MPSoC Implementation of Secure Systems Based on Synchronized 3D Chaotic Spherical Attractors.

Roberto Herrera Charles [a], Vincent Ademola Adeyemi [b], José Cruz Núñez-Pérez [c], Opeyemi Micheal Afolabi [d].

Centro de Investigación y Desarrollo de Tecnología Digital Instituto Politécnico Nacional, 22435, Tijuana, B.C, Mexico.
[a]robccharles@citedi.mx. [b]vademola@citedi.mx. [c]nunez@citedi.mx.
[d]oafolabi@citedi.mx.

Resumen

El desarrollo masivo del internet de las cosas (IoT), Big Data y otras tecnologías ha generado preocupaciones de seguridad con respecto a la protección de datos. Se ha vuelto imperativo desarrollar soluciones para proteger nuestros datos, como imágenes, textos y audios, del acceso no autorizado. Este trabajo presenta un esquema de transmisión de imágenes cifradas basado en una configuración dinámica caótica de dos atractores caóticos esféricos sincronizados de 3 dimensiones en una topología maestro-esclavo. Sincronizamos la evolución futura de los sistemas caóticos comenzando con diferentes condiciones iniciales utilizando el enfoque basado en observadores hamiltonianos y luego utilizamos los puntos del espacio de fase resultantes como números pseudoaleatorios para asegurar la imagen transmitida a través del canal de comunicación. El esquema diseñado se realiza e implementa en la plataforma Multiprocessor System-on-Chip (MPSoC) aprovechando las funciones de programación fáciles y sintetizables de Python con MPSoC. La imagen se transmite a través de las variables de estado x_1, x_2 y x_3 y se analiza utilizando dos técnicas estadísticas, a saber, entropía de información y análisis de correlación, donde el resultado muestra la recuperación completa de la imagen que se transmitió a través de las variables de estado.

Palabras clave— *Caos, FPGA, MPSoC, Comunicación Segura, Python.*

Abstract

The massive development of internet of things (IoT), Big Data and other technologies has led to security concerns with respect to data protection. It has become imperative to develop solutions to protect our data, such as images, texts, and audios from unauthorized access. This work presents an encrypted image transmission scheme based on a chaotic dynamic configuration of two synchronized spherical chaotic attractors of 3 dimension in a master-slave topology. We synchronized the future evolution of the chaotic systems starting with different initial conditions using the Hamiltonian observer-based approach and then utilized the resulting phase space points as the pseudo-random numbers for securing image transmitted through the communication channel. The scheme designed is realized and implemented on the Multiprocessor System-on-Chip (MPSoC) platform by harnessing the easy and synthesizable programming features of Python with MPSoC. The image is transmitted through the state variables x_1, x_2, and x_3, and analyzed using the two statistical techniques namely, information entropy and correlation analysis where the result shows the full recovery of the image that was transmitted through the state variables.

Keywords— *Chaos, FPGA, MPSoC, Secure Communication, Python.*

1. INTRODUCTION

Since the creation of the Lorenz chaotic system, researchers in chaos theory have worked extensively to develop various chaotic systems for generating and applying chaos. Nowadays, chaos has become a multidisciplinary research area, which has been widely applied in communications, robotics, security, medicine, so on.

In today's digital landscape, the secure transmission of sensitive information, particularly within real-time image processing systems, is imperative. Image data often harbors private and confidential information, underscoring the necessity to safeguard it from unauthorized access and interception. With the escalating volume of image data shared across networks, communication channels, social media, big data, and the Internet of Things (IoT), implementing algorithms that ensure confidentiality and privacy has become a critical challenge. Traditional image transmission methods are vulnerable to interception and unauthorized access, exposing the data to potential breaches and compromising sensitive information.

Chaos-based communication hinges on the synchronization of chaotic oscillators, acting as the backbone of the system [1]. Achieving synchronization between the chaotic transmitter and receiver is pivotal for information transmission. Various synchronization schemes, such as Pecora and Carroll, Ott-Grebogi-Yorke (OGY), Hamiltonian forms, observer approach, open-plus-close-loop, and others, contribute to this endeavor. [2] The synchronization of two chaotic attractor systems in a master-slave topology represents a significant contribution made by this paper [3].

2. 3D SPHERICAL CHAOTIC ATTRACTOR

In the investigation done by the authors in [4], a smooth quadratic autonomous chaotic system was proposed from an earlier system constructed in [5] based on the Shilnikov criterion. The Shilnikov criterion is an analytic method for proving chaos in nonlinear dynamical systems [6, 7]. It consists of two theorems, which give a theoretical foundation for classification of chaos. One theorem is based on the presence of heteroclinic orbit while the other is based on the existence of homoclinic orbit.

Consider a third-order autonomous system of the form:

$$\frac{dx}{dt} = f(x), \quad x \in \boldsymbol{R}^3, \quad t \in \boldsymbol{R} \tag{1}$$

where the vector field $f(x)$: $R^3 \rightarrow R^3$ is r-times differentiable ($k \geq 1$) with a continuous derivative C^k. Let $x_e \in R^3$ be an equilibrium point of system (1), then x_e is called a saddle

focus if the eigenvalues of the Jacobian *J* of *f(x)* evaluated at x_e are of the form

$$\lambda_1 = \alpha, \ \lambda_{2,3} = \beta \pm i\gamma, \quad \alpha\beta < 0, \quad \gamma \neq 0 \qquad (2)$$

where α, β and γ are real.

Theorem 1 *(Shilnikov Homoclinic theorem) [8]: For a 3D autonomous system (1), let x_e be a saddle focus equilibrium point whose eigenvalues satisfy $|\alpha| > |\beta| > 0$, there exists a homoclinic orbit connected at x_e. Then the 3D autonomous system has horseshoe chaos.*

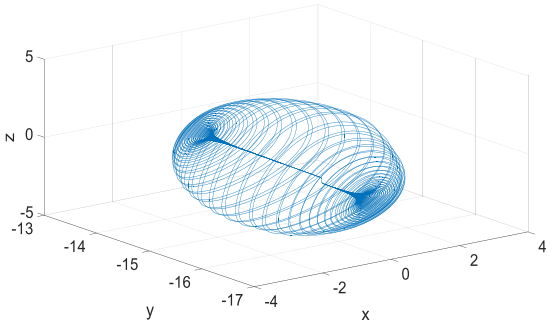
Theorem 2 *(Shilnikov Heteroclinic theorem) [8]: Suppose that two distinct equilibrium points x_e^1 and x_e^2 of a 3D autonomous system (1) are saddle foci, whose eigenvalues at these points are α_n and $\beta_n \pm i\gamma_n$ (n = 1, 2), satisfy the Shilnikov inequality $|\alpha_n| > |\beta_n| > 0$, n = 1, 2, under the constraint $\beta_1\beta_2 > 0$ or $\alpha_1\alpha_2 > 0$. Suppose also that there exists a heteroclinic orbit connecting x_e^1 and x_e^2. Then the 3D autonomous system has horseshoe chaos.*

According to the authors, the chaotic system in [4] can display a 3-layer attractor. The 3D spherical chaotic system is perturbed by a hyperbolic tangent function as given in (3).

$$\left.\begin{aligned} \dot{x} &= a_1 x - a_2 y + a_3 z + 2\left(\frac{1-\exp(-200\sin y)}{1+\exp(-200\sin y)}\right) \\ \dot{y} &= -dxz + b + ex \\ \dot{z} &= c_1 xy + c_2 yz + c_3 z + c \end{aligned}\right\} \qquad (3)$$

where $a_i \neq 0$, $c_i \neq 0$ $(1 \leq i \leq 3)$, $d \neq 0$, $b \neq 0$, and $c \neq 0$ are all real parameters. At a_1= -4.1, a_2 = 1.2, a_3 = 13.45, c_1 =2.76, c_2 = 0.6, c_3 = 13.13, c = 3.5031, d = 1.6, and e = 0, the system in (3) has only one equilibrium point (x, y, z) = (0.7217, -2.5698, 0.1394), which is chaotic. The associated eigenvalues are (λ_1, λ_2, λ_3) = (3.7747+6.0632i, 3.7747-6.0632i, -0.0612). The Lyapunov exponents corresponding to this chaotic state are (*LE1*, *LE2*, *LE3*) = (0.041, 0, -0.117).
The phase diagrams, plotted with data of last 100 secs to remove transient states, are shown in Fig. 1 below. In this work, 4th-order Runge-Kutta numerical method, with fixed step-size h = 0.001, was applied to perform all numerical integrations. Except specifically stated, the initial conditions were (x_0, y_0, z_0) = (-0.04, -15.8, -1.4) and the system parameter values are as stated above.

Fig 1. *Phase space portrait of 3D-spherical chaotic system.*



3. MASTER-SLAVE SYNCHRONIZATION USING HAMILTONINAN FORM AND OBSERVER APPROACH

In this investigation, the Hamiltonian system and observer approach [9] was applied to synchronize two chaotic oscillators of system (3) in a master-slave topology. In this way, the slave system serves as the observer of states, meaning that the state variables of the slave system will approximate the master. Mathematically, the master and slave of a dynamical system are expressed in Hamiltonian form as follows. Consider a dynamical system of the form:

$$\dot{x} = f(x) \qquad (4)$$

where $\dot{x} \in R^n$ is the state variable and $f: R^n \rightarrow R^n$ is the nonlinear function.

The dynamical system can be written also as:

$$\dot{x} = A\frac{\partial H}{\partial x} + \mathcal{F}(x) \qquad (5)$$

where $A = \frac{A-A^T}{2} + \frac{A+A^T}{2}$. Therefore,

$$\dot{x} = \frac{A-A^T}{2}\frac{\partial H}{\partial x} + \frac{A+A^T}{2}\frac{\partial H}{\partial x} + \mathcal{F}(x) \qquad (6)$$

Let $\mathcal{J}(x) = \frac{A-A^T}{2}$ and $\mathcal{S}(x) = \frac{A+A^T}{2}$, hence (4) can be written in the Generalized Hamiltonian canonical form as follows:

$$\dot{x} = \mathcal{J}(x)\frac{\partial H}{\partial x} + \mathcal{S}(x)\frac{\partial H}{\partial x} + \mathcal{F}(x), \quad x \in R^n \qquad (7)$$

where $H(x) = \frac{1}{2}x^T\mathrm{M}x$ denotes a positive smooth energy function definite in R^n, M is a constant, symmetric positive definite matrix, and hence, $\frac{\partial H}{\partial x}$ = Mx. $\frac{\partial H}{\partial x}$ is the column gradient vector of H(x), while matrix $\mathcal{J}(x)$ satisfies $\mathcal{J}(x) + \mathcal{J}^T(x) = 0$ and $\mathcal{S}(x)$ satisfies $\mathcal{S}(x) = \mathcal{S}^T(x)$ for all $x \in R^n$. The vector field $\mathcal{J}(x)\frac{\partial H}{\partial x}$ exhibits the conservative part and $\mathcal{S}(x)$ represents the nonconservative part of the system.

In the case of the observer design approach, a special class of the Generalized Hamiltonian forms with destabilizing vector field and output *y(t)*, which is the master system, is given by:

$$\begin{cases} \dot{x} = \mathcal{J}(y)\frac{\partial H}{\partial x} + \mathcal{S}(y)\frac{\partial H}{\partial x} + \mathcal{F}(y), & x \in R^n \\ y = \mathcal{C}\frac{\partial H}{\partial x}, & y \in R^m \end{cases} \qquad (8)$$

where $\mathcal{S}$ is a constant symmetric matrix and $\mathcal{C}$ is a constant matrix.

Similarly, the dynamical nonlinear state observer, the slave system, is defined as follows. The estimate of the state vector x is denoted by $\hat{\xi}$ and the estimated output is denoted by η. Thus, the slave system is:

$$\begin{cases} \dot{\xi} = \mathcal{J}(y)\frac{\partial H}{\partial \xi} + \mathcal{S}(y)\frac{\partial H}{\partial \xi} + \mathcal{F}(y) + \mathcal{K}e_y, \quad \xi \epsilon R^n \\ \eta = \mathcal{C}\frac{\partial H}{\partial \xi}, \quad \eta \epsilon R^m \end{cases} \tag{9}$$

where $\mathcal{K}$is the gain of the observer and $e_y = y - \eta$ is the output estimation error. The state estimation error is defined by $e = x - \xi$.

The synchronization by Hamiltonian systems is considered successful according to the following definition and theorems.

Definition 1 [10]: The basic condition for the slave to synchronize with the master in Hamiltonian form is when:

$$\lim_{t\to\infty} \|x(t) - \xi(t)\| = 0 \tag{10}$$

regardless of what the initial conditions $x(0)$ and $\xi(0)$ are.

Theorem 3 *[10]: The state x of the nonlinear system in (8) can be globally, exponentially, and asymptotically estimated by the state ξ of the nonlinear observer (9) if the pair of matrices $(\mathcal{C}, \mathcal{S})$ are observable.*

Theorem 4 *[10]: The state x of the nonlinear system in (8) can be globally, exponentially, and asymptotically estimated by the state ξ of the nonlinear observer (9) if and only if there exists a constant matrix $\mathcal{K}$ such that the symmetric matrix.*

$$[W - KC] + [W - KT]^T = [S - KC] + [S - KC]^T = 2\left[S - \frac{1}{2}(KC + C^T K^T)\right] \tag{11}$$

is negative definite.

Therefore, the master system is constructed as follows:

$$\mathcal{J}(x) = \begin{bmatrix} 0 & \frac{-a_2-e}{2} & \frac{a_3}{2} \\ \frac{a_2+e}{2} & 0 & \frac{-c_1x-dx}{2} \\ -\frac{a_3}{2} & \frac{c_1x+dx}{2} & 0 \end{bmatrix} \tag{12}$$

$$\mathcal{S}(x) = \begin{bmatrix} a_1 & \frac{-a_2+e}{2} & \frac{a_3}{2} \\ \frac{-a_2+e}{2} & 0 & \frac{c_1x-dx}{2} \\ \frac{a_3}{2} & \frac{c_1x-dx}{2} & c_2y + c_3 \end{bmatrix} \tag{13}$$

$$\mathcal{F}(x) = \begin{bmatrix} 2\left(\frac{1-e^{-200\sin y}}{1+e^{-200\sin y}}\right) \\ b \\ c \end{bmatrix} \tag{14}$$

According to (8),

$$\begin{bmatrix} \dot{x} \\ \dot{y} \\ \dot{z} \end{bmatrix} = \begin{bmatrix} 0 & \frac{-a_2-e}{2} & \frac{a_3}{2} \\ \frac{a_2+e}{2} & 0 & \frac{-c_1x-dx}{2} \\ -\frac{a_3}{2} & \frac{c_1x+dx}{2} & 0 \end{bmatrix} \frac{\partial H}{\partial x} + \begin{bmatrix} a_1 & \frac{-a_2+e}{2} & \frac{a_3}{2} \\ \frac{-a_2+e}{2} & 0 & \frac{c_1x-dx}{2} \\ \frac{a_3}{2} & \frac{c_1x-dx}{2} & c_2y + c_3 \end{bmatrix} \frac{\partial H}{\partial x} + \begin{bmatrix} 2\left(\frac{1-e^{-200\sin y}}{1+e^{-200\sin y}}\right) \\ b \\ c \end{bmatrix} \tag{15}$$

where

$H(x) = \frac{1}{2}[x^2 + y^2 + z^2]$ and the gradient vector is $\frac{\partial H}{\partial x} = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$.

The manipulation of (15) resulted in the following master system in (16).

$$\begin{bmatrix} \dot{x} \\ \dot{y} \\ \dot{z} \end{bmatrix} = \begin{bmatrix} a_1x - a_2y + a_3z \\ -dxz + ex \\ -c_1xy + c_2yz + c_3z \end{bmatrix} + \begin{bmatrix} 2\left(\frac{1-e^{-200\sin y}}{1+e^{-200\sin y}}\right) \\ b \\ c \end{bmatrix} \tag{16}$$

Similarly, for the slave system and according to (9),

$$\begin{bmatrix} \dot{\xi}1 \\ \dot{\xi}2 \\ \dot{\xi}3 \end{bmatrix} = \begin{bmatrix} 0 & \frac{-a_2-e}{2} & \frac{a_3}{2} \\ \frac{a_2+e}{2} & 0 & \frac{-c_1x-dx}{2} \\ -\frac{a_3}{2} & \frac{c_1x+dx}{2} & 0 \end{bmatrix} \frac{\partial H}{\partial \xi} + \begin{bmatrix} a_1 & \frac{-a_2+e}{2} & \frac{a_3}{2} \\ \frac{-a_2+e}{2} & 0 & \frac{c_1x-dx}{2} \\ \frac{a_3}{2} & \frac{c_1x-dx}{2} & c_2y + c_3 \end{bmatrix} \frac{\partial H}{\partial \xi} + \begin{bmatrix} 2\left(\frac{1-e^{-200\sin y}}{1+e^{-200\sin y}}\right) \\ b \\ c \end{bmatrix} + \begin{bmatrix} k_1 \\ k_2 \\ k_3 \end{bmatrix} e_y \tag{17}$$

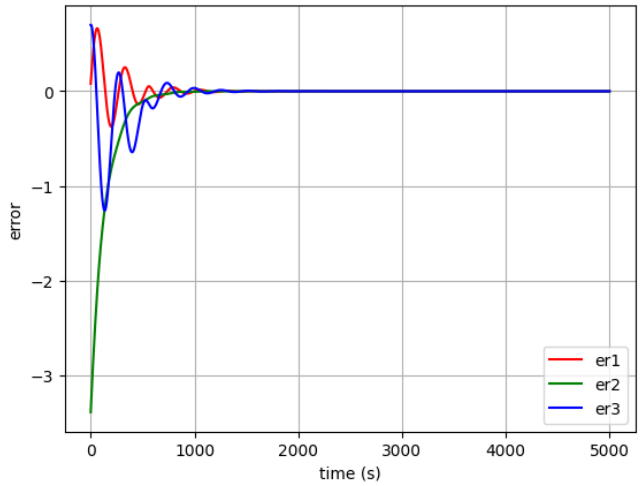
Upon simplification, the receiver dynamics (17) becomes (18).

$$\begin{bmatrix} \dot{y}1 \\ \dot{y}2 \\ \dot{y}3 \end{bmatrix} = \begin{bmatrix} a_1x - a_2y + a_3z \\ -dxz + ex \\ -c_1xy + c_2yz + c_3z \end{bmatrix} + \begin{bmatrix} 2\left(\frac{1-e^{-200\sin y}}{1+e^{-200\sin y}}\right) \\ b \\ c \end{bmatrix} + \begin{bmatrix} k_1 \\ k_2 \\ k_3 \end{bmatrix} e_y \tag{18}$$

The gains of the observer selected according to Theorem 4 were k_1 = 2, k_2 = 7, and k_3 = 5. The initial condition for the master and slave systems were [-0.04, -15.8, -1.4] and [-0.12, -12.41, -2.1], respectively.

The synchronization errors of the master-slave system are $e_1=x_1-y_1$, $e_2=x_2-y_2$, $e_3=x_3-y_3$, where x_i represents the master while y_i denotes the slave. The master and slave systems were synchronized within a very short time after which the error signal e_1, e_2 and e_3 became zero. Therefore, the ratio of the master and the slave states x_i and y_i was 1 after a very short time as shown in figure 2.

Fig 2. *Synchronization error between master and slave state variables of 3D shepherical chaotic atractor.*



4. SECURE COMMUNICATION BASED ON SYNCHRONIZED 3D CHAOTIC ATTRACTOR

The secure communication system was successfully implemented in python by adopting the encryption model in Fig 3 which utilizes the synchronization configuration in master-slave topology as shown in Fig 4. Within the master system, the chaotic transmission signal *Xm* is employed to encrypt the original image using the X-OR operator. This encrypted image, denoted as *IMt*, is then transmitted to the receiver in the slave system. Ultimately, since the slave system approximates the master system, the recovered image *IMr* is obtained by performing the inverse of the encryption procedure.

Fig 3. *Master-slave topology-based secure communication system implemented on MPSoc.*

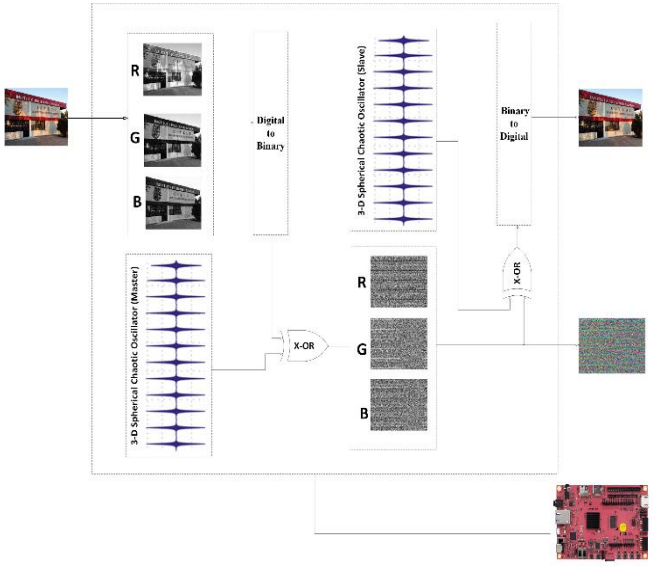
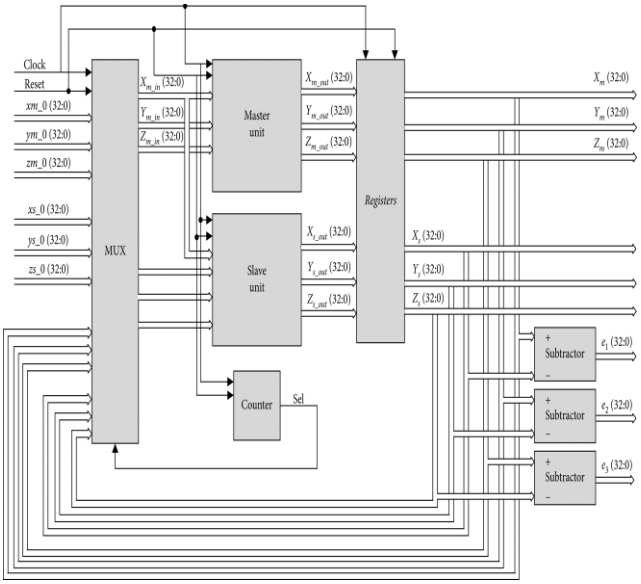


Fig 4. *Master-slave topology-based secure communication system implemented on MPSoc*



In the implementation of the secure transmission system, grayscale and RGB images of dimensions 256 x 256 pixels were utilized. The image transmission commenced following the successful synchronization of the master and slave systems. In this study, each of the three state variables x_1, x_2, and x_3 was employed as a transmission variable for RGB images. The obtained results were analyzed statistically. Due to space limitations, only the results related to the transmission variable yielding the best output, based on the correlation coefficients outlined in Table I, are presented. These results are depicted in Fig. 5 for the RGB image, showcasing the original, encrypted, and received images for variable x_1 for grayscale and x_3 for RGB.

The system was implemented by utilizing FPGA technology, specifically leveraging the support provided by the PYNQ-Z1 module. This module enables programming in the Hardware Description Language and in high-level languages like Python [11]. PYNQ is an open-source project that aims to simplify the design of embedded systems with Zynq, a Multi- Processor System on Chip (MPSoC) device manufactured by Xilinx [12,13]. This device succeeded its precursor, the Zynq-7000 [12,13], and integrates two ARM-Cortex core processors and various interfaces vital for embedded systems, including I2C, SPI, CAN, UART, GPIO, and more.

Next, the performance of the chaotic communication system was examined by carrying out security and statistical analyses on the results of the image transmission. As expected, a reliable encryption system should be robust against different kinds of attacks.

In the implemented chaos-based secure communication system, the system parameters a_1, a_2, a_3, b, c, c_1, c_2, c_3, d, and e of the master and slave systems in (16) and (18),

respectively, can be taken as the primary secret key. Let's assume the precision of each of the ten parameters is 10^{-12}, then the secret key space will be equal to 10^{100}, which is quite large enough to resist exhaustive hacker's attack [14].

The concept of information entropy is used to measure the average information content associated with a random outcome. It describes the degree of uncertainty in a system. In image processing, information entropy is applied to measure the distribution of gray data values in the image [15]. Information entropy *H* is expressed mathematically as:

$$H(G) = -\sum_{i=1}^{n} P(g_i)\log_2 P(g_i) \quad (19)$$

where, for image information, *G* is the image matrix, g_i are the gray values of the image, $P(g_i) = Pr\,(G = g_i)$ is the probability of the i^{th} value of *G*.

For example, if image *G* is a true random source producing 2^N symbols, where $N = 8$ for 256x256 image, the theoretical value of information entropy of a true random image is 8. Therefore, it is expected that the information entropy of a well-encrypted image should be close to 8. According to Table I, the entropy values are very close to 8. This shows that the chaos-based encryption system is very effective.

The coefficient is computed as follows:

$$r = \frac{\sum_m \sum_n (A_{mn} - \overline{A})(B_{mn} - \overline{B})}{\sqrt{\left(\sum_m \sum_n (A_{mn} - \overline{A})^2\right)\left(\sum_m \sum_n (B_{mn} - \overline{B})^2\right)}} \quad (20)$$

where $\overline{A}$ and $\overline{B}$ are the mean of all values in arrays *A* and *B*.

Also, the computation of the pixel correlation coefficients in horizontal, vertical, and diagonal directions, between the original and encrypted images, is defined and computed by the following formula:

$$\rho(g,h) = \frac{\mathrm{cov}(g,h)}{\sigma_g \sigma_h} \quad (21)$$

where

$$\mathrm{cov}(g,h) = \frac{1}{n}\sum_{i=1}^{n}(g_i - \mu_g)(h_i - \mu_h) \quad (22)$$

Variables *g* and *h* are the gray values of two adjacent pixels in the image, σ_g and σ_h are the standard deviations of *g* and *h* respectively, and μ_g and μ_h are the means of *g* and *h* respectively.

In Table I for grayscale and RGB, respectively, it is seen that correlation between the original and encrypted images is very close to 0 in all the transmission variables. Specifically, according to the correlation between the original and encrypted images, the best result in the grayscale image transmission was given by transmission variable x_1, where $r = 7.3793\text{e-}05$ while for RGB it was variable x_3, where $r = 0.00113$.

Fig 5. *Transmission of RGB image using x_3 as transmission variable (a) original (b) encrypted (c) received.*

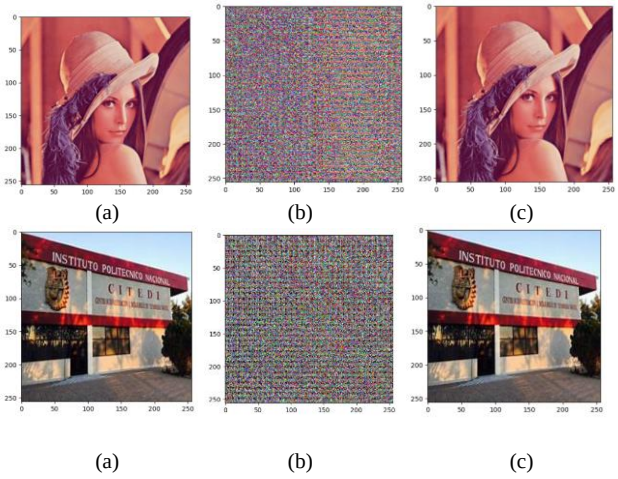


Table 1. *Statistical Analysis of Grayscale and RGB Image Transmission Results by Entropy and Correlation*

Transmission variable	Entropy of the encrypted image	Correlation	
		Original and encrypted	*Original and received*
Grayscale Image			
x_1	7.9916	7.3793e-05	1
x_2	7.9918	0.00216	1
x_3	7.9908	0.00727	1
RGB Image			
x_1	7.9961	–0.00145	1
x_2	7.9981	0.00380	1
x_3	7.9965	0.00113	1

The correlation between the adjacent pixels in the original grayscale and RGB images was very high, but after the encryption, the correlation was greatly reduced, as seen in the pixel correlation coefficients presented in Table II for grayscale and RGB, respectively. For example, the correlation coefficients of two horizontally adjacent pixels in the original grayscale image for x_1 transmission variable was 0.94084 while for the encrypted grayscale, it was –0.00101. In transmission variable x_3 for RGB, the correlation coefficients of two horizontally adjacent pixels in the original image was 0.93858 but for the encrypted image, it was 0.00040. The results were similar in all cases. Hence, the encryption performed in this investigation effectively removes relativity between the original and encrypted images.

Table 2. *Statistical Analysis of Grayscale and RGB Image Transmission Results by Pixel Correlation Coefficient in Horizontal, Vertical and Diagonal Direction.*

Variable	Original			Encrypted		
	Horizontal	*Vertical*	*Diagonal*	*Horizontal*	*Vertical*	*Diagonal*
Grayscale Image						
x_1	0.94084	0.97213	0.91711	-0.00101	-0.00182	-0.00500
x_2	0.94084	0.97213	0.91711	-0.00853	-0.00162	0.00458
x_3	0.94084	0.97213	0.91711	-0.00053	-0.00093	-0.00419

RGB Image						
x_1	0.93858	0.94349	0.92708	0.00040	-0.00183	0.00225
x_2	0.93858	0.94349	0.92708	0.00121	0.01624	0.00148
x_3	0.93858	0.94349	0.92708	-0.00182	0.00111	-0.00075

5. CONCLUSION

In this work, a multimedia encryption system utilizing a synchronized 3-dimensional chaotic oscillators in master and slave topology was presented, where the synchronization was achieved by applying the Hamiltonian system with the observer-based approach. The process demonstrated rapid convergence, achieving zero synchronization errors, and thereby confirming successful synchronization between the master and slave systems.

Furthermore, the synchronized system was applied to develop a secure communication system for transmitting RGB and grayscale images, whereby the state variables x1, x2, and x3 were used as the transmission variables. Statistical and security assessments of the streaming results showcased the robustness of the system against extensive attacks. Notably, the correlation between the original and encrypted images approached zero, confirming the system's efficacy in secure image transmission.

Moreover, this work was implemented by leveraging the Multipurpose System-on-Chip (MPSoC) platform through Interactive Python in Jupyter Notebook to unlock the untapped potentials within modern programming languages for hardware design. This approach allowed for high-level abstractions, parameterized generators, and freedom from specific computational models, culminating in the generation of superior RTL logic programming code in Verilog. The integration of fast Python-based simulation, efficient synthesis, and seamless interaction with other high-level languages emphasized the versatility and power of this platform for advanced hardware development and design.

Finally, based on the synchronization and image transmission done in this work, the 3-D chaotic spherical system is capable of being used to implement secure communication system.

6. RECOMMENDATIONS

Based on the successful implementation and results of the synchronized 3D spherical chaotic oscillator in a master-slave topology as presented in this article which was utilized for securing information transmitted through communciation system. The potential future direction recommended herein as as follows:

1. **Enhanced Security Protocol:** The scientific body can explore advance security protocols and encryption techniques by utilizing the MPSoC platform. This could involve integrating additional encryption methods with the one presented in this paper to enhance data confidentiality.
2. **Integration with IoT Devices:** The scientific body can explore the integration of the secure communication system with IoT devices for secure data transmission in IoT environments.

7. REFERENCES

[1] O.E. Rössler, "Different types of chaos in two simple differential equations," Zeitschrift fur Naturforschung A, vol. 31, no. 12, pp. 1976-1231, Nov. 1976.

[2] O.E. Rössler, "Continuous chaos - Four prototype equations," Annals of the New York Academy of Sciences, vol. 316, no. 1, pp. 376-392, Dec. 2006.

[3] G. Chen, "The Chen system revisited," Dynamics of continuous, discrete and impulsive systems, Series B: Applications & algorithms, vol. 20, pp. 691-696, Nov. 2013.

[4] Z. Wang, Y. Sun, and S. Cang, "A 3-D spherical chaotic attractor," Acta Physica Polonica B, vol. 42, no. 2, pp. 235-247, Feb. 2011.

[5] T. Zhou and G. Chen, "A simple smooth chaotic system with a 3-layer attractor," International Journal of Bifurcation and Chaos, vol. 14, no. 5, pp. 1795-1799, May 2004.

[6] G. Li and X. Chen, "Constructing piecewise linear chaotic system based on the heteroclinic Shilnikov theorem," Communications in Nonlinear Science and Numerical Simulation, vol. 14, no. 1, pp. 194-203, Jan. 2009.

[7] T.S. Zhou and G. Chen, "Classification of chaos in 3-D autonomous quadratic systems-I. Basic framework and methods," International Journal of Bifurcation and Chaos, vol. 16, no. 9, pp. 2459-2479, Sept. 2006.

[8] Ding, Y., & Zheng, L. (2023). Existence of homoclinic orbit of Shilnikov type and the application in Rössler system. *Mathematics and Computers in Simulation, 206*, 770–779. https://doi.org/10.1016/j.matcom.2022.12.013

[9] H. Sira-Ramirez and C. Cruz-Hernandez, "Synchronization of chaotic systems: A generalized Hamiltonian systems approach," International Journal of Bifurcation and Chaos, vol. 11, no. 5, pp. 1381-1395, May 2001.

[10] L.J. Pei and S.H. Liu, "Application of generalized Hamiltonian systems to chaotic synchronization," Nonlinear Dynamics and Systems Theory, vol. 9, no. 4, pp. 415-432, Sept. 2009.

[11] Herrera-Charles, R., Álvarez-Sánchez, T., &; Álvarez-Cedillo, J. A. (2020). Synthesis of video processing with open-source hardware descriptor languages. In A. G. Tescher & T. Ebrahimi (Eds.), Applications of Digital Image Processing XLIII (p. 65). SPIE. https://doi.org/10.1117/12.2568949

[12] Xilinx, Inc., "Zynq UltraScale+ Device: Technical Reference Manual", UG1085, v1.9, January 2019. Available:

[13] Xilinx, Inc., "Zynq UltraScale+ MPSoC Overview: Advance Product Specification", DS891, v1.7, November 2018. Available: https://www.xilinx.com/support/documentation/data_sheets/ds891-zynq-ultrascale-plus-overview.pdf

[14] Sun, F., Lü, Z., & Liu, S. (2010). A new cryptosystem based on spatial chaotic system. *Optics Communications, 283*(10), 2066–2073. https://doi.org/10.1016/j.optcom.2010.01.028

[15] G. Zhang and Q. Liu, "A novel image encryption method based on total shuffling scheme," Optics Communications, vol. 284, no. 12, pp. 2775-2780, June 2015.