Indonesian Journal of Electrical Engineering and Computer Science
Vol. 13, No. 1, January 2019, pp. 129~137
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v13.i1.pp129-137

FPGA implementation of color image encryption using a new chaotic map

Hamsa A. Abdullah, Hikmat N. Abdullah
College of Information Engineering, Al-Nahrain University, Baghdad, Iraq

Article Info

Article history:

Received Jul 13, 2018
Revised Oct 2, 2018
Accepted Oct 19, 2018

Keywords:

FPGA
Image encryption
Nahrain chaotic map
Scrambling
Security analysis

ABSTRACT

In this paper, an FPGA implementation of efficient image encryption algorithm using a chaotic map has been proposed. The proposed system consists of two phases image encryption technique. First phase consists of scrambling of pixel position and second phase consist of diffusion of bit value. In the first phase, original pixel values remain unchanged. In second phase, pixel values are modified. These modifications are done by using chaotic behavior of a recently developed chaotic map called Nahrain. A color image encryption using Nahrain chaotic map is simulated in software via Matlab, Altera Quartus Prime 17.0 Lite EditionI and ModelSim software tools then implemented in hardware via Cyclone V GX Starter Kit FPGA platform. The results show the feasibility and effectiveness of the cryptosystem. As a typical application, the image encryption/decryption is used to demonstrate and verify the operation of the cryptosystem hardware. Complete analysis on robustness of the method is investigated. Correlation, Encryption time, Decryption time and key sensitivity show that the proposed crypto processor offers high security and reliable encryption speed for real-time image encryption and transmission. To evaluate the performance, histogram, correlation, information entropy, number of pixel change rate (NPCR), and unified average changing intensity (UACI) measures are used for security analysis. The simulation results and security analysis have demonstrated that the proposed encryption system is robust and flexible. For example the amount of entropy obtained by the proposed algorithm is 7.9964, which is very close to its ideal amount: 8, and NPCR is 99.76 %, which is the excellent value to obtain. The hardware simulation results show that the number of pins that used of the proposed system reaches to 6% of total pins and Logic utilization (in ALMs) is 1%.

Copyright © 2019 Institute of Advanced Engineering and Science.
All rights reserved.

Corresponding Author:

Hamsa A. Abdullah,
Department of System Engineering,
Al- Nahrain University, Baghdad, Iraq.
Email: hamsa.abdulkareem@coie-nahrain.edu.iq

1. INTRODUCTION

Chaotic system of simple structure can demonstrate complex dynamical properties in infinite mathematical world, such as sensitivity to initial conditions, topological transitivity and mixing, expansiveness, and decaying autocorrelation function. Chaotic system can be divided into two types of model: chaotic flow model and chaotic map model [1]. Such properties have subtle relation with some requirements of secure encryption system, especially sensitivity with respect to change of secret key [2-3]. So, designing chaos-based encryption schemes emerged as a new research direction to reinforce information security of data sent through the Internet.

Cryptography are realized in software to verify the effectiveness of algorithms other than in hardware for communication and storage applications. In fact, the main advantage of using of hardware for

cryptosystem is that multiple parts of system can operate simultaneously, i.e. the generator of secret keys, substitution and permutation processes. That makes chaotic cryptosystems suitable for applications in high speed communications or massive storage [4]. In general, the encryption process conducted by using software that is programmed in computer. In practice, only a few applications requiring throughput while flexible solutions and low cost encryption / decryption is needed to protect the data that makes sense, especially for embedded hardware applications. Some small devices such as Field Programmable Gate Array (FPGA) have been potential to be applied to replace the computer as a medium for image encryption. The data encryption system will be optimized when implemented into the FPGA because it has advantages which include flexibility, development cost and costs low per-unit, high speed and has a good level of security [5].

In [4], an implementation of secure SPN chaos-based cryptosystem on FPGA is introduced. In this paper, the secure substitution permutation network (SPN) chaos-based cryptosystem is realized using software tools C/C++, Altera Quartus II and ModelSim and implemented in hardware using FPGA platform. In [5], the Sum of Product (SOP) Encryption using simple algorithm based on Boolean algebra is introduced. It is implemented using image encryption algorithm to produce a quick image encryption system. However it has drawback of having fixed encryption pattern. In [6], FPGA Implementation of Chaotic based AES Image Encryption Algorithm is presented. The algorithm is a combination of chaotic maps and AES. The proposed architecture is implemented using Verilog HDL and Xilinx ISE Design Suite 14.5. However it has drawback of having complex structures of image encryption.

In [7], Comparative analysis of color image encryption using 3D chaotic maps is presented. The color image encryption using different 3D chaotic maps, including 3D logistic map, Henon map, Baker map and cross chaos map which are the further extension of 2D chaotic maps. In [8], color image encryption using chaotic maps triangular scrambling, with DNA Sequences is introduced, The scheme takes a master key with a length of 320 bit, and produces a group of sub-keys with two length (32 and 128 bit) to encrypt the blocks of images, then a new triangular scrambling method is used to increase the security of the image. However it has drawback of having limited length of master key. In [9], Finite precision logistic map between computational efficiency and accuracy with encryption applications is introduced. Digital implementation of the generalized logistic map with signed parameter is considered. They present a fixed-point hardware realization of a pseudo-random number generator using the logistic map that experiences a trade-off between computational efficiency and accuracy. The trade-off factors include: the used precision, the order of execution of the operations, parameter, and initial point values affect the properties of the finite precision map. In [10], a color image encryption scheme based on arnold scrambling and quantum chaotic is introduced. In this paper, an algorithm for image encryption based on two-dimensional Arnold transform with keys and quantum chaotic map is proposed.

In 2018, we have proposed a new dynamical system called Nahrain chaotic system [11]. We proved that it has excellent performance for multimedia encryption and secure transmission [12]. However, in [11] we have presented only a part standard randomness tests to prove the system randomness behavior. In this paper, we will introduce the hardware implementation of image encryption based on Nahrain chaotic map. The hardware implementation is based on a programmable hardware which allows the experimental characterization of the system dynamics with low cost, reconfigurable and rapid experimental setup. The paper is organized as follows. Section 1 presents presents the current stage of chaos based image encryption. Section 2 includes description of proposed encryption algorithm. Section 3 includes the simulation results and discussion of the proposed algorithm. Finally, section 4 gives the conclusions of the paper.

2. IMAGE ENCRYPTION BASED ON CHAOTIC ALGORITHM

The Block Diagram of the proposed image encryption algorithm based on Nahrain chaotic system is shown in Figure1. This encryption algorithm consists of two blocks: the first block is the Image Scrambling and second block is diffusion based on Nahrain Chaotic system. The nonlinear equations that describe the Nahrain chaotic system are given in (1):

$$\begin{aligned} X_{n+1} &= 1 - aX_nY_n - X_n^2 - Y_n^2 \\ Y_{n+1} &= X_n \\ Z_{n+1} &= Y_n - bZ_n \end{aligned} \quad (1)$$

Where a and b are the bifurcation parameters of the system. Through a series of numerical modeling and simulation associated with MATLAB, The phase portraits of chaotic behavior have been acquired by using system parameter values: a=1.52 and b=0.05. The schematic block diagram of the proposed Nahrain chaotic generator is shown in Figure 1. Figure 2 shows the phase portraits of the proposed system when its initial

conditions are: X(0)=0.3, Y(0)=0.2 and Z(0)=0.1 [11]. The proposed scrambling method consist of two types of scrambling, the first method is Block Scrambling and the second method is negative diagonal scan. The main steps of encryption method are listed:

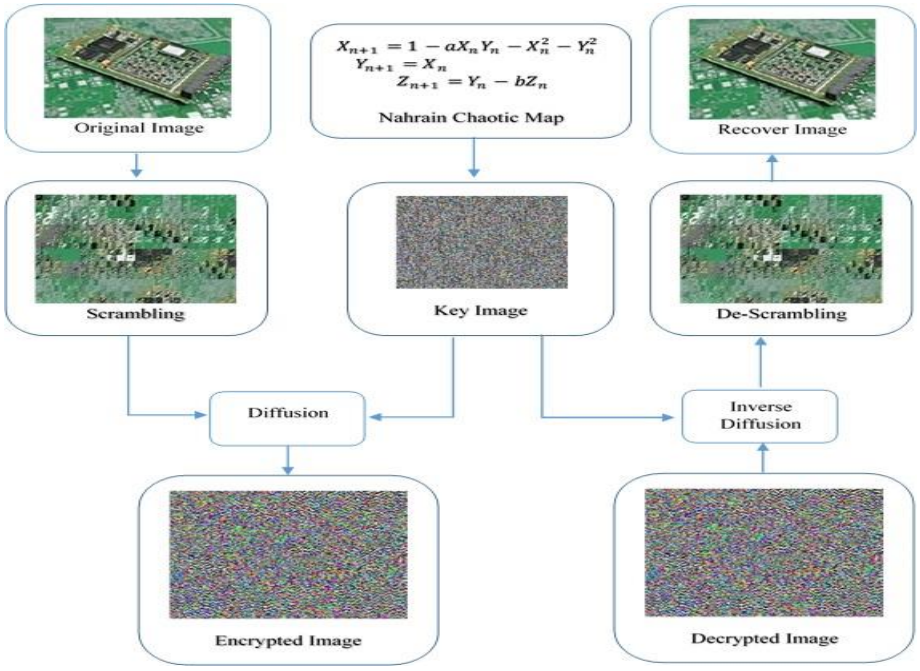


Figure 1. Proposed Algorithm

Step 1: Block Scrambling: the image is divided to four blocks [Block 1, Block2; Block3, Block 4] and then scrambling the blocks in the order [Block3, Block 4; Block1, Block2] as shown in Figure 2 (a).
Step 2: Each block is divided in to four sub block, and scrambled diagonally.
Sterp 3: Negative diagonal scan: the image is divided into blocks of size 8*8 and then each block is read from right to left diagonally as shown in Figure 2 (b).

(a). Block scrambling (b). Negative diagonal scrambling

Figure 2. Image scrambling

Step 4: Three dimensional chaotic map is generated by using (1).
Step 5: Chaotic (X1, Y1, and Z1) is converted to binary by using random bit generator method as shown [10]:

$$BX(X1,X2) = \begin{Bmatrix} 1\ if\ X1 > X2 \\ 0\ if\ X1 \leq X2 \end{Bmatrix}\ where\ X1_0 \neq X2_0 \quad (2)$$

$$BY(Y1,Y2) = \begin{Bmatrix} 1\ if\ Y1 > Y2 \\ 0\ if\ Y1 \leq Y2 \end{Bmatrix}\ where\ Y1_0 \neq Y2_0 \quad (3)$$

$$BZ(Z1,Z2) = \begin{Bmatrix} 1\ if\ Z1 > Z2 \\ 0\ if\ Z1 \leq Z2 \end{Bmatrix}\ where\ Z1_0 \neq Z2_0 \quad (4)$$

The random bit generator method based on comparing the outputs of two Nahrain chaotic maps running side-by-side and starting from random independent initial conditions and same parameters value where (X1=0.3, Y1=0.2, Z1=0.1, X2=0.2, Y2=0.1, Z2=0.2, a=1.52, and b=0.05).
Step 6: The output of row Scrambled image is XORed with the key image generated in steps (4 and 5) to get color level encrypted image.

The main steps of Decryption Method are listed below:
Step 1: Generate three dimensional chaotic map by using (1).
Step 2: Convert chaotic (X1, Y1, and Z1) to binary by using random bit generator method as shown in (2-4).
Step 3: The Encrypted image is XORed with key image generated in step 1 to get color level Scrambled image.
Step 4: Scrambled image is divided to block of size 8*8 and then each block is read in negative diagonal scan as shown in Figure 2.b.
Step 5: The descrambled image is passed through Block Scrambling where image is divided into four blocks [Block 1, Block2; Block3, Block4] and then scramble the block in the order [Block3, Block4; Block1, Block2] as shown in Figure 2.a.

3. RESULT AND DISCUSSION

In this section, the simulation results of the security measurements for the proposed color image encryption using a new chaotic map is simulated in software via Matlab, Altera Quartus Prime 17.0 Lite Edition I and ModelSim software tools then implemented in hardware via Cyclone V GX Starter Kit FPGA platform. As a typical application, the image encryption/decryption is to demonstrate and verify the operation of the cryptosystem hardware. This project is implemented in two ways, namely.

a) By using MATLAB
b) By using FPGA

Here an VHDL block is used as an intermediate between the Matlab as shown in Figure 3, which means by the VHDL code we can't read the image directly so to overcome that one we use Matlab at the first, were an image is converted into text form and once more any random image is taken and converted into text form by Matlab, which acts as key image for the encryption this key should be same for encryption as well as decryption. Firstly the text file read by VHDL and then the two types of scrambling implemented on it. Finally an XOR operation is done between scrambled text matrix and key text matrix to get an encrypted result.

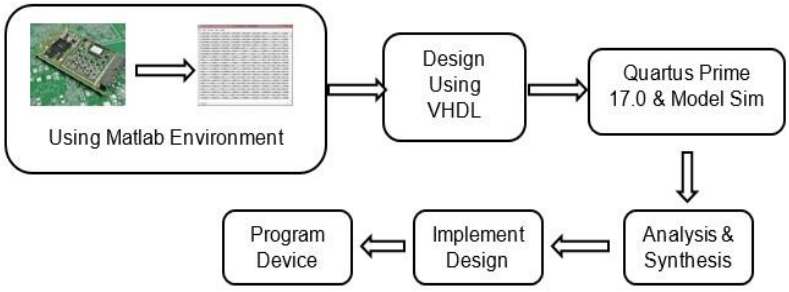


Figure 3. Hardware implementation steps

3.1. MATLAB Implementation

Color image of sizes (64x64, 128x128, 176x144, and 256×256) are considered for experimental tests. The parameters of Nahrain map are taken to be a=1.52, b=0.05, and the initial conditions of state variables are X0=0.3; Y0=0.2; and Z0=0.1. Figure 4 shows the plain and encrypted images using Nahrain

map. The security analysis of encrypted images is performed by using six statistical methods as: histogram analysis, PSNR, Information Entropy, Correlation, NPCR and UACI [12-14].

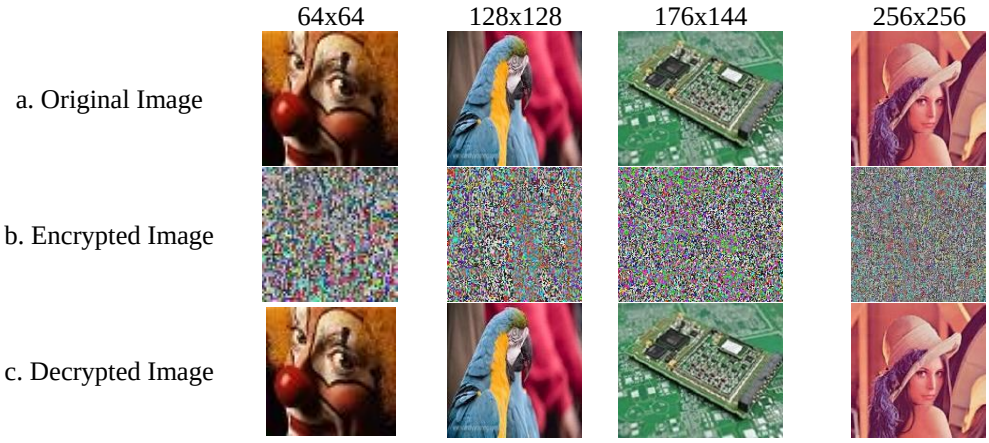


Figure 4. Plain and encrypted images

3.1.1 Histogram Analysis

Figure 5 shows the histogram analysis results. In Figure 5(a-e) are the histograms of color plain-image Red, Green, and Blue while (f-i) the histograms of encrypted-images Red, Green, and Blue using Nahrain chaotic map. As it is clearly seen, the histogram of proposed algorithm is fairly uniform and significantly different from that of the plain image and the encrypted image [4] of in Figure 5 (j). This reveals that the attacker cannot use any valid statistical data in the encrypted image to start any statistical attacks to the cryptosystem.

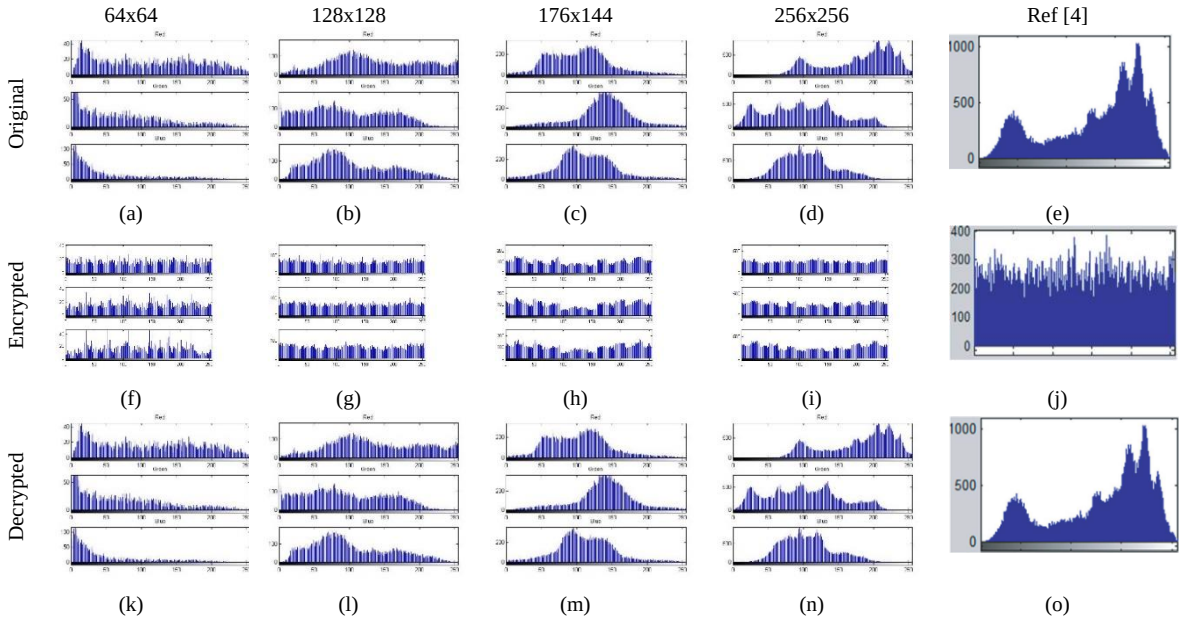


Figure 5. Histogram analysis

3.1.2 PSNR

Table 1 show the results of MSE and PSNR test between the original image, cipher image and reconstructed image. The comparison of PSNR values between the original image and the reconstructed

image denoted that the two images are identical. Whereas the similarity PSNR values between the original image and cipher image are very low which means the encrypted image is very strong against the attacks.

Table 1. PSNR and MSE Result using the Proposed Algorithm

Image size	Color layer	Cipher Image		Reconstructed Image	
		PSNR	MSE	PSNR	MSE
64x64	R	12.2946	3.8337e+03	Inf	0
	G	12.0084	4.0949e+03	Inf	0
	B	11.3235	4.7943e+03	Inf	0
128x128	R	12.7008	3.4914e+03	Inf	0
	G	12.6868	3.5027e+03	Inf	0
	B	12.9555	3.2926e+03	Inf	0
176x144	R	13.1289	3.1637e+03	Inf	0
	G	13.2544	3.0736e+03	Inf	0
	B	13.1379	3.1571e+03	Inf	0
256x256	R	12.6553	3.5282e+03	Inf	0
	G	12.9418	3.3029e+03	Inf	0
	B	13.2404	3.0835e+03	Inf	0

3.1.3 Correlation Coefficients of Two Adjacent Pixels

The correlation coefficients of plain and encrypted images are shown in Table 2. The correlation coefficients of encrypted images using the proposed algorithm are closed to zero, which means that the correlations of neighboring pixels in the plain image can be removed by using proposed algorithm, and can hold statistical attacks [15].

Table 2. Correlation Coefficients Results

Algorithm	Image size	Color layer	Horizontal	Vertical	Diagonal
Proposed Algorithm	64x64	R	0.0121	-0.0624	0.1083
		G	-0.1360	-0.1550	0.0919
		B	-0.1171	0.0535	0.0319
	128x128	R	-0.0214	0.0178	0.0586
		G	0.0779	0.0154	-0.0032
		B	0.0016	0.0707	-0.0373
	176x144	R	-0.0525	-0.0866	-0.0757
		G	0.0239	-0.1727	0.1079
		B	-0.0553	7.1453e-04	-0.0448
	256x256	R	0.0079	0.0245	0.1259
		G	-0.0921	0.0372	0.1013
		B	-0.0410	-0.0079	0.0316
Ref [7]	256x256	Average	0.0124	-0.00564	0.0276
Ref [8]	256x256	Average	0.0007	0.0037	-0.0051
Ref [9]	256x256	R	-0.0071	0.0007	0.0014
		G	0.0006	0.0006	0.0001
		B	0.0001	0.0045	-0.0022

3.1.4 The Information Entropy

The entropies of plain and encrypted images are shown in Table 3. The results in this table show that the entropies of the encrypted image generated by the proposed algorithm are closed to 8, and that means the encrypted images are closed to a random.

3.1.5 NPCR

NPCR calculates the percentage of different pixel numbers between two Images. This analysis helps in determining the vulnerability of the system towards differential attacks. The analysis report for encrypted image is given in the Table 3. We note from this table that the proposed algorithm has the excellent performance where the value of NPCR is 99.74%.

3.1.6 UACI

UACI calculate the average intensity of differences between two images. The analysis reported for encrypted image is given in the Table 3. The value of UACI is over 33 % which indicate that the rate of influence due to one pixel change is very large.

Table 3. EC, NPCR and UACI Result

Algorithm	Image size	Color layer	EC	NPCR	UACI
Proposed Algorithm	64x64	R	7.9503	99.66	34.81
		G	7.9342	99.49	34.59
		B	7.8427	99.73	40.24
	128x128	R	7.9692	99.54	32.33
		G	7.9774	99.62	33.46
		B	7.9666	99.64	31.94
	176x144	R	7.9064	99.66	32.31
		G	7.8169	99.76	32.91
		B	7.8271	99.74	33.14
	256x256	R	7.9964	99.58	32.60
		G	7.9628	99.65	32.19
		B	7.8294	99.74	32.70
Ref [7]	256x256	Average	7.9437	98.92	33.50
Ref [10]	256x256	Average	-	99.69	33.44

3.1.7 Key Space Analysis

The size of the key space is the total number of different keys that can be applied in the encryption/ decryption process. The key space should be large enough to make brute-force attacks infeasible. From the cryptographic point of view, the size of the key space should not be smaller than 2100 to ensure a high level of security. The set of all initial numbers compose the key space. The key space of the image encryption scheme has five secret key values x0, y0, z0, a, and b. As stated in IEEE floating-point standard, the computational precision of the 64-bit double-precision number is about 2−52 [16-18]. Therefore, the key space of the proposed algorithm is (252)5=2260, which very much higher than the classical encryption schemes.

3.2. FPGA Implementation

The secure image encryption based on chaotic system has been implemented on the Altera FPGA Board, Cyclone V GX Starter Kit as shown in Figure 6 and 7. The color image with different sizes (64x64, 128x128, 176x144, and 256×256) shown in Figure 4 are used to test the hardware implementation performance. The amount of time is required for encryption and decryption are shown in Table 4. The hardware resource required for the cryptosystem is considerably large due to simultaneous operation in key generator and encryption/decryption processes. The hardware resources that used shown in Table 5. The plain, Encrypted and Decrypted images obtained from the operation of cryptosystem on FPGA are shown in Figure 4(a-c). Decryption is exactly reverse to the encryption and final Encryption and Decryption simulation result as Figure 8.

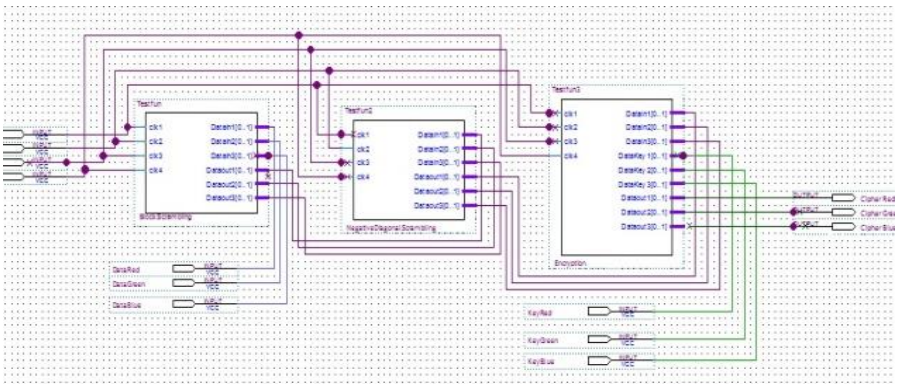


Figure 6. Block diagram of toe proposed system in FPGA

Table 4. Analysis & Synthesis CPU Time

Image size	Encryption time (in sec.)	Decryption time (in sec.)
64x64	0.44	1.16
128x128	1.20	1.24
176x144	1.55	2.04
256x256	4.14	4.35

Table 5. Hardware Resources

	Total	Used	%
Logic utilization (in ALMs)	29,080	1	<1%
Pins	364	22	6%

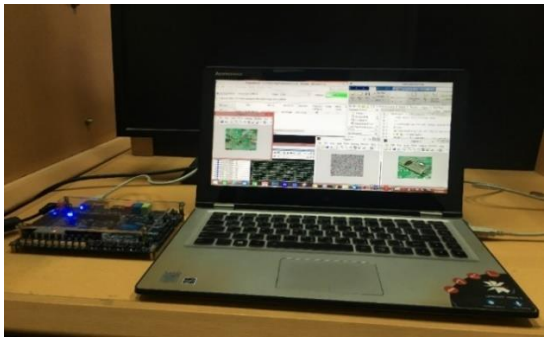
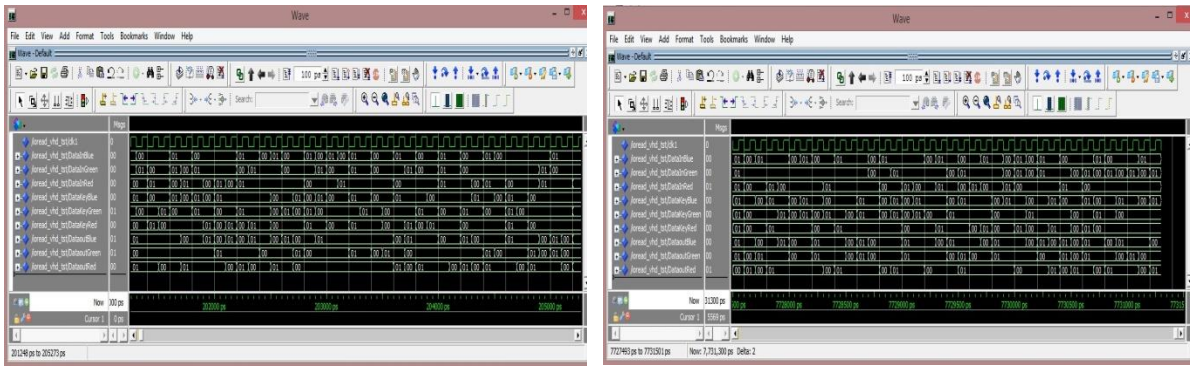


Figure 7. Altera FPGA board, cyclone V GX starter kit



(a). Encryption data (b). Decryption data

Figure 8. Encryption and decryption data of image size 256x256

4. CONCLUSION

A color image encryption using a new chaotic map is simulated in software via Matlab, Altera Quartus Prime 17.0 Lite Edition I and ModelSim software tools then implemented in hardware via Cyclone V GX Starter Kit FPGA platform. The result shows the feasibility and effectiveness of the cryptosystem. As a typical application, the image encryption/decryption is to demonstrate and verify the operation of the cryptosystem hardware. The proposed scheme provides large key space, which is sensitive to slight change. The used security measurements demonstrated that the joint weaknesses existed in other encryption algorithms can be defeated by the proposed algorithm, and the security measurements show that the proposed algorithm robust against all types of attacks such as statistical, differential and brute-force attacks. The encryption execution time of the proposed encryption scheme is relatively fast and flexible to different applications.

REFERENCES

[1] Branislav J., "Synchronization Techniques for Chaotic Communication Systems," *New Zealand: Springer*, 2011.
[2] Qianxue Wang, Simin Yu, Chengqing Li, Jinhu L¨u, Xiaole Fang, Christophe Guyeux, and Jacques M. Bahi,, "Theoretical Design and FPGA-Based Implementation of Higher-Dimensional Digital Chaotic Systems," *IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS–I: REGULAR PARER*, vol. 63, no. 3, p. 12, 2016.
[3] Bikash Baruah, Monjul Saikia,, "An FPGA Implementation of Chaos based Image Encryption and its Performance Analysis," *International Journal of Computer Science and Network (IJCSN)*, vol. 5, no. 5, pp. 712-720, 2016.
[4] Safwan AI Assad, Ta Thi Kim Hue, Chu Van Lam, Thang Manh Hoang,, "Implementation of secure SPN chaos-based cryptosystem on FPGA," in *IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, Ho Chi Minh City, Vietnam, 2012.

[5] Barlian Henryranu Prasetio, Eko Setiawan, Adharul Muttaqin,, "Image Encryption using Simple Algorithm on FPGA," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 13, no. 4, pp. 1153-1161, 2015.
[6] Syed Shahzad Hussain Shah, Gulistan Raja,, "FPGA Implementation of Chaotic based AES Image Encryption Algorithm," in *IEEE International Conference on Signal and Image Processing Applications (ICSIPA)*, Kuala Lumpur, Malaysia, 2015.
[7] Bhavna Sinha, Shubhendu Kumar, Chittaranjan Pradhan,, "Comparative Analysis of Color Image Encryption using 3D Chaotic Maps," in *International Conference on Communication and Signal Processing,IEEE*, India, 2016.
[8] Haider M. Al-Mashhadi, Iman Q. Abduljaleel,, "Color Image Encryption using Chaotic Maps Triangular Scrambling, with DNA Sequences," in *International Conference on Current Research in Computer Science and Information Technology (ICCIT)*, Slemani, Iraq, 2017.
[9] A. A. R. a. H. H. F. Wafaa S. Sayed Ahmed G. Radwan, "Finite Precision Logistic Map between Computational Efficiency and Accuracy with Encryption Applications," Complexity, Hindawi., vol. 2017, p. 21, 2017.
[10] Hui Liu, Cong Jin,, "A Color Image Encryption Scheme Based on Arnold Scrambling and Quantum Chaotic," *International Journal of Network Security*, vol. 19, no. 3, pp. 347-357, 2017.
[11] Hamsa A. Abdullah, Hikmat N. Abdullah,, "A New Chaotic Map for Secure Transmission," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 16, no. 3, pp. 1135-1142, 2018.
[12] Hikmat N. Abdullah, Hamsa A. Abdullah, "Two-level Secure Colored Image Transmission Using Novel Chaotic Map," in *Second Al-Sadiq International Conference on Multidisciplinary in IT and Communication Science and Applications (2nd-AIC-MITC'17)*, Baghdad, Iraq, 2017.
[13] Hongyao Deng, Qingxin Zhu, Xiuli Song, Jingsong Tao,, "Chaos-Based Image Encryption Algorithm Using Decomposition," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 12, no. 1, pp. 575-583, 2014.
[14] Alia Karim Abdul Hassan, "Proposed Hyperchaotic System for Image Encryption," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 7, no. 1, 2016.
[15] Shivaputra, HS Sheshadri, V Lokesha, "A Naïve Visual Cryptographic Algorithm for the Transfer of Compressed Medical Images," *Bulletin of Electrical Engineering and Informatics*, vol. 5, no. 3, pp. 347-365, 2016.
[16] Borislav Stoyanov, Krasimir Kordov, "Image Encryption Using Chebyshev Map and Rotation Equation," Entropy, vol. 17, pp. 2117-2139, 2015.
[17] An American National Standard, "754-1985 - IEEE Standard for Binary Floating-Point Arithmetic," *Standards Committee of the IEEE Computer Society*, 1985.
[18] Ruisong Ye, "An Image Encryption Scheme with Efficient Permutation and Diffusion Processes," in In: Zhou M., Tan H. (eds) *Advances in Computer Science and Education Applications, Communications in Computer and Information Science*, Berlin, Heidelberg, Springer, 2011, pp. 32-39.

BIOGRAPHIES OF AUTHORS

Hamsa A. Abdullah was born in Baghdad, Iraq in 1984. She obtained her B.Sc. in Information Engineering in 2005, M.Sc in Information Engineering in 2008 at Al-Nahrain University, Iraq. She worked as a lecturer in the College of Information Engineering at Al-Nahrain University, Iraq since 2008. She is interested in subjects Multimedia, Multimedia security transmission over wireless communication systems, Pattern Recognition and Network Security.

Hikmat. N. Abdullah was born in Baghdad, Iraq in 1974. He obtained his B.Sc. in Electrical Engineering in 1995, M.Sc. in Communication Engineering in 1998 at University of Al-Mustansiryah, Iraq and Ph.D. in Communication Engineering in 2004 at University of Technology, Iraq. From 1998 to 2015 he worked as lecturer in the Electrical Engineering Department, at Al-Mustansiryah University, Iraq. Since the beginning of 2015 he works as professor in college of Information Engineering at Al-Nahrain university, Iraq. From 2011–2013 he got a research award from International Institute of Education (IIE/USA) at Bonn-Rhein-Sieg university of applied sciences, Germany. He is a senior member of IEEE association since 2014. He is interested in subject of modulation and coding schemes for wireless communication systems.