STATISTICS, OPTIMIZATION AND INFORMATION COMPUTING
Stat., Optim. Inf. Comput., Vol. **x**, Month 202x, pp 0–12.
Published online in International Academic Press (www.IAPress.org)

Image encryption based on Blowfish cipher and D-BPSK for security network communication

Mays Kifah Faeq [1,*], Eman Shakir Mahmood [2], Azhar Faisal Habboo [3]

[1] *Computer Science and Information Technology College, Computer Science Department, University of Kirkuk, Iraq*
[2] *College of Computer Science, University of Technology, Baghdad, Iraq*
[3] *Middle Technical University, Baghdad, Iraq*

Abstract In this article, a secure high-speed optical communication system was proposed and analyzed at 40 Gb/s using the Blowfish algorithm in combination with D-BPSK modulation. The proposed system is designed and simulated on the OptiSystem platform to investigate its effectiveness in signal integrity, BER performance, transmission distance, and security robustness. Both encryption and modulation (D-BPSK) can be carried out at sufficiently low complexity for 100 Gb/s systems. Simulated results indicate that the system can achieve transmission distance up to 600 km if there is no D-BPSK. However, with D-BPSK implemented, the distance increases significantly to 1080 km with improving 80%.

Keywords Blowfish, D-BPSK, Security, fiber optic, Image cryptography, OptiSystem–MATLAB program simulation

DOI: 10.19139/soic-2310-5070-4823

1. Introduction

Secure optical communication systems have attracted attracting interest because of the possibility for high-capacity, long-distance transmission and inherent resistance to electromagnetic interference. Various techniques have been suggested to improve the physical-layer security of such systems, addressing the increasing threat of eavesdropping in modern networks. For example, chaos-based modulation has been demonstrated to show how signal confidentiality can be significantly improved in hybrid optical links [1]. Similarly, it has been showed that integrating reconfigurable intelligent surfaces (RIS) into hybrid RF/FSO links can enhance secrecy performance by optimizing reflection parameters and mitigating atmospheric turbulence effects [2]. On the other hand, capacity need in infrastructure for internet access is always increasing in both business and academics, necessitating further innovation to reach acceptable levels [3]. In comparison to single-link systems, other research shows that relay optimization and adaptive resource allocation can significantly increase secrecy capacity and lower secrecy outage probability [4]. Related work has focused on modulation methods and channel impacts. For example, [5] examined how atmospheric turbulence and fog dramatically reduce bit error rate (BER) performance and demonstrated that these disadvantages may be somewhat mitigated by increasing optical power. Furthermore, state-of-the-art studies on physical-layer security in multimode fiber networks have shown how dynamic channel conditions and mode-dependent losses may naturally favor the legitimate receiver over eavesdroppers [6].

*Correspondence to: Mays Kifah Faeq (Email: mayskifah@uokirkuk.edu.iq). Computer Science and Information Technology College, Computer Science Department, University of Kirkuk, Iraq.

ISSN 2310-5070 (online) ISSN 2311-004X (print)
Copyright © 202x International Academic Press

2. Related work

Blowfish is unique among symmetric encryption techniques because of its speed, effectiveness, and robust cryptographic resistance. While comparative performance tests (AES, 3DES, and Blowfish) demonstrate Blowfish's favorable trade-off between encryption speed and security [7], thorough security studies confirm its resistance to brute-force and differential assaults [8]. To increase its resilience and efficiency, a number of algorithmic improvements, such as improved round structures, have been suggested [9]. Furthermore, robustness and high critical sensitivity with respect to statistical and qualitative attacks emphasize the necessity of strong encryption for safe data transfer [10]. Applied implementations in optical environments, such as photo encryption using Blowfish, illustrate its practical utility without affecting system performance [11]. Additionally, data security has been enhanced by employing numerous chaotic maps to disrupt statistical patterns in encrypted images and randomizing transmission channels [12, 13]. Blowfish's superior encryption efficiency and throughput for huge data types are validated by empirical investigations. The Blowfish encryption algorithm has garnered interest among the many cryptographic algorithms because to its quick speed, minimal memory needs, and demonstrated security strength. Blowfish has been included into optical systems in a number of studies, mainly for the purpose of encrypting image or data streams before modulation in order to improve security against unwanted access [14]. Many approaches to data protection have been put forth. Machine learning algorithms have demonstrated promising outcomes for QoT prediction and net management; however, a lot of These techniques rely on single-model architectures or brief samples, which may impede accuracy in applicability over a range for the framework circumstances [15]. High level of safety In an effort to improve the speed of data as well as safety transfer for PON, the Blowfish encryption method was used in the development of the GPON technique [16]. It also includes secured optic communication employing the hill approach encryption [17, 18], security strategy that incorporates the Blowfish cipher [19]. Recently, we demonstrated the feasibility and efficiency of integrating Blowfish encryption in wavelength-division multiplexed passive optical networks to safeguard user data without compromising network throughput [20]. The quick growth of requests for more internet connectivity makes these changes quite difficult for communication engineers [21].

2.1. Our contribution

Despite these advancements, previous work has focused on either optical–encryption methods without advanced modulation or modulation schemes without integrated encryption. The distinction from our previous work is as follows. References [14], [16], and [20] investigated Blowfish-based security in different optical communication contexts, including a secure optical communication system, GPON, and TWDM-PON, respectively. In contrast, the present study focuses on a 40-Gb/s long-haul optical link employing D-BPSK and evaluates the effect of the modulation scheme on transmission performance while maintaining Blowfish-based data security. The main communication-level investigation is therefore the comparative evaluation of the same optical architecture with and without D-BPSK under the considered transmission conditions.

To address this gap, more specifically, this work emphasizes the following contributions:

1. System-level integration: Blowfish image encryption is incorporated into a 40-Gb/s optical transmission chain together with D-BPSK modulation, rather than treating encryption and modulation as independent studies.
2. Transmission-performance investigation: The study quantitatively evaluates Q-factor, BER, eye diagrams, input-power dependence, and transmission distance for the system with and without D-BPSK. The simulations indicate an achievable distance of approximately 600 km without D-BPSK and approximately 1080 km with D-BPSK under the investigated conditions, corresponding to an approximately 80% increase in transmission reach.
3. Joint security and communication assessment: In addition to optical-link performance, the encrypted images are evaluated using histogram, correlation, entropy, NPCR, UACI, PSNR, MSE, MAE, and encryption-time analyses. This provides a combined assessment of the security processing and optical transmission performance within the simulated system.

4. Clearer positioning relative to previous work: The proposed work now explicitly acknowledges that Blowfish encryption and D-BPSK are established technologies. The contribution is therefore positioned as an application-oriented system integration and performance study rather than as the introduction of a new encryption algorithm or a new modulation format. The structure of this work is as follows: Section 1 provides an introduction, Section 2 discusses related work with contributions, and Section 3 presents the Blowfish Algorithm's implementation. Section 4 presents the simulation model, Section 5 presents the findings, and Section 6 concludes the study.

3. Blowfish Algorithm Implementation

A variety of techniques have been utilized to guarantee safe transfer of data. The block of 64 bits encryption technique because it is compact, simple to use and incredibly safe even under close inspection, Blowfish is an excellent choice for encryption. Because Blowfish use the identical key secret for both encoding and restoration, it splits messages into blocks of a fixed length. Furthermore, it supports keys with lengths between 32 and 448 bits [22]. Figure 1 illustrates the Blowfish encryption technique utilized in this investigation. The Feistel network architecture is shown in subfigure (a). To obtain the final encryption image, the plain image is split into left (L) and right (R) halves, processed via 16 iterative rounds of XOR and F-function operations, and then subjected to two further permutations (P17 and P18). A substantial avalanche effect, in which a little change in the input dramatically changes the output, is guaranty by this recurrent procedure. The F-function, Blowfish's primary nonlinear component, is described in subfigure (b). Four distinct S-boxes are used to replace the four segments (L1, L2, L3, and L4) that make up the input L. Modular additions and XOR techniques are used to aggregate the outcomes in order to reduce confusion and dispersion. Due to its design, Blowfish is resistant to statistical and differential attacks and can quickly encrypt massive volumes of data, including images. Twofish and AES are not the same as Blowfish, a symmetric key block cipher. Blowfish offers improved throughput, quick encryption, and efficiency by using variable key lengths up to 448 bits, as opposed to Twofish's 256-bit maximum. Additionally, in contrast to DES's Feistel structure, it uses a special F-function that works on half blocks. Because Blowfish uses smaller 64-bit blocks instead of AES's fixed 128-bit block sizes, it is better suited for applications requiring less memory or processing resources [22]. Blowfish algorithm's distinctive architecture allows it to balance safety and speed. Because of its speed and ease of use, it works especially well with hardware implementations. Blowfish is appropriate for encrypting real-time long-distance messages because of its quick encryption rate and lower complexity when compared to twofish or AES. Since the key remains fixed and secure, there's no necessity to reset the S and P arrays. Every text block in Cipher Block Chaining (CBC) mode is XORed with the preceding ciphertext block using the blowfish algorithm before being encrypted. Stages describing the operation of CBC mode: 1. Add data from images to a matrix. 2. Choose a secret key that ranges in length from 32 to 448 bits (a least of 128 bits is recommended to attain safety). 3. Make a random IV identical dimensions as my information block (8 bytes for blowfish). Figure 2 shows the CBC phase's mode of the blowfish method. The sole difference between decoding and encoding is the order in which P1, P2, and P18 are used.

4. Simulation Set Up

To guaranty security and spectral efficiency, the transmitter design of the suggested 40 Gb/s optical communication system depicted in figure 3 combines sophisticated modulation and data encryption. The input bit stream, which represents an original picture to be safely transferred, is created using a Random-Pseudo Binary Sequence generator. The picture is transformed into a randomly encrypted form by applying the Blowfish cipher method. The signal is then prepared for dual modulation by passing this encrypted binary sequence through a coded with a one-bit delay. A 1x2 electrical fork is used to separate the pre-coded signal once it has been transformed into a non-return-to-zero (NRZ) electrical format. The optical carrier is provided by a continuous-wave (CW) laser and is modulated by two cascaded LiNbO Mach-Zehnder modulators (MZM). The data-carrying electrical signal is imprinted onto the optical carrier by the first modulator. A sine wave generator creates two out-of-phase

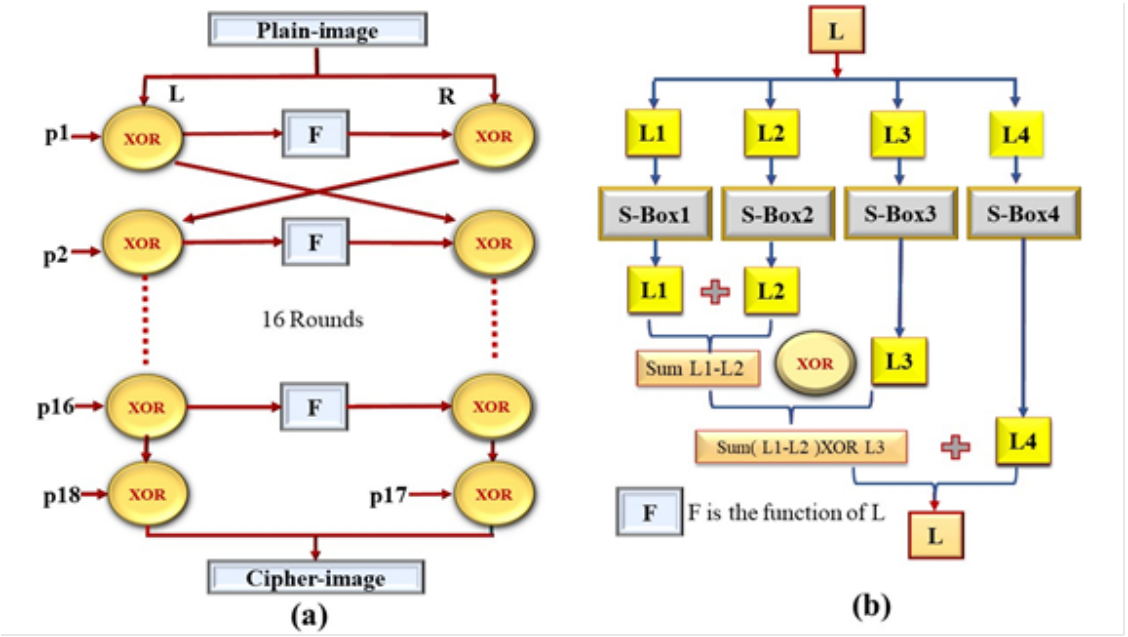


Figure 1. Encryption of Blowfish's technique [20].

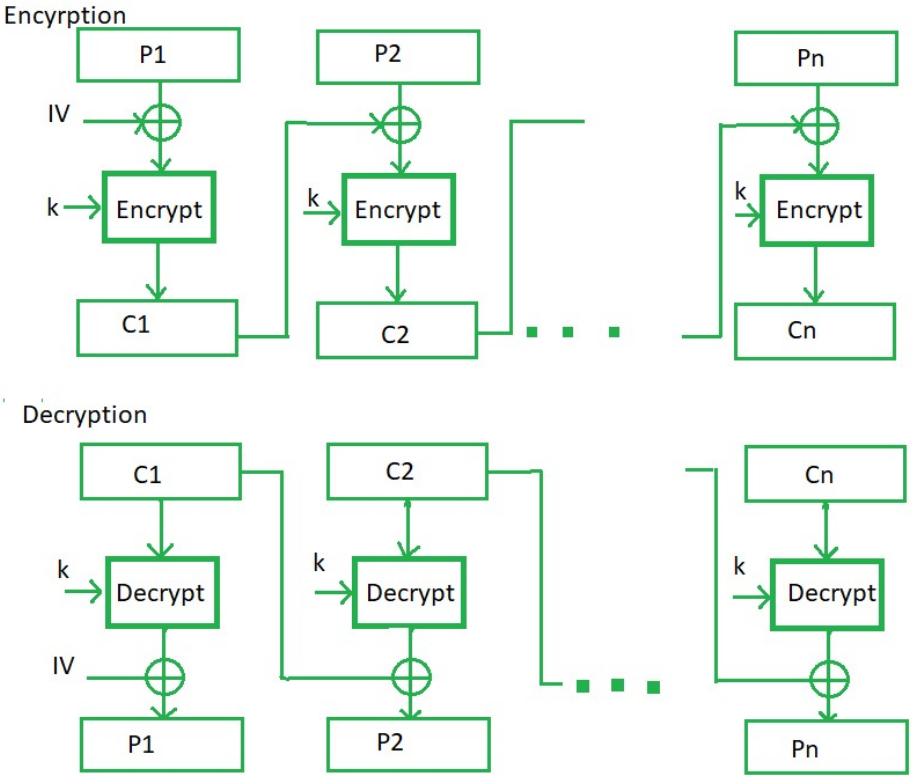


Figure 2. Illustration of the Blowfish cipher's CBC mode phases.

components by splitting a sinusoidal signal and passing it through a gain block with a gain of -1 in one direction. The second MZM, which carries out the D-BPSK modulation, is driven by these. A phase-modulated optic signal that is tailored for long-distance fiber transmission with lower bandwidth needs and improved data security is the end result. All 40Gbps optical channels use NRZ line coding and intensity modulation with direct detection (IM/DD), which is in line with the standard DBSK physical layer arrangement. According to communication conditions, the forward-error-correction (FEC) free sensitivity reference used in the performance evaluation is the BER = 10^{-9} and Q-factor = 6 threshold. The outcome of the simulation in OptiSystem was used to determine the BER and Q-factor values. Due of its simplicity of utilize, low hardware complexity, and interoperability with the intensity-modulated PON transceiver architecture employed in the OptiSystem environment simulation, the NRZ style was chosen. This confirms that the quoted 40Gbps bidirectional throughput is directly related to the encryption technology and optical link, not to coding overhead.

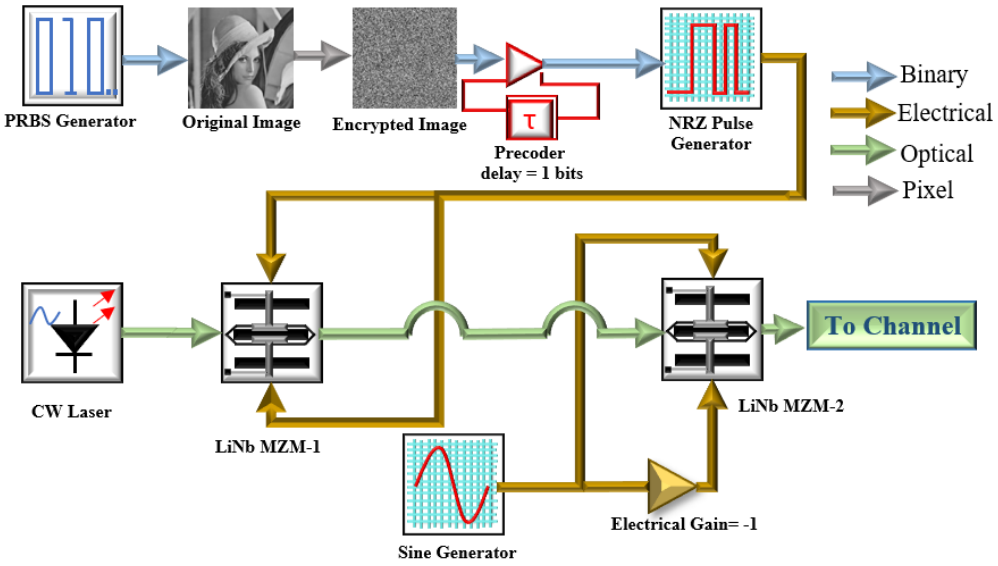


Figure 3. Architecture of the transmitter.

The optic transmission system depicted in Figure 4 uses a looped structure composed of segments of Standard Single-Mode Fiber (SMF) and Dispersion Compensating Fiber (DCF) to evaluate long-distance data delivery. For every loop iteration, the structure has one 5 km DCF segment and two 12.5 km SMF spans. To reduce chromatic dispersion and maintain signal integrity over long distances, the DCF is positioned precisely in between SMF spans. Three optical amplifiers, each with a gain of 2.5 dB, are placed after each fiber section to counteract signal attenuation. The amount of circulations the signal makes via this segment combination is managed by a loop control device.

Coherent detection and digital signal processing methods are used in the receiver part of Figure 5 to efficiently recover and assess the sent optical data. In order to remove carrier noise, the incoming optical signal is first divided, with one channel going into a Mach-Zehnder interferometer (MZI) and the other heading into an optical null. The MZI converts the phase-modulated output into an intensity-modulated signal that may be directly detected. After that, two PIN photodetectors pick up the optical outputs and transform them into electrical signals. An electrical subtractor processes these electrical signals to improve signal quality and reduce common-mode noise. A 3R regenerator performs re-amplification, re-shaping, and re-timing after a low-pass Bessel filter eliminates high-frequency noise components from the recoverable electrical signal. After decryption, the picture is recreated and its fidelity assessed. Lastly, by comparing the received data with the original encrypted input, a Bit Error Rate (BER) analyzer is utilized to measure the system performance.

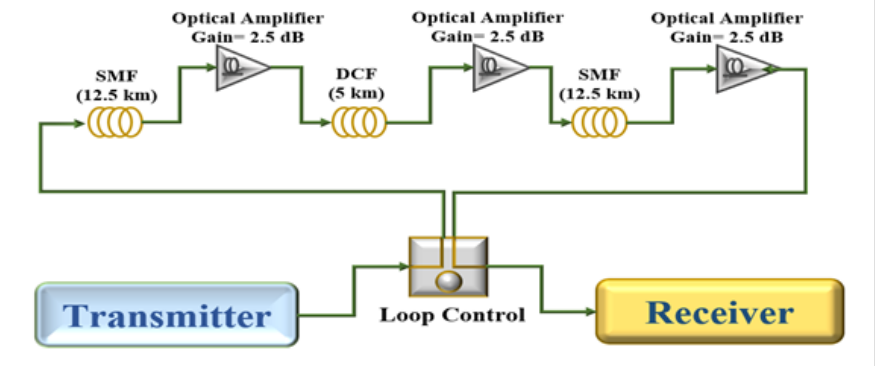


Figure 4. Optical transmission system.

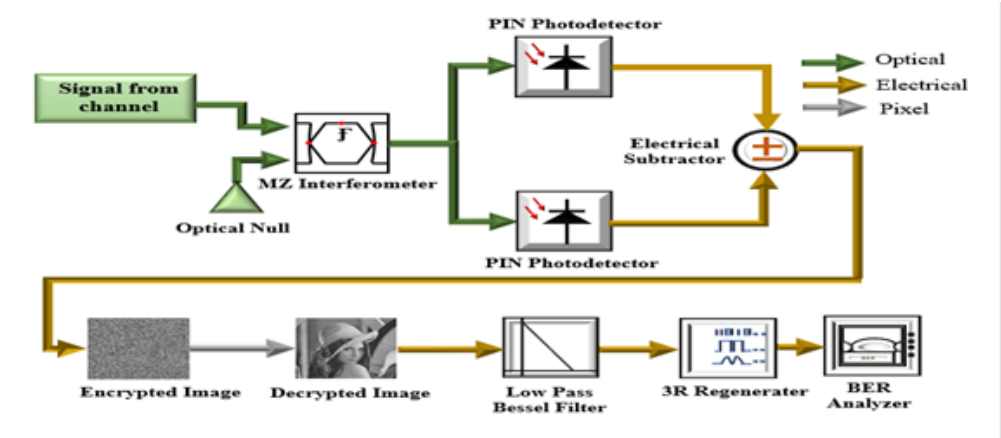


Figure 5. The receiver.

The grayscale Lena image is first represented as an array of pixel intensity values. The pixel values are then converted into their binary representation to generate a serial binary data stream. The resulting binary sequence is encrypted using the Blowfish algorithm before being supplied to the optical communication system. Blowfish operates on fixed 64-bit data blocks and uses a secret key. The manuscript specifies the supported Blowfish key-length range as 32–448 bits. The encoded output is later mentioned as a sequence binary and mapped to the input data stream of the OptiSystem transmitter.

The simulation workflow is summarized as follows:

1. A grayscale Lena image is used as the input data.
2. The photo data are converted into a binary sequence.
3. The binary data are encrypted using the Blowfish algorithm before optical transmission.
4. The encoded binary sequence is supplied to the OptiSystem transmitter through the MATLAB–OptiSystem interface.
5. A PRBS/data-generation stage is used to represent the transmitted binary sequence.
6. The encrypted sequence is processed by the precoding stage and converted to an NRZ electrical signal.
7. The electrical impulse is applied to the optical transmitter based on a CW laser and cascaded LiNbO3 Mach–Zehnder modulators.
8. D-BPSK modulation is applied to generate the phase-modulated optical signal.
9. The optical information is sent via the looped SMF–DCF fiber link.
10. Optical amplification is applied between the fiber sections.

11. At receiver, the optic signal is split and processed through the Mach–Zehnder interferometer for differential phase detection.
12. PIN photodetectors, an electrical subtractor, and a low-pass Bessel filter are used for electrical recovery.
13. A 3R regenerator is subsequently used for re-amplification, re-shaping, and re-timing.
14. The retrieved encrypted data is sent back to the MATLAB processor stage, where picture reconstruction and Blowfish decryption are carried out.
15. Q-factor, BER, eye-diagram, and image-encryption metrics are used to assess the recovered signal.

The transmitting data at the transmitter is the binary encoded sequence. The optical communication system's cascaded LiNbO3 Mach–Zehnder modulator configuration receives the sequence after it has been processed by the precoding stage and transformed into an NRZ electrical signal. After then, D-BPSK modulation is used prior to transmission via the SMF–DCF link.

5. Results and Discussion

5.1. Communication Results

Instead of using an absolute phase reference, D-BPSK is a straightforward but efficient modulation technique that hides data in the variation between the phases of subsequent bits. A binary "1" in this system is represented by a 180° shift in the carrier phase, whereas a binary "0" maintains the same phase. Strict synchronization of phases is not necessary since judgments are made at the receiver by contrasting the phase of each symbol with the preceding one. Because of this characteristic, D-BPSK is more resilient to nonlinear impairments that usually build up over long fiber lengths, such as phase noise and fluctuations in laser linewidth [23]. The proposed 40 Gb/s optical communication system's Q-factor fluctuation with respect to input power is shown in Figure 6, which compares performance with and without the use of D-BPSK. As can be seen, the Q-factor steadily rises with input power, reaches an optimal value, and subsequently decreases at higher power levels as a result of nonlinear impairments. When D-BPSK is employed, the technology achieves a significantly higher Q-factor across the whole input power range. Specifically, at an input level of 5 dBm, the highest Q-factor of around 81 is reached, while the system without D-BPSK records a lower peak Q-factor of roughly 45 at 3 dBm. The Q-factor drops after these optimal points because nonlinear processes take over signal quality. These findings unequivocally show that using D-BPSK modulation significantly improves system performance by increasing the working range and enhancing signal integrity under a range of input power circumstances.

Before using D-BPSK, Figure 7 shows the system's efficacy regarding Q-factor and BER in proportion to distance transmission at 3 dBm input power. As can be seen, the Q-factor rapidly diminishes with fiber distance, beginning at around 18 at 300 km and falling to a minimal range of 6 at 600 km. On the other hand, the BER increases steadily with distance until it reaches its limit of 10^{-9} at 600 km. The findings unequivocally show that transmission defects such dispersion and nonlinearities build up with distance, lowering signal quality and reducing the reach that may be attained. Significant distortion and decreased eye opening are also shown in the eye diagram at 600 km, which is consistent with the reported decrease in Q-factor and increase in BER. These results demonstrate the shortcomings of the system without sophisticated modulation techniques and support the use of D-BPSK to improve long-distance performance.

The system performance at 3 dBm input power using D-BPSK modulation is shown in Figure 8. Transmission reach is significantly improved as compared to the non-D-BPSK situation. Starting at about 20 at 500 km and staying over the crucial barrier of 6 up to 1080 km, the Q-factor sustains a higher level. As a result, the BER performance is greatly improved, staying below 10^{-45} till extended distances and barely getting close to 10^{-9} at about 1080 km. With a broader eye opening than in the pre-D-BPSK situation, the eye diagram at this distance also attests to better signal clarity. These findings show that D-BPSK successfully reduces transmission impairments, increasing the system's transmission range from 600 km to 1080 km and 80% increase in reach while maintaining a respectable level of signal quality.

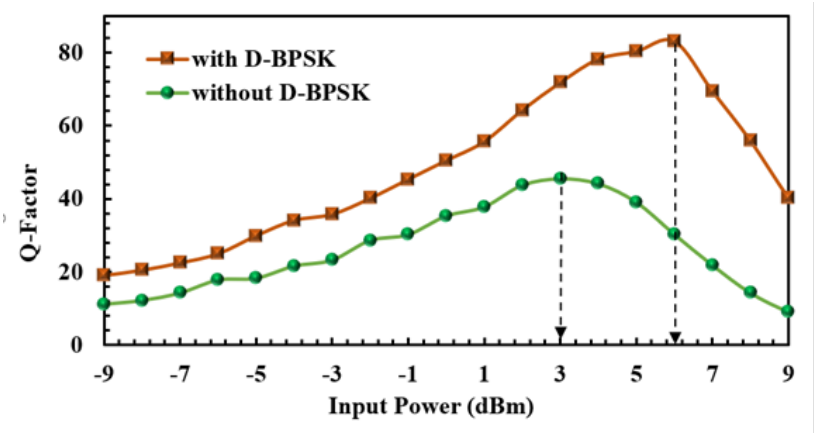


Figure 6. Q-factor with respect to input power.

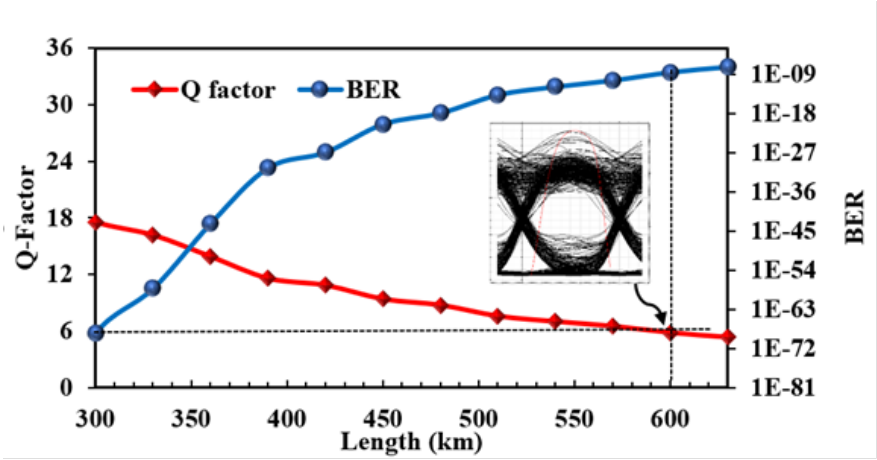


Figure 7. System performance before applying D-BPSK.

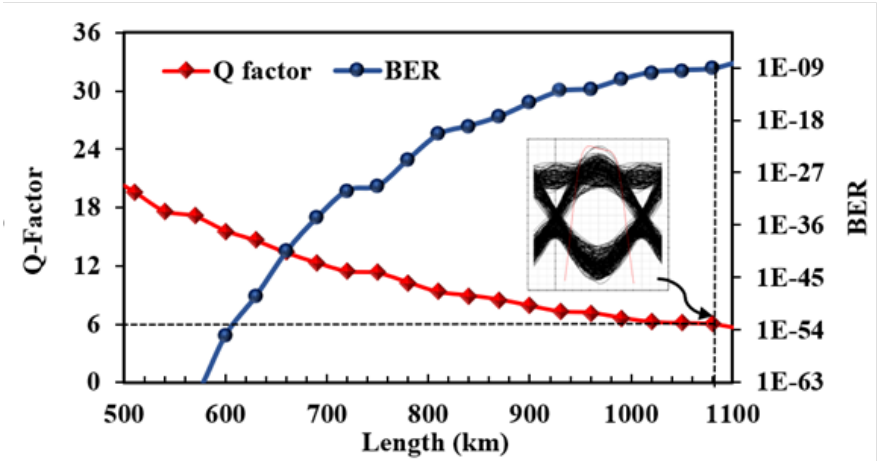


Figure 8. Performance of the system after D-BPSK is used.

5.2. Security Results

One of the most popular techniques for assessing the actual safety of an encryption method in picture encryption is histogram analysis. A histogram displays the distribution of pixel values in an image. The histogram typically shows peaks and troughs that indicate the frequency of specific gray levels for an original (simple) picture. If the picture is not adequately encrypted, attackers may be able to take advantage of the statistical information included in this uneven distribution [24]. This kind of non-uniform histogram is seen in the Lena picture in Figure 9 (a), which has many strong peaks that represent dominating pixel intensities. On the other hand, the histogram in Figure 9 (b) becomes almost flat once Blowfish encryption is applied. Since of this flatness, there are no discernible patterns since pixel values are dispersed uniformly throughout all gray levels. This is exactly what we want from a strong encryption scheme as it hides the underlying image features and makes statistical attacks extremely difficult.

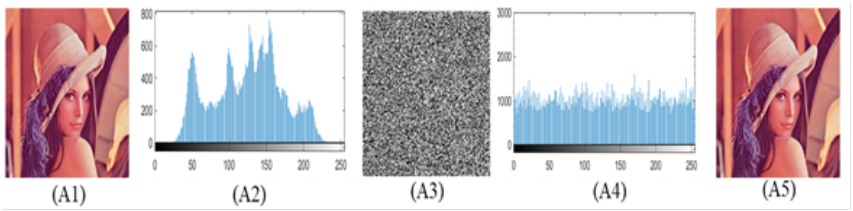


Figure 9. Simulation results: plain image (A1), its corresponding histogram (A2), encrypted image (A3), its corresponding histogram (A4), and recovered image (A5).

The distribution of pixel in the Lena testing images' D', V', and orientations is seen in Figure 10. For precise imaging, adjacent pixels in the horizontal (H'), vertical (V'), and diagonal (D') planes typically exhibit substantial relationships with one another. A secured picture is substantially different from the plain picture when correlations equal zero. When correlations are zero, a protected image differs significantly from a plain image. We assessed the Blowfish approach on a typical Lena image using a set of commonly used assessment criteria in table 1 to better understand its performance. Each statistic highlights a different element of the encryption process. CORR shows how independent the encrypted image is from the original, while UACI shows how sensitive the cipher is to pixel changes. When taken as a whole, these figures offer a reasonable evaluation of the encryption strength and allow us to ascertain Blowfish's actual resilience [25].

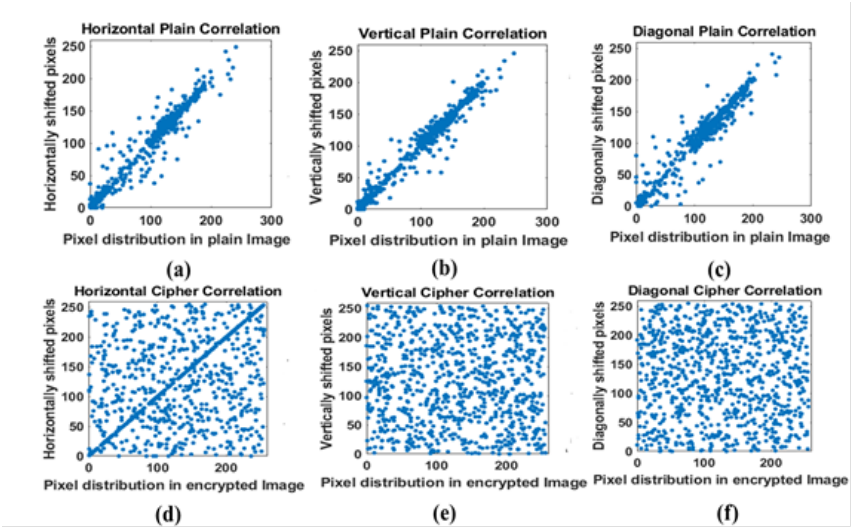


Figure 10. Correlation analysis for the Lena image: plain-image pixels (a–c) and encrypted-image pixels (d–f).

Table 1. Security analysis of the Blowfish cipher compared with another cipher.

Security analysis	Parameter security analysis	Proposed cipher	[26]	Interpretation
Perceptual security analysis	peak signal-to-noise ratio (PSNR)	9.33	11.9524	A very low PSNR (<20 dB) is considered good in encryption since it reflects strong distortion and prevents visual similarity.
	mean square error (MSE)	7653.58	-	High MSE is desirable in encryption, as it shows large differences between the plain and cipher images.
	mean absolute error (MAE)	72.53	-	A high MAE indicates significant average deviation, confirming effective encryption.
	Structural Similarity Index (SSIM) Original with Decrypted Image	1	-	When comparing index (SSIM) is a popular metric for determining image quality. Comparability is based on three factors: brightness, contrast, and structural features. An SSIM score of 1 indicates a perfect match between the reference and the distorted picture, implying that there is no obvious difference. In contrast, a near-zero SSIM score implies a significant divergence in the image's structure, brightness, and contrast, suggesting a considerable dissimilarity [27].
	SSIM Original with Encrypted Image	0.012032	-	
	Visual Information Fidelity (VIF) Original with Decrypted Image	0.99987	-	When evaluating fidelity (VIF) measure determines the percentage of the original image's visual information that survives after distortion. VIF quantifies how much of the information in a distorted image is preserved. A high VIF score implies little degradation and high-quality reproduction since the majority of the critical features have been kept. A low VIF score, on the other hand, indicates severe information loss and increased levels of distortion [27].
	VIF Original with Encrypted Image	0.060809	-	
Correlation analysis	Horizontal	-0.0406	0.0003	Correlation close to zero demonstrates excellent statistical independence between original and encrypted pixels.
	Vertical	-0.0720	0.0004	
	Diagonal	-0.0110	0.0025	
Differential attack analysis	NPCR (Number of Pixels Change Rate)	99.720	99.6175	NPCR is a metric used to test the sensitivity of an image encryption algorithm to changes in the original image. Ideally close to 100% (or 99.6094% in some contexts) [28].
	UACI (Unified Average Changing Intensity)	33.52	33.4152	Moderate value: UACI measures intensity changes between original and cipher images. While effective, ideal values are closer to ~33%.
Entropy analysis	Entropy of ciphered image	7.9981	7.9972	The Shannon entropy is a widely used approach for determining unpredictability and close to the theoretical value of 8.
Time encryption analysis		2.22	3.5015	demonstrating how rapidly our method proved to be faster than other algorithm

5.3. Evaluation of System Throughput and Latency

The length of time needed or the overall delay finishing a particular task or function inside a computer is known as latency. One crucial component of real-life software interactions is the almost instantaneous connectivity that users anticipate while talking, making phone calls, and streaming real-time videos. Significant latency degrades the user interface by causing delays in phone calls, message transmission, and file synchronization, especially with regard to video files [25]. The end-to-end delay that an optical signal experiences while traveling from Tx to Rx is referred to as latency in the system. The suggested D-BPSK structure's latency is measured using time-domain tracking instruments created within the OptiSystem modeling environment. Two Optical Time Domain Visualizers (OTDVs) are placed appropriately along the transmission chain:

1. To obtain the sent timestamp at the MZM output in the Tx, and
2. The data bit's receipt timestamp is recorded by the APD/Bessel in the Rx.

The delay is calculated in the following manner after PRBS is started:

$$t_{\text{latency}} = t_{\text{arrival}} - t_{\text{sent}}. \tag{1}$$

The transmitted timestamp of the packet is shown by t_{sent}, while the successful reception timestamp is indicated by t_{arrival}. Fiber propagation delay, MUX/DEMUX computation, and photodetector reaction time are among the contributing factors. The predicted delay of around $100\,\mu$s is increased by less than $0.6\,\mu$s due to the fiber (≤ 180 m). The total system latency is around $101\,\mu$s, which is compatible with next-generation high-capacity access networks and within the millisecond-level latency constraints of 5G/6G fronthaul. A machine, service, or device's throughput is the amount of work it can complete in a given time [25]. Throughput is influenced by the D-BPSK structure's aggregate wavelength in the suggested setup. A channel wavelength modulated at 40 Gb/s is the OLT's entire nominal capacity.

$$\text{Throughput} = 1 \times 40\,\text{Gb/s} = 40\,\text{Gb/s}. \tag{2}$$

This information shows the tested conditions, the system reliably provides 40 Gbps of speed. From the perspective of computation, the suggested encrypted D-BPSK design places a higher central processing burden at the Tx side because the processing downstream chain entails encryption of the binary photo pixels prior to MZM-driven optical modulation and NRZ production across the multi-channel configuration. For 256x256 test images, the results that were achieved with 2017a MATLAB on a purpose-general PC show encrypted timings of about 3.44-3.92 s. This does not directly reflect the use of hardware in real-time at deployment Tx/Rx devices.

5.4. Comparison with prior works

In this section, we contrast our study's results with those of other investigations. It shows that both the connection distance and data rate are much higher. They are all included in Table 2.

Table 2. Assessment of previous studies with the proposed strategy.

Ref.	Secure techniques	Bitrate	Transmission distance (km)
[29]	No security	2.5D/S/1.25U/S Gbps	60
[30]	No security	2.5D/S/1.25U/S Gbps	17
[31]	No security	2.5D/S/1.25U/S Gbps	40
[32]	No security	2.5D/S/1.25U/S Gbps	20
[16]	Blowfish ciphering	2.5D/S/1.25U/S Gbps	65
[18]	Hill ciphering	10D/S/5U/S Gbps	75
Proposed work	Blowfish ciphering	40 Gbps	1080

The key space for Blowfish is 2^{64}, with $(2^{64})^2 \times (10^{14})^2 \times (10^{14})^2 = 2^{314} \approx 3.3 \times 10^{94} > 2^{100}$; it is large enough to withstand a prolonged attack. Table 3 compares the key spaces of the proposed approach with those of modern techniques reported in research articles.

Table 3. Comparison between source and recommended key spaces.

Cipher	Ref. [33]	Ref. [34]	Ref. [35]	Ref. [36]	Ref. [37]	Suggested cipher
Key space	2^{186}	2^{149}	2^{203}	2^{199}	$3.4 \times 10^{80} \approx 2^{267}$	$10^{84} \approx 2^{314}$

6. Conclusion

In this work, we designed and analyzed a 40 Gb/s secure optical communication system that integrates the Blowfish encryption algorithm with Differential Binary Phase Shift Keying (D-BPSK) modulation. The Blowfish algorithm was evaluated using several image-based cryptographic metrics such as MSE, PSNR, RMSE, MAE, correlation coefficient, and UACI. The results confirmed its strong ability to generate highly distorted cipher texts with low correlation to the original image, ensuring effective data confidentiality and robustness against statistical attacks. Histogram analyses further verified the uniform distribution of pixel intensities, proving the cipher's ability to withstand statistical and differential cryptanalysis. D-BPSK's impact on the transmission side was clearly demonstrated. System efficiency declined beyond 600 km in the absence of D-BPSK due to cumulative flaws in the optical connection. However, by employing D-BPSK, the maximum broadcast range was further extended to 1080 km at 3 dBm launch power. This enhancement demonstrates that D-BPSK's resistance to phase noise and nonlinear fiber effects makes it an excellent modulation format for high-speed, long-distance optical communication systems. When everything is taken into consideration, the combination of D-BPSK modulation for transmission resilience and Blowfish encryption for data security provides a practical method for attaining security and dependability in next-generation optical networks. To further boost system capacity and security, future research may examine fusing relatively straightforward encryption algorithms with intricate modulation formats like QPSK or DP-QPSK.
Disclosures: The authors declare no conflicts of interest.

REFERENCES

1. H. M. Jasim, A. Qasim, A. Ali, and E. N. Abdulla, *Color image encryption strategy of Ro-FSO network systems based on CBC and Blowfish cipher*, Stat., optim. inf. comput., Oct. 2026. https://doi.org/10.19139/soic-2310-5070-4335.
2. L. Fan, W. Lu, R. Wang, and Y. Wang, *Research on Physical Layer Security Performance of Multi-user Mixed RF/FSO Communication System in FSO Eavesdropping Environment,* 2024 IEEE 12th Int. Conf. Inf. Commun. Networks, ICICN 2024 16, 246–251 (2024).
3. E. N. Abdulla, R. A. Hussien, F. F. Rashid, A. A. Abdulkafi, A. K. Abass, and M. A. Saleh, *Design and Performance Analysis of Symmetrical 160 Gbps TWDM-PON Utilizing Bidirectional Configuration,* J. Opt. (2023).
4. S. Althunibat, S. C. Tokgoz, S. Yarkan, S. L. Miller, and K. A. Qaraqe, *Physical Layer Security of Dual-Hop Hybrid FSO-mmWave Systems,* IEEE Access 11, 58209–58227 (2023).
5. A. Fakchich, M. Bouhadda, R. El Alami, F. M. Abbou, A. Essahlaoui, M. El Ghzaoui, H. Qjidaa, and M. O. Jamil, *Performance of BPSK-FSO Communication Over Turbulence and Fog Attenuation,* Lect. Notes Networks Syst. 668 LNNS, 326–334 (2023).
6. S. Rothe, N. Koukourakis, H. Radner, A. Lonnstrom, E. Jorswieck, and J. W. Czarske, *Physical Layer Security in Multimode Fiber Optical Networks,* Sci. Rep. 10, 1–11 (2020).
7. A. Alabaichi, F. Ahmad, and R. Mahmod, *Security analysis of blowfish algorithm,* 2013 2nd Int. Conf. Informatics Appl. ICIA 2013 12–18 (2013).
8. B. A. Buhari, H. Abdulkadir, S. A. Ahmad, R. Sulaiman, M. M. Umar, S. Shehu, A. Almu, A. M. Abubakar, and J. O. Nwoji, *Performance and Security Analysis of Symmetric Data Encryption Algorithms: AES, 3DES and Blowfish,* Int. J. Adv. Netw. Appl. 16, 6473–6486 (2025).
9. R. Patel and P. Kamboj, *Security enhancement of blowfish block cipher,* Commun. Comput. Inf. Sci. 628 CCIS, 231–238 (2016).
10. M. Hanif, *Advanced 3D Image Encryption for Multiple RGB Images Using Hybrid Chaotic Maps,* Riphah Int. Univ. 0–39 (2025).
11. A. T. Hashim, A. H. Jassem, and S. A. Ali, *A Novel Design of Blowfish Algorithm for Image Security,* J. Phys. Conf. Ser. 1818, (2021).
12. K. M. Hosny, Y. M. Elnabawy, R. A. Salama, and A. M. Elshewey, *Multiple image encryption algorithm using channel randomization and multiple chaotic maps,* Sci. Rep. 14, 1–18 (2024).
13. B. A. Buhari, A. A. Obiniyi, K. Sunday, and S. Shehu, *Performance Evaluation of Symmetric Data Encryption Algorithms: AES and Blowfish,* Saudi J. Eng. Technol. 04, 407–414 (2019).
14. Riyadh, Marwah, Hadi, Ban K., Salman, Lina A. and Abdulla, Essam N.. *Security performance analysis of symmetric 112.5 Gbps coexistence 50G-PON, XGS-PON and GPON architecture based on Blowfish group cipher* Journal of Optical Communications, 2026. https://doi.org/10.1515/joc-2026-0027.
15. Ridha, Fay F., Abdulla, Essam N. and Abdulhadi, Ali H.. *Machine learning based on raw ensemble predictions scheme for TWDM-PON* Journal of Optical Communications. https://doi.org/10.1515/joc-2025-0373.

16. R. Musadaq, S. N. Abdulwahid, Nassren N. Abd Alwahed, and E. N. Abdulla, *Security analysis of an image encryption algorithm based on Blowfish in GPON,* J. Opt. Commun. 32–34 (2025).
17. A. F. Mushatet, E. A. Fadil, and E. N. Abdulla, *High bit rate secure FSO system utilizing Hill coding,* J. Opt. Commun. 0147, 1–14 (2025).
18. E. Mousa, E. N. Abdulla, and S. A. Adnan, *Enhancing network security based on 10G-EPON with the use of the Hill cipher algorithm,* J. Opt. Commun. 1–13 (2025).
19. Ali, Ahmed Hussein, Zaal, Riam M., Abdulla, Essam N. and Al-khaylani, Hayder H.. *Capacity and security enhancement in TWDM-NG-PON2 networks based on hybrid algorithms for image transmission* Journal of Optical Communications. https://doi.org/10.1515/joc-2025-0363.
20. Z. Hasan, A. Hussain, A. Hussein, E. N. Abdulla, and H. H. Al-khaylani, *Deep Learning-Enabled Multi-Parameter Optimization for TWDM-PON Systems with Extended Reach*, Stat., optim. inf. comput., vol. 16, no. 4, pp. 3432–3453, Aug. 2026..
21. Mohammed ABFA, Al-hadeethi ST, Al-khaylani HH, Elwi TA, Abdulla EN. An investigation of success probability and fidelity of quantum repeater in asymmetry in midpoint placement in fiber-based quantum networks. J Opt 2025. https://doi.org/10.1007/s12596-025-02866-6. In press.
22. Priya Thakur and Anurag Rana, *A Symmetrical key Cryptography Analysis using Blowfish Algorithm,* Int. J. Eng. Res. V5, (2016).
23. A. GOVIND P, Fiber-Optic Communications Systems, Third Edition., Third Edit (John Wiley & Sons, Inc, 2002), Vol. 6.
24. A. D. and M. Frunzete, *Image Encryption Using Chaotic Maps : Development , Application , and Analysis,* Mathematics 13, 1–16 (2025).
25. Lina A. Salman, Essam N. Abdulla, Capacity and security enhancement in hybrid TWDM–FSO–NG–PON2 access network with self-protected fiber–FSO link paths effective against fiber breaks, Optik, Volume 350, 2026, 172734, ISSN 0030-4026, https://doi.org/10.1016/j.ijleo.2026.172734.
26. Y. Liu, J. Wang, J. Fan, and L. Gong, *Image encryption algorithm based on chaotic system and dynamic S-boxes composed of DNA sequences,* Multimed. Tools Appl. 75, 4363–4382 (2016).
27. D. R. I. M. Setiadi, S. Rustad, P. N. Andono, et al., *Digital image steganography survey and investigation (goal, assessment, method, development, and dataset),* Signal Process. 206, 108908 (2023).
28. Ali, Alaa Hussein, Abdulla, Essam N. and Al-Azawi, Razi J.. *Security and network performance analysis of coexistence TWDM – NG-PON2, GPON and 10G-EPON systems based on Hill Cipher* Journal of Optical Communications, 2025. https://doi.org/10.1515/joc-2025-0435.
29. Z. Abdellaoui, Y. Dieudonne, and A. Aleya, *Design, implementation and evaluation of a Fiber To The Home (FTTH) access network based on a Giga Passive Optical Network GPON,* Array 10, 100058 (2021).
30. W. Awalia and A. B. Pantjawati, *Performance Simulation of Fiber to the Home (FTTH) Devices Based on Optisystem,* IOP Conf. Ser. Mater. Sci. Eng. 384, (2018).
31. C. Kherici and M. Kandouci, *Performance study of a coexistence system in a PON network taking into account the stimulated scattering of Raman,* in 10th International Conference on Innovation, Modern Applied Science & Environmental Studies (ICIES'2022) (2022), Vol. 351, pp. 4–8.
32. R. Kaur and S. Singh, *Polarization multiplexing and hybrid modulation based bandwidth efficient NG-PON2 coexisting with GPON and XG-PON,* J. Opt. Technol. 88, 196 (2021).
33. Wang, Xingyuan & Zhu, Xiaoqiang & Wu, Xiangjun. (2017). Image encryption algorithm based on multiple mixed hash functions and cyclic shift. Optics and Lasers in Engineering. 107. 10.1016/j.optlaseng.2017.06.015.
34. Chen, Jun-xin & Zhang, Yu & Qi, Lin & Fu, Chong & Xu, Lisheng. (2017). Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression. Optics & Laser Technology. 99. 10.1016/j.optlastec.2017.09.008.
35. Wu, Xiangjun & Wang, Kunshu & Wang, Xingyuan & Kan, Haibin & Kurths, Jürgen. (2018). Color image DNA encryption using NCA map-based CML and one-time keys. Signal Processing. 148. 10.1016/j.sigpro.2018.02.028.
36. Chen, Jun-xin & Zhu, Zhi-liang & Fu, Chong & Yu, Hai & Zhang, Li-bo. (2015). A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. Communications in Nonlinear Science and Numerical Simulation. 20. 846–860. 10.1016/j.cnsns.2014.06.032.
37. Guesmi, Ramzi & Farah, M. & Kachouri, Abdennaceur & Samet, Mounir. (2015). A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2. Nonlinear Dynamics. 83. 10.1007/s11071-015-2392-7.