Heliyon 10 (2024) e25257

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

Research article

Chaotic image encryption algorithm with improved bonobo optimizer and DNA coding for enhanced security

Ahmed S. Almasoud [a], Bayan Alabduallah [b,*], Hamed Alqahtani [c], Sumayh S. Aljameel [d], Saud S. Alotaibi [e], Abdullah Mohamed [f]

[a] Department of Information Systems, College of Computer and Information Sciences, Prince Sultan University, Saudi Arabia
[b] Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh, 11671, Saudi Arabia
[c] Department of Information Systems, College of Computer Science, Center of Artificial Intelligence, Unit of Cybersecurity, King Khalid University, Abha, Saudi Arabia
[d] SAUDI ARAMCO Cybersecurity Chair, Department of Computer Science, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam, 31441, Saudi Arabia
[e] Department of Information Systems, College of Computing and Information System, Umm Al-Qura University, Saudi Arabia
[f] Research Centre, Future University in Egypt, New Cairo, 11845, Egypt

ARTICLE INFO

Keywords:
Cryptography
Digital image encryption
Chaotic concepts
DNA encoding
Bonobo optimizer

ABSTRACT

Image encryption involves applying cryptographic approaches to convert the content of an image into an illegible or encrypted format, reassuring that illegal users cannot simply interpret or access the actual visual details. Commonly employed models comprise symmetric key algorithms for the encryption of the image data, necessitating a secret key for decryption. This study introduces a new Chaotic Image Encryption Algorithm with an Improved Bonobo Optimizer and DNA Coding (CIEAIBO-DNAC) for enhanced security. The presented CIEAIBO-DNAC technique involves different processes such as initial value generation, substitution, diffusion, and decryption. Primarily, the key is related to the input image pixel values by the MD5 hash function, and the hash value produced by the input image can be utilized as a primary value of the chaotic model to boost key sensitivity. Besides, the CIEAIBO-DNAC technique uses the Improved Bonobo Optimizer (IBO) algorithm for scrambling the pixel position in the block and the scrambling process among the blocks takes place. Moreover, in the diffusion stage, DNA encoding, obfuscation, and decoding process were carried out to attain encrypted images. Extensive experimental evaluations and security analyses are conducted to assess the outcome of the CIEAIBO-DNAC technique. The simulation outcome demonstrates excellent security properties, including resistance against several attacks, ensuring it can be applied to real-time image encryption scenarios.

1. Introduction

With the progress of network science and the multimedia industries, data transmission has become the main choice for many people where Digital images are stored or transmitted via public channels [1]. Thus, data security is of great importance [2]. Due to vast quantities of data in digital images, higher redundancy, and stronger relationship between neighboring pixels and is not effective, and

* Corresponding author.
E-mail address: bialabdullah@pnu.edu.sa (B. Alabduallah).

https://doi.org/10.1016/j.heliyon.2024.e25257
Received 12 July 2023; Received in revised form 3 December 2023; Accepted 23 January 2024

it has been found that the classical data encryption technique has many technical defects [3]. When compared to other classical encryption algorithms, the experimental outcome shows that image encryption depends on the concept of chaos and has better features [4]. In many aspects, the study of Chaos has made tremendous progress [5]. Chaos meets the requirement of image encryption due to its features of chaos, like inherent randomness, and maximum sensitivity to primary conditions and control parameters in recent times, chaos research has become increasingly popular [6]. Pseudo-randomness, unpredictability, and high sensitivity to primary value are the features of a chaotic system making it well-suited for image encryption methods [7]. Also, the image encryption approach depends on chaos is extensively studied [8]. Generally, this encryption technique involves two different steps: scrambling and diffusion [9]. Shuffling is used to reduce the relationship between pixels, and Diffusion is used to make the pixel value equally distributed [10].

Image scrambling and diffusion can be integrated to encrypt the images to accelerate the encryption technique [11]. The scrambling process splits the plaintext images into pixel blocks, later changing the pixel value while scrambling the pixel block through spatiotemporal chaos [12]. As well, low energy consumption, high storage density, and large parallelism of DNA make it unique during encryption [13]. The Lorenz system can be used for scrambling the DNA sequence matrix encoded via the plaintext images, later the attained DNA sequence is operated circularly [14]; lastly, DNA decoding is conducted for obtaining the ciphertext images [15]. The reverse procedure of encryption is called Decryption [16]. Also, based on optimization, there exists an image encryption technique that enhances encryption effects by choosing the proper fitness function (FF) to improve the information entropy or enhance the generated key to the ciphertext images [17]. With the optimization technique, the information entropy or pixel relation of the ciphertext images is closer to the ultimate values which considerably decreases the data contained in the ciphertext images [18]. Thus, it is nearly possible to get the plaintext data from the ciphertext images without the key [19]. A few metaheuristic optimization techniques include the ant colony algorithm (ACO), genetic algorithm (GA), particle swarm optimization (PSO), differential evolution (DE), and so on [20].

This study introduces a new Chaotic Image Encryption Algorithm with an Improved Bonobo Optimizer and DNA Coding (CIEAIBO-DNAC) for enhanced security. The presented CIEAIBO-DNAC technique involves different processes such as initial value generation, substitution, diffusion, and decryption. Primarily, the key is related to the input image pixel values by the MD5 hash function, and the hash values produced by the input image can be utilized as the primary value of the chaotic model to boost key sensitivity. Besides, the CIEAIBO-DNAC technique uses the Improved Bonobo Optimizer (IBO) algorithm for scrambling the pixel position in the block and the scrambling process among the blocks takes place. Moreover, in the diffusion stage, DNA encoding, obfuscation, and decoding process were carried out to attain encrypted images. Extensive experimental evaluations and security analyses are conducted to assess the performance of the CIEAIBO-DNAC technique.

2. Related works

Alohali et al. [21] introduce a Blockchain Driven Image Encryption using an arithmetic optimization algorithm (AOA) with the Fractional-Order Lorenz System (BDIE-AOFOLS) algorithm. This proposed model employed the Fractional-Order Lorenz System (FOLS) model that incorporates the Fractional Lorenz, Arnold Map, and Tent Map schemes. Additionally, an AOA is performed for the optimum key generation procedure for achieving the optimum value of peak signal-to-noise ratio (PSNR). Zhu et al. [22] presented a Chaotic Digital Image encrypting system that depends on a maximized Artificial Fish Swarm (AFS) approach and coding of DNA. Firstly, the key is related to the normal image pixels via the MD5 hash function, and the value of the hash produced by the normal images is utilized as the primary value of the hyperchaotic scheme to enhance the key sensitivity. Then, the AFS approach is implemented to disorganize the pixel position in the block.

The authors in Ref. [23], introduced an image encryption technique that depends on the upgrading procedures of PSO and Hyperchaotic Complex Lü (HCL) systems. Particularly, a mechanism of key generation incorporated with the Secured Hash approach of 256 hash is initially presented for generating the HCL scheme's primary values. Later, the plain images are disorganized by the velocity and position upgrading procedure of the PSO method. Khaitan et al. [24] suggested a public key crypto scheme that integrates the Chaos Tent Map (CTM) function along with an Improved Salp Swarm Optimization (ISSO) approach for the image's decrypting and encrypting process. This ISSO approach is upgraded by enforcing mutation and crossover for generating a decrypting key. This encrypting system encompasses a circular shit operation and a permutation, which are controlled by control parameters and chaos-based keys. At the time of the encrypting procedure, an eight-bit shift catalogue is utilized with XOR operation to improve the cypher image's randomness.

Maniyath and Thanikaiselvan [25] present an analytical research model for proposing a state-of-the-art framework, in which the Deep Neural Network (DNN) is utilized for the optimization of the plain encryption method's achievement. The vigorousness of the optimizing principles is additionally supplemented with a chaotic map notion for improved safety accomplishments. Ferdush et al. [26] proposed a technique that utilizes the Genetic Algorithm (GA) for an improved pixel value encryption and PSO to enhance the process of optimization. This technique is segmented into two sectors. Firstly, the plain RGB images are implemented for the primary populace and later the GA is employed for image encryption. Secondly, the PSO model is employed for determining the best-encryption images. Lastly, the best images are put under a re-encryption process still an optimal value is achieved.

Zeng and Wang [27] present a scheme for Hyperchaotic Image Encryption (HIE) which is based on Cellular Automata (CA) and PSO algorithms. At first, to enhance the capacity for resisting the outbreaks of the plaintext, the hyperchaotic scheme's primary conditions are produced by the values of hash functions that are closely associated with the plaintext images yet to undergo encryption. Additionally, PSO's fitness is the correlative coefficient among the image's neighboring pixels. In Ref. [28], a fusion technique is proposed by implementing the Tent Chaotic Mapping (TCM) and DNA Sequence (DNA-S) models. At first, the initial and TCM images are put under the encryption process distinctly by implementing the DNA-S model. Later, the logical XOR operator is enforced on the models

and the encrypted imageries are generated by employing chaotic schemes.

3. The proposed model

In this study, we have focused on the development of the CIEAIBO-DNAC for enhanced security. The presented CIEAIBO-DNAC technique involves different processes such as initial value generation, substitution, diffusion, and decryption. Fig. 1 displays the workflow of the CIEAIBO-DNAC methodology.

3.1. Initial value generation

Consider the plain image size A as $(M \times N)$, and split as to $(M \times N)/(m \times n)$ blocks by $(m \times n)$. In general, after the MD5 hash, a 128-bit summary will be attained. Although there is a 1-bit difference, the summary created would be quite distinct. Thus, this stage is to relate the main procedure with plaintext images that increase security. Using Eq. (8), the 128-bit summary was divided into 8 blocks.

$$K = k_1, k_2 \ldots k_7, k_8, \tag{1}$$

The four primary values of Chen's hyper-chaotic model are attained based on the calculation process. Amongst them, $x_0, y_0, z_0,$ *and* w_0 are the initial values, $\oplus$ is for operation.

$$\begin{cases} x_0^{'} = x0 + \dfrac{k_1 \oplus k_2}{256}, \\ y_0^{'} = y_0 + \dfrac{k_3 \oplus k_4}{256}, \\ z_0^{'} = z_0 + \dfrac{k_5 \oplus k_{60}}{256}, \\ w_0^{'} = w_0 + \dfrac{k_7 \oplus k_8}{256}, \end{cases} \tag{2}$$

3.2. Design of IBO algorithm

BO algorithm is a recent optimization technique derived from the social and reproductive behaviours of bonobos are promiscuous,

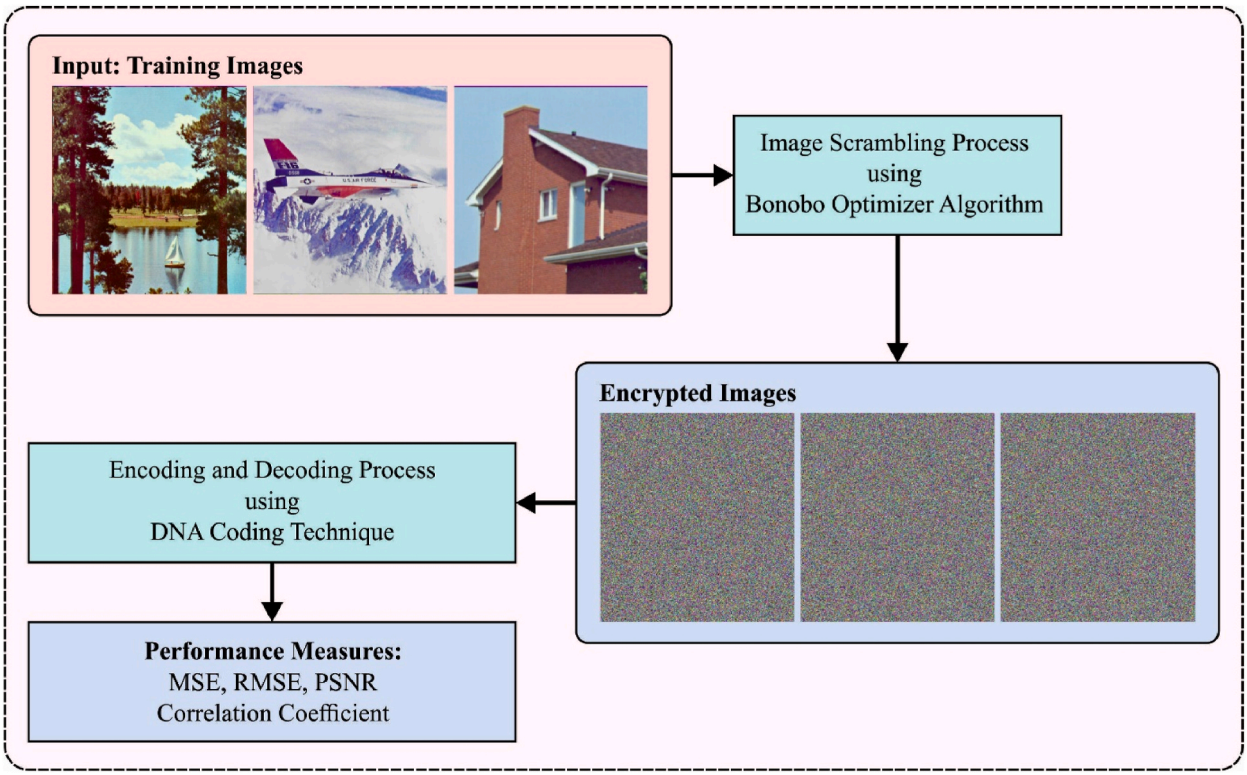

Fig. 1. Workflow of CIEAIBO-DNAC method.

consortship, restrictive, and extra-group mating strategies [29]. This mating strategy was subjected to the living conditions of the bonobos are the positive phase (*PP*) and negative phase (*NP*). Here, *PP* defines peaceful living where mating occurs. In contrast, NP expresses a hard life. Here, every solution is named X_B and the fittest solution is X_B^{α}. The mathematical expression of BO is given as follows.

The solution update of BO relies on the mating strategy exposed to the existing stage. The bonobo lives in smaller groups with dissimilar sizes (unpredictable and random) and the community re-joins to the main community. Therefore, a bonobo for mating was chosen based on this behavior. The mathematical formula for the maximal amount of temporary subgroups N_{stub} is formulated below:

$$N_{sub} = \max\left(2, (\varepsilon_{sub} \times N)\right) \tag{3}$$

In Eq. (3), N denotes the overall amount of the population and ε_{sub} represents the subgroup size factor. When the fittest bonobo in the subgroups with respect to the FF is greater than X_B^i, afterwards, it can be chosen as X_B^P, otherwise, an arbitrary one must be chosen from the subgroups to search for the bonobo X_B^P selected to mate with X_B^i to construct the newest bonobo X_B^{new}.

Afterwards accomplishing the chosen bonobo X_B^P, four mating tactics are utilized from the BO for creating a novel bonobo X_B^{new} via *PP* or *NP*. In the case of *PP*, restrictive and promiscuous mating have a high probability (ρ_{ph}) of existence. In contrast to *NP*, the probability (ρ_{ph}) of extra-group and consortship mating is high.

The new bonobo was generated by Eq. (4) at the Promiscuous and Restrictive Mating stage:

$$X_B^{new} = X_B^i + r_1 \times S_{coef}^{\alpha} \times \left(X_B^{\alpha} - X_B^i\right) + (1 - r_1) \times S_{coef}^P \times c_{flag} \times \left(X_B^i - X_B^P\right)s \tag{4}$$

Now r_1 denotes the random integer within $[0, 1]$. S_{coef}^{α} and S_{coef}^P show the sharing coefficient for X_B^{α} the alpha bonobo and X_B^P the chosen bonobo, correspondingly, c_{flag} shows the flag value that is equivalent to -1 or 1 for promiscuous and restrictive mating, correspondingly. The controlling variable with respect to ρ_{ph} the phase probability is utilized for adopting the mating strategies [30]. At first, ρ_{ph} is fixed as 0.5. Therefore, once an arbitrary integer r is shown that lesser than or equivalent to ρ_{ph}, a novel bonobo is generated by using restrictive and promiscuous mating, or else, extra-group and consortship mating can be used.

Once r is higher than ρ_{ph}, consortship, and extra-group mating take place. But a newly generated random value r_2 within zero and one, is utilized with the probability of extra-group mating ρ_{xg} to characterize the existence of extra-group mating once r_2 is lesser than or equivalent to ρ_{xg}:

$$X_B^{new} = \begin{cases} X_B^i + \beta_1 \times \left(X^i{}_{\max} - X_B^i\right), & X_B^{\alpha} \geq X_B^i, and\ r_4 \leq \rho_d \\ X_B^i - \beta_2 \times \left(X_B^i - X^i{}_{\min}\right), & X_B^{\alpha} \geq X_B^i, and\ r_4 > \rho_d \\ X_B^i - \beta_1 \times \left(X_B^i - X^i{}_{\min}\right), & X_B^{\alpha} < X_B^i, and\ r_4 \leq \rho_d \\ X_B^i + \beta_2 \times \left(X^i{}_{\max} - X_B^i\right), & X_B^{\alpha} < X_B^i, and\ r_4 > \rho_d \end{cases} \tag{5}$$

$$\begin{aligned} \beta_1 &= e^{\left(r_4^2 + r_4 - \frac{2}{r_4}\right)} \\ \beta_2 &= e^{\left(-r_4^2 + 2r_4 - \frac{2}{r_4}\right)} \end{aligned} \tag{6}$$

Where r_3 and r_4 denote randomly generated integers within zero and one and $r_4 \neq 0$. ρ_d shows the directional probability with an initial value that is equivalent to 0.5. β_1 and β_2 represent the intermediate parameters within zero and one. $X^i{}_{\min}$ and $X^i{}_{\min}$ denote the values of upper and lower boundaries.

When r_2 is higher than ρ_{xg}, the newest bonobo was generated by the consortship mating strategy:

$$X_B^{new} = \begin{cases} X_B^i + c_{flag} \times e^{-r_5} \times \left(X_B^i - X_B^P\right), & c_{flag} = 1\ or\ r_6 \leq \rho_d \\ X_B^P, Otherwise \end{cases} \tag{7}$$

In Eq. (7), r_5 and r_6 denote the two randomly generated integers.

During the iterative process, the BO parameter was updated based on the fittest solution X_B^{α} at all the iterations, but once there was an enhancement in the concluding solution to the prior iteration, the parameters of BO were updated.

The PP count raises with the increment of one $(PP_{cont} = PP_{cont} + 1)$ and the count of *NP* is fixed as zero $(NP_{coni} = 0)$. Furthermore, $\rho_{xg} = \rho_{xg\_initml}$ and $\rho_{ph} = 0.5 + Cp$ where Cp denotes the amount of change and is evaluated as $Cp = \min\left(0.5, PP_{coni} \times r\psi\right)$ where rcp denotes the rate of changes in the phase [31]. Furthermore $\rho_d = \rho_{ph}$ and

$$\varepsilon_{sub} = \min\left(\varepsilon_{sub\_\max}\left(\varepsilon_{sub_{initial}} + PP_{cont} \times rcp^2\right)\right) \tag{8}$$

where $\varepsilon_{sub_{initial}} = 0.5 * \varepsilon_{sub\_\max}$.

At the same time, the parameters of BO were updated if there was no improvement:

$$NP_{cont} = NP_{cont} + 1 \text{ and } PP_{cont} = 0,$$

$$Cp = \min(0.5, NP_{cont} \times rcp),$$

$$\rho_{xg} = \rho_{xg\_initial} \min\left(0.5, \rho_{xg\_initial} + NP_{cont} \times rcp^2\right),$$

and

$$\varepsilon_{sub} = \min\left(\varepsilon_{sub\_\max}, \left(\varepsilon_{sub_{initial}} - NP_{cont} \times rcp^2\right.\right.$$

With the population-based technique, BO has certain challenges including falling in the local optima. However, BO based on quasi-opposition-based learning and three leaders' selection are introduced. Three leaders are used for increasing the diversity of the solution, rather than utilizing the alpha bonobo X_B^{α} (better solution) for updating the newest bonobo X_B^{new} and ignoring the other fittest solutions, as follows

$$\begin{gathered} X_B^{\alpha} = w_1 \times X_{best_1} + w_2 \times X_{best_2} + w_3 \times X_{best_3} \\ w_1 = \frac{r_7}{r_7 + r_8 + r_9}, w_2 = \frac{r_8}{r_7 + r_8 + r_9}, \text{and } w_1 = \frac{r_9}{r_7 + r_8 + r_9} \end{gathered} \tag{9}$$

Where r_7, r_8, and r_9 denote the random integer between zero and one. Opposition-based learning (OBL) was more commonly used for improving optimization approaches. In the IBO algorithm, an improvement could be accomplished by applying the candidate solution. The opposite solution of BO model X_B^i was formulated as follows:

$$X_B^{qnew} = C + r_{10}\left(C - \overline{X_B^{new}}\right) \tag{10}$$

In Eq. (10), r_{10} denotes the random value within $[0, 1]$, and C shows the middle point between $X^i{}_{\min}$ and $X^i{}_{\max}$ that is evaluated using Eq. (11):

$$C = \frac{X^i{}_{\min} + X^i{}_{\max}}{2} \tag{11}$$

Furthermore, $\overline{X_B^{new}}$ shows the opposite solution that is evaluated as follows can be calculated as follows:

$$\overline{X_B^{new}} = X^i{}_{\min} + X^i{}_{max - B^{new}} \tag{12}$$

3.3. Substitution

Consider that the greater the influence is, the nearer the pixel is, in the digital image, and the image block processing could process all the pixels and attain further information. The images are block-processed. When the plaintext image size is $(M \text{x} N)$, then it is split as $(M \text{x} N)/(m \text{x} n)$ sub-blocks. N must be an integer multiple of n, *and* M must be an integral multiple of m, Or else, the missing part would be spontaneously filled in black, hence the encrypting process will not have the limitations of image size. Image pixel can be attained depending on the filling place of all the sub-blocks. The pixel of all the image blocks is exchanged by the pixel of other image blocks after the block from the conversion of all the sub-blocks.

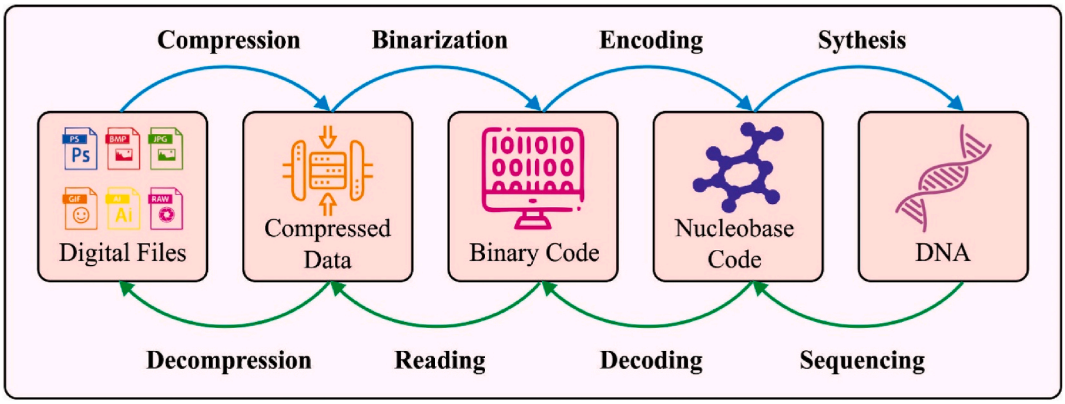

Fig. 2. DNA Encoding process.

3.4. Diffusion

The diffusion method could considerably improve the capability of the encryption scheme to resist differential and statistical attacks. We select DNA coding technology with low energy consumption, high density, and strong parallel computing ability for diffusion operation to attain the best diffusion effects. Fig. 2 represents the flow of the DNA encoding method. The specific operation is given below.

Step1 Chen's hyper-chaotic system repeats $N_0 + M \times N$ times to attain sequences $X_1,\ Y_1,\ Z_1,$ and W_1, and later discard the first N_0 value to remove the transient effects of the chaotic model.

Step2 Evaluate all the elements of $X_1,\ Y_1,\ Z_1$, and W_1 based on Eqs. (13)–(16) for obtaining four vectors $R_i,\ R_y,\ R_z$, and R.

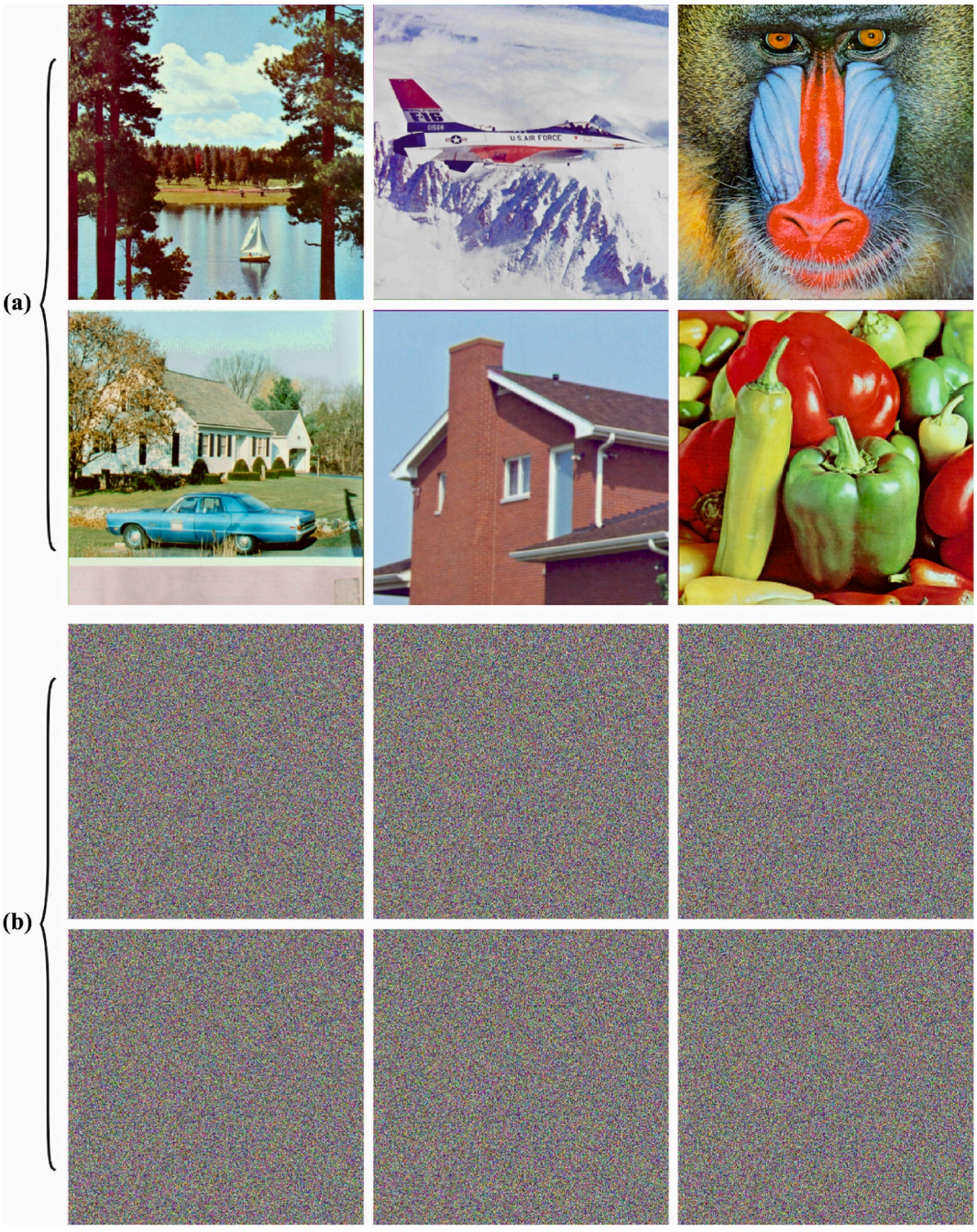

Fig. 3. Sample images.

$$R_x(i) = mod\left(floor\left(X_1(i) \times 10^{14}\right), 8\right) + 1, \tag{13}$$

$$R_y(i) = mod\left(floor\left(Y_1(i) \times 10^{14}\right), 8\right) + 1, \tag{14}$$

$$R_z(i) = mod\left(floor\left(Z_1(i) \times 10^{14}\right), 8\right) + 1 \tag{15}$$

$$R(i) = mod\left(floor\left(W_1(i) \times 10^{14}\right), 256\right), \tag{16}$$

where $X_1(i)$, $Y_1(i)$, $Z_1(i)$, and $W(i)$ denotes the i^{th} elements of X_1, Y_1, Z_1, and W_1, $i \in [1, M \times N]$, $floor(a)$ shows the rounding down of a. The results of *the mod* (a, b) are the remainder divided by b.

Step3 Enlarge the scrambling matrix Pl into a vector (i), $i \in [1, M \times N]$. Determine variable *temp* and *i*, where the first value of *i* is 1, and the first value of *temp* is given in Eq. (17).

$$temp = mod\left(\sum_{i=1}^{M \times N} P1, 256\right), \tag{17}$$

Step4 based on the DNA coding principles equivalent to $R_z(i)$, perform DNA coding on $R(i)$ to attain $DNA\_R(i)$, simultaneously, based on the DNA coding rules respective to R_y, DNA code $E(i)$ to attain $DNA\_E(i)$. Next, the XOR of $DNA\_R(i)$ and $DNA\_E(i)$ are calculated for getting New-E(i).

Step5 Decode $New\_E(i)$ to get $de\_New\_E(i)$ based on the DNA coding rules equivalent to $R_x(i)$. Computation of XOR of $de\_New\_E(i)$ and *temp* to attain $C\_New\_E(i)$. Simultaneously, change the values of parameter *temp* to $C\_New\_E(i)$ and the value of parameter *i* is $i + 1$.

Step6 Repeat steps 4 & 5. If $i = M \times N + 1$, change the resultant vector to the matrix of $M \times N$, that is, encode the resultant images.

3.5. Decryption process

The decryption technique is the reverse process of encryption. During encryption, first, we scramble the image and later spread it. Thus, there is a need to implement diffusion decryption first, and later scrambling. Note that we must attain the parameter values, and the first value of the hyper-chaotic system is used for generating a sequence before decryption.

4. Performance validation

The experimental outcome of the CIEAIBO-DNA technique was executed on five different images. Fig. 3 displays the sample images with their encrypted versions.

Table 1 represents the encryption outcomes of the CIEAIBO-DNA method on five images. The outcomes point out that the CIEAIBO-DNA method gains effective outcomes under all images. On IMG_1, the CIEAIBO-DNA technique offers MSE, RMSE, PSNR, and CC of 0.045, 0.212, 61.599 dB, and 99.78 % respectively. Also, on IMG_2, the CIEAIBO-DNA algorithm offers MSE, RMSE, PSNR, and CC of 0.076, 0.276, 59.323 dB, and 99.92 % respectively. Additionally, on IMG_4, the CIEAIBO-DNA method provides MSE, RMSE, PSNR, and CC of 0.078, 0.279, 59.210 dB, and 99.92 % correspondingly. Finally, on IMG_6, the CIEAIBO-DNA system offers MSE, RMSE, PSNR, and CC of 0.067, 0.259, 59.870 dB, and 99.86 % correspondingly.

Table 2 and Fig. 4 represent the information encryption values of the CIEAIBO-DNA algorithm on 3 channels. The outcomes show that the CIEAIBO-DNA system reaches improved performance over other models with maximum information entropy values of 7.9997, 7.9999, and 7.9998 correspondingly.

Table 3 signifies the MSE and PSNR examination of the CIEAIBO-DNA approach with other approaches [21,32]. The simulation values highlighted that the CIEAIBO-DNA technique reaches minimal MSE and maximum PSNR values.

Fig. 5 inspects the MSE outcome of the CIEAIBO-DNA system with recent algorithms. The experimental values portrayed that the CIEAIBO-DNA technique reaches improved performance under all images. On IMG_1, the CIEAIBO-DNA technique offers an MSE of 0.045 while the BDIE-AOFOLS, SSO–HCNN, WOA-HCNN, and GWO-HCNN techniques accomplish an MSE of 0.0590, 0.0636, 0.1850, and 0.2875 respectively. Moreover, on IMG_3, the CIEAIBO-DNA system offers an MSE of 0.038 while the BDIE-AOFOLS, SSO–HCNN,

Table 1
Encryption outcome of CIEAIBO-DNA method under five images.

Test Images	MSE	RMSE	PSNR (dB)	CC (%)
IMG_1	0.045	0.212	61.599	99.78
IMG_2	0.076	0.276	59.323	99.92
IMG_3	0.038	0.195	62.333	99.89
IMG_4	0.078	0.279	59.210	99.92
IMG_5	0.103	0.321	58.002	99.98
IMG_6	0.067	0.259	59.870	99.86

Table 2
Information encryption values of the CIEAIBO-DNA method on three channels.

Methods	Information Entropy Values		
	R_Channel	G_Channel	B_Channel
CIEAIBO-DNA	7.9997	7.9999	7.9998
BDIE-AOFOLS	7.9995	7.9998	7.9997
SSO–HCNN	7.9992	7.9990	7.9992
WOA-HCNN	7.9941	7.9935	7.9933
GWO-HCNN	7.9938	7.9921	7.9930

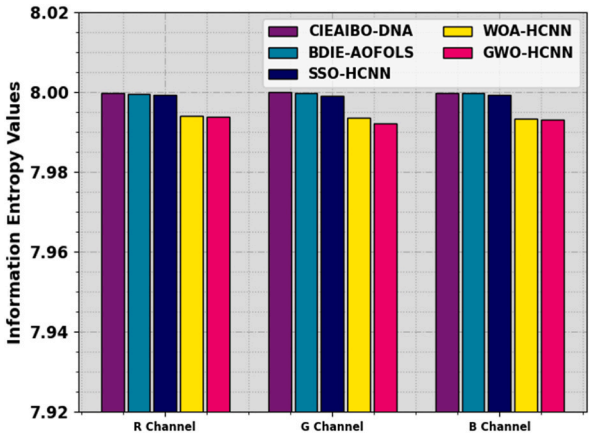

Fig. 4. Information encryption values of the CIEAIBO-DNA method on three channels.

Table 3
MSE and PSNR outcomes of CIEAIBO-DNA approach with other methods.

Test Images	CIEAIBO-DNA		BDIE-AOFOLS		SSO–HCNN		WOA- HCNN		GWO-HCNN	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
IMG_1	0.045	61.599	0.0590	60.42	0.0636	60.10	0.1850	55.46	0.2875	53.54
IMG_2	0.076	59.323	0.0820	58.99	0.0841	58.88	0.1724	55.77	0.2312	54.49
IMG_3	0.038	62.333	0.0430	61.80	0.0487	61.26	0.2027	55.06	0.2352	54.42
IMG_4	0.078	59.210	0.0880	58.69	0.0926	58.46	0.2123	54.86	0.2613	53.96
IMG_5	0.103	58.002	0.1100	57.72	0.1117	57.65	0.1798	55.58	0.2318	54.48
IMG_6	0.067	59.870	0.0881	58.54	0.0925	57.98	0.2119	54.89	0.2574	54.12

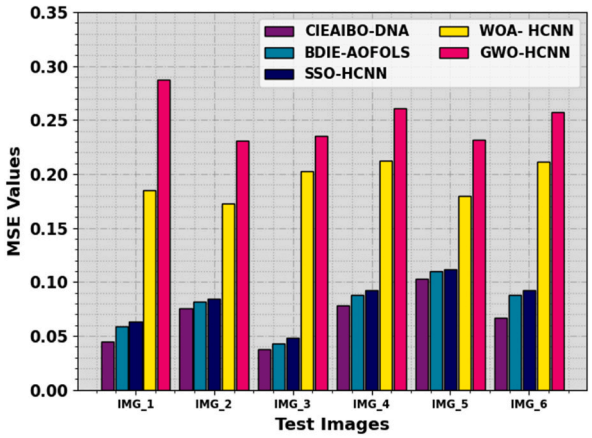

Fig. 5. MSE outcome of CIEAIBO-DNA approach under five images.

WOA-HCNN, and GWO-HCNN methods realize an MSE of 0.0430, 0.0487, 0.2027, and 0.2352 correspondingly. Furthermore, on IMG_6, the CIEAIBO-DNA methodology offers an MSE of 0.067 while the BDIE-AOFOLS, SSO–HCNN, WOA-HCNN, and GWO-HCNN approaches achieve an MSE of 0.0881, 0.0925, 0.2119, and 0.2574 correspondingly.

Fig. 6 examines the PSNR study of the CIEAIBO-DNA methodology with recent systems. The experimental values depicted that the CIEAIBO-DNA system attains enhanced performance under all images. On IMG_1, the CIEAIBO-DNA technique offers a PSNR of 61.599 dB while the BDIE-AOFOLS, SSO–HCNN, WOA-HCNN, and GWO-HCNN methods achieve PSNR of 60.42 dB, 60.10 dB, 55.77 dB, and 53.54 dB correspondingly. Besides, on IMG_3, the CIEAIBO-DNA method offers a PSNR of 62.333 dB while the BDIE-AOFOLS, SSO–HCNN, WOA-HCNN, and GWO-HCNN algorithms gain PSNR of 61.80 dB, 61.26 dB, 55.06 dB, and 54.42 dB correspondingly. Additionally, on IMG_6, the CIEAIBO-DNA technique provides a PSNR of 59.870 dB while the BDIE-AOFOLS, SSO–HCNN, WOA-HCNN, and GWO-HCNN methodologies realize a PSNR of 58.54 dB, 57.98 dB, 54.89 dB, and 54.12 dB correspondingly.

Table 4 and Fig. 7 inspect the CC outcome of the CIEAIBO-DNA algorithm with recent approaches. The experimental values demonstrated that the CIEAIBO-DNA approach reaches improved performance under all images. On IMG_1, the CIEAIBO-DNA method provides a CC of 99.89 % while the BDIE-AOFOLS, SSO–HCNN, WOA-HCNN, and GWO-HCNN methods reach a CC of 99.48 %, 99.56 %, 99.34 %, and 99.23 % correspondingly. Followed by, on IMG_3, the CIEAIBO-DNA approach offers a CC of 99.79 % while the BDIE-AOFOLS, SSO–HCNN, WOA-HCNN, and GWO-HCNN techniques achieve a CC of 99.52 %, 99.67 %, 99.34 %, and 99.03 % respectively. Finally, on IMG_6, the CIEAIBO-DNA methodology offers a CC of 99.69 % while the BDIE-AOFOLS, SSO–HCNN, WOA-HCNN, and GWO-HCNN approaches achieve a CC of 99.43 %, 99.25 %, 99.13 %, and 99.34 % respectively.

In Table 5 and Fig. 8, a comparison computation time (CT) study of the CIEAIBO-DNA method is clearly given. The outcomes display the enhanced outcome of the CIEAIBO-DNA method with the least CT values. On IMG_1, the CIEAIBO-DNA technique attains a decreasing CT of 0.8s while the BDIE-AOFOLS, SSO–HCNN, WOA-HCNN, and GWO-HCNN models obtain increasing CT of 0.91s, 1.97s, 1.37s, and 1.87s respectively. Meanwhile, on IMG_6, the CIEAIBO-DNA method accomplishes reducing CT of 0.57s while the BDIE-AOFOLS, SSO–HCNN, WOA-HCNN, and GWO-HCNN approaches acquire higher CT of 0.981s, 0.95s, 1.34s, and 1.80s correspondingly. Therefore, the CIEAIBO-DNA technique exhibited better performance than other models.

The higher outcome of the CIEAIBO-DNAC has been recognized for its innovative combination of key elements that together develop security and resilience against several attacks. Unlike typical methods, CIEAIBO-DNAC utilizes the MD5 hash function to create a unique connection among the input image pixel values and the encryption key, therefore highly boosting key sensitivity. The combination of the IBO technique establishes an effective scrambling process at the pixel level from the blocks, more stimulating the encryption process. Furthermore, the use of DNA coding in the diffusion phase increases an extra layer of difficulty through obfuscation, encoding, and decoding procedures, contributing to heightened security. These combined features make a secure encryption method that determines exceptional resistance against varied attacks in widespread experimental assessments, positioning CIEAIBO-DNAC as a capable performance for real-time image encryption scenarios.

5. Conclusion

In this study, we have focused on the development of the CIEAIBO-DNAC for enhanced security. The presented CIEAIBO-DNAC technique involves different processes such as initial value generation, substitution, diffusion, and decryption. Primarily, the key is related to the input image pixel values by the MD5 hash function, and the hash value produced by the input images can be utilized as the primary value of the chaotic model to boost key sensitivity. Besides, the CIEAIBO-DNAC technique uses the BO algorithm for scrambling the pixel position in the block and the scrambling process among the blocks takes place. Moreover, in the diffusion stage, DNA encoding, obfuscation, and decoding process were carried out to attain encrypted images. Extensive experimental evaluations and security analyses are conducted to consider the efficiency of the CIEAIBO-DNAC technique. The experiment outcome illustrates that the system exhibits excellent security properties, including resistance against several attacks, ensuring it can be applied to real-time image encryption scenarios. Therefore, the CIEAIBO-DNAC technique offers an effective solution for securing images against unauthorized access and ensuring their confidentiality. Its utilization of chaotic maps and encryption operations provides robust protection and makes it suitable for a wide range of applications.

Data availability statement

Data sharing does not apply to this article as no datasets were generated during the current study.

Consent to participate

Not applicable.

Informed consent

Not applicable.

CRediT authorship contribution statement

Ahmed S. Almasoud: Conceptualization, Project administration, Writing – original draft. **Bayan Alabduallah:** Funding

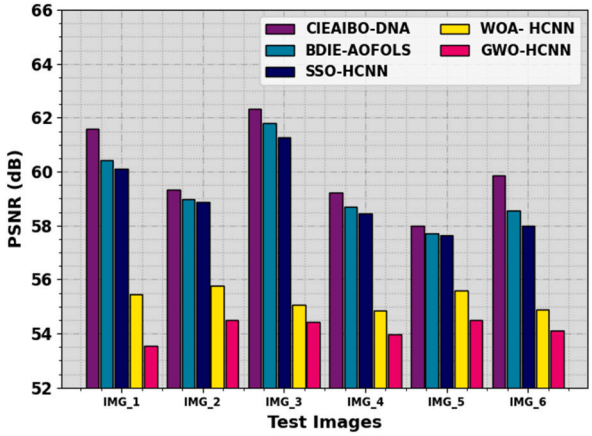

Fig. 6. PNSR outcome of CIEAIBO-DNA approach under five images.

Table 4
CC outcome of CIEAIBO-DNA system with other methodologies under five images.

Correlation Coefficient (CC %)					
Test Images	CIEAIBO-DNA	BDIE-AOFOLS	SSO–HCNN	WOA- HCNN	GWO-HCNN
IMG1	99.89	99.48	99.56	99.34	99.23
IMG2	99.9	99.69	99.78	99.45	99.22
IMG3	99.79	99.52	99.67	99.34	99.03
IMG4	99.85	99.77	99.38	99.49	99.25
IMG5	99.98	99.83	99.89	99.71	99.11
IMG6	99.69	99.43	99.25	99.13	99.34

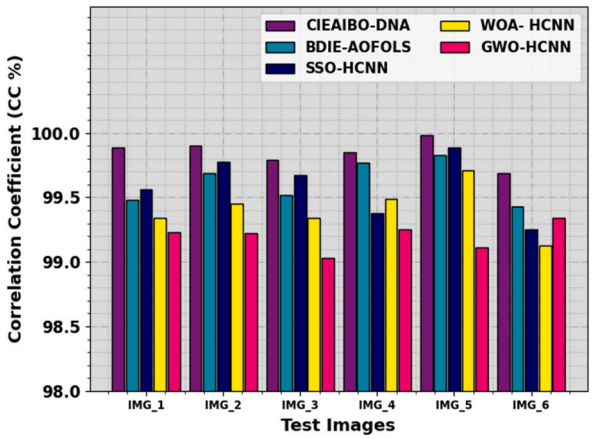

Fig. 7. CC outcome of CIEAIBO-DNA approach under five images.

Table 5
CT outcome of CIEAIBO-DNA approach with other methods under five images.

Computational Time (sec)					
Test Images	CIEAIBO-DNA	BDIE-AOFOLS	SSO–HCNN	WOA- HCNN	GWO-HCNN
IMG_1	0.80	0.91	0.91	1.37	1.87
IMG_2	0.92	0.99	1.03	1.15	1.53
IMG_3	0.75	1.24	1.27	1.52	1.63
IMG_4	0.72	0.82	0.86	1.39	1.90
IMG_5	0.63	0.89	0.93	1.45	1.71
IMG_6	0.57	0.98	0.95	1.34	1.80

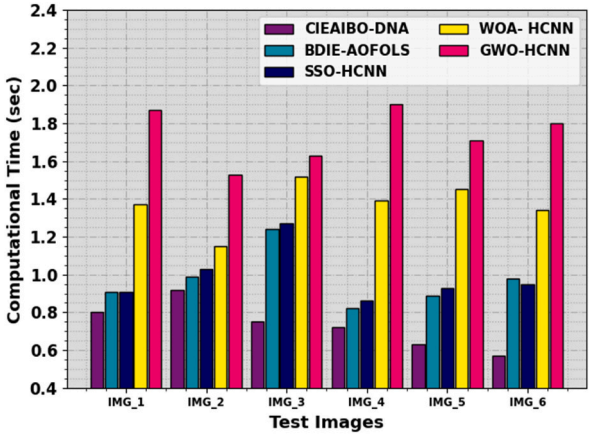

Fig. 8. CT outcome of CIEAIBO-DNA approach under five images.

acquisition, Project administration, Supervision, Writing – review & editing. **Hamed Alqahtani:** Data curation, Formal analysis. **Sumayh S. Aljameel:** Investigation, Methodology. **Saud S. Alotaibi:** Software, Supervision. **Abdullah Mohamed:** Validation, Visualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through large group Research Project under grant number (RGP2/248/44). Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2024R440), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. We Would like to thank SAUDI ARAMCO Cybersecurity Chair for funding this project. This study is partially funded by the Future University in Egypt (FUE)."

References

[1] S. Arifin, A. Nicholas, H. Baskoroputro, A.S. Prabowo, M.A. Ibrahim, A. Rahayu, Algorithm for digital image encryption using multiple hill ciphers, a unimodular matrix, and a logistic map, International Journal of Intelligent Systems and Applications in Engineering 11 (6s) (2023) 311–324.
[2] R.D.A. Raj, K.A. Naik, Optimal Reconfiguration of PV Array Based on Digital Image Encryption Algorithm: A Comprehensive Simulation and Experimental Investigation, vol. 261, Energy Conversion and Management, 2022 115666.
[3] A.U.S. Muhammad, F. Özkaynak, SIEA: secure image encryption algorithm based on chaotic systems optimization algorithms and PUFs, Symmetry 13 (5) (2021) 824.
[4] H. Wen, L. Ma, L. Liu, Y. Huang, Z. Chen, R. Li, Z. Liu, W. Lin, J. Wu, Y. Li, C. Zhang, High-quality restoration image encryption using DCT frequency-domain compression coding and chaos, Sci. Rep. 12 (1) (2022) 16523.
[5] S.B. Hebbale, V.S. Akula, P. Baraki, Tuna Swarm Optimization with 3D-chaotic map and DNA encoding for image encryption with lossless image compression based on FPGA, Int. J. Electr. Comput. Eng. Syst. 14 (1) (2023) 59–72.
[6] I.V. Korolkov, N. Zhumanazar, Y.G. Gorin, A.B. Yeszhanov, M.V. Zdorovets, Enhancement of electrochemical detection of Pb 2+ by sensor based on track-etched membranes modified with interpolyelectrolyte complexes, J. Mater. Sci. Mater. Electron. 31 (2020) 20368–20377.
[7] D.A. Vinnik, A.Y. Starikov, V.E. Zhivulin, K.A. Astapovich, V.A. Turchenko, T.Y.I. Zubar, S.V. Trukhanov, J. Kohout, T. Kmjec, O. Yakovenko, L. Matzui, Changes in the structure, magnetization, and resistivity of BaFe12–x Ti x O19, ACS Appl. Electron. Mater. 3 (4) (2021) 1583–1593.
[8] D.I. Shlimas, A.L. Kozlovskiy, M.V. Zdorovets, Study of the formation effect of the cubic phase of LiTiO 2 on the structural, optical, and mechanical properties of Li 2±x Ti 1±x O 3 ceramics with different contents of the X component, J. Mater. Sci. Mater. Electron. 32 (2021) 7410–7422.
[9] M.A. Almessiere, Y. Slimani, N.A. Algarou, M.G. Vakhitov, D.S. Klygach, A. Baykal, T.I. Zubar, S.V. Trukhanov, A.V. Trukhanov, H. Attia, M. Sertkol, Tuning the structure, magnetic, and high frequency properties of Sc-doped Sr0. 5Ba0. 5ScxFe12-xO19/NiFe2O4 hard/soft nanocomposites, Advanced Electronic Materials 8 (2) (2022) 2101124.
[10] X. Wang, M. Zhao, An Image Encryption Algorithm Based on Hyperchaotic System and DNA Coding, vol. 143, Optics & Laser Technology, 2021 107316.
[11] Q. Wang, X. Zhang, X. Zhao, Image encryption algorithm based on improved Zigzag transformation and quaternary DNA coding, J. Inf. Secur. Appl. 70 (2022) 103340.
[12] W. Bao, C. Zhu, A secure and robust image encryption algorithm based on compressive sensing and DNA coding, Multimed. Tool. Appl. 81 (11) (2022) 15977–15996.
[13] Q. Zhang, J. Han, Y. Ye, Image encryption algorithm based on image hashing, improved chaotic mapping and DNA coding, IET Image Process. 13 (14) (2019) 2905–2915.
[14] Y. Wan, S. Gu, B. Du, A new image encryption algorithm based on composite chaos and hyperchaos combined with DNA coding, Entropy 22 (2) (2020) 171.
[15] S. Zhu, C. Zhu, Secure image encryption algorithm based on hyperchaos and dynamic DNA coding, Entropy 22 (7) (2020) 772.
[16] M.A. Tahiri, H. Karmouni, A. Bencherqui, A. Daoui, M. Sayyouri, H. Qjidaa, K.M. Hosny, New Color Image Encryption Using Hybrid Optimization Algorithm and Krawtchouk Fractional Transformations, The Visual Computer, 2022, pp. 1–26.

[17] S. Saravanan, M. Sivabalakrishnan, A hybrid chaotic map with coefficient improved whale optimization-based parameter tuning for enhanced image encryption, Soft Comput. 25 (2021) 5299–5322.
[18] H. Khan, S.S. Jamal, M.M. Hazzazi, M. Khan, I. Hussain, New image encryption scheme based on Arnold map and cuckoo search optimization algorithm, Multimed. Tool. Appl. 82 (5) (2023) 7419–7441.
[19] H. Ghanbari, R. Enayatifar, H. Motameni, Chaos-based image encryption using hybrid model of linear-feedback shift register system and deoxyribonucleic acid, Multimed. Tool. Appl. 81 (22) (2022) 31815–31830.
[20] M. Kaur, S. Singh, M. Kaur, A. Singh, D. Singh, A systematic review of metaheuristic-based image encryption techniques, Arch. Comput. Methods Eng. (2021) 1–15.
[21] M.A. Alohali, M. Aljebreen, F. Al-Mutiri, M. Othman, A. Motwakel, M.I. Alsaid, A.A. Alneil, A.E. Osman, Blockchain-driven image encryption process with arithmetic optimization algorithm for security in emerging virtual environments, Sustainability 15 (6) (2023) 5133.
[22] Y. Zhu, C. Wang, J. Sun, F. Yu, A chaotic image encryption method based on the artificial fish swarms algorithm and the DNA coding, Mathematics 11 (3) (2023) 767.
[23] Y. Luo, X. Ouyang, J. Liu, L. Cao, Y. Zou, An image encryption scheme based on particle swarm optimization algorithm and hyperchaotic system, Soft Comput. (2022) 1–27.
[24] S. Khaitan, S. Sagar, R. Agarwal, Chaos Cryptosystem with Optimal Key Selection for Image Encryption, Multimedia Tools and Applications, 2022, pp. 1–16.
[25] S.R. Maniyath, V. Thanikaiselvan, An efficient image encryption using deep neural network and chaotic map, Microprocess. Microsyst. 77 (2020) 103134.
[26] J. Ferdush, G. Mondol, A.P. Prapti, M. Begum, M.N.A. Sheikh, S.M. Galib, An enhanced image encryption technique combining genetic algorithm and particle swarm optimization with chaotic function, Int. J. Comput. Appl. 43 (9) (2021) 960–967.
[27] J. Zeng, C. Wang, A Novel Hyperchaotic Image Encryption System Based on Particle Swarm Optimization Algorithm and Cellular Automata, vol. 2021, Security and Communication Networks, 2021, pp. 1–15.
[28] S.Y.D. Nezhad, N. Safdarian, S.A.H. Zadeh, New method for fingerprint images encryption using DNA sequence and chaotic tent map, Optik 224 (2020) 165661.
[29] M. Kharrich, O.H. Mohammed, S. Kamel, A. Selim, H.M. Sultan, M. Akherraz, F. Jurado, Development and implementation of a novel optimization algorithm for reliable and economic grid-independent hybrid power system, Appl. Sci. 10 (18) (2020) 6604.
[30] A.K. Das, D.K. Pratihar, Bonobo optimizer (BO): an intelligent heuristic with self-adjusting parameters over continuous spaces and its applications to engineering problems, Appl. Intell. 52 (3) (2022) 2942–2974.
[31] A.K. Das, D.K. Pratihar, A new bonobo optimizer (BO) for real-parameter optimization, in: 2019 IEEE Region 10 Symposium (TENSYMP), IEEE, 2019, June, pp. 108–113.
[32] M.M. Khayyat, M.M. Khayyat, S. Abdel-Khalek, R.F. Mansour, Blockchain enabled optimal Hopfield Chaotic Neural network based secure encryption technique for industrial internet of things environment, Alex. Eng. J. 61 (12) (2022) 11377–11389.