Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.028969
Article

Tech Science Press

VLSI Implementation of Optimized 2D SIMM Chaotic Map for Image Encryption

M. Sundar Prakash Balaji[1,*], V. R. Vijaykumar[2], Kamalraj Subramaniam[3], M. Kannan[4] and V. Ayyem Pillai[5]

[1]Department of Electronics and Communication Engineering, RVS College of Engineering and Technology, Coimbatore, 641402, India
[2]Department of Electronics and Communication Engineering, Anna University Regional Campus, Coimbatore, 641046, India
[3]Department of Biomedical Engineering, Karpagam Academy of Higher Education, Coimbatore, 641021, India
[4]Department of Electronics, MIT Campus, Chennai, 600044, India
[5]Department of Electronics and Communication Engineering, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, 500090, India
*Corresponding Author: M. Sundar Prakash Balaji. Email: rvssundarbalaji@gmail.com
Received: 22 February 2022; Accepted: 29 March 2022

Abstract: The current research work proposed a novel optimization-based 2D-SIMM (Two-Dimensional Sine Iterative chaotic map with infinite collapse Modulation Map) model for image encryption. The proposed 2D-SIMM model is derived out of sine map and Iterative Chaotic Map with Infinite Collapse (ICMIC). In this technique, scrambling effect is achieved with the help of Chaotic Shift Transform (CST). Chaotic Shift Transform is used to change the value of pixels in the input image while the substituted value is cyclically shifted according to the chaotic sequence generated by 2D-SIMM model. These chaotic sequences, generated using 2D-SIMM model, are sensitive to initial conditions. In the proposed algorithm, these initial conditions are optimized using JAYA optimization algorithm. Correlation coefficient and entropy are considered as fitness functions in this study to evaluate the best solution for initial conditions. The simulation results clearly shows that the proposed algorithm achieved a better performance over existing algorithms. In addition, the VLSI implementation of the proposed algorithm was also carried out using Xilinx system generator. With optimization, the correlation coefficient was −0.014096 and without optimization, it was 0.002585.

Keywords: Chaotic mapping; 2D-SIMM; encryption; decryption; jaya optimization

1 Introduction

Digital image contains more information owing to which it should be secured from unauthorized persons during transmission over communication channel. Conventional cryptosystems such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES) are not suitable for digital image and video encryption on real-time basis. This is because of its low speed due to large data volume and correlation among pixels. In order to overcome this challenge, chaotic maps are used in image encryption process.

A two-dimensional Sine ICMIC Modulation Map (2D-SIMM) is derived from Sine map while Iterative Chaotic Map with Infinite Collapse (ICMIC) and its chaotic performance are analyzed by a few means namely phase diagram, Lyapunov exponent spectrum and complexity [1]. It shows that the map has good ergodicity, hyperchaotic behavior, maximum Lyapunov exponent and heavy complexity. Based on this map, a fast image encryption algorithm is proposed. In this algorithm, both confusion and diffusion processes are combined at one stage. Chaotic Shift Transform (CST) is proposed to change the position of image pixel efficiently whereas the row and column substitutions are applied to scramble the pixel values simultaneously. The optimization algorithm is proposed to resolve the constrained and unconstrained optimization problems for encryption [2]. This algorithm is based on the concept that the solution obtained for a given problem should move towards the best solution leaving beside the worst solution. This algorithm requires only the common control parameters and does not require any algorithm-specific control parameters. The performance of the algorithm was investigated through implementation on 24-constrained benchmark functions and the outcome was compared against other optimization algorithms such as Genetic Algorithm (GA), Particle Swarm Optimization (PSO), Artificial Bee Colony (ABC) etc.,

In literature, a singular value decomposition-based digital image watermarking using optimization algorithms like Particle Swarm Optimization (PSO) and Jaya algorithm was proposed [3]. At the time of watermark embedding and extraction, optimization algorithms such as Jaya and PSO algorithms were applied to improve the robustness and imperceptibility by assessing its fitness function. In order to evaluate the performance of the proposed watermarking algorithm, robustness and imperceptibility were calculated using 2D correlation coefficient under various noise attacks like additive Gaussian noise, JPEG compression, scaling, rotation and filtering. The experimental analysis results shows that performance of Jaya algorithm was better than PSO in terms of imperceptibility and robustness since the best and worst values of fitness functions are selected directly in this regard. The complexity of Jaya algorithm is less compared to PSO. Logistic map is a chaos function to confuse the pixels and modified Knuth shuffling algorithm is used to diffuse the pixels in the image. Logistic map parameter is used as 256-bit secret key whereas these parameters are optimized using Teaching Learning Based Optimization algorithm (TLBO) and Gravitational Search Algorithm (GSA) by using correlation coefficient as fitness function that results in the least correlation among adjacent pixels [4]. A combination of sine map and logistic map was used to derive 2D-SLMM (two dimensional sine logistic modulation map). 2D-SLMM model is used to generate chaotic sequences. A 256-bit key is used to generate the initial condition for 2D-SLMM model. In order to reduce the correlation between the adjacent pixels, Chaotic Magic Transform (CMT) is used to substitute and permute the pixel of the original image [5]. It randomly connects the pixels from different rows and columns into circles, and then shifts them within circles which results in encrypted image.

Image encryption is based on three chaotic maps. The algorithm is based on the concept of shuffling the position of pixels and changing the gray values of image pixels [6]. A plain-image is first decomposed into 8 x 8 size blocks after which block-based shuffling of image is carried out using 2D Cat map. Further, the control parameters of shuffling are randomly generated by 2D-coupled Logistic map. After that, the shuffled image is encrypted using chaotic sequence generated by 1D logistic map. This encryption algorithm has information entropy close to the ideal value 8 and has low correlation coefficients close to the ideal value i.e., 0. Lorenz system is used to encrypt and decrypt the image with the help of a symmetric key. It performs two rounds of diffusion operation, one round of pixel permutation and three rounds of matrix rotation (180 degrees). This system is used to generate chaotic sequences. Diffusion is achieved with the help of three different secret key streams whereas XOR operation is used for encryption for the permutation of pixels [7]. In order to improve the pseudo randomness of Skew Tent map (STM), a new chaotic system named ‘Enhanced Skew Tent map (ESTM)’ was proposed. The image was encrypted using the Enhanced Skew Tent map whereas this study evaluated the pseudo randomness between classic STM and ESTM [8].

The conceptual description of hardware & software simulation for image processing, using Xilinx System Generator (XSG), provides both theoretical as well as practical aspects of the technique. This also provides a set of Simulink models for several hardware operations using different Xilinx that could be implemented on various FPGA. This research paper also explained about the efficient architecture for various image processing algorithms to be used in image negatives, image enhancement, contrast stretching, Image Edge Detection, image Brightness Control, Parabola transformation for gray scale and color images. This is done so with the help of a few possible system generator blocks, implemented in Virtex5 hardware [9]. Various image encryption algorithms are proposed to improve the image encryption techniques [10–14].

In current study, the authors propose a novel optimization-based 2D-SIMM (two-dimensional Sine Iterative chaotic map with infinite collapse Modulation Map) model for image encryption. The proposed 2D-SIMM model is derived from sine map and Iterative Chaotic Map with Infinite Collapse (ICMIC). In this technique, scrambling effect is achieved with the help of Chaotic Shift Transform (CST). Chaotic Shift Transform is used to change the value of pixels in input image and the substituted value is shifted cyclically, as per the chaotic sequence generated by 2D-SIMM model. These chaotic sequences, generated using 2D-SIMM model, are sensitive to initial conditions. In the proposed algorithm, these initial conditions are optimized using JAYA optimization algorithm. Correlation coefficient and Entropy are considered to be the fitness functions to evaluate the best solution for initial conditions.

Rest of the paper is organized as follows; Section 2 discusses about the chaotic maps for image encryption, Section 3 describes about the proposed image encryption algorithm, Section 4 deals with optimization algorithm. Section 5 discusses about simulation, performance metrics and results. Finally, Section 6 concludes the paper by highlighting the novelty of the proposed work.

2 Chaotic Mapping for Image Encryption

Chaotic map is a map that exhibits some sort of chaotic behavior. It is useful in studying about dynamic systems. Different types of chaotic maps exists while some of the 1-D chaotic maps are logistic map, sine map, ICMIC map, henon map and Arnold cat map. Generally, in image encryption, these chaotic maps are used to generate pseudo random numbers. Thus, the image can be encrypted using chaotic sequences generated by the chaotic map. Since the chaotic maps are used in image encryption, this technique is also called as chaotic cryptography.

2.1 2D-SIMM Model

Sine map and Iterative Chaotic Map with Infinite Collapse (ICMIC) are two commonly used 1D chaotic maps. They are defined through the following Eqs. (1) and (2) respectively.

$$\mathrm{Xi}+\ 1=\ \mu\mathrm{Sin}\ (\pi\mathrm{Xi}),\quad \mathrm{Xi}\ \epsilon[0,\ 1],\quad \mu>1 \tag{1}$$

$$\mathrm{Xi}\ +\ 1\ =\ \mathrm{Sin}\ (\mathrm{a}/\mathrm{Xi}),\quad -1\ \leq\ \mathrm{Xi}\ \leq+\ 1\cdots\mathrm{a}\varepsilon[0,\ +\infty] \tag{2}$$

The orbits of both of the one-dimensional chaotic maps are easy to predict with the help of chaotic signal estimation technologies. In order to overcome this problem, 2D-SIMM (two dimensional sine ICMIC modulation map) model is used. It can be defined by the Eq. (3).

$$\begin{aligned}\mathrm{X\ i}\ +\ 1\ &=\ \mathrm{a}\ \sin\ (\pi\mathrm{Yi})\sin\ (\mathrm{b}/\mathrm{Xi})\\ \mathrm{Y\ i}\ +\ 1\ &=\ \mathrm{a}\ \sin\ (\pi\mathrm{X\ i}\ +\ 1)\sin\ (\mathrm{b}/\mathrm{Yi})\end{aligned} \tag{3}$$

Here, a and b are control parameters and a, b (0, +∞). When a = 1, b = 5, the system has two positive Lyapunov exponents [1]. Therefore, 2D-SIMM model is a hyperchaotic map.

2.2 Characteristics of Chaotic Map

A chaotic map can be characterized with the help of two important parameters such as Lyapunov Exponent and Phase diagram.

2.2.1 Lyapunov Exponent

Chaotic behaviors of a dynamic system can be evaluated by Lyapunov exponent (LE). This exponent explains the divergence between two nearby points in a phase plane. Lyapunov exponent has positive values only, when the divergence between nearby points increases. If close trajectories converge at each other, then Lyapunov exponent remains negative. A HD chaotic map has at least two LE values and the maximum LE (MLE) value determines its predictability. There are chaotic behaviors when MLE value is positive and exhibits hyper chaotic behaviors, when it has more than one positive LE value. A HD chaotic map with hyper chaotic behaviors generally has high complexity and its trajectories are extremely difficult to predict.

2.2.2 Phase Diagram

Fig. 1 shows the attractor of 2D-SIMM with initial conditions (x0, y0) = (0.3, 0.4) and control parameters for a = 1 and b = 5 [1]. The attractor of 2D-SIMM gets distributed in much larger regions. It means that they have better ergodicity and large keys pace. In addition, the attractor of 2D-SIMM is symmetrical on both x-axis and y-axis, which is suitable for designing a pseudo-random sequence generator.

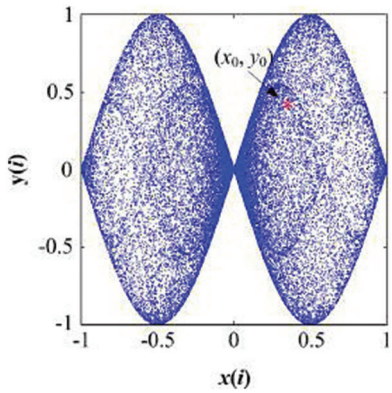

Figure 1: Phase diagram of 2D-SIMM

2.3 Structure of the Secret Key

The size of the secret key, used to encrypt the image, is a 256-bit sequence as shown in Fig. 2. It is composed of initial condition of 2D-SIMM (X01, Y01, X02, Y02) where, X01 and X02 are used for diffusion of pixels during round 1 and round 2 respectively whereas Y01 and Y02 are used for confusion of pixels during round 1 and round 2 respectively.

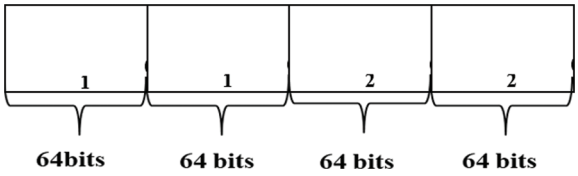

Figure 2: Secret key structures

2.4 Chaotic Shift Transform

To reduce the correlation between the adjacent pixels of a digital image, Chaotic Shift Transform is used to scramble the pixel value and pixel position of an original image. Let S be a chaotic series matrix generated by 2D-SIMM. Through specific quantification algorithm, a row shift matrix A= [a1, a2, …, aM]T and a column shift matrix B=[b1, b2, …, bN]T are obtained. Here, ai represents the step size of cyclic right shift in row i whereas bi represents the step size of cyclic upward shift in column i and ai [0, M−1] and bi [0, N−1] are integers. Chaotic Shift Transform (CST) is defined by T = F (P, S) where S denotes the CST function, P is the original image with the size of M*N and T be the corresponding shuffled image.

Step by step procedure

Step 1: Generate the row and column shift matrices, A and B by S respectively.

Step 2: Consider the pixels of the row in original image. The number of elements in the chaotic sequence should be equal to the number of pixel in row (or column) of the input image.

Step 3: These pixels are cyclically shifted in row i of the image P towards right with the step size of ai in row matrix A.

Step 4: If all the row pixels are shifted, then consider the row shift results as T1.

Step 5: Now consider the row shift matrix T1 and column matrix B. These pixels are cyclically shifted in column i of T1 to the top with a step size of bi in column matrix, B.

Step 6: When all the column pixels are shifted, the encrypted image T is obtained.

During decryption, the direction of shift is opposite (i.e.,) for column decryption while the image pixels are cyclically shifted towards the bottom of the column. In case of row decryption, the row pixels are shifted toward the left of that row.

3 Proposed Image Encryption Algorithm

A gray scale image sized 128 * 128 pixels and a secret key size of 256-bit sequence is used for encryption and decryption processes. During encryption, the image is substituted by the chaotic sequence generated by 2D-SIMM. Then, the permutation of pixels is achieved with the help of Chaotic Shift Transform (CST). The encryption algorithm for one round is shown in Fig. 3.

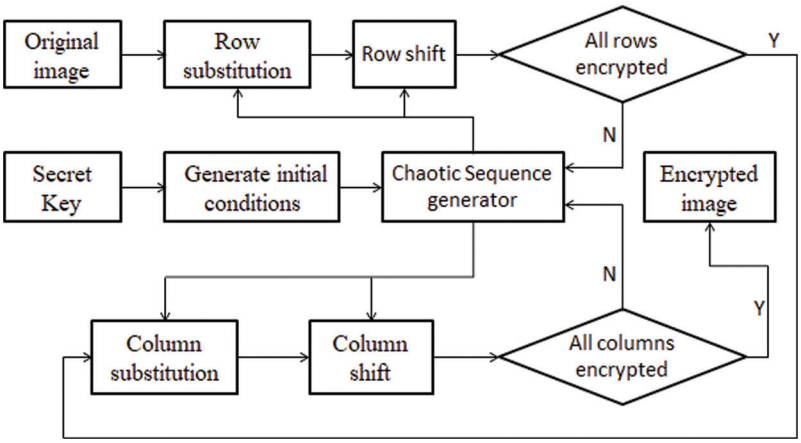

Figure 3: Encryption flowchart for one round

3.1 Row Encryption

Consider the input image of size M × N, then the first round of row encryption can be accomplished based on the following steps,

Step 1: Consider the first row i of the input image. The initial conditions (X01, Y01) are substituted in 2D-SIMM model Eq. (3) and is iterated for 50 times (N0 = 50)to avoid the transient effect and enhance initial value sensitivity.

Step 2: Iterate Eqs. (4) and (5) for i= 1 to 128 so as to obtain the chaotic sequence. The range of the generated sequence is from −1 to + 1. Therefore, to obtain the chaotic sequences around the pixel value, the obtained sequence is then substituted in the following equation as follows

$$K1 = \mathrm{mod}\left(\lfloor x^{*}(10\text{^}5)\rfloor,\ 255\right) + 1 \tag{4}$$

$$K2 = \mathrm{mod}\left(\lfloor y^{*}(10\text{^}5)\rfloor,\ R\right) + 1 \tag{5}$$

where K1 and K2 are integers, and K1 [1, 255], K2 [1, R]. When the row is shifted, then R=N−1. When the column is shifted, then R=M−1.

Step 3: For I th row pixels, calculate P (i, ·) = P(i, ·) K1.

Step 4: Connect P (i, ·) into circle, and shift these pixels to right with a step size of k2.

Step 5: Repeat steps 1 to 4 in a loop, until all the rows are encrypted.

3.2 Column Encryption

Step 1: The initial conditions i.e., (X01, Y01) are substituted in 2D-SIMM Eq. (3) and iterated for 50 times (N0 = 50 times) to avoid the transient effect and enhance the initial value sensitivity.

Step 2: Iterate Eq. (3.3) for i= 1 to 128 to obtain the chaotic sequence. To obtain the chaotic sequences around the pixel value, the obtained sequence is substituted in the Eqs. (4) and (5)

Step 3: Now consider the row has an encrypted image. For i^{th} column pixel, calculate

P (·, i) = P(·, i) K1.

Step 4: Connect P (·, i) into circle, and shift these pixels upward with a step size of k2.

Step 5: Repeat steps 1 to 4 in a loop until all the columns get encrypted. Thus, the encrypted image is obtained for one round.

3.3 Decryption Algorithm

Decryption is just the reverse operation of encryption. The difference between encryption and decryption is that the column is decrypted first while the row is decrypted next. Also, the direction of shift is opposite in decryption. Decryption algorithm for one round is shown in Fig. 4.

4 Optimization Algorithm

Optimization is a process of searching for the most optimal solution among the available solutions of a particular problem. By considering the nature of optimization algorithms, these can be categorized broadly under two groups such as Evolutionary algorithms (EA) and Swarm Intelligence (SI)0based algorithms. Both evolutionary and swarm intelligence-based algorithms are probabilistic algorithms and require common controlling parameters like population size, number of generations, elite size etc. Besides, in case of common control parameters, different algorithms require their own algorithm-specific control parameters. For example, GA uses mutation probability, crossover probability, selection operator; and PSO uses

inertia weight, particle position and particle velocity. Algorithm-specific parameters must be appropriately tuned which remains a very crucial factor since it affects the performance of the above-mentioned algorithms. In order to overcome this challenge, a new parameter-less optimization technique known as JAYA optimization algorithm is used in current study.

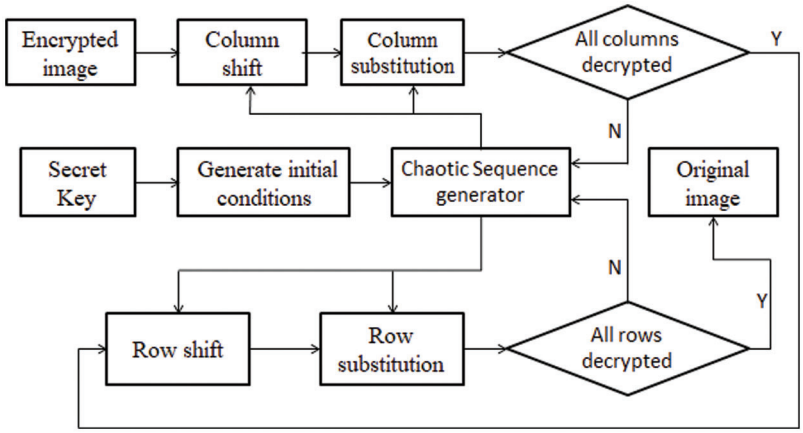

Figure 4: Decryption flow chart for one round

4.1 JAYA Optimization Algorithm

JAYA algorithm is a powerful heuristic method to solve the optimization problem. This algorithm tries to move as close as possible towards success (i.e., reaching the best solution) and avoids the failure (i.e., moving away from the worst solution). Further, it also strives to achieve victory by reaching the best solution. Hence, it is named after Jaya (a Sanskrit word meaning victory). It does not require any algorithm-specific parameter except three common control parameters namely, population size, number of design variables and number of generations to solve the optimization problem using fitness function. A single-objective optimization algorithm requires correlation coefficient and entropy or PSNR as its fitness functions. JAYA optimization algorithm is explained herewith.

Step 1: The number of design variables, population size and the termination criteria should be defined for the optimization problem.

Step 2: The population is initiated using random numbers, which forms the first generation. Each of these numbers in population is a possible solution of optimization problem.

Step 3: Each solution of current generation is tested using the fitness function so as to get the best and worst solutions

Step 4: Now each and every solution of the current generation is modified using Eq. (6).

If Xj, k, i are the values of j^{th} variable for k^{th} candidate during i^{th} iteration, then this value is modified as follow

$$X'j,\ k,\ i\ =\ Xj,\ k,\ i\ +\ r1,\ j,\ i\ (Xj,\ best,\ i-\ |Xj,\ k,\ i|)r2,\ j,\ i\ (Xj,\ worst,\ i-|Xj,\ k,\ i|) \tag{6}$$

where, X‟j, k, i is the updated value of Xj, k, i

X_j, $best_i$–the value of the variable j for the best candidate X_j, worst, i–value of the variable j for the worst candidate r1, j, i, r2, j, i–two random numbers in the range [0, 1].

Step 5: The new set of solutions, obtained from Eq. (6), gives the next generation of population.

Step 6: Now compare the performance of current generation population and the next generation population with the help of fitness function.

Step 7: If the solution of next generation population is better than the current generation population, then update the current generation. Otherwise, keep the current generation as it is.

The above steps are continued till the termination criterion is met.

4.2 Fitness Function Correlation Coefficient

Correlation is a method of establishing the degree of probability that exists in a linear relationship between two measured quantities. Generally, an image has high data redundancy. Thus, the pixels between two different images possess high correlations. A good image encryption algorithm should have the ability of breaking the correlations between original and the encrypted image. Therefore, correlation coefficients for two adjacent pixels, x and y can be defined as follows

$$Cov(x,\ y) = E\{(x - E(x)) - (y - E(y))\} \tag{7}$$

$$r_{xy} = \frac{\mathrm{cov}(x,\ y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{8}$$

where x and y are the grey values of two adjacent pixels in the image and E(x) and D(x) denote the expectation and variance of variable x, respectively.

The randomness of gray scale value can be measured by information entropy and can be defined as follows

$$H(m) = \sum_{i=0}^{M-1} p(m_i) \log \frac{1}{p(m_i)} \tag{9}$$

where M is the total number of symbols, p (mi) represents the probability of occurrence of symbol mi and log denotes base 2 logarithm so that the entropy is expressed in bits.

4.3 Generation of Initial Conditions

The initial conditions are generated using JAYA optimization with the help of correlation coefficient as fitness function. For this, 100 sets (population size) of four design variables are generated randomly in the range of 0 to 1. These four design variables are converted into double precision floating point format and are combined to form the secret key. Each candidate in this population, with 4 design variables, are used as initial condition for the 2D-SIMM model and the image is encrypted. Now, the correlation coefficient is calculated between the original and encrypted image for each candidate. The candidate with minimum correlation coefficient is selected as the best solution and the maximum as the worst solution. Now the design variables are updated based on best and worst solutions and are used to generate new population. The above steps are repeated for 25 times (termination criterion) and the best variables at the end of 25^{th} iteration are selected as initial condition for 2D-SIMM model. Generally, an image has high data redundancy. Thus, its pixels have high correlations with their neighboring pixels. A good image encryption algorithm should be able to break these correlations. Since optimization technique is a single objective optimization, correlation coefficient is used as the fitness function to evaluate the performance of the encrypted image.

Among four design variables, two variables are used for first round encryption whereas the other two variables are used for second round encryption. The initial conditions for the column encryption are the same as row encryption for each round. The images, thus encrypted using optimization technique, possess

low correlation coefficient which proves that the information in the encrypted image is different from the original image.

5 Simulation Results for JAYA Optimization Using MATLAB

This section discusses the simulation result and correlation coefficient with and without optimization. The best solutions were found to be 0.588643, 0.900000, 0.231928, and 0.773181. The correlation coefficient with optimization was −0.014096 and without optimization was 0.002585. The pixel distribution of the encrypted image is shown in Fig. 5 and the comparison results of correlation coefficients, with and without optimization, for different input image is shown in Tab. 1.

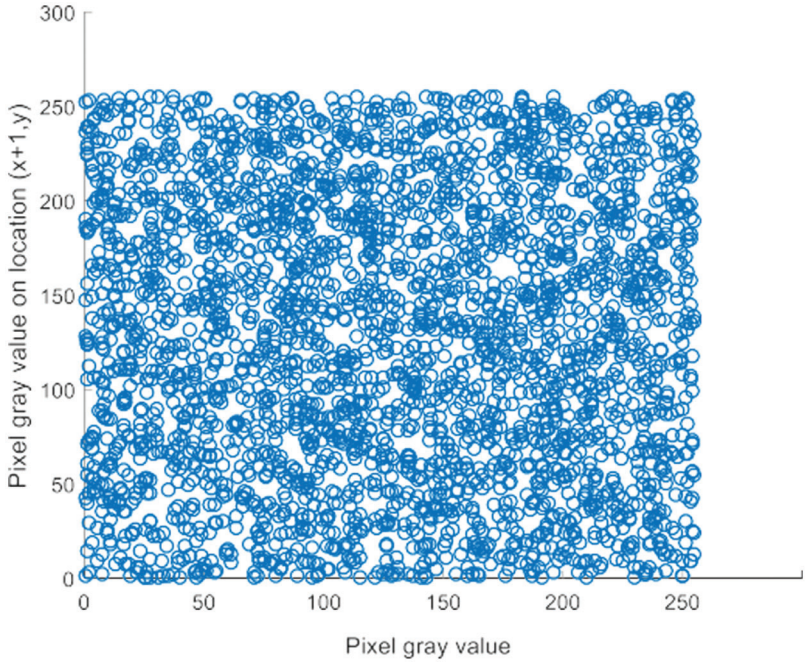

Figure 5: Pixel distribution of encrypted image

Table 1: Comparison of correlation coefficients with and without optimization

Name	CC of encrypted image without optimization	CC of encrypted image with optimization
Lena.jpg	0.0002	−0.0226
Fruit.jpg	−0.0479	−0.0643
Horse.jpg	−0.0012	−0.0182
Girl.jpg	−0.0012	−0.0023

After the generation of chaotic sequence, row encryption and column encryption using chaotic shift transform were executed for two rounds to obtain the encrypted image. Its reverse operation generated the decrypted image using MATLAB R2016a. Fig. 6 shows the encrypted image and its decrypted format.

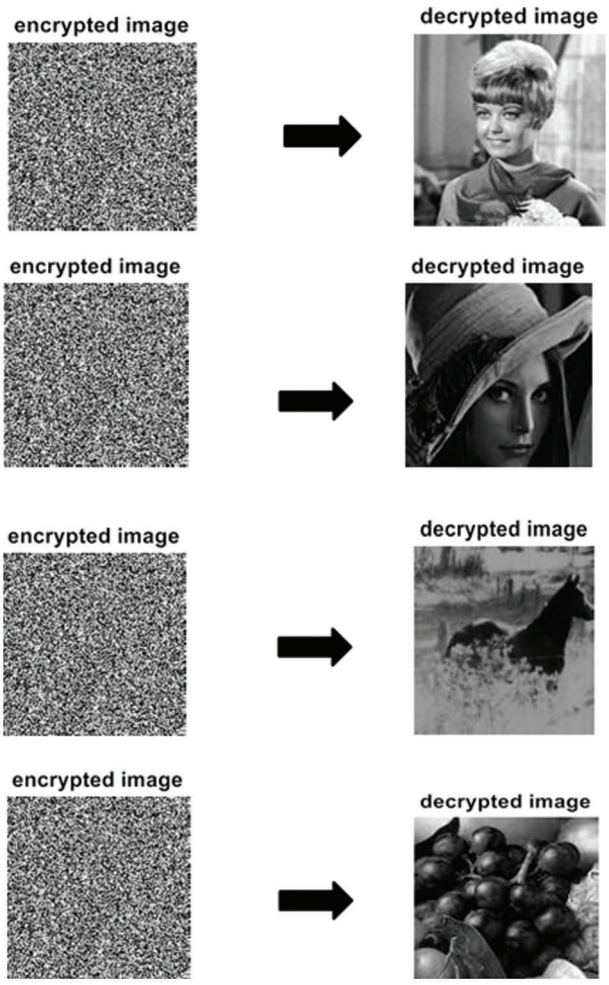

Figure 6: Encryption and decryption result

5.1 Performance Metrics

The performance metrics helps in understanding the performance and characteristics of the encryption algorithm. Some of the performance metrics measured using MATLAB R2016a are shown in Tab. 2.

Table 2: Correlation coefficient and entropy

Name	Correlation of original image	Correlation of encrypted image	Entropy of encrypted image
Hatgirl.jpg	0.9149	0.0002	7.9861
Fruit.jpg	0.9502	−0.0479	7.9879
Horse.jpg	0.9580	−0.0012	7.9860
Testi2.jpg	0.9471	0.0300	7.9886

5.2 Simulation Results Using System Generator

To generate the chaotic sequence, 2D-SIMM model was designed in system generator and the result is shown in Fig. 7 which also displays the width of the generated sequence.

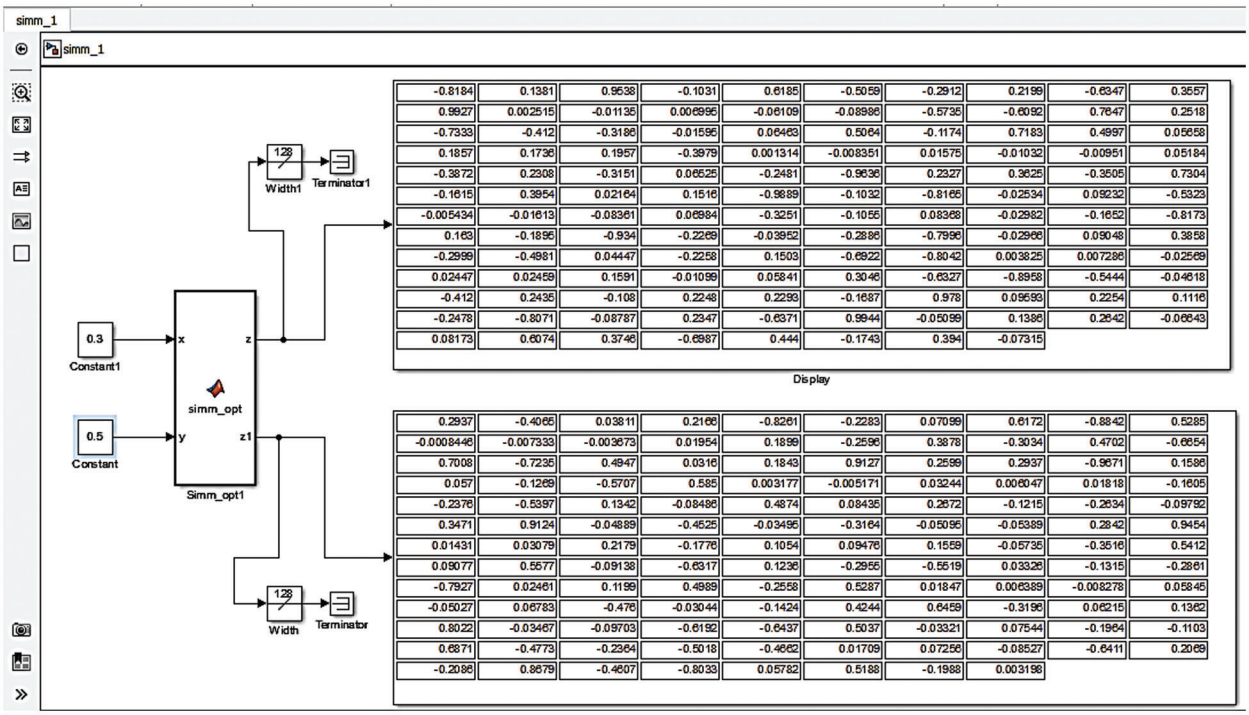

Figure 7: System generator design for 2D-SIMM model

5.3 VLSI Implementation of Proposed Encryption Model

In order to find the optimized initial condition, image encryption technique using 2D-SIMM model was designed as a subsystem in system generator as shown in Fig. 8 which was used to evaluate the fitness function.

5.4 Design for Image Encryption with Optimization

The system generator model, for image encryption technique using optimization, is designed as shown in Fig. 9. This figure displays the encrypted image and its correlation coefficient along with the corresponding decrypted image.

5.5 Simulation Results for Encryption and Decryption

The simulation result for image encryption and decryption, using system generator, is shown in Fig. 10.

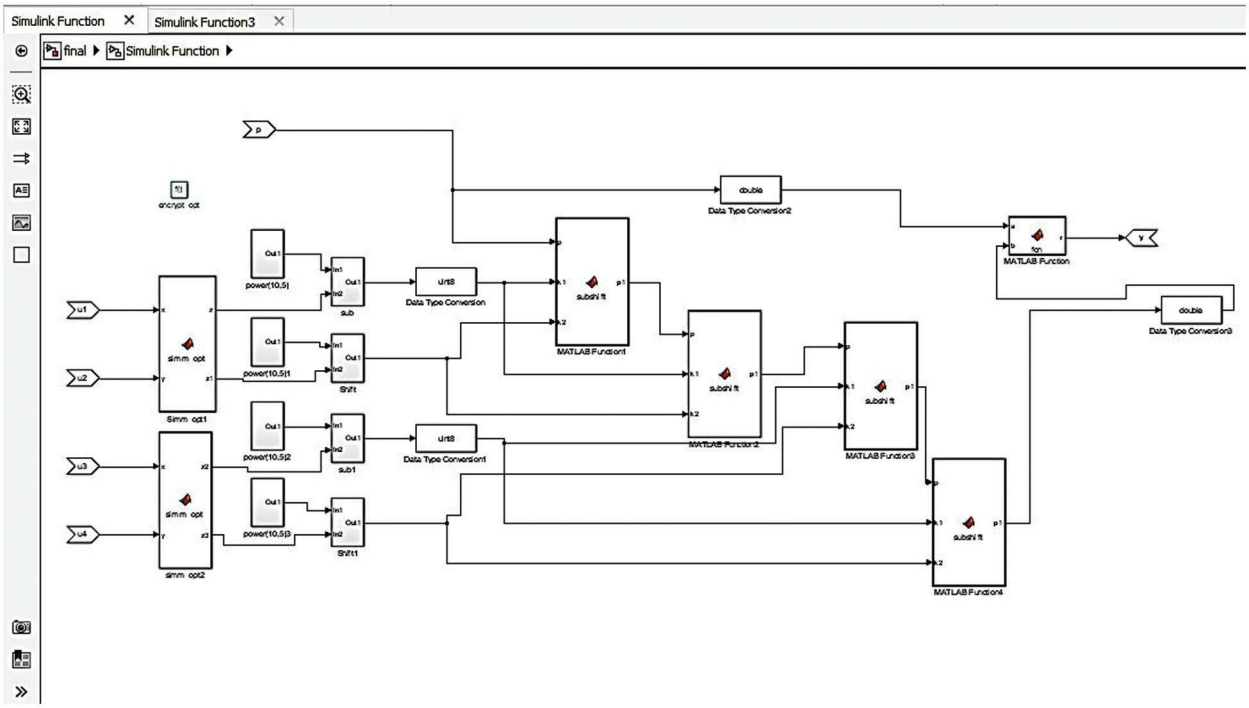

Figure 8: System generator design for Encryption technique

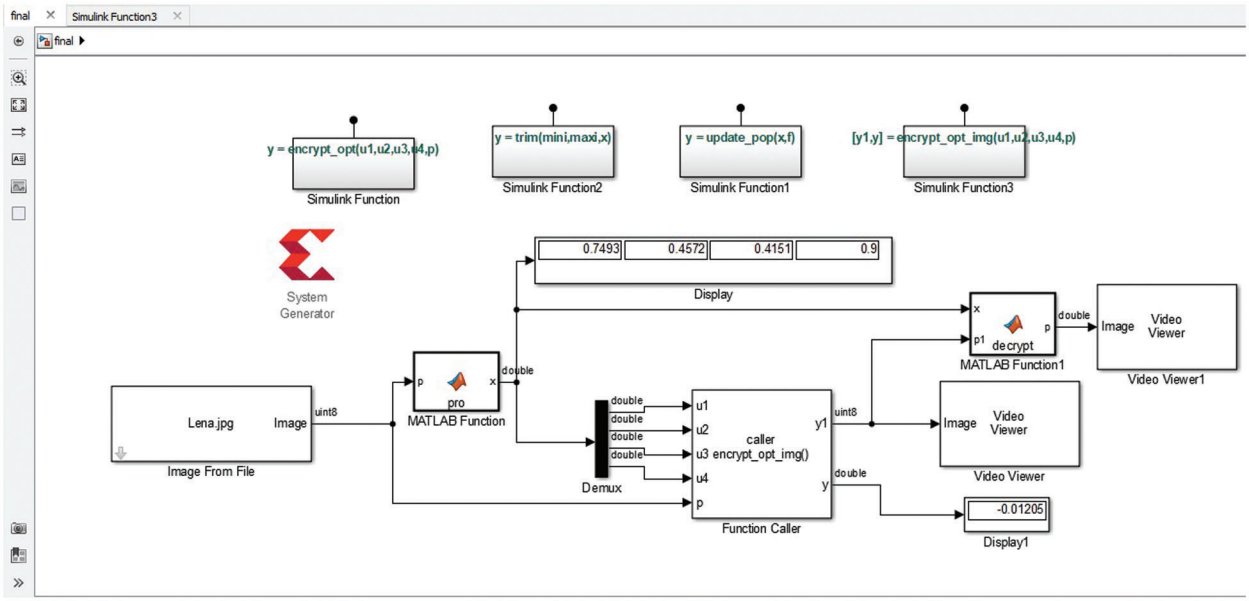

Figure 9: VLSI Implementation for encryption with optimization

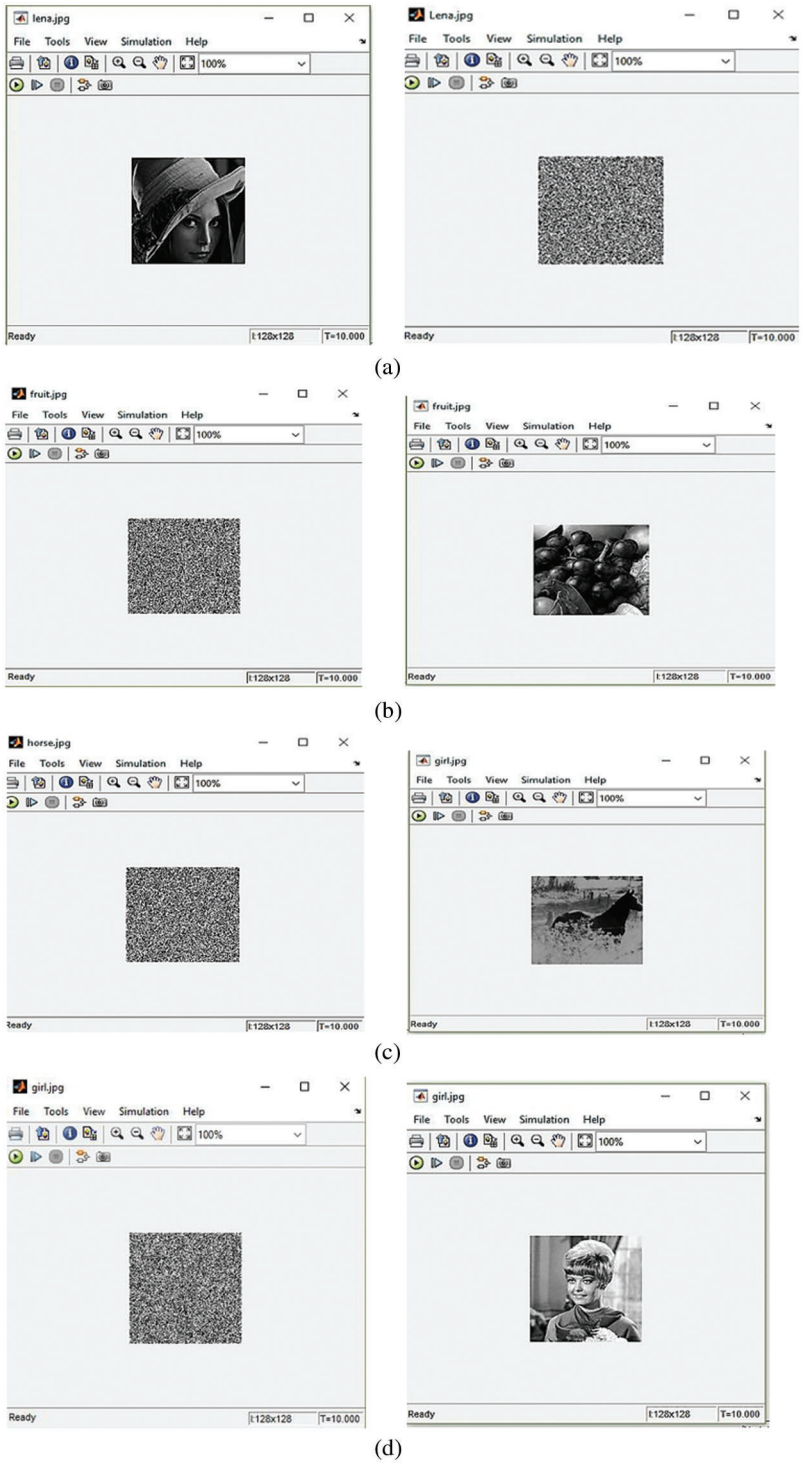

Figure 10: Encrypted image and its corresponding decrypted image

6 Conclusion

The initial condition for the proposed 2D-SIMM model was generated using optimization technique to minimize the correlation coefficient between the original and encrypted images. Further, Chaotic Shift Transform was deployed for confusion and diffusion of pixels in input gray scale image with the help of chaotic sequences generated from 2D-SIMM model. After CST, the resultant pixel matrix obtained the encrypted image. The simulation results obtained for the performance metrics show that the encrypted image has good scrambling effect and less correlation. VLSI implementation was performed using Xilinx System generator. Therefore, the proposed model seems to have good application prospects in image or video encryption communication. In future, the proposed model can be employed in real-time environment as well.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] W. Liu, K. Sun and C. Zhu, "A fast image encryption algorithm based on chaotic map," *Optics and Lasers in Engineering*, vol. 84, pp. 26–36, 2016.

[2] F. Masood, "A new color image encryption technique using DNA computing and chaos-based substitution box," *Soft Comput*, 2021. https://doi.org/10.1007/s00500-021-06459-w.

[3] F. N. Thakkar and V. K. Srivastava, "Performance comparison of recent optimization algorithm jaya with particle swarm optimization for digital image watermarking in complex wavelet domain," *Multidimensional Systems and Signal Processing*, vol. 30, no. 4, pp. 1769–1791, 2018.

[4] J. S. Khan, W. Boulila, J. Ahmad, S. Rubaiee, A. U. Rehman *et al.,* "DNA and plaintext dependent chaotic visual selective image encryption," *IEEE Access*, vol. 8, pp. 159732–159744, 2020, https://doi.org/10.1109/ACCESS.2020.3020917.

[5] Z. Hua, Y. Zhou, C. M. Pun and C. L. P. Chen, "2D sine logistic modulation map for image encryption," *Information Sciences*, vol. 297, pp. 80–94, 2015.

[6] A. Qayyum, J. Ahmad, W. Boulila, S. Rubaiee, F. Masood *et al.,* "Chaos-based confusion and diffusion of image pixels using dynamic substitution," *IEEE Access*, vol. 8, pp. 140876–140895, 2020, https://doi.org/10.1109/ACCESS.2020.3012912.

[7] X. R. Zhang, X. Sun, W. Sun, T. Xu and P. P. Wang, "Deformation expression of soft tissue based on BP neural network," *Intelligent Automation & Soft Computing*, vol. 32, no. 2, pp. 1041–1053, 2022.

[8] X. R. Zhang, X. Chen, W. Sun and X. Z. He, "Vehicle Re-identification model based on optimized densenet121 with joint loss," *Computers, Materials & Continua*, vol. 67, no. 3, pp. 3933–3948, 2021.

[9] L. Zhang, X. Liao and X. Wang, "An image encryption approach based on chaotic maps," *Chaos*," *Solitons and Fractals*, vol. 24, no. 3, pp. 759–765, 2005.

[10] D. He, C. He, L. G. Jiang, H. W. Zhu and G. R. Hu, "A chaotic map with infinite collapses," in *2000 TENCON Proc.. Intelligent Systems and Technologies for the New Millennium (Cat. No.00CH37119)*, Kuala Lumpur, Malaysia, vol. 2, pp. 95–99, 2000.

[11] Y. Wu, "Image encryption using the two-dimensional logistic chaotic map," *Journal of Electronic Imaging*, vol. 21, no. 1, pp. 013014, 2012.

[12] J. Chen, Z. Zhu, C. Fu, H. Yu and L. Zhang, "An efficient image encryption scheme using gray code based permutation approach," *Optics and Lasers in Engineering*, vol. 67, pp. 191–204, 2015.

[13] D. Chen and Y. Chang, "A novel image encryption algorithm based on logistic maps," *Advances in Information Sciences and Service Sciences Issues*, vol. 03, no. 7, pp. 364–372, 2011.

[14] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 08, pp. 2129–2151, 2006.