International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: SJIF: 5.995
Available Online at www.journalijcar.org
Volume 7; Issue 1(B); January 2018; Page No. 8848-8853
DOI: http://dx.doi.org/10.24327/ijcar.2018.8853.1441

Research Article

DESIGN OF MULTI-IMAGE PIXEL INTEGRATION TECHNIQUE FOR SECURITY USING SIMON ALGORITHM

Senthil Kumar A.D[1]*., Anandhi T.S[2] and Ranganath Muthu[3]

[1,2]Department of Electronics and Instrumentation, Annamalai University, Chidambaram, India
[3]Department of Electrical and Electronics, SSN College of Engineering, Kalavakkam (near Chennai), India

A R T I C L E I N F O

Article History:
Received 17th October, 2017
Received in revised form 21st November, 2017
Accepted 05th December, 2017
Published online 28th January, 2018

Key words:

Simon Cryptography, Encryption, Image Processing, Pixel Integration, Compression, Image Interleaving

A B S T R A C T

This paper focuses on security application for digital image processing that enables to select one of several images. The techniques involve image interleaving followed by Simon cryptography algorithm and last by proposed pixel integration techniquefor securing the images and to generate integrated multi-image. The user can choose any of the images among the several integrated inputs displayed with a unique security key. With the secure key assigned for each image input, the original image is displayed by decrypting it from multiple images. This method is useful when access permissions need to be restricted to certain viewers. The design is simulated using Matlab and Modelsim software and synthesized using Xilinx ISE.Performance of the design is evaluated with co-relation coefficient and information entropy.

INTRODUCTION

Modern digital technology with computer algorithms performance in image processing has made it possible to manipulate multi-dimensional signals with systems that range from simple digital circuits to advanced parallel computers. Because of the rapid advancement in semiconductors and microprocessor industry, digital technology grew in popularity among broadcasting over the analogy techniques due to the availability of high-speed data transmission with flexibility and environmental variations. As a result, general-purpose computers need to be faster, they started to take over the role of dedicated hardware for all but the most specialized and computer-intensive operations.

With the current trends in digital processing and multimedia applications, security is a critical issue in image storage and communication. Encryption algorithms play a key role in security. An image can be encrypted to convert the original image to another image format which changes the property of the image and makes difficult to identify as the original image. The main purpose for encrypting the image is to keep confidential among users, in other words, it is essential to secure to avoid the piracy or terrorism misleading the contents of the image. The images are transmitted can also be copied or saved during their transmission without loss of image quality by hacking.

Corresponding author:* **Senthil Kumar A.D
Department of Electronics and Instrumentation, Annamalai University, Chidambaram, India

The images can be hacked in time of digital information storage and can be reproduced illegally. It is, therefore, necessary to develop software for effective protection of transferred data against arbitrary interferences. Data encryption with image integration is very often the only effective way to meet these requirements Image information loss and its recovery is still one of the biggest concern in digital communication networks. Interleaving schemes are an important mechanism for reducing the effect of network error on image transmission. Interleaving schemes spatially de-correlate neighboring image blocks by putting them into packets that are far distant apart from each other in the transmission sequence.

To develop proposed PIT based on encryption algorithm for multiple images is focused to enhance security. This paper presents implementing security for multiple images that enables to select one of the several images displayed simultaneously with a unique security key. This process involves compression methods with image interleaving and encrypting of the multiple images and video inputs and finally integrating them using the PIT. To increase the entropy value, compression ratio and to decrease the high correlation among pixels, and thus an improved security level of the encrypted images, we propose a process based on 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 frame before the encryption process starts. The image which

generated is then processed into the Simon encryption algorithm.

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

Sinha A *et al*. [10] proposed a new technique for image encryption and decryption in which the image is broken up into bit planes. A new method to jigsaw the image has been proposed in which every block is translocated 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*. [11] 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*. [12] proposed interleaving scheme where the de-correlation process is applied to coefficient or pixel level in the compressed domain. Frank Dellaert *et al*. [13] 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.

Proposed Method

Each multiple image inputs of size mxn are considered in the work, where m represents column and n represent row. In this work, a set of nine input images with a random size image size of mxn are taken for PIT to test the performance. Each image is resized to 64x64 for pixel-based integration method as shown in Fig.1(a). Each resized image is divided into a block size of 4x4 which will produce 16 sub-blocks as shown in Fig.1(b) and each sub-block has a size of 2x2 as shown Fig.1(c). The input of nine images is interleaved with pixel integration to form a single image of size 64x64. The encryption algorithm is applied to generate secured multi-image integrated single output. For extracting the required specific image out of nine images a unique key is used. The image is retrieved to its original format by the reverse process.

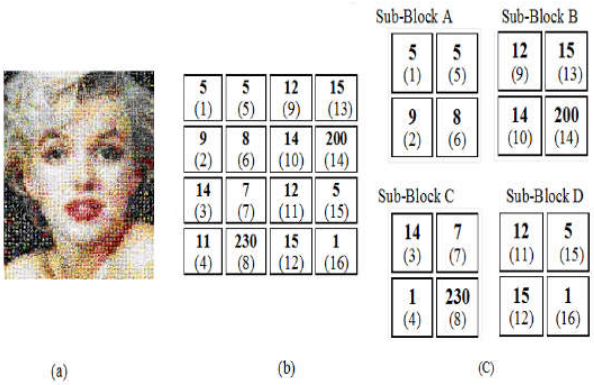

Fig 1 (a) Input Image of Size 64*64 (b) Image Pixel value for 4*4 Block Size (c)Sub-blocks image pixel value for (b)

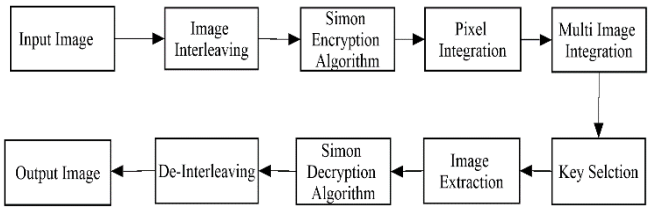

Fig 2 Block Diagram of Proposed System

Image Interleaving

Encrypted RGB frames are divided small blocks [16], [17] as 4*4. Keeping small sub-blocks can achievegood encryption standard. These sub-block input frames are interleaved row or column wise. The interleaverinput is fixed with the number of sub-block pixel values from each block. Now selecting the initial location of the pixel randomly to apply block-based interleaving. Assigning the value of seed as row-wise and column-wise torow-wise andcolumn-wise interleaver. The new locationof bits after interleaving is given below, where p_{row} represents row-wise and p_{col} represents column-wise seeds.

Row-wise	**Column-wise**
$1 \rightarrow 1$	$1 \rightarrow 1$
$2 \rightarrow (1+p_{row}) \bmod n_r$	$2 \rightarrow (1+p_{col}) \bmod n_c$
$3 \rightarrow (1+2p_{row}) \bmod n_r$	$3 \rightarrow (1+2p_{col}) \bmod n_c$
$4 \rightarrow (1+3p_{row}) \bmod n_r$	$4 \rightarrow (1+3p_{col}) \bmod n_c$
... ...	

$n_r \rightarrow (1+(n_r -1)\ p_{row)} \bmod n_r nc \rightarrow (1+(n_c-1)\ p_{col}) \bmod n_c$

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

a

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

b

Fig 3 (a) Block interleaving(b)Proposed method block interleaved sequence

Simon Algorithm

SIMON [16] is a flexible algorithm that enough to provide excellent performance and highly-optimized block ciphers, in both hardware and software environments. For this reason, we have chosen to comb hardware and software co-simulation to achieve better results.In this work, simon algorithm is developed using Verilog HDL and simulated using ModelSim software.In addition, Simon has a range of block and key sizes. The Simon block cipher with an n-bit word (and hence a 2n-bit block) is denoted SIMON2n, where n is required to be 16, 24, 32, 48, or 64. SIMON2n with an m-word (mn-bit) key will be referred to as SIMON2n/mn. Table 1 lists the different block and key sizes, in bits, for SIMON Algorithm.

Table I SIMON Block and Key Size

Block Size	Key Sizes
32	64
48	72,96
64	96,128
96	96,144
128	128,192,256

Simon Algorithm Definition

n = word size (16, 24, 32, 48, or 64)
m = number of key words (must be 4 if n = 16,
3 or 4 if n = 24 or 32,
2 or 3 if n = 48,
2, 3, or 4 if n = 64)
z=[11111010001001010110000111001101111101000100101
011000011100110,
10001110111110010011000010110101000111011111001001
100001011010,
10101111011100000011010010011000101000010001111110
010110110011,
11011011101011000110010111100000010010001010011100
110100001111,
11010001111001101011011000100000010111000011001010
010011101111]
(T, j) = (32,0) if n = 16
= (36,0) or (36,1) if n = 24, m = 3 or 4
= (42,2) or (44,3) if n = 32, m = 3 or 4
= (52,2) or (54,3) if n = 48, m = 2 or 3
= (68,2), (69,3), or (72,4)if n = 64, m = 2, 3, or 4
x,y = plaintext words
k[m-1] …k[0] = key words
---------- key expansion ----------
for i = m.. T-1
tmp ← S−3 k[i-1]
if (m = 4) tmp ← tmp ⊕ k[i-3]
tmp ← tmp ⊕ S−1tmp
k[i] ← ~k[i-m] ⊕ tmp ⊕ z[j][(i-m) mod 62] ⊕3
end for
---------- encryption ----------
for i = 0..T-1
tmp ← x
x ← y ⊕ (Sx & S8x) ⊕ S2x ⊕ k[i]

Co-Simulation Simon Algorithm

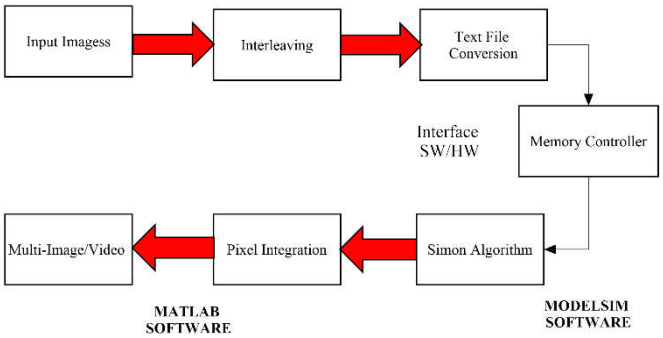

Fig 3 System Architecture-Hardware/ Software co-simulation platform

Figure.3 shows the system architecture being developed for Simon encryption algorithm. MATLAB is used as the software platform and ALTERA-ModelSim 6.3g is used as the hardware platform. QUARTUS II (8.1 web edition) design flow is used to simulate and verify the functionality of HDL code. Xilinx ISE 14.3 is used to understand the device and logic utilization, memory design, and test control of the architecture developed.

To maintain the resolution and decrease redundancy, the images are resized to 64 × 64 pixels. Once the input images are obtained, they are converted to grayscale values within a range of 0–255. The database obtained is read on the computer using MATLAB. The software converts the entire database image frames into text files. These files are stored in the memory using the command "$readmemh." The ALTERA-ModelSim is being called from the MATLAB using HDLDAEMON as shown in Figure 5 HDLDAEMON.

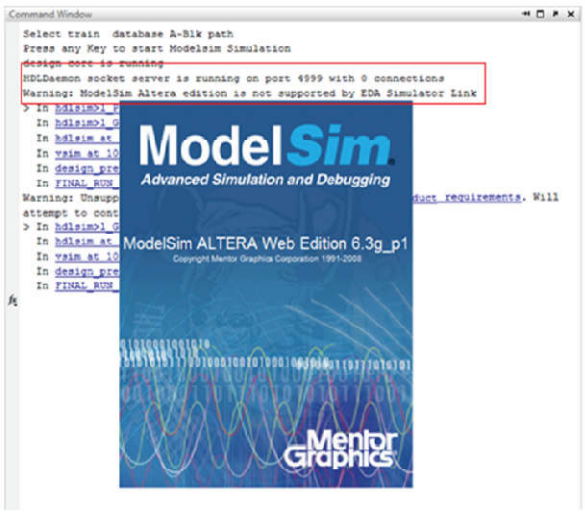

Fig 4 HDLDAEMON as the interface between MATLAB and ALTERA-ModelSim

Text File Conversion

The images are converted into text files which contain the hexadecimal value of the pixels. Each image is configured and stored with the appropriate configuration ID. The text file of each image contains 4096 values to be read and stored in the memory of the ALTERA-ModelSim. The figure displays the pixel values.

```
0001 0001 0001 0001 0001 0001 0002 0001 0000 0001
0002 0002 0002 0001 0001 0001 0001 0002 0002 0001
0002 0002 0001 0002 0002 0002 0002 0002 0002 0002
0002 0002 0001 0002 0002 0001 0002 0002 0001 0001
0001 0002 0002 0001 0002 0002 0002 0002 0002 0003
0002 0002 0003 0004 0003 0002 0002 0002 0003 0003
0002 0003 0003 0002 0003 0003 0005 0004 0002 0001
00CF 00D3 00DF 00E3 00E2 00E0 00D7 00CB 00DC 00DE
00B3 00C4 00C5 00C4 00C8 00CE 00D6 00DA 00DB 00DE
00D9 00D7 00D1 00C7 00C0 00C2 00C1 00BA 00BC 00B9
0004 0003 0004 0003 0067 00C8 00CE 00B0 00A8 00B0
00C6 00D1 00CB 00C2 00B5 009D 00A8 00B3 00AD 0095
00A4 008A 00A5 00A5 00A6 00B8 00CF 00D8 00DD 00DA
00AE 00AD 00A6 009C 0098 008E 0088 0081 007A 0069
0002 0002 0002 0002 0002 0001 0001 0002 0002 0001
0003 0003 0003 0003 0003 0004 0004 0004 0005 0004
0005 0006 0006 0005 0006 0006 0007 0007 0004 0005
0008 0008 0009 0007 0006 0005 0004 0004 0005 0004
0004 0002 0003 0004 0002 0002 0002 0003 0002 0002
0003 0003 0004 0003 0003 0003 0003 0002 0003 0005
```

Fig 5 Pixel Values in Memory Location

Memory Controller on ALTERA-ModelSim

The text files obtained from the image files are stored onto another file in the memory locations of the ALTERA-ModelSim. The files contain data represented by hexadecimal values and hence contain 16 digits of length. For every negative edge of the clock cycle, the data is read into the memory location.

Color Format

16-bit color is represented as pixel[3] using16 bits or 2 bytes. These bytes or bits of color are divided as R G B layer each having values i.e. Red-5, Green-6, and Blue-5 bits respectively

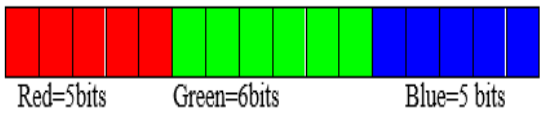

Fig 6 16-bit color format

Pixel Integration Technique

Consider image input of size m*m,

Step:1 Theimage input is represented as pixel values ranging from 0-255.

Step:2 Table for pixel integration is formed in row wise and column wise, assigning the input images are taken as row-wise pixel values and column wise with starting value as 1 to ending value 266.

Step:3 Considering the color depth of each frame as 16-bit and choosing 4*4 as sub-blocks.The image is converted into frames as shown in fig.7.

Step:4 The RGB input as shown in fig.1(a) with size of 64x64 and dividing into 4x4 blocks as shown in fig.1(b)will produce 16 blocks which are represented as A, B, C, and D. A(i,j) is first sub-block of A, where i is pixel value and j is index location of pixel. Pixel integration table is created as shown in fig.11

Step:5 Assign the pixel index with respect to the pixel value for the first block of all input images and then the second block of every image. This process is continued for all blocks of input frames.

Step:6 16-bit colour 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 with reference to fig.7, and finding their corresponding value as shown in fig.10

Step:7This process is repeated for all the blocks of the input RGB frames individually. By adding all RGB pixel indices value for each pixel value for all the frames, Image Integration is done.

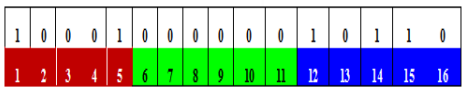

Fig 7 Multiple values location in RGB format

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 8 Pixel Integration values

RESULTS AND DISCUSSION

The proposed method has been implemented in a Windows-10 operating system using I7 Processor with 16GB Ram. A good quality encryption algorithm should be strong against all types of attack. Another key factor that evaluates the efficiency of algorithms is measuring the amount of time required for the overall process. Some experiments are given in this section to demonstrate the efficiency of the proposed technique.

Correlation Co-Efficient

The correlation [19] is analyzed between the input image and encrypted image, which is called the correlation coefficient, 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 totally different, i.e., the original image has no features and is highly independent of 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 following equation (1), (2) and (3),

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

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

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.

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

The obtained correlation coefficient for encrypted counterpart is shown in Table II, III and IV.

Information Entropy

Information entropy [20] is defined to express the degree of uncertainties in the system. A secure encryption should provide a situation which the encrypted image is not provided any information about the original image. On the other hand, 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, the pixel cannot be compressed as much as low entropy images. Entropy indicated that each symbol has an equal probability. The information entropy for encrypted is calculated using equation no (4),

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

Result Analysis

High information entropy valuesachieve good encryption along with low correlation values. The simulation time for imageencryption and decryption with the specific key is 197.1251 sec

Results for the compression ratio for each frame for RGB layer, correlation coefficient value, and the entropy values are shown in Tables III and IV. Synthesis results are shown below.

Table II Timing Parameter using Xilinx ISE

Parameters	Time in ns
Minimum Period	17.021
Minimum input Arrival time before clock	6.656
Maximum output required time after clock	6.455

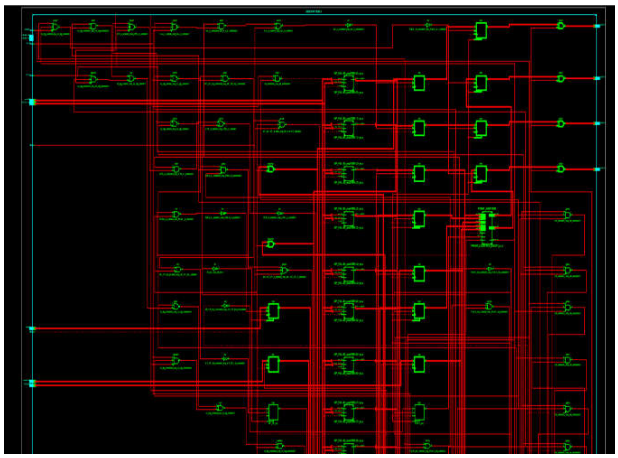

Fig 9 Simon Algorithm RTL View-Xilinx ISE

Logic Utilization	Used
Number of Slices	10401
Number of Slice Flip Flops	3506
Number of 4 input LUTs	19342
Number of bonded IOBs	358
Number of MULT18X18SIOs	4
Number of GCLKs	24

Fig 10 Simon Algorithm Device Utilization Factor-Xilinx ISE

Fig 11 Input Images for Pixel Integration

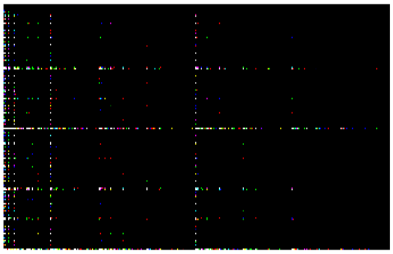

Fig12 Pixel Integrated Encryption Image

Fig 13 Extracted Image with Key No.3

Table III Entropy and Correlation Values

Image Name	Entropy Value	Correlation Value
Bush	1.8322	0.0443
Jeff	1.7627	0.0313
Kejriwal	1.7925	0.0353
Modi	1.6654	0.0164
Obama	1.7058	0.0455
Putin	1.7116	0.0200
Rahul	1.7352	0.0040
Sushma	1.7842	0.0272
Trump	1.7030	0.0485

Fig 14 Input Images for Pixel Integration

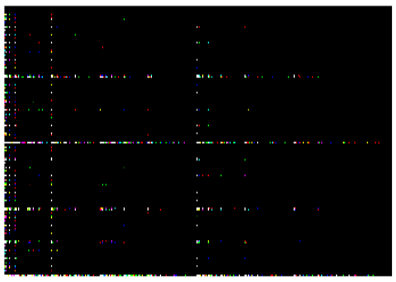

Fig 15 Pixel Integrated Encryption Image

Fig 16 Extracted Image with Key No.3

Table IV Entropy and Correlation Values

Image Name	Entropy Value	Correlation Value
Hill	1.8563	0.0531
Hydrangeas	1.7925	0.0313
Jellyfish	1.5838	0.0260
Koala	1.9008	0.0377
Lena	1.8583	0.0328
Lighthouse	1.7642	0.0576
Penguins	1.7593	0.0253
Peppers	1.6931	0.0134
Tulips	1.7375	0.0212

CONCLUSION AND FUTURE SCOPE

Due to data transmission of digital information using wireless and processing systems, security has become a primary concern. To increase the security and to avoid data hacking, interleaving and encryption with pixel integration method are approached in this paper. First, interleaving the input image using Matlab along with the encrypting using Verilog HDL and then by pixel integration using Matlabproduce an integrated image which makes difficult to decode. Test results have been carried out utilizing detailed numerical analysis which shows the strength of the proposed algorithm. The proposed algorithm presented exists a direct relationship between the number of blocks and entropy and inverse relationship between the number of blocks and correlation this technique is expected to show good performance with low correlation coefficient value, high information entropy. Moreover, test result shows performance evaluation of proposed image encryption algorithm is highly secure which makes to encrypt large sets of data simultaneously and efficiently. The proposed method will be used in transmission applications and real-time video encryption.

References

1. Christof Paar and Jan Pelzl,2010," *Understanding Cryptography: A Textbook for Students and Practitioners*," Springer, pp.1-24
2. Chris Solomon and Toby Breckon,"2010, Fundamentals of Digital Image Processing," Wiley, pp1-18
3. Ray Beaulieu,Douglas Shors, Jason Smith, Stefan Treatman and Clark Bryan Weeks ,2013, "The Simon And Speck Families of Lightweight Block Ciphers", National Security Agency.
4. Li. Shujun and X. Zheng,2002,"Cryptanalysis of a chaotic image encryption method,"IEEE International Symposium on Circuits and Systems, ISCAS, May.
5. Norman D. Jorstad, 1997, "*Cryptographic Algorithm Metrics*,"Institute for Defense Analyses Science and Technology Division-.
6. Ozturk and I. Sogukpinar, 2004, "Analysis and comparison of image encryption algorithm," *Journal of transactions on engineering, computing and technology*, pp.38-43.
7. Ahmed Bashir Abugharsa, Abd Samad Bin Hasan Basari and Hamida Almangush,2010, "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,
8. Mitra, Y V. Subba Rao, and S. R. M. Prasnna, 2006, "A new image encryption approach using combinational permutation techniques," *Journal of Computer Sciece*, pp.127-135.
9. Aloka Sinha and Kehar Singh,2004,"Image encryption using fractional Fourier transform and 3D Jigsaw transform, "Department of Physics, Indian Institute of Technology Delhi, New Delhi-110016,India.
10. G.Zhi-Hong, H.Fangjun, and G.Wenjie, 2005, "Chaos-base, Image Encryption Algorithm,"Elsevier, pp**.** 153-157.
11. Rogelio Hasimoto-Beltran and Ashfaq Khichari,1998, *"Pixel Level Interleaving scheme for Robust,"* Image Communication Scalable and Parallel Algorithm Labs, University of Delaware, Newark.
12. Frank Dellaert and Robert Collins, 2010, "Fast Image-Based Tracking by Selective Pixel Integration,"Computer Science Department and Robotics Institute Carnegie Mellon University, Pittsburgh.
13. Soheil Feizi, Arash Ahmadi and Ali Nemati,"2014, *A* hardware implementation of Simon cryptography algorithm", 4th International eConference on Computer and Knowledge Engineering (ICCKE).
14. Hanpinitsak and C. Charoenlarpnopparut,2013,"*2D* Interleaver Design for Image Transmission over Severe Burst-Error Environment," *International Journal of Future Computer and Communication*, pp.308-312.
15. Shengyong Guan, Fuqiang Yao and Chang Wen Chen, 2002, "A novel interleaver for image communications with theoretical analysis of characteristics," Communications, Circuits and Systems and West Sino Expositions,IEEE 2002 International Conference (Vol.1.,pp-36-42.
16. Satoru Yoneyama and Go Murasawa, 2008, "Digital Image Correlation," Encyclopedia of Life Support Systems, Digit Imaging.
17. Du-Yih Tsai, Yongbum Lee and Eri Matsuyama,2008,"Information Entropy Measure for Evaluation of Image Quality".

How to cite this article:

Senthil Kumar A.D., Anandhi T.S and Ranganath Muthu (2018) 'Design of Multi-Image Pixelintegration Technique For Security Using Simon Algorithm', *International Journal of Current Advanced Research,* 07(1), pp. 8848-8853.
DOI: http://dx.doi.org/10.24327/ijcar.2018.8853.1441

****