2024, 21(5 Special Issue): 1754-1764
https://doi.org/10.21123/bsj.2024.10521
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

Design and Enhancing Security Performance of Image Cryptography System Based on Fixed Point Chaotic Maps Stream Ciphers in FPGA

Ahmed Amir Salih*[1], ***Zaid Abdulsattar Abdulrazaq***[2], ***Harith Ghanim Ayoub***[2]

[1]Department of Vocational Education, Nineveh Education Directorate, Mosul, Iraq.
[2]Northern Technical University (NTU), Mosul, Iraq.
*Corresponding Author.
ICCDA2023: International Conference on Computing and Data Analytics 2023.

Received 26/12/2023, Revised 20/04/2024, Accepted 22/04/2024, Published 25/05/2024

Abstract

Within this document, a novel system for image cryptography design utilizing fixed-point stream cipher chaotic maps is proposed. The system consists of fixed chaotic maps combined with generated 32-bit Pseudo Number (PN) all implemented using Field Programmable Gate Arrays (FPGA) through the Xilinx System Generator (XSG) environment. The most common chaotic maps-based cryptography involved in this work are Logistic, Lozi and Tent. The parameters of each type determine the key space required for decrypt the original pixel of plain image, Logistic map has one parameter r, Lozi has two parameters α and β, Tent has one parameter μ. The main idea was to combine another parameter pseudo number (PN) to increase key space, which is the main measure of security performance against brute force attack. An innovative pseudorandom bit generator (PRBG) referred to as XORing these chaotic maps were called the fixed-point cascade chaotic maps-PRBG (FPCCM-PRBG), with an eight least significant bits of 32-bit pseudo number generator (PN) this method is known as fixed point cascade chaotic maps-PNBG (FPCCM-PRNBG). The randomness of the generated keys was evaluated using the National Institute of Standards and Technology (NIST) tests, including frequency, Frequency (Mono bit) and runs test. The security performance assessed through histogram analysis, correlation coefficient analysis, information entropy, pixel changing rate, and structural similarity. Xilinx system generator is an effective tool embedded in MATLAB/SIMULINK environment utilized for the work implementation. The system implemented using co-simulation method on the ZYNQ 7000 SoC ZC702 Evaluation Kit, with a key space of 2^{288} and a throughput of 269. 32 MB/sec.

Keywords: Chaotic maps, FPGA, Image cryptography, Pseudo number, Security, Xilinx system generator.

Introduction

Today, with the high use of digitization in internet, the use of digital image is the main concern of digital environments like 5G, so its high need for protection for that image by using more confident encryption algorithms. The process of protection information from unauthorized access is known as cryptography, it is not easy for traditional cryptographic algorithms such as DES, RSA, IDEA, AES to maintain high level of security know the need of chaos system comes on [1-3]. Chaotic map is used for many

2024, 21(5 Special Issue): 1754-1764
https://doi.org/10.21123/bsj.2024.10521
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

application science fields specially in the last decades because it has a good randomness factor and also very sensitive on parameter changes, the huge randomness range of chaos enhance the cryptographic process specially for large bits like 32 or 64 fixed point parameters [4,5].

The FPGA implementation of chaotic maps [6,7] is quite simple because of the simple equations needed for them made the Xilinx System generator the suitable tool used for the design [8]. For modern stream ciphers, WEN, Heping, et al concentrates on frequency, block frequency, serial, etc. for the produced key generated by chaotic maps and histogram, correlation, entropy, pixel similarity, key space.

The main contribution of this paper is to increase security performance by increasing the key space of the image encryption/decryption by using hybrid chaos with pseudo number bits generator (PRNBG) and acceleration the process of that encryption/decryption by using FPGA through Xilinx System Generator methodology. AYUBI, Peyman, et al [9] proposed image encryption based on chaos game with pseudo random generator number generator (PRBG) with a key space 2^{232}. FPGA technique via Cyclone V GX Starter Kit FPGA platform using for Nahrain digital image encryption implementation by MA, Yunling, et al [10] produced a 2^{260} key space. ZHOU, Minjun et al in [11] presented an image encryption model to extend advanced encryption standard algorithm (AES) to enhance the algorithm ability to brute force attack with 2^{128} key space. Quantum image encryption-based Henon chaos mapping presented in [12] with 10^{-15} sensitivity level. While the key space for hybrid chaotic scheme presented in [13] was 2^{122} for fixed point chaotic parameters. RAHIMOV, Hamed et al in [14] presented digital image encryption scheme chaotic maps associated with elliptic curve AlGAMAL encryption method provided 2^{100} key space. The key space in [15] used for enhancement of image crypto system using hyper chaos was 2^{128}. FPGA in [16] used for fractional order chaotic maps for sound application with 2^{149} key space. BONNY, Talal, et al [17] proposed two main image encryption ciphers Fixed Point XOR Chaotic Map-PRBG (FPXORCM-PRBG) and Fixed-Point Cascade Chaotic Map-PRBG (FPCCM-PRBG) used for image encryption with 2^{256} key space.

Methods

Fixed Point Chaotic Maps Based PRBG

The image encryption process involves utilizing Fixed-Point Chaotic Maps (FPCMs), namely Logistic, Lozi, and Tent. The mathematical equation for the Logistic map is expressed as follows in Eq. 1 [16,17]:

$$X_n = r\, X_n\, (1 - X_n) \quad \ldots\ldots 1$$

Here, Xn represents the variable state ranging between [0-1]. The parameter 'r' lies within the interval. To implement Eq.1 and incorporate it into the system as a Fixed-Point Logistic Map Pseudo Random Bit Generator (FPLoM-PRBG) [17],Xilinx System Generator (XSG) is employed. The logistic map is set with an Integer length of 4 bits and a Fractional Length of 28 bits, while the value of r is assigned as 4 (r = 4).

The presented chaotic introduces a straightforward two-dimensional representation [12 can 19], as shown in Eq. 2 and Eq. 3:

$$X_{(n+1)} = 1 - \alpha / X_n / + Y_n \ldots\ldots 2$$

$$Y_{(n+1)} = \beta\, X_n \ldots\ldots 3$$

Here, α and β are the parameters of the Lozi map, and Xn represents the state variable. Xilinx System Generator (XSG) is employed to implement Eq. 2 and incorporate it into the system, resulting in the generation of a Fixed-Point Lozi Map Pseudo Random Bit Generator (FPLM-PRBG). For this system, the Integer length is set to 4 bits, and the Fraction Length is 28 bits. The values of α and β are assigned as 1.4 and 0.3, respectively.

In mathematical terms, the tent map represents another type of discrete time dynamic system. It maps the point Xn from the real part and plans it to another point, as described in Eq. 4 [18].

$$X(n+1) = \begin{cases} \mu Xn & \text{for } Xn < \frac{1}{2} \\ \mu(1 - Xn) & \text{for } 1/2 \le X(n) \end{cases} \quad \ldots 4$$

2024, 21(5 Special Issue): 1754-1764
https://doi.org/10.21123/bsj.2024.10521
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

In the context of the tent map, where μ is a real positive factor (set to 0.5 in this case) and Xn represents the state variable, a diverse range of dynamic behaviors is observed, ranging from computable to chaotic. To realize Eq. 4, Xilinx System Generator (XSG) is utilized, integrating it into the chaotic system to create a Fixed-Point Tent Map-Pseudo Random Bit Generator (FPTM-PRBG). The parameters for this map are consistent with the previous chaotic maps, with an Integer Length (IL) of 4 bits and a Fraction Length (FL) of 28 bits.

Proposed (FPCCM-PRNBG)

Image encryption can exhibit varying levels of randomness based on different comparisons of Fixed-Point Chaotic Maps. These chaotic maps can be combined through exclusive XOR or cascade connections to create two distinct Pseudo Random Bit Generators (PRBGs): Fixed-Point Cascade Chaotic Maps-PRBG (FPCCM-PRBG) and Fixed-Point XOR Chaotic Maps-PRBG (FPXORCM-PRBG).

To enhance the key space and randomness, this paper introduces a novel approach. It involves performing XOR operations between FPCCM-PRBG and a Pseudocode (PN) generator, resulting in the development of a new ciphering bit generator named FPCCM-PNBG. This innovative method aims to improve security performance in image encryption, as demonstrated in the following Eq. 5:

FPCCM-PRNBG= FPCCM-PRBG⊕PN ……. 5

FPGA Model of Image Encryption

The image encryption process is illustrated in Fig. 1. It involves utilizing the ZYNQ702 evaluation board, which operates at a clock frequency of 667 MHz within the encryption system, the gateway-in and gateway-out functions from Xilinx system generator are employed to facilitate data conversion between the MATLAB/SIMULINK environment and XSG (Xilinx System Generator) as well as from XSG back to MATLAB/SIMULINK, respectively. The encryption and decryption procedures are part of the system, with the input being a one-dimensional signal derived from an image. The data represented in an unsigned integer format (uint8).

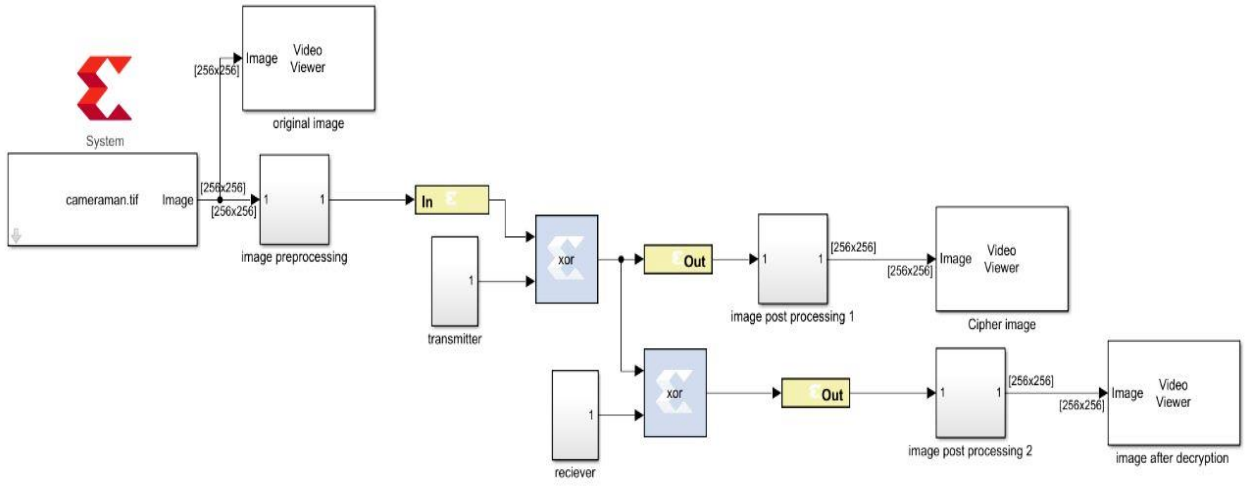

Figure 1. Block diagram of proposed image cryptography system in XSG environment.

The original image, having two dimensions (256*256), is transformed into serial samples using the image preprocessing block. This block encompasses the following SIMULINK components: "convert 2-d to 1-d" and "unbuffered." The purpose of these image preprocessing blocks is to convert the input matrix image into serial samples with an unsigned format (8-bit width). These serial samples are then XORed with the key generated by the chaotic transmitter, resulting in the Cipher image as shown in Fig. 2

2024, 21(5 Special Issue): 1754-1764
https://doi.org/10.21123/bsj.2024.10521
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

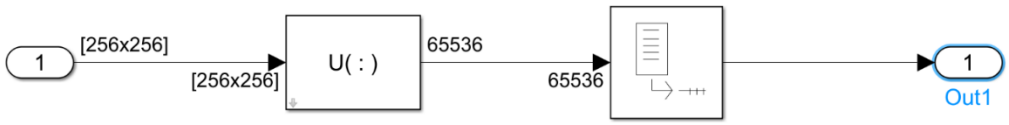

Figure 2. Preprocessing Simulink blocks.

During the decryption stage, the same XOR operation is applied, this time using the key generated from the received image. This process yields the plaintext image. However, before obtaining the original image, the plaintext image is passed through the image post-processing block, which consists of three blocks: "buffered," "reshape," and "data type conversion." These blocks serve to convert the processed samples back to the original image dimensions (256*256) shown in Fig. 3.

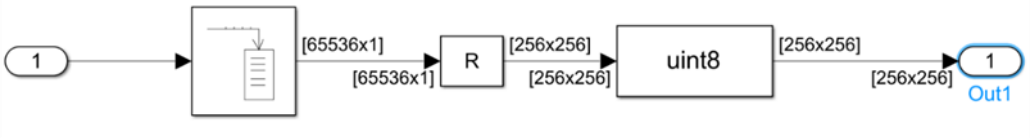

Figure 3. Post processing Simulink blocks.

Results and Discussion

XSG Based Fixed Point Chaotic Maps-PRBG

The chaotic maps based fixed point, namely FPLOM-PRBG, FPLM-PRBG, and FPTM-PRBG are utilized with a fixed-point representation having a word length (WL) of 32 bits and a fractional length (FL) of 28 bits. Additionally, specific initial values are assigned to each chaotic map: (r = 4, X0 = 0.939243) for FPLoM, (α = 1.4, β = 0.3, x0 = 0.5271427, y0 = 0.4574243) for FPLM, and (μ = 0.5, X0 = 0.5271456) for FPTM.

To implement the chaotic pseudo-random number generators (PRBG), first namely FPLOM or Fixed-Point Logistic map, the Xilinx system generator tool is employed for this work. The corresponding implementation is depicted in Fig. 4

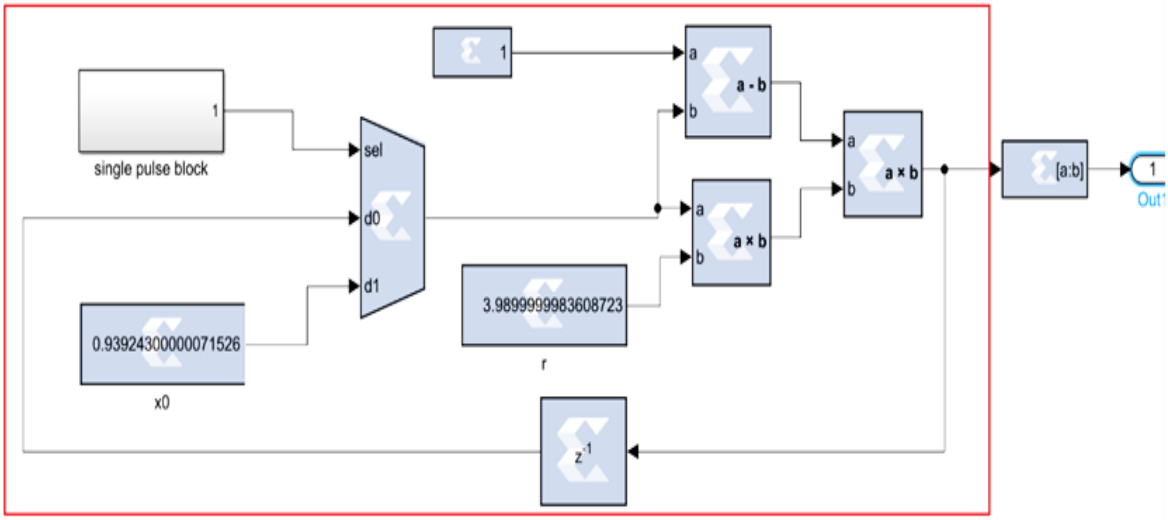

Figure 4. Fixed Point Logistic chaotic map (FPLOM) via XSG environment.

2024, 21(5 Special Issue): 1754-1764
https://doi.org/10.21123/bsj.2024.10521
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

Second namely FPLM-PRBG or Fixed-Point Lozi Map, the corresponding implementation via Xilinx system generator tool is depicted in Fig. 5.

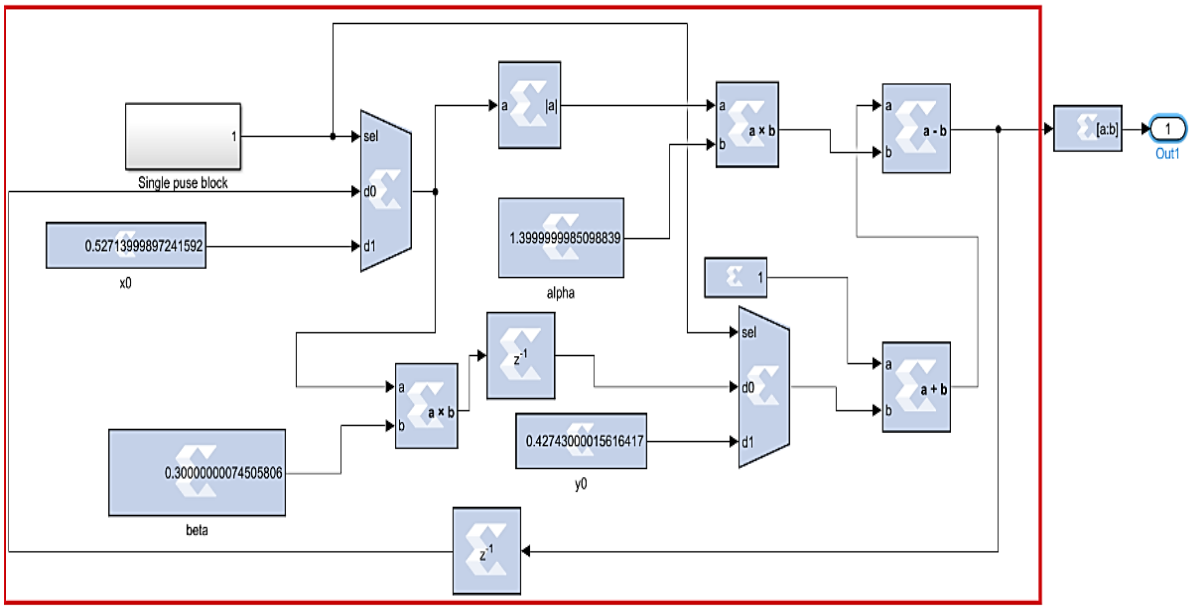

Figure 5. XSG Based Fixed Point Lozi chaotic maps (FPLM).

Third namely FPTM-PRBG or Fixed-Point Tent map, the corresponding implementation via Xilinx system generator tool is depicted in Fig. 6

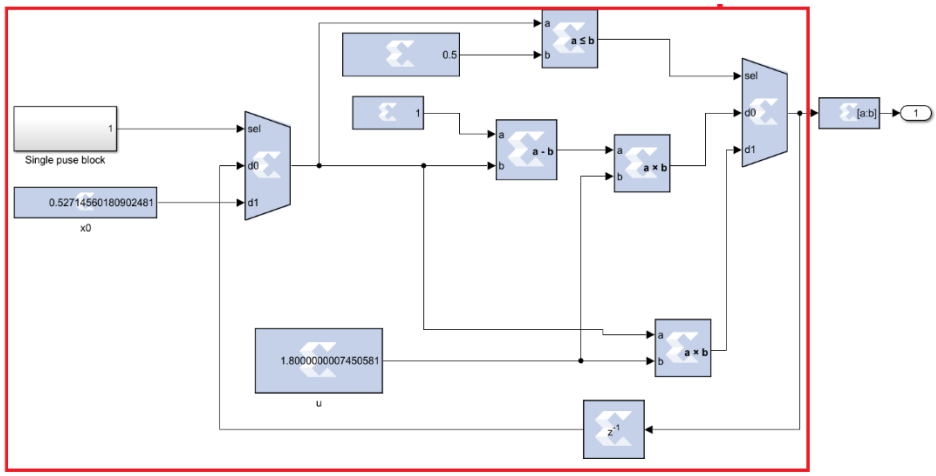

Figure 6. XSG Based Fixed Point Tent chaotic maps (FPTM).

Fourth namely FPXORCM-PRBG or Fixed-Point XOR map, the corresponding implementation via Xilinx system generator tool is depicted in Fig. 7

2024, 21(5 Special Issue): 1754-1764
https://doi.org/10.21123/bsj.2024.10521
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

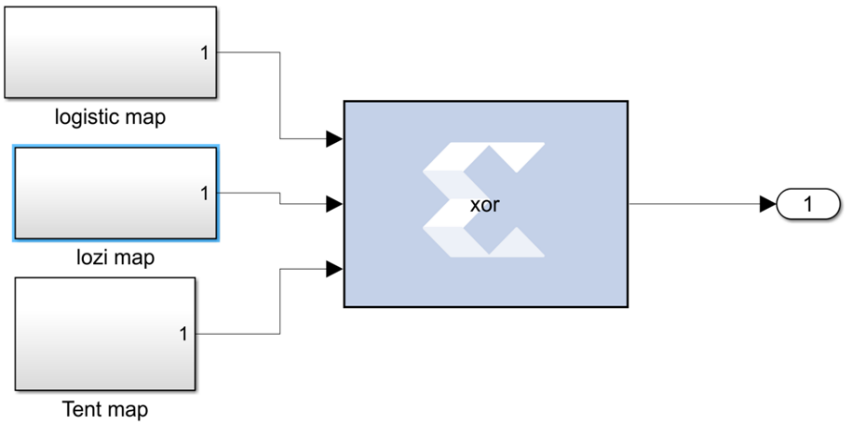

Figure 7. XSG Based Fixed Point XOR chaotic maps (FPXORCM-PRBG).

Fifth namely FPCCM-PRBG or Fixed-Point Cascade map, the corresponding implementation via Xilinx system generator tool is depicted in Fig. 8

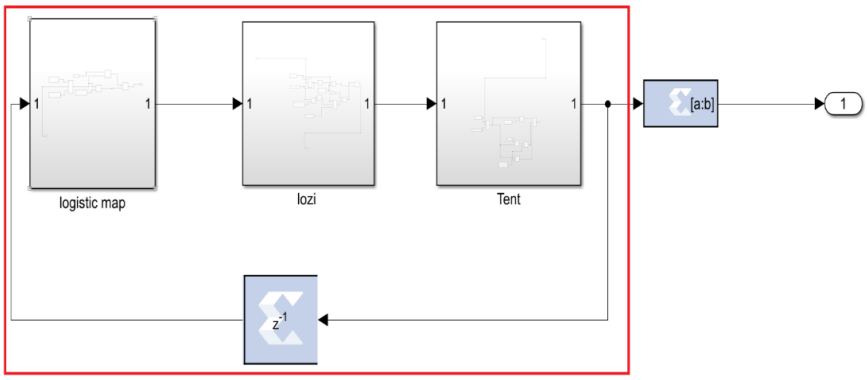

Figure 8. XSG Based Fixed Point Cascade chaotic maps (FPCCM-PRBG).

The proposed encryption system (FPCCM-PRNBG) is achieved by XORing the cascade encryption system FPCCM-PRBG with the PN sequence generated by the Linear Feedback Shift Registers (LFSR) block as shown in Fig. 9.

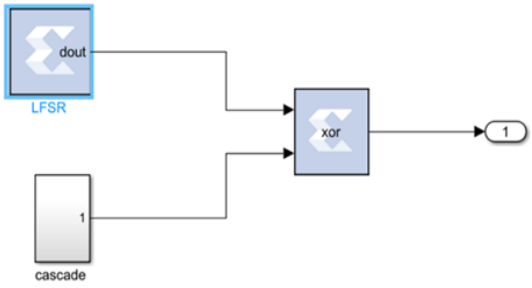

Figure 9. XSG Based Fixed Point cascade chaotic maps with PN generator (FPCCM-PRNBG).

The configuration of the linear feedback shift registers via Xilinx system generator was used for designing PN sequence generator as illustrate in Fig. 10.

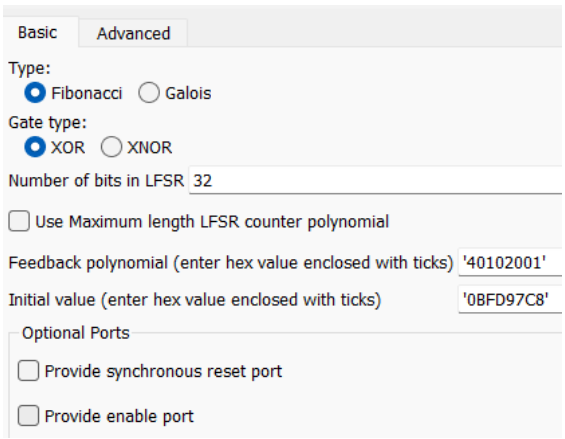

Figure 10. Linear Feedback Shift Register (LFSR) configuration in XSG.

2024, 21(5 Special Issue): 1754-1764
https://doi.org/10.21123/bsj.2024.10521
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

The pulse clock cycle generation used for iteration loop over all the design is shown in Fig. 11.

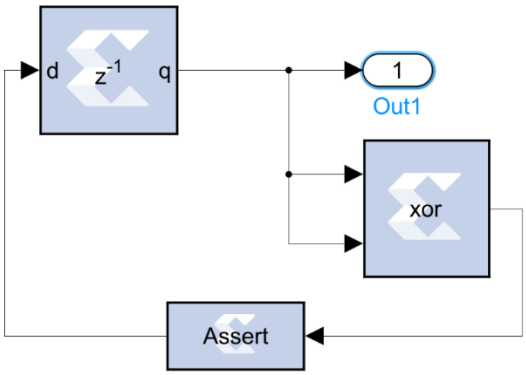

Figure 11. Pulse clock generation block with XSG (single pulse block).

Randomness Test Results

The National Institute of Standards and Technology (NIST) provides 15 tests for measuring randomness. Among these tests, the most popular ones are Frequency (Mono bit) and runs-test as shown in (Table 1). The generated random bits undergo these tests, and they are considered successful if the P-value is greater than 0.01. The P-value acts as a threshold to determine whether to agree or refuse the generated random bits. A P value if equal zero flags that the bits are not random at all, while a P value of one flag the highest level of randomness.

Table 1. The P-Value of the proposed system

Number	P-value of randomness Tests/test name	Our enhanced
1	Frequency test	0.5953
2	Frequency (Mono bit)	0.328074 32408
3	Runs test	0.6375

Performance Security Analysis

Several analyses are presented in this section to examine the security performance of the systems involve histogram analysis, correlation, entropy, key space, pixel changing rate, structural similarity as shown in (Table 2). The analysis was added to (256*256) size of images and carried out using MATLAB and Xilinx System Generator domains.

Histogram is the distribution of all the pixels of image, the pixels distribution inside the original image are unsystematic therefore to be resist to attack the ciphering should make the distribution with equalized property to prevent the image from attack, Fig. 12 shows the histogram of the ciphered image.

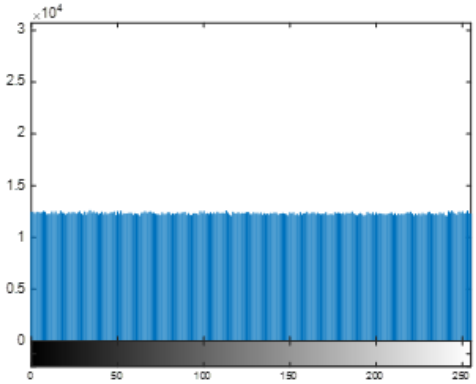

Figure 12. Histogram of the ciphered image.

The correlation is 3.7742e-04 which showed good image encryption should effectively conceal all the details of the original image, resulting in a ciphered image that appears random and uncorrelated. If the correlation coefficient is 1, it indicates that the two images are identical. On the other hand, a correlation coefficient of -1 suggests that the ciphered image is the exact opposite of the original image [19]. The entropy is another security measurement used to test uncertainty of image which equal 7.99 [20]. If the value is most closed to 8 then the ciphering is better.

The extensive key space within cryptography signifies a more secure algorithm against brute force attacks. The key space of the proposed system in terms of its robustness is (2^{288}) [21]. Another two metrics, namely Number of Pixels Change Rate (NPCR) which equals (33.9229606179630) which is very high compared to the ciphering process measurements and Unified Average Changing Intensity (UACI) which equals (99.612808227539060) which indicates that ciphered image is totally different from the original image. These metrics gauge the average intensity of variances between the original and encrypted images [22]. An additional metric provided by MATLAB environment employed to calculate the resemblance between the original and encrypted images is SSIM (Structural Similarity Index) equals (0.0555) which indicates the very small value similarity between the original and ciphered images. A lower SSIM value

2024, 21(5 Special Issue): 1754-1764
https://doi.org/10.21123/bsj.2024.10521
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

indicates reduced similarity between the plaintext and cipher images.

Table 2. Security tests performance

Test name	Our enhanced
Correlation coefficients	3.7742e-04
Information Entropy	7.9997
Key Space Analysis	2 288
Number of Pixels Change Rate (NPCR)	33.922960617963 0
Unified Average Changing Intensity (UACI)	99.612808227539 060
SSIM (Structural Similarity Index)	0.0555

FPGA Hardware Co-simulation of Proposed Algorithm

The VHDL code for all models is obtained through the utilization of the Xilinx System Generator (XSG) block. The design under scrutiny was implemented using the ZYNQ 7000 SoC ZC702 Evaluation Kit [23]. (Table 3) presents the device utilization details. The system's throughput, which represents the number of bits processed per second, can be calculated as (f × 8), where f stands for the maximum frequency. Throughput serves as a primary metric for evaluating the effectiveness of secure cryptographic systems.

The FPGA implementation involves the cryptography system showed in Fig. 13. The image data is sent in a serial manner through the USB JTAG connection to the FPGA board. Once the JTAG configuration is established, the processed data is transmitted back from the FPGA to the MATLAB/Simulink environment. The encrypted image is displayed using a video viewer block, allowing the observation of both the encrypted image and a comparison between the original and decrypted images.

Table 3. Device Area on Xilinx ZC702 Evaluation Kit

Resource Type	FPCCM-PRNBG
LUT	424
LUTRAM	1
FF	392
BRAM	2
DSP	16
IO	2
BUFG	4
MMCM	1
Minimum period (ns)	29.681
Maximum frequency (MHZ)	33.69
Peak memory usage (MB)	2 internal block rams +1 LUT RAM
Throughput (MB/sec)	269.532

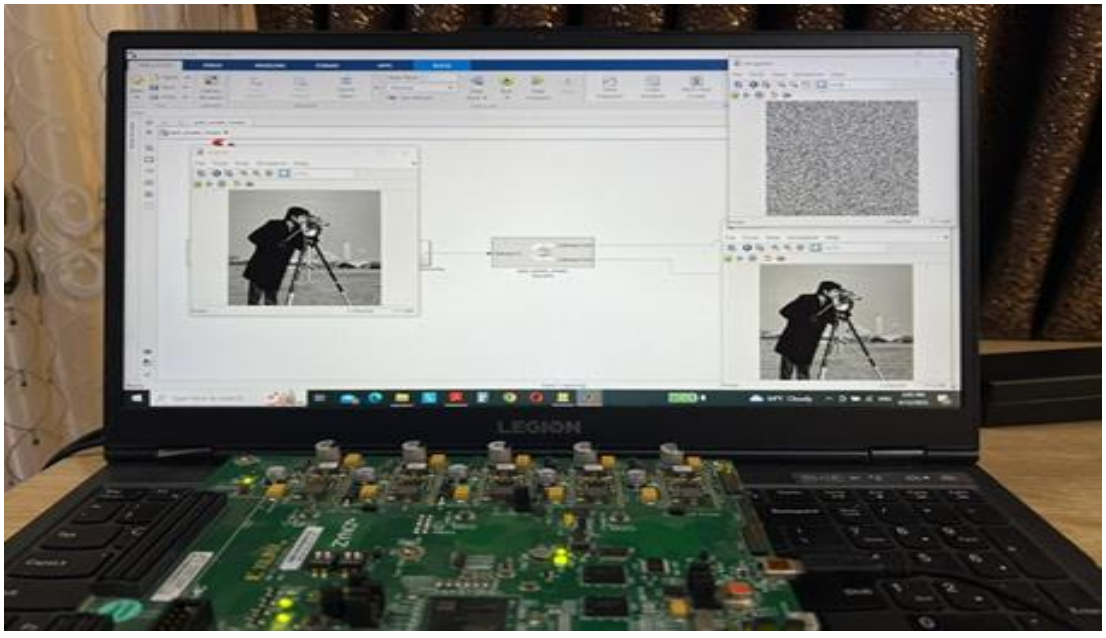

Figure 13. Real time hardware co- simulation of proposed image encryption system.

2024, 21(5 Special Issue): 1754-1764
https://doi.org/10.21123/bsj.2024.10521
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

(Table 4) shows the key space comparisons between our enhanced fixed point cascade chaotic maps with other researches (FPCCM-PRNBG) indicated the high level of security in comparison.

Table 4. Key space comparisons

Ref[7](2020)	Ref[8](2019)	Ref[9](2019)	Ref[11](2020)	Ref[12](2019)	Ref[13](2021)	Ref[14](2019)	Ref[15](2020)	Proposed
2^{232}	2^{260}	2^{128}	2^{122}	2^{100}	2^{128}	2^{249}	2^{256}	2^{288}

Conclusion

In this paper, the image encryption system involved fixed-point chaotic maps with PN sequence-based stream cipher are designed using Xilinx system generator (XSG) methodology implemented in FPGAs, Field Programmable Gate Arrays (FPGA) is a flexible, efficient hardware tool used to accelerate chaos encryption system implementation via Xilinx system generator environment with MATLAB/SIMULINK platform in an efficient manner.

The work started by transforming chaotic maps to fixed-point format with three types Logistic, Lozi and Tent. These maps are used alone or mixed using XOR or cascaded to produce a new model of PRBG, the proposed work was constructing a PN code generator and applying it to cascade topology of the chaotic maps in XORed manner to improve both randomness of keys and security of image. This design is named Fixed Point with Cascade Chaotic Maps with PN generator (FPCCM-PRNBG). Three randomness tests such as frequency, Frequency (Mono bit) and runs-test used for testing the generated keys then the security analysis applied to compare the design key space with previous chaotic maps to test ciphering process.

The key space got better to 2^{288} in comparison with other researches illustrated in (Table 4). The comparison showed that the role of employing PN (pseudo number generator) will increase the key space factor for providing high security performance against brute force attacks.

For FPGA implementation, the maximum frequency was 33.69 MHZ, throughput 269.532 MB/sec which are more convenient to meet the needs of security systems. At last, the real time of the investigated system examined using hardware co-simulation via Xilinx ZC702 Evaluation Kit.

Authors' Declaration

- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are ours. Furthermore, any Figures and images, that are not ours, have been included with the necessary permission for re-publication, which is attached to the manuscript.
- Authors sign on ethical consideration's approval.
- No animal studies are present in the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee at Northern Technical University (NTU) and Nineveh Education Directorate, Mosul, Iraq.

Authors' Contribution Statement

This work was carried out in collaboration between all authors. A.S. presented a survey of chaos types in general with their advantages, applications and limitations. Z.A. showed all the types of chaotic maps and employed them for FPGA implementation. H.A wrote and provided the arrangement and clarity of the article.

2024, 21(5 Special Issue): 1754-1764
https://doi.org/10.21123/bsj.2024.10521
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

References

1. Malik MGA, Bashir Z, Iqbal N, Imtiaz MdA. Color Image Encryption Algorithm Based on Hyper-Chaos and DNA Computing. IEEE Access. 2020; 8: 88093–107. https://doi.org/ 10.1109/ACCESS.2020.2990170.
2. Shengtao G, Tao W, Shida W, Xuncai Z, Ying N. A Novel Image Encryption Algorithm Based on Chaotic Sequences and Cross-Diffusion of Bits. IEEE Photonics J. 2021 Feb; 13(1): 1–15. https://doi.org/10.1109/JPHOT.2020.3044222.
3. Tanveer M, Shah T, Rehman A, Ali A, Siddiqui GF, Saba T, et al. Multi-Images Encryption Scheme Based on 3D Chaotic Map and Substitution Box. IEEE Access. 2021; 9: 73924–37. https://doi.org/10.1109/ACCESS.2021.3081362.
4. Anwar S, Meghana S. A pixel permutation based image encryption technique using chaotic map. Multimed. Tools Appl. 2019 Jun 24; 78(19): 27569–90. https://doi.org/10.1007/s11042-019-07852-2.
5. Rehman MU, Shafique A, Khalid S, Hussain I. Dynamic Substitution and Confusion-Diffusion-Based Noise-Resistive Image Encryption Using Multiple Chaotic Maps. IEEE Access. 2021; 9: 52277–91. https://doi.org/10.1109/ACCESS.2021.3069591.
6. Al-Hassani MD. A Novel Technique for Secure Data Cryptosystem Based on Chaotic Key Image Generation. Baghdad Sci J. 2022 Jan 20; 19(4): 0905-. https://doi.org/10.21123/bsj.2022.19.4.0905
7. Al-Bahrani EA, Kadhum RN. A New Cipher Based on Feistel Structure and Chaotic Maps. Baghdad Sci J. 2019 Mar 17; 16(1(Suppl.)): 270–80. https://doi.org/10.21123/bsj.2019.16.1(Suppl.).0270.
8. Wen H, Zhang C, Chen P, Chen R, Xu J, Liao Y, et al. A Quantum Chaotic Image Cryptosystem and Its Application in IoT Secure Communication. IEEE Access. 2021 ; 9: 20481–92. https://doi.org/ 10.1109/ACCESS.2021.3054952
9. Ayubi P, Setayeshi S, Rahmani AM. Deterministic chaos game: A new fractal based pseudo-random number generator and its cryptographic application. . J Inf Secur Appl. 2020 Jun; 52: 102472. https://doi.org/10.1016/j.jisa.2020.102472.
10. Ma Y, Li C, Ou B. Cryptanalysis of an image block encryption algorithm based on chaotic maps. J Inf Secur Appl. 2020 Oct;54:102566. https://doi.org/10.1016/j.jisa.2020.102566.
11. Zhou M, Wang C. A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks. Signal Process. 2020 Jun; 171: 107484. https://doi.org/10.1016/j.sigpro.2020.107484.
12. Fan S, Li K, Zhang Y, Tan H, Fang Q, Han K, et al. A Hybrid Chaotic Encryption Scheme for Wireless Body Area Networks. IEEE Access. 2020 Jan 1; 8: 183411–29. https://doi.org/ 10.1109/ACCESS.2020.3029263.
13. Li M, Xu M, Luo J, Fan H. Cryptanalysis of an Image Encryption Using 2D Henon-Sine Map and DNA Approach. IEEE Access. 2019 Jan 1; 7: 63336–45. https://doi.org/ 10.1109/ACCESS.2019.2916402.
14. Rahimov H, Babaei M, Farhadi M. Cryptographic PRNG Based on Combination of LFSR and Chaotic Logistic Map. Appl Math. 2011; 02(12): 1531–4. https://doi.org/ 10.4236/am.2011.212217.
15. Abd El-Maksoud AJ, Abd El-Kader AA, Hassan BG, Rihan NG, Tolba MF, Said LA, et al. FPGA implementation of sound encryption system based on fractional-order chaotic systems. Microelectron. J. 2019 Aug; 90: 323–35. https://doi.org/10.1016/j.mejo.2019.05.005.
16. Hasan FS, Saffo MA. FPGA Hardware Co-Simulation of Image Encryption Using Stream Cipher Based on Chaotic Maps. Sens Imaging. 2020 Jul 9; 21(1). https://doi.org/10.1007/s11220-020-00301-7.
17. Bonny T, Al Debsi R, Majzoub S, Elwakil AS. Hardware Optimized FPGA Implementations of High-Speed True Random Bit Generators Based on Switching-Type Chaotic Oscillators. Circuits Syst Signal Process. 2018 Jul 27; 38(3): 1342–59. https://doi.org/10.1007/s00034-018-0905-6.
18. Merah L, Ali-Pacha A, Hadj-Said N, Mecheri B, Dellassi M. FPGA Hardware Co-simulation of New Chaos-Based Stream Cipher Based on Lozi Map. IJET. 2018 Oct; 9(5): 420–5. https://doi.org/10.7763/IJET.2017.V9.1010.
19. Ahmad M, Doja MN, Beg MMS. Security analysis and enhancements of an image cryptosystem based on hyperchaotic system. J. King Saud Univ Comput. Inf Sci. 2021 Jan 1 [cited 2022 Nov 21]; 33(1): 77–85. https://doi.org/10.1016/j.jksuci.2018.02.002.
20. Rodríguez-Orozco E, García-Guerrero EE, Everardo Inzunza-González, Oscar Roberto López-Bonilla, Flores-Vergara A, José Ricardo Cárdenas-Valdez, et al. FPGA-based Chaotic Cryptosystem by Using Voice Recognition as Access Key. Electronics. 2018 Dec 9; 7(12): 414–4. https://doi.org/10.3390/electronics7120414.
21. Zhu S, Zhu C, Wang W. A New Image Encryption Algorithm Based on Chaos and Secure Hash SHA-256. Entropy. 2018 Sep 19; 20(9): 716. https://doi.org/10.3390/e20090716.
22. Pourjabbar Kari A, Habibizad Navin A, Bidgoli AM, Mirnia M. A new image encryption scheme based on hybrid chaotic maps. Multimed. Tools Appl. 2020 Sep 16; 80(2): 2753–72. https://doi.org/10.1007/s11042-020-09648-1.

2024, 21(5 Special Issue): 1754-1764
https://doi.org/10.21123/bsj.2024.10521
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

23. Xiling, ZC702 Evaluation Board for the Zynq-7000 XC7Z020 All Programmable SoC, UG850 (v1.5), Xiling, Inc., 2015.

تصميم وتعزيز أداء أمن نظام تشفير الصور المستند إلى تشفير الخرائط الفوضوية ذات النقطة الثابتة في منظومة البوابات القابلة للبرمجة حقلياً

احمد عامر صالح[1]، زيد عبد الستار عبد الرزاق[2]، حارث غانم أيوب[2]

[1]قسم التعليم المهني، المديرية العامة لتربية نينوى، الموصل، العراق.
[2]الجامعة التقنية الشمالية، الموصل، العراق.

الخلاصة

تقترح هذه الورقة البحثية نظامًا جديدًا لتصميم تشفير الصور باستخدام الخرائط الفوضوية ذات النقطة الثابتة ومولدات التشفير المتسلسل (PN). يتكون النظام من خرائط فوضوية ثابتة مدمجة برقم إفتراضي (PN) مكون من 32 بت، يتم تنفيذها جميعًا باستخدام مصفوفات البوابات المنطقية القابلة للبرمجة ميدانيًا (FPGA) من خلال بيئة مولد النظام (XSG) . خرائط التشفير المعتادة المستخدمة في هذا العمل هي خرائط (Logistic) و (Lozi) وTent . تحدد متغيرات كل نوع من الخرائط حجم المفتاح المطلوبة لفك تشفير البكسل الأصلي للصورة الأصلية، حيث تحتوي خريطة (Logistic) على متغير واحد (r)، وتحتوي خريطة (Lozi) على متغيرين α و β، وتحتوي خريطة (Tent) على متغير واحد μ كانت الفكرة الرئيسية هي دمج متغير أخر وهو الرقم الإفتراضي (PN) لزيادة مساحة المفتاح، والتي تعد المقياس الرئيسي لتحسين الأمن ضد هجمات القوة القاهرة. تم اقتراح مولد بت عشوائي زائف (PRBG) مبتكر يعتمد على عملية XOR بين الخرائط الفوضوية هذه وأطلق عليه اسم FPCCM-PRBG (مولد بت عشوائي زائف بخرائط فوضوية متتالية ذات نقطة ثابتة). كما تم اقتراح طريقة أخرى تعتمد على أقل 8 بتات ذات دلالة من مولد الرقم الإفتراضي 32 بت وأطلق عليها اسم FPCCM-PRNBG (مولد بت عشوائي غير ثابتة بخرائط فوضوية متتالية ذات نقطة ثابتة). تم إختبار عشوائية المفاتيح المتولدة باستخدام اختبارات المعهد الوطني للمعايير والتكنولوجيا (NIST)، بما في ذلك اختبارات التردد والتردد أحادي البت والاختبار التنفيذي. كما تم تقييم أداء الأمن من خلال تحليل الهستوغرام، وتحليل معامل الارتباط، وإنتروبيا المعلومات، ومعدل تغيير البكسل، والتشابه البنيوي. يعتبر مولد النظام (XSG) أداة فعالة مضمنة في بيئة MATLAB/SIMULINK وتم استخدامها لتنفيذ العمل. تم تنفيذ النظام باستخدام طريقة المحاكاة المشتركة على لوحة ZC 7000 SoC ZYNQ702، مع مساحة مفتاح تبلغ (2^288) وسرعة تبلغ 269.32 ميجابايت/ثانية..

الكلمات المفتاحية: الخرائط الفوضوية، البوابات المنطقية القابلة للبرمجة، تشفير الصور، الاعداد الزائفة، الامن، مولد النظام اكساينس.