input images, getting the final encryption image. Experimental result shows good performance with low correlation and high entropy which demonstrate that the proposed pixel based image encryption algorithm is highly secure. It is also able to encrypt large data sets efficiently and simultaneously. The proposed method is expected to be useful for transmission applications and real-time image encryption system. Future work includes the incorporation of other encryption algorithm and extending the images to videos.

6. REFERENCES

[1] Christof Paar and Jan Pelzl," Understanding Cryptography: A Textbook for Students and Practitioners," Springer, 2010,pp.1-24

[2] Joan Daemen and Vincent Rijmen,"The Design of Rijndael: AES - The Advanced Encryption Standard," Ist edition, New York: Spinger,2002, pp.1-29

[3] Chris Solomon and Toby Breckon,"Fundamentals of Digital Image Processing," Wiley,2010, pp1-18

[4] I. Ozturk and I. Sogukpinar,"Analysis and comparison of image encryption algorithm,"Journal of transactions on engineering, computing and technology, pp.38, Dec 2004.

[5] Li. Shujun and X. Zheng,"Cryptanalysis of a chaotic image encryption method,"IEEE International Symposium on Circuits and Systems, ISCAS, May 2002.

[6] Rinki Pakshwar, Vijay Kumar Trivedi and Vineet Richhariya,"A Survey On Different Image Encryption and Decryption Techniques," International Journal of Computer Science and Information Technologies, pp.113-116, April 2013.

[7] Mohammad Ali Bani Younes and Aman Janta,"Image Encryption Using Block-Based Transformation Algorithm,"IAENG International Journal of Computer, Feb 2008.

[8] Ahmed Bashir Abugharsa, Abd Samad Bin Hasan Basari and Hamida Almangush,"A Novel Image Encryption Using an Integration Technique of Blocks Rotation Based on the Magic Cube and the AES Algorithm," International Journal of Computer Applications, pp.38-45, March 2012.

[9] A. Mitra, Y V. Subba Rao, and S. R. M. Prasnna,"A new image encryption approach using combinational permutation techniques," Journal of Computer Sciece, pp.127, Feb 2006.

[10] Hanpinitsak and C. Charoenlarpnopparut,"2D Interleaver Design for Image Transmission over Severe Burst-Error Environment," International Journal of Future Computer and Communication, pp.308-312, Aug 2013.

[11] Shengyong Guan, Fuqiang Yao and Chang Wen Chen,"A novel interleaver for image communications with theoretical analysis of characteristics," Communications, Circuits and Systems and West Sino Expositions,IEEE 2002 International Conference (Volume:1), July 2002.

[12] B.Subramanyan, V.M.Chhabria and T.G.S.Babu,"Image Encryption Based on AES Key Expansion," Emerging Applications of Information Technology (EAIT), 2011 Second International Conference, Feb 2011.

[13] Rogelio Hasimoto-Beltran and Ashfaq Khichari,"Pixel Level Interleaving scheme for Robust Image Communication," Scalable and Parallel Algorithm Labs, University of Delaware, Newark, Oct 1998.

[14] Aloka Sinha and Kehar Singh,"Image encryption using fractional Fourier transform and 3D Jigsaw transform,"Department of Physics, Indian Institute of Technology Delhi, New Delhi-110016,India,Dec 2004.

[15] Frank Dellaert and Robert Collins, "Fast Image-Based Tracking by Selective Pixel Integration,"Computer Science Department and Robotics Institute Carnegie Mellon University,Pittsburgh,Sep 1999

[16] Norman D. Jorstad, "Cryptographic Algorithm Metrics,"Institute for Defense Analyses Science and Technology Division-Jan 1997.

[17] Satoru Yoneyama and Go Murasawa, "Digital Image Correlation," Encyclopedia of Life Support Systems, Digit Imaging. 2008 Sep.

[18] Du-Yih Tsai, Yongbum Lee and Eri Matsuyama,"Information Entropy Measure for Evaluation of Image Quality", Sep 2008.

[19] G.Zhi-Hong, H.Fangjun, and G.Wenjie, "Chaos-base, Image Encryption Algorithm,"Elsevier, pp. 153-157, Oct 2005.

[20] NIST (National Institute of Standards and Technology) Special Publication 800-57,May 2006