

# Four dimensional hyperchaotic communication system based on dynamic feedback synchronization technique for image encryption systems

Hayder Mazin Makki Alibraheemi, Qais Al-Gayem, Ehab AbdulRazzaq Hussein

Department of Electrical Engineering, University of Babylon, Babylon, Iraq

## Article Info

### Article history:

Received Jan 9, 2021

Revised Jul 10, 2021

Accepted Jul 28, 2021

### Keywords:

Dynamic feedback modulation

Hyperchaotic

Hyperchaotic synchronization

Lorenz generator

MATLAB Simulink

## ABSTRACT

This paper presents the design and simulation of a hyperchaotic communication system based on four dimensions (4D) Lorenz generator. The synchronization technique that used between the master/transmitter and the slave/receiver is based on dynamic feedback modulation technique (DFM). The mismatch error between the master dynamics and slave dynamics are calculated continuously to maintain the sync process. The information signal (binary image) is masked (encrypted) by the hyperchaotic sample  $x$  of Lorenz generator. The design and simulation of the overall system are carried out using MATLAB Simulink software. The simulation results prove that the system is suitable for securing the plain-data, in particular the image data with a size of  $128 \times 128$  pixels within 0.1 second required for encryption, and decryption in the presence of the channel noise. The decryption results for gray and colored images show that the system can accurately decipher the ciphered image, but with low level distortion in the image pixels due to the channel noise. These results make the proposed cryptosystem suitable for real time secure communications.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



## Corresponding Author:

Hayder Mazin Makki Alibraheemi

Department of Electrical Engineering, University of Babylon

Iraq-Babil-Najaf Road, PO Box: 4 Iraq-Babylon-Hilla, Iraq

Email: hayder.makki.engh278@student.uobabylon.edu.iq

## 1. INTRODUCTION

The recent decade has been known by exponential growth in the trendy applications, especially in the field of multimedia communications. The main types of the multimedia communications, which are video, image, and audio files are taking place more frequently in the transmission operation through the communication networks, which result in the huge growth of data exchange (for a single person). This growth in the data exchange for a single person comes with a massive increase in the number of communication devices, which lead to more and more data exchange over the network [1].

The data integrity and confidentiality of these multimedia contents are becoming more and more important with time due to the high sensitivity of these exchanged data. Massive efforts by the researchers are spent to develop a new robust cryptographic system in order to meet the security requirements for the data transmission over the network. In this context, a huge number of cryptographic algorithms have been developed over the past years in order to provide the security requirements for the user's data [2].

The developed cryptographic algorithms can be classified according to the number of keys required for encryption and decryption process into private key cryptography and public key cryptography. The private key cryptography algorithms use only one private key for encryption and decryption, this type of algorithms is relatively fast and suitable for high speed applications, but the key exchange between the transmitter and

receiver (synchronization) is considered as a disadvantage of such algorithms. On the other hand, the public key cryptography algorithms use two keys, the first is the encryption key which is public and the other is the decryption key that is private and considered to be secret key. The public key cryptography provides a solution to the key exchange problem, but this type of algorithms is suffering from slow speed in processing [3], [4].

According to the previous classification (number of required keys), a huge number of cryptographic algorithms have been developed, such as data encryption standard (DES), triple data encryption standard (3DES), advanced encryption standard (AES), rivest shamir adleman (RSA), and IDEA [5], [6]. These traditional cryptography systems suffer from some weak points, such as low efficiency, especially for real time processing applications and with the invention of high computational power machines, these algorithms became more hackable through a brute force attack.

So far, the past few years have seen an urgent requirement for developing and designing a robust and fast cryptographic algorithm to be used for real time multimedia encryption systems. Due to the pseudo-random properties, ergodicity and non-periodicity, that chaotic systems have, they are considered a perfect solution for designing a robust security system for multimedia communication purposes [7]. Chaotic and hyperchaotic systems are considered one of the most prominent candidates for information security purposes, because their properties that match the designing requirements for a robust cryptographic system such as, extremely sensitive to initial conditions and system parameters as well as they have unpredictable behavior [8].

Many techniques based on chaos theory have been proposed to be a security system that is alternative to the traditional algorithms which mentioned above. Cuomo *et al.* [9] additive chaos masking is proposed, where the information signal is masked (encrypted) using one of the dynamics of the chaotic system generators. Dedieu *et al.* [10] proposed the chaos switching or chaos shift keying, where the binary information signal is used to select the carrier signal between different chaotic generators. Another technique that based on dynamic modulation principle is presented in [11], where in this technique the information signal is used as input to modulate the parameters of a chaotic generator system. The continuously increasing demand for securing the user's personal data push the researchers to develop high order hyperchaotic based cryptosystem, where in [12] 7 dimensional hyperchaotic system is proposed for securing the passive optical network in a corporation with orthogonal frequency division multiplexing (OFDM) technique. Zhang [13] proposed a new method to build a cryptosystem, where they combined the hyperchaotic Lorenz attractor with cat map to cipher the images with fast speed; the proposed combination between two or more chaotic behaviors add more complex behavior to the cryptosystem which will defy the conventional cryptographic attacks.

Mathematically increasing the order of the differential equations that composed the hyperchaotic system lead to increase the complexity of the cryptosystem which will enhance the confidentiality of the transmitted data, based on this fact a new hyperchaotic system is proposed with 9 dimensional parameters in [14] for bitstream ciphering issues. The logistic map is adopted in [15], [16] for securing the image by means of bit distribution balancing. Zhu *et al.* [17] present an eight dimension with seven order hyperchaotic systems, the eight dimension system is implemented using operational amplifiers with some resistors and capacitors. The implementation results are in a good agreement with preprocessed Multisim simulations, where these results prove that the system can be used for information security purposes. In this paper, the design and simulation of hyperchaotic four dimensional systems for image encryption are presented. The system generator is based on the Lorenz system [18]. The transmitter and receiver of the communication system are designed separately. The synchronization between the TX and RX is achieved based on dynamic feedback modulation DFM, where the error between the responses of the TX and RX are calculated dynamically in continuous mode to maintain the synchronization between the two components [19]-[21]. The rest of this paper is organized as follows, section 2 presents the research method, which contains the proposed research design, mathematical description and other related system implementations, section 3 shows the obtained results using MATLAB Simulink software. Finally, the conclusions and future improvement are described in section 4.

## 2. RESEARCH METHOD

The mathematical foundation of the cryptographic communication system with the proposed synchronization technique as well as the MATLAB system implementation is presented in this section as follow.

### 2.1. Mathematical description of the hyperchaotic system

The dynamical system that adopted in order to generate the chaotic behavior of the master (transmitter) system is described in the set of differential equations as shown in (1) [18]. On the other hand, the slave (receiver) system is using the differential equations presented in (2), where the ( $m$ ) and ( $s$ ) subscript refers to the master and slave systems respectively.

$$\begin{aligned}
x_m &= \sigma(y_m - x_m) \\
y_m &= x_m(r - z_m) - y_m + w_m \\
z_m &= x_m y_m - b z_m \\
w_m &= -\gamma x_m \\
\sigma &= 10, b = \frac{8}{3}, r = 28, \gamma = -5
\end{aligned} \tag{1}$$

$$\begin{aligned}
x_s &= \sigma(y_s - x_s) \\
y_s &= x_s(r - z_s) - y_s + w_s \\
z_s &= x_s y_s - b z_s \\
w_s &= -\gamma x_s \\
\sigma &= 10, b = \frac{8}{3}, r = 28, \gamma = -5
\end{aligned} \tag{2}$$

## 2.2. System synchronization

The synchronization of two dynamical systems means that, the trajectory (or the behavior) of one system is converging to the same trajectory value as the other and they will remain in synch with each other. At the first glance, any two or more hyperchaotic systems would seem to be a dynamical system that cannot be synchronized, since these systems are defying the synchronization. The practical implementation of the synchronization between two systems is not possible, until the publication of Pecora and Carroll [22], where since that time the synchronization has become possible. The synchronization that adopted in our system implementation is based on reducing the dynamical error between the trajectories of the master and slave subsystems gradually until reaching zero error (difference) [22]. The dynamical error is calculated by subtracting the system in (2) from the system in (1) to get the error as shown in (3).

$$\begin{aligned}
e_x &= x_m - x_s = \sigma[(y_m - x_m) - (y_s - x_s)] \\
e_y &= y_m - y_s = (x_m(r - z_m) - y_m + w_m) - (x_s(r - z_s) - y_s + w_s) \\
e_z &= z_m - z_s = (x_m y_m - b z_m) - (x_s y_s - b z_s) \\
e_w &= w_m - w_s = -\gamma x_m + \gamma x_s
\end{aligned} \tag{3}$$

These error values will be used to provide the necessary synchronization, where the error first will be multiplied with a specific value of gain (usually 10 to 20), then the result is dynamically added to the as shown in (2) to get the required synchronization after a few milliseconds of operation:

$$\begin{aligned}
cs_1 &= G e_x \\
cs_2 &= G e_y \\
cs_3 &= G e_z \\
cs_4 &= G e_w \\
cs &= \text{control signal}
\end{aligned} \tag{4}$$

The nonlinear system in (2) should be modified to achieve the synchronization as (5):

$$\begin{aligned}
x_s &= \sigma(y_s - x_s) + cs_1 \\
y_s &= x_s(r - z_s) - y_s + w_s + cs_2 \\
z_s &= x_s y_s - b z_s + cs_3 \\
w_s &= -\gamma x_s + cs_4
\end{aligned} \tag{5}$$

The  $cs_x$  refers to control signal that provides the necessary synchronization. The system in (1) and in (5), will be used in the next subsection to build the master and the slave subsystems. The system is summarized in Figure 1.

## 2.3. MATLAB implementation

In this section, the implementation and system design of the 4D Lorenz generator using MATLAB, Simulink will be presented based on the nonlinear equation subsystems in (1) and (5) [23]. The initial conditions of the generator selected to be -10 in both transmitter and receiver. The system parameters are selected to be  $\sigma=10$ ,  $r=28$ ,  $b=8/3$ , and  $\gamma=-5$  [18]. The Lorenz system shows chaotic behavior, according to the values that selected [24]. Figure 2 shows the master subsystem of the overall communication system. This subsystem is built based on the dynamical equations that presented in (1). The time response of the master subsystem is illustrated in Figure 3.

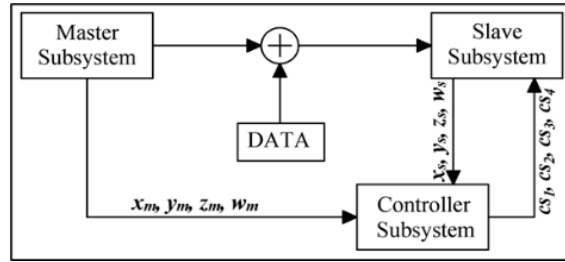


Figure 1. Overall system block diagram

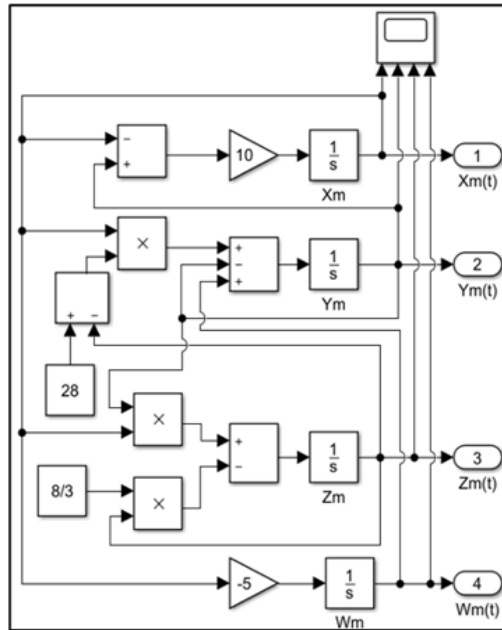


Figure 2. Master subsystem

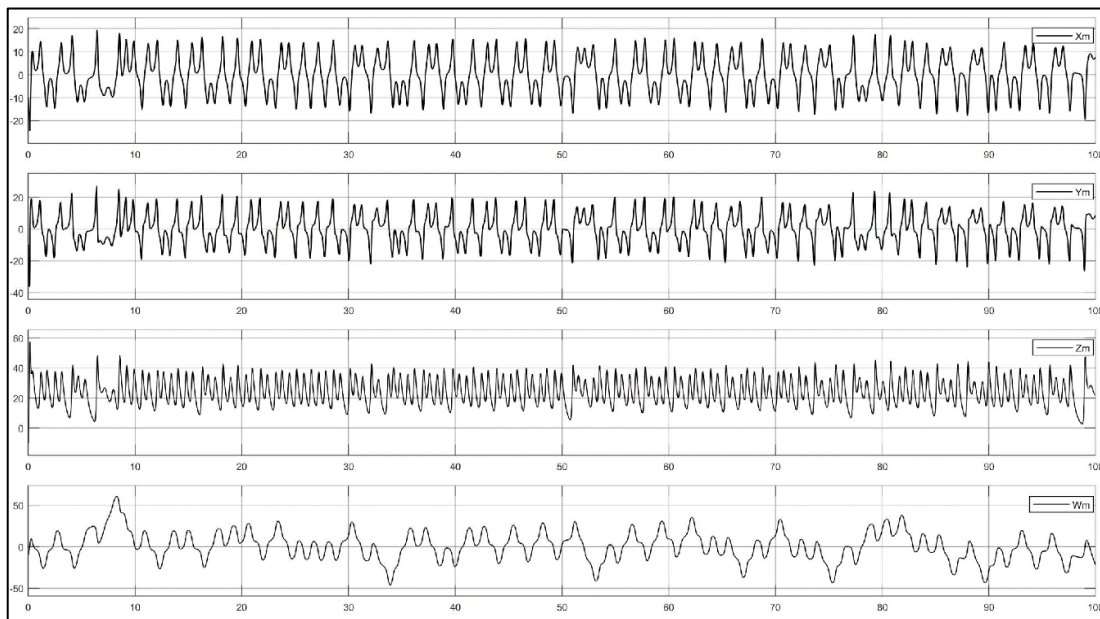


Figure 3. Master subsystem response

Figure 4 represents the slave subsystem, where it is built up based on the nonlinear equation system in (5). The control signals ( $cs_x$ ) also appear as an equation that varying with time. These control signals provide the necessary synchronization with master subsystem with the existence of channel noise. The response of the slave subsystem is depicted in Figure 5. To ensure that the two subsystems are operating in synchronous mode, Figure 6 shows the behavior of the X dynamical component of master and slave subsystems and proofs that  $x_m$  and  $x_s$  are successfully synchronized after a few milliseconds. Figure 7 illustrate the hyperchaotic behavior of the designed subsystems in the XY plane.

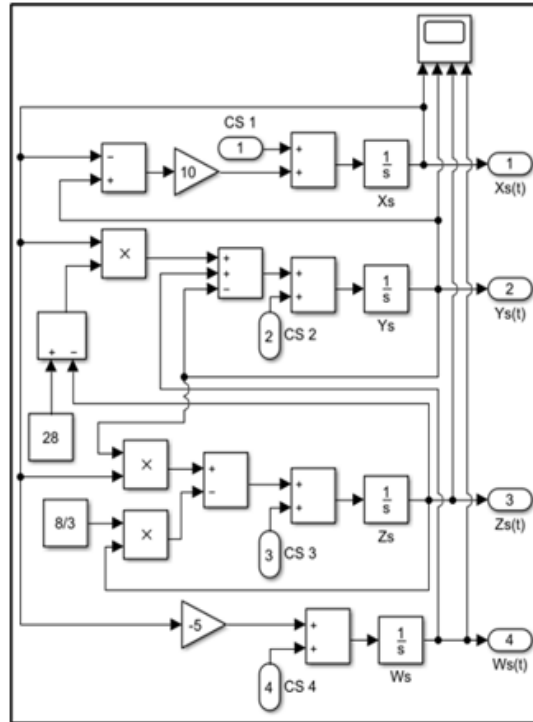


Figure 4. Slave subsystem

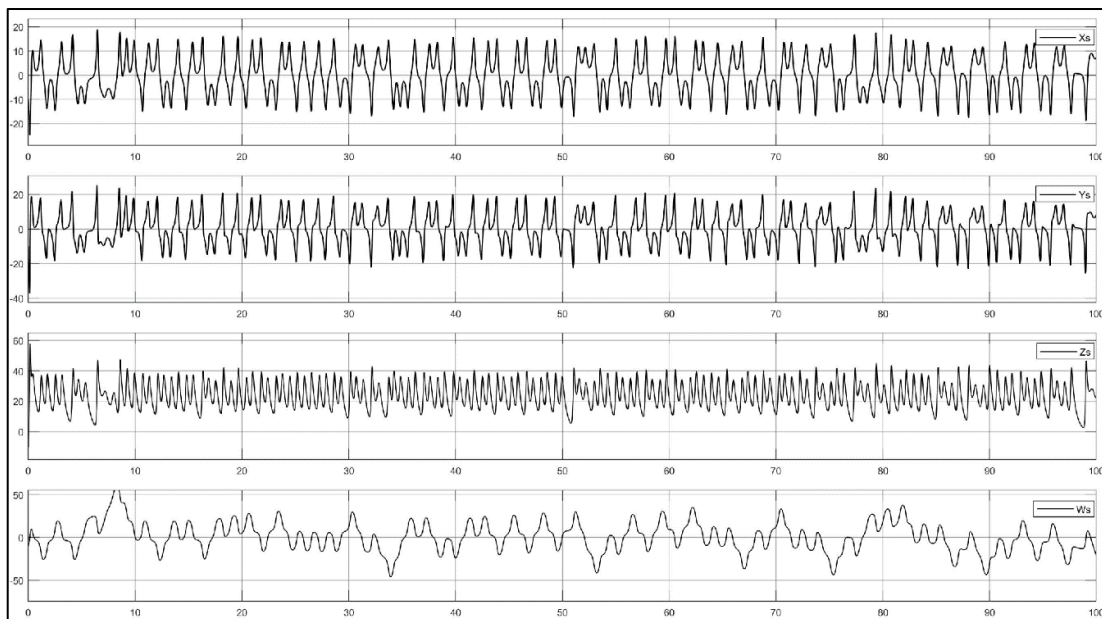


Figure 5. Slave subsystem response

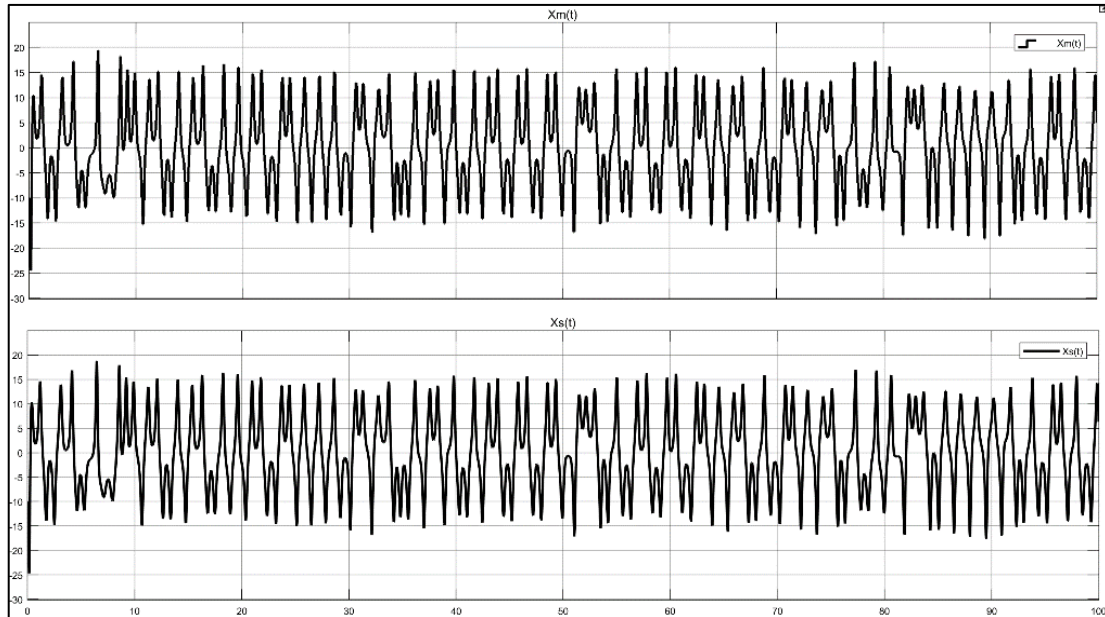


Figure 6. X components behavior of master and slave subsystems

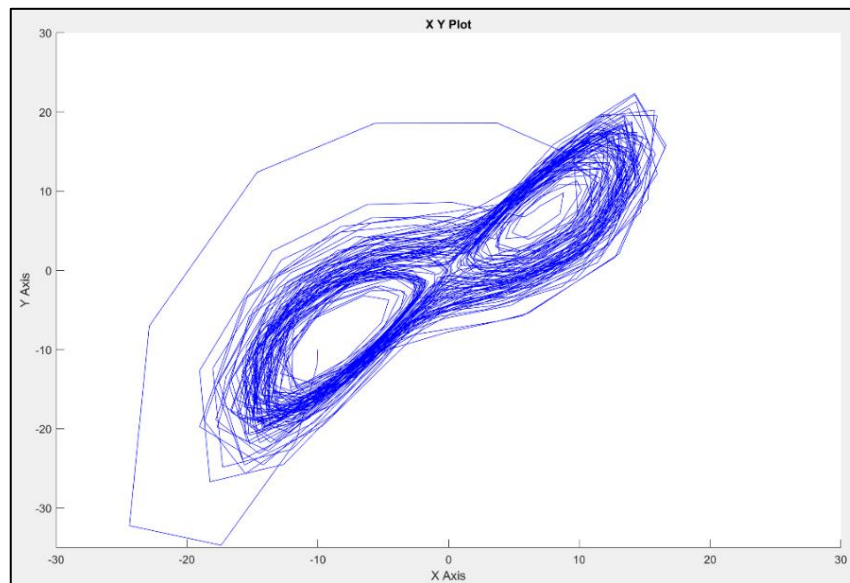


Figure 7. Hyperchaotic behavior in XY plane

### 3. RESULTS AND ANALYSIS

Since the designed master and slave subsystems are showing perfect synchronization after a few milliseconds from their operation. These two subsystems are used in this paper for the purpose of an image encryption for both, color, and grayscale image. The image firstly is converted to a binary matrix form by using the auto-threshold block in Simulink or by using manually written MATLAB M-file. The encryption process can be carried out by a means of adding the binary matrix to the x component of the master dynamical subsystem ( $x_m$ ), and in this case the x component can be considered as a carrier signal. The result of this addition is the encrypted message or can be called the masked message.

The encrypted message is then transmitted through the wireless channel towards the receiver. The receiver should be in sync with the master and start in the generation of the exact master carrier signal. Then the slave subsystem starts recovering the original message by subtracting the generated carrier signal ( $x_s$ ), which should be exactly like ( $x_m$ ), from the received encrypted message in order to recover the original



message [13]-[15]. The overall communication system that consists of master, slave, synchronization, control, and the image to binary conversion units are shown in Figure 8.

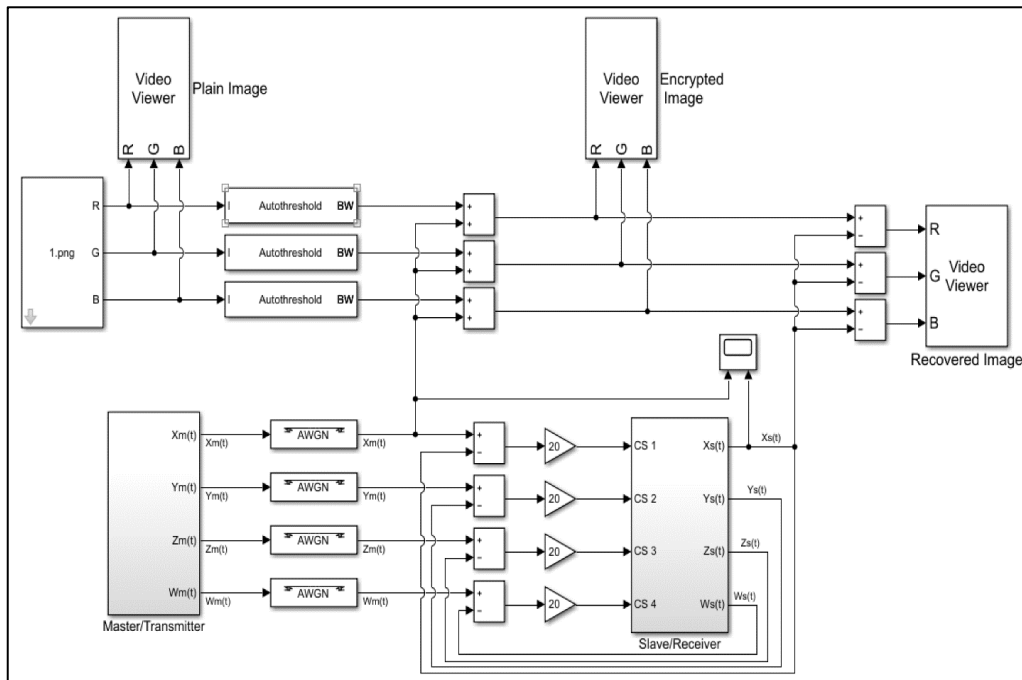


Figure 8. Overall communication system

The proposed communication system has been tested for both color and grayscale images. Figure 9(a)-(c) shows plain image, encrypted image, and the recovered image to grayscale image. While Figure 10(a)-(c) shows the plain image, encrypted image, and the recovered image of a color image. The simulation results of the proposed system show that, it is suitable for enciphering the plain-images in gray and color modes, where it requires a 0.1 second of time to provide the necessary synchronization between master and slave and to encrypt the input image of 128×128 pixels.

The decryption process for the ciphered image is carried out too, the retrieval plain image show that there is some distortion in the image pixels and this due to the channel noise that disturbed the transmission. This result makes the system suitable for real time applications compared with similar proposed hyperchaotic cryptosystems, and this due to the high processing speed that the proposed system has [25], [26]. The robust and fast behavior of the proposed system in the synchronization as well as in the encryption/decryption process makes it suitable and compatible to operate with high speed real time transmission wireless communication systems especially with OFDM modulation based systems [27].

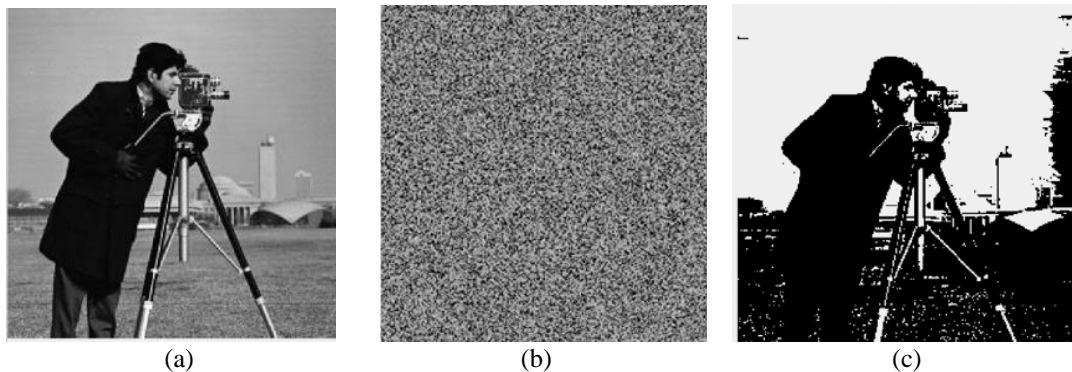


Figure 9. Grayscale image: (a) is the plain image, (b) is the encrypted message, (c) is the recovered image

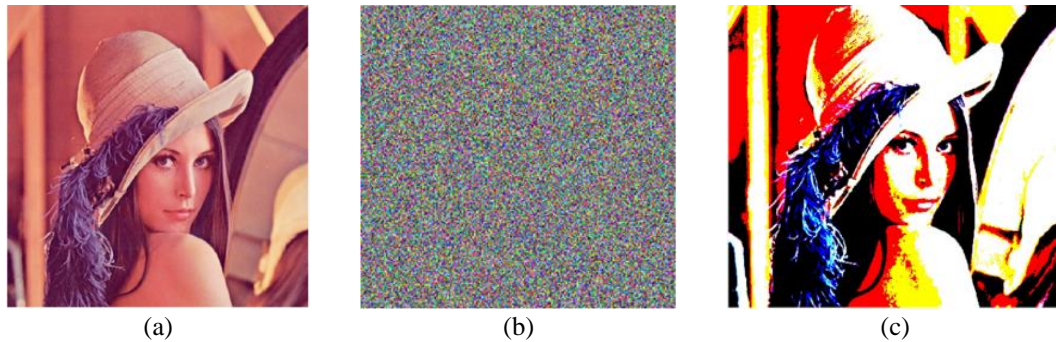


Figure 10. Color image: (a) is the plain image, (b) is the encrypted message, (c) is the recovered image

#### 4. CONCLUSION

This paper presents the design and simulation of a hyperchaotic 4D Lorenz system generator. The designed generator has been adopted for designing a secure communication system for real time applications. The synchronization between the transmitter and receiver has been achieved by using new dynamic feedback techniques based on an error calculation between the master and slave subsystem. The designed system achieves a high level of security for image encryption for color and grayscale images. The system shows a high transmission security with fast performance, and this proof that hyperchaotic systems are perfect candidates for new cryptography systems in the next communication systems. The proposed hyperchaotic based cryptosystem shows that, it is suitable for ciphering the plain image and deciphering the ciphered images, especially of the size  $128 \times 128$  pixels with less than 0.1 second of time, the results also show that there are some distorted pixels for both image types and this distortion is due to the high level of channel noise. Which makes it suitable for real time applications and in particular for wireless sensor network applications.

#### ACKNOWLEDGEMENTS

The authors wish to thank the educational family in the Electrical Engineering Department in the College of Engineering at University of Babylon for their support to complete this research paper.

#### REFERENCES




- [1] M. A. Albreem, M. Juntti and S. Shahabuddin, "Massive MIMO detection techniques: a survey," in *IEEE Communications Surveys and Tutorials*, vol. 21, no. 4, pp. 3109-3132, Fourthquarter 2019, doi: 10.1109/COMST.2019.2935810.
- [2] Q. Lai, X. W. Zhao, K. Rajagopal, G. Xu, A. Akgul, and E. Guleryuz, "Dynamic analyses, FPGA implementation and engineering applications of multi-butterfly chaotic attractors generated from generalised Sprott C system," *Pramana – Journal of Physics*, vol. 90, no. 1, pp. 1-12, 2018, doi: 10.1007/s12043-017-1493-x.
- [3] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 8, pp. 2129-2151, 2006, doi: 10.1142/S0218127406015970.
- [4] J. Zambreno, D. Nguyen, and A. Choudhary, "Exploring area/delay tradeoffs in an AES FPGA implementation," *International Conference on Field Programmable Logic and Applications*, vol. 3203, pp. 575-585, 2004, doi: 10.1007/978-3-540-30117-2\_59.
- [5] X. Yi, C. H. Tan, C. K. Slew and M. R. Syed, "Fast encryption for multimedia," in *IEEE Transactions on Consumer Electronics*, vol. 47, no. 1, pp. 101-107, Feb. 2001, doi: 10.1109/30.920426.
- [6] R. B. Gandara, G. Wang and D. N. Utama, "Hybrid cryptography on wireless sensor network: a systematic literature review," *2018 International Conference on Information Management and Technology (ICIMTech)*, 2018, pp. 241-245, doi: 10.1109/ICIMTech.2018.8528147.
- [7] W. D. Chang, "Digital secure communication via chaotic systems," *Digital Signal Processing*, vol. 19, no. 4, pp. 693-699, 2009, doi: 10.1016/j.dsp.2008.03.004.
- [8] M. G. Bosque, A. P. Resa, C. S. Azqueta, C. Aldea and S. Celma, "A new technique for improving the security of chaos-based cryptosystems," *2018 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2018, pp. 1-5, doi: 10.1109/ISCAS.2018.8351195.
- [9] K. M. Cuomo, A. V. Oppenheim and S. H. Strogatz, "Synchronization of Lorenz-based chaotic circuits with applications to communications," in *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 40, no. 10, pp. 626-633, Oct. 1993, doi: 10.1109/82.246163.
- [10] H. Dedieu, M. P. Kennedy and M. Hasler, "Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits," in *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 40, no. 10, pp. 634-642, Oct. 1993, doi: 10.1109/82.246164.
- [11] P. Prakash *et al.*, "A novel simple 4-D hyperchaotic system with a Saddle-Point Index-2 Equilibrium point and multistability: design and FPGA-based applications," *Circuits, Systems, and Signal Processing*, vol. 39, pp. 4259-4280, 2020, doi: 10.1007/s00034-020-01367-0.
- [12] Z. Hu and C. Chan, "A 7-D hyperchaotic system-based encryption scheme for secure fast-OFDM-PON," *Journal of Lightwave Technology*, vol. 36, no. 16, pp. 3373-3381, 15 Aug.15, 2018, doi: 10.1109/JLT.2018.2841042.






- [13] J. Zhang, "An image encryption scheme based on cat map and hyperchaotic Lorenz system," *2015 IEEE International Conference on Computational Intelligence and Communication Technology*, 2015, pp. 78-82, doi: 10.1109/CICT.2015.134.
- [14] E. E. Mahmoud, M. Higazy, and T. M. Al-Harathi, "A new nine-dimensional chaotic Lorenz system with quaternion variables: Complicated dynamics, electronic circuit design, anti-anticipating synchronization, and chaotic masking communication application," *Mathematics*, vol. 7, no. 10, 2019, doi: 10.3390/math7100877.
- [15] T. M. Hoang, "A chaos-based image cryptosystem using nonstationary dynamics of logistic map," *International Conference on Information and Communication Technology Convergence (ICTC)*, 2019, pp. 591-596, doi: 10.1109/ICTC46691.2019.8939826.
- [16] M. A. Al-Khasawneh, S. M. Shamsuddin, S. Hasan and A. A. Bakar, "An improved chaotic image encryption algorithm," *Int. Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, 2018, pp. 1-8, doi: 10.1109/ICSCEE.2018.8538373.
- [17] J. Zhu, D. Zhang, and C. Yu, "Eight dimension seven-order hyperchaotic system and its circuit implementation," *Proceedings of 2013 2nd Int. Conference on Measurement, Information and Control*, 2013, pp. 950-954, doi: 10.1109/MIC.2013.6758116.
- [18] R. Barboza, "Dynamics of a hyperchaotic Lorenz system," *International Journal of Bifurcation and Chaos*, vol. 17, no. 12, pp. 4285-4294, 2007, doi: 10.1142/S0218127407019950.
- [19] V. Milanović and M. E. Zaghoul, "Improved masking algorithm for chaotic communications systems," *Electronic Letters*, vol. 32, no. 1, pp. 11-12, 1996, doi: 10.1049/el:19960004.
- [20] J. H. Park, "Chaos synchronization between two different chaotic dynamical systems," *Chaos, Solitons and Fractals*, vol. 27, no. 2, pp. 549-554, 2006, doi: 10.1016/j.chaos.2005.03.049.
- [21] M. Eisencraft and A. M. Batista, "Discrete-time chaotic systems synchronization performance under additive noise," *Signal Processing*, vol. 91, no. 8, pp. 2127-2131, 2011, doi: 10.1016/j.sigpro.2011.01.021.
- [22] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Physical Review Letters*, vol. 64, no. 8, pp. 821-824, Mar. 1990, doi: 10.1063/1.4917383.
- [23] E. W. Bai and K. E. Lonngren, "Sequential synchronization of two Lorenz systems using active control," *Chaos, Solitons and Fractals*, vol. 11, no. 7, pp. 1041-1044, 2000, doi: 10.1016/S0960-0779(98)00328-2.
- [24] O. A. Gonzales, G. Han, J. P. de Gyvez and E. Sanchez-Sinencio, "Lorenz-based chaotic cryptosystem: A monolithic implementation," in *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 47, no. 8, pp. 1243-1247, Aug. 2000, doi: 10.1109/81.873879.
- [25] Li Chuanmu and H. Lianxi, "A new image encryption scheme based on hyperchaotic sequences," *2007 International Workshop on Anti-Counterfeiting, Security and Identification (ASID)*, 2007, pp. 237-240, doi: 10.1109/IWASID.2007.373734.
- [26] S. Sadoudi, C. Tanougast, M. S. Azzaz, and A. Dandache, "Design and FPGA implementation of a wireless hyperchaotic communication system for secure real-time image transmission," *EURASIP Journal on Image and Video Processing*, vol. 2013, pp. 1-18, 2013, doi: 10.1186/1687-5281-2013-43.
- [27] H. Alibraheemi and M. Al Ibraheemi, "Wireless communication system with frequency selective channel OFDM modulation technique," *TELKOMNIKA Telecommunication, Computing, Electronics and Control*, vol. 18, no. 3, pp. 1206-1211, 2020, doi: 10.12928/TELKOMNIKA.v18i3.14683.

## BIOGRAPHIES OF AUTHORS






**Hayder Mazin Makki Alibraheemi**    was born in Iraq in 1989. He received B.Sc. degree in communication engineering from a technical engineering college in 2011. He got the Ms degree in electronic and communication engineering in 2013 from Eastern Mediterranean University in Cyprus. The research topic was around the multiband antenna and the fractal behavior of these structures. Nowadays he is too interested in networking security, cryptography steganography, and studying the mechanisms to prevent information hacking. He can be contacted at email: hayder.makki.engh278@student.uobabylon.edu.iq.



**Qais Al-Gayem**    received the B.S. degree in Electrical and Electronic Engineering from the University of Babylon, and the M.S. degree in Electronic Engineering from the University of Technology, Iraq, in 1999 and 2001, respectively. Between 2002 and 2008, he worked as a lecturer in the Electrical Department, University of Babylon, Iraq. Following this, he studies for his PhD. in the Engineering Department, Lancaster University, UK, and graduated in 2012. He is currently an associate professor in the Electronic and Electrical Department, Faculty of Engineering, University of Babylon, Iraq. His research interests include built-in-self-test (BIST) of MEMS and NEMS, health monitoring, and dependability in Bio-fluidic microsystems. He can be contacted at email: eng.qais.karem@uobabylon.edu.iq.



**Ehab AbdulRazzaq Hussein**    has Ph.D. M.Sc. In Electrical Engineering, he was born in Babylon on January 1, 1976. He obtained his B.Sc. degree in (1997) in Electrical Engineering at the Faculty of Engineering, University of Babylon and the M.Sc. degree in (2000), in electrical engineering at the Department of Electrical Engineering, University of Technology and his PhD. Degree from the Department of Electrical Engineering at the Faculty of Engineering, University of Basrah. He currently works as a professor at the Electrical Department-Faculty of Engineering, University of Babylon. His main interest is signal processing, analysis, information transition, sensors, and control system. He can be contacted at email: dr.ehab@uobabylon.edu.iq.