Alexandria Engineering Journal (2022) **61**, 11377–11389

HOSTED BY

Alexandria University

Alexandria Engineering Journal

www.elsevier.com/locate/aej
www.sciencedirect.com

Blockchain enabled optimal Hopfield Chaotic Neural network based secure encryption technique for industrial internet of things environment

Manal M. Khayyat [a], **Mashael M. Khayyat** [b], **S. Abdel-Khalek** [c,*], **Romany F. Mansour** [d]

[a] *Department of Information Systems, College of Computers and Information Systems, Umm Al-Qura University, Makkah, Saudi Arabia*
[b] *Department of Information Systems and Technology, College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia*
[c] *Department of Mathematics, College of Science, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia*
[d] *Department of Mathematics, Faculty of Science, New Valley University, El-Kharga 72511, Egypt*

Received 9 March 2022; revised 15 April 2022; accepted 7 May 2022
Available online 19 May 2022

KEYWORDS

Internet of Things;
Security;
Shark smell optimization;
Self diffusion;
Hopfield Chaotic Neural Network

Abstract Industrial Internet of Things (IIoT) denotes a network of interlinked sensors, instruments, and other devices for industrial applications in the domains of manufacturing, logistics, transportation, etc. IIoT security is a major crucial research area for several applications. Image encryption techniques gained popularity in the recent years, thanks to increasing requirements for secure image transmission in IIoT environments. At the same time, conventional security solutions built for sensitive data protection are getting outdated in IIoT environment due to the participation of third party. Blockchain (BC) is one of the recent solutions used for security purpose which eliminates the involvement of a third party. With this motivation, the current research article presents a new BC-Enabled Shark Smell Optimization with Hopfield Chaotic Neural Network (SSO-HCNN) for secure encryption in IoT environment. The proposed SSO-HCNN model exploits a composite Chaotic Map (CM) which is integrated into staged logistic and tent maps to initially process the images and develop the variables needed for Arnold mapping. In addition, the SSO algorithm is developed with maximum PSNR and coefficient fitness function to select the optimum secret and public keys of the system amongst the random numbers. Besides, the diffusion phase utilizes HCNN to create a self-diffusion chaotic matrix whereas the jumbled image performs XOR operation using the keys to obtain the cipher image. In SSO-HCNN model, the cryptographic pixel value in the image is saved on BC thus guaranteeing the security and privacy of the images. To examine the superior performance of SSO-HCNN model over state-of-the-art methods, a set of

* Corresponding author.
E-mail addresses: mmkhayat@uqu.edu.sa (M.M. Khayyat), sabotalb@tu.edu.sa (S. Abdel-Khalek).
Peer review under responsibility of Faculty of Engineering, Alexandria University.

https://doi.org/10.1016/j.aej.2022.05.002

simulations was conducted on benchmark test images. The simulation results of the proposed SSO-HCNN model were promising under different evaluation parameters.

1. Introduction

Industry 4.0 has gained significant attention in the recent years since it has transformed from Internet of Things (IoT) to Industrial IoT (IIoT). IIoT offers unique solutions to overcome the industrial issues. IoT enables the simultaneous connection of many devices at a time, with no human interference. It can be deployed in diverse areas such as productivity, surveillance, maintenance, etc. Compared to IoT, IIoT utilizes highly sensible and accurate sensors that are comprised of numerous location-aware approaches on supply chain perspective [1,2]. At present, smart devices are utilized in several sectors namely, drones, sensors, water handling equipment, etc. At the same time, IoT has also been integrated with IIoT in smart city concept. IIoT considerably enhances the connectivity and scalability with decreased cost and time for organizations. IoT is a collection of noticeable connected devices that can interact with one another. It denotes the association among several devices through physical and digital modes through internet. It comprises of an embedded system that assists in various real-time platforms including intelligent transport and healthcare. IoT gadgets hold physical objects with the help of sensors, RFID tags, digital actuators, and transmission units.

IoT gadgets are frequently considered as a limited computation with ultra-low bandwidth and transmission abilities. The aim of IoT is to enhance the comfort by increasing the interconnection of an improved diversity of embedded processing gadgets that utilize the present internet framework component. This enables the communication among sensors in factory mechanisms, mobile phones, home appliances, laptops, cars, etc., which can access network through the present protocols such as ZigBee, 3G, Wi-Fi, and Bluetooth. Real-world applications of this novel technique are abundant that range from environment monitoring to framework managing and home automation. This is a wholesome concept of universal processing in which the computer appears ubiquitously. While the applications run effortlessly among devices to manage the entire ecosystem starting from effective energy consumption in industries to daily shopping.

The development of upcoming generations of mobile networks and wireless system (5G) can create things easily to determine IIoT over a unified IP network layer [3]. It remains highly suitable as it adapts to a huge number of networks that are previously determined. It is a challenge to possess highly interrelated things together and are accessible in 5G network since, with the data availability using sensors, the chances for malicious attack are high. If the network or sensitive private information is hijacked, it could be disclosed to unauthorized individuals due to insufficient privacy. Thus, security architecture should be in place to assist the clients in controlling their device access, alert the clients when there is an unauthorized access and predict the risks. Some researchers have contributed in the research upon implementation of security architecture without degrading the convenience.

With large number of related entities, both network traffic and storage capacity would rise in an exponential manner. This scenario presents crucial security problems since public key architecture, the existing effective encryption may not function consistently. This limitation makes the IIoT gadgets prone to extensive malicious attacks. Cloud Computing (CC) technology provides a resolution to overcome the asset constraint of IIoT gadgets. Several private data is created by IIoT device that strengthens the privacy and overcomes the security problems in cloud-enabled IIoT network. Since the acceptance of IIoT is increasing, the cost advantage of implementing difficult protocols would turn into main study concept with huge effects. Henceforth, the IoT applications are meant to handle various problems though its focus would be on complications relevant to security and privacy problems [4–6]. Similar to other kinds of network frameworks, security is the main stimulation for IIoT networks that comprises of availability, data confidentiality, data freshness, data integrity, and authentication. Some modified IIoT frameworks and their regular protocols should assume essential limitations like scalability, dynamicity, reliability, and so on. Data exchange that occurs between IIoT gadgets and cloud should be encoded with sufficient security before communication.

Image encryption methods have attracted more attention in the recent years, owing to increasing need for secure image communication [7,8]. Chaotic system is one of the significant tools in cryptography. In recent times, several encryption techniques were developed with chaotic systems, for instance [9]. In literature [10], an effective double-optical image encryption system was proposed through distinct Chirikov regular mapping and chaotic fractional arbitrary transformation. Further, in the study conducted earlier [11], an advanced technique was proposed that utilizes scan pattern and true arbitrary key stream. A new encryption system was established in [12] depending on Josephus's problem and filtering technique while these techniques followed traditional diffusion and confusion structures.

The state-of-the-art image encryption approaches are found to be ineffective in IIoT in case if the peers are not centralized. The development of blockchain (BC) arises from cryptocurrency or bitcoins. BC is a register which stores every transaction made between the individuals. Being a decentralized model, BC is highly secure and cannot be mutated. Once a transaction or any such entry is made into the ledger, it could not altered or removed. BC is a consensus-based scheme i.e., the nodes verify the existence of transaction and derives it to a consensus regarding the details prior to its placement in the ledger. BC has been developed as a security solution for several applications. Owing to adaptive features, many industries started adopting BC for IIoT. It can be employed in industries not only for security, but also to attain transparency and regulatory compliance. BC considerably transforms the IIoT and offers privacy, peer-to-peer device communication, and the latest functionalities with the help of smart contract.

The current research study presents a new BC-enabled Shark Smell Optimization with Hopfield Chaotic Neural Network (SSO-HCNN) for secure encryption in IIoT environment. The proposed SSO-HCNN model uses a composite Chaotic Map (CM) for initial processing and parameter initialization of Arnold mapping. In addition, the SSO algorithm is developed with maximum PSNR and coefficient fitness function to choose an optimal set of secret and public keys of the system amongst the random numbers. In SSO-HCNN model, the cryptographic pixel values of the image are saved on BC thus it guarantees the security and privacy of the images. To highlighted the outcomes of the proposed SSO-HCNN model in a better way, extensive experimentation was carried out on benchmark test images. The results of the experimental analysis established that the proposed SSO-HCNN model accomplished a promising performance in ensuring reliability and security with better quality images. The key contributions of the paper are as follows.

- A Blockchain-enabled secured image encryption technique SSO-HCNN encompassing BC technology, HCNN-based encryption, and SSO-based optimal key generation algorithm has been proposed in this study. As per the researcher's knowledge, no studies have been conducted so far with SSO-HCNN model.
- Chaotic models are sensitive to initial conditions and system parameters. Further, it possesses the character of white noise, pseudorandom sequence, and interval ergodic chaos. So, HCNN model is applied along with SSO algorithm which is the novelty of this work.
- Besides, in the proposed model, the use of BC technology guarantees the security and privacy of image transmission process in IIoT environment.
- The performance of the proposed SSO-HCNN model was validated using benchmark test images and the outcomes were examines under several performance measures.

The rest of the paper is planned as follows. Section 2 offers the literature review, section 3 provides the proposed model, and section 4 discusses the performance validation. Lastly, section 5 draws the conclusion.

2. Related works

In literatures [13–15], a novel permissioned private BC-based scheme is presented to secure the images during encryption process. Here, the pixel value in the image is saved on BC which offers privacy and security for the imaging data. Zhang et al. [16] solved three major security threats in IoT, transport, application, and perception layers. The gateway node of the perception layer follows an unknown data process in which the identity authentications and private data access cannot be prevented from exterior hackers. However, it can resolve security problems like identity authentication and human attacks in transmission layer. In addition to this, the system provides a secure key sharing technique that enhances the security of the scheme. Furthermore, they implemented two fault tolerant modules to ensure proper decryption of the ciphertext if cloud server fails in IoT platform.

Jang and Lee [17] presented a technique for partial encryption of confidential data in images by FF1 and FF3-1. The technique introduced tend to encrypt the private data with no raise in data size and also resolve the challenges involved in unused memory. Additionally, the presented technique also recognized certain segments of encrypted image and whole data that address the problem of attacking conventional privacy covering image encryption techniques. Muhammad et al. [18] projected a rapid probabilistic and lightweight technique for encrypting key frames before communication. In this study, the researchers considered processing and memory needs of the restricted devices that raise their appropriateness for IoT systems. The study outcomes proved the efficiency of the presented technique in terms of security, robustness, and execution time compared to other image encryption methods.

Al Sibahee et al. [19] introduced a lightweight system that could allow content-based search process. Particularly, the images are denoted by local features. The researchers validated and developed a secured system to measure the Euclidean distance between two feature vectors. Additionally, they also utilized hashing techniques, to be specific, local sensitive hashing to devise the search index. Refining vector methods were utilized to improve security and effectiveness of the related outcomes. Meshram et al. [20] presented an effective SSS method that utilizes FCM for safe transmission in IoT-based smart gadgets. The safety is nearly connected to an arbitrary oracle module depending on FCM demonstration. The researchers utilized difficult tasks to perform verification and signing processes related to human signature, validation of the signature in document and verification based on witness.

Saddam et al. [21] conducted security analysis and calculated the efficiency of the projected method. The technique was implemented as a combination of emotion and unified switch network. The simulated analysis exposed that the technique provides sufficient security after five iterations of encryption. The hardware executed the method with lower cost eight-bit micro-controller. The impacts created by memory consumption, code size, and decoding or encryption performance cycle were compared against the reference encryption technique. In Roy et al. [22], IoT accessible PCA-based block cipher named IECA was presented. Additionally, arbitrariness in the produced cipher image was verified by several statistical tests that exist in DIEHARD and NIST test suites. Hamza et al. [23] proposed an effective cryptosystem to secure the IoT-based surveillance systems. The presented cryptosystem architecture is composed of three portions. Initially, a lightweight automated summarization method is presented depending on fast histogram clustering method to extract the keyframes from investigation video. Next, they utilized a DCT method to compress the extracted data size. At last, the presented architecture executes an effective image encryption technique with DFRT. Jin et al. [24] implemented an RLWE-enabled homomorphic encryption transmission technique for client validation and data management in CC-enabled IoT convergence platform. The researchers conducted efficiency analyses on transmission protocols for the presented IoT platform and the presented transmission protocol guaranteed both security and safety. Also, some applications of security have been provided based on the counting-based secret sharing scheme and the combination of both techniques: cryptography and steganography [25,26]. In addition, some deep learning and deep convolutional neural network models have been successfully used in image retrieval [27,28,29].

Though several state-of-the-art image encryption techniques are available in literature, none of them fulfill the requirements of industries. Smart industry has a decentralized network of peers. The smart industry encompasses several interlinked IoT gadgets and these gadgets distribute sensitive data that are prone to exposure and hacking. BC offers a set of comprehensive solutions for decentralized device, and the encryption scheme is highly safe and effective for smart industry.

3. The proposed SSO-HCNN model

The overall working principle involved in the presented model is discussed in this section. SSO-HCNN model is proposed based on HCNN model. Initially, the key selection process takes place followed by the execution of staged CM. Then, the scrambling process is carried out after which the scrambled image gets serialized. Followed by, the series attained by HCNN model is secondarily diffused to produce the cipher image. Furthermore, in order to enhance the efficiency of HCNN model, SSO algorithm is applied that optimally selects the secret and public keys amongst arbitrary numbers. In SSO-HCNN model, the cryptographic pixel value in the image is saved on BC, thus guaranteeing the security and privacy of the images. The detailed working processes are discussed in subsequent sections.

3.1. Proposed Blockchain scheme for IIoT

In the proposed SSO-HCNN model, cryptographic pixel value of the image is saved on BC thus it ensures the security and privacy of images. BC is considered as a beneficial ledger to ensure the quality of data. It generates ‘controlling operations’ for several decentralized industrial devices. It performs peer-to-peer communication among globally decentralized devices. Further, BC offers amenability as well as authority for every independent system, while at the same time, it also resolves the security issues. In industrial sectors, private BC can be employed to achieve security. Hyperledger fabric is an environment that depends upon BC and satisfies the need for IIoT environment. It is a freely accessible environment that comes under Linux foundation category. It is useful in several domains such as healthcare, supply chain, transportation, and large scale IoT data. Further, BC helps in attaining privacy, trust, and decentralization [13]. BC enables simple connection with several devices. Such devices can be ab end node one or supercomputer that is involved in data computation. The node can communicate the secured data to other peer nodes in such a way that none of the attackers can attack the data. It could transmit the data to a center place or decentralized device that is linked with other devices. The hash values in BC are exclusive fingerprints of each data in the chain. The hash indicates all the transactions occurred in the block. A pair of hash values is iteratively hashed in a block so as to obtain an individual hash value. Fig. 1 depicts the fundamental structure of BC [13].

Server computer or client can act as a node and it begins the transactions. The transactions are combined together to produce a block; however, this block gets appended to the chain only after the verification from endorse nodes. The transaction gets started when the clients start submission of the proposals. It gets initialized from data transmission over the user, SDK. The transaction processes utilize two distinct kinds of peers namely, endorser and committer peers. The former one is accountable for simulation and signing the transaction proposal. The latter one validates the transaction results, prior to writing a block of transactions to the distributed ledger. Certificate Authority (CA) allocates the credential to users since it is mandatory by client applications to obtain permissions for submitting new transactions. In order to initiate new transactions, the client application transmits the transaction proposal to peer so that they can read or update the ledger. The endorser-peer gets the virtual result as specific read-and-write data. The reply from endorser-peer comprises of read-and-write dataset. The read data captures the recent state whereas the write data holds data which is printed to world that states the execution of transaction. As soon as the reply and validation of the transaction are received, the user then broadcasts it to the orderer who commands the transaction into a block and pass the blocks to every committer-peer. They can read it and authenticate the endorsement policies. If it is ensured, they can perform the writing operation. At last, the committer-peer creates an asynchronous announcement related to transaction status. The orderer-peer notifies the other nodes, if the transaction is ineffective or not. When a block saves the transaction, it could not be interfered.

3.2. Structure of HCNN model

HNN was initially presented by American physicist Hopfield [30] in 1982. It is mostly utilized for the simulation of memory method of biological NN. HNN is a kind of fully connected NN. Therefore, the output signal for every neuron is fed as input to itself by another neuron thus creating a feedback NN. Eq (1) provides a demonstration of its general form in which ‘v’ represents the double tangent functions and ‘w’ denotes the weight matrix. Fig. 2 shows the processes involved in HCNN model.

$$x = -x_i + \sum_{i=1}^{3} w_{ij} v_i, \tag{1}$$

$$v_i = tanh(x_i) = \frac{e^{x_i} - e^{-x_i}}{e^{x_i} + e^{-x_i}}, \tag{2}$$

$$w = \begin{bmatrix} 2 & -1 & 0 \\ 1.7 & 1.71 & 1.1 \\ -2.5 & -2.9 & 0.56 \end{bmatrix}. \tag{3}$$

3.3. Composite Chaotic map

The logistic CM contains unsteadiness and ergodicity and is broadly utilized in CMs. It is appropriate for image encryption, NN, digital envelope transmission, secure communication, and pattern recognition [31]. Though this technique provides benefits similar to cryptography such as quasi arbi-

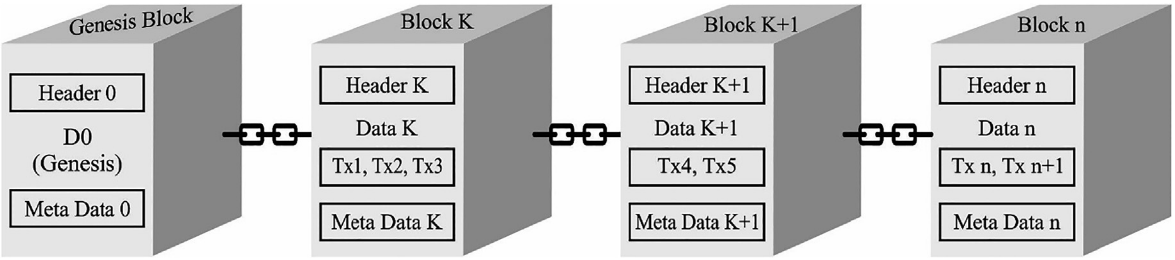


Fig. 1 Structure of BC.

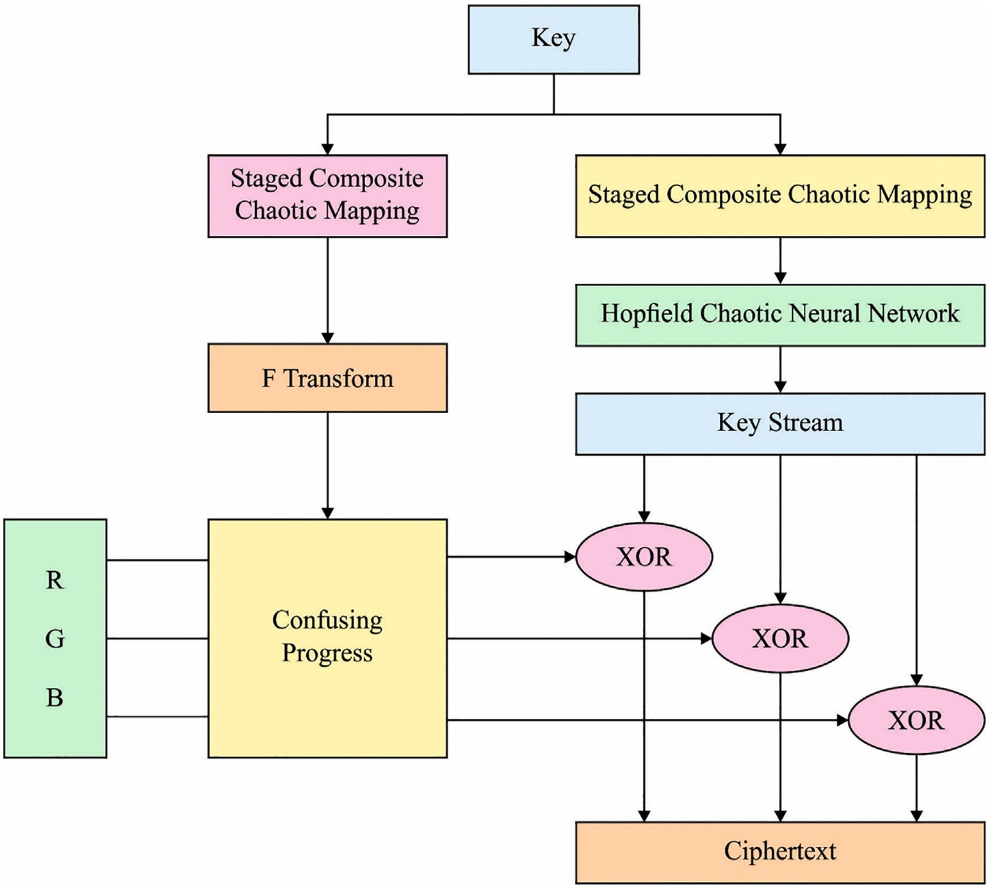

Key
Staged Composite Chaotic Mapping
Staged Composite Chaotic Mapping
Hopfield Chaotic Neural Network
F Transform
Key Stream
R
G
B
Confusing Progress
XOR
XOR
XOR
Ciphertext

Fig. 2 HCNN processes.

trariness, the security of cryptosystem is lower due to its small key space and low complexity of ordering. Few enhancements are required for anti-decipherability and security of the scheme. Therefore, a logistic map is integrated with tent mapping to create a novel phased CM. Primarily, the logistic map is separated into two portions and is formulated in Eq. (4):

$$x_{n+1} = \begin{cases} 4\mu x_n(0.5 - x_n)\ (0 \leqslant x < 0.5) \\ 4\mu(1 - x_n)(x_n - 0.5)(0.5 \leqslant x \leqslant 1) \end{cases} \tag{4}$$

By separating the tent mapping into four portions and substituting it in Eq. (4), the staged composite CMs are defined as follows.

$$x_{n+1} = \begin{cases} 16\mu \cdot x_n \cdot (0.5 - \mu x_n) & (0 \leq x < 0.25) \\ 16\mu \cdot (0.5 - x_n)(0.5 - \mu \cdot (0.5 - x_n)) & (0.25 \leq x < 0.5) \\ 16\mu \cdot (x_n - 0.5)(0.5 - \mu \cdot (x_n - 0.5)) & (0.5 \leq x < 0.75) \\ 16\mu \cdot (1 - x_n)(0.5 - \mu \cdot (1 - x_n)) & (0.75 \leq x \leq 1) \end{cases}, \tag{5}$$

where $\in [0,\ 2]$, $x_i \in [0,\ 1]$.

3.4. Processes involved in SSO-HCNN model

In this section, different processes involved in SSO-HCNN model such as confusion, diffusion, optimal key generation, encryption, and decryption processes are discussed in brief.

3.4.1. Confusion process

Though is managed by Arnold's cat mapping, p, q in these confusing equations are created using phased composite CMs. The variables and initial states of the staged composite CM are denoted by x_1 and μ_1 respectively. The staged composite CM iteratively generates the variables i.e., p, q of Cat mapping, with m_0, and time. x_1, μ_1, m_0 represents three encryption keys of the SSO-HCNN model.

3.4.2. Diffusion process

In this stage, HCNN performs on tricolour series signal outputs to change the pixel value (i.e. image equalization) for image diffusion. Here, the phased composite CM utilizes district initial conditions whereas the controlled variables are known as x_2, μ_2 that can generate the initial state of higher order chaotic scheme. In this method, phased composite CM is repeated m_r, m_g, m_b times and three initial states of the HNN are attained. With regards to scrambling procedure, x_2, μ_2 and m_r, m_g, m_b represent the encryption keys. The generation of keystream using HCNN for image equalization is defined in the remaining steps.

3.4.3. Optimal key generation using SSO algorithm

The chaotic models are non-linear and highly sensitive to initial conditions. So, there is a need exists to properly initialize the keys involved in HCNN model. Therefore, SSO algorithm is employed in the initialization of secret and public keys involved in encryption process. This occurs in such a way that PSNR gets increased. The fitness function of SSO algorithm for HCNN model is as follows.

$$Fitnessfunction = \max(PSNR) \tag{6}$$

Sharks commonly use their strong smell sense to identify the location of prey and capture it. Shark smell sense is one of the most efficient senses known. Its efficiency can be understood by its capacity i.e., shark could smell a harmed fish located 1 km away [32]. Shark smell sense can act as a guide for current procedure. This procedure assists the sharks in detecting the source of smell. In this motion, the concentration performs a major part in guiding the shark to its prey. Alternatively, a high concentration outcome is produced in an accurate motion of shark. This feature is the base for designing an optimization technique in finding the optimum solution. The search procedure initiates if the shark smells odour. Indeed, the odour particle contains weaker diffusion from an injured fish (prey). To model this procedure, a population of first solution is arbitrarily created to optimize the problem from possible search space [33]. Every solution denotes an odour particle that demonstrates a feasible location of shark at initial search procedure.

$$\left[x_1^1, x_2^1, \cdots, x_{\mathrm{NP}}^1\right] \tag{7}$$

where $x_i^1 = i$th which denotes the first location of population vector or i th solution; and NP denotes the population size. The interrelated optimization problem is given herewith.

$$x_i^1 = \left[x_{\mathrm{i},1}^1, x_{\mathrm{i},2}^1, \cdots, x_{\mathrm{i,\,NP}}^1\right] i = 1, 2, \cdots, NP, \tag{8}$$

where $x_{i,j}^1 = j$th dimension of shark at i th location or j th decision parameter of i th location of shark $\left(x_i^1\right)$; and $ND =$ amount of decision parameters in optimization problem. Odour intensity, at every location, reflects their proximity to the prey. The shark, at every location, travels with a velocity to go nearer to the prey. According to the location vector, the primary velocity vector is given by:

$$\left[V_1^1, V_2^1, \cdots, V_{\mathrm{NP}}^1\right] \tag{9}$$

In Eq. (9), the velocity vector has a set of elements in every dimension.

$$V_i^1 = \left[V_{\mathrm{i},1}^1, V_{\mathrm{i},2}^1, \cdots, V_{\mathrm{i,NP}}^1\right] i = 1, \cdots, ND \tag{10}$$

The shark tracks the odour and its course of motion is designed according to the intensity of odour. The velocity of sharks increases when the concentration of odour increases. The gradient shows the direction in which the process raises with maximum rate, as defined in Eq. (11):

$$V_i^k = \eta_k.R1.\nabla(OF)|_{x_i^k} i = 1, \cdots, NPk = 1, \cdots, k_{max}, \tag{11}$$

Where V_i^k is the velocity of shark, OF is the Objective Function, r is the gradient of objective function, $k_{\max}$ denotes the highest number of stages to forward the motion of shark ,k denotes the stage count, $\eta_k =$ a value in the range of 0 and 1, and $R1$ is an arbitrary value that follows uniform distribution in the range of 0 and 1 . η_k represents the range [0,1] since it is not possible for a shark to attain the velocity defined by gradient function. Fig. 3 demonstrates the flowchart of SSO.

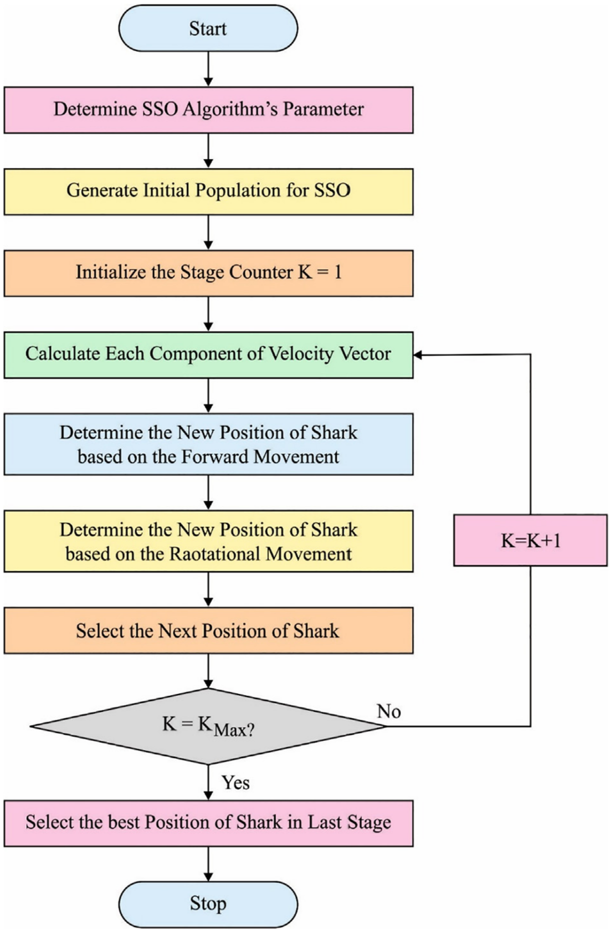

Start
Determine SSO Algorithm's Parameter
Generate Initial Population for SSO
Initialize the Stage Counter K = 1
Calculate Each Component of Velocity Vector
Determine the New Position of Shark based on the Forward Movement
Determine the New Position of Shark based on the Raotational Movement
K=K+1
Select the Next Position of Shark
K = K_{Max}?
No
Yes
Select the best Position of Shark in Last Stage
Stop

Fig. 3 Flowchart of SSO.

Variable $R1$ provides an additional arbitrary search inherent to SSO technique. The velocity in every dimension is evaluated in Eq. (12):

$$V_{\mathrm{i},j}^{k} = \eta_k.R1 = \frac{\partial(\mathrm{OF})}{\partial x_j}|_{x_{ij}^{k}}.\mathrm{i} = 1,\cdots,\mathrm{NP}\,\mathrm{j} = 1,\cdots,$$
$$NDk = 1,\cdots,k_{\max} \tag{12}$$

Since inertia is present, the acceleration of shark gets restricted and its velocity is decided based on prior velocity. These procedures are demonstrated in Eq. (12):

$$V_{\mathrm{i},j}^{k} = \eta_k.R1.\frac{\partial(\mathrm{OF})}{\partial x_j}|_{x_{ij}^{k}} + \alpha_k.\mathrm{R2}.\,V_{\mathrm{i},j}^{k-1} \tag{13}$$

$i = 1,\cdots,NPk = 1,\cdots,k_{\max}$,

where α_k denotes the rate of momentum/inertia coefficient and $R2$ is an arbitrary amount generator that is uniformly distributed on the range [0,1]. The ratio of maximum to minimum velocities of the shark is restricted. The velocity controller is utilized in every stage of the SSO technique as given herewith.

$$\left|V_{ij}^{k}\right| = \min\left[\left|\eta_k.R1.\frac{\partial(\mathrm{OF})}{\partial x_j}|_{x_{ij}^{k}} + a_k.R2.V_{i,j}^{k-1}\right|, \left|\beta_k.V_{ij}^{k-1}\right|\right], \tag{14}$$

$i = 1,\cdots,NP, j = 1,\cdots,ND, k = 1,\cdots,k_{\max}$

Where $\beta_k =$ velocity limiter ratio for stage k. Since sharks have forwarding motion, its novel location Y_i^{k+1} is defined according to its prior location and velocity:

$$Y_i^{k+1} = X_i^k + V_i^k.\Delta t_k i = 1,\cdots,NPk = 1,\cdots,k_{\max} \tag{15}$$

Where $\Delta t_k =$ time interval of stage k. Δt_k is consider 1 to every stage for the intention of simplicity.

Every component of $V_{i,j}^k(j = 1,\cdots,ND)$ of vector V_i^k is attained by Eq. (14). Additionally, in forwarding motion, the shark contains a rotational motion in its direction to detect the strong odour particle. Indeed, it increases its growth. From optimization to solution detection, the shark ensures a local search in every stage. This local search in SSO technique is demonstrated herewith.

$$Z_i^{k+1,m} = Y_i^{k+1} + R3.Y_i^{k+1}m = 1,\cdots,Mi = 1,\cdots,$$
$$NPk = 1,\cdots,k_{\max}, \tag{16}$$

where $Z_i^{k+1,m}$ is the location of point m in local search; $R3$ is the arbitrary number that is uniformly distributed in the range of -1 and 1; and M represents the number of points in local search of every stage. As this operator ensures a local search nearby Y_i^{k+1}, $R3$ is assumed to have been restricted in the range of -1 and 1. M points the local search $Z_i^{k+1,m}$ represents the vicinity of Y_i^{k+1} (When arbitrary amount generator produces 0, then Y_i^{k+1} is attained). A closed-form is attained by connecting M points that are equivalent to rotational motion of the shark. In rotational motion, when a shark detects a point with strong odour, it starts searching that point which is represented using Eq. (17):

$$x_i^{k+1} = \mathrm{arg}max\{OF(Y_i^{k+1}), OF(Z_i^{k+1,i}),\cdots,$$
$$OF(Z_i^{k+1,M})i = 1,2,\cdots,NP \tag{17}$$

In Eq. (17), the Objective Function (OF) should be reduced. Alternatively, Y_i^{k+1} is attained from forwarding motion and $Z_i^{k+1,m}(m = 1,2,\cdots,\mathrm{M})$ is attained from rotational motion, a solution with maximum objective function is chosen as the succeeding location of the shark (x_i^{k+1}). The cycle of forwarding and rotational motions would continue till k is equivalent to $k_{\max}$.

3.4.4. *Encryption and decryption processes*

Assume the input image as a grayscale digital image of size $M \times N$, in which M represents the line length and N indicates the column length. In a confusing procedure, x_1, μ_1, m_0 represent the initial input as key. Later, the key functions on the basis of obtaining an iterative value $x_1(m_0)$. Then, $x_1(m_0)$ is expanded and converted to attain q, and the expanded F convert. It is given as follows.

$$\begin{cases} p = floor\left(mod\left(x_1(m_0) \times 2^{24},\ N\right)\right) \\ q = floor\left(mod\left(mod\left(x_1(m_0) \times 2^{48}, 2^{24}\right),\ N\right)\right)' \end{cases} \tag{18}$$

Once p and q are obtained, Arnold Cat mapping is employed and the conversion technique is defined as follows.

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \mathrm{mod}\, N, \tag{19}$$

When RGB channels of the colour image are fed as input, the scrambled colour image is attained. After scrambling, the matrix is represented as follows:

$$s = \begin{bmatrix} S_{R,1} & S_{R,2} & \cdots & S_{R,M\times N} \\ S_{G,1} & S_{G,2} & \cdots & S_{G,M\times N} \\ S_{B,1} & S_{B,2} & \cdots & S_{B,M\times N} \end{bmatrix}. \tag{20}$$

During diffusion procedure, x_2, μ_2, m_r, m_g, m_b represent the initial input as keys. Later, the keys are computed based on obtaining the values such as $x_1(m_r)$, $x_1(m_g)$, and $x_1(m_b)$ after iterating m_r, m_g, m_b times. Next, $x_1(m_r)$, $x_1(m_g)$, $x_1(m_b)$ are utilized as primary values of HCNN and $N \times N$ iterations are executed to acquire the series X_R, X_G, X_B; The resultant is equivalent to S, as displayed in Eq (21).

$$X = \begin{bmatrix} X_{R,1} & X_{R,2} & \cdots & X_{R,M\times N} \\ X_{G,1} & X_{G,2} & \cdots & X_{G,M\times N} \\ X_{B,1} & X_{B,2} & \cdots & X_{B,M\times N} \end{bmatrix}. \tag{21}$$

Later, the matrix X is functioned which attains a modulo, and keystream K is created as defined below.

$$K(\mathrm{i},\mathrm{j}) = mod\left(round\left((abs(X(\mathrm{i},\mathrm{j})) - floor(X(\mathrm{i},\mathrm{j}))) * 10^{14}\right), 256\right), \tag{22}$$

where $\in [R,\ G,\ B], j \in [1,\ M \times N]$. Lastly, the bitwise exclusive OR components of K and S matrices are given by Eq. (23).

$$C(i,j) = bitxor(K(i,j), S(i,j)), \tag{23}$$

Where $i \in [R,\ G,\ B] j \in [1,\ M \times N]$. At this stage, the encryption process gets terminated and the ciphered image is generated. During decryption process, for conditions of known key and ciphertext, essential variables like p, q, $K(i,\ j)$ are created. Afterwards, $K(i,\ j)$ and $C(i,\ j)$ are XORed, and S matrix can be attained. Additionally, with p, q as variables, Arnold inverse conversion is executed to get the actual image.

```
Algorithm 1: Pseudocode of SSO algorithm
Begin
Step 1. Parameter Initialization
Initialize $NP$, $k_{\max}$, $\eta_k$, $\alpha_k$, and $\beta_k(k = 1, 2, \cdots, k_{\max})$
Create an initial population with every individual
Create decisions arbitrarily with the permissible interval
Initiate the stage counter $k = 1$
For $= 1{:}k_{\max}$
Step 2. Forward motion
Evaluate every element of the velocity vector,$v_{i,j}(i = 1, \cdots, NP, j = 1, \cdots, ND)$
Attain new location of shark according to forwarding motion,$Y_i^{k+1}(i = 1, \cdots, NP)$
Step 3. Rotational motion
Attain location of shark depending upon rotational motion,$z_i^{k+1,m}(m = 1, .., M)$
Choose following location of shark according to 2 motions $X_i^{k+1}(i = 1, \cdots, NP)$
End for $k$
Fixed $k = k + 1$
Choose an optimum location of shark in the previous stage that contains maximum $OF$ value
End
```

4. Performance validation

This section provides a detailed investigation of the results obtained by the presented SSO-HCNN model on a set of benchmark test images [34]. Some of the sample images are shown in Fig. 4.

Table 1 and Fig. 5 visualizes the results offered by SSO-HCNN model in terms of MSE, PSNR, and CC. From the table, it can be observed that the presented SSO-HCNN model effectively encrypted and decrypted the images by offering minimal MSE and maximum PSRN and CC. For instance, on the applied image 1, SSO-HCNN model attained a MSE of 0.061, PSNR of 60.278 dB, and CC of 0.996. Next to that, on the applied image 2, SSO-HCNN model attained a MSE of 0.084, PSNR of 58.888 dB, and CC of 0.998. Meanwhile, on the applied image 3, SSO-HCNN model attained a MSE of 0.049, PSNR of 61.229 dB, and CC of 0.997. Eventually, on the applied image 4, the presented SSO-HCNN model attained a MSE of 0.092, PSNR of 58.493 dB, and CC of 0.998. Lastly, on the applied image 5, the proposed SSO-HCNN model attained a MSE of 0.112, PSNR of 57.639 dB, and CC of 0.999.

An information entropy analysis of the presented SSO-HCNN model with existing techniques under R, G, and B channels is shown in Table 2 and Fig. 6. On the applied R channel, the proposed SSO-HCNN model obtained a high information entropy of 7.9998, whereas other models such as WOA-HCNN, GWO-HCNN, and HCNN achieved the least information entropy values such as 7.9945, 7.9942, and 7.9938 respectively.

Simultaneously, on the applied G channel, the proposed SSO-HCNN model obtained a high information entropy of 7.9997, whereas other models such as WOA-HCNN, GWO-HCNN, and HCNN achieved the least information entropy values such as 7.9932, 7.9926, and 7.9923 respectively. At last, on the applied B channel, the proposed SSO-HCNN model obtained a high information entropy of 7.9998, whereas WOA-HCNN, GWO-HCNN, and HCNN models accomplished the least information entropy values such as 7.9936, 7.9929, and 7.9918 respectively.

Fig. 4 Sample Test Images.

Table 1 Visualization of the Proposed SSO-HCNN method on Sample Images.

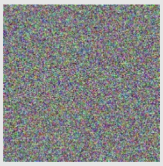
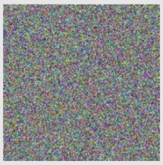
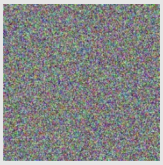
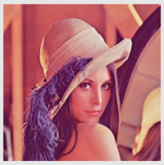
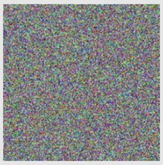
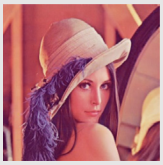
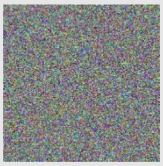
Original Images	Encrypted Images	Decrypted Images	MSE	PSNR	CC
			0.061	60.278	0.996
			0.084	58.888	0.998
			0.049	61.229	0.997
			0.092	58.493	0.998
			0.112	57.639	0.999

Table 3 shows a brief comparative analysis of the SSO-HCNN model with existing techniques in terms of MSE and PSNR. The results for the MSE analysis of SSO-HCNN model with existing techniques are shown in Fig. 7. The figure showcase that the SSO-HCNN model attained a better performance with the least MSE of 0.061, whereas WOA-HCNN, GWO-HCNN, and HCNN models accomplished inferior outcomes with increased MSE values of 0.185, 0.287, and 1.573 respectively. In addition, on the applied test image 3, the SSO-HCNN model achieved a better performance with the least MSE of 0.049, whereas WOA-HCNN, GWO-HCNN, and HCNN models accomplished inferior outcomes with increased MSE values such as 0.203, 0.235, and 2.228 respectively. Besides, on the applied test image 5, the SSO-HCNN model reached a better performance with the least MSE of 0.112. However, WOA-HCNN, GWO-HCNN, and HCNN models attained inferior outcomes with increased MSE values such as 0.179, 0.232, and 2.550 respectively.

Fig. 8 shows the results of PSNR analysis of the SSO-HCNN model with other techniques on the applied test images. The figure portrays that the SSO-HCNN model achieved a high PSNR value on all the applied test images. For instance, on the applied test image 1, the SSO-HCNN model achieved the maximum PSNR of 60.278 dB, whereas the WOA-HCNN, GWO-HCNN, and HCNN models accomplished minimum PSNR values such as PSNR of 55.489 dB, 53.552 dB, and 46.164 dB respectively. Moreover, on the applied test image 3, the SSO-HCNN model achieved the highest PSNR value of 61.229 dB, whereas the WOA-HCNN, GWO-HCNN, and HCNN models resulted in minimum PSNR values such as 55.056 dB, 54.420 dB, and 44.652 dB respectively. Furthermore, on the applied test image 5, the SSO-HCNN model achieved a maximum PSNR of 57.639 dB, whereas the WOA-HCNN, GWO-HCNN, and HCNN models produced minimum PSNR values such as 55.602 dB, 54.476 dB, and 44.065 dB respectively.

Table 4 and Fig. 9 shows the results for CC analysis of the proposed SSO-HCNN model with other techniques on the applied test images. From the figure, it can be understood that the presented SSO-HCNN model offered a high CC value on all the applied test images. For instance, on the applied test image 1, the SSO-HCNN model achieved a maximum CC of 0.996, whereas the WOA-HCNN, GWO-HCNN, and HCNN models accomplished minimum CC values such as 0.994, 0.993, and 0.993 respectively. Moreover, on the applied test image 3, the SSO-HCNN model accomplished a maximum CC of 0.997, whereas WOA-HCNN, GWO-HCNN, and HCNN models produced minimum CC values such as 0.995, 0.992, and 0.990 respectively. Furthermore, on the applied test image 5, the SSO-HCNN model achieved a maximum CC of 0.999, whereas WOA-HCNN, GWO-HCNN, and HCNN models produced minimum CC values such as 0.997, 0.991, and 0.988 respectively.

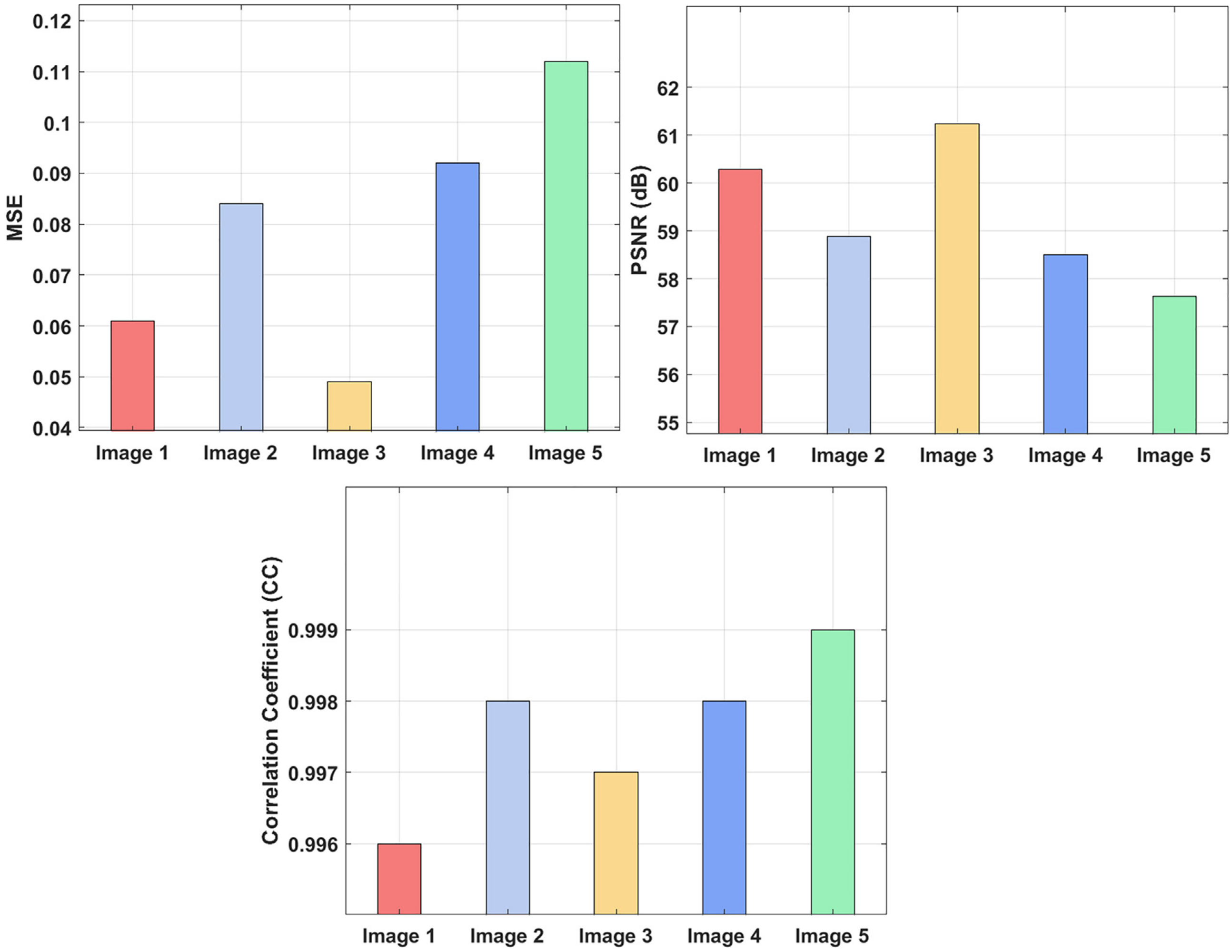


Fig. 5 Result analysis of SSO-HCNN method.

Table 2 Result of the Analysis of SSO-HCNN with Existing Methods in terms of Information Entropy.

Methods	Information Entropy Values		
	R Channel	G Channel	B Channel
SSO-HCNN	7.9998	7.9997	7.9998
WOA-HCNN	7.9945	7.9932	7.9936
GWO-HCNN	7.9942	7.9926	7.9929
HCNN	7.9938	7.9923	7.9918

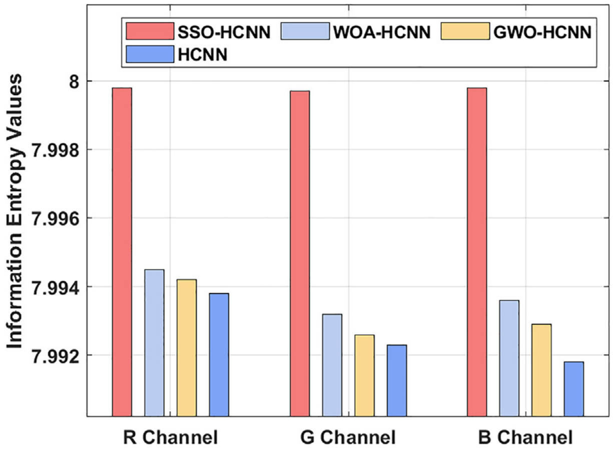


Fig. 6 Information entropy analysis of SSO-HCNN model.

Table 5 and Fig. 10 shows the results of CT analysis of SSO-HCNN model with existing techniques. The figure infers that SSO-HCNN model reached a better performance with the least CT of 1.201 s, whereas other models such as WOA-HCNN, GWO-HCNN, and HCNN accomplished inferior outcomes with high CT values being 1.627 s, 2.112 s, and 2.834 respectively. In addition, on the applied test image 3, the SSO-HCNN model reached a better performance with the least CT of 1.551 s, whereas the WOA-HCNN, GWO-HCNN, and HCNN models accomplished inferior outcomes with increased CT values being 1.781 s, 1.912 s, and 2.722 s respectively.

Besides, on the applied test image 5, the SSO-HCNN model reached a better performance with the least CT of 1.219 s, whereas other models such as WOA-HCNN, GWO-HCNN, and HCNN models accomplished inferior outcomes with increased CT values such as 1.729 s, 1.982 s, and 2.164 s

Table 3 Result of the Analysis of the Proposed SSO-HCNN Method with Existing Methods in terms of MSE and PSNR.

Test Images	SSO-HCNN		WOA- HCNN		GWO-HCNN		HCNN	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
Image 1	0.061	60.278	0.185	55.459	0.287	53.552	1.573	46.164
Image 2	0.084	58.888	0.172	55.776	0.231	54.495	2.071	44.969
Image 3	0.049	61.229	0.203	55.056	0.235	54.420	2.228	44.652
Image 4	0.092	58.493	0.212	54.867	0.261	53.964	2.071	44.969
Image 5	0.112	57.639	0.179	55.602	0.232	54.476	2.550	44.065

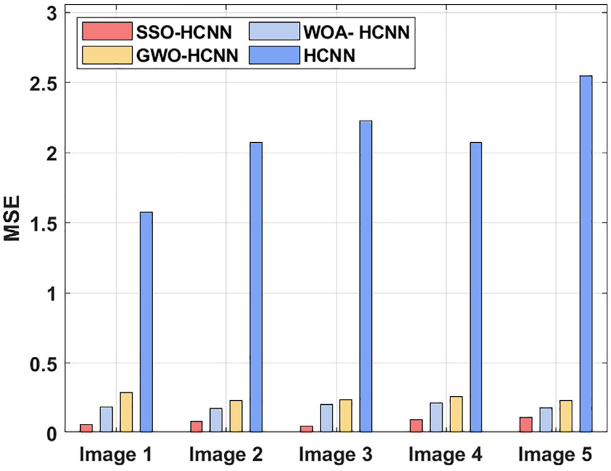


Fig. 7 MSE analysis of SSO-HCNN model.

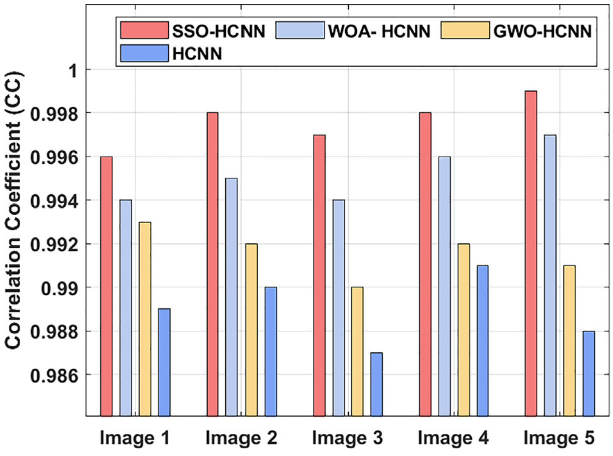


Fig. 9 Correlation coefficient analysis of SSO-HCNN model.

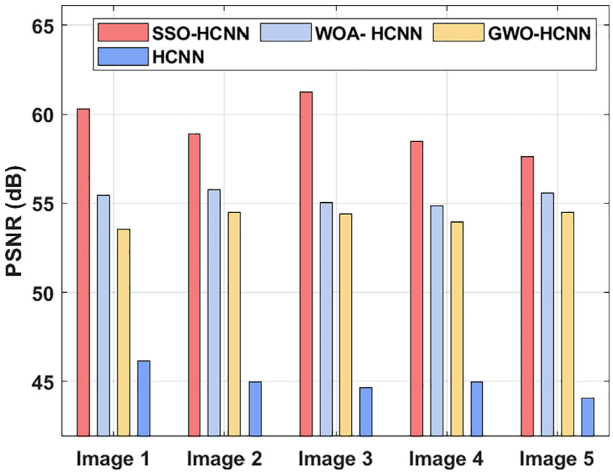


Fig. 8 PSNR analysis of SSO-HCNN model.

respectively. From the above mentioned results, it is inferred that the proposed SSO-HCNN model showcases promising results over existing state-of-the-art methods.

5. Conclusion

The current research paper devised a novel BC-enabled SSO-HCNN model for secure data transmission in IoT environment. In SSO-HCNN model, the cryptographic pixel value in the image is saved on BC thus it ensures the security and privacy of the images. The proposed SSO-HCNN model involves a composite CM for initial processing and parameter initialization of Arnold mapping. Moreover, the SSO algorithm is designed with maximum PSNR and coefficient fitness function in order to select the optimum set of secret and public keys of the system amongst the random numbers. In order to highlight the supremacy of the proposed SSO-HCNN model, extensive experimentation was carried out on benchmark test images. The proposed SSO-HCNN model demonstrated promising results under different evaluation parameters. As a part of

Table 4 Result of the Analysis of the Proposed SSO-HCNN Method with Existing Methods in terms of Correlation Coefficient (CC).

Test Images	SSO-HCNN	WOA- HCNN	GWO-HCNN	HCNN
Image 1	0.996	0.994	0.993	0.989
Image 2	0.998	0.995	0.992	0.990
Image 3	0.997	0.994	0.990	0.987
Image 4	0.998	0.996	0.992	0.991
Image 5	0.999	0.997	0.991	0.988

Table 5 Result Analysis of Proposed SSO-HCNN Method with Existing Methods in terms of Computation Time (s).

Test Images	SSO-HCNN	WOA- HCNN	GWO-HCNN	HCNN
Image 1	1.201	1.627	2.112	2.834
Image 2	1.292	1.451	1.803	2.267
Image 3	1.551	1.781	1.912	2.722
Image 4	1.127	1.627	2.167	2.198
Image 5	1.219	1.729	1.982	2.164

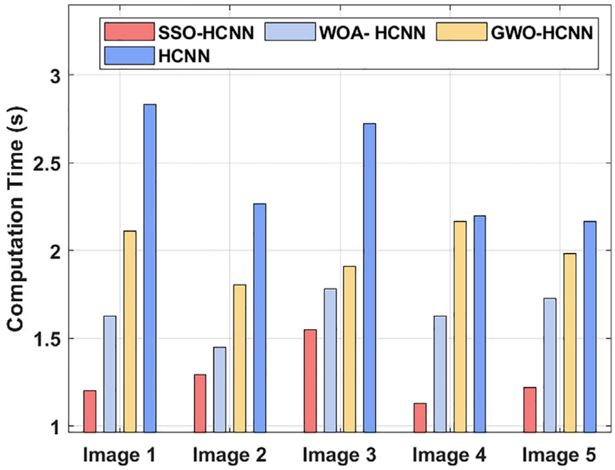


Fig. 10 Computation time analysis of SSO-HCNN model.

future extension, light weight cryptographic technique with biometric authentication schemes can be developed to guarantee the security in IoT environment.

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 would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by Grant Code: (22UQU4400271DSR05); Taif University Researchers Supporting Project number (TURSP-2020/154), Taif University, Taif, Saudi Arabia.

References

[1] X. Huang, P. Craig, H. Lin, Z. Yan, SecIoT: a security framework for the Internet of Things, Security Communication Networks 9 (16) (2016) 3083–3094.

[2] H. Boyes, B. Hallaq, J. Cunningham, T. Watson, The industrial internet of things (IIoT): An analysis framework, Comput. Ind. 101 (2018) 1–12.

[3] S. Mumtaz, A. Alsohaily, Z. Pang, A. Rayes, K.F. Tsang, J. Rodriguez, Massive Internet of Things for industrial applications: Addressing wireless IIoT connectivity challenges and ecosystem fragmentation, IEEE Ind. Electron. Mag. 11 (1) (2017) 28–33.

[4] S. Medileh, A. Laouid, E.M.B. Nagoudi, R. Euler, A. Bounceur, M. Hammoudeh, M. AlShaikh, A. Eleyan, O.A. Khashan, A flexible encryption technique for the internet of things environment, Ad Hoc Netw. 106 (2020) 102240.

[5] B. Sujitha, V.S. Parvathy, E.L. Lydia, P. Rani, Z. Polkowski, K. Shankar, Optimal deep learning based image compression technique for data transmission on industrial Internet of things applications, Trans. Emerging Telecommunications Technologies (2020) e3976.

[6] Uthayakumar, J., Vengattaraman, T. and Dhavachelvan, P., 2018. A survey on data compression techniques: From the perspective of data quality, coding schemes, data type and applications. Journal of King Saud University-Computer and Information Sciences.

[7] R. Hosseinzadeh, M. Zarebnia, R. Parvaz, Hybrid image encryption algorithm based on 3D chaotic system and choquet fuzzy integral, Opt. Laser Technol. 120 (2019) 105698.

[8] J. Uthayakumar, T. Vengattaraman, J. Amudhavel, A simple data compression algorithm for anomaly detection in Wireless Sensor Networks, Int. J. Pure Applied Mathematics 117 (19) (2017) 403–410.

[9] Ü. Çavuşoğlu, S. Kaçarb, I. Pehlivanb, A. Zengina, Secure image encryption algorithm design using a novel chaos based S-Box, Chaos Solit. Fract. 95 (2017) 92–101.

[10] Y. Zhang, D. Xiao, Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform, Opt. Lasers Eng. 51 (4) (2013) 472–480.

[11] T. Sivakumar, P. Li, A secure image encryption method using scan pattern and random key stream derived from laser chaos, Opt. Laser Technol. 111 (2019) 196–204.

[12] Z. Hua, B. Xu, F. Jin, H. Huang, Image encryption using josephus problem and filtering diffusion, IEEE Access 7 (2019) 8660–8674.

[13] P.W. Khan, Y. Byun, A blockchain-based secure image encryption scheme for the industrial Internet of Things, Entropy 22 (2) (2020) 175.

[14] M.M. Althobaiti, K. Pradeep Mohan Kumar, D. Gupta, S. Kumar, R.F. Mansour, An intelligent cognitive computing based intrusion detection for industrial cyber-physical systems, Measurement 186 (2021) 110145.

[15] R.F. Mansour, S.A. Parah, Reversible Data Hiding for Electronic Patient Information Security for Telemedicine Applications, Arabian J. Sci. Engineering 46 (9) (2021) 9129–9144.

[16] P. Zhang, J. Gao, W. Jia, X. Li, Design of compressed sensing fault-tolerant encryption scheme for key sharing in IoT Multi-cloudy environment (s), J. Information Security Applications 47 (2019) 65–77.

[17] W. Jang, S.Y. Lee, Partial image encryption using format-preserving encryption in image processing systems for Internet of things environment, Int. J. Distrib. Sens. Netw. 16 (3) (2020), 1550147720914779.

[18] K. Muhammad, R. Hamza, J. Ahmad, J. Lloret, H. Wang, S.W. Baik, Secure surveillance framework for IoT systems using probabilistic image encryption, IEEE Trans. Ind. Inf. 14 (8) (2018) 3679–3689.

[19] M.A. Al Sibahee, S. Lu, Z.A. Abduljabbar, A. Ibrahim, Z.A. Hussien, K.A.A. Mutlaq, M.A. Hussain, Efficient encrypted image retrieval in IoT-cloud with multi-user authentication, Int. J. Distrib. Sens. Netw. 14 (2) (2018), 1550147718761814.

[20] C. Meshram, R.W. Ibrahim, A.J. Obaid, S.G. Meshram, A. Meshram, A.M.A. El-Latif, Fractional chaotic maps based short signature scheme under human-centered IoT environments, J. Adv. Res. 32 (2021) 139–148.

[21] M.J. Saddam, A.A. Ibrahim, A.H. Mohammed, A Lightweight Image Encryption And Blowfish Decryption For The Secure Internet Of Things, IEEE, 2020, pp. 1–5.

[22] S. Roy, U. Rawat, H.A. Sareen, S.K. Nayak, IECA: an efficient IoT friendly image encryption technique using programmable cellular automata, J. Ambient Intell. Hum. Comput. 11 (11) (2020) 5083–5102.

[23] R. Hamza, A. Hassan, T. Huang, L. Ke, H. Yan, An Efficient Cryptosystem for Video Surveillance in the Internet of Things Environment, Complexity 2019 (2019) 1–11.

[24] B.W. Jin, J.O. Park, H.J. Mun, A design of secure communication protocol using RLWE-based homomorphic encryption in IoT convergence cloud environment, Wireless Pers. Commun. 105 (2) (2019) 599–618.

[25] N. Al-Juaid, A. Gutub, Combining RSA and audio steganography on personal computers for enhancing security, SN Appl. Sci. 1 (2019) 830.

[26] T.M. Alkhodaidi, A.A. Gutub, Scalable shares generation to increase participants of counting-based secret sharing technique, Int. J. Inf. Comput. Secur. 17 (2022) 119–146.

[27] M.M. Khayyat, A. Lamiaa, Elrefaei, Image Retrieval Using Deep Learning Incorporating a Variety of Fusion Levels, IEEE Access 8 (2020) 136460.

[28] M.M. Khayyat, L.A. Elrefaei, M.M. Khayyat, Historical Arabic Images Classification and Retrieval Using Siamese Deep Learning Model, CMC 72 (2022) 2109–2125.

[29] M. AlGhamdi, M. Abdel-Mottaleb, DV-DCNN: Dual-view deep convolutional neural network for matching detected masses in mammograms, Comput. Methods Programs Biomed. 207 (2021) 106152.

[30] J.J. Hopfield, Neural networks and physical systems with emergent collective computational abilities., PNAS 79 (8) (1982) 2554–2558.

[31] X.Y. Wang, Z.M. Li, A color image encryption algorithm based on Hopfield chaotic neural network, Opt. Lasers Eng. 115 (2019) 107–118.

[32] O. Abedinia, N. Amjady, A. Ghasemi, A new metaheuristic algorithm based on shark smell optimization, Complexity 21 (5) (2016) 97–116.

[33] S. Mohammad-Azari, O. Bozorg-Haddad, X. Chu, Shark smell optimization (SSO) algorithm. In *Advanced Optimization by Nature-Inspired Algorithms*, Springer, Singapore, 2018, pp. 93–103.

[34] http://sipi.usc.edu/database/.