Received: 18 June 2024 | *Revised:* 15 August 2024 | *Accepted:* 1 September 2024
DOI: 10.37917/ijeee.21.1.6 *Early View* | *June 2025*

Iraqi Journal for Electrical and Electronic Engineering
Original Article

Open Access
IJEEE University of Basrah College of Engineering

Design and FPGA Implementation of a Hyper-Chaotic System for Real-time Secure Image Transmission

Abdul-Basset A. Al-Hussein*[1], Fadhil Rahma Tahir[1], Ghaida A. Al-Suhail[2]
[1]Department of Electrical Engineering, University of Basrah, Basrah, Iraq
[2]Department of Computer Engineering, University of Basrah, Basrah, Iraq

Correspondance
*Abdul-Basset A. Al-Hussein
Department of Electrical Engineering, University of Basrah,
Basrah, Iraq
Email: abdulbasset.jasim@uobasrah.edu.iq

Abstract
Recently, chaos theory has been widely used in multimedia and digital communications due to its unique properties that can enhance security, data compression, and signal processing. It plays a significant role in securing digital images and protecting sensitive visual information from unauthorized access, tampering, and interception. In this regard, chaotic signals are used in image encryption to empower the security; that's because chaotic systems are characterized by their sensitivity to initial conditions, and their unpredictable and seemingly random behavior. In particular, hyper-chaotic systems involve multiple chaotic systems interacting with each other. These systems can introduce more randomness and complexity, leading to stronger encryption techniques. In this paper, Hyper-chaotic Lorenz system is considered to design robust image encryption/ decryption system based on master-slave synchronization. Firstly, the rich dynamic characteristics of this system is studied using analytical and numerical nonlinear analysis tools. Next, the image secure system has been implemented through Field-Programmable Gate Arrays (FPGAs) Zedboard Zynq xc7z020-1clg484 to verify the image encryption/decryption directly on programmable hardware Kit. Numerical simulations, hardware implementation, and cryptanalysis tools are conducted to validate the effectiveness and robustness of the proposed system.

Keywords
Chaos, FPGA, Hyper-chaotic System, Image Encryption, Xilinx System Generator.

I. Introduction

The current revolution in media exchange, along with the abundance and volume of information available via the internet, satellites, mobile devices, and various networks, has made it simple to obtain the information's content and made accessing content easier than ever. Concurrently, Since unlawful individuals might now access private material, one of the main issues facing individuals is protecting their data from these users. High security can usually be ensured conveniently with encryption, and several encryption schemes have lately been developed to meet these objectives. Indeed, given today's computational capabilities, the majority of conventional ciphering methods, including the linear feedback shift register (LFSR), advanced encryption standard (AES), international data encryption algorithm (IDEA), and data encryption standard (DES), are not fast enough for real-time image/video encryption due to high pixel correlation and large data volumes [1, 2]. Exploiting chaotic dynamics has attracted a lot of attention lately in the realms of encryption and communications.

Chaos is among the greatest discoveries in the engineering and physics fields. A class of dynamic systems that are very sensitive to disturbances in their unexcited states (initial conditions) or algebraic structures experience chaos, which is a nonlinear phenomenon that makes it unpredictable how these systems will evolve in time and space in the future. Both natu-

ral and artificial systems exhibit chaotic dynamics, and a deep comprehension of these properties has led to a wide range of applications in modeling, controlling, and improving the performance of engineering systems. The unique duality property of deterministic and stochastic properties in chaotic systems makes them particularly appealing for electronic engineering applications. This is because the signals produced by chaotic systems can be utilized as controlled noise sources, providing a compelling reason to investigate and develop hardware implementations of these systems [3].

Numerous domains of contemporary human endeavor, including architecture, landscaping, economics, finance, health, psychology, and meteorology, have discovered broad uses for chaos. Chaotic dynamics has been utilized in engineering to resemble real-world systems and improve the performance of already-existing ones, particularly in secure communications [4,5], antenna and radar systems [6], biomedical engineering [7–9], civil, mechanical, robotics [10], power systems [11–13] etc.

Given that hyperchaotic systems have many positive Lyapunov exponents, they are characterized by dynamic reactions that expand in several directions. According to [14], this feature results in dynamical behavior that is more complicated than that of typical chaotic systems. Using hyperchaotic systems in image encryption offers several advantages, particularly in terms of enhanced security and complexity. Hyperchaotic systems exhibit more intricate dynamics compared to regular chaotic systems, and these dynamics can be harnessed to create stronger encryption schemes.

Numerous scholarly papers have shown the superior performance and efficacy of chaos-based cryptography in comparison to traditional cryptography [15,16]. The foundation of chaos-based secure communication is the chaos synchronization principle, which states that two divergent state trajectories of identical or non-identical chaotic systems can be brought into partial, antiphase, phase, or complete synchronous state in a finite amount of time by developing nonlinear control strategies. The possibility of encrypting and decrypting communications sent via communication channels is primarily explained by this theory. The original data could now be recovered as it was possible to recreate the chaotic sequence that was used for encryption on the emitter side at the receiving side. The literature has investigated a number of synchronization strategies, including generalized synchronization [17], fuzzy synchronization [18], hybrid feedback synchronization [19,20], and intelligent control-enhanced synchronization approaches. In order to confirm the safe operation of the communication strategy, Bian and Yu [21] conducted a circuit simulation and presented a novel chaotic communication encryption technique based on a 6-D hyperchaotic Lorenz system. A 6-D hyperchaotic system was developed by Wang et al. [22] and used to wrap up designing the circuits for signal encryption and decryption in a secure communication strategy. A novel 5-D hyperchaotic system for secure communication based on Micro Controller Units (MCUs) was suggested by Peng et al. [23]. A cellular neural network (CNN) based memristive hyperchaotic system was proposed and its hardware circuit design was detailed by Xiu et al. [24]. The design and modeling of a 4-D hyperchaotic communication system based on the chaotic Lorenz attractor were reported by Alibraheemi et al. [25].

While software-based encryption solutions are widely used, they may not always provide the highest level of security. Hardware-based encryption, on the other hand, involves implementing encryption algorithms directly on dedicated chips or processors. This offers several advantages such that: hardware-based encryption can be more resistant to various attacks, such as side-channel attacks, compared to software-based solutions. Moreover, Dedicated encryption chips can process data more efficiently, leading to better performance and faster encryption/decryption speeds.

The use of FPGA instead of analogue circuits is better for several reasons. Analogue chaotic generators in communication systems require precise synchronization between the transmitter and receiver, which is challenging due to the variability of analogue components with age and temperature [26]. Digital hardware, such as FPGA, offers a more reliable solution. FPGAs provide practical advantages over analogue components, including easier specification of initial conditions, insensitivity to component tolerance, and avoidance of saturation issues [27]. Additionally, FPGAs can achieve high frequencies, making them superior for this application [28].

Motivated by the above discussions, in this paper we presented the following aspects: investigating the hyper-chaotic dynamics of the four-dimensional Lorenz system. The analysis shows the elegant characteristics of the introduced hyperchaotic model that are useful for the cryptographic encryption process. The hardware implementation of the presented hyperchaotic model is shown using FPGA technology. The fixed point representation is provided to optimize the FPGA resource utilization. The chaotic generators are first represented by a set of nonlinear equations and a system-based model is developed to represent these equations directly. The complicated VHDL code is developed from a block design, which is then utilized to set up the intended FPGA board. When generating an FPGA programming file, all downstream FPGA development processes—such as synthesis and place and route—are carried out automatically. Then applied a chaotic signal to encrypt the image, ensuring secure transmission and access in an open network environment by transforming the meaningful image into an unrecognized noise-like image.

This paper consists of six sections. Following this intro-

duction, Sec. II. , introduces the mathematical model of the presented hyperchaotic Lorenz system. Nonlinear analysis tools are used to reveal the dynamic behavior of the model and discuss the elegant features of the introduced hyperchaotic model. In Sec. III. , the FPGA realization of the introduced system is investigated, along with the design optimization aspects. In Sec. IV. , the chaos synchronization model used in this work has been elaborated. The FPGA implementation results of the proposed cryptographic system and cryptanalysis measures are given in Sec. V. The main conclusions and discussion are presented in Sec. VI.

II. Hyperchaotic System Dynamics

This section will go through the main attractive and elegant properties of the considered hyperchaotic system. The presented mathematical model is an extended version of the Lorenz model but with many advantages for the application as a chaotic generator for cryptographic applications. The model is given by (1) as follows [29]:

$$\begin{cases} \dot{x} = a(y-x) \\ \dot{y} = -xz - w \\ \dot{z} = xy - b \\ \dot{w} = my \end{cases} \tag{1}$$

where a and b are system (1) parameters. The first elegant property of the presented model is that it has no equilibrium points, where equating the left side of the model to zero gives no real solution, satisfying that a and b are nonzero. This feature is very useful for building chaotic generators (nonlinear oscillators) with no danger that the oscillations would stop. Furthermore, related to systems with no equilibrium states, so any attractors of the system are hidden. And this is increasing the complexity of the system dynamics and making it a better choice for cybersecurity applications. Also, even that the system has no equilibrium state, the system solution is bounded as the hypervolume rate of change is negative as demonstrated by the Lie type derivative as follows (2):

$$\nabla V = \frac{\partial \dot{x}}{\partial x} + \frac{\partial \dot{y}}{\partial y} + \frac{\partial \dot{z}}{\partial z} + \frac{\partial \dot{w}}{\partial w} = -a \tag{2}$$

where a is a positive parameter. As a result, system (1) is dissipative, and its responses contract onto an attractor of zero measure in 4-D state space as time approaches infinity.

Another elegant feature of the considered chaotic model, is that the system has two positive Lyapunov exponents. So, its dynamical responses expand in multi-direction, this fact leads to dynamics with more complex behavior and render the model as hyperchaotic system, which is very sensitive to initial conditions and system parameters, and this is making it preferred in security applications. The four Lyapunov exponent of the considered hyperchaotic system are given in Figs. 1 and 2 . It is commonly recognized that no nonlinear system control parameter can sustain the chaotic behavior of a given chaotic system; as a result, factors that do not produce chaotic behavior produce weak keys. We may distinguish chaotic from non-chaotic areas of a given system with the use of the Lyapunov exponents. Each parameter that is utilized as a key should thus be outside of areas that are not chaotic. We provide a straightforward approach that involves choosing limiting ranges for the keys around each parameter value in order to stay out of this scenario. In accordance to Lyapunov exponents spectrum of introduced hyperchaotic Lorenz model; the chaotic behavior is maintained for $a \in [4.5,\ 10]$ and $m \in [0,\ 11]$. So, the keys should be selected from these predetermined ranges.

A Poincaré section plotted in Fig. 3 shows the hyperchaotic region whose dimension is at least 2.0. The map shows the symmetry property of the hyperchaotic model and a dense area. The considered model has a strong nonlinear interaction that can be shown by finding the higher-order spectra and the relationship between system different frequency modes. Let x(t) be a stationary random process defined as [30]:

$$x(t) = \sum_{n=1}^{N} A_n e^{j\omega_n t} + A_n^* e^{-j\omega_n t} \tag{3}$$

where the complex Fourier coefficients are A_n, the frequency mode index is n, and the radian frequency is given by w. Then one could describe the power spectrum as follows:

$$P(\omega_k) = E\left[A_{\omega_k} A_{\omega_k}^*\right] \tag{4}$$

and discrete bispectrum can be defined as,

$$B(\omega_k, \omega_j) = E\left[A_{\omega_k} A_{\omega_j} A_{\omega_k+\omega_j}^*\right] \tag{5}$$

The time series are split into M sections, each of which has a length of N, in order to compute the bispectrum. Both biperiodogram and Fourier transformations are then computed. They are subsequently averaged over all segments. Bicoherence functions have two distinct frequencies as inputs and their sum as outputs, but their output is one-dimensional. Bicoherence can therefore be thought of as an aspect of the sum of two frequencies. Pezeshki [31] provides the chaotic system's autobispectrum. The Fourier coefficients are used to compute autobispectrum:

$$B(\omega_1, \omega_2) = E\left[A(\omega_1) A(\omega_2) A^*(\omega_1 + \omega_2)\right] \tag{6}$$

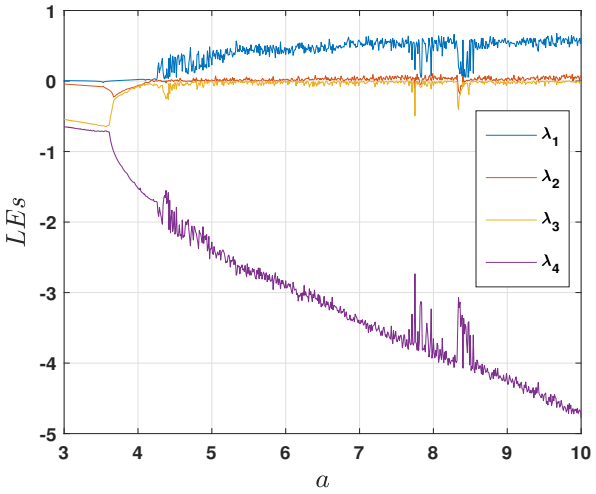


Fig. 1. Lyapunov Exponent of (1), with respect to a.

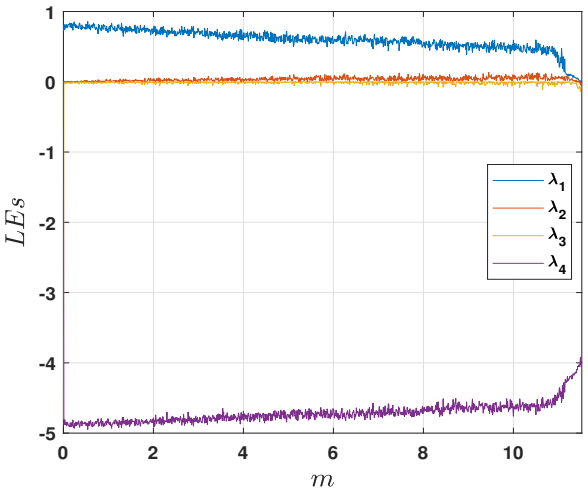


Fig. 2. Lyapunov Exponent of (1), with respect to m.

where w_n is the angular frequency and A is the Fourier coefficients. The value of bicoherence square can be provided as follows:

$$b(\omega_1,\omega_2) = |B(\omega_1,\omega_2)|^2 / P(\omega_1)P(\omega_2)P(\omega_1+\omega_2) \quad (7)$$

where $P(\omega_1)$ and $P(\omega_2)$ are the power spectrums at f_1 and f_2.

Fig. 4 shows the bicoherence contours of the considered system for state x. As it is shown in Fig. 4, the cross-bicoherence is nonzero and non-constant; hence, the state relationship is nonlinear with broadband power spectral density. Due to the broadband spectrum feature of the chaotic system, it is very suitable to use this system in secure communication applications [32]. All the previously discussed

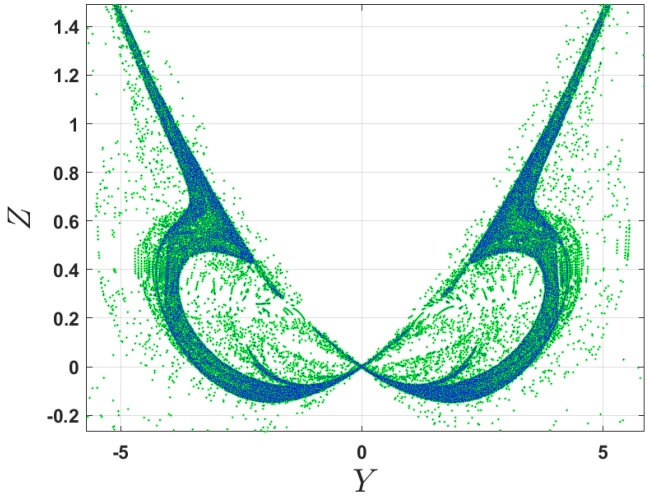


Fig. 3. Poincaré Map of (1) at the surface $z = xy/10$.

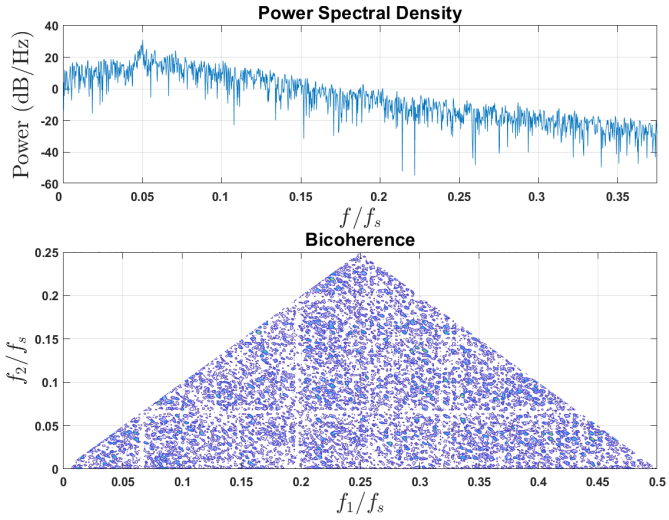


Fig. 4. Bicoherence and PSD of (1).

measures emphasize the usefulness of the presented model as a chaotic generator.

III. FPGA Realization

The discrete integration approach can be employed to decrease FPGA resource utilization when designing chaotic generators like the Lorenz attractor; however, it may introduce rounding errors and cause the result to not converge. As long as the differential equation solutions converge at a certain step size, the issue of fixed-point approximation inaccuracies will always exist and may be tolerated [33]. One of the first-order numerical approach for resolving ODEs is the Euler method. A diminished Taylor series expansion serves as the foundation

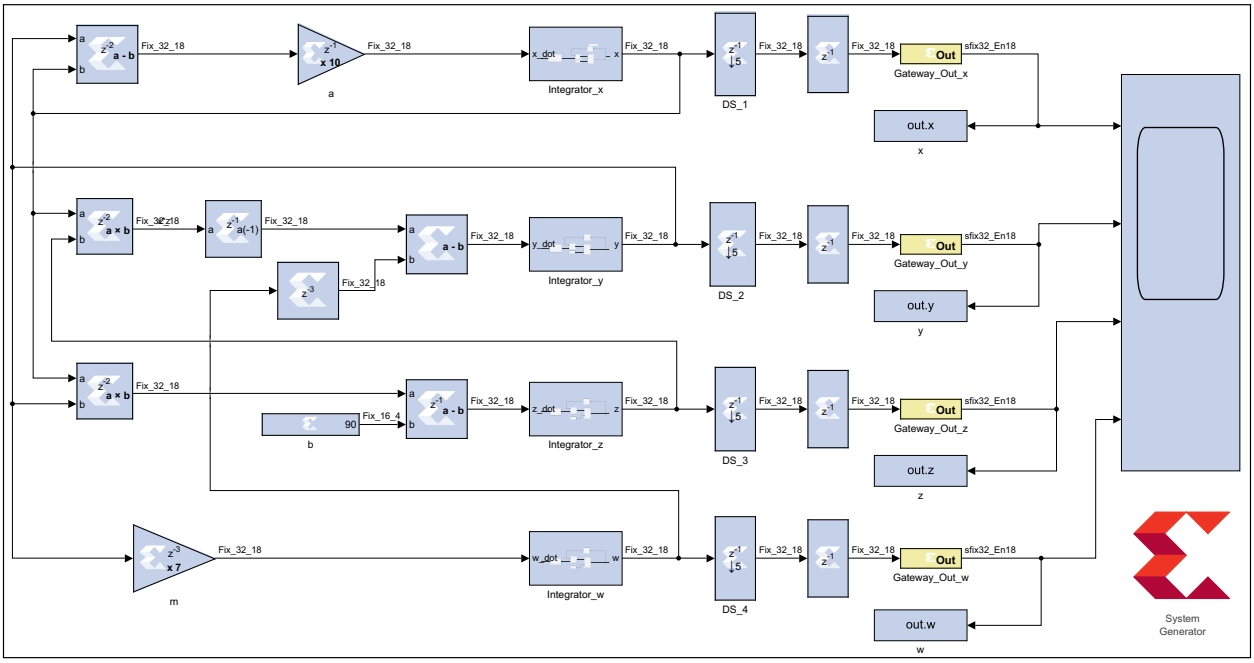


Fig. 5. Optimized FIX-32-18 FPGA realization of the hyperchaotic Lorenz system (1).

for the forward Euler technique. The dynamical system given by n ODEs with n- state variables in equation (8), can be expressed using the forward Euler technique for FPGA implementation as time course solution that given by the system of equations (9) stated as follows:

$$\begin{aligned} \frac{dx_1}{dt} &= f_1(x_1,\ldots,x_n) \\ \frac{dx_n}{dt} &= f_n(x_1,\ldots,x_n) \end{aligned} \tag{8}$$

by applying the forward method of Euler:

$$\begin{aligned} x_1(t+dt) &= x_1 + f_1(x_1(t),\ldots,x_n(t))\,dt \\ &\vdots \\ x_n(t+dt) &= x_n + f_n(x_1(t),\ldots,x_n(t))\,dt \end{aligned} \tag{9}$$

It is mentioned in previous studies that chaotic oscillator may exhibit abnormalities if their step size (dt) is big [34]. ODEs can also be solved numerically using other methods, such as the fourth order Runge-Kutta technique (RK-4) [35].

32-Bits Fixed-point FPGA Implementation

Fixed-point representation is a method of representing numbers with a specific number of fractional and integer bits in digital systems like Field-Programmable Gate Arrays (FPGAs). Unlike floating-point representation, which uses separate bits to represent the mantissa and exponent, fixed-point representation allocates a fixed number of bits to represent both the integer and fractional parts of a number. This is particularly useful in FPGA designs where hardware resources are limited, and fixed-point arithmetic can be implemented more efficiently than floating-point arithmetic. A prevalent signed fixed-point encoding notation is $Qm.n$ provides m integer bits, n fractional bits, and 1 sign bit. Its accuracy is 2^{-n}, and its corresponding limit is between -2^m and $2^m - 2^{-n}$. In system generator model, a 32-bit fixed-point data format with 13 integer bits, 18 fractional bits, and 1 bit to represent the sign of the signal. The format has been used to realize Lorenz hyperchaotic system (1) in this work. The system generator model has been optimized to meet the constraints by including delay blocks to cut critical paths and meet the timing closure. Critical long time pathways can be divided into small pieces to satisfy the timing constraints by introducing delay blocks [36]. Fig. 5, shows the optimized design of the presented Lorenz hyperchaotic system (1).

IV. Chaotic Systems Synchronization

Despite being aperiodic and appearing randomly in the time domain, chaotic systems may be synchronized and employed for data encryption in secure communication systems to send text, picture, video, and audio files [37]. The highly unpredictable and random-look nature of chaotic signals is the most attractive feature of deterministic chaotic systems that may used for data encryption schemes [38].

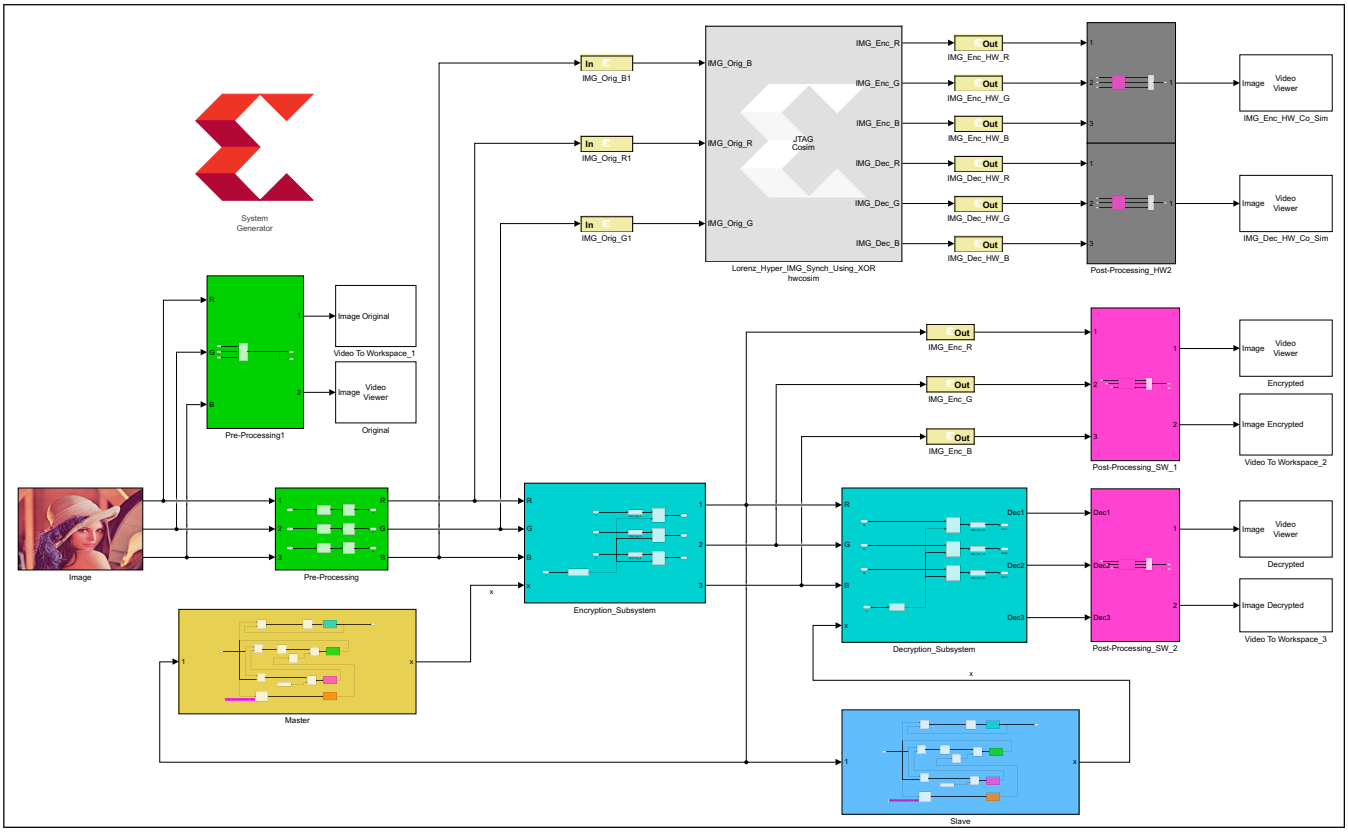


Fig. 6. The proposed FPGA image encryption/ decryption system with the Lorenz hyperchaotic master-slave synchronization model.

Up to Pecora and Carroll's demonstration that it is feasible for two or more dynamically chaotic and/or hyperchaotic entities to synchronize, the chaos or hyperchaos synchronization remained irrelevant [39]. Additive masking, chaotic switching, chaotic parameter modulation, chaotic shift keying, and chaotic frequency modulation are among some of the common approaches for chaos-based secure transfer of confidential information signals [40].

In this work the the XOR-masking method has been implemented to facilitate synchronization between the master and slave chaotic systems, leveraging its numerous advantages. This approach offers robustness against external disturbances and noise, which are common challenges in chaotic systems, and able to enhance the stability of synchronization, ensuring reliable and consistent communication between the systems even in the presence of perturbations. These features are particularly valuable in practical applications where, the computational efficiency of this method makes it suitable for real-time synchronization tasks, enabling rapid response and seamless integration into dynamic environments. The synchronization scheme is shown in Fig. 6.

V. Experimental Results

The objective was to assess the performance and effectiveness of the proposed hyperchaotic-based cryptosystem through encryption and decryption processes applied to this image. The cryptosystem utilizes hyperchaotic dynamics, which are characterized by complex, unpredictable behavior ideal for cryptographic applications.

During the encryption phase, the plain image undergoes a series of transformations based on hyperchaotic dynamics. These transformations typically involve nonlinear operations. This process scrambles the image content in a highly chaotic manner, making it unintelligible to unauthorized parties without the appropriate decryption key.

Subsequently, the encrypted image is subjected to the decryption process using the same hyperchaotic-based cryptosystem. The decryption algorithm reverses the operations applied during encryption, effectively recovering the original plain image from the encrypted data. This process demonstrates the ability of the cryptosystem to securely restore the original content from the encrypted form, provided the correct decryption key is utilized.

The experimentation with the "Lena" colour plain image serves to validate the efficiency and the feasibility of the proposed cryptosystem in real-world scenarios. By employing a widely recognized test image, researchers can assess various aspects of the cryptosystem's performance, including encryption speed, decryption accuracy, resistance to attacks, and preservation of image quality. The results obtained from this experimental testing provide valuable insights into the practical applicability and robustness of the hyperchaotic-based cryptosystem for securing digital images and other sensitive data.

A. Cryptanalysis

This section assesses the recommended hyperchaotic-based image cryptosystem's performance efficiency using a variety of security test techniques. As is often known, a good cryptosystem should have a large amount of keyspace to foil explorer efforts, strong resilience to various attacks, and high sensitivity to the key or keys [41]. In this work, the following popular measures were investigated: key sensitivity, histogram, information entropy, correlation coefficients of neighboring pixels, and other typical statistics used as indicators of the effectiveness of the proposed image cryptosystem design.

1) Histogram Check

The histograms common metric are often used to measure and visualize the values of pixels (pixel brightness levels) distributed in a photograph. The original color image may be regarded as a 24-bit image since it has three bands (R, B, and B), each of which is an 8-bit image. Therefore, for each of these three bands, which range from 0 to 255, there are 256 (2^8) potential brightnesses. Consequently, 256 values indicating the distribution of the picture pixels and their levels of intensity will be shown by the histogram [42].

The encrypted image's histogram count should be statistically distinct from the plain image's histogram. This is necessary to prevent statistical attacks, which rely on identifying patterns in the pixel intensity levels. A uniform histogram in the encrypted image makes it difficult for attackers to infer any meaningful information from the pixel distribution. Moreover, the encrypted image's histogram should also be aesthetically different from the plain image's histogram. This means that the visual representation of the pixel intensity levels should be distinct and unintelligible, making it difficult for an attacker to visually identify any patterns or features of the original image. The histograms of the red (R), green (G), and blue (B) bands of the encrypted image should be somewhat uniform in form. This uniformity is important because it indicates that the pixel values are unpredictable and do not follow any discernible pattern. A uniform distribution in the histograms of the R, G, and B bands makes it difficult for attackers to exploit any correlations between the color channels.

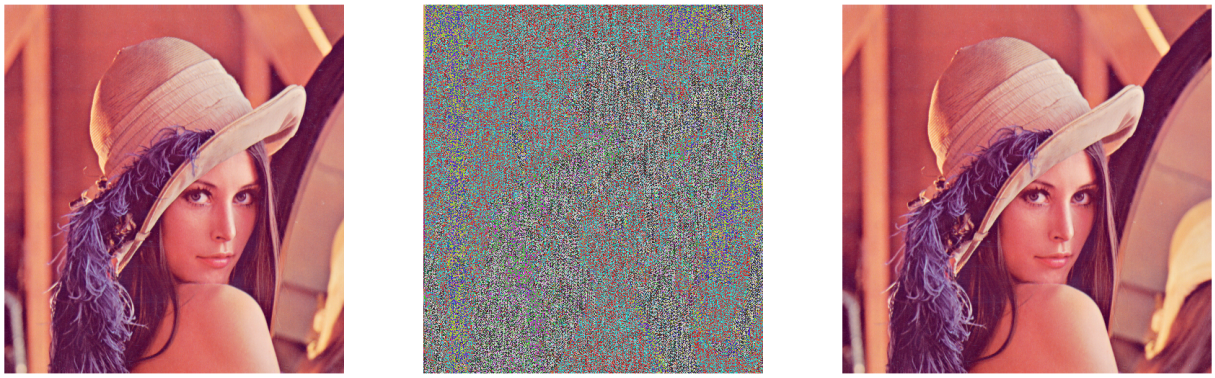
Fig. 7a, and Fig. 7d show the plain colored Lena image and its histograms spectrum, respectively. The histograms of the encrypted images of the respective original Lena, R, G, and B depicted in Fig. 7b, is provided in Fig. 7e. The recovered image Fig. 7c is consistent with the plain image displayed in Fig. 7a, in their appropriate arrangements respectively. It is clear from Figs. 7d and 7e that the pattern of distribution of the encrypted image histograms distinct considerably from that of the initial image, while the pixel intensities of the encrypted image have a flat distribution (uniform). These findings show that the proposed cryptosystem algorithm provides exceptional resilience against statistical attacks. Stated otherwise, the histograms of the encrypted picture have equal distribution. Consequently, the encrypted pictures provide no details about the original pictures. Moreover, Fig. 7f that shows the histogram distribution of the recovered picture, which is precisely the same as Fig. 7d that shows the histogram of the plain image. Consequently, it is possible to successfully and precisely extract and recover the original image.

2) Keyspace Analysis

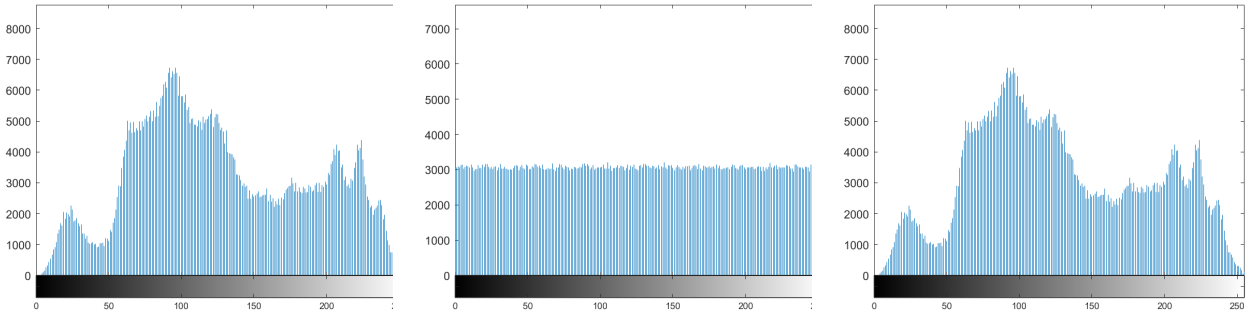
In the situation of a pirate force attack happens, one important aspect of the security in any system of cryptography is the keyspace [43]. In our study, the hyperchaotic Lorenz system, denoted by equation (1), generates the secret keys components. Thus, the parameters (a, b, and m), as well as the system (1) initial condition values $(x(0), y(0), z(0), w(0))$, are included in the secret keys list. Hyperchaotic systems are very sensitive to even little changes in the initial conditions and model characteristics, as was mentioned in the introductory section. If every utilized key undergoes 10^{-15} step modification, the total keyspace may be calculated as follows: $(10^{16})^7 = 10^{112} = 2^{372}$. These results show that the employed encryption method's keyspace is sufficiently big to fend off all types of brute force attempt.

3) Key Sensitivity Analysis

Strong key sensitivity is necessary in any cryptography system to validate strong and secure encryption techniques. This implies that effective recovery of the ciphered picture is impossible, even with minor modifications to the encryption and decryption keys. This ensures that the cryptosystem technique is secure from brute force threats [44]. The unified average changing intensity (UACI) and net pixel change rate (NPCR) are often computed to assess the key sensitivity aspects. These measures evaluate the effect of slight variations in the secret keys on the original image retrieval. Greater resistance against different types of pirate assaults is shown by higher NPCR and UACI scores for the encryption technique [45]. The percentage of variation in the degree of pixel



(a) Plain Lena (b) Encrypted Lena (c) Decrypted Lena



(d) Plain Lena histogram (e) Encrypted Lena histogram (f) Decrypted Lena histogram

Fig. 7. The results of the histogram distribution.

number modification between two images is computed by the NPCR. However, the average brightness of the discrepancies between the two pictures is determined by UACI. The NPCR and UACI may be evaluated using the next given formulas (10) and (11), respectively [46]:

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}|\,\mathrm{sign}(I(i,j)-D(i,j))|}{M\cdot N}\times 100\% \quad (10)$$

$$UACI = \frac{1}{255}\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}|I(i,j)-D(i,j)|}{M\cdot N}\times 100\% \quad (11)$$

where equation (10) provides the following: $M\times N$ gives the image size; $I(i,j)$ provides the plain image; $D(i,j)$ represents the recovered image; (i,j) confers the pixel image location; and if $I(i,j)\neq \mathrm{D}(i,j)$, then $|\,\mathrm{sign}(\cdot)|=1$; and if not, then $|sign(\cdot)|=0$. Table I illustrates the results of key sensitivity comparative assessments of NPCR and UACI.

4) Correlation Coefficients Analysis

The correlation coefficients are employed to quantify the degree of data unpredictability in the encrypted pictures. They are computed by comparing the values of two neighboring pixels. The plain image has a substantial amount of connectivity between two head-to-head pixels. This value, however, ought to be as low as practical for the encrypted image, that is, the least amount of correlation that may exist between two adjacent pixels. Reducing the correlation between an encrypted image's adjacent pixels is a necessary feature of a high-security image encryption system [47].

Correlation coefficient values are typically calculated for a certain number of neighboring pixels in the diagonal (D), vertical (V), and horizontal (H) arrangements. According to [48], the correlation coefficients of two head-to-head pixel x, y values

TABLE I. NPCR AND UACI OF THE PLAIN AND ENCRYPTED IMAGES.

Test	Lena	R Band	G Band	B Band
NPCR	99.563980	99.563980	99.563980	99.563980
UACI	30.4252	32.9877	30.6866	27.6013

TABLE II. CORRELATION RESULTS OF THE PLAIN AND ENCRYPTED IMAGES, RESPECTIVELY.

Direction	Plain Image				Encrypted Image			
	Lena	R Band	G Band	B Band	Lena	R Band	G Band	B Band
Vertical	0.9855	0.9900	0.9846	0.9540	-0.0108	-0.0180	-0.0241	-0.0275
Horizontal	0.9786	0.9833	0.9728	0.9314	-0.0109	-0.0135	-0.0132	-0.0179
Diagonal	0.9632	0.9698	0.9562	0.9098	0.0261	-0.0807	0.0034	-0.0124

in an image are calculated:

$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{12}$$

In (12), x and y signify the two neighbouring pixel values, $cov(x,y)$ presents the covariance function, and $D(.)$ denotes the variance. The values $cov(x,y)$ and $D(.)$ can be computed as in equations (13) and (14), respectively [49]:

$$\operatorname{cov}(x,y) = \frac{\sum_{i=1}^{N}(x_i - E(x))(x_i - E(y))}{N} \tag{13}$$

$$D(k) = \frac{\sum_{i=1}^{N}(k_i - E(k))^2}{N} \tag{14}$$

where the average is $E(k)$, which may be computed using (15), and the total number of chosen pixels in the image is represented by N in (10) as in the following:

$$E(k) = \frac{\sum_{i=1}^{N} k_i}{N} \tag{15}$$

In our study, we selected pairs of neighboring pixels in vertical, horizontal, and diagonal layouts from the original and its encrypted pictures for the correlation confection computation. The obtained correlation confections of neighboring pixels for the original image and its consistent encrypted image are displayed in Table II.

As can be observed in Table II, the encrypted image exhibit a very small correlation compared to the initial image pixels' highly strong correlation. This indicates that the cryptosystem technique being used is quite resilient against brute force attempt.

Additionally, the correlation coefficient plots of the unencrypted Lena picture and its consistent encrypted image are shown in horizontal, vertical, and diagonal orders in figures within Table III. It can be seen from these figures that the plain image show a very weighty correlation of the related pixels. In other words, all of the pixel points in the plain image and are concentrated along with the diagonal alliance. On the other hand, conversely, the corresponding encrypted picture pixel dots are dispersed over the plane. This confirms that there are much less correlations between different pixels in the encrypted image. An ideal quality of an encryption technique is the capacity to transform closely related pixels of a plain picture into unrelated pixels of an encrypted image. Because of this increased unpredictability, it is harder for attackers to do statistical analysis on the encrypted picture. This illustrates the high level of security efficacy provided by the proposed system of cryptography, which is based on a Lorenz hyperchaotic system.

5) Entropy Evolution

The pattern of distribution of an image's pixel values from 0 and 255 is determined by its entropy [50]. It establishes how ambiguous and unpredictable the image is. Since 8 bits specify each of the 256 intensity levels of a pixel picture, the ideal hypothetical amount of information entropy in the encrypted image is 8. In practical terms, the information entropy value of the encrypted image need to be as near to 8 as achievable.

The image entropy measure is expressed as given in the following formula (16), adopted from [51]:

$$H(s) = \sum_{i=1}^{255} p(s_i) \log_2 \left(\frac{1}{p(s_i)} \right) \tag{16}$$

where, $p(.)$ denotes the probability of the pixel value in (16). The calculated entropy values of the plain color (Lena picture) and its R, G, and B bands, together with their corresponding encrypted images, are shown in Table IV.

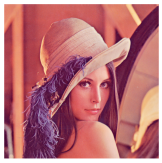
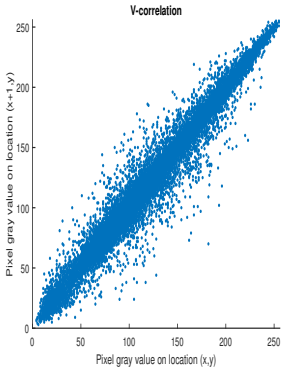
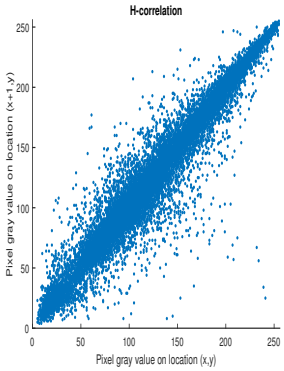
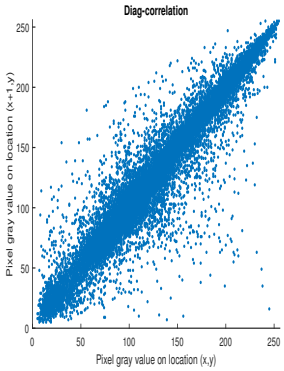
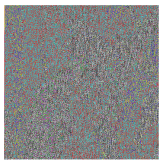
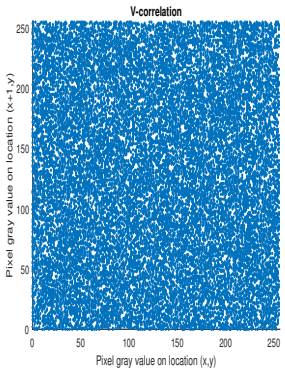
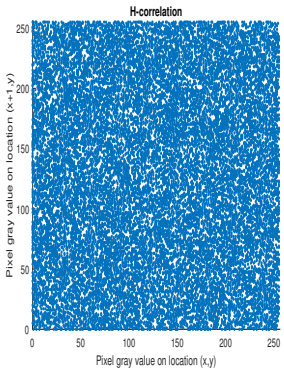
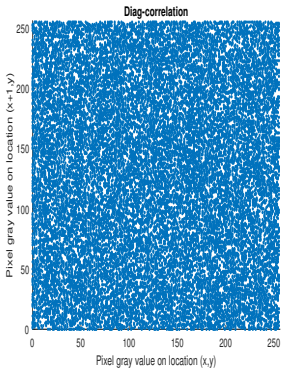
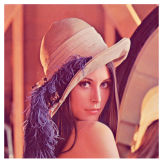
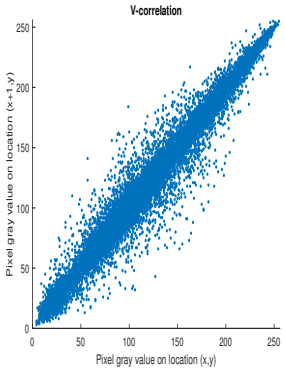
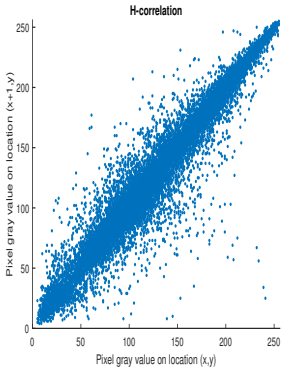
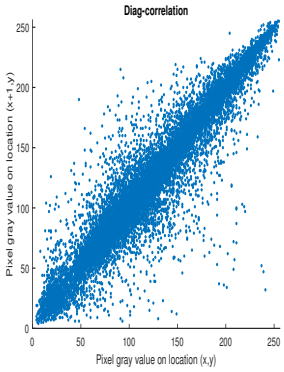
Image	Vertical	Horizontal	Diagonal
			
			
			

TABLE III. CORRELATION PLOTS OF THE PLAIN, ENCRYPTED AND DECRYPTED IMAGES, RESPECTIVELY.

B. Hardware Co-Simulation Of Image Encryption And Decryption System

The proposed model is formulated using the FPGA Zedboard Zynq xc7z020-1clg484. The image encryption and, decryption process are co-simulated with FPGA hardware as in Fig. 8. When JTAG port is connected, serial image signal data are transmitted via a USB JTAG port to FPGA. Then serial samples were returned to PC using the Simulink / Matlab Viewer to test the image.

The right insets images in the top and bottom of Fig. 8, represent the results of the encrypted and decrypted images in the FPGA hardware co-simulation, respective. The encrypted

TABLE IV. ENTROPY INFORMATION OF THE PLAIN AND ENCRYPTED IMAGES.

	Original Image	Encrypted Image
Lena	7.271855	7.999292
R Band	7.253102	7.999200
G Band	7.594037	7.999303
B Band	6.968426	7.999375

image has proved to be the same for system generators and, co-simulation. The summary of system resource utilization, power consumption and timing of the proposed Lorenz hyperchaotic cryptographic system are shown in Fig. 9. These reports are provided using the Xilinx Vivado HLx Edition 2020.2 software. The power report of the FPGA within Fig. 9 demonstrates that the power consumption is within the expected range and meets the design specifications. This indicates that the FPGA is operating efficiently and its power usage is appropriate for the proposed application, and that the digital encryption/decryption system are meeting the design constraints.

VI. CONCLUSIONS

On a final note, the proposed hyperchaotic Lorenz based encryption and decryption algorithm is demonstrated to be an effective system for encrypting and decrypting of colour images. Additionally, it has been demonstrated that the suggested scheme satisfies every security analysis tests, producing a system with strong security efficacy and resilience to cryptanalysis assaults. FPGAs provide a flexible and high-performance platform for accelerating cryptographic operations, including image encryption. The FPGA resource utilization, power consumption and timing reports have been measured. Finally, the real-time evaluation of the system proposed was co-simulated using the ZedBoard Zynq-7000 FPGA SoC xc7z020-1clg484 development kit. Future work may be directed for leveraging AI in image encryption and decryption on FPGAs to combine the reconfigurable hardware's efficiency with the intelligent processing capabilities of AI. This approach allows for real-time processing, benefiting applications requiring high security and quick response times. Additionally, the adaptability of FPGAs enables continuous optimization and scaling of AI models, ensuring robust and secure image encryption and decryption solutions.

AUTHOR CONTRIBUTIONS

The authors contributed equally to this work. All authors have read and agreed to the published version of the manuscript.

CONFLICT OF INTEREST

The authors have declared no conflict of interest.

REFERENCES

[1] V. Das and N. Thankachan, *Computational Intelligence and Information Technology: First International Conference, CIIT 2011, Pune, India, November 7-8, 2011. Proceedings*, vol. 250. Springer Science & Business Media, 2013.

[2] L. Merah, A. Ali-Pacha, N. Hadj-Said, B. Mecheri, and M. Dellassi, "Fpga hardware co-simulation of new chaos-based stream cipher based on lozi map," *International Journal of Eng. And Technology*, vol. 9, no. 5, pp. 420–425, 2017.

[3] L. De Micco and H. A. Larrondo, "Fpga implementation of a chaotic oscillator using rk4 method," in *2011 VII Southern Conference on Programmable Logic (SPL)*, pp. 185–190, IEEE, 2011.

[4] S. Wang, J. Kuang, J. Li, Y. Luo, H. Lu, and G. Hu, "Chaos-based secure communications in a large community," *Physical Review E*, vol. 66, no. 6, p. 065202, 2002.

[5] G. A. Beyene, F. Rahma, K. Rajagopal, A.-B. A. Al-Hussein, and S. Boulaaras, "Dynamical analysis of a 3d fractional-order chaotic system for high-security communication and its electronic circuit implementation," *Journal of Nonlinear Mathematical Physics*, vol. 30, no. 4, pp. 1375–1391, 2023.

[6] G. A. Al-Suhail, F. R. Tahir, M. H. Abd, V.-T. Pham, and L. Fortuna, "Modelling of long-wave chaotic radar system for anti-stealth applications," *Communications in Nonlinear Science and Numerical Simulation*, vol. 57, pp. 80–96, 2018.

[7] N. Debbouche, A. Ouannas, G. Grassi, A.-B. A. Al-Hussein, F. R. Tahir, K. M. Saad, H. Jahanshahi, A. A. Aly, *et al.*, "Chaos in cancer tumor growth model with commensurate and incommensurate fractional-order derivatives," *Computational and Mathematical Methods in Medicine*, vol. 2022, 2022.

[8] A.-B. A. Al-Hussein, F. Rahma, L. Fortuna, M. Bucolo, M. Frasca, and A. Buscarino, "A new time-delay model for chaotic glucose-insulin regulatory system," *International Journal of Bifurcation and Chaos*, vol. 30, no. 12, p. 2050178, 2020.

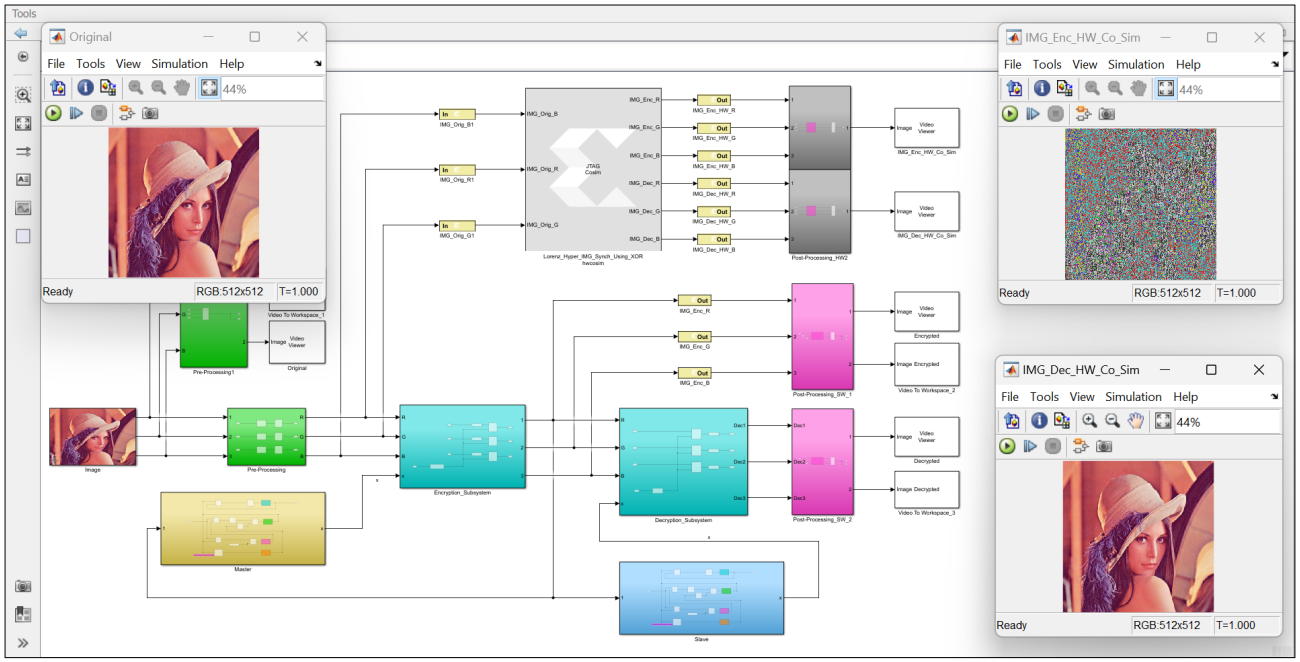


Fig. 8. FPGA hardware co-simulation of the proposed cryptography system using ZedBoard Zynq-7000 FPGA SoC xc7z020-1clg484 development board.

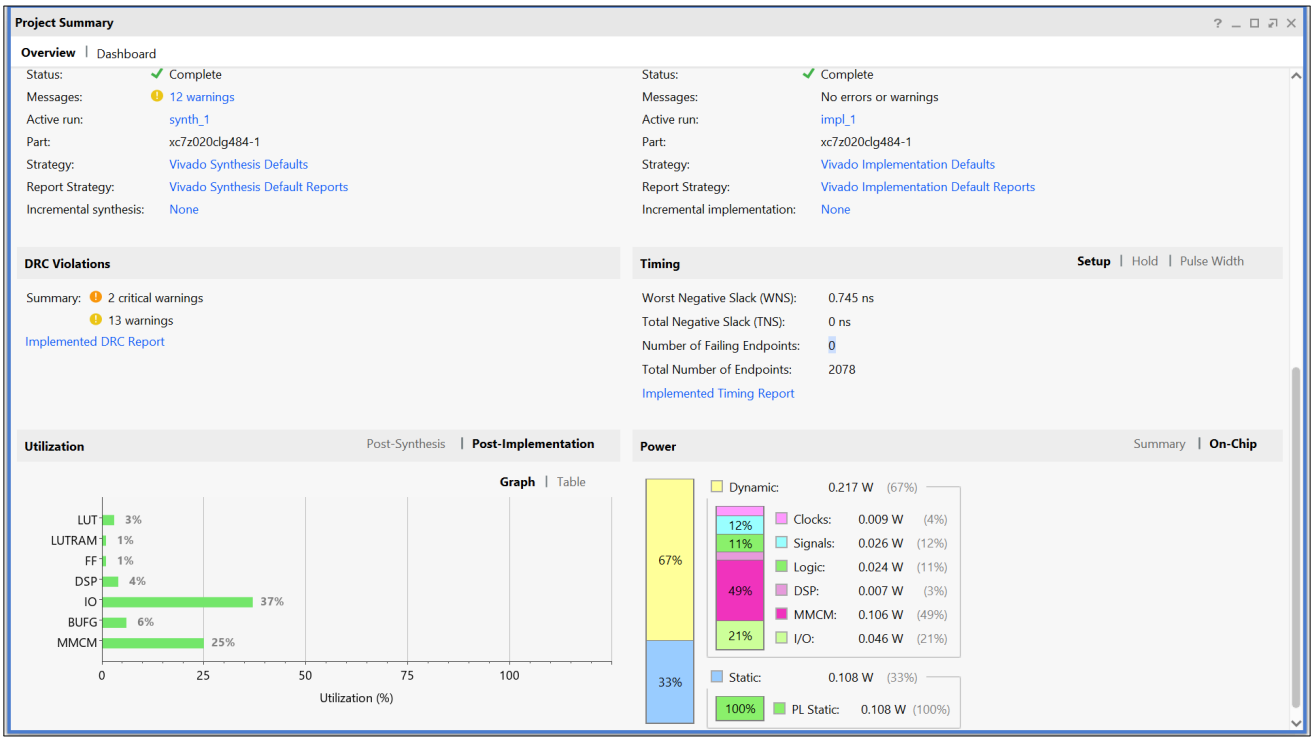


Fig. 9. FPGA ZedBoard Zynq xc7z020-1clg484 kit resource utilization, power consumption and timing constraints reported from Xilinx Vivado HLx 2020.2 software.

[9] A.-B. A. Al-Hussein and F. R. Tahir, "A new model for endocrine glucose-insulin regulatory system," *Iraqi J. Electr. Electron. Eng*, vol. 16, no. 1, 2020.

[10] Y. Nakamura and A. Sekiguchi, "The chaotic mobile robot," *IEEE Transactions on Robotics and Automation*, vol. 17, no. 6, pp. 898–904, 2001.

[11] A.-B. A. Al-Hussein, F. R. Tahir, and O. Boubaker, "Chaos elimination in power system using synergetic control theory," in *2021 18th International Multi-Conference on Systems, Signals & Devices (SSD)*, pp. 340–345, IEEE, 2021.

[12] A.-B. A. Al-Hussein and F. R. Tahir, "Quenching chaos in a power system using fixed-time fractional-order sliding mode controller," *Journal of Energy Systems*, vol. 7, no. 3, pp. 243–256, 2023.

[13] A.-B. A. Al-Hussein, "Chaos phenomenon in power systems: A review.," *Iraqi Journal for Electrical & Electronic Engineering*, vol. 17, no. 2, 2021.

[14] H. M. M. Alibraheemi, Q. Al-Gayem, and E. A. Hussein, "Design and fpga implementation of high-speed cryptographic system for wireless communications based on multi-dimensional hyperchaotic generator," *NeuroQuantology*, vol. 20, no. 7, p. 559, 2022.

[15] X.-Y. Wang and S.-X. Gu, "New chaotic encryption algorithm based on chaotic sequence and plain text," *IET Information Security*, vol. 8, no. 3, pp. 213–216, 2014.

[16] S. M. Seyedzadeh and S. Mirzakuchaki, "A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map," *Signal processing*, vol. 92, no. 5, pp. 1202–1215, 2012.

[17] E. A. Umoh, "Generalized synchronization of topologically-nonequivalent chaotic signals via active control," *Int. J. Signal Process. Syst*, vol. 2, no. 2, pp. 139–143, 2014.

[18] M. Sargolzaei, M. Yaghoobi, and R. A. G. Yazdi, "Modelling and synchronization of chaotic gyroscope using ts fuzzy approach," *Advances in Electronic and Electric Engineering*, vol. 3, no. 3, pp. 339–346, 2013.

[19] E. A. Umoh, "Synchronization of chaotic flows with variable nonlinear hyperbolic functions via hybrid feedback control," in *Proceedings of the 2nd Pan African International Conference on Science, Computing and Telecommunications (PACT 2014)*, pp. 7–11, IEEE, 2014.

[20] E. A. Umoh, "Chaos antisynchronization of the complex deng's toroidal system via hybrid feedback control," *Journal of Computational Intelligence and Electronic Systems*, vol. 3, no. 2, pp. 138–142, 2014.

[21] Y. Bian and W. Yu, "A secure communication method based on 6-d hyperchaos and circuit implementation," *Telecommunication Systems*, vol. 77, no. 4, pp. 731–751, 2021.

[22] J. Wang, W. Yu, J. Wang, Y. Zhao, J. Zhang, and D. Jiang, "A new six-dimensional hyperchaotic system and its secure communication circuit implementation," *International Journal of Circuit Theory and Applications*, vol. 47, no. 5, pp. 702–717, 2019.

[23] Z. Peng, W. Yu, J. Wang, Z. Zhou, J. Chen, and G. Zhong, "Secure communication based on microcontroller unit with a novel five-dimensional hyperchaotic system," *Arabian Journal for Science and Engineering*, vol. 47, no. 1, pp. 813–828, 2022.

[24] C. Xiu, J. Fang, and Y. Liu, "Design and circuit implementation of a novel 5d memristive cnn hyperchaotic system," *Chaos, Solitons & Fractals*, vol. 158, p. 112040, 2022.

[25] H. M. M. Alibraheemi, Q. Al-Gayem, and E. A. Hussein, "Four dimensional hyperchaotic communication system based on dynamic feedback synchronization technique for image encryption systems," *International Journal of Electrical and Computer Engineering*, vol. 12, no. 1, p. 957, 2022.

[26] T. Matsumoto, "Chaos in electronic circuits," *Proceedings of the IEEE*, vol. 75, no. 8, pp. 1033–1057, 1987.

[27] M. A. Aseeri, M. I. Sobhy, and P. Lee, "Lorenz chaotic model using filed programmable gate array (fpga)," in *The 2002 45th Midwest Symposium on Circuits and Systems, 2002. MWSCAS-2002.*, vol. 1, pp. I–527, IEEE, 2002.

[28] A. G. Soriano-Sánchez, C. Posadas-Castillo, M. A. Platas-Garza, and A. Arellano-Delgado, "Synchronization and fpga realization of complex networks with fractional–order liu chaotic oscillators," *Applied Mathematics and Computation*, vol. 332, pp. 250–262, 2018.

[29] Z.-Z. GAO and C. ZHANG, "A novel hyperchaotic system," *Journal of Jishou University (Natural Sciences Edition)*, vol. 32, no. 5, p. 65, 2011.

[30] C. Pradhan, S. K. Jena, S. R. Nadar, and N. Pradhan, "Higher-order spectrum in understanding nonlinearity in

eeg rhythms," *Computational and mathematical methods in medicine*, vol. 2012, 2012.

[31] C. Pezeshki, S. Elgar, and R. Krishna, "Bispectral analysis of possessing chaotic motion," *Journal of sound and vibration*, vol. 137, no. 3, pp. 357–368, 1990.

[32] S. Çiçek, A. Ferikoğlu, and İ. Pehlivan, "A new 3d chaotic system: dynamical analysis, electronic circuit design, active control synchronization and chaotic masking communication application," *Optik*, vol. 127, no. 8, pp. 4024–4030, 2016.

[33] J. Cuautle and L. Fraga, "Engineering applicaitons of fpgas-chaotic systems, artificial neural networks, random number generators, and secure communication systems," *Switzerland: Springer*, 2016.

[34] B. Muthuswamy and S. Banerjee, *A route to chaos using FPGAs*, vol. 16. Springer, 2015.

[35] M. Azzaz, C. Tanougast, S. Sadoudi, and A. Dandache, "Real-time fpga implementation of lorenz's chaotic generator for ciphering telecommunications," in *2009 Joint IEEE North-East Workshop on Circuits and Systems and TAISA Conference*, pp. 1–4, IEEE, 2009.

[36] L. Zhang, "System generator model-based fpga design optimization and hardware co-simulation for lorenz chaotic generator," in *2017 2nd Asia-Pacific Conference on Intelligent Robot Systems (ACIRS)*, pp. 170–174, IEEE, 2017.

[37] A. Abel and W. Schwarz, "Chaos communications-principles, schemes, and system analysis," *Proceedings of the IEEE*, vol. 90, no. 5, pp. 691–710, 2002.

[38] L. Gámez-Guzmán, C. Cruz-Hernández, R. López-Gutiérrez, and E. Garcia-Guerrero, "Synchronization of multi-scroll chaos generators: application to private communication," *Revista mexicana de física*, vol. 54, no. 4, pp. 299–305, 2008.

[39] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Physical review letters*, vol. 64, no. 8, p. 821, 1990.

[40] L. Merah, A. Ali-Pacha, N. H. Said, and M. Mamat, "A pseudo random number generator based on the chaotic system of chua's circuit, and its real time fpga implementation," *Applied Mathematical Sciences*, vol. 7, no. 55, pp. 2719–2734, 2013.

[41] A. Akhavan, A. Samsudin, and A. Akhshani, "Cryptanalysis of an image encryption algorithm based on dna encoding," *Optics & Laser Technology*, vol. 95, pp. 94–99, 2017.

[42] K. H. Moussa, A. I. El Naggary, and H. G. Mohamed, "Non-linear hopped chaos parameters-based image encryption algorithm using histogram equalization," *Entropy*, vol. 23, no. 5, p. 535, 2021.

[43] Y. Xiang, D. Xiao, R. Zhang, J. Liang, and R. Liu, "Cryptanalysis and improvement of a reversible data-hiding scheme in encrypted images by redundant space transfer," *Information Sciences*, vol. 545, pp. 188–206, 2021.

[44] M. K. Mandal, M. Kar, S. K. Singh, and V. K. Barnwal, "Symmetric key image encryption using chaotic rossler system," *Security and Communication Networks*, vol. 7, no. 11, pp. 2145–2152, 2014.

[45] D. H. ElKamchouchi, H. G. Mohamed, and K. H. Moussa, "A bijective image encryption system based on hybrid chaotic map diffusion and dna confusion," *Entropy*, vol. 22, no. 2, p. 180, 2020.

[46] B. Yousif, F. Khalifa, A. Makram, and A. Takieldeen, "A novel image encryption/decryption scheme based on integrating multiple chaotic maps," *AIP Advances*, vol. 10, no. 7, 2020.

[47] G. Situ and J. Zhang, "Position multiplexing for multiple-image encryption," *Journal of Optics A: Pure and Applied Optics*, vol. 8, no. 5, p. 391, 2006.

[48] A. Pourjabbar Kari, A. Habibizad Navin, A. M. Bidgoli, and M. Mirnia, "A new image encryption scheme based on hybrid chaotic maps," *Multimedia Tools and Applications*, vol. 80, pp. 2753–2772, 2021.

[49] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal processing*, vol. 92, no. 4, pp. 1101–1108, 2012.

[50] G. Ye, C. Pan, X. Huang, Z. Zhao, and J. He, "A chaotic image encryption algorithm based on information entropy," *International Journal of Bifurcation and Chaos*, vol. 28, no. 01, p. 1850010, 2018.

[51] X. Peng and Y. Zeng, "Image encryption application in a system for compounding self-excited and hidden attractors," *Chaos, Solitons & Fractals*, vol. 139, p. 110044, 2020.