sustainability

MDPI

Article

Blockchain-Driven Image Encryption Process with Arithmetic Optimization Algorithm for Security in Emerging Virtual Environments

Manal Abdullah Alohali [1], Mohammed Aljebreen [2], Fuad Al-Mutiri [3], Mahmoud Othman [4], Abdelwahed Motwakel [5,*], Mohamed Ibrahim Alsaid [6], Amani A. Alneil [6] and Azza Elneil Osman [6]

[1] Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
[2] Department of Computer Science, Community College, King Saud University, P.O. Box 28095, Riyadh 11437, Saudi Arabia
[3] Department of Mathematics, Faculty of Sciences and Arts, King Khalid University, Muhayil Asir 61913, Saudi Arabia
[4] Department of Computer Science, Faculty of Computers and Information Technology, Future University in Egypt, New Cairo 11835, Egypt
[5] Department of Information Systems, College of Business Administration in Hawtat bani Tamim, Prince Sattam bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia
[6] Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia
* Correspondence: am.ismaeil@psau.edu.sa

Abstract: The real world is bounded by people, hospitals, industries, buildings, businesses, vehicles, cognitive cities, and billions of devices that offer various services and interact with the world. Recent technologies, including AR, VR, XR, and the digital twin concept, provide advanced solutions to create a new virtual world. Due to the ongoing development of information communication technologies and broadcast channels, data security has become a major concern. Blockchain (BC) technology is an open, decentralized, and transparent distributed database that can be maintained by the group. BC's major features are high credibility, decentralization, transparency, versatility, autonomy, traceability, anonymity, intelligence, reward mechanisms, and irreversibility. This study presents a blockchain-driven image encryption technique using arithmetic optimization with a fractional-order Lorenz system (BDIE-AOFOLS). The BDIE-AOFOLS technique uses the FOLS method, which integrates the Arnold map, tent map, and fractional Lorenz system. Besides this, an arithmetic optimization algorithm (AOA) was carried out for the optimum key generation process to achieve the maximum PSNR value. The design of an AOA-based optimal generation of keys for the FOLS technique determines the novelty of the current work. Moreover, the cryptographical pixel values of the images can be stored securely in the BC, guaranteeing image security. We compared the outcomes of the proposed BDIE-AOFOLS technique against benchmark color images. The comparative analysis demonstrated the improved security efficiency of the BDIE-AOFOLS technique over other approaches, with a mean square error of 0.0430 and a peak signal-to-noise ratio of 61.80 dB.

Keywords: virtual environment; blockchain; image encryption; cybersecurity; key generation; privacy

check for updates

Citation: Alohali, M.A.; Aljebreen, M.; Al-Mutiri, F.; Othman, M.; Motwakel, A.; Alsaid, M.I.; Alneil, A.A.; Osman, A.E. Blockchain-Driven Image Encryption Process with Arithmetic Optimization Algorithm for Security in Emerging Virtual Environments. *Sustainability* **2023**, *15*, 5133. https://doi.org/10.3390/su15065133

Academic Editors: Ming Hour Yang, Vijayalakshmi Murugesan and Mercy Shalinie Selvaraj

Received: 15 February 2023
Revised: 5 March 2023
Accepted: 7 March 2023
Published: 14 March 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

With the substantial growth of WiFi and 5G, digital images containing huge amounts of data are transferred frequently over multiple communication networks. In the meantime, tampering with and stealing digital images of high potential values are common [1]. Thus, the security and privacy of such images must be preserved before transmission. Typical digital image protection techniques include image encryption, digital watermarking,

secret-sharing, and information hiding. Among these techniques, image encryption is the most direct way [2]. The diffusion and permutation stages are the two main steps of digital image encryption. The permutation stage alters the pixel positions of the original images arbitrarily, while the diffusion stage requires that all pixel values of the original images be altered [3]. The main tools utilized in image encrypting contain frequency domain transformations, Chaos, evolutionary algorithms, neural networks (NNs), and DNA coding [4]. Sensitivity and Chaos's unpredictability in its primary state make it a widely used tool in image encrypting techniques [5].

Recently, authors have modeled numerous digital image encryption techniques related to NNs [6]. Cyber-attacks on automation on the Internet of Things (IoT) platform have far-reaching impacts. They can disturb manufacturing tasks, causing data loss and harming the quality and the standard of products [7]. Current solutions for image encryption do not assist those smart industries in which the peers are decentralized. There are several prevailing methods of image encryption. However, none of them complies with industrial needs. Smart industrial units are decentralized networks of interconnected IIoT devices that can share sensitive information, which is at risk of exposure [8]. The blockchain (BC) offers comprehensive solutions for decentralized devices, and its secure encrypted architecture is ideal for smart industrial units.

The history of BC technology (BCT) originates from Bitcoin or cryptocurrency. BC can act as a ledger that records every transferable transaction between individuals. This ledger can be decentralized; therefore, there are no centralized authorities [9]. It can be cryptographically immutable and secure. This ledger cannot be changed or deleted once modified. BC is a consensus-related mechanism, which means that all nodes verify the incidence of the transaction and derive a consensus regarding every unit of data before it can be positioned into a BCT-related ledger. BCT solves security issues. Owing to its dynamic properties, businesses quickly understood that BCT had a serious role in the IIoT [10]. This technology is implemented in industrial units to achieve security, regulatory complements, and transparency. BC can markedly transform the IIoT. It grants new functionality via smart contracts, security, and peer-to-peer device communications.

With the increased utilization of virtual reality and augmented reality in several industrial sectors, such as healthcare, education, and entertainment, the requirement of confidentiality in the context of sensitive images has become important. Encryption ensures that only authorized users have access to the images, defending the confidentiality of the data. It also ensures that the images remain unaltered during storage or transmission. This helps to maintain the data integrity of the images and ensures that they are reliable and trustworthy. Therefore, an image encryption technique with BC can be used to accomplish enhanced security.

With this motivation, this study develops blockchain-driven image encryption using arithmetic optimization with a fractional-order Lorenz system (BDIE-AOFOLS). The BDIE-AOFOLS procedure uses the FOLS technique, which is an integration of the Arnold map, tent map, and fractional Lorenz system. In addition, an arithmetic optimization algorithm (AOA) is carried out for the optimum key generation process, with the objective of achieving maximum PSNR value. The design of the AOA-based optimal generation of keys for the FOLS technique determines the novelty of the current work. Moreover, the cryptographical pixel values of the images can be stored securely in BC, guaranteeing image security. The experimental outcome investigation of the BDIE-AOFOLS technique was tested utilizing benchmark color images.

2. Related Works

Khayyat et al. [11] examined a novelty BC-enabled shark smell model, optimized with Hopfield Chaotic NN (SSOHCNN), for securing encryption on the IIoT platform. The proposed SSOHCNN approach offers a merged chaotic map (CM), which is combined in the form of staged logistic and tent maps to complete the primary processing of the image and improve the variable required for Arnold mapping. Neelakandan et al. introduced a

novel BC system with DL that enabled a secure medicinal data transmission and diagnosis (BDL-SMDTD) technique. Initially, the moth flame optimizer with ECC, known as the MFO-ECC approach, was utilized for the image encryption method, whereas better keys for ECC can be produced by utilizing the MFO system. In addition, BC technology has been employed for storing image encryption [12].

In one study [13], a novel fingerprint-related chaotic image encryption system was presented. The creation of key streams is influenced by the "fingerprints" of distributors instead of the plain-text form of images. Moreover, the BC infrastructure was implemented to ensure that the image encryption had been sent, following proper procedure, to the distributor. Furthermore, the distributor fingerprints embedded in the image encryption can be encoded by the anti-collusion code used for recording several fingerprints with a predetermined data length. Bhaskaran et al. [14] introduce a novel BC-allowed secure optimum lightweight cryptography-based image encryption (BC-LWCIE) system for Industry 4.0 platforms. The BC-LWCIE system supplies the cryptographic pixel value of image encryption from the BCT for ensuring privacy on the IIoT platform.

In another study [15], the authors established novel multiple share creation techniques with block technology for secure image management (MSCCBT-SIM) approaches. The MSCCBT-SIM technique permits the consumer to create a consensus without relying on central government input. In addition, the BC was utilized as a distributing data-storing process for generating a ledger intended to permit access to users and prevent third-party access to encrypted shares. Sammeta and Parthiban [16] introduced a new data control and secure medicinal information broadcast method, utilizing optimal multiple key-based homomorphic encryptions (MHE) with a Hyperledger BC (OMHE-HBC). The optimum key generation procedure from the MHE systems works by utilizing a hosted cuckoo optimization (HCO) technique. Mahesh Kumar et al. [17] presented a new multi-instance iris authentication model, BMIAE, for controlling malicious attacks on the broadcast channel and untrusted servers. BMIAE encrypted the iris template utilizing ElGamal to assure confidentiality, with a smart contract running on BC supports ensuring the integrity of templates and equivalent outcomes.

In a further study, Karim [18] suggested how to secure V2V and V2I transmission in the context of the VANET against a large number of cyberattacks. A hybrid cryptography system incorporating ABS and IBS, known as AIBS (attribute identity-based signature), was constructed to provide effective message authentication and integrity while ensuring vehicle privacy and safeguarding vehicular transmission. A JPEG image encryption with the adaptive key and run consistency of MCUs was developed by the authors of [19]. The chosen plain-text attack (CPA) was given here on this encryption system. First, the adaptive key can be reproduced from the encrypted image, such that the plain-text images with a similar adaptive key can be constructed. Second, the existence of the run consistency of MCUs (RCM) between the original image and the encrypted image facilitates rapid estimation. Sabir and Guleria [20] developed a novel multiple-image encryption system using an affine Hill cipher (AHC), reality-preserving 2D discrete fractional Hartley transform (RP2DFrHT), and a generalized 2D Arnold map (AM). In this work, three indexed images are attained from three color images. Third, AHC performs a strong degree of confusion and diffusion operations and RP2DFrHT provides a real domain output image. Fourth, the 2D AM dislocates the image pixel position.

3. The Proposed Model

In this study, we have developed a novel BDIE-AOFOLS system for a color image encryption process. The BDIE-AOFOLS technique mainly relies on the FOLS technique, which is an integration of an Arnold map, tent map, and fractional Lorenz system. In addition, an AOA was executed for an optimum key generation process, with the objective of achieving the maximum PSNR value. Figure 1 represents the workflow of the BDIE-AOFOLS approach.

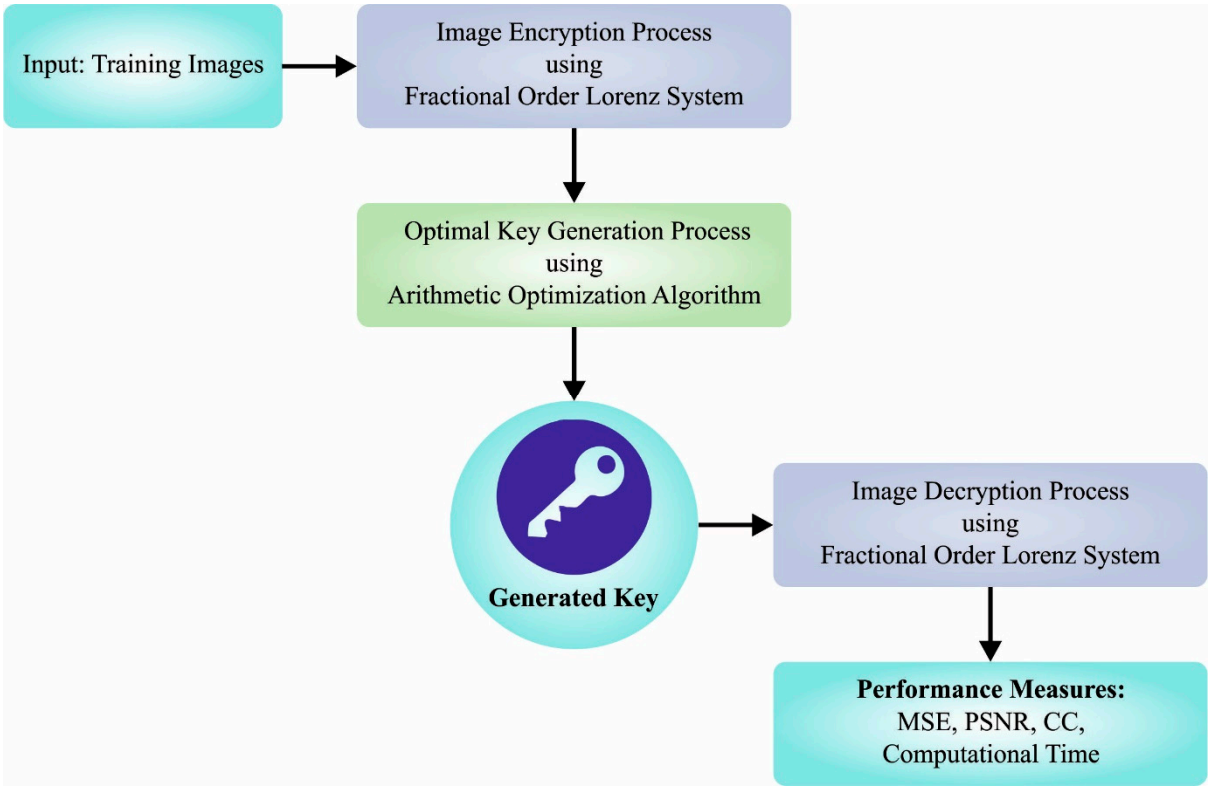


Figure 1. Workflow of the BDIE-AOFOLS approach.

3.1. Blockchain Technology in the BDIE-AOFOLS Technique

In the presented technique, the cryptographic pixel values of images can be stored on the BC, thereby assuring the privacy and security of images. BC is a beneficial ledger for assuring data quality. It has generated "controlling operations" for numerous decentralized industrial gadgets and has performed peer-to-peer interactions between globally decentralized gadgets. Moreover, BC offers amenability along with authority for all independent systems; simultaneously, it resolves security problems. In industrial fields, a private BC has been used for ensuring security. The phrase "Hyperledger fabric" refers to an environment that hinges on BC and satisfies the necessity for an IIoT platform. This is helpful in numerous fields, such as transportation, healthcare, large-scale IoT data, and the supply chain. Moreover, BC aids in accomplishing decentralization, privacy, and trust. BC also enables simple connections with numerous gadgets.

Figure 2 shows the basic framework of the BC. The client or server computer acts as a node and then commences making the connections.

The nodes exchange encrypted data with other peer nodes, without any invader being able to steal the information. They may transfer the information to a central location or distributed gadget, which can be connected to other gadgets. The hashing value specifies every transaction that happened in the block.

The transactions will be integrated together to generate a block, which will be added to the chain next to the confirmation from the endorsed node. The operation starts if the client begins to submit a proposal. The transaction procedures employ two types of peers: committer peers and endorsers. The certificate authority (CA) allows the credentials to the client as is compulsory for user applications for gaining permission to submit novel communications.

To start a novel transaction, the user application transfers the transaction proposals to a peer, thereby updating or reading the ledger. The peer could then read it and validate the authorization policy. Finally, the committer–peer makes an asynchronous announcement that is relevant to the transaction's rank.

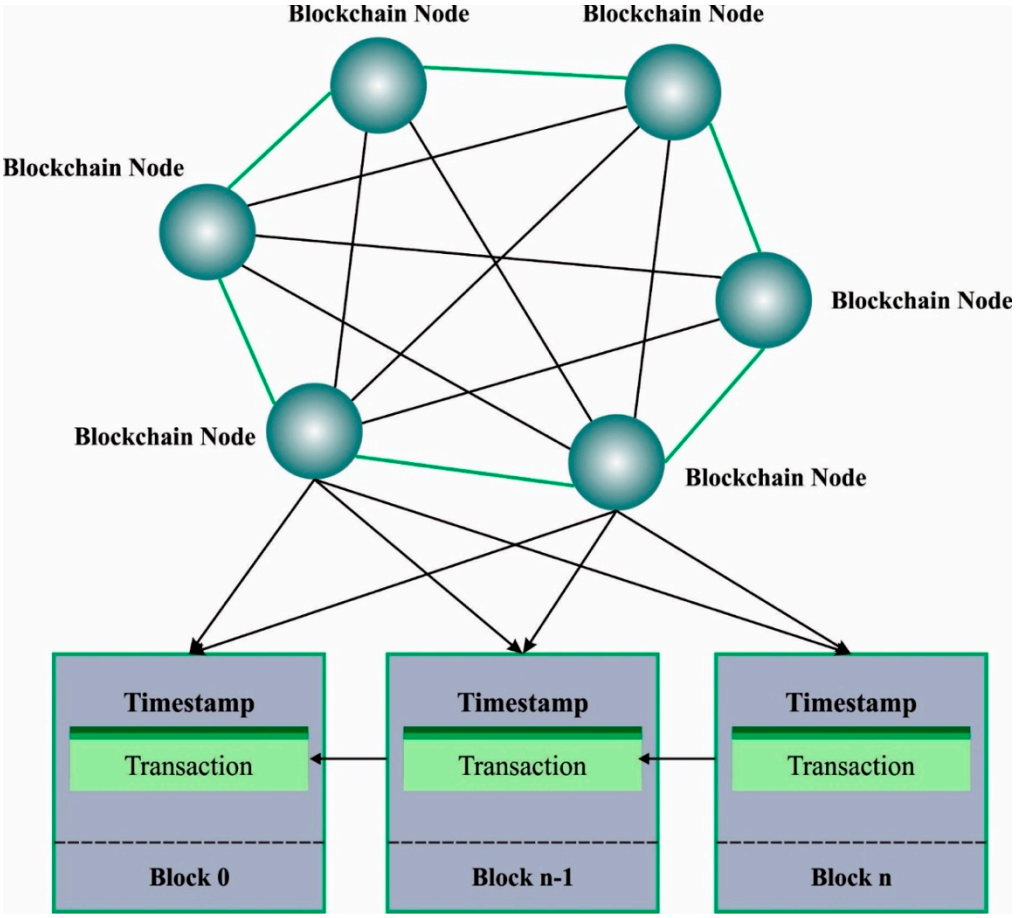


Figure 2. The structure of a blockchain.

3.2. Image Encryption Using the FOLS Technique

To encrypt the color images, a FOLS technique is used in this work. In this study, a novel color image encryption technique dependent upon a fractional order chaotic system was introduced with the combination of three chaotic systems (a tent map (TM), an Arnold map (AM), and a fractional Lorenz system (FLS)) [21]. Initially, the plain color images are separated into their R, B, and G layers. In the scrambling phase, these three layers are scrambled with the AM, among which the first value of initial scrambling is the key, and the first values of the remaining two scrambles are the R and G layers.

The gray value of RGB is molded and is later applied as the initial value of FLS. Following this, add-mode diffusion is performed. Finally, an encrypted image is achieved. The plain image is represented as A, the pixel matrix size was M $\times$ N $\times$ 3, and the encryption technique is determined by the following process:

Step 1: Enter the A plain image and the key, K, and assume that the size of A is $M \times N \times 3$. Read the first value and parameter of the AM in K, then apply an AM for scrambling the plain image R layer. Choose the latter 2 pixels of the R layer after scrambling, obtaining the gray value as a parameter of AM while scrambling the G layer, and apply a similar function to scrambling the B layer for obtaining image P_1.

$$P_1 = \left\{ \begin{array}{c} R \\ G \\ B \end{array} \right\} = \left\{ \begin{array}{cccc} r(1), r(2), r(3), & \cdots & r(m) \\ g(1), g(2), g(3), & \cdots & g(m) \\ b(1), b(2), b(3), & \cdots & b(m) \end{array} \right\} \quad m = MIN \tag{1}$$

Step 2: Read the first value of TM $X(0)$ from the key, K. The TM is reiterated 800 times; the initial 300 transition conditions are abandoned and take the state value, which is defined by K_r.

$$K_\zeta = [x_t(200), x_t(300), x_t(400), x_t(500)]) \tag{2}$$

Step 3: Use Equation (3) for turning K_ζ into s_1 and s_2 coordinates for placing the pixel in P_1.

The FLS is reiterated MlV and $2MN$ times, respectively, with a small perturbation of the model every 3000 times, to obtain a size of $3 \times MlV$ and $3 \times 2MlV$ for the novel pseudo-random sequences S_1 and S_2, which are transmuted by Equation (4) to password K_1 and K_2.

$$\begin{cases} s_1 = (x_t(300) \times 100 - floor(x_t(300) \times 100)) \times 10^6 mod\ m \\ s_2 = (x_t(500) \times 100 - floor(x_t(500) \times 100)) \times 10^6 mod\ m \end{cases} \tag{3}$$

$$K_o = \begin{bmatrix} K_{o1} \\ K_{o2} \end{bmatrix} = \begin{bmatrix} R_{s1}, & G_s & B_{s1} \\ R_{s2}, & G_{s2} & B_{s2} \end{bmatrix} \tag{4}$$

$$\begin{cases} K_1(j) = \left(floor\left(S_1(j) \times 2^{16}\right) mod 256\right) + 1 \\ K_2(j) = \left(floor\left(S_2(j) \times 2^{16}\right) mod 256\right) + 1 \end{cases} \tag{5}$$

Step 4: Utilize the password, K_1, to spread the data between the layers of images; this can be computed, as follows:

$$\begin{cases} r'(i) = r(i) \oplus k_1(1,i) \oplus b(i) \\ g'(i) = g(i) \oplus k_1(2,i) \oplus r,(i) \\ b'(i) = b(i) \oplus k_1(3,i) \oplus g'(i) \end{cases}, i = 1, 2, \cdots, MIN \tag{6}$$

In Equation (6), $r'(i),\ g'(i), b'(i)$ denotes the pixel value after diffusing for the initial time. After pixel diffusion between the layers, the plain data of all the layers are diffused to the other 2 layers. This phase could improve the model's capability for resisting a chosen-plain attack.

3.3. Optimal Key Generation Using AOA

The aim of key generation is to offer the secure encryption and decryption of data. An optimum key generation process ensures that the keys utilized for encryption and decryption are random, unique, and sufficiently complex, making it hard for attackers to decrypt the data. The system generates the keys rapidly and precisely, with no need for high computation resources. Therefore, in this work, an AOA was executed for the optimal key generation process, with the objective of achieving the maximum PSNR value [22]. AOA operates following the distribution behavior of mathematical operations, such as multiplication (M), division (D), subtraction (S), and addition (A), which aims at finding the optimum solution covering a large number of search spaces.

The AOA operation depends on four major processes—inspiration, initialization, exploration, and exploitation. The steps that are adopted to establish an optimum solution by applying the AOA technique are given below.

Step 1: Inspiration is based on the operation of a simple arithmetical operator to determine better values when subjected to specific conditions from a large number of candidate solutions. The applicability of an arithmetic operator is used to find a solution for the arithmetical problem.

Step 2: Initialization, where the candidate solution can be determined as follows:

$$Y(t) = \begin{Bmatrix} y_{11} & \cdots & y_{1i} & y_{1,n-1} & y_{1n} \\ y_{21} & \cdots & y_{2i} & y_{2,n-1} & y_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ y_{m-1,1} & y_{m-1,2} & y_{m-1,i} & y_{m-1,n-1} & y_{m-1,n} \\ y_{m1} & y_{m2} & y_{mi} & y_{m,n-1} & y_{mn} \end{Bmatrix}. \quad (7)$$

We then calculate the math optimizer acceleration (moa) coefficient:

$$moa(Iter_{current}) = \alpha_{\min} + Iter_{current} \times \left(\frac{\alpha_{\max} - \alpha_{\min}}{Iter_{\max}} \right). \quad (8)$$

In Equation (8), $\alpha_{\max}$ and $\alpha_{\min}$ denote the maximal and minimal values of the accelerated function, $Iter_{current}$ shows the existing iteration, and , $Iter'_{\max}$ indicates the maximal iteration.

Step 3: The exploration operators of AOA are the D and M operators. The exploration process recognizes the near-optimum solution that should be attained after various iterations. The D and M operators are used to support the exploitation phase via effective transmission. The higher dispersion possibility does not allow this exploration operator to approach the optimum solution.

In this phase, the division and multiplication search strategies implement the location update and are given by the following equation:

If $r_1 > moa$, then

$$y_{ij}(Iter_{current} + 1) = \begin{cases} y_{j_Best} \div (mop + \varepsilon) \times \left(\left(UB_j - LB_j \right) \times \lambda + LB_j \right), \ r_2 < 0.5 \\ y_{i_Best} \times (mop) \times \left((UB_i - LB_i) \times \lambda + LB_i \right), \ Otherwise \end{cases} \quad (9)$$

In Equation (9), r_1 and r_2 denote the smaller random integers; the D operator implements when $r_2 < 0.5$, while the M operators do not implement until the D' operator finishes the existing process. The better solution that has been assessed so far is 'y'_{j_Besi}. λ' characterizes the control parameter for altering the searching process, ε' denotes the small number, LB_j and UB_j indicate the lower and upper bounds of the existing location, and 'mop' represents the math optimizer probability shown in the following equation:

$$mop(Iter_{current}) = \left(1 - \frac{Iter_{current}^{\frac{1}{\beta}}}{Iter_{\max}^{\frac{1}{\beta}}} \right). \quad (10)$$

In Equation (10), β' indicates the sensitivity parameter determining the exploration accuracy.

Step 4: Exploitation can be performed by the S and A operators that move through the searching space and attain a more highly dense solution. Owing to a lower dispersion, the above two operators are more effective in approaching the better t solution point than the higher dispersion operators, D and M.

The addition and subtraction search strategies evolve the location of the near-optimum solution by moving through the deep dense region and are updated as follows:

If $r_1 < moa(Iter_{current})$ then

$$y_{ij}(Iter_{current} + 1) = \begin{cases} y_{j_Best} - (mop) \times \left(\left(UB_j - LB_j \right) \times \lambda + LB_j \right), \ r_3 < 0.5 \\ y_{j_Besi} + (mop) \times \left(\left(UB_j - LB_j \right) \times \lambda + LB_j \right), \ Otherwise \end{cases} \quad (11)$$

The S and A operators assist in overcoming the existence of local minima; this exploitation process facilitates the exploration method to accomplish an optimum solution by retaining the diversity of candidate solutions. The hierarchical order of the D, M, S,

and A operators evaluate the location of the near-optimum solution and overcome the optimum stagnation occurrence toward the end of the final iterations. The AOA system was utilized in the initialization of the public as well as secret keys contained in the encryption procedure. This ensures that the method that PSNR obtained is improved. The fitness function of the AOA system for the FOLS approach is provided, as follows:

$$Fitness\ function = \max\{PSNR\}. \quad (12)$$

4. Performance Validation

In this section, the experimental validation of the BDIE-AOFOLS approach was tested utilizing benchmark color images. Figure 3 shows the sample images. In Table 1, the encryption results of the BDIE-AOFOLS technique are clearly depicted. The results indicated that the input image is properly encrypted and reconstructed without any loss of information. It is evident that the BDIE-AOFOLS technique has obtained increasing values of PSNR and CC. At the same time, the BDIE-AOFOLS technique has obtained decreasing values of MSE under all images.



Figure 3. The sample images.

Table 2 and Figure 4 illustrate the information entropy values (IEV) outcomes of the BDIE-AOFOLS with the existing models [11]. The results indicated that the BDIE-AOFOLS approach has reached enhanced IEV values under all channels. For the sample, on the R channel, the BDIE-AOFOLS technique has reached a higher IEV of 7.9995, while the SSOHCNN, WOAHCNN, GWOHCNN, and HCNN models have obtained lower IEV levels of 7.9992, 7.9941, 7.9938, and 7.9931, respectively. Meanwhile, on the G channel, the BDIE-AOFOLS method has reached a higher IEV of 7.9998, while the SSOHCNN, WOAHCNN, GWOHCNN, and HCNN methods have gained lower IEV levels of 7.9990, 7.9935, 7.9921, and 7.9922, respectively. Furthermore, on the B channel, the BDIE-AOFOLS approach has reached a higher IEV of 7.9997, while the SSOHCNN, WOAHCNN,

GWOHCNN, and HCNN methods have attained lower IEV levels of 7.9992, 7.9933, 7.9930, and 7.9915, respectively.

Table 1. Encryption outcome of the BDIE-AOFOLS approach.

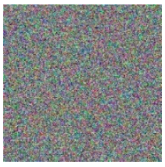
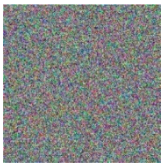
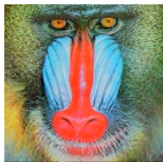
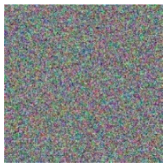
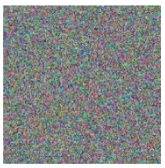
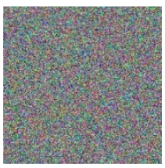
Original Image	Encrypted Images	Decrypted Images	MSE	PSNR (dB)	CC (%)
			0.059	60.42	99.68
			0.082	58.99	99.89
			0.043	61.80	99.66
			0.088	58.69	99.87
			0.110	57.72	99.93

Table 2. IEV analysis of BDIE-AOFOLS approach with existing algorithms.

Methods	Information Entropy Values		
	R_Channel	G_Channel	B_Channel
BDIE-AOFOLS	7.9995	7.9998	7.9997
SSOHCNN	7.9992	7.9990	7.9992
WOAHCNN	7.9941	7.9935	7.9933
GWOHCNN	7.9938	7.9921	7.9930
HCNN	7.9931	7.9922	7.9915

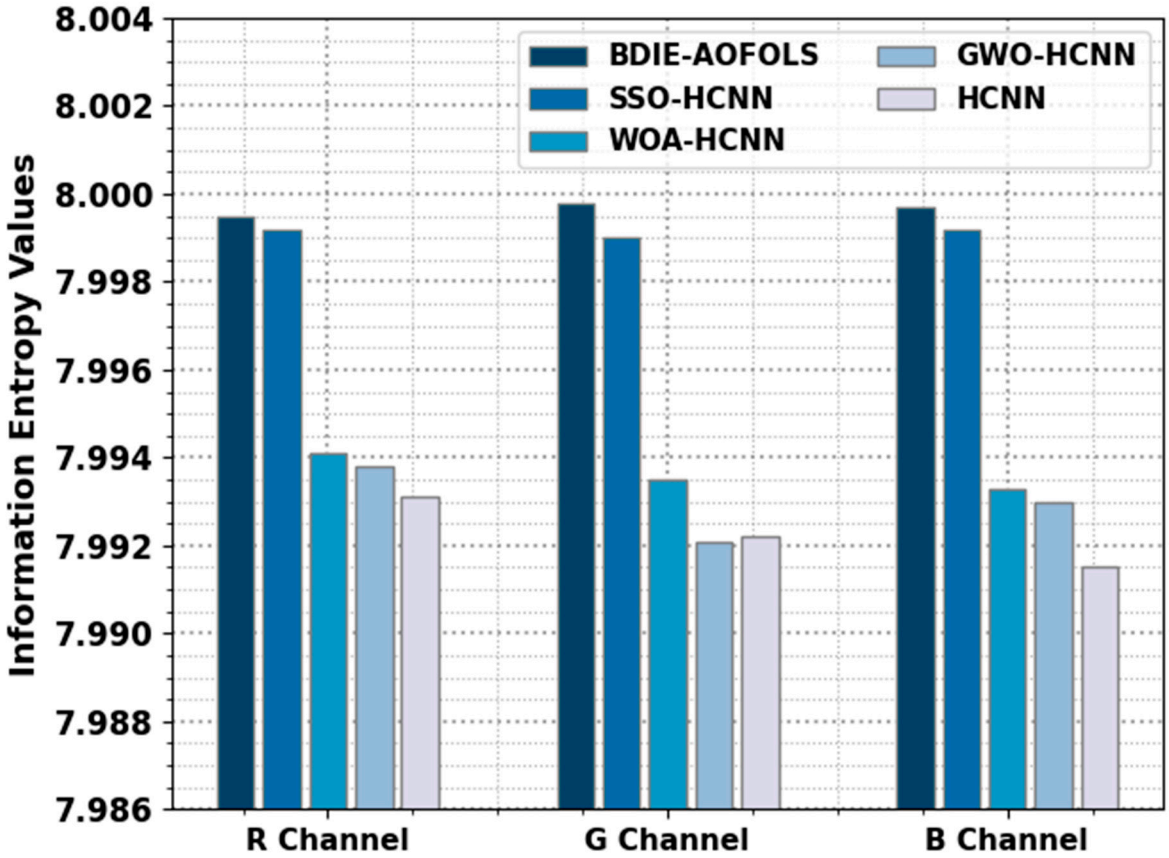


Figure 4. IEV analysis of the BDIE-AOFOLS system with existing algorithms.

Table 3 reveals a comparative MSE and PSNR inspection of the BDIE-AOFOLS with recent models. A comparative analysis of the BDIE-AOFOLS with existing approaches in terms of MSE is reported in Figure 5. The results represent the improvised outcomes of the BDIE-AOFOLS model using minimal values of MSE. For instance, on IMG-1, the BDIE-AOFOLS technique attains a reduced MSE value of 0.0590, while the SSOHCNN, WOAHCNN, GWOHCNN, and HCNN models have resulted in improved MSE values of 0.0636, 0.1850, 0.2875, and 1.5733, respectively.

Table 3. Comparative analysis of BDIE-AOFOLS system with the existing algorithms, under varying test images.

Test Images	BDIE-AOFOLS		SSOHCNN		WOAHCNN		GWOHCNN		HCNN	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
IMG-1	0.0590	60.42	0.0636	60.10	0.1850	55.46	0.2875	53.54	1.5733	46.16
IMG-2	0.0820	58.99	0.0841	58.88	0.1724	55.77	0.2312	54.49	2.0708	44.97
IMG-3	0.0430	61.80	0.0487	61.26	0.2027	55.06	0.2352	54.42	2.2278	44.65
IMG-4	0.0880	58.69	0.0926	58.46	0.2123	54.86	0.2613	53.96	2.0717	44.97
IMG-5	0.1100	57.72	0.1117	57.65	0.1798	55.58	0.2318	54.48	2.5501	44.07

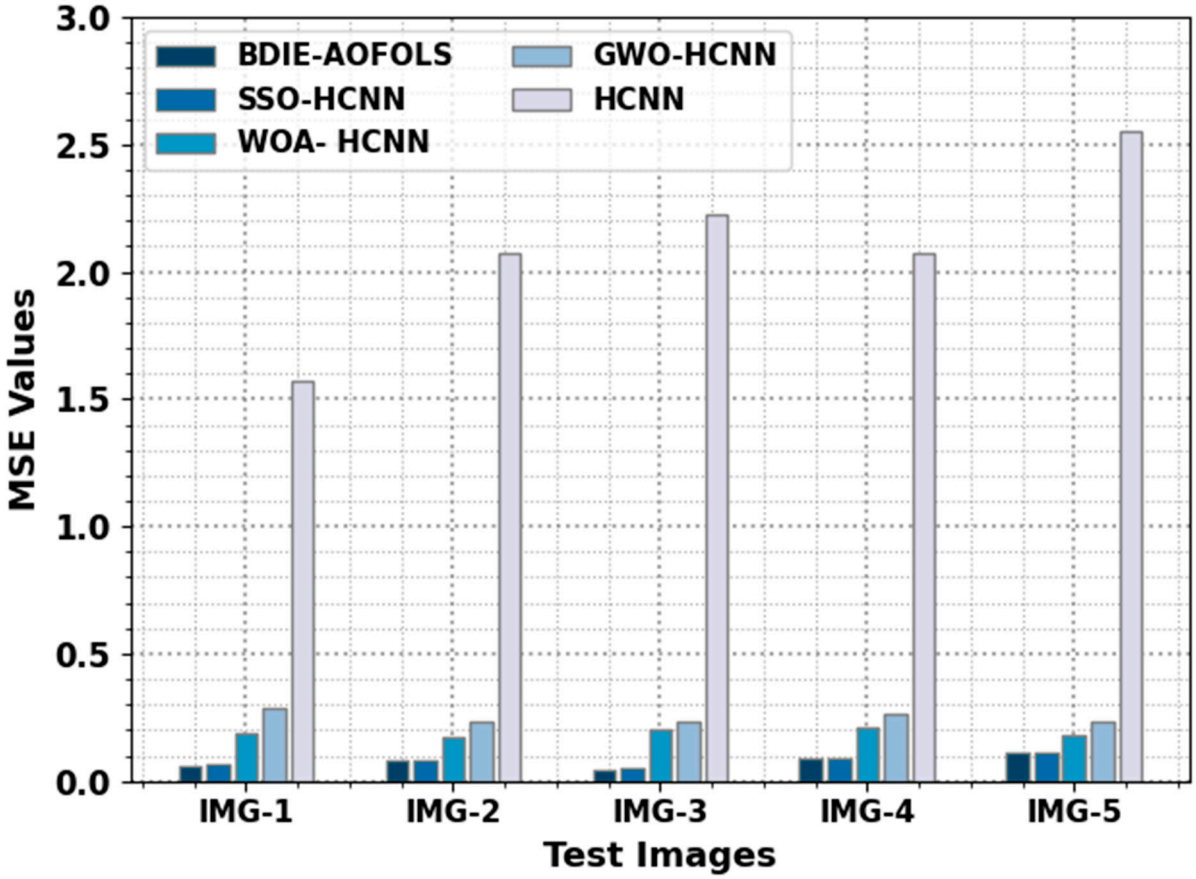


Figure 5. MSE analysis of the BDIE-AOFOLS approach with various test images.

Along with these findings, for IMG-3, the BDIE-AOFOLS method achieved a reduced MSE of 0.0430, while the SSOHCNN, WOAHCNN, GWOHCNN, and HCNN methods resulted in increased MSE values of 0.0487, 0.2027, 0.2352, and 2.2278, respectively. Finally, for IMG-5, the BDIE-AOFOLS algorithm attained a reduced MSE of 0.1100, while the SSOHCNN, WOAHCNN, GWOHCNN, and HCNN approaches resulted in increased MSE values of 0.1117, 0.1798, 0.2318, and 2.5501, respectively.

In Figure 6, a comprehensive PSNR analysis of the BDIE-AOFOLS with recent algorithms is reported. The obtained values show the superior performance of the BDIE-AOFOLS technique, with improved PSNR values. For instance, for IMG-1, the BDIE-AOFOLS technique accomplished an enhanced PSNR value of 60.42 dB, while the SSO-HCNN, WOAHCNN, GWOHCNN, and HCNN models obtained decreased PSNR values of 60.10 dB, 55.46 dB, 53.54 dB, and 46.16 dB, respectively. Meanwhile, for IMG-3, the BDIE-AOFOLS method accomplished an enhanced PSNR value of 61.80 dB, while the SSOHCNN, WOAHCNN, GWOHCNN, and HCNN methods achieved decreased PSNR values of 61.26 dB, 55.06 dB, 54.42 dB, and 44.65 dB, respectively. Eventually, for IMG-5, the BDIE-AOFOLS technique achieved an enhanced PSNR value of 57.72 dB, while the SSOHCNN, WOAHCNN, GWOHCNN, and HCNN methods attained decreased PSNR values of 57.65 dB, 55.58 dB, 54.48 dB, and 44.07 dB, respectively.

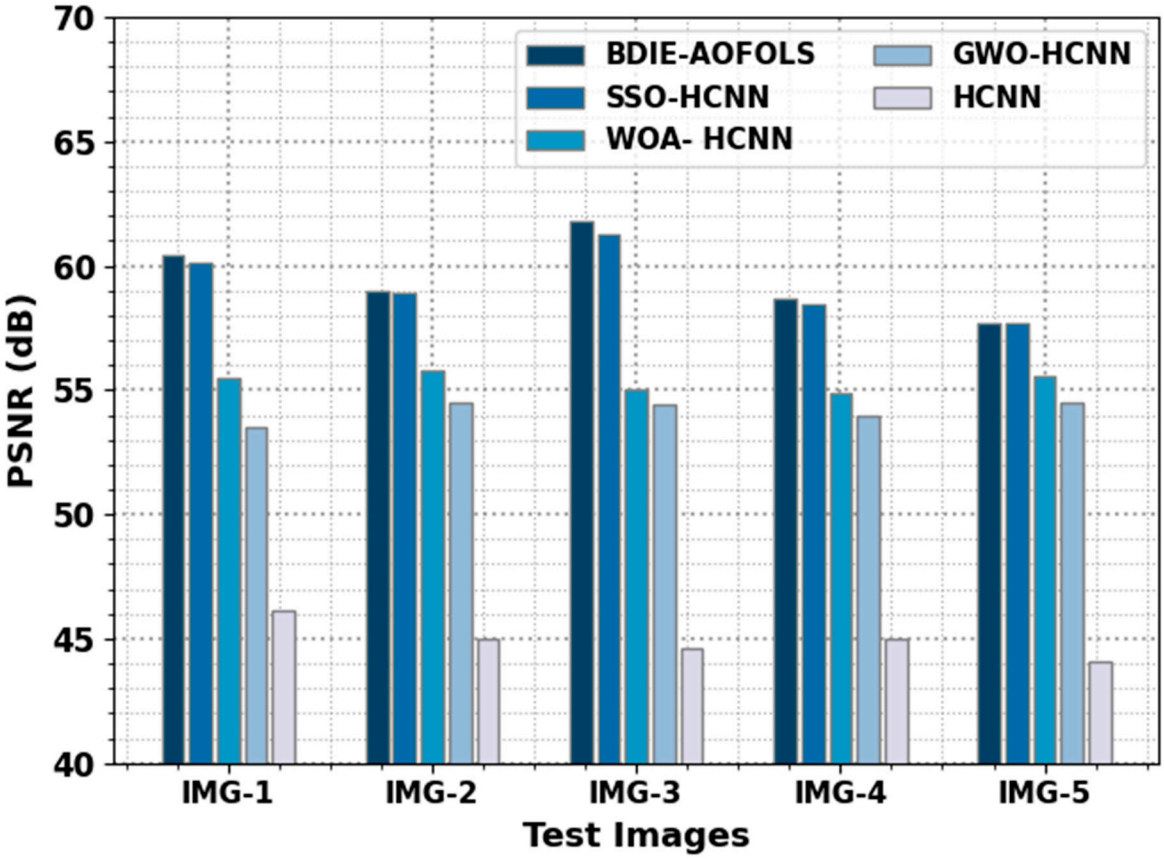


Figure 6. PSNR analysis of the BDIE-AOFOLS approach with various test images.

In Table 4 and Figure 7, a detailed CC comparison of the BDIE-AOFOLS approach with recent methods is given. The obtained values show the superior performance of the BDIE-AOFOLS method, with improved CC values. For example, for IMG-1, the BDIE-AOFOLS technique accomplished an enhanced CC value of 99.68%, while the SSO-HCNN, WOAHCNN, GWOHCNN, and HCNN methods obtained decreased CC values of 99.60%, 99.40%, 99.30%, and 98.90%, respectively. Meanwhile, for IMG-3, the BDIE-AOFOLS approach achieved an enhanced CC value of 99.72%, while the SSOHCNN, WOAHCNN, GWOHCNN, and HCNN methods showed decreased CC values of 99.58%, 99.46%, 99.35%, and 99.21%, accordingly. Eventually, for IMG-5, the BDIE-AOFOLS method accomplished an enhanced CC value of 99.93%, while the SSOHCNN, WOAHCNN, GWOHCNN, and HCNN methods obtained decreased CC values of 99.90%, 99.70%, 99.10%, and 98.80%, respectively.

Table 4. CC analysis of the BDIE-AOFOLS approach with the existing algorithms, with various test images.

	Correlation Coefficient (CC %)				
Test Images	**BDIE-AOFOLS**	**SSOHCNN**	**WOAHCNN**	**GWOHCNN**	**HCNN**
IMG-1	99.68	99.60	99.40	99.30	98.90
IMG-2	99.89	99.80	99.50	99.20	99.00
IMG-3	99.72	99.70	99.40	99.00	98.70
IMG-4	99.87	99.58	99.46	99.35	99.21
IMG-5	99.93	99.90	99.70	99.10	98.80

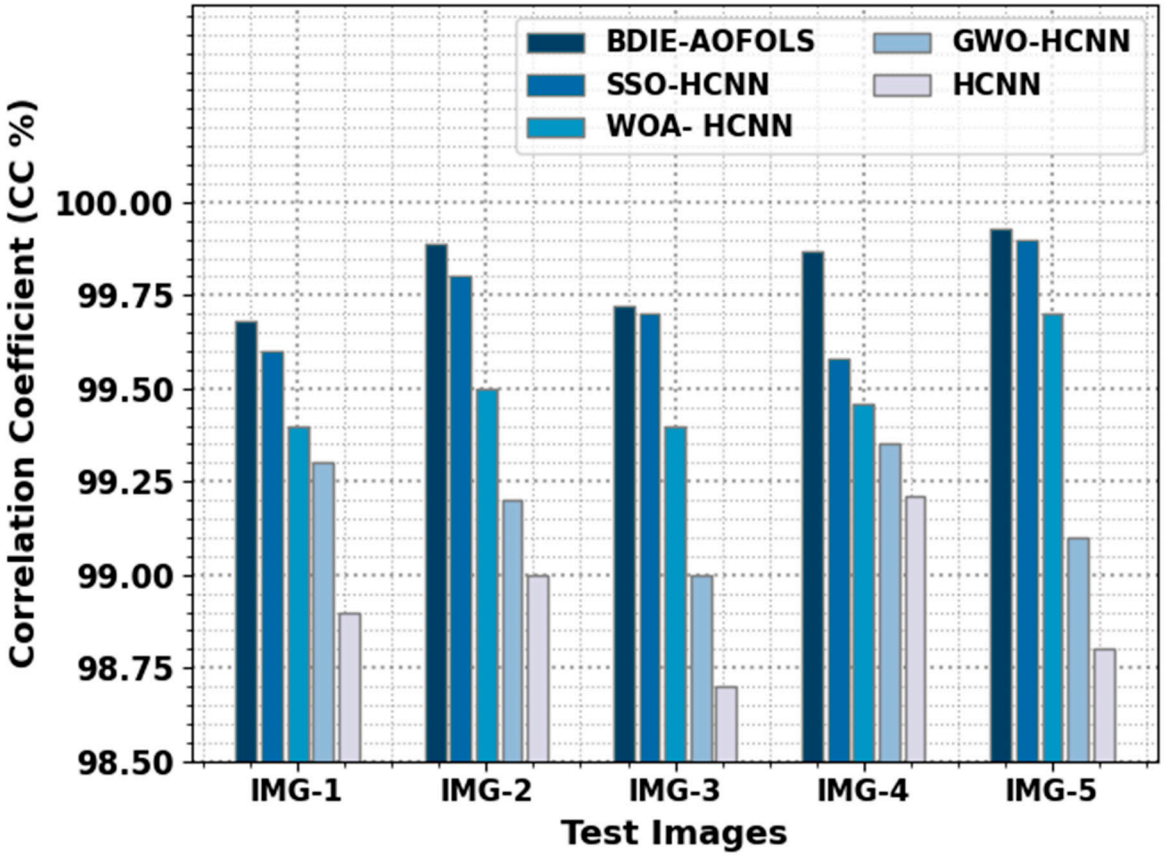


Figure 7. CC analysis of the BDIE-AOFOLS approach, with the various test images.

A comparative analysis of the BDIE-AOFOLS with existing methods in terms of CT is reported in Table 5 and Figure 8. The results represent the improvised outcomes of the BDIE-AOFOLS approach, with minimal values of MSE. For example, for IMG-1, the BDIE-AOFOLS method reached a reduced CT value of 1.164 s, while the SSOHCNN, WOAHCNN, GWOHCNN, and HCNN methods resulted in increased CT values of 1.192 s, 1.619 s, 2.117 s, and 2.837 s, respectively. In addition, for IMG-3, the BDIE-AOFOLS method attained a reduced CT value of 1.528 s, while the SSOHCNN, WOAHCNN, GWOHCNN, and HCNN methods resulted in increased CT values of 1.549 s, 1.774 s, 1.910 s, and 2.718 s, respectively.

Table 5. CT analysis of the BDIE-AOFOLS system with the existing algorithms, using the various test images.

	Computational Time (s)				
Test Images	**BDIE-AOFOLS**	**SSOHCNN**	**WOAHCNN**	**GWO-HCNN**	**HCNN**
IMG-1	1.164	1.192	1.619	2.117	2.837
IMG-2	1.260	1.284	1.448	1.810	2.274
IMG-3	1.528	1.549	1.774	1.910	2.718
IMG-4	1.103	1.123	1.638	2.162	2.118
IMG-5	1.190	1.214	1.736	1.973	2.161

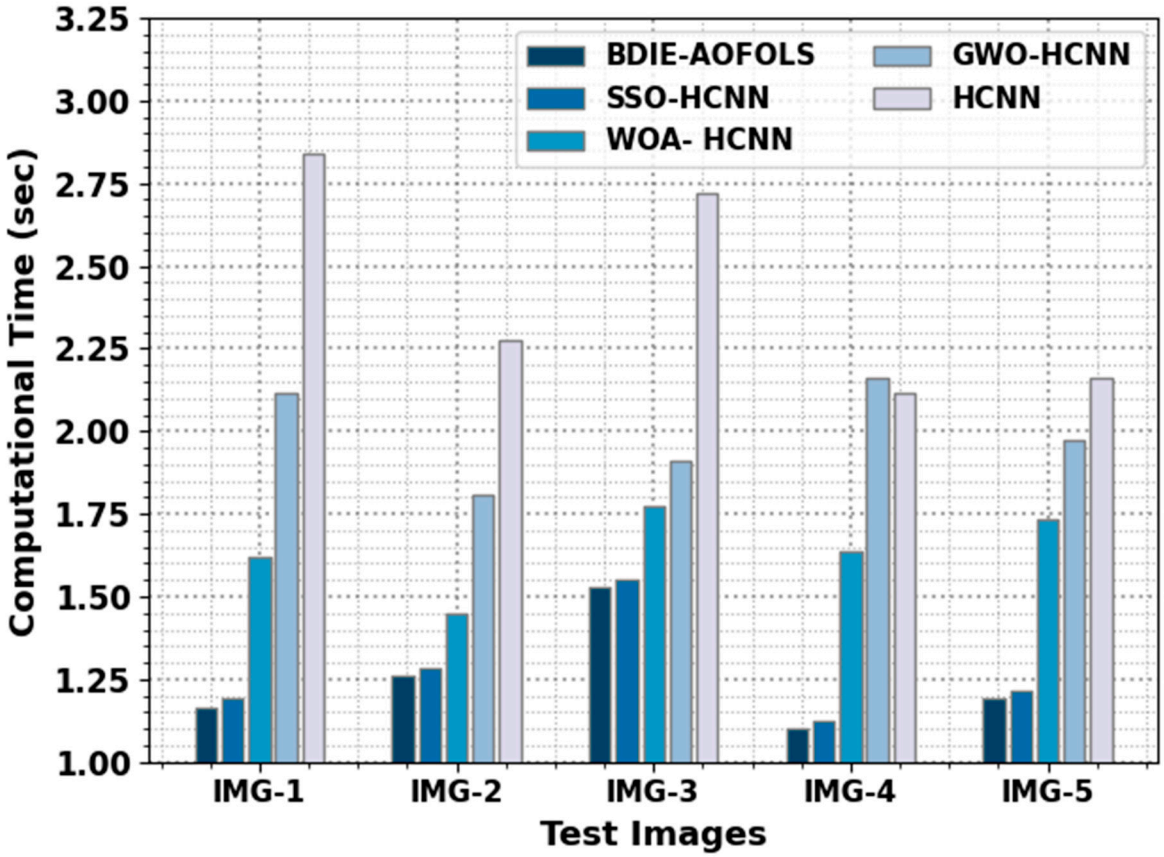


Figure 8. CT analysis of the BDIE-AOFOLS approach, using the various test images.

Finally, for IMG-5, the BDIE-AOFOLS method attains a reduced CT value of 1.190 s, while the SSOHCNN, WOAHCNN, GWOHCNN, and HCNN methods have resulted in increased CT values of 1.214 s, 1.736 s, 1.973 s, and 2.161 s, respectively. These results emphasized the improvement offered by the suggested technique over other existing models. The proposed image encryption with BC offers several benefits, including enhanced security, transparency, and tamper-proof storage. It is particularly useful for protecting sensitive images in virtual environments where the confidentiality and integrity of data are critical.

5. Conclusions

In this study, we have developed a new BDIE-AOFOLS technique for color image encryption processing. The BDIE-AOFOLS technique secures the images using three major processes, namely, BC technology, image encryption, and optimal key generation. At the initial stage, the FOLS technique was employed for the encryption of the images. Next, AOA was conducted to complete the optimum key generation process, with the objective of achieving the maximum PSNR value. Finally, BC was used to securely store the cryptographical pixel values of the images and thereby guarantee image security. The experimental outcome investigation of the BDIE-AOFOLS technique demonstrated the promising performance of the BDIE-AOFOLS technique over other approaches, with a mean square error of 0.0430 and a peak signal-to-noise ratio of 61.80 dB. In the future, the optimal key generation process can be employed to explore the use of quantum key generation algorithms and technologies to provide even more secure and efficient key generation processes.

Author Contributions: Conceptualization, M.A.A.; Methodology, M.A.; Software, M.O. and A.A.A.; Validation, M.A., F.A.-M., M.O., A.M., M.I.A. and A.A.A.; Formal analysis, F.A.-M.; Investigation, F.A.-M.; Resources, M.O.; Data curation, A.A.A.; Writing—original draft, M.A.A., M.A., A.M., M.I.A. and A.E.O.; Writing—review & editing, M.A., F.A.-M., M.O., A.M., M.I.A., A.A.A. and A.E.O.; Visualization, F.A.-M.; Supervision, M.A.A.; Project administration, A.M.; Funding acquisition, M.A.A., F.A.-M. and A.M. All authors have read and agreed to the published version of the manuscript.

Funding: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through Large Group Project under grant number (35/44). Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R330), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. Research Supporting Project number (RSP2023R459), King Saud University, Riyadh, Saudi Arabia. This study is supported via funding from Prince Sattam bin Abdulaziz University project number (PSAU/2023/R/1444).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare that they have no conflict of interest. The manuscript was written via the contributions of all authors. All authors have given approval for the final version of the manuscript.

References

1. Pustokhina, I.V.; Pustokhin, D.A.; Shankar, K. Blockchain-Based Secure Data Sharing Scheme Using Image Steganography and Encryption Techniques for Telemedicine Applications. In *Wearable Telemedicine Technology for the Healthcare Industry*; Academic Press: Cambridge, MA, USA, 2022; pp. 97–108.
2. Acharya, M.; Sharma, R.S. A Novel Image Encryption Based on Feedback Carry Shift Register and Blockchain for Secure Communication. *Int. J. Appl. Eng. Res.* **2021**, *16*, 466–477.
3. Khan, A.A.; Laghari, A.A.; Gadekallu, T.R.; Shaikh, Z.A.; Javed, A.R.; Rashid, M.; Estrela, V.V.; Mikhaylov, A. A drone-based data management and optimization using metaheuristic algorithms and blockchain smart contracts in a secure fog environment. *Comput. Electr. Eng.* **2022**, *102*, 108234. [CrossRef]
4. Shankar, K.; Elhoseny, M.; Perumal, E.; Ilayaraja, M.; Sathesh Kumar, K. An Efficient Image Encryption Scheme Based on Signcryption Technique with Adaptive Elephant Herding Optimization. In *Cybersecurity and Secure Information Systems*; Springer: Cham, Switzerland, 2019; pp. 31–42.
5. Subathra, G.; Antonidoss, A. A Multiobjective Based Encryption Scheme for Content-Based Addressing in Blockchain. In Proceedings of the 2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2–4 December 2021; pp. 702–709.
6. Banik, A.; Laiphrakpam, D.S.; Agrawal, A.; Patgiri, R. Secret image encryption based on chaotic system and elliptic curve cryptography. *Digit. Signal Process.* **2022**, *129*, 103639. [CrossRef]
7. Singh, K.N.; Singh, A.K. Towards integrating image encryption with compression: A survey. *ACM Trans. Multimed. Comput. Commun. Appl. (TOMM)* **2022**, *18*, 1–21. [CrossRef]
8. efa Tunçer, S.; Karakuzu, C. Performance Analysis of Chaotic Neural Network and Chaotic Cat Map Based Image Encryption. *J. Comput. Inf. Sci.* **2022**, *5*, 37. [CrossRef]
9. Chen, Y.; Chen, H.; Han, M.; Liu, B.; Chen, Q.; Ma, Z.; Wang, Z. Miner revenue optimization algorithm based on Pareto artificial bee colony in blockchain network. *EURASIP J. Wirel. Commun. Netw.* **2021**, *2021*, 146. [CrossRef]
10. Khan, P.W.; Byun, Y. A blockchain-based secure image encryption scheme for the industrial Internet of Things. *Entropy* **2020**, *22*, 175. [CrossRef] [PubMed]
11. Khayyat, M.M.; Khayyat, M.M.; Abdel-Khalek, S.; Mansour, R.F. Blockchain enabled optimal Hopfield Chaotic Neural network based secure encryption technique for industrial internet of things environment. *Alex. Eng. J.* **2022**, *61*, 11377–11389. [CrossRef]
12. Neelakandan, S.; Beulah, J.R.; Prathiba, L.; Murthy, G.L.N.; Irudaya Raj, E.F.; Arulkumar, N. Blockchain with deep learning-enabled secure healthcare data transmission and diagnostic model. *Int. J. Model. Simul. Sci. Comput.* **2022**, *13*, 2241006. [CrossRef]
13. Li, R. Fingerprint-related chaotic image encryption scheme based on blockchain framework. *Multimed. Tools Appl.* **2021**, *80*, 30583–30603. [CrossRef]
14. Bhaskaran, R.; Karuppathal, R.; Karthick, M.; Vijayalakshmi, J.; Kadry, S.; Nam, Y. Blockchain Enabled Optimal Lightweight Cryptography Based Image Encryption Technique for IIoT. *Intell. Autom. Soft Comput.* **2022**, *33*, 1593–1606. [CrossRef]
15. Padmavathi, U.; Rajagopalan, N. Blockchain enabled emperor penguin optimizer based encryption technique for secure image management system. *Wirel. Pers. Commun.* **2022**, *127*, 2347–2364. [CrossRef]

16. Sammeta, N.; Parthiban, L. Data Ownership and Secure Medical Data Transmission using Optimal Multiple Key-Based Homomorphic Encryption with Hyperledger Blockchain. *Int. J. Image Graph.* **2021**, 2240003. [CrossRef]
17. Mahesh Kumar, M.; Prasad, M.V.; Raju, U.S.N. BMIAE: Blockchain-based multi-instance iris authentication using additive ElGamal homomorphic encryption. *IET Biom.* **2020**, *9*, 165–177. [CrossRef]
18. Karim, A. Development of secure Internet of Vehicle Things (IoVT) for smart transportation system. *Comput. Electr. Eng.* **2022**, *102*, 108101. [CrossRef]
19. He, H.; Yuan, Y.; Ye, Y.; Tai, H.M.; Chen, F. Chosen plaintext attack on JPEG image encryption with adaptive key and run consistency. *J. Vis. Commun. Image Represent.* **2023**, *90*, 103733. [CrossRef]
20. Sabir, S.; Guleria, V. Multi-layer security based multiple image encryption technique. *Comput. Electr. Eng.* **2023**, *106*, 108609. [CrossRef]
21. Chen, J.; Li, C.; Yang, X. Chaos synchronization of the distributed-order Lorenz system via active control and applications in chaotic masking. *Int. J. Bifurc. Chaos* **2018**, *28*, 1850121. [CrossRef]
22. Zheng, R.; Jia, H.; Abualigah, L.; Liu, Q.; Wang, S. Deep ensemble of slime mold algorithm and arithmetic optimization algorithm for global optimization. *Processes* **2021**, *9*, 1774. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.