International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 14, No.1 (Aug-2023)

http://dx.doi.org/10.12785/ijcds/140136

Secure Image Transmission Through Differential Chaos Shift Keying Communication System

Yasmine M. Khazaal[1], **Yassine Aydi**[1] **and Mohamed Abid**[1]

[1]*CES Laboratory, National Engineering School of Sfax, Sfax, Tunisia*

Received 01 Sep. 2022, Revised 05 Jul. 2023, Accepted 09 Jul. 2023, Published 01 Aug. 2023

Abstract: In this paper, we investigate Chaos-based communication systems in the context of secure image transmission. The proposed model combined the secure image transmission process with non-coherent chaos communication system over multipath fading channel. Security of image signal is required to be transmitted reliably through a communication channel or when information is managed by computing units. Security issues are becoming problematic in multimedia applications and network systems. Thus, providing a secure transmission of data is an important theme tackled by researchers. The pace at which data is sent is an important consideration. Wireless communications are dominated by coherent communications at this time. To decode received data, such systems need exact knowledge of the receiver's channel condition. In chaotic communication systems, noncoherent detection, which doesn't need a lot of complicated the synchronization of the transmitter and receiver, perhaps an interesting alternative. The proposed system is evaluated through measures such as complexity, data throughput, and security. In order to take use of chaotic signals and noncoherent detection while avoiding chaotic synchronization, which performs poorly in the presence of additive noise, non-coherent chaos systems have attracted a lot of attention. The results presented in this research disclose new ideas related to the design of a new non-coherent differential chaos shift keying communication system.

Keywords: Image encryption, Chaos, Differential chaos shift keying (DCSK).

1. INTRODUCTION

The exponential evolution of internet of things (IoT) technologies and massive communication networks has led to a big growth of amount data generated by applications. Security issues regarding computing and transmission of data through communication platforms became more critical and costly. So, efficient and spread spectrum Chaos communication system is an important and relevant alternative over the two past decades. Chaotic signals have reconfigurable features [1], [2]. Also, they present a good correlation property, as well as a flexibility generation. So, they are proposed as a potential alternative for robust and secure communications over multi-path fading channels (MF) [3].The growing importance of data security is reflected in the variety of research methods that depict digital image encryption. In [4] chaos-based image cryptosystem in the spatial domain involving confusion and diffusion processes, providing secure transmission for images through networks. Chaos-based image encryption is a novel approach to image encryption that uses a random chaos sequence to solve the difficult problems of providing high security without sacrificing speed. Researches are increasingly interested about this data's security. Image-based encryption is more secure than text-based [5].

Communication system security must be upgraded. Several studies and investigations have examined. Images are less secure with traditional text encryption. New communication system security measures are needed. Physical layer security improves wireless device connectivity. Physical layer protection techniques enhance higher-layer security procedures. Physical layer security includes key generation and encryption. Chaos-based wireless communication systems may be categorized by coherent and non-coherent receiver detection. The coherent system at the receiver needs complete Channel Status Information (CSI) and an exact copy of the chaotic carrier to reduplicate information. These estimate strategies increase receiver complexity and overhead signaling, making chaotic coherent detection in a rapidly fading channel impractical. Chaos-based coherent communication systems suffer from channel estimation problems. This system's major issue is degradation. Non-coherent detections don't need synchronized transmitter and receiver [1]. Image encryption converts the original image into a difficult-to-understand form, enhancing resistance against brute force, statistical, and differential assaults. Medical imaging, telemedicine, commerce, biometric ID, and military communication employ image encryption. Several picture encryption techniques, including digital watermarking, image scrambling, image steganography, and

E-mail address: yasminemustafa95@yahoo.com, yassine.aydi@enis.tn, Mohamed.abid@enis.tn

image cryptography, have been suggested to solve these security concerns. Exploiting chaos in cryptography has gained popularity in recent decades owing to its essential trait of sensitivity to beginning circumstances, resulting in data sets that, although deterministic, look random. Chaos-based cryptographic models have been utilized to create unique ways for designing efficient picture encryption systems that display excellent performance in various areas such as speed, cost, processing power, computational overhead, complexity, vulnerability, and so on.

The contribution of this paper can be summarized as:

1) Image encryption using stream cipher system is combined with DCSK system and transmitted through MF channel.
2) Pseudo random bit generator (PRBG) is designed using logistic map.
3) The performance analysis of the security is investigated using PSNR, histogram, and correlation function, information entropy, key space analysis, and differential attack analysis.
4) The simulation results are compared with recent works.

The reset of the paper can be summarized as: related work is presented in section 2. Section 3 contains the chaos theory. DCSK communication system is presented in section 4. PRBG based on logistic map is presented in section 5. DCSK based image encryption framework is studied in section 6. Section 7 contains simulation results. The security analysis is investigated in section 8. Finally, the conclusion is depicted in section 9.

2. RELATED WORK

Differential chaos shift keying (DCSK) was proposed by Kolumbán et al. [2] as the first noncoherent chaos-based digital communication approach. This technique is known as DCSK, which uses a binary symbol to modulate a chaotic signal. A chaotic signal is associated with a chaotic signal at the receiver. Based on the sign of the correlator outputs [3], [4], [5], [6], [7], the binary symbol is then decoded. It has been suggested by Hasler and Schimming [8] to use a noncoherent detection approach that can be used to the CSK modulation scheme [8], [9], [10], [11]. By picking the symbol with the lowest a posteriori probability, an optimum classifier is used to maximize the bit error rate (BER). Lau and Tse [12] investigate the classifier's computational complexity further and give an approximation of the ideal detection strategy [13]. There is a third noncoherent detector for CSK that was disclosed by Tse etal. There are two main parts to this system: a regression method and a way to figure out where the chaotic signals return. These two parts are the foundation for the detection principles that will be used. A variety of DCSK-based variants have been developed to augment the DCSK method in addition to the aforementioned fundamental noncoherent detection systems. It has been suggested that frequency-modulated DCSK (FM-DCSK) may be used to address the issue of fluctuating bit-energy in DCSK. An FM modulation of a sinusoidal carrier is created instead of a modulation of a DCSK modulator, which produces a chaotic FM signal. The FM-DCSK modulator produces a steady-state FM-DCSK output, which means it has the same power and energy per bit time as the chaotic FM signal. This is done by modulating the chaotic FM signal. Quadrature CSK (QCSK), which is a multilayer DCSK, has been looked at by Galias and Maggio [14]. People can send more data through QCSK, which generates chaotic functions that are orthogonal to each other, than through DCSK, which only takes up the same amount of bandwidth. It's easy to figure out the bit rate of a DCSK system because the reference and information-bearing chaotic samples look a lot alike. If we want to keep the signal from being picked up by the wrong people, this may not be the best option. There is no correlation between the reference and information-bearing samples when utilizing a permutation-based DCSK (P-DCSK) approach [15], [16], [17], [18]. The bit rate can no longer be detected in the frequency spectrum, strengthening the security of the data. The CDSK system, like the DCSK technique, incorporates a reference chaotic signal into the broadcast signal [19]. In CDSK, the reference and information-carrying signals are joined with a temporal delay, as opposed to a rapid addition in DCSK. Each communicated signal sample comprises a reference sample and an information-bearing sample. The bandwidth efficiency is increased since no single reference signal is delivered. CDSK also enables the transmitter to operate continuously since it eliminates the requirement for a switch in the DCSK system to transition between the information-bearing signal and the chaotic reference signal. The signal is more homogeneous since it is less likely to be intercepted. Because two chaotic signals are delivered, there is increased uncertainty (interference) when the received signal resembles the delayed version. This is due to the transmission of two chaotic signals. As a result, CDSK is inferior to DCSK. That improve the system performance that show in [20], designed a novel correlation receiver with nonlinearity blanking considered the fundamental and studied non-coherent DCSK system under the pulse jamming environment.

As in traditional DCSK, a new multi-user multi-level non-coherent scheme has been proposed and analyzed for chaos-based communication Systems in [21], and this scheme uses time-multiplexing to separate reference and data-bearing sequences. The messages are iteratively exchanged between the detector and the decoder in [22]. Indeed, the demodulation of system takes into consideration both characteristics of chaotic modulation and transmission to enhance the received SNR. Modern communication systems demand data transfer at a greater rate and with a wider bandwidth to accommodate multimedia transmission. Existing modulation methods cannot offer a full answer. The writers of this article tried to outline existing modulation approaches to assess what tweaks or revisions may address the issue or whether a new technique is still needed to fulfill current communication system needs.

3. CHAOS THEORY

Uncertainty and sensitivity to starting circumstances are the hallmarks of chaotic dynamical systems [16]. Chaos and noise are both unexpected. Which is why they are often compared. Due to their pseudorandom, unpredictable, and sensitive properties, chaotic systems may be used in cryptography [17]. Due of their seeming unpredictability and their sensitivity to the beginning circumstances, chaotic systems are effective for encryption [17]. This randomness may be hard to predict because of how sensitive it is to the start.

Two kinds of chaos-based communication systems exist:

- Coherent System: consistent synchronization between transmitter and receiver chaotic systems is critical for coherent detection, since it needs synchronized copies of chaotic signals to be available at the receiver. Coherent detection in low signal-to-noise (SNR) settings has been demonstrated to have substantial difficulties due to the applied chaotic synchronization strategy to the communication system Systems with long coherence times are difficult to implement in fast-fading environments. Due to excessive pilot broadcasts on slow-fading channels, the transmitter will repeatedly send pilot symbols, squandering resources. Coherent communication suffers greatly from channel estimate errors, and this deterioration is exacerbated under conditions of high mobility [18], [19], [20], [21], [22], [23].
- Non- Coherent System: These methods do not need the receiver to regenerate any local chaotic signal, which are based on chaos and use non-coherent detection to recover data by recognizing aspects of the received signal [24], [25], [26].

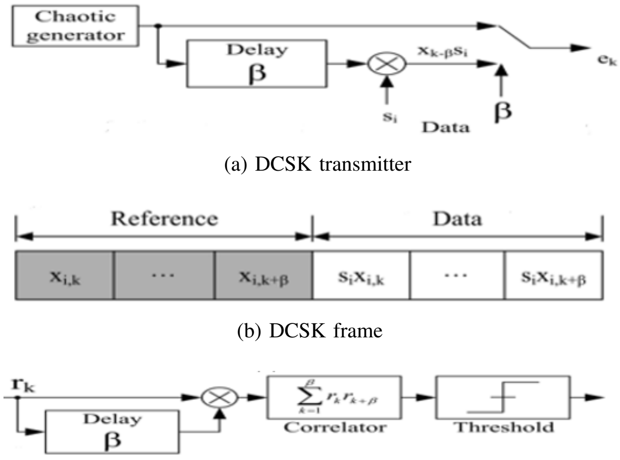
Chaotic communications with coherent receivers have significant demodulation challenges due to the poor performance of certain chaotic synchronization models in noisy settings [24], [25], [26], [27]. DCSK system don't need chaotic signal creation and synchronization in order to get the data that was sent to them [24], [25], [26], [27]. Many new ideas for non-coherent chaos-based communication systems are coming up because of this big advantage. This has led to a lot more research in this field. Therefore, we will complete the remainder of the paper, talking about the non coherent technologies, how they can be used, and how they can be categorized and performance measured.

4. DCSK COMMUNICATION SYSTEM

This is because the modulator's bits are represented by two sets of chaotic signal samples, +1 for reference and -1 for data in Fig. 1. So, if +1 is sent, the data-bearing sequence is identical to the reference sequence, and vice versa. Let 2β the spreading factor, defined as the number of chaotic samples supplied each bit. The transmitter $s_{i,k}$ output is as (1):

$$s_{i,k} = \begin{cases} x_{i,k}, & for\ 1 < k \leq \beta \\ b_i x_{i,k-\beta}, & for\ \beta < k \leq 2\beta \end{cases} \tag{1}$$

The reference sequence is xk, while the delayed version is $x_{k-\beta}$. A half-bit duration T_c (where $T_b = 2\beta T_c$ and T_c = the chip time) is added to the received signal rk to demodulate the sent bits. The received bits may be approximated by subtracting the correlator's output (i.e. see Fig. 1c the DCSK receiver). This study's time chip is one ($T_c = 1$), and in Figure 2 show the model of two-ray Rayleigh fading channel.



(a) DCSK transmitter

(b) DCSK frame

(c) DCSK receiver units.

Figure 1. DCSK communication system block diagram.

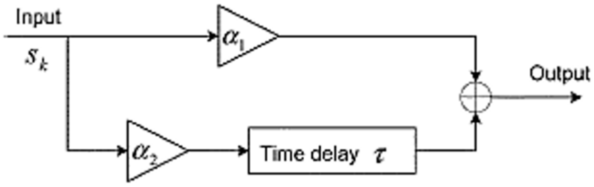


Figure 2. Two-ray Rayleigh fading channel model [28].

The channel's output, expressed in terms of the discrete-time baseband equivalent model, looks like this in (2):

$$output = \alpha_1 s_k + \alpha_2 s_{k-T} \tag{2}$$

Given two random variables independent and Rayleigh distributed are α_1 and α_2, a time lag between them is τ, and scattering function s_{k-T} we get in the following

$$s_{k-T} = \begin{cases} b_{l-1} x_{k-\beta-\tau}, & k = 2\,(l-1)\beta + 1, \ldots, 2(l-1)\beta + \tau \\ x_{k-\tau}, & k = 2\,(l-1)\beta + \tau + 1, \ldots, (2l-1) \\ x_{k-\tau}, & k = (2l-1)\beta + 1, \ldots, (2l-1)\beta + \tau \\ b_l x_{k-\beta-\tau}, & k = (2l-1)\beta + \tau + 1, \ldots, 2l\beta. \end{cases}$$

For the receiver's signal (the correlator's input), we have (3):

$$r_k = \alpha_1 s_k + \alpha_2 s_{k-T} + \varepsilon_k, \; k = 0, 2, \ldots, 2\beta - 1 \tag{3}$$

With mean equal to zero in AWGN is ε_k and $\frac{N_0}{2}$ is variance. When thinking about the lth symbol, the output of the correlate is the choice variable, which is provided by (4):

$$\begin{aligned} z_l = & \sum_{k=(2l-1)\beta+1}^{(2l-1)\beta+\tau} (\alpha_1 b_l x_{k-\beta} + \alpha_2 x_{k-T} + \varepsilon_k) \\ & \times (\alpha_1 x_{k-\beta} + \alpha_2 b_{l-1} x_{k-2\beta-\tau} + \varepsilon_{k-\beta}) \\ & + \sum_{k=(2l-1)\beta+\tau+1}^{2l\beta} \left(\alpha_1 b_l x_{k-\beta} + \alpha_2 b_l x_{k-\beta-\tau} + \varepsilon_k\right) \\ & \times \left(\alpha_1 x_{k-\beta} + \alpha_2 x_{k-\beta-\tau} + \varepsilon_{k-\beta}\right). \end{aligned} \tag{4}$$

Then, the lth decoded symbol is determined according to the following rule (5):

$$\widetilde{b_l} = \begin{cases} +1, & if \; z_l \geq 0 \\ -1, & if \; z_l < 0. \end{cases} \tag{5}$$

If the logistic map is used, the conditional BER may be simplified as (6):

$$BER\,(\alpha_1, \alpha_2) = \frac{1}{2} erfc\Big((\frac{4}{\gamma_b} + \frac{2\beta}{\gamma_b^2})^{-\frac{1}{2}} \Big) \tag{6}$$

Where $\gamma_b = ({}^{E_b}/_{N_0}) \left(\alpha_1^2 + \alpha_2^2\right) = \gamma_1 + \gamma_2, \gamma_1 = ({}^{E_b}/_{N_0}) \left(\alpha_1^2\right)$, and $\gamma_2 = ({}^{E_b}/_{N_0}) \left(\alpha_2^2\right)$. Denoting $\bar{\gamma_1} = E\{\gamma_1\} = ({}^{E_b}/_{N_0})\, E\{\alpha_1^2\}$. and $\bar{\gamma_2} = E\,\{\gamma_2\} = ({}^{E_b}/_{N_0})\, E\left\{\alpha_2^2\right\}$, in MF channel the probability density function of γ_b becomes in (7):

$$\widetilde{b_l} = \begin{cases} \frac{\gamma_b}{\bar{\gamma}_1^2} e^{-{}^{\gamma_b}/_{\bar{\gamma}_1}}, & E\left\{\alpha_1^2\right\} = E\alpha_2^2 \\ \frac{1}{\bar{\gamma}_1 - \bar{\gamma}_2} \left(e^{-{}^{\gamma_b}/_{\bar{\gamma}_1}} - e^{-{}^{\gamma_b}/_{\bar{\gamma}_2}}\right), & E\left\{\alpha_1^2\right\} \neq E\left\{\alpha_2^2\right\}. \end{cases} \tag{7}$$

As a last step, we may derive the BER in the MF channel by averaging the conditional BER, which is defined as (8):

$$BER_{MF} = \int_0^{\infty} BER\,(\gamma_B)\, f\,(\gamma_b)\, d\,(\gamma_b) \tag{8}$$

In AWGN channel the $\gamma_b = ({}^{E_b}/_{N_0})$is obtained by setting α_1 and α_2 to get BER in (9):

$$BER_{AWGN} = \frac{1}{2} erfc\left(\left(\frac{4}{{}^{E_b}/_{N_0}} + \frac{2\beta}{{}^{E_b}/_{N_0}{}^2} \right)^{-\frac{1}{2}} \right) \tag{9}$$

In the next sections, we'll use these formulas to assess the system's resilience to bit-errors over a range of channel qualities.

5. PSEUDO RANDOM BIT GENERATOR (PRBG) BASED ON LOGESTIC MAP

Logistic maps are a common mathematical model for describing the expansion of biological populations. [29] Shown that the seemingly straightforward behavior of this model is really rather complicated. In later years, researchers [30], [31] documented some of the quantitative universals that have come to define modern chaos research. Due to its ease of mathematical representation, this model has served as a proving ground for several developments in chaos theory and cryptographic applications [32]. In Equation (10) we see the simplified mathematical version of the modified logistic map:

$$X_{n+1} = \lambda X_n \,(1 - X_n) \tag{10}$$

Where X_n is a state variable, which lies in the interval [0, 1] and λ is called system parameter. To generate a seemingly length of random binary sequence that $l >> k$, a PRBG takes as input a genuinely random binary sequence of length k (the seed) and as output a binary sequence of length $l >> k$ (the faux random sequence). The PRBG's output is not completely random since the number of output sequences is bounded by the integers $({}^{2^k}/_{2^l})$, which is a tiny number compared to the total number of potential binary sequences of length l. The objective is to multiply a short, really random sequence of length k by a factor that makes it hard for an opponent to detect the difference between the PRBG sequence and a truly random sequence of length l [33]. In Fig. 3, we can see a simplified block diagram of the PRBG.

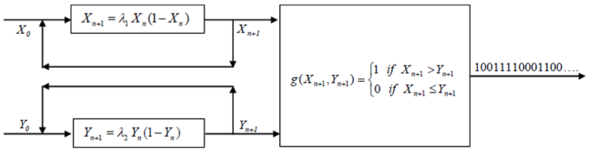

X_0
$X_{n+1} = \lambda_1 X_n (1 - X_n)$
X_{n+1}
Y_0
$Y_{n+1} = \lambda_2 Y_n (1 - Y_n)$
Y_{n+1}
$g(X_{n+1}, Y_{n+1}) = \begin{cases} 1 & if \; X_{n+1} > Y_{n+1} \\ 0 & if \; X_{n+1} \leq Y_{n+1} \end{cases}$
10011110001100....

Figure 3. Schematic block diagram of PRBG.

6. DCSK BASED IMAGE ENCRYPTION FRAMEWORK

The proposed system combined the secure image transmission with non-coherent chaos communication system over MF and AWGN channels. Fig. 4 shows the general idea of the proposal system. In the first the color image $A^{N \times M \times 3}$, where N and M is the size of image, is converted to stream bits using Decimal to Binary (D2B)) converter, $B^{1 \times 8MN} = \{b_1, \; b_2, \ldots, b_{8MN}\}$, where $b_j \in 0, 1, j = 1, 2, \ldots, 8M$. After that, the binary message is encrypted using the PRBG key generated by chaotic map according to in (11):

$$c_j = b_j \oplus k_j, \;\; j = 1, 2, \ldots, 8MN \tag{11}$$

where c_j is the j-th stream bits of the ciphered message. k_j is the PRBG that is generated in section 5. The operator ⊕ is the XOR function. The ciphered bits are then modulated by DCSK system according to Equation (1) and send through MF and AWGN according to Equation (3). At the receiver, the received signal, $r_k, k = 0,..,2\beta - 1$ is passing through DCSK demodulation to recover the encrypted detected bits $\widetilde{c}_j,\ j = 1, 2, \ldots, 8MN$ and then the original detected bits is obtained by (12):

$$\widetilde{b}_j = \widetilde{c}_j \oplus k_j,\ \ j = 1, 2, \ldots, 8MN \qquad (12)$$

where k_j is the identical PRBG generated in synchronized with PRBG at transmitter side. Finally the binary to decimal converter and reshaping function are used to recover the decrypted color image.

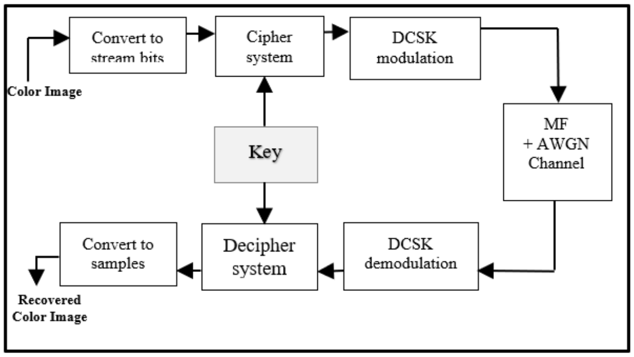


Figure 4. The DCSK based image encryption.

7. SIMULATION RESULTS

In this section that explain the BER and PSNR in various value of SNR under AWGN and MF channel, although the two pathways' average power gains are the same in this simulation, the second path's average power increase is 3 dB lower than the first. In this situation, the mean powers of the two directions add up to (13):

$$E\left\{(\alpha_1)^2\right\} = \frac{2}{3} \text{ and } E\left\{(\alpha_2)^2\right\} = \frac{1}{3} \qquad (13)$$

The PSNR measure is expressed as [36]:

$$PSNR = 10\ log_{10} \frac{255^2}{\frac{1}{NM}\sum_{n=0}^{M}\sum_{m=1}^{N}\left[x(n,m) - y(n,m)\right]^2} \qquad (14)$$

where x and y are the original and recovered image, respectively. N and M are the row and column dimension of the image.

Figs (5,6) show ,respectively; In these figures, the correct key at receiver is used to recover the original image, it can be seen that the BER performance for the secure proposed system is matching with BER theory and no degradation is occurred. Also, increased SNR will enhance the performance of PSNR and hence recovered the clear image. Increase β will degrade the performance of the system. Furthermore, more SNR needed to reach BER approach 10-3 for MF comparing with AWGN.

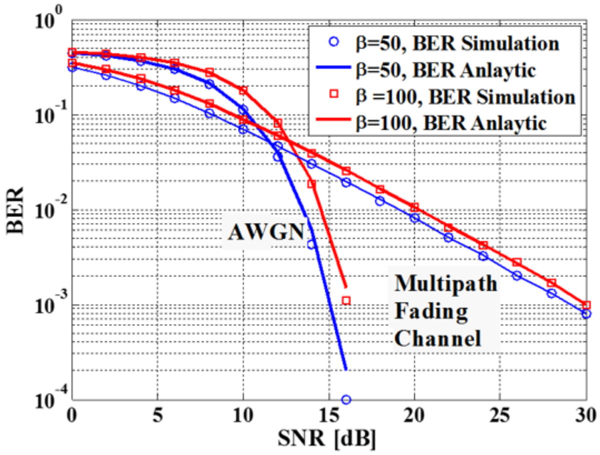


Figure 5. BER comparisons for various value of β under AWGN and Multipath fading channel.

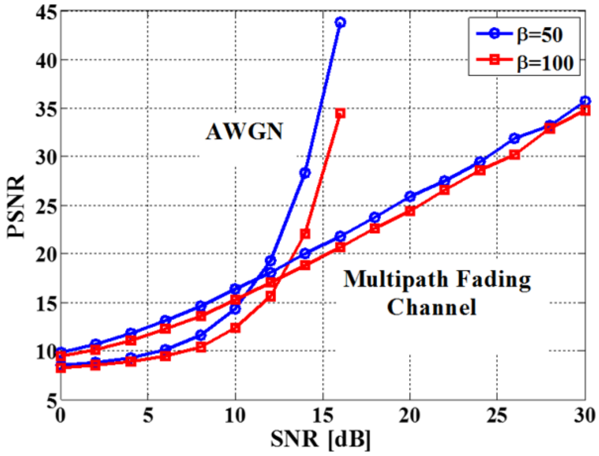


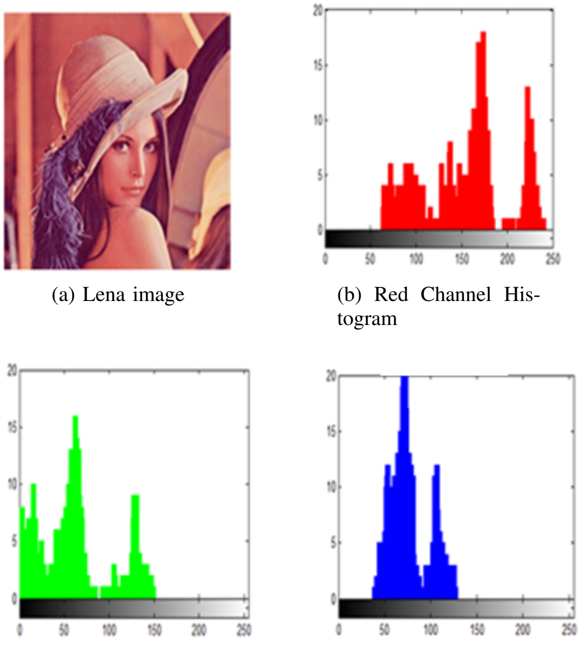
Figure 6. PSNR comparisons for various value of β under AWGN and Multipath fading channel.

8. SECURITY ANALYSIS

One way to assess the quality of an encryption method is by how well it defends against all known threats. Analysis of the histogram, information entropy, the correlation coefficient, NPCR, and UACI, key space analysis, will be used to evaluate the safety of the proposed technique.

A. Analysis of the histogram

The histogram shows how evenly spaced each pixel value is. When looking at a basic image, you may notice that certain pixels appear more often than others. It's valuable enough to warrant manipulation. The cipher image must be dispersed such that an attack on the cipher image is minimized, allowing the encryption system to withstand assaults. In Fig.7 (a) showed the original colored image Lena image with size 256×256, and Figs. 7(b), (c) and (d) respectively with histogram of the red, green, and blue channels, while Fig. 8(a) shows a Lena ciphered image using proposed system. Figs. 8 (b), (c) and (d) showed the histogram of the three RGB chains, that consistently provide high-quality histograms. We can see that the encrypted image has uniform histogram which means that the distribution of the pixel are identical and the security is established.



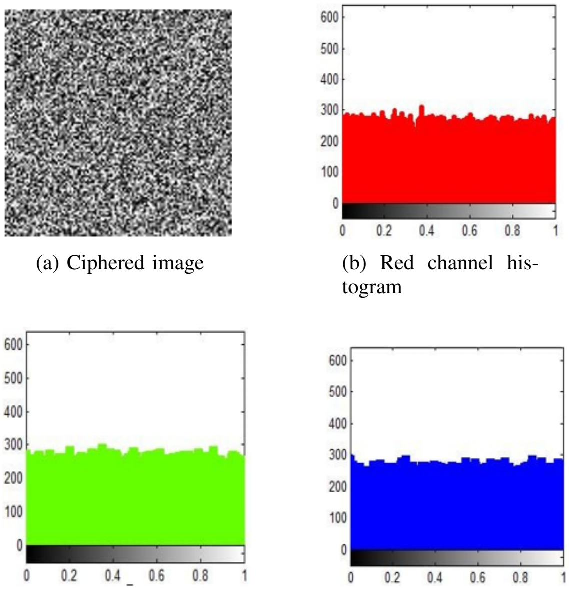
(a) Lena image

(b) Red Channel Histogram

(c) Green Channel Histogram.

(d) Blue Channel Histogram

Figure 7. Original image.



(a) Ciphered image

(b) Red channel histogram

(c) Green channel histogram.

(d) Blue channel histogram

Figure 8. Image Encryption.

B. *Correlation Coefficient Analysis*

The examination of the correlation coefficient provides the greatest statistical insight into the encrypted picture. The association between two pixels in the plain picture and encrypted images is examined. If the encrypted picture is fully random and substantially uncorrelated with the original, then the image encryption technique may be considered successful. Images are distinct if the coefficient of similarity is less than 1, else they are mirror images with a degree of similarity of 1. Furthermore, the encryption is useless here. The meaning = -1 of the encrypted picture is completely at odds with the meaning of the transparent image. To determine the correlation coefficient between two pixels of the same location in the original and cipher pictures [34], we assess the pixel correlation in horizontal, vertical, and diagonal directions (using (15-18)).

$$CorCoef = \frac{Covar(x, y)}{\sqrt{Vari\,(x)} \times \sqrt{Vari(y)}} \tag{15}$$

$$Vari\,(x) = \frac{1}{N}\sum_{i=1}^{N}\left[(x_i - E\,(x)\right)^2 \tag{16}$$

$$Vari\,(y) = \frac{1}{N}\sum_{i=1}^{N}\left[(y_i - E\,(y))^2\right] \tag{17}$$

$$Covar\,(x, y) = \frac{1}{N}\sum_{i=1}^{N}\left[(x_i - E\,(x)) \times (y_i - E\,(y))\right] \tag{18}$$

The coefficient of correlation between x and y is $CorCef$, the original image variance of x is represents $asVari(x)$, the original image variance of y is represents $asVari(y)$, $Covar(x, y)$ is the original image variance of x and y, predicted is $E(x)$, and the total number of pixels in the image matrix is N.

Table I and Table II for different images with a scale of 256×256, different β, and (SNR=5), Table III show the ciphered Lena image with size 512×512 and compare the correlation coefficient analysis between our proposed and other traditional systems are [35], and [36].

TABLE I. CORRELATION COEFFICIENT OF THE PROPOSED SCHEME WHERE B=50, SNR=5.

Image	Channels		Ours	
house	Red	Horizontal	Basic	0.9666
			Encrypted	-0.0022
		Vertical	Basic	0.7816
			Encrypted	0.0298
		Diagonal	Basic	0.9305
			Encrypted	0.0028
	Green	Horizontal	Basic	0.9502
			Encrypted	-0.0562
		Vertical	Basic	0.9069
			Encrypted	0.0684
		Diagonal	Basic	0.9674
			Encrypted	0.0844
	Blue	Horizontal	Basic	0.9289
			Encrypted	0.0195
		Vertical	Basic	0.9408
			Encrypted	-0.0370
		Diagonal	Basic	0.9747
			Encrypted	-0.0484
baboon	Red	Horizontal	Basic	0.5753
			Encrypted	-0.0083
		Vertical	Basic	0.9479
			Encrypted	-0.0042
		Diagonal	Basic	0.9183
			Encrypted	-0.0769
	Green	Horizontal	Basic	0.5336
			Encrypted	0.0327
		Vertical	Basic	0.9267
			Encrypted	0.0521
		Diagonal	Basic	0.8610
			Encrypted	0.0743
	Blue	Horizontal	Basic	0.7484
			Encrypted	-0.0607
		Vertical	Basic	0.9169
			Encrypted	0.0591
		Diagonal	Basic	0.9380
			Encrypted	-0.0502
lena	Red	Horizontal	Basic	0.9067
			Encrypted	-0.0225
		Vertical	Basic	0.9846
			Encrypted	0.0089
		Diagonal	Basic	0.8660
			Encrypted	0.0819
	Green	Horizontal	Basic	0.9434
			Encrypted	0.0034
		Vertical	Basic	0.9785
			Encrypted	0.0267
		Diagonal	Basic	0.8568
			Encrypted	-0.0289
	Blue	Horizontal	Basic	0.8629
			Encrypted	-0.0154
		Vertical	Basic	0.9286
			Encrypted	0.1064
		Diagonal	Basic	0.7155
			Encrypted	0.0263

TABLE II. CORRELATION COEFFICIENT OF THE PROPOSED SCHEME WHERE B=100, SNR=5.

Image	Channels		Ours	
house	Red	Horizontal	Basic	0.9666
			Encrypted	-0.0302
		Vertical	Basic	0.7816
			Encrypted	0.0095
		Diagonal	Basic	0.9305
			Encrypted	0.0679
	Green	Horizontal	Basic	0.9502
			Encrypted	0.0507
		Vertical	Basic	0.9069
			Encrypted	0.0005
		Diagonal	Basic	0.9674
			Encrypted	0.0809
	Blue	Horizontal	Basic	0.9289
			Encrypted	-0.0673
		Vertical	Basic	0.9408
			Encrypted	0.0039
		Diagonal	Basic	0.9747
			Encrypted	-0.0006
baboon	Red	Horizontal	Basic	0.5753
			Encrypted	-0.0105
		Vertical	Basic	0.9479
			Encrypted	0.0748
		Diagonal	Basic	0.9183
			Encrypted	-0.0187
	Green	Horizontal	Basic	0.5336
			Encrypted	-0.0552
		Vertical	Basic	0.9267
			Encrypted	0.1198
		Diagonal	Basic	0.8610
			Encrypted	0.0023
	Blue	Horizontal	Basic	0.7484
			Encrypted	-0.0550
		Vertical	Basic	0.9169
			Encrypted	0.0083
		Diagonal	Basic	0.9380
			Encrypted	0.0184
lena	Red	Horizontal	Basic	0.9067
			Encrypted	-0.0359
		Vertical	Basic	0.9846
			Encrypted	-0.0224
		Diagonal	Basic	0.8660
			Encrypted	-0.0328
	Green	Horizontal	Basic	0.9434
			Encrypted	-0.0054
		Vertical	Basic	0.9785
			Encrypted	-0.0143
		Diagonal	Basic	0.8568
			Encrypted	0.0034
	Blue	Horizontal	Basic	0.8629
			Encrypted	0.0113
		Vertical	Basic	0.9286
			Encrypted	0.0762
		Diagonal	Basic	0.7155
			Encrypted	0.0429

TABLE III. Evolution of test-bed clusters

Channels		Ours	Ref. [34]	Ref.[35]
Red	Horizontal	0.0306	0.0033	-0.0015
	Vertical	0.0241	0.0155	-0.0015
	Diagonal	-0.0205	0.0158	0.0014
Green	Horizontal	0.0398	0.0294	0.0006
	Vertical	-0.0728	0.0146	-0.0007
	Diagonal	-0.0650	0.0102	-0.00004
Blue	Horizontal	0.0040	0.0086	-0.0009
	Vertical	0.0353	-0.0229	-0.0014
	Diagonal	0.0056	-0.0366	0.0001

9. Analysis of Information Entropy

One such knowledge security element that may be used to describe the degree of uncertainty or unpredictability in a picture is the entropy analysis. The information entropy of a signal may be written as (19):

$$Entrp\,(s) = \sum_{n=0}^{2^N-1} P\,(s_i) \times \log_2 \left(\frac{1}{P(s_i)}\right) bits \qquad (19)$$

Where the probability of the symbol s_i is $P\,(s_i)$, the basic unit of the sources number of bits representing is N and all basic unit combinations is 2^N. Table IV demonstrate a comparative analysis of the different Image with size 256×256 of Information Entropy for various channels sizes.

TABLE IV. ENTROPY ANALYSIS.

Cipher image	Channels	Ours
House	Red	7.9974
	Green	7.9966
	Blue	7.9969
Baboon	Red	7.9970
	Green	7.9969
	Blue	7.9974
Lena	Red	7.9973
	Green	7.9974
	Blue	7.9973

TABLE V. COMPARISON OF INFORMATION ENTROPIES.

Channels	Ours	Ref.[37]
Red	7.9993	7.2797
Green	7.9993	7.5993
Blue	7.9992	7.0041

A. Key Space Analysis

Key space is the collection of all possible image encryption keys. If you want your encryption to be secure against brute force attacks, the key space must be sufficiently large. The keys are the initial values of parameters $x_0, \lambda_1, y_0, \lambda_2$, if the computation precision is around 2^{32}. Then the key space is $2^{128}\left(2^{32} \times 2^{32} \times 2^{32} \times 2^{32}\right)$. When compared to other systems, as shown in Table VI, the value is staggering. Thus, the suggested approach is very resistant to attacks using brute force.

TABLE VI. COMPARISON OF INFORMATION ENTROPIES.

Key Space	Ours	Ref.[38]	Ref.[39]
	12^{128}	2^{145}	10^{45}

B. Differential Attack Analysis

The attackers attempt to connect the plain image to the encrypted image, for instance, by altering only one pixel for two photos and assessing the accompanying chip images by shifting two identical single images by an infinitesimal amount. For this purpose, Chen etc. [40] used the two metrics Shift Rate Number of Pixels (NPCR and UACI) to measure the average difference between the two images. The NPCR and UACI steps can be described in the following Eqs. (20,21) respectively [40]:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100 \qquad (20)$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1\,(i,j) - C_2\,(i,j)|}{255}\right] \times 100 \qquad (21)$$

Where W and H are the widths and ciphered image height. C_1 is the authenticated image and the ciphered image C_2 is produced if a pixel of C1 is changed in random. $D(i,j)$ that show in (22) is provided with [40]:

$$D\,(i,j) = \begin{cases} 0, & ifC1i,j = C2i,j \\ 1, & otherwise \end{cases} \qquad (22)$$

Table VII show NPCR Tests for each different Image system size 256×256 of different channels. Table VIII show UACI Tests for each different Image system size 256×256 of different channels. The comparative studies among our system and others listed in Table IX show that NPCR is better than systems such as [41] and [42].

TABLE VII. NPCR ANALYSIS.

Cipher image	Channels	Ours
House	Red	99.6368
	Green	99.5834
	Blue	99.6109
Baboon	Red	99.6323
	Green	99.6262
	Blue	99.6201
Lena	Red	99.6292
	Green	99.6292
	Blue	99.5834

TABLE VIII. UACI ANALYSIS.

Cipher image	Channels	Ours
House	Red	27.3145
	Green	29.7356
	Blue	31.4275
Baboon	Red	29.2778
	Green	27.4769
	Blue	29.8482
Lena	Red	32.5927
	Green	31.2368
	Blue	28.2644

TABLE IX. UACI ANALYSIS.

Cipher image	Channels	Ours	Ref.[41]	Ref.[42]
Lena	Red	99.6246	99.60	99.599
	Green	99.6117	99.60	99.599
	Blue	99.6101	99.60	99.620

10. CONCLUSION

Data security has become more critical as the internet and digital communications have grown in amount of data transmitted through communication platforms. Secure image encryption is required because of the widespread use of data over networks. We presented in our research a new approach of color image encryption technique using DCSK. The impact of our model is proved through comparison of previous work done. The Lena image's simulation findings of BER and PSNR with varied SNR are presented. Also the protection analysis's histogram, the correlation coefficient, the entropy, and the key space analyses are analyzed and compared. The limitations and boundary conditions of this work is: Increase β will degrade the BER performance. The reference of DCSK will affect the security of the system. The model designed have important features related to data security. The future work of this system is extended the DCSK to permutation index DCSK to increase the security of DCSK system.

References

[1] C. Tse and F. Lau, "Chaos-based digital communication systems," *Operating Principles, Analysis Methods and Performance Evaluation (Springer Verlag, Berlin, 2004)*, 2003.

[2] G. Kolumbán, B. Vizvári, W. Schwarz, and A. Abel, "Differential chaos shift keying: A robust coding for chaos communication," in *Proc. NDES*, vol. 96, 1996, pp. 87–92.

[3] G. Kolumbán, M. P. Kennedy, and L. O. Chua, "The role of synchronization in digital communications using chaos. ii. chaotic modulation and chaotic synchronization," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 45, no. 11, pp. 1129–1140, 1998.

[4] H. Elkamchouchi, R. Anton, and Y. Abouelseoud, "New encryption algorithm for secure image transmission through open network," *Wireless Personal Communications*, vol. 125, no. 1, pp. 45–62, 2022.

[5] Y. Pourasad, R. Ranjbarzadeh, and A. Mardani, "A new algorithm for digital image encryption based on chaos theory," *Entropy*, vol. 23, no. 3, p. 341, 2021.

[6] G. Kolumbán, M. P. Kennedy, and L. O. Chua, "The role of synchronization in digital communications using chaos. ii. chaotic modulation and chaotic synchronization," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 45, no. 11, pp. 1129–1140, 1998.

[7] G. Kolumbán, M. P. Kennedy, Z. Jákó, and G. Kis, "Chaotic communications with correlator receivers: theory and performance limits," *Proceedings of the IEEE*, vol. 90, no. 5, pp. 711–732, 2002.

[8] M. Hasler and T. Schimming, "Chaos communication over noisy channels," *International Journal of Bifurcation and Chaos*, vol. 10, no. 04, pp. 719–735, 2000.

[9] F. C. Lau and C. K. Tse, "On optimal detection of noncoherent chaos-shift-keying signals in a noisy environment," *International journal of bifurcation and chaos*, vol. 13, no. 06, pp. 1587–1597, 2003.

[10] F. C. Lau and C. K. Tse, "Approximate-optimal detector for chaos communication systems," *International Journal of Bifurcation and Chaos*, vol. 13, no. 05, pp. 1329–1335, 2003.

[11] C. K. Tse, F. Lau, K. Cheong, and S. Hau, "Return-map-based approaches for noncoherent detection in chaotic digital communications," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 49, no. 10, pp. 1495–1499, 2002.

[12] G. Kolumbán, G. Kis, M. Kennedy, and Z. Jáko, "Fm-dcsk: A new and robust solution to chaos communications," in *Proc. Int. Symp. Nonlinear Theory Appl.* IEICE (institute of electronics information and communication engineers) Hawaii, 1997, pp. 117–120.

[13] M. P. Kennedy and G. Kolumban, "Digital communications using chaos," *Signal processing*, vol. 80, no. 7, pp. 1307–1320, 2000.

[14] Z. Galias and G. M. Maggio, "Quadrature chaos-shift keying: theory and performance analysis," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, no. 12, pp. 1510–1519, 2001.

[15] F. C. Lau, K. Y. Cheong, and C. K. Tse, "Permutation-based dcsk and multiple-access dcsk systems," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 50, no. 6, pp. 733–742, 2003.

[16] P. R. Sankpal and P. Vijaya, "Image encryption using chaotic maps: a survey," in *2014 fifth international conference on signal and image processing*. IEEE, 2014, pp. 102–107.

[17] Z.-H. Guan, F. Huang, and W. Guan, "Chaos-based image encryption algorithm," *Physics letters A*, vol. 346, no. 1-3, pp. 153–157, 2005.

[18] H. Dedieu, M. P. Kennedy, and M. Hasler, "Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing chua's circuits," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 40, no. 10, pp. 634–642, 1993.

[19] U. Parlitz, L. O. Chua, L. Kocarev, K. S. Halle, and A. Shang, "Transmission of digital signals by chaotic synchronization," *In-*

ternational Journal of Bifurcation and Chaos, vol. 2, no. 04, pp. 973–977, 1992.

[20] D.-P. Vuong, D.-K. Le, K.-K. Nguyen, and B. Van Nguyen, "Correlation receiver with nonlinearity blanking for dcsk systems under pulse jamming attack," *IEEE Access*, vol. 7, pp. 25 037–25 045, 2019.

[21] M. Herceg, G. Kaddoum, D. Vranješ, and E. Soujeri, "Permutation index dcsk modulation technique for secure multiuser high-data-rate communication systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 4, pp. 2997–3011, 2017.

[22] P. Chen, Y. Fang, K. Su, and G. Chen, "Design of a capacity-approaching chaos-based multiaccess transmission system," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 12, pp. 10 806–10 816, 2017.

[23] G. Kolumbán, M. P. Kennedy, and L. O. Chua, "The role of synchronization in digital communications using chaos. i. fundamentals of digital communications," *IEEE Transactions on circuits and systems I: Fundamental theory and applications*, vol. 44, no. 10, pp. 927–936, 1997.

[24] C. Tse and F. Lau, "Chaos-based digital communication systems," *Operating Principles, Analysis Methods and Performance Evaluation (Springer Verlag, Berlin, 2004)*, 2003.

[25] M. P. Kennedy, G. Kolumbán, G. Kis, and Z. Jákó, "Performance evaluation of fm-dcsk modulation in multipath environments," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 47, no. 12, pp. 1702–1711, 2000.

[26] M. Kennedy, R. Rovatti, and G. Setti, *Chaotic electronics in telecommunications*. CRC press, 2000.

[27] G. Kolumbán, B. Vizvári, W. Schwarz, and A. Abel, "Differential chaos shift keying: A robust coding for chaos communication," in *Proc. Int. Workshop Non-Linear Dyn. Electron. Syst. (NDES)*, vol. 96, 1996, pp. 87–92.

[28] T. S. Rappaport, *Wireless communications: Principles and practice, 2/E*. Pearson Education India, 2010.

[29] R. M. May, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, pp. 459–467, 1976.

[30] M. J. Feigenbaum, "The universal metric properties of nonlinear transformations," *Journal of Statistical Physics*, vol. 21, pp. 669–706, 1979.

[31] M. FEIGENBAUM, "Universal behavior in nonlinear systems," *Los Alamos Sci.*, vol. 1, pp. 4–27, 1980.

[32] N. K. Pareek, V. Patidar, and K. Sud, "Discrete chaotic cryptography using external key," *Physics Letters A*, vol. 309, no. 1-2, pp. 75–82, 2003.

[33] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, ", handbook of applied cryptography, crc press, boca raton," *New York, London, Tokyo*, 1997.

[34] M. Ahmad, M. N. Doja, and M. M. S. Beg, "Security analysis and enhancements of an image cryptosystem based on hyperchaotic system," *Journal of King Saud University-Computer and Information Sciences*, vol. 33, no. 1, pp. 77–85, 2021.

[35] G. Kolumbán, "Performance improvement of chaotic communication systems," in *Proc. ECCTD'97*, 1997, pp. 284–289.

[36] R. I. Abdelfatah, "Secure image transmission using chaotic-enhanced elliptic curve cryptography," *IEEE Access*, vol. 8, pp. 3875–3890, 2019.

[37] Y. M. Khazaal, K. A. Zidan, and F. S. Hasan, "Fpga hardware image encryption co-simulation utilizing hybrid lfsr and chaos maps," in *Intelligent Systems and Networks: Selected Articles from ICISN 2021, Vietnam*, vol. 243. Springer, 2021, pp. 487–498.

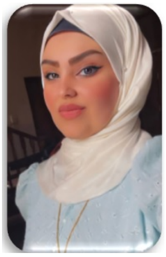
[38] M. Kumar, A. Iqbal, and P. Kumar, "A new rgb image encryption algorithm based on dna encoding and elliptic curve diffie–hellman cryptography," *Signal Processing*, vol. 125, pp. 187–202, 2016.

[39] W. Wang, M. Si, Y. Pang, P. Ran, H. Wang, X. Jiang, Y. Liu, J. Wu, W. Wu, N. Chilamkurti *et al.*, "An encryption algorithm based on combined chaos in body area networks," *Computers & Electrical Engineering*, vol. 65, pp. 282–291, 2018.

[40] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3d chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[41] X.-L. Chai, Z.-H. Gan, Y. Lu, M.-H. Zhang, and Y.-R. Chen, "A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system," *Chinese Physics B*, vol. 25, no. 10, p. 100503, 2016.

[42] C.-H. Yang and S.-J. Huang, "Secure color image encryption algorithm based on chaotic signals and its fpga realization," *International journal of circuit theory and applications*, vol. 46, no. 12, pp. 2444–2461, 2018.



Yasmine M. Khazaal was born in Baghdad, Iraq in 1995. She has got her B.Sc. in Software Engineering in 2017, and M.Sc. in Computer Engineering in 2021 at College of Engineering / Iraqi University, Baghdad, Iraq. She is interested in subjects: Computer Security, Image Processing, FPGA's and Xilinx System Generator, Chaotic Modulation and Digital Signal Processing.

Yassine Aydi Computer Science Associate professor. Received the PhD degree in computer science engineering, M.S. degrees from the National Engineering School of Sfax, Tunisia in 2007 and 2011, respectively. Also, I received the Engineer degree from the National Engineering School of Monastir, Tunisia in 1994. My research interests include Co-design, Networks-on-Chip design, and formal verification of parallel computing, HCI, Interaction Design.

Mohamed Abid Professor on Computer science. Received the Ph.D. degree from the National Institute of Applied Sciences, Toulouse, France, in 1989, and the “thèse d’état” degree from the National School of Engineering of Tunis, Tunisia, in 2000, in the area of Computer Engineering and Microelectronics.,He is currently the Head of Computer Embedded System Laboratory CES-ENIS, Tunisia. He is also a Professor with the Engineering National School of Sfax (ENIS), University of Sfax, Tunisia.