pISSN 1976-913X
eISSN 2092-805X

J Inf Process Syst, Vol.9, No.3, September 2013 http://dx.doi.org/10.3745/JIPS.2013.9.3.499

Hardware Software Co-Simulation of the Multiple Image Encryption Technique Using the Xilinx System Generator

Panduranga H T*, Dr. Naveen Kumar S K* and Sharath Kumar H S*

Abstract—Hardware-Software co-simulation of a multiple image encryption technique shall be described in this paper. Our proposed multiple image encryption technique is based on the Latin Square Image Cipher (LSIC). First, a carrier image that is based on the Latin Square is generated by using 256-bits of length key. The XOR operation is applied between an input image and the Latin Square Image to generate an encrypted image. Then, the XOR operation is applied between the encrypted image and the second input image to encrypt the second image. This process is continues until the nth input image is encrypted. We achieved hardware co-simulation of the proposed multiple image encryption technique by using the Xilinx System Generator (XSG). This encryption technique is modeled using Simulink and XSG Block set and synthesized onto Virtex 2 pro FPGA device. We validated our proposed technique by using the hardware software co-simulation method.

Keywords—Image Encryption, Latin Square

1. INTRODUCTION

With the increasing growth of multimedia applications and the usage of the Internet, information security is an important issue in the areas if communication and the storage of images. Encryption is one of the ways to ensure security. Many efficient image encryption schemes have been proposed and practiced so far. Zhengjun Liu et al. [1] presented and designed the amplitude scrambling operation that was introduced into the image encryption process to enhance the security of double random phase encoding. Nanrun Zhou et al. [2] proposed an image encryption scheme that is based on the fractional Mellin transform and the phase retrieval technique. This particular encryption scheme reduced the burden of transmission and enlarged encrypting key space. Guodong Ye et al. [3] proposed a novel image encryption scheme that is based on time-delay and a hyperchaotic system. The time-delay phenomenon is incorporated into the generation of pseudo-random chaotic sequences. To further increase the degree of randomness, the output of the hyperchaotic system is processed before appending shuffled sequence to the generated sequence. A novel permutation function for shuffling the position index, combined together with the double diffusion operations in both forward and reverse directions of an array is employed to enhance the encryption performance.

Manuscript received January 21, 2013; first revision April 10, 2013; accepted June 20, 2013.
Corresponding Author: Panduranga H T
* Dept. of Studies in Electronics, University of Mysore, Hemagangothri PG Center-Hassan, Karnataka–INDIA. (ht_pandu@yahoo.co.in, nave12@gmail.com, sharath.kr83@gmail.com)

It has been also observed that, image encryption and steganography can be done by using Sudoku and Latin Square. The Duc Kieu et al. [4] proposed a Sudoku based wet paper hiding scheme in which a secret key is used to randomly select a subset of pixels from a cover image as dry pixels. Then a toral automorphism is applied to the cover image to maximize the number of dry pixel pairs and each secret digit in the base-9 numeral system is embedded into one dry pixel pair. Chin-Chen Chang et al. [5] presented a Sudoku based secret image (random image) sharing scheme to lossless reveal (decrypted image is exactly equal to original image) of secret image Their approach also derives the secret shadows from first random/secret image and generates a meaningful shadow images by adopting the Sudoku. Roshan Shetty B et al. [6] proposed an information scheme that uses the Sudoku puzzle, in which they used Sudoku solutions to guide cover pixels to modify pixel values so that secret messages can be embedded in encrypted image. Yue Wu et al. [7] have introduced a symmetric-key Latin Square Image Cipher (LSIC) for grayscale and color images.

Instead of single image encryption, multiple image encryption schemes have been presented in many works. Narendra Singh and Aloka Sinha [8] proposed a new method for multiple image encryption using linear canonical transforms and chaotic maps. Three linear canonical transforms and three chaotic maps are used in the proposed technique. The three linear canonical transforms that have been used are the fractional Fourier transform, the extended fractional Fourier transform, and the Fresnel transform. The three chaotic maps that have been used are the tent map, the Kaplan–Yorke map, and the Ikeda map. These chaotic maps are used to generate the random phase masks and these random phase masks are known as "chaotic random phase masks." Xiaogang Wang and Daomu Zhao [9] presented an improved method for multiple-image encryption that is based on nonlinear operations in the Fourier domain. Xiaopeng Deng and Daomu Zhao [10] proposed a novel method for multiple-image encryption using a phase retrieve algorithm and intermodulation in the Fourier domain. All plaintexts to be encoded are first encoded separately into a phase-only function in the Fourier domain with the help of the phase retrieve algorithm. Then these phase-only functions mutually serve as the second encryption keys, which are to be intermodulated into a single image. M.Z. He et al. [11] proposed a novel method of multiple image encryption and watermarking by random phase matching, which can encrypt and then decrypt more than one image with the same set of transmitted patterns based on the idea of double phase encoding and the wave field superposition. Xiaogang Wang and Daomu Zhao [12] have proposed an optoelectronic image encryption and decryption technique based on the coherent superposition principle and digital holography. Haozhi Zhao et al. [13] proposed a multiple image encryption approach based on the position multiplexing of the Fresnel phase. Qu Wang et al. [14] presented a novel method for double image encryption by using a linear blend operation and double random phase encoding (DRPE) in the fractional Fourier domain. Zhi Zhong et al. [15] proposed a novel double image encryption method by utilizing a double pixel scrambling technique and random fractional Fourier domain encoding. One of the two original images is encoded into the phase of a complex signal after being scrambled by one matrix, and the other original image is encoded into its amplitude after being scrambled by another matrix. The complex signal is then encrypted into stationary white noise by utilizing double random phase encoding in the fractional Fourier domain.

It's necessary to evaluate the performance of image processing algorithms on reconfigurable hardware. This is achieved by using FPGA as a reconfigurable device. The Xilinx System Generator (XSG) is an Integrated Design Environment (IDE) for FPGAs. It uses Simulink as a de-

velopment environment and is presented in the form of a blockset. Alba M. Sánchez G. et al. [16] proposed the architecture for filters (pixel by pixel) and region filters for image processing by using the Xilinx System Generator. This architecture offers an alternative to hardware description language (HDL) through a graphical user interface that combines MATLAB, Simulink, and XSG and it explores important aspects related to hardware implementation. Ana Toledo Moreo et al. [17] showed how the Xilinx System Generator (XSG) environment could be used to develop hardware-based computer vision algorithms from a system level approach, which makes it suitable for developing co-design environments. Mrs. S. Allin Christe et al [18] presented an efficient architecture for various image filtering algorithms and tumor characterization by using the Xilinx System Generator. This architecture offers an alternative to HDL through a graphical user interface that combines MATLAB, Simulink, and XSG and it explores important aspects that are related to hardware implementation. V.Elamaran et al. [19] explained the FPGA implementation of Spatial Image Filters by using the Xilinx System Generator.

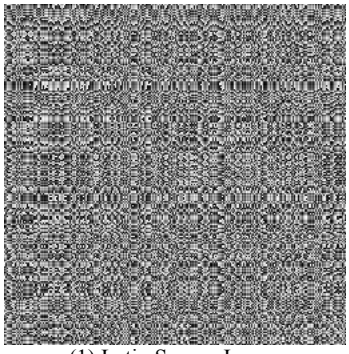
The evaluation of image encryption algorithms is an important task. The efficiency of an image encryption algorithm can be analyzed by using Statistical Analysis, Differential Analysis, Image Entropy, Mean Square Error (MSE), and Peak Signal to Noise Ratio (PSNR) [20].

This paper is organized as follows: following the introduction, we present an overview of the Latin Square in Section 2. Section 3 explains our proposed approach for multiple image encryption. Software and hardware co-simulation of the proposed approach for multiple image encryption is explained in Section 4. Section 5 consists of results and discussions proposed multiple image encryption technique. In Section 6, we conclude this paper by providing a summary of our work.

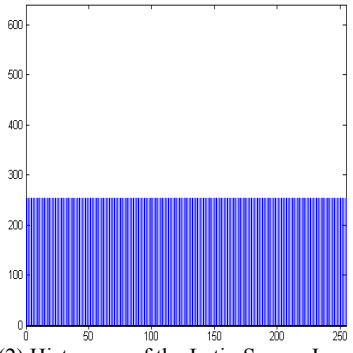
2. OVERVIEW OF THE LATIN SQUARE IMAGE

The Latin Square of order n is an $n \times n$ array in which each of the n^2 cells contains a symbol from an alphabet of size n, such that each symbol in the alphabet occurs just once in each row and once in each column. The name "Latin Square" was inspired by mathematical papers by Leonhard Euler, who used Latin characters as symbols.

In this study we derived the theory for our Latin Square and the generation of a Latin Square



(1) Latin Square Image



(2) Histogram of the Latin Square Image

Fig. 1. The Latin Square Image and its Histogram

Image (LSI) from the work that was presented by Yue Wu [7]. To generate a LSI we used a key that was 64 hexadecimal characters in length. Each character is 4-bits in length (i.e., the length of a key is 256-bits.) The used key is "F5A172F6E8B163D987C23A78B12F73A6519D76C534 B12A64CC67B8981267ABFD". Figure 1 shows the Latin Square Image (LSI) that was generated from the above-mentioned key that is 256-bits in length and histogram of LSI.

3. PROPOSED APPROACH FOR MULTIPLE IMAGE ENCRYPTION

Our proposed approach consists of multiple stages. Except for the first stage, each stage is dedicated to the encryption of each input image. However, Stage 1 is dedicated for the generation of the Latin Square Image. In Stage 2, the XOR operation is applied between "Input Image 1" and the Latin Square Image that was generated in Stage 1 which results in "Encrypted Image 1." In Stage 2, the XOR operation is again applied between "Encrypted Image 1" and "Input Image 2" to produce "Encrypted Image 2." A similar process is performed up to Stage n, where the XOR operation is applied between "Input Image n" and "Encrypted Image n-1" to produce "Encrypted Image n."

The proposed concept for multiple image encryption includes the following considerations:

1. This multiple image encryption is not applicable for video frames that have highly correlated consecutive frames. It is applicable to multiple images (i.e., medical images – MRI-images etc.).
2. The concept of the Latin Square Image (LSI) has been borrowed from reference [7]. LSI is very important because the entropy of this LSI is 8. (i.e., the entropy of the random image is equal to 8.) Just by conducting a simple xor operation with any image the randomness of the encrypted image is increased. However, it is easy to guess if two consecutive frames are the same.
3. Since here we used a 256-bit key, we get multiple LSIs that are changed by 1-bit. It is very difficult to break the key or guess the LSI.

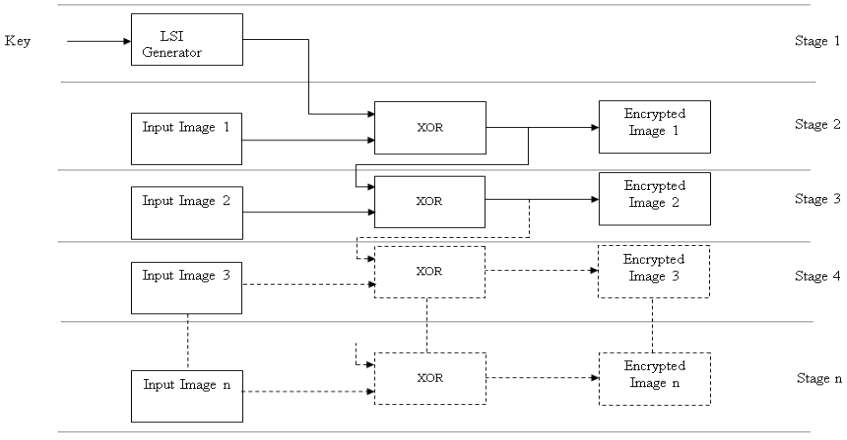


Fig. 2. Block Diagram Representation of the Proposed Approach for Multiple Image Encryption

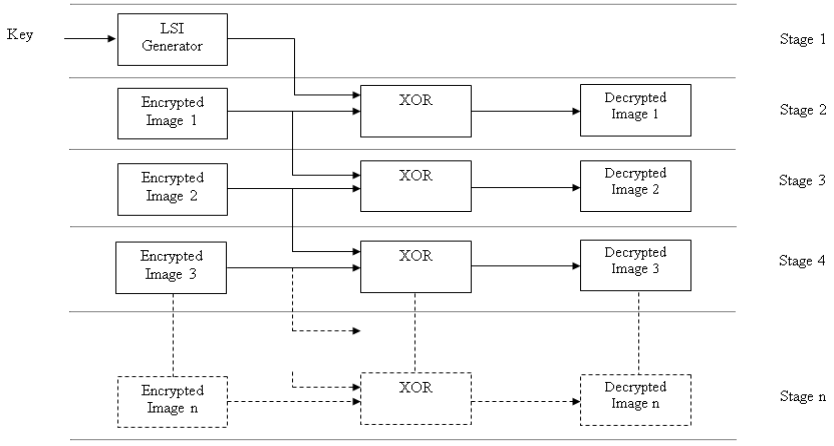


Fig. 3. Block Diagram Representation of the Decryption Approach for Encrypted Images

Figure 2 shows the proposed approach for multiple image encryption. Figure 3 shows the block diagram representation for the decryption of the proposed approach.

4. THE SOFTWARE AND HARDWARE CO-SIMULATION OF THE PROPOSED APPROACH

The software simulation of the proposed approach is as shown in Figure 4. Figure 5 shows the Hardware Co-Simulation of the proposed multiple image encryption approach. For Software Simulation, the XSG Blockset in available in Simulink are utilized. After software simulation,

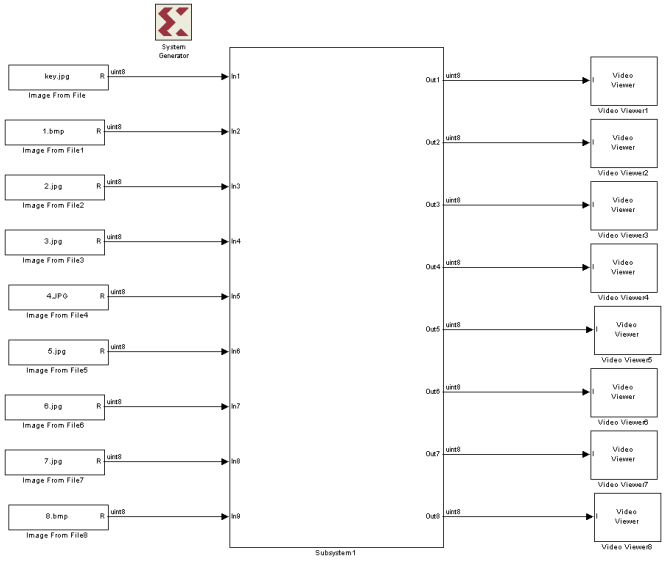


Fig. 4. Software Simulation of the Proposed Encryption Approach

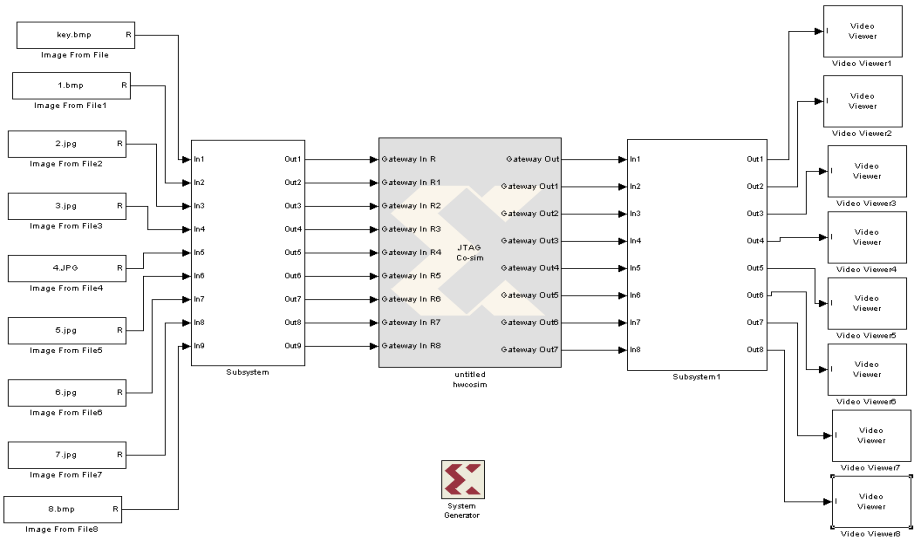
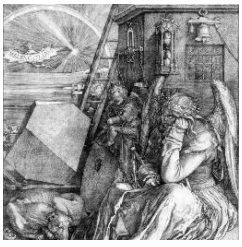


Fig. 5. Hardware Simulation of the Proposed Encryption Approach.

the hardware co-simulation block can be generated and then it will be used to program the FPGA for implementing our proposed approach.

5. RESULTS AND DISCUSSION

In this section, some of the security analyses, which include the most important ones like statistical analysis and differential analysis, on the results from the proposed approach are de-



Input Image 1

Input Image 2

Input Image 3

Input Image 4

Input Image 5

Input Image 6

Input Image 7

Input Image 8

Fig. 6. Input Images

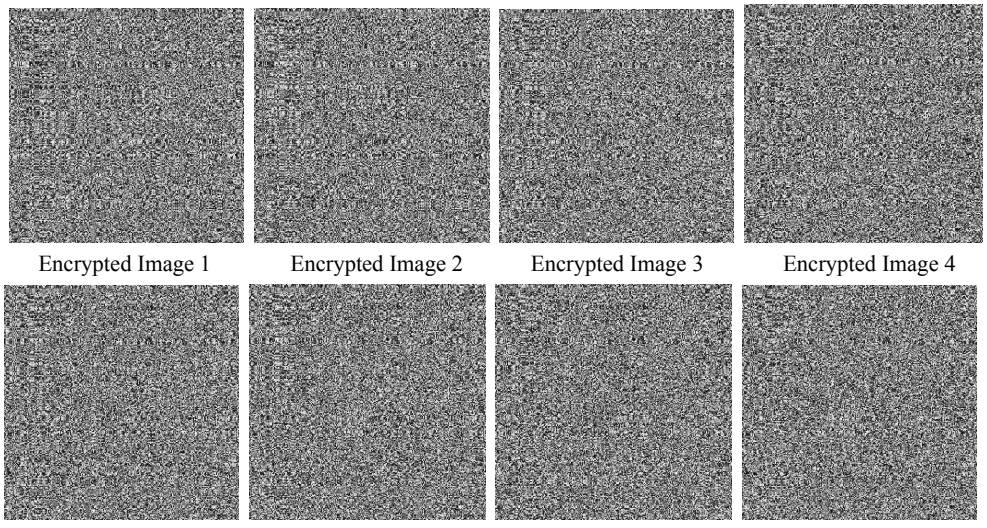


Fig. 7. Encrypted Images

scribed. Figure 6 shows input images and Figure 7 shows respective encrypted images.

5.1 Statistical Analysis

In order to resist statistical attacks, the encrypted images should possess certain random properties. A detailed study has been conducted on encrypted image and the results of this study are summarized as listed below.

5.1.1 The Histogram of Encrypted Images

In order to appear random, the histograms of the encrypted image should be uniformly distributed in all of the gray levels. Figures 8 and 9 show the histograms of the original and the encrypted images respectively. It can be observed that flat histograms result from the encrypted images.

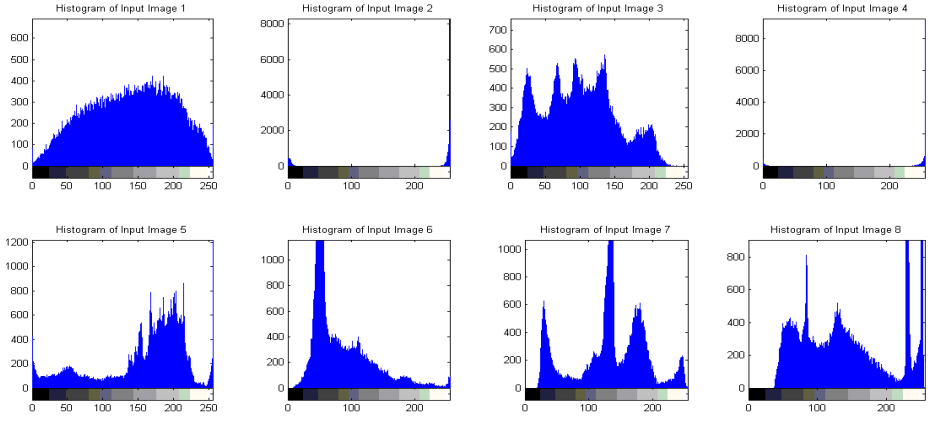


Fig. 8. The Histograms of the Original Images

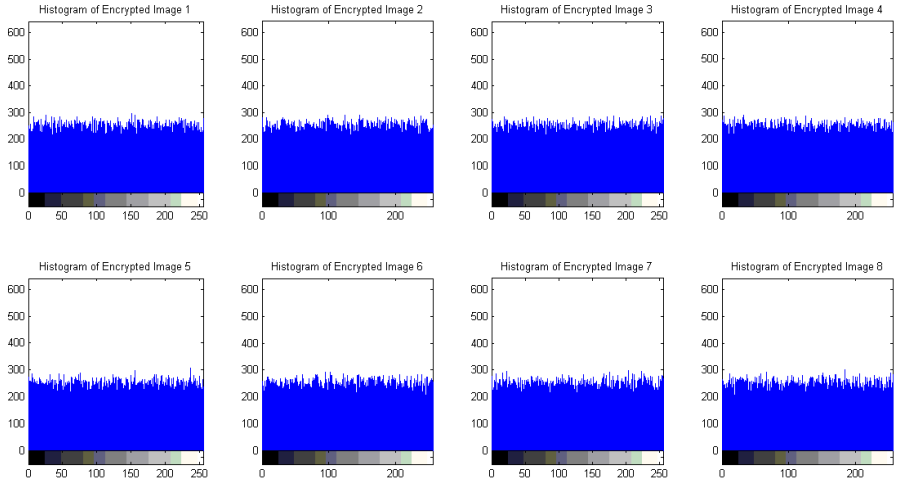


Fig. 9. The Histograms of Encrypted Images

5.1.2 Correlation of Adjacent Pixels

The correlation between two vertically adjacent pixels and two horizontally adjacent pixels in a cipher image can be computed by using Eq. (2):

$$cov(x,y) = E\big(x - E(x)\big)\big(v - E(v)\big) \tag{1}$$

$$r_{xy} = \frac{cov(x,y)}{\sqrt{var(x)}\sqrt{var(y)}} \tag{2}$$

where x and y are the gray levels of the two adjacent pixels in the image. The correlation coefficients of both images are computed in both horizontal and vertical directions and are tabulated in Table 1**.**

Table 1.

		Input Image	Encrypted Image
Image 1	Horizontal	0.8471	0.1015
	Vertical	0.6852	0.302
Image 2	Horizontal	0.996	0.1211
	Vertical	0.9993	0.2941
Image 3	Horizontal	0.8816	0.0864
	Vertical	0.8943	0.1099
Image 4	Horizontal	0.8649	0.0721
	Vertical	0.9243	0.0989
Image 5	Horizontal	0.9734	0.0914
	Vertical	0.9907	0.2352
Image 6	Horizontal	0.9917	0.0623
	Vertical	0.9917	0.2097
Image 7	Horizontal	0.9974	0.0788
	Vertical	0.9968	0.0852
Image 8	Horizontal	0.9869	0.0575
	Vertical	0.9938	0.1423

5.2 Differential Analysis

The major requirement of all the encryption techniques is that the encrypted image should greatly differ from its original form. Two measures are adopted to quantify this requirement. These two measures are the Number of Pixel Change Rate (NPCR) and the Unified Average Changing Intensity (UACI). The NPCR is used to measure the number of pixels in the difference of the gray level in two images. Let *C(i, j)* and *C'(i, j)* be the i^{th} row and j^{th} column pixel of two images *C* and *C'*, respectively. The NPCR can be defined as:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{N} \times 100 \tag{3}$$

where *N* is the total number of pixels in the image and *D(i, j)* is defined as:

$$D(i,j) = \begin{cases} 0 & C(i,j) = C'(i,j) \\ 1 & C(i,j) \neq C'(i,j) \end{cases}$$

Another quantity, the Unified Average Changing Intensity (UACI) measures the average intensity of differences between the two images. It can be defined as:

$$UACI = \frac{1}{N}\left[\sum_{i,j} \frac{|C(i,j) - C'(i,j)|}{255}\right] \times 100 \tag{4}$$

The two quantities, NACP and UACI, are calculated for various images using Eq. (3) and Eq. (4), respectively. The results are tabulated in Table 2**.**

Along with Statistical Analysis & Differential Analysis, the Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) and image entropy (amount of information in an image) for the proposed technique has been computed for different images. We know that as the MSE increases the PSNR decreases, which results in more randomness in the encrypted image. The MSE is calculated using the following formula:

$$MSE = \frac{1}{MN}\sum_{i=1}^{N}\sum_{j=1}^{M}[C(i,j) - C'(i,j)]^2 \tag{5}$$

where, *C(i, j)* and *C'(i, j)* be the *i*th row and *j*th column pixel of the two images *C* and *C'*, respectively. M and N are the number of the rows and columns of the original image.

Table 2.

	NPCR	UACI
Image 1	98.2864	30.6131
Image 2	99.6353	48.8613
Image 3	99.6353	30.713
Image 4	99.5773	49.7168
Image 5	99.5834	33.68
Image 6	99.5804	31.5697
Image 7	99.6155	29.7801
Image 8	99.6216	32.3013

Table 3.

	MSE	PSNR
Image 1	127.8313	8.5774
Image 2	226.5284	4.9534
Image 3	88.4034	8.5666
Image 4	235.3135	4.8299
Image 5	152.6521	7.7119
Image 6	70.4915	8.3031
Image 7	122.3777	8.8819
Image 8	134.0774	8.0965

Table 4.

	Input Image	Encrypted Image
Image 1	7.85	7.9973
Image 2	1.7253	7.9973
Image 3	7.628	7.9975
Image 4	1.0411	7.9976
Image 5	7.2587	7.9974
Image 6	6.9953	7.9971
Image 7	7.1737	7.9972
Image 8	7.4112	7.9969

PSNR can be computed by:

$$PSNR = 10 \times log_{10}\left[\frac{R^2}{MSE}\right] \tag{6}$$

where R is 255, as we used an 8-bit image for this experiment.

The calculated results of the MSE and PSNR are tabulated in Table 3.

The image entropy of the input and encrypted images are calculated and tabulated in Table 4.

An increase in the entropy of encrypted images can be seen in Table 4. This resultant entropy of the encrypted image is almost equal to the entropy of a random image. entropy of random image is equal to 8.

Our technique is more useful in the following areas:

1. Medical image security (MRI-images)
2. Satellite image security (securing and constructing 3D images by using multiple 2D images)
3. Video conferencing with multiple users (in 3G mobile communication)
4. TV news channels and the sub-images in a main video frame.

6. CONCLUSION

In this study we have proposed a hardware software co-simulation of the multiple image encryption technique. LSIC is used to create a base image for encryption. A sequential XOR operation is performed to generate the encrypted image and the hardware software co-simulation of the proposed approach is carried out using the Xilinx System Generator and the Xilinx Virtex 2 Pro FPGA device. The performance of the proposed approach was tabulated and based on the results we can say that this proposed technique is more suitable when all of the images are different or even just slightly different.

REFERENCES

[1] Zhengjun Liu, She Li, Wei Liu, Yanhua Wang, Shutian Liu, "Image encryption algorithm by using fractional Fourier transform and pixel scrambling operation based on double random phase encoding", Optics and Lasers in Engineering 51 (2013) 8–14.

[2] Nanrun Zhou, XingbinLiu, YeZhang, YixianYang, "Image encryption scheme based on fractional Mellin transform and phase retrieval technique in fractional Fourier domain", Optics & Laser Technology 47 (2013) 341–346.

[3] Guodong Ye, Kwok-WoWong, "An image encryption scheme based on time-delay and hyperchaotic system", Nonlinear Dyn (2013) 259–267.

[4] The Duc Kieu, Zhi-Hui Wang, Chin-Chen Chang, and Ming-Chu Li, "A Sudoku Based Wet Paper Hiding Scheme", International Journal of Smart Home, 2009, 1-12.

[5] Chin-Chen Chang, Pei-Yu Lin, Zhi Hui Wang and Ming Chu Li, "A Sudoku-based Secret Image Sharing Scheme with Reversibility", Journal Of Communications, Vol. 5, No. 1, January 2010, 5-12.

[6] Roshan Shetty B R, Rohith J, Mukund V, Rohan Honwade, Shanta Rangaswamy, "International Conference on Advances in Recent Technologies in Communication and Computing", 2009.

[7] Yue Wu, Yicong Zhou, Joseph P. Noonan, Sos Agaian, C. L. Philip Chen, "A Novel Latin Square Image Cipher", IEEE transactions on information forensics and security, 2012.

[8] Narendra Singh, Aloka Sinha, "Chaos based multiple image encryption using multiple canonical transforms", Optics & Laser Technology 42 (2010) 724–731.

[9] Xiaogang Wang, Daomu Zhao, "Multiple-image encryption based on nonlinear amplitude-truncation and phase-truncation in Fourier domain", Optics Communications 284 (2011) 148–152.

[10] Xiaopeng Deng, Daomu Zhao, "Multiple-image encryption using phase retrieve algorithm and intermodulation in Fourier domain", Optics & Laser Technology 44 (2012) 374–377.

[11] M.Z. He, L.Z. Cai, Q. Liu, X.C. Wang, X.F. Meng, "Multiple image encryption and watermarking by random phase matching", Optics Communications 247 (2005) 29–37.

[12] Xiaogang Wang, Daomu Zhao, "Fully phase multiple-image encryption based on superposition principle and the digital holographic technique", Optics Communications 285 (2012) 4280–4284.

[13] Haozhi Zhao, JuanLiu, JiaJia, NanZhu, JinghuiXie, YongtianWang, "Multiple-image encryption based on position multiplexing of Fresnel phase", Optics Communications 286 (2013) 85–90.

[14] Qu Wang, Qing Guo, Jinyun Zhou, "Double image encryption based on linear blend operation and random phase encoding in fractional Fourier domain", Optics Communications 285 (2012) 4317–4323.

[15] Zhi Zhong, Jie Chang, Mingguang Shan, Bengong Hao, "Double image encryption using double pixel scrambling and random phase encoding", Optics Communications 285 (2012) 584–588.

[16] Alba M. Sánchez G., Ricardo Alvarez G., Sully Sánchez G, "Architecture for filtering images using Xilinx System Generator", International journal of mathematics and computers in simulation, Issue 2, Volume 1, 2007, 101-107.

[17] Ana Toledo Moreo, Pedro Navarro Lorente, F. Soto Valles, Juan Suardı´az Muro, Carlos Ferna´ndez Andre´s, "Experiences on developing computer vision hardware algorithms using Xilinx system generator", Microprocessors and Microsystems 29 (2005) 411–419.

[18] S. Allin Christe, Mr.M.Vignesh, A.Kandaswamy, "An efficient fpga implementation of MRI Image filtering and tumor Characterization using Xilinx System Generator", International Journal of VLSI design & Communication Systems (VLSICS) Vol.2, No.4, December 2011, 95-109.
[19] V.Elamaran, Angam Praveen, Medapati Srinivasa Reddy, Lanka Venkata Aditya, Kunta Suman, "FPGA implementation of Spatial Image Filters using Xilinx System Generator", Procedia Engineering 38 (2012) 2244-2249.

Panduranga H T
Pursuing his Ph.D in Dept. of studies in Electronics, University of Mysore and received his M.Tech degree in Digital Electronics and communication systems from Visvesvaraya Technological University, Belagaum, Karnataka, India. His research interests are related to Image security and Partial image encryption. He has published research papers at national and international journals, conference proceedings.

Dr. Naveenkumar S K
He received his Ph.D from University of Mysore. He is a Associate Professor at the Department of Studies in Electronics, University of Mysore - Hassan, karnataka. His research interests are related to Nano technology, Nano materials and Image security. He has published research papers at national and international journals, conference proceedings as well as chapters of books.

Sharath Kumar H S
Puseving Ph.D in dept of studies in Electronics. He received his M.Sc from Kuvempu University in 2009. He has published research papers at international journals, conference proceedings.