FPGA Hardware Co-Simulation of Image Encryption using Hybrid Chaotic Maps Based Stream Cipher

Fadhil Sahib Hasan, Maryam Amer Saffo

Abstract*: In This paper, new model of image encryption is designed. This model using stream cipher based on finite precision chaotic maps. The model designed in efficient way by using Xilinx System Generator (XSG). Pseudo Random Bit Generator (PRBG) depends on chaotic maps is proposed to design Fixed Point Hybrid Chaotic Map-PRBG (FPHYBCM-PRBG). National Institute of Standards and Technology (NIST) randomness measures tested the randomness of the proposed FPHYBCM-PRBG system. The security analysis, such as histogram, correlation coefficient, information entropy, differential attack (NPCR and UACI) are used to analyze the proposed system. Also, FPGA Hardware Co-Simulation over Xilinx SP605 XC6SLX45T provided to test the reality of image encryption system. The results show that FPHYBCM-PRBG is suitable for image encryption based on stream cipher and outperform some encryption algorithms in sufficient way to enhance the security and robust against brute force attack with low maximum frequency and throughput.

Keywords*: Image encryption. Chaotic Maps. Fixed point representation. Stream cipher. Xilinx system generator. FPGA hardware co-simulation.

I. INTRODUCTION

In the last years, the communication technologies like mobiles and internet networks have rapidly evolved and the domain of information transmission is extended. However, this area presents new challenges for saving and exchanging multimedia messages from unauthorized eavesdropping when transmit it. Therefore, to make the transmission secure over the internet, the multimedia messages such as images and videos must have encrypted to avoid attacks from unauthorized parties. Different techniques were proposed transmit data securely and also to identify the important levels of security depending on the purpose of the communication. Traditional encryption types have lower efficient in securing images by using encryption systems and they have some drawbacks and weakness in high stream data encryption [1]. To make the transmission of data over the internet secure, encryption of image must be designed in efficient way with low complexity and high security [2].

The use of chaotic system in cryptography to encrypt images has occurred as a potential solution for many security problems because chaotic systems have many advantages for random characteristics like sensitive dependence on initial-conditions and parameter settings, simple design and has an aperiodic signal which make it suitable choice for cryptography system [3].

In the last years, researchers developed variety image encryption algorithms. These algorithms have been designed using chaotic system techniques to encrypt images. Because of chaotic systems have many sensitive properties and show better performance than traditional encryption techniques (e.g., DES [4], and AES [5]), many researchers aimed to implement encryption models to encrypt images with chaotic maps [6], [7]. Amin et al. [8], designed an image encryption system by using chaotic block cipher, this work used chaotic system to encrypt 256 block bits of plain image. Abd Al-Latif et al. [9], increased the security and the key-space of the encryption system by combining chaotic systems with Linear Feedback Shift Register(LFSR) as permutation based on hybrid domain. Zhang and Liu [10], designed a system based on skew-tent map and permutation-diffusion-algorithm to enhance the security and the key space of the encryption system. Zhu et al. [11], added the compression with encryption techniques in which the original image is firstly shuffled using 2D-hyper-chaotic-discrete design, then Chinese-remainder-theorem is utilized to encrypt and compress the pixels of image. Also, Zhang et al. [12], design an image encryption system by using circular substitution box with key stream buffer. Tang et al. [13], divided the original image into overlapping blocks, conducted random block shuffling, and exploited Arnold transform and a chaotic map to generate secure matrix for block-wise encryption. By the same researchers but another study, Tang et al. [14], proposed Multiple-image encryption using Henon map, Logistic map and bit-plane decomposition, this algorithm can convert four gray-scale images into an encrypted PNG image.

For encrypt colour image, Chai et al. [15], proposed an encryption algorithm by recombined the 24 bit planes of the colour image channels red, blue, and green into four bit planes to make these components effected by each other.

Revised Manuscript Received on March 17, 2020.

Fadhil Sahib Hasan, Electrical Engineering Department, Mustansiriyah University, Baghdad, Iraq. Email: fadel_sahib@uomustansiriyah.edu.iq .

Maryam Amer Saffo, Computer Engineering Department, Al-Farabi University College, Baghdad, Iraq. Email: maryam.saffo@alfarabiuc.edu.iq.

They used SHA 256 of the original image with memristive-hyper-chaotic model to generate streams of pseudorandom key and its initial values. Li et al. [16], design a quantum colour image encryption system by combining various chaotic maps using XOR operation. One and more chaotic systems are combined together to improve the security and key space for image encryption system.

Wang et al. [17], proposed an encryption model by combining Logistic and Kent maps to generate two sub-matrices, then generate a combined matrix by XORing it with the original pixels. The results indicate that the proposed model with large key-space. Parvaz and Zarebnia [18], combined chaotic maps like logistic and sine maps with tent map to propose a model to encrypt images.

In other words, Wu et al. [19], proposed new image encryption system by hybrid pixel diffusion using DNA approach and pixel permutation using a two-dimensional Henon-Sine map. This system is robust against statistical, differential and noise attacks. Hayata and Azamb, [20], proposed a valuable image encryption technique by using a dynamic S-box and pseudo-random numbers over an elliptic curve. This technique is robust to known and chosen plaintext attacks. Tang et al. [21], designed double spiral scans with chaotic maps for image encryption algorithm. A key contribution is the double spiral scans, which can efficiently scramble pixels of image block with good encryption performance comparing with some popular image encryption algorithms.

In systems of digital-signal-processing, FPGA has become a main system for implementation in high-performance system especially in image processing applications. Also FPGA has the capability to implement highly signal processing system performances with high speed designs [22]. In other words, Xilinx system generator (XSG) makes FPGA more power and adds efficient tools to design an image encryption models in comfortable way which it is work with MATLAB/Simulink in friendly. In the last years, different researches implemented image encryption systems using FPGA techniques. Leong et al. [23], implement the output of the image encryption algorithm on the Altera Cyclone II Development board besides, this implementation aimed to be fabricated into integrated circuit chip to be used in handheld gadgets in today's highly technology-dependent society. Baruah and Saikia [24], proposed a new chaotic map based two levels image encryption/decryption scheme in hardware implementation using Verilog-code combined with an external secret key of 48-bit. Two chaotic maps, namely Arnold Cat Map and 3D Logistic Map are used in two levels confusion level and diffusion level. Yang and Huang [25], implemented a 3D chaotic image encryption system based on FPGA DE2-115 board and the cipher image can be stored by the SD card device. Abdullah and Abdullah [26], proposed a colour image encryption system based on a new chaotic map simulated via Matlab then the system is implemented over Cyclone V FPGA kit.

In this paper, a chaotic map like lozi map is combined with tent map that is used as permutation to get Pseudo Random Bit Generator (PRBG) named Fixed Point Hybrid Chaotic Map-PRBG (FPHYBCM-PRBG). This combination is designed to implement an image encryption model based on stream cipher in sufficient way to enhance the security. The New design of PRBG based on finite precision chaotic maps is presented and designed using Xilinx System Generator (XSG). The proposed FPHYBCM-PRBG is implemented in efficient way in XSG and applied for image encryption system. Fixed point is used to decrease the complexity of the chaotic encryption system and hence enhanced the maximum frequency, throughput and worst delay time of the system. Finally, FPGA hardware co-simulation is used to test the time reality of the proposed system.

The rest of the paper can be organized as follows: Sect. 2 describes fixed point chaotic maps based PRBG that are including PRBG based on fixed point lozi map, Tent map, and hybrid maps. In Sect. 3, FPGA platform of image encryption is performed. Sect. 4 represents the randomness tests of the proposed PRBG. In Sect. 5, presents the performance and security analysis of the proposed model. Next, Sect. 6 which design the FPGA hardware co-simulation of image encryption based on fixed point chaotic maps. Finally, the conclusion of this paper is given in Sect. 7.

II. FIXED POINT CHAOTIC MAPS BASED PRBG

Figure 1 shows the general structure of fixed point chaotic map based PRBG (FPCM-PRBG). In the first, the initial value X_o and Y_0 with N bits are derived into the digitization functions $X_{n+1} = f(X_n, Y_n)$ and $Y_{n+1} = g(X_n, Y_n)$, where X_{n+1} and Y_{n+1} are the next state values of chaotic map functions. The sample of X_n is finite precision format with N bits length, $X_n = (b_1, b_2, .., b_N)_2, b_j \in \{0,1\}$. The fixed point format is designed with word length (WL)=32 bits that is found to be the best choice to obtain chaotic signal. The N bits are then passes through slicing function to select M bits which is the least significant eight bits and converting it to serial bits using parallel to serial converter. Here M=8 bits that is suitable to synchronize with plain image. Figure 2 shows the slicing function. The purpose of select the least significant bits (LSBs) is the high randomness bits are existing in these bits compared with the most significant bits (MSBs). In this section, cryptographic PRBG based on combination of chaotic lozi map and tent map (as permutation) are introduced. The reason of selection these maps is the simplicity and efficiently performance in image encryption.

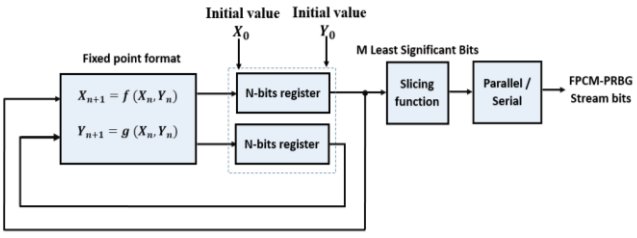


Fig. 1. General structure of FPCM-PRBG.

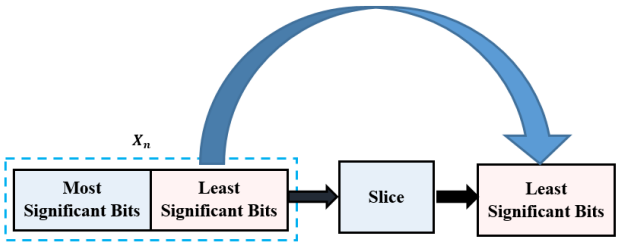


Fig. 2. Slicing Function.

A. Chaotic Lozi Map

This chaotic map presents a simple two-dimensional map [27] as given in Eq. (1):

$$X_{n+1} = 1 - \alpha|X_n| + Y_n$$
$$Y_{n+1} = \beta X_n \qquad (1)$$

where α and β are the control parameters of lozi map and X_n is an initial variable. XSG is used to implement Eq. (1) and apply to the system in Figure 1 to produce Fixed Point Lozi Map-PRBG (FPLM-PRBG). The parameters of fixed point presentation for this map are the integer length (IL)=4 bit and the fraction length (FL)=28 bits. The value of α=1.4 and β =0.3.

B. Chaotic Tent Map

In mathematics, Tent map is an iterated function, in the figure of a tent forming a discrete-time dynamical system. It takes a point X_n on the real line and maps it to another point as written in Eq. (2), [28].

$$X_{n+1} = \begin{cases} \mu X_n & \text{for } X_n < \frac{1}{2} \\ \mu(1 - X_n) & for \ \frac{1}{2} \le X_n \end{cases} \qquad (2)$$

where μ is a positive real constant (here equals 0.5) and X_n is the state variable. Depending on the value of μ, the tent map demonstrates a range of dynamical behavior ranging from predictable to chaotic. XSG is used to implement Eq. (2) and apply to the system in Fig. 1 to produce Fixed Point Tent Map (FPTM). The parameter of fixed point presentation for this map are the integer length (IL)=4 bit and the fraction length (FL)=28 bits.

C. Fixed Point Hybrid Chaotic Map Based PRBG

In this subsection, we proposed a new version of cryptographic PRBG can be generated by combined tent chaotic map as permutation with lozi chaotic map. Each chaotic maps are designed using XSG with fixed point presentation as mentioned before. Figure 3 shows the proposed subsystem block diagram of Fixed Point Hybrid Chaotic Map based on Pseudo Random Bit Generator (FPHYBCM-PRBG) to design FPHYBCM-sub-PRBG.

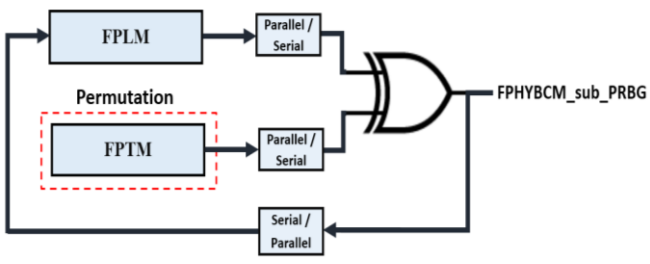


Fig. 3. FPHYBCM-sub-PRBG system.

Figure 4 shows the final design of our proposed system by combining two FPHYBCM-sub-PRBG systems with same parameters and component but with different initial values x_0 and y_0. The combination is occurred by using XOR operation between FPHYBCM-sub01-PRBG and FPHYBCM-sub02-PRBG to obtain FPHYBCM-PRBG.

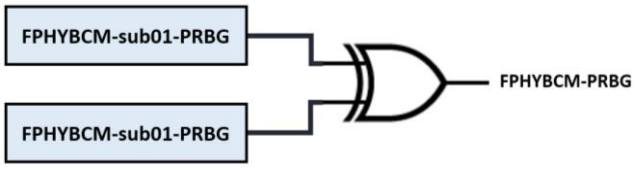


Fig. 4. FPHYBCM-PRBG proposed system.

III. FPGA PLATFORM OF IMAGE ENCRYPTION

The general XSG block diagram of the proposed image encryption is shown in Fig. 5. SP605 FPGA board is used with clock frequency of 27 MHz. The XSG functions gateway-in and gateway-out are used to convert from Simulink/Matlab to XSG environment and from XSG to Simulink/Matlab environment in respectively. The system consists of encryption and decryption stages. The source colour image is separated into red, green, and blue images. The data type of this image is Unint8 format. In the first of encryption stage, the original image, I ∈ $L_r \times L_c$ dimension, (where L_r is row numbers and L_c is column numbers) is converted to serial samples using pre-processing block. Figure 6 shows the pre-processing block which contains the following Matlab/Simulink blocks: *Transpose*, *Reshape*, *to-frame*, *Unbuffer* blocks. Pre-processing block used to convert the matrix I into serial samples of 8 bits (Unit8). The gateway-in is used to convert the format of serial sample to unsigned fixed point format with WL=8 and FL=0. Then serial bits are obtained using parallel to serial converter that is XORed with any type of PRBG based on chaotic map to produce the ciphered message. In the decryption stage, the same PRBG key is used to recover the original stream bits that are passing through serial to parallel converter and back to Matlab/Simulink environment using gateway-out. To recover the original plain image with the same size, post-processing block is used to convert the serial sample to original size ($L_r \times L_c$). Figure 7 shows the post-processing block which contains the following Matlab/Simulink blocks: *Buffer*, *Reshape*, *Transpose* and *Unit8* blocks.

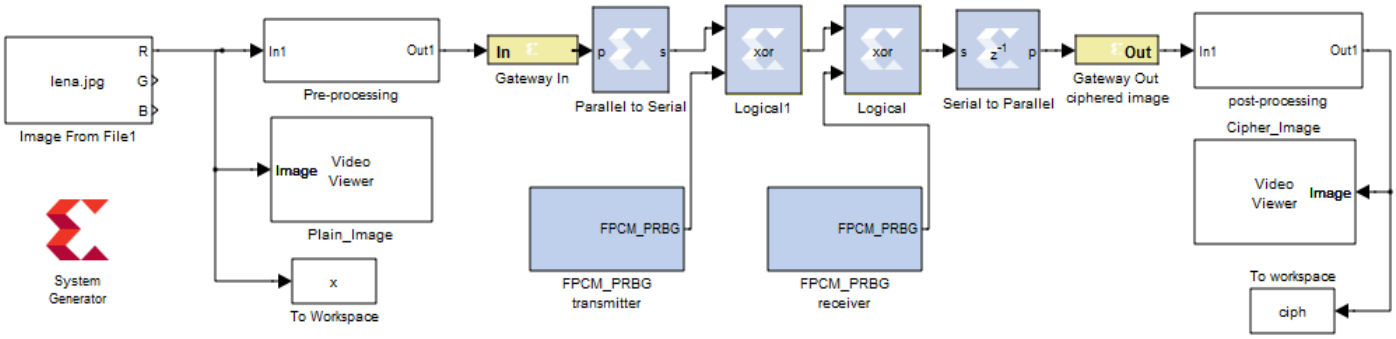


Fig. 5. General XSG block diagram of the proposed image encryption system.

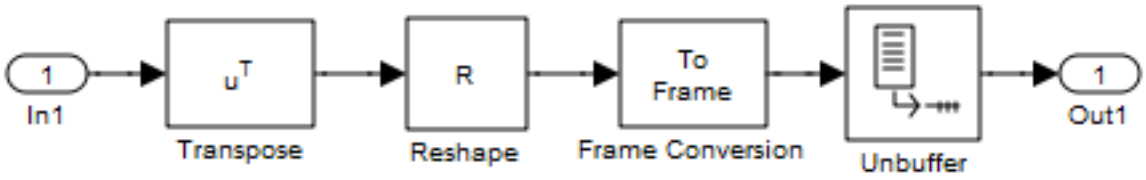


Fig. 6. Pre-processing Simulink block.

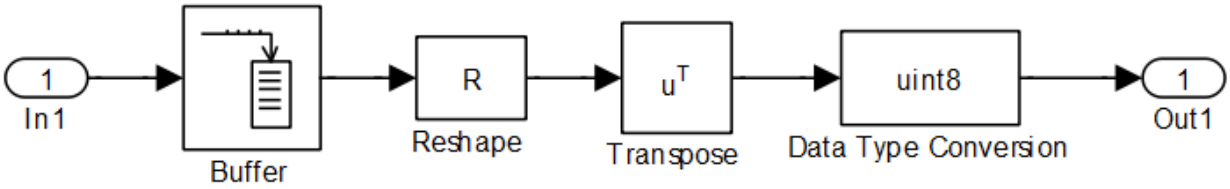


Fig. 7. Post-Processing Simulink block.

A. XSG based Fixed Point Chaotic Maps-PRBG

For both fixed point chaotic maps including FPLM and FPTM, fixed point representation with WL=32 bits and FL=28 bits are used. Also, the initial values of FPLM and FPTM in FPHYBCM-sub01-PRBG system are ($\alpha = 1.4, \beta = 0.3, x_0 = 0.5271427, y_0 = 0.4574243$), and ($\mu = 0.5, x_0 = 0.5271456$) respectively. In FPHYBCM-sub02-PRBG system the initial values of FPLM and FPTM are ($\alpha = 1.4, \beta = 0.3, x_0 = 0.7279423, y_0 = 0.6578243$), and ($\mu = 0.5, x_0 = 0.8271428$) respectively. The implementation of FPLM, FPTM, FPHYBCM-sub-PRBG, and FPHYBCM-PRBG using system generator are illustrated in Figures (8-11) respectively. Figure 12 shows single pulse system generator block which is used to control the initial values in these systems.

IV. RANDOMNESS TEST RESULTS

The National Institute of Standards and Technology (NIST) [29] are utilized to examine the randomness of proposed FPHYBCM-PRBG. There are 15 tests in NIST measures among all the most popular tests include; Frequency, Block Frequency, Runs, Rank, Discrete Fourier Transform (DFT), Serial, Cumulative-Sums and Auto correlation tests. The generator random bits are successful passing the tests if P-value≥0.01 for all tests, where P-value is the threshold that is used to accept or refuse the random bits.

These tests have better randomness if a P-value for a test is equal to 1. A P-value of zero indicates that the sequence appears to be completely non-random. The P-values of the randomness tests for FPHYBCM-PRBG are shown in Table I.

Table- I: NIST suite tests for the proposed PRBG.

No.	P-Value of Randomness Tests/ Test name	FPHYBCM-PRBG
1.	Frequency	0.6055
2.	Block-Frequency	0.2283
3.	Runs Test	0.3107
4.	Rank	0.2918
5.	DFT	0.5164
6.	Serial	0.7890
7.	Cumulative-Sums	0.9439
8.	Auto Correlation	0.9999

V. PERFORMANCE AND SECURITY ANALYSIS

Different analysis are presents to test the performance and the security of the proposed design including histogram, Correlation Coefficient Analysis(CCA), information entropy, key space and differential analysis attack. The analysis in this section is applied for a different size of colour images. Experiments are carried out and the data are analyzed using Simulink/Matlab and XSG environment.

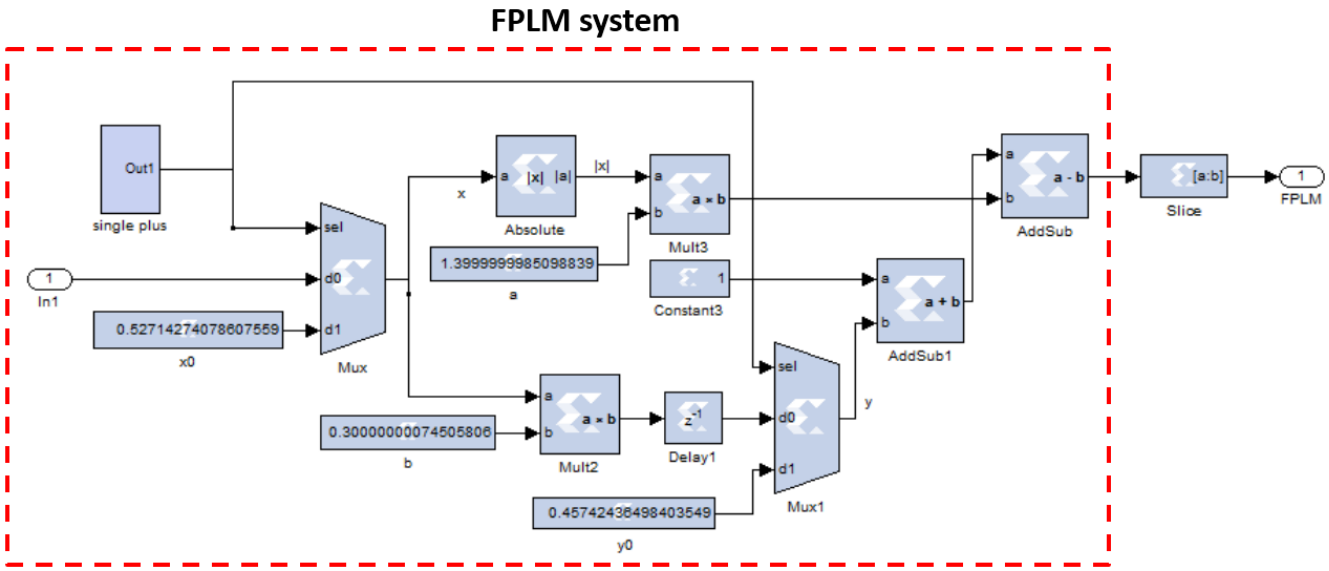


Fig. 8. XSG block diagram of FPLM.

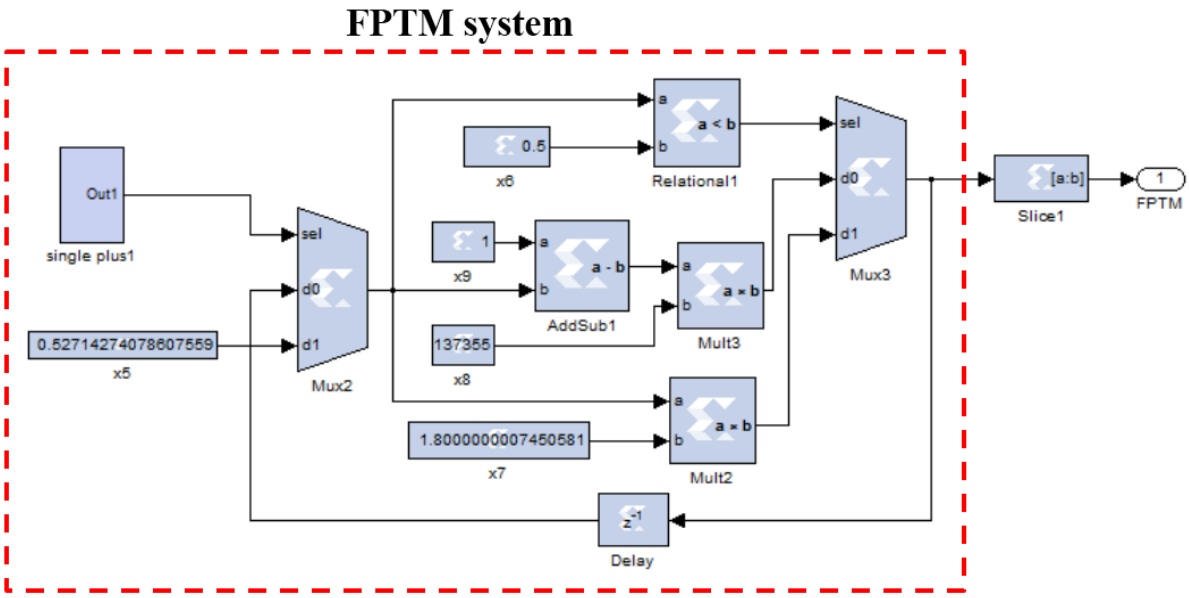


Fig. 9. XSG block diagram of FPTM.

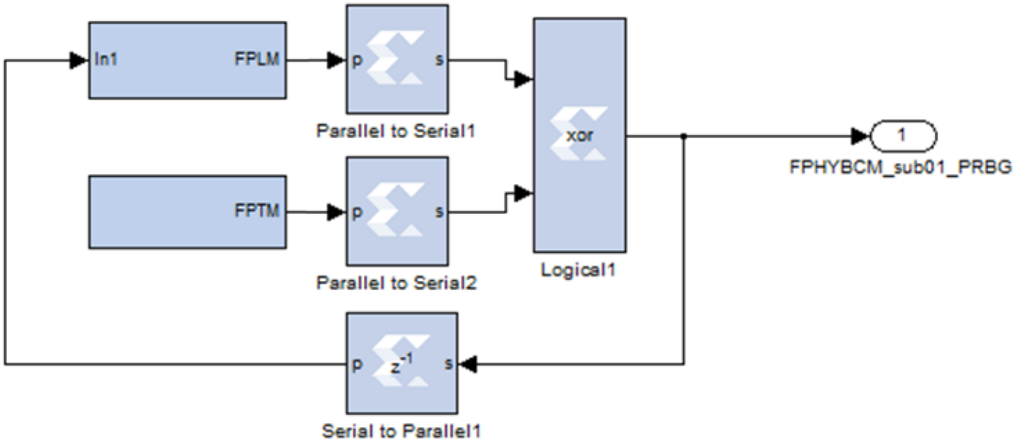


Fig. 10. XSG block diagram of FPHYBCM-sub-PRBG.

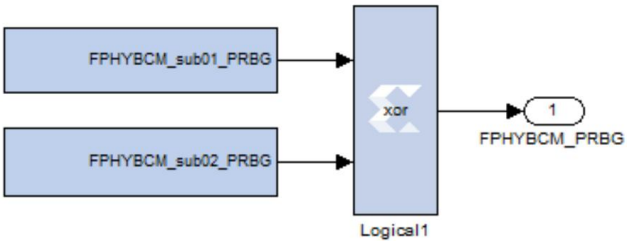


Fig. 11. XSG block diagram of FPHYBCM-PRBG.

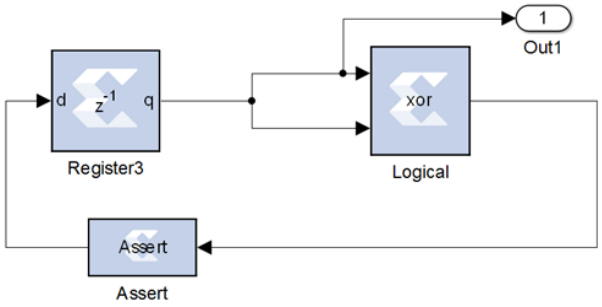


Fig. 12. XSG block diagram of single pulse block.

A. Histogram Analysis

The histogram analysis represents the distribution of all pixel values. In general, the distribution pixels of the original plain image are very uneven, and some pixel values have a high frequency in the plain Image. Therefore, it is capable of exploitation. In order to resist the attacks, the encryption system should make the cipher image distributed as much as possible to prevent the cipher image to be attacked. Figure 13 (a), shows the original colour image, Lena.jpg, with size 256×256, and Fig. 13 (b), (c), and (d) show the histogram of red, green, and blue channels of the original image respectively, while Fig. 14 (a) shows the ciphered Lena image using FPHYBCM-PRBG system. The histogram of three RGB channels of this ciphered image is shown in Fig. 14 (b), (c), and (d) respectively, which are balance and excellent histograms distribution.

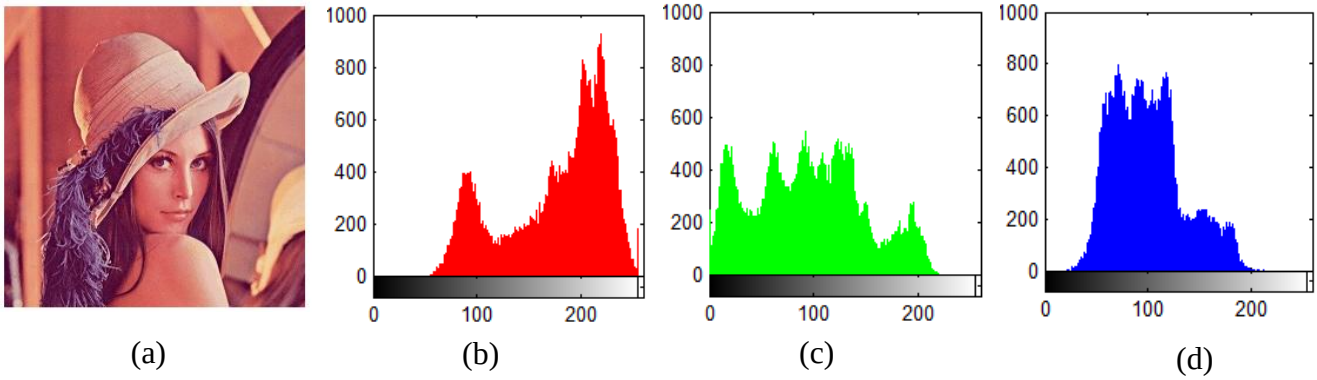


Fig. 13. Original image. (a) Original image of Lena size 256 x 256, (b) Histogram of red channel of Lena, (c) Histogram of green channel of Lena, (d) Histogram of blue channel of Lena.

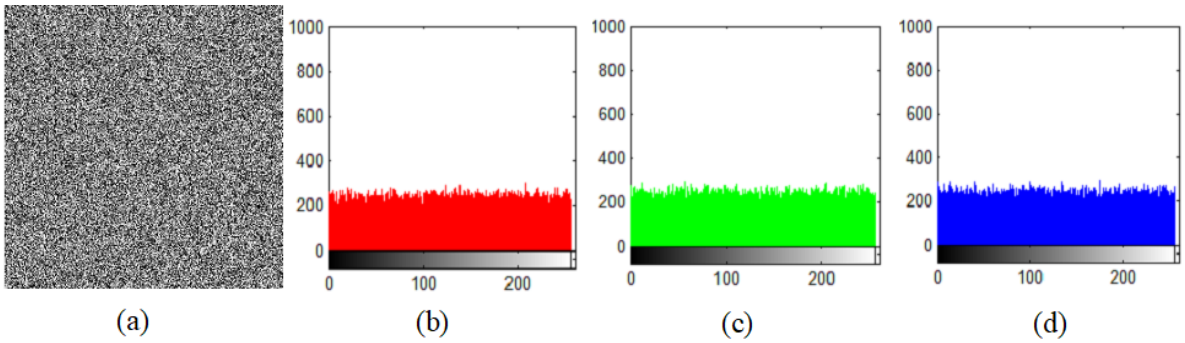


Fig. 14. Image encryption by using FPHYBCM-PRBG. (a) Ciphered image, (b) Histogram of ciphered image red channel, (c) Histogram of ciphered image green channel, (d) Histogram of ciphered image blue channel.

B. Correlation Coefficient Analysis (CCA)

CCA is widely used as statistical measure between the original and the ciphered images. An image encryption algorithm is said to be good, if it hides all the attributes of a plain image and the encrypted image is totally random and highly uncorrelated. If the correlation coefficient =1, then the two images are identical. So in this cases the encryption fails. When its value = -1, the encrypted image is totally opposite of the plain image. To calculate the correlation coefficient of any colour values of two pixels in the same position in the original and cipher images, the pixel correlation in horizontal, vertical, and diagonal directions can be calculated by the Eqs. (3-5), [30-31].

$$CorCoef = \frac{Covar(x,y)}{\sqrt{Vari(x)} \times \sqrt{Vari(y)}} \quad (3)$$

$$Vari(x) = \frac{1}{N}\sum_{i=1}^{N}[(x_i - E(x))^2] \quad (4)$$

$$Covar(x,y) = \frac{1}{N}\sum_{i=1}^{N}[(x_i - E(x)) \times (y_i - E(y))] \quad (5)$$

where *CorCef* is the correlation coefficient between x and y, *Vari(x)* is the variance of the original image *x*, *Covar(x,y)* is the covariance between *x* and *y*, *E(x)* is expected value operator and *N* is total number of pixels in image matrix.

The experimental values of pixels correlation for different test images are shown in Tables II and III for Lena image with size 256×256 and 1024×1024 respectively to make comparison on the correlations between the FPLM-PRBG, FPTM-PRBG, and our proposed chaotic system FPHYBCM-PRBG. Tables IV and V show comparative study of correlation coefficient for 512×512 ciphered Lena image between our system FPHYBCM-PRBG and other conventional systems like: [33], [25], [32], [17], and [15].

Table- II: Comparative study of the correlation coefficient of Lena image sized 256 x 256 with different channels and chaotic maps system.

Channels		FPLM-PRBG	FPTM-PRBG	FPHYBCM-PRBG
Red	Horizontal	9.23006e-005	5.75746e-004	-0.00325
	Vertical	0.00172	0.00149	-0.00479
	Diagonal	8.30834e-005	0.00264	-0.00394
Green	Horizontal	-0.00268	-0.00508	-0.00490
	Vertical	-0.00251	-0.00424	-0.00474
	Diagonal	-0.00141	-0.00387	-0.00468
Blue	Horizontal	-0.00162	-0.00323	-0.00295
	Vertical	4.30088e-005	-0.00211	-0.00323
	Diagonal	3.91790e-004	-0.00274	-0.00291

Table- III: Comparative study of the correlation coefficient of Lena image sized 1024 x 1024 with different channels and chaotic maps system.

Channels		FPLM-PRBG	FPTM-PRBG	FPHYBCM-PRBG
Red	Horizontal	7.99736	7.99709	7.99740
	Vertical	7.99733	7.99711	7.99741
	Diagonal	7.99735	7.99709	7.99739
Green	Horizontal	7.99690	7.99730	7.99732
	Vertical	7.99693	7.99730	7.99737
	Diagonal	7.99691	7.99734	7.99732
Blue	Horizontal	7.99698	7.99658	7.99762
	Vertical	7.99692	7.99657	7.99759
	Diagonal	7.99692	7.99656	7.99761

Table- IV: Comparative study of correlation coefficient of Lena 512 x 512 ciphered image for different directions between our system and known systems.

Channels		FPHYBCM-PRBG (our proposed)	Ref. [33]	Ref. [25]
Red	Horizontal	-0.0022	0.0033	3.8×10^{-4}
	Vertical	-0.0015	0.0155	1.9×10^{-3}
	Diagonal	-0.0017	0.0158	4.1×10^{-5}
Green	Horizontal	-0.0017	0.0294	-4.9×10^{-4}
	Vertical	-8.398e-004	0.0146	2.3×10^{-3}
	Diagonal	-0.0011	0.0102	-3.4×10^{-3}
Blue	Horizontal	8.445e-004	0.0086	-1.1×10^{-3}
	Vertical	0.0013	-0.0229	-1.1×10^{-3}
	Diagonal	0.0013	-0.0366	-1.2×10^{-3}

Table- V: Comparative study of correlation coefficient of Lena 512 x 512 ciphered image between our system and known systems.

Channels	FPHYBCM-PRBG (our proposed)	Ref. [32]	Ref. [17]	Ref. [15]
Red	-0.001495	0.000626	0.0027	-0.0031
Green	-8.232667e-004	0.000021	-0.0019	0.0160
Blue	0.000145	-0.000475	0.0003	-0.0190

C. Information Entropy Analysis

Another security measure is the information entropy analysis that is often used to describe the uncertainty or randomness of an image. The information entropy of the signal *s* is expressed as [34].

$$Entrp(s) = \sum_{n=0}^{2^N-1} P(s_i) \times \log_2\left(\frac{1}{P(s_i)}\right) \quad bits \quad (6)$$

where $P(s_i)$ is the symbol s_i probability, N is The bits number, which representing the basic unit of the sources s and 2^N is all the combinations of the basic unit.

Tables VI and VII show the Information Entropy comparative study of Lena Image with size of 256×256 and 1024×1024 respectively for different channels and chaotic map systems. Table VIII shows the comparative study of Information Entropy of ciphered Lena image with size 512 × 512 of our system FPHYBCM-PRBG and other known systems such as: [32], [25], [17], and [15].

Table- VI: Comparative study of the information entropy of Lena image sized 256 x 256 with different channels and chaotic maps system.

Table- VII: Comparative study of the information entropy of Lena image sized 1024 x 1024 with different channels and chaotic maps system.

Channels		FPLM-PRBG	FPTM-PRBG	FPHYBCM-PRBG
Red	Horizontal	7.99980	7.99980	7.99980
	Vertical	7.99980	7.99980	7.99980
	Diagonal	7.99980	7.99980	7.99980
Green	Horizontal	7.99981	7.99980	7.99982
	Vertical	7.99981	7.99980	7.99982
	Diagonal	7.99981	7.99980	7.99982
Blue	Horizontal	7.99980	7.99973	7.99982
	Vertical	7.99980	7.99973	7.99981
	Diagonal	7.99980	7.99973	7.99981

Table- VIII: The information entropy comparison of Lena ciphered image sized 512 x 512 between our system and known systems.

Channels	FPHYBCM-PRBG (our proposed)	Ref. [32]	Ref. [25]	Ref. [17]	Ref. [15]
Red	7.99933	7.99932	7.99930	7.9974	7.9993
Green	7.99934	7.99932	7.99921	7.9969	7.9993
Blue	7.99939	7.99927	7.99933	7.9884	7.9993

D. Key Space Analysis

In cryptography, the larger key space, the more secure algorithm, and also the stronger ability to resist brute force attacks [21] and [35]. The key space of lozi and tent maps and our proposed algorithms are listed in Table IX. The parameter settings and initial values of each chaotic maps required 32 bits and hence the key space of the proposed algorithm is 2^{384}. Therefore, this key is effective key against brute force attack since is greater than 2^{100} [36]. By comparison, the key space of our proposed design is better than last encryption algorithm's key space like: [17], [37], [38], [39], and [40] as listed in Table X.

Table- IX: Key spaces of chaotic maps and our proposed system.

Chaotic Maps	Parameters	Key Space
FPLM-PRBG	α, β, x_0, and y_0	$(2^{32})^4 = 2^{128}$
FPTM-PRBG	μ, and x_0	$(2^{32})^2 = 2^{64}$
FPHYBCM-PRBG (our proposed)	$(\alpha_1, \beta_1, x_{01}, y_{01}, \mu_1, x_{01}, \alpha_2, \beta_2, x_{02}, y_{02}, \mu_2, and\ x_{02})$	$(2^{32})^{12} = 2^{384}$

Table- X: Key space comparisons.

Encryption Algorithms	Key Space
FPHYBCM-PRBG (our proposed)	2^{384}
Ref. [17]	10^{45}
Ref. [37]	2^{199}
Ref. [38]	2^{203}
Ref. [39]	2^{149}
Ref. [40]	2^{200}

E. Differential Attack Analysis

The attackers try to find out a relationship between the plain image and the encrypted image, by making an infinitesimal change between two identical plain images for example change only one pixel for two images, and observes the corresponding ciphered images. Wherefore, Chen et al. [41], used two measurements Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) for this purpose which measures the average intensity of differences between the two images. The NPCR and The UACI measures can be presented as [41]:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad (7)$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \quad (8)$$

Where W is width and H is height of the ciphered image. C_1 is the encrypted image and if one pixel is changed of C_1 in random, the ciphered image C_2 is obtained. $D(i, j)$ is given by [41]:

$$D(i,j) = \begin{cases} 0 & if\ C_1(i,j) = C_2(i,j) \\ 1 & otherwise \end{cases} \quad (9)$$

Tables XI and XII show NPCR test comparisons between different channels and chaotic map systems for Lena Image sized 256×256 and 1024×1024 respectively. The comparative study of NPCR between our proposed system FPHYBCM-PRBG and other systems is listed in Table XIII which shows that NPCR of our proposed system is better than other systems like [32], [25], and [15]. Tables XIV and XV show UACI test comparison between different channels and chaotic map systems for Lena Image sized 256×256 and 1024×1024 respectively.

Table- XI: NPCR test comparison between different channels and chaotic maps system for Lena Image with size 256×256.

Channels		FPLM-PRBG	FPTM-PRBG	FPHYBCM-PRBG
Red	Horizontal	99.61550	99.59099	99.59099
	Vertical	99.65379	99.62316	99.60324
	Diagonal	99.57093	99.61399	99.57862
Green	Horizontal	99.61550	99.59099	99.59099
	Vertical	99.59865	99.65533	99.60018
	Diagonal	99.58323	99.61707	99.60938
Blue	Horizontal	99.61550	99.59099	99.60019
	Vertical	99.59252	99.59712	99.60631
	Diagonal	99.55247	99.63091	99.64475

Table- XII: NPCR test comparison between different channels and chaotic maps system for Lena Image sized 1024 x 1024.

Channels		FPLM-PRBG	FPTM-PRBG	FPHYBCM-PRBG
Red	Horizontal	99.60250	99.58245	99.61090
	Vertical	99.61452	99.59581	99.61032
	Diagonal	99.61902	99.59332	99.60870
Green	Horizontal	99.60250	99.58245	99.61090
	Vertical	99.60106	99.59916	99.60288
	Diagonal	99.61682	99.60010	99.60010
Blue	Horizontal	99.60250	99.58245	99.61090
	Vertical	99.61701	99.59935	99.61223
	Diagonal	99.63058	99.59704	99.60335

Table- XIII: NPCR test comparison for Lena Image sized 512 x 512 between our system and known systems.

Channels	FPHYBCM-PRBG (our proposed)	Ref. [32]	Ref. [25]	Ref. [15]
Red	99.635	99.627	99.5990	99.60
Green	99.636	99.631	99.5990	99.60
Blue	99.633	99.624	99.6200	99.60

Table- XIV: UACI test comparison between different channels and chaotic maps system for Lena Image with size 256× 256.

Channels		FPLM-PRBG	FPTM-PRBG	FPHYBCM-PRBG
Red	Horizontal	32.67191	32.66762	32.68546
	Vertical	32.62367	32.64601	32.63294
	Diagonal	32.65147	32.63513	32.57193
Green	Horizontal	31.21738	31.15879	31.15090
	Vertical	31.20101	31.15448	31.16047
	Diagonal	31.20138	31.14090	31.17428
Blue	Horizontal	28.16832	28.05184	28.15384
	Vertical	28.15306	28.02153	28.18017
	Diagonal	28.14499	28.03877	28.16424

Table- XV:UACI test comparisons between different channels and chaotic maps system for Lena Image with size 1024×1024.

Channels		FPLM-PRBG	FPTM-PRBG	FPHYBCM-PRBG
Red	Horizontal	32.63348	32.53004	32.58812
	Vertical	32.63167	32.53197	32.58834
	Diagonal	32.63182	32.53111	32.58834
Green	Horizontal	31.09172	30.93597	31.06013
	Vertical	31.09301	30.93863	31.06079
	Diagonal	31.09155	30.93712	31.06086
Blue	Horizontal	27.96807	27.81537	27.96813
	Vertical	27.96892	27.81638	27.97270
	Diagonal	27.96903	27.81538	27.96909

VI. FPGA HARDWARE CO-SIMULATION OF IMAGE ENCRYPTION BASED ON FPCM

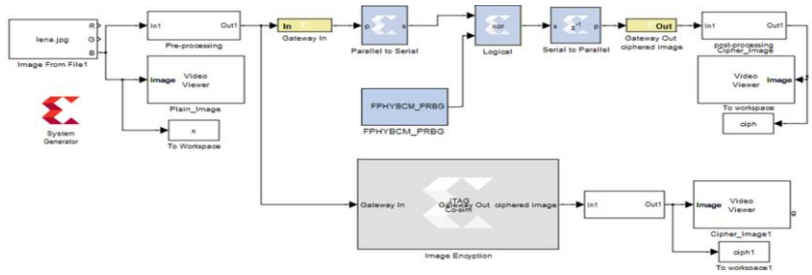
The generator instruction in system generator block can be used to obtain the VHDL code for FPCM-PRBG. The proposed system is designed using SP605 XC6SLX45T-3FGG484 evaluation board [42]. The device utilization summary for the proposed PRBG is shown in Table XVI. The throughput of the system is the amount of bits for each second and is defined as: Throughput=($f_{max} \times 8$), where f_{max} is the maximum allowed of clock frequency. From this table, it can be seen that FPHYBCM-PRBG has maximum frequency and throughput better than FPLM-PRBG, and lower than FPTM-PRBG with high security and robust against brute force attack.

FPGA hardware co-simulation of the image encryption system is depicted in Fig. 15. The serial data of the image signal transmitted to the FPGA through USB JTAG port when JTAG co-simulation link is established. Then, the serial samples output from the FPGA device is send back to the PC and test the picture using Simulink/Matlab viewer as shown in Fig. 15 (a).

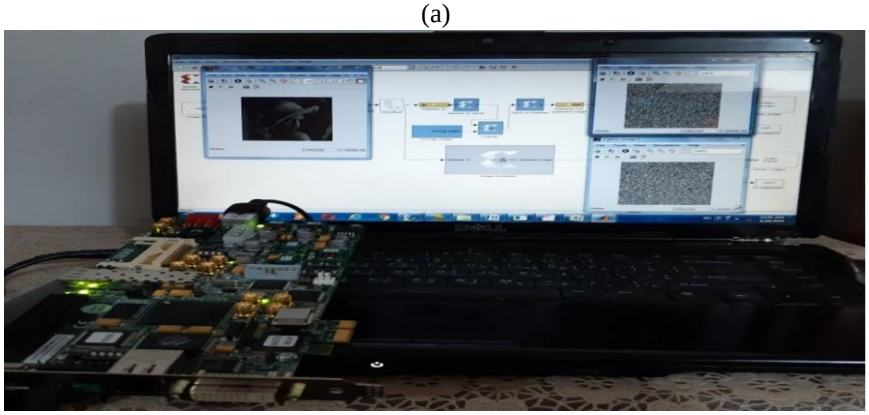
In Fig. 15 (b), the pictures on the right side represent the encryption image for the proposed system using system generator (in the top) and hardware co-simulation (in the bottom). It can be shown that the ciphered image for system generators and hardware co-simulation are the same which proved that the real time of the proposed image encryption is working correctly and matching the expected design.

Table- XVI: Device utilization summary on Xilinx Spartan XC6SLX45T.

Resource type	Available	Used		
		FPLM-PRBG	FPTM-PRBG	FPHYBCM-PRBG
Slice Registers	54,576	98	51	267
Slice LUT's	27,288	124	71	276
Occupied Slices	6,822	53	27	146
MUXCYs used	13,644	64	32	112
BUFG/BUFGMUXs	16	1	1	1
DSP48A1s	58	16	8	36
Minimum period (ns)		43.104	21.408	28.363
Maximum Clock Frequency (MHz)		23.200	46.712	35.257
Peak memory usage		320	288	445
Throughput (Mb/sec)		185.6	373.96	282.056



(a)



(b)

Fig. 15. Real time hardware Co-Simulation of the image encryption system. (a) XSG block diagram, (b) Hardware test with Xilinx Spartan XC6SLX45T kit.

VII. CONCLUSION

In this paper, a colour image encryption algorithms using chaotic maps-based stream cipher are implemented using XSG technique. The chaotic maps are converted to fixed point format and these maps are used either as alone or combined lozi map with tent map (used as permutation) by using XOR operation to generate new model of PRBG. The security analysis like, histogram, correlation coefficient, entropy, and key space analysis are determined for different sizes of Lena image, and the results are compared with previous reported systems. Also the proposed system provides the best key space, which is sensitive to slight change. The synthesis results of the FPHYBCM-PRBG show that it has maximum frequency about 35.257 MHz with throughput about 282.056 Mb/s. Finally, the real time of the proposed system is tested using hardware co-simulation via FPGA Xilinx SP605 XC6SLX45T kit.

ACKNOWLEDGMENT

This work is supported by the cooperation between the college of Engineering/ Mustansiriyah University (https://webmail.uomustansiriyah.edu.iq) and Al-Farabi University College (www.alfarabiuc.edu.iq). The experiment is established in the Lab of Electrical Engineering Department/ University of Mustansiriyah.

REFERENCES

1. Y. Cao, R. Qiu, and Y. Fu, “Color image encryption based on hyper-chaos”, IEEE 2nd International Congress on Image and Signal Processing, 2009, pp. 1-6.
2. P. Dang, and P. Chau, “Image encryption for secure internet multimedia applications”, IEEE Transactions on consumer electronics, 2000, 46(3), pp. 395-403.
3. M. Khan, “Chaotic cryptography and its applications in telecommunication systems”, Telecommunication systems, 2013, 52(2), pp. 513-514.
4. S. Banerjee, “High speed implementation of DES”, Computers & Security, 1982, 1(3), pp. 261-267.
5. N. Standard, “Announcing the advanced encryption standard (AES)”, Federal Information Processing Standards Publication, 2001, 197(1-51), pp. 3-3.
6. J. Fridrich, “Symmetric ciphers based on two-dimensional chaotic maps”, International Journal of Bifurcation and chaos, 1998, 8(06), pp. 1259-1284.
7. G. Chen, Y. Mao, and C. Chui. “A symmetric image encryption scheme based on 3D chaotic cat maps”, Chaos Solitons & Fractals, 2004, 21(3), pp. 749-761.
8. M. Amin, O. Faragallah, and A. El-Latif, “A chaotic block cipher algorithm for image cryptosystems”, Communications in Nonlinear Science and Numerical Simulation, 2010, 15(11), pp. 3484-3497.
9. A. El-Latif, X. Niu, and M. Amin, “A new image cipher in time and frequency domains”, Optics Communications, 2012, 285(21-22), pp. 4241-4251.
10. G. Zhang, and Q. Liu, “A novel image encryption method based on total shuffling scheme”, Optics communications, 2011, 284(12), pp. 2775-2780.
11. H. Zhu, C. Zhao, and X. Zhang, “A novel image encryption–compression scheme using hyper-chaos and Chinese remainder theorem”, Signal Processing: Image Communication, 2013, 28(6), pp. 670-680.
12. X. Zhang, Z. Zhao, and J. Wang, “Chaotic image encryption based on circular substitution box and key stream buffer”, Signal Processing: Image Communication, 2014, 29(8), pp. 902-913.
13. Z. Tang, X. Zhang, and W. Lan, “Efficient image encryption with block shuffling and chaotic map”, Multimedia tools and applications, 2015, 74(15), pp. 5429-5448.
14. Z. Tang, J. Song, X. Zhang, and R. Sun, “Multiple-image encryption with bit-plane decomposition and chaotic maps”, Optics and Lasers in Engineering, 2016, pp. 1-1.
15. X. Chai, Z. Gan, Y. Lu, M. Zhang, and Y. Chen, “A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system”, Chinese Physics B, 2016, 25(10), pp. 100503-100515.
16. L. Li, B. Abd-El-Atty, and A. El-Latif, A. Ghoneim, “Quantum color image encryption based on multiple discrete chaotic systems”, IEEE Federated Conference on Computer

Science and Information Systems (FedCSIS), 2017, pp. 555-559.
17. W. Wang, M. Si, Y. Pang, P. Ran, H. Wang, X. Jiang, Y. Liu, J. Wu, W. Wu, N. Chilamkurti, and G. Jeon, "An encryption algorithm based on combined chaos in body area networks", Computers & Electrical Engineering, 2018, 65, pp. 282-291.
18. R. Parvaz, and M. Zarebnia, "A combination chaotic system and application in color image encryption", Optics & Laser Technology, 2018,101, pp. 30-41.
19. J. Wu, X. Liao, and B. Yang, "Image encryption using 2D Hénon-Sine map and DNA approach", Signal Processing, 2018,153, pp. 11-23.
20. U. Hayat, and N. Azam, "A novel image encryption scheme based on an elliptic curve", Signal Processing, 2019,155, pp. 391-402.
21. Z. Tang, Y. Yang, S. Xu, C. Yu, and X. Zhang, "Image encryption with double spiral scans and chaotic maps", Security and Communication Networks, 2019, pp. 1-15.
22. B. Lakshmi, E. Kirubakaran, and T. Prabakar, "Design and Implementation of FPGA Based Dual Key Encryption", International Journal of Computer Applications, 2010, 3(3), pp. 21-27.
23. M. Leong, S. Naziri, and S. Perng, "Image encryption design using FPGA", IEEE International Conference on Electrical, Electronics and System Engineering (ICEESE), 2013, pp. 27-32.
24. B. Baruah, and M. Saikia, "An FPGA Implementation of Chaos based Image Encryption and its Performance Analysis", IJCSN-International Journal of Computer Science and Network, 2016, 5(5), pp. 712-720.
25. C. Yang, and S. Huang, "Secure color image encryption algorithm based on chaotic signals and its FPGA realization", International Journal of Circuit Theory and Applications, 2018, 46(12), pp. 2444-2461.
26. H. Abdullah, and H. Abdullah, "FPGA implementation of color image encryption using a new chaotic map", Indonesian Journal of Electrical Engineering and Computer Science, 2019, 13(1), pp. 129-137.
27. L. Merah, A. Ali-Pacha, N. Hadj-Said, B. Mecheri, and M. Dellassi, "FPGA hardware co-simulation of new chaos-based stream cipher based on Lozi map", International Journal of Eng. And Technology, 2017, 9(5), pp. 420-425.
28. G. Sathishkumar, and D. Sriraam, "Image encryption based on diffusion and multiple chaotic maps", International Journal of Network Security & Its Applications (IJNSA), 2011, 3(2), pp. 181-194.
29. A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications", NIST Special Publication, 2011, pp. 1-131.
30. M. Ahmad, M. Doja, and M. Beg, "Security analysis and enhancements of an image cryptosystem based on hyperchaotic system", Journal of King Saud University-Computer and Information Sciences, 2018, pp. 1-9.
31. M. Dridi, M. Hajjaji, and A. Mtibaa, "Hardware implementation of encryption image using Xilinx System Generator", IEEE 17th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA), 2016, pp. 772-775.
32. M. Ahmad, A. E. Solami, X. Wang, M. Doja, M. Beg, and A. Alzaidi, "Cryptanalysis of an image encryption algorithm based on combined chaos for a BAN system and improved scheme using SHA-512 and hyperchaos", Symmetry, 2018, 10(7), pp. 266-283.
33. C. Fu, G. Zhang, M. Zhu, Z. Chen, and W Lei, "A new chaos-based color image encryption scheme with an efficient substitution keystream generation strategy", Security and Communication Networks, 2018, pp. 1-13.
34. E. Rodríguez-Orozco, E.García-Guerrero, E. Inzunza-Gonzalez, O. López-Bonilla, A. Flores-Vergara, J. Cárdenas-Valdez, and E. Tlelo-Cuautle, "FPGA-based chaotic cryptosystem by using voice recognition as access key", Electronics, 2018, 7(12), pp. 414-429.
35. S. Zhu, C. Zhu, and W. Wang, "A new image encryption algorithm based on chaos and secure hash SHA-256", Entropy, 2018, 20(9),716, pp. 22-39.
36. G. Alvarez, and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems", International journal of bifurcation and chaos, 2006, 16(08), pp. 2129-2151.
37. Z. Bashir, J. Wątróbski, T. Rashid, S. Zafar, and W. Sałabun, "Chaotic dynamical state variables selection procedure based image encryption scheme", Symmetry, 2017, 9(12), pp. 312-326.
38. X. Wu, K. Wang, X. Wang, H. Kan, and J. Kurths, "Color image DNA encryption using NCA map-based CML and one-time keys", Signal Processing, 2018, 148, pp. 272-287.
39. X. Wang, X. Zhu, X. Wu, and Y. Zhang, "Image encryption algorithm based on multiple mixed hash functions and cyclic shift", Optics and Lasers in Engineering, 2018, 107, pp. 370-379.
40. M. Barakat, A. Mansingka, A. Radwan, and K. Salama, "Hardware stream cipher with controllable chaos generator for colour image encryption", IET image processing, 2014, 8(1), pp. 33-43.
41. G. Chen, Y. Mao, and C. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps", Chaos, Solitons & Fractals, 2004, 21(3), pp. 749-761.
42. Xilinx, SP605 hardware user guide, UG526 (v1.7), 2012.

AUTHORS PROFILE

Fadhil S. Hasan was born in Baghdad, Iraq in 1978. He received his B.Sc. degree in Electrical Engineering in 2000 and his M.Sc. degree in Electronics and Communication Engineering in 2003, both from the Mustansiriyah University, Iraq. He received Ph.D. degree in 2013 in Electronics and Communication Engineering from the Basrah University, Iraq. In 2005, he joined the faculty of Engineering at the Mustansiriyah University in Baghdad. His recent research activities are Wireless Communication Systems, Multicarrier System, Wavelet based OFDM, MIMO System, Speech Signal Processing, Image Signal Processing, Cryptography and Computer Security, Chaotic Modulation, FPGA and Xilinx System Generator based Communication System. Now he has been an Assist. Prof. at the Mustansiriyah University, Iraq. Email: fadel_sahib@uomustansiriyah.edu.iq

Maryam A. Saffo was born in Baghdad, Iraq in 1988. She has got her B.Sc. in Computer Engineering Techniques in 2010, and M.Sc. in Computer Engineering Techniques in 2012 at Computer Engineering Techniques department, Electrical and Electronic Technical College, Middle Technical University, Baghdad, Iraq. She worked as a lecturer in Computer Engineering Department in Al- Farabi University College, Iraq since 2013-present. She is interested in subjects: Cryptography and Computer Security, Image Processing, FPGA's and Xilinx System Generator, and Arduino Microcontroller. E-mail: maryam.saffo@alfarabiuc.edu.iq