Computers, Materials & Continua
DOI: 10.32604/cmc.2022.024775
Article

Tech Science Press

Encryption with Image Steganography Based Data Hiding Technique in IIoT Environment

Mahmoud Ragab[1,2,3,*], Samah Alshehri[4], Hani A. Alhadrami[5,6,7], Faris Kateb[1], Ehab Bahaudien Ashary[8] and S. Abdel-khalek[9,10]

[1]Information Technology Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[2]Centre of Artificial Intelligence for Precision Medicines, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[3]Department of Mathematics, Faculty of Science, Al-Azhar University, Naser City, 11884, Cairo, Egypt
[4]Department of Pharmacy Practice, Faculty of Pharmacy, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[5]Department of Medical Laboratory Technology, Faculty of Applied Medical Sciences, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[6]Molecular Diagnostic Lab, King Abdulaziz University Hospital, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[7]Special Infectious Agent Unit, King Fahd Medical Research Center, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[8]Electrical and Computer Engineering Department, Faculty of Engineering, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[9]Department of Mathematics, Faculty of Science, Taif University, Taif, 21944, Saudi Arabia
[10]Department of Mathematics, Faculty of Science, Sohag University, Sohag, 82524, Egypt
*Corresponding Author: Mahmoud Ragab. Email: mragab@kau.edu.sa

Received: 30 October 2021; Accepted: 05 January 2022

Abstract: Rapid advancements of the Industrial Internet of Things (IIoT) and artificial intelligence (AI) pose serious security issues by revealing secret data. Therefore, security data becomes a crucial issue in IIoT communication where secrecy needs to be guaranteed in real time. Practically, AI techniques can be utilized to design image steganographic techniques in IIoT. In addition, encryption techniques act as an important role to save the actual information generated from the IIoT devices to avoid unauthorized access. In order to accomplish secure data transmission in IIoT environment, this study presents novel encryption with image steganography based data hiding technique (EIS-DHT) for IIoT environment. The proposed EIS-DHT technique involves a new quantum black widow optimization (QBWO) to competently choose the pixel values for hiding secrete data in the cover image. In addition, the multi-level discrete wavelet transform (DWT) based transformation process takes place. Besides, the secret image is divided into three R, G, and B bands which are then individually encrypted using Blowfish, Twofish, and Lorenz Hyperchaotic System. At last, the stego image gets generated by placing the encrypted images into the optimum pixel locations of the cover image. In order to validate the enhanced data hiding performance of the EIS-DHT technique, a set of simulation analyses take place and the results are inspected interms of different measures. The experimental outcomes stated the supremacy of the EIS-DHT technique over the other existing techniques and ensure maximum security.

Keywords: IIoT; security; data hiding technique; image steganography; encryption; secure communication

1 Introduction

Industry 4.0 is the 4th generation industrial revolution that has dramatically increased from the Internet of Things (IoT) to the industrial IoT (IIoT). Such innovations have given a solution to novel problems for the industrial sectors. IoT enables linking a number of devices at once more convenient with no requirements of human interference [1]. IIoT is employed in the supply chain, monitoring system, management, and manufacturing process. It handles the connectivity of machines, management systems, smart factories, and another streamlined business operation. It employs more precise and sensitive sensor nodes when compared to IoT, comprising further location aware technology on the supply chain management [2]. Currently, smart device is employed in various field of industries, like sensor nodes for monitoring factories, drones for monitoring oil pipelines, tractors in agriculture, and water treating equipment. Smart cities might be an integration of commercial IoT & IIoT. Fig. 1 depicts the overview of IIoT [3].

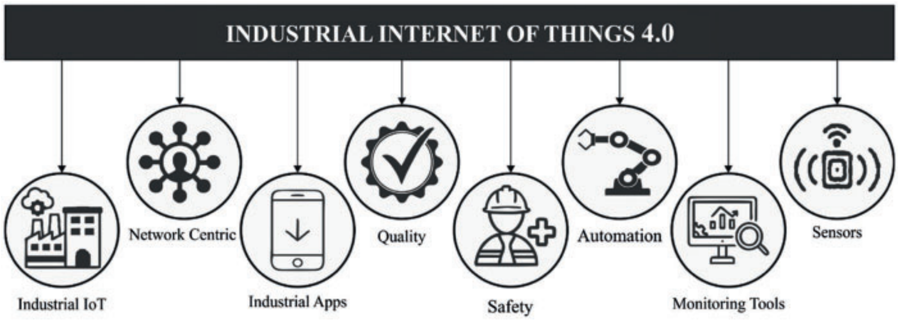


Figure 1: Overview of IIoT

Industry 4.0 is based on the number of new technologies. Several commercial enterprises near this reality are set on industry 4.0. It can be being utilized for building business intelligence, data management systems, realtime analyses, and scientific research [4]. Image sensor based solution helps in improving work process and maintenance securely. Moreover, they considerably enhance the quality of productivity. Computer vision technologies are employed for the visual quality control of production and continuous monitoring procedures. Increasingly state-of-the-art sensors and cameras are being employed in the industry. Also, this development brought additional problems, like absence of built-in security. Such problems request secure and safe devices and applications without human interference. Cyberattacks against automation in the IIoT environments have essential impacts [5]. They could disturb the manufacturing procedure, and secure information might be lost.

The direct solution is to encrypt the information with standard encryption tool beforehand outsourcing. Although there are several high and robust secured data preserving methods, and there is an advancement to make sure the robustness and security of the approach regarding its efficiency [6]. Image steganography has established an extensive application in the fields of mobile computing, communication, content, online voting systems, personalized secure image retrieval, privacy of medical records, and surveillance system [7,8]. Security is the major concern in present times, for hiding a sensitive piece of information from hackers and intruders becomes a tedious process [9]. The researcher didn't pay much attention to the problems like, when cover image dimension isn't appropriate for forming an image block to embed, next how to execute data hiding and either this technique is prone to different kinds of stego attack. Hence, further means should be used like modification to lesser number of pixels or transform coefficient, employ encrypted form of hidden message to be embedded so on. Still, several works in these fields are needed for choosing appropriate tradeoffs among the efficacy calculation measures like payload capacity, security, and imperceptibility

Xiang et al. [10] proposed a privacy preserving tucker train decomposition through blockchain based encrypted IIoT information. Especially, employ blockchain methods for enabling IIoT data provider for securely and reliably allocate its information by encrypting them beforehand recording them blockchain. They utilize tucker train (TT) concept for building an effective TT decomposition according to gradient descent which greatly decreases the number of components to be upgraded at the time of Tucker decomposition. This study exploits the huge resource of clouds and fogs for implementing an effective privacy preserving tucker train decomposition system. Feng et al. [11] proposed a robust cramer shoup delay optimized fully homomorphic encryption (RCSD-DOFHE) approach. This technique consists of 3 stages. Initially, minimalize the transmission time and overhead, Kullback Leibler divergences are employed in the RCSD method. Then, to minimalize the network delay and data latency, DOFHE method is proposed. In this study, delivery delay is evaluated among the IIoT device signal and base station (BS). Lastly, privacy preserving DOFHE and RCSD were introduced for privacy preserved secure data transmission. Li et al. [12] focus on the secured method of image data on cloud servers. The experimental result and security analyses demonstrate the effectiveness and security of this system.

In Xia et al. [13], a new detection method of encrypted traffic is presented for manually extracting the features for effective traffic classification, i.e., depending on spatio-temporal features. It consists of the classification and preprocessing phases. In preprocessing stage, raw traffic information is treated using sampling, vectorization, and flow segmentation, so on. Lin et al. [14] proposed permissioned private blockchain based solutions for securing the image when encrypting. In this system, the cryptographic pixel value of images is kept on the blockchain, ensuring the security and privacy of image data. Depending on the number of changing pixel rate (NPCR), unified averaged changed intensity (UACI), and data entropy analyses, they calculate the strength of presented image encryption method cipher regarding different attacks.

Khan et al. [15] proposed 3 data hiding methods to protect transmission in crucial IoT framework using steganography, in which RGB image is applied as a carrier for the data. They examine experimentally and mathematically. Mathematically, they demonstrate that the adversary could not forecast the real data using analyses. Bairagi et al. [16] proposed an effective data hiding system on the basis of multi-dimension mini SuDoKu reference matrix (RM). The presented RM has higher difficulty and could efficiently enhance the security of data hiding. Moreover, this work determines a range locator function that could considerably enhance the embedding efficacy of multi-dimension RM.

Horng et al. [17] proposed an interpolation-based reversible data hiding (IRDH) system which enhances Lee and Huang's scheme and Malik et al.'s system by integrating its embedding methods and the optimal pixel adjustment process (OPAP) rises the embedding capability and the visual quality of the systems. In this proposed work, they begin by stretching the size of the original image with the present enhanced neighbor mean interpolation (ENMI) interpolation approach later the data is embedded to the interpolated pixel with this new embedding technique which is based on the intensity of the pixel and the maximized variance value. Hassan et al. [18] proposed a technique named Harris hawks optimization-integer wavelet transform (HHO-IWT) for hidden data and transmission in the IIoT environments on the basis of digital image steganography. The technique embedded hidden information in the cover images with a Meta heuristic optimization method named HHO for effectively selecting image pixels which are employed for hiding bits of hidden information within integer wavelet transform. The HHO based pixel election process utilizes an objective function calculation based on succeeding 2 stages: exploration and exploitation. The objective functions are used for determining optimum encoding vectors to convert hidden information to an encoded version made using HHO approach.

This study presents novel encryption with image steganography based data hiding technique (EIS-DHT) for IIoT environment. The proposed EIS-DHT technique involves a new quantum black widow optimization (QBWO) for optimal pixel selection to hide secrete data in the cover image. In addition, the multi-level discrete wavelet transform (DWT) based transformation process takes place. Besides, the secret image is divided as to three R, G, and B bands which are then individually encrypted using Blowfish, Twofish, and Lorenz Hyperchaotic System. Finally, the stego image gets generated by placing the encrypted images into the optimum pixel locations of the cover image. For examining the improved data hiding performance of the EIS-DHT technique, a set of experimentation were carried out and the results are examined based on distinct metrics.

2 The Proposed EIS-DHT Technique

In this study, an efficient EIS-DHT technique has been developed for secure communication in IIoT environment. The presented model involves different stages of operations such as channel extraction, decomposition, optimal pixel selection, encryption, and embedding process. Firstly, the input cover image is divided into RGB channels to better understand the color space. Next to that, the multilevel DWT based transformation process takes place to generate a set of vector coefficients to determine the location of the pixels in the cover image. Besides, the optimal pixel selection process is carried out using the QBWO algorithm over the encrypted R, G, and B channels. On the other hand, the channel separation and encryption of the three channels of the secret image also take place. The encryption of the three R, G, and B channels takes place by the use of three encryption techniques. Finally, the encrypted images are embedded as to optimal pixel locations of the cover image and generate the stego image for secure data transmission. Fig. 2 illustrates the overall process of proposed EIS-DHT model.

2.1 Multi-level DWT Based Decomposition Process

At the initial stage, the multi-level DWT technique is applied to decompose the image into diverse sets of vector coefficients. The 2D-DWT is the most significant spatial to frequency domain conversion method. The partition is made with two processes namely, vertical and horizontal processes. The horizontal function decomposes an image to High (H) and Low (L) frequency bands. The RGB cover image is divided on the basis of HH, LH, LL, and HL bands for finding pixel position. Later, the vertical function decomposes the image to HH_1 LL_1, LH_1, and HL_1, frequency bands. For next decompositions, LL_1 band decompose to LL_2, LH_2, HL_2, and HH_2, where the image size represents ‘M ∗ N’. Initially, to down sample and filter the image, the horizontal decomposition decreases an image to $M \times \frac{N}{2}$ size.

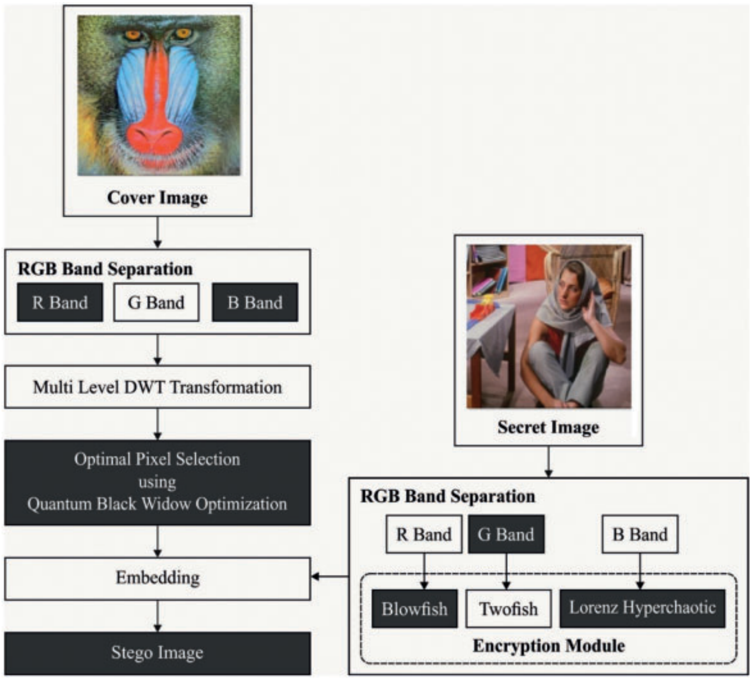


Figure 2: Overall process of EIS-DHT model

The vertical one decrease down-sample the images to $\frac{M}{2} \times \frac{N}{2}$. The single level decomposition outcomes are done using Eq. (1)

$$[C_1 C_2 C_3 C_4] = \mathrm{DWT}(C) \tag{1}$$

Whereas 'C_1', 'C_2', 'C_3', and 'C_4' denotes coefficient numbers of decomposing frequency band. 'C_1' denotes low level frequency band i.e., additionally decomposing for extracting subbands as provided under as [19]:

$$[C_1^{\mathrm{LL1}} C_1^{\mathrm{LH1}} C_1^{\mathrm{HL1}} C_1^{\mathrm{HH1}}] = \mathrm{DWT}(C_1) \tag{2}$$

The coefficient in lower frequency band C_1^{LL1} is over decomposed, since it produces the edge and texture interrelated details of an image. The following decompositions are executed on low band LL_1. The decomposition formation of frequency bands is presented by:

$$[C_1^{\mathrm{LL2}} C_1^{\mathrm{LH2}} C_1^{\mathrm{HL2}} C_1^{\mathrm{HH2}}] = \mathrm{DWT}(\mathrm{LL}_1) \tag{3}$$

Whereas C_1^{LL2} denotes low level frequency band of next level decomposition.

2.2 Optimal Pixel Selection (OPS) Using QBWO Algorithm

The multi-level DWT transformed image offers a set of vector coefficients and the optimal pixel values are elected by the use of QBWO algorithm. The BWO technique starts with a primary spider's population, therefore, all the spiders are referred to as feasible solutions. In pairs, these primary spiders are obvious for reproducing the novel generation. As premature as 11 days following being laid, during the egg sacs, the spiderling performs. In order to various days, it can be alive composed on parental web; the sibling cannibalism has been exposed at that period. Consequently, it takes off my life focused on the wind.

With the intention of resolving an optimized problem, this challenge of variables values must set up an appropriate structure for current issue solution. In BWO algorithm, a feasible solution to all problems is allocated to Black widow spider. All the black widow spider displays the problem variables value [20]. During the N_{var}- optimized problem, the widow signified as array of $1 \times N_{var}$ referring the problem solution and it can be demonstrated as under:

$$Widow = \lfloor y_1, y_2, \ldots y_{N_{var}} \rfloor \tag{4}$$

All the variable values $(y_1, y_2, \ldots y_{N_{var}})$ signifies the floating-point number. The fitness of widow is reached utilizing assessment of fitness method f at a widow of $(y_1, y_2, \ldots y_{N_{var}})$. Therefore

$$fitness = f(widow) = f(y_1, y_2, \ldots y_{N_{var}}) \tag{5}$$

The candidate widow matrix of size $N_{pop} \times N_{var}$ is generated with primary spider's population for establishing the optimized method. Next, by mating, couples of parents randomly were elected for performing the procreating method, where the female black widow eats the male during or succeeding to that.

Since they are self-governing, it starts for mating with the purpose of replicating a new generation, in correspond, obviously, all the couple mates in their web, individually from the options. During all the mating, nearly a thousand eggs were created in the real-world; but, eventually, some spider babies have been continued that is burly. Currently, during this manner with the purpose of repeating, an array called as alpha necessity more created giving widow array with random numbers including, afterward offspring has been created by developing α with succeeding to Eq. (6) where y_1 and y_2 represents the parents z_1 and z_2 are offspring.

$$\begin{cases} z_1 = \alpha \times y_1 + (1 - \alpha) \times y_2 \\ z_2 = \alpha \times y_2 + (1 - \alpha) \times y_1 \end{cases} \tag{6}$$

This process is reiterated for $\frac{N_{var}}{2}$, if the randomly elected numbers are essential not be reproduced. Eventually, the mother as well as children are continuous as array and considered utilizing its fitness function, at the current reliable with cannibalism rating; some of optimum those are comprised in the presently formed population. These steps are provided to every couple.

At this point, three types of cannibalism are present. A primary one has been sexual cannibalism, where during or succeeding for mating, the male black widow has been eaten by female. During this technique, distinguish the male as well as female are predictably utilizing its fitness values. More than one group has been sibling cannibalism where the burly spiderlings utilize their smaller siblings. During this technique, the CR is set reliable that survivor number has been obvious. In some situations, the third kind of cannibalism are often experiential which the child spider utilizes its mother.

During the mutation phase, $Mute_{pop}$ demonstrates the number of individuals was elected arbitrarily in the population. During the array, all elected solutions randomly swap 2 elements. Utilizing the mutation rate $Mute_{pop}$ was calculated. Same as other evolutionary manners, 3 stop conditions are dealt with: i) an existing number of iterations, ii) a few iterations, compliance of no change in value of fitness to optimum widow, iii) obtaining to specific level of accuracy.

The QBWO algorithm is designed by the incorporation of quantum computing into the BWO algorithm. Quantum Computing is a new kind of processing model which accepts the concept relevant to quantum modules like quantum entanglement, state superposition, and measurements. The basic component of quantum computing is qubit. The 2 fundamental conditions $|0\rangle$ and $|1\rangle$ make a qubit which is stated by linear integration as given by

$$|Q\rangle = \alpha|0\rangle + \beta|1\rangle \tag{7}$$

where $|\alpha|^2$ denotes the likelihood of observing condition $|0\rangle$, $|\beta|^2$ and $|1\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$. A quantum is comprised of n qubits. Due to the quantum superposition nature, each quantum has 2^n possible values. A set of n qubits quantum is represented by

$$\Psi = \sum_{x=0}^{2^n-1} C_x|x\rangle, \sum_{x=0}^{2^n-1} |C_x|^2 = 1 \tag{8}$$

Quantum gates could change the qubit states like rotation gate, NOT gate, Hadamard gate, and so on. The rotation gate is determined by mutation function to make quanta approach an optimum solution and finally, detect global optimum solutions. The rotation gate is determined by

$$\begin{bmatrix} \alpha^d(t+1) \\ \beta^d(t+1) \end{bmatrix} = \begin{bmatrix} \cos(\triangle\theta^d) & -sin(\triangle\theta^d) \\ sin(\triangle\theta^d) & cos(\triangle\theta^d) \end{bmatrix} \begin{bmatrix} \alpha^d(t) \\ \beta^d(t) \end{bmatrix} for\ d = 1, 2, \ldots, n \tag{9}$$

$\triangle\theta^d = \triangle \times S(\alpha^d,\ \beta^d)$, $\triangle\theta^d$ represents the rotation angle of qubit, when $\triangle$ and $S(\alpha^d,\ \beta^d)$ denotes direction and size of rotations, respectively. The QBWO algorithm derives an objective function depending upon the fitness function. The major goal of the QBWO algorithm is to design an image steganography technique in such a way that the mean square error (MSE) gets minimized and peak signal to noise ratio (PSNR) gets maximized. It can be denoted by

$$F = \{min(MSE),\ max(PSNR)\} \tag{10}$$

The preferable maximum and minimum values are attained by the use of QBWO algorithm.

2.3 Encryption and Embedding Process

During the encryption process, the secret image gets converted into three elements namely R, G, and B. They are separately encrypted by the Blowfish, Twofish, and Lorenz Hyperchaotic System. Finally, the encrypted RGB elements get embed into the optimal chosen pixel points in the cover image to ensure security.

2.3.1 R Band Encryption Using Blowfish

The R band of the secret image is primarily encrypted by the use of Blowfish technique. The blowfish is a symmetric block cipher which encrypts data from 8-byte blocks. The Blowfish technique contains 2 parts: data encryption as well as key expansion. The key expansion connections a variable-length key as a maximum of 64 bytes (512 bits) as to arrays of subkeys totaling 4168 bytes [21].

A huge amount of subkeys is utilized by Blowfish technique where these keys were pre-computed previously some data encrypted/decrypted. The P-array have 1832-bit subkeys. There are also 4 32-bit S-boxes with 256 entries.

$$\begin{array}{l} "S_{1,0}, S_{1,1}, \ldots, S_{1,255}; \\ S_{2,0}, S_{2,1}, \ldots, S_{2,255}; \\ S_{3,0}, S_{3,1}, \ldots, S_{3,255}; \\ S_{4,0}, S_{4,1}, \ldots, S_{4,255};" \end{array} \tag{11}$$

The point of view behind the Blowfish is the simplicity of this technique planned and this produces simplicity for implementation. Utilizing a streamlined Feistel network, an easy S-Box exchange and easy P-box substitution creates the body of Blowfish as easy as feasible, but preserving the chosen encryption features of the framework. All bits of xL have been utilized only as input for one S box that is importantly improved the technique against different attacks. The function F is given as follows:

Divide XL into 4 eight-bit quarters: a, b, c, and d. Afterward,

$$F(xL) = ((S_{1,a} + S_{2,b} mod\ 2^{32}) XOR\ S_{3,c}) + S_{4,d} mod 2^{32}. \tag{12}$$

2.3.2 G Band Encryption Using Blowfish

Then, the G band image is encrypted by the Twofish technique. It is a symmetric block cipher; a single key is employed for decryption and encryption. It has a block size of 128 bits and accepts a key of some length upto 256 bits. (National Institute of Standards and Technology (NIST) needed the approach for accepting 128-, 192-, and 256-bit keys.) It is fast on 32 and 8-bits CPU (embedded chips, smart cards,), and in hardware. Also, it is flexible; it is employed in the network application in which keys are altered continuously and in applications where there is slightly or no read only memory (ROM) and random access memory (RAM) accessible. Twofish is a Feistel network. It implies that in all the rounds, half of the text blocks are transmitted with an F function, and later XORed using another half of the text blocks. Data encryption standard (DES) is a Feistel network. Blowfish (other Schneier approach) is a Feistel network. Five of the advanced encryption standard (AES) submission is a Feistel network. Feistel networks have been studied long in cryptography, and we all know how they work. In all rounds of Twofish, 2 thirty two bit words (the 2 vertical lines with the left) serves as an input to the F function. All the words are divided into 4 bytes. These 4 bytes are transmitted via 4 distinct key based S-box. The 4 output bytes (the S-box has eight bit output and input) are integrated with a Maximum Distance Separable (MDS) matrix and integrated with thirty two-bit words. Next the 2 thirty two-bit words are integrated with a PHT, included in 2 round sub-keys, later XORed using the right half of the text. Also, it consists of 2 one-bit rotations, one after and before the XOR. As well, Twofish has somewhat named “postwhitening” & “prewhitening”; further subkeys are XORed to the text block beforehand of the initial and final rounds. The approach could seem random, however, they performed all for the purpose. Not anything is in Twofish accidentally. Everything in the approach cannot describe. The results are mean algorithm, lean i.e., simple and stronger.

All steps of the round functions are bijective. Specifically, each output is probable. We have seen numerous attacks against cipher that does not do not pose these properties to add it. The round functions mix-up the operation from distinct arithmetical sets: MDS matrix, S-box substitution, along with Galois field (GF) 2 (known as XOR), 1-bit rotations, and addition in GF (232). This makes the approach complex to attack arithmetically. The key based S-boxes are made to be strong against the 2 bigger attacks of the earlier 1990s—linear and differential cryptanalyses—and strong against any unknown attacks that occur. Numerous approach designer optimizes their design against certain attacks, without considering resistance against the unknown. This designed philosophy was quite distinct: good enough nastiness to (hopefully) resists unknown attacks and enough against known attacks. Key based S-boxes weren’t randomly elected, since they are in Blowfish. Rather, they carefully design S-box construction rules and verified them with each probable 128-bit keys (and a subset of probable longer keys) to ensure that each S-box is quite stronger. This method allows to integration of the strong S-box, strength of fixed with the strength of secret S-box. Also, Twofish has no weaker keys, since Blowfish ensures in decreased round variant.

2.3.3 B Band Encryption Using Blowfish

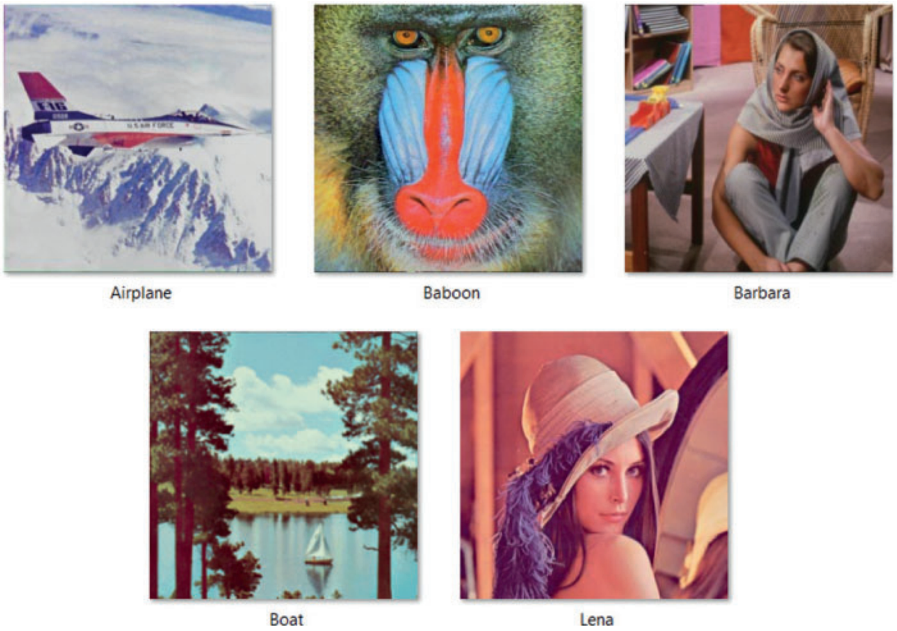
Next, the encryption of ‘B’ band takes place by the use of Lorenz Hyperchaotic system. The chaotic methods are extremely utilized in the data encryption field as its primary value and parameter were sensitive as well as pseudorandom. The low-dimension chaotic models are small key space and weak pseudorandom. So, several researchers are enhanced on low-dimension chaotic models by rising chaotic techniques to superior dimension. These enhanced high-dimension chaotic techniques are named hyperchaotic schemes. For generating the 4 pseudorandom orders which are needed by the encryption technique, it can implement the Lorenz hyperchaotic method for encrypting technique [22]. The Lorenz hyperchaotic scheme was explained as follows.

$$\begin{cases} x = a(y\dot{-}x) + w, \\ y = cx\dot{-}y - xz, \\ \dot{z} = xy - bz, \\ \dot{w} = -yz + rw, \end{cases} \tag{13}$$

where a, b, c, and r refers the 4 parameters of Lorenz hyperchaotic model. If $a = 10,\ b = 8/3,\ c = 28$, and $-1.52 \le r \le 0.06$, the Lorenz hyperchaotic method is a hyperchaotic state. The hyperchaotic technique was restated by utilizing Runge-Kutta approach if $r = -1$.

3 Performance Validation

The performance of the EIS-DHT technique is investigated using a benchmark USC-SIPI image dataset [23]. It contains a numerous collection of digital images with varying sizes of 256 ∗ 256, 512 ∗ 512, and 1024 ∗ 1024 pixels. The results are investigated interms of PSNR, structural similarity (SSIM), MSE, quality index (QI), embedding capacity, and execution time. Fig. 3 illustrates the sample images [24].



Airplane Baboon Barbara

Boat Lena

Figure 3: Sample images

Tab. 1 and Fig. 4 demonstrate the results analysis of the EIS-DHT technique under different images (256 ∗ 256) pixels. The table values denoted that the effective performance of the EIS-DHT technique with the higher PSNR, SSIM, and QI values along with lower MSE. For instance, with Lena cover image, the EIS-DHT technique has gained an increased PSNR of 56.50 dB, SSIM of 0.9971, and QI of 1.000 along with the reduced MSE of 0.1456. Simultaneously, with Baboon cover image, the EIS-DHT method has reached an improved PSNR of 56.76 dB, SSIM of 0.9992, and QI of 1.000 along with the lower MSE of 0.1372. Besides, with Barbara cover image, the EIS-DHT method has reached a maximum PSNR of 56.60 dB, SSIM of 0.9987, and QI of 1.000 along with the decreased MSE of 0.1423. Also, with Airplane cover image, the EIS-DHT technique has gained a higher PSNR of 55.95 dB, SSIM of 0.9979, and QI of 1.000 along with the reduced MSE of 0.1652. Moreover, with Boat cover image, the EIS-DHT methodology has obtained an increased PSNR of 55.70 dB, SSIM of 0.9995, and QI of 1.000 along with the minimal MSE of 0.1752.

Table 1: Performance of proposed EIS-DHT method on different images (256 ∗ 256)

Cover images	Secret images	MSE	PSNR	SSIM	QI
		0.1456	56.50	0.9971	1.000
		0.1372	56.76	0.9992	1.000
		0.1423	56.60	0.9987	1.000
		0.1652	55.95	0.9979	1.000
		0.1752	55.70	0.9995	1.000

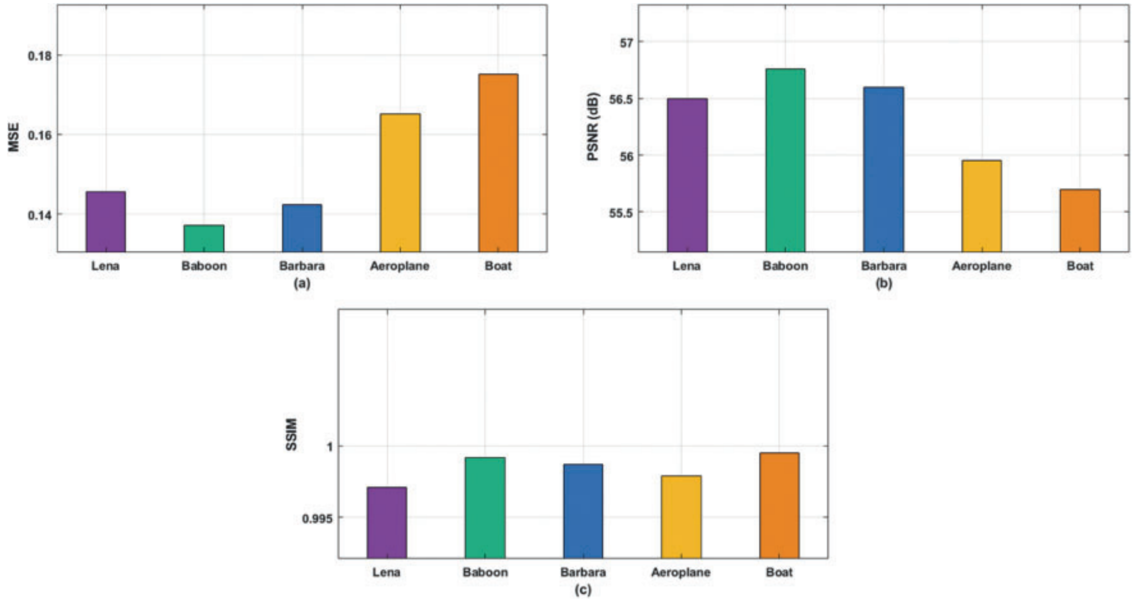


Figure 4: Result analysis of EIS-DHT model with different measures

Tab. 2 and Fig. 5 showcases the embedding capacity of the EIS-DHT technique under different test images. The EIS-DHT technique has resulted in effective performance with the maximum embedding capacities on all the applied images. For instance, the EIS-DHT technique has achieved an embedding capacity of 16.34% on the ‘Lena’ image. Furthermore, the EIS-DHT manner has reached an embedding capacity of 15.58% on the ‘Baboon’ image. In line with, the EIS-DHT manner has obtained an embedding capacity of 16.33% on the ‘Barbara’ image. Along with that, the EIS-DHT approach has gained an embedding capacity of 16.40% on the ‘Aeroplane’ image. Eventually, the EIS-DHT algorithm has reached an embedding capacity of 17.37% on the ‘Boat’ image.

Table 2: Embedding capacity analysis of EIS-DHT method

Images	Embedding capacity (%)
Lena	16.34
Baboon	15.58
Barbara	16.33
Aeroplane	16.40
Boat	17.37

Tab. 3 and Fig. 6 investigates the execution time analysis of the EIS-DHT technique on different test images. The results ensured that the EIS-DHT technique has demonstrated effective performance with a reduced embedding, extraction, and total time. For instance, on the test ‘Lena’ image, the EIS-DHT approach has obtained a lower embedding, extraction, and total time of 33.75, 17.82, and 51.57 s respectively. Concurrently, on the test ‘Barbara’ image, the EIS-DHT approach has reached a lesser embedding, extraction, and total time of 34.56, 18.72, and 53.28 s correspondingly. Simultaneously, on the test ‘Boat’ image, the EIS-DHT methodology has achieved a minimum embedding, extraction, and total time of 35.06, 18.57, and 53.63 s respectively.

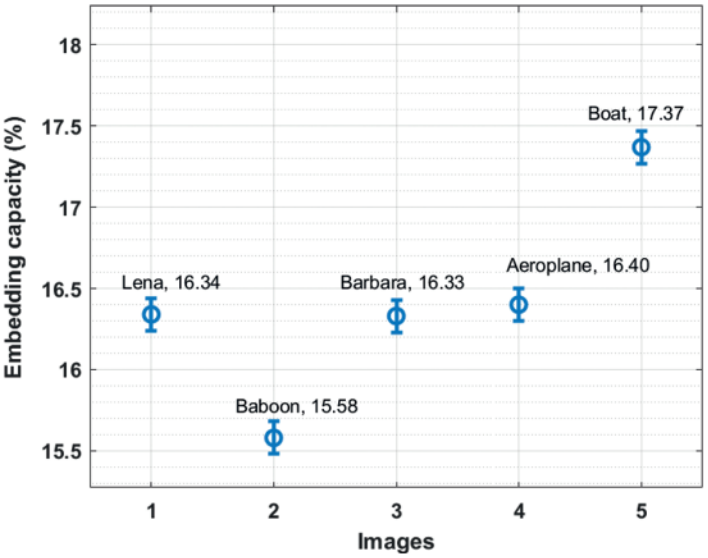


Figure 5: Embedding capacity analysis of EIS-DHT model

Table 3: Execution time analysis of the EIS-DHT technique on applied test images

Images	Embedding time (s)	Extraction time (s)	Total time (s)
Lena	33.75	17.82	51.57
Baboon	34.26	18.02	52.28
Barbara	34.56	18.72	53.28
Aeroplane	34.52	18.85	53.37
Boat	35.06	18.57	53.63

A brief comparative study of the EIS-DHT technique with existing methods take place in Fig. 7 and Tab. 4. The results denoted that Goa et al. have shown worse performance on all the applied images with the least PSNR value. Likewise, the techniques devised by Hou et al., Ou et al., and Dragoi and Coltuc have reached a moderately significant performance over the earlier methods. However, the proposed EIS-DHT technique has resulted in a superior outcome over the existing techniques with the higher PSNR value on the applied test images.

In order to showcase the improved security performance of the EIS-DHT technique, a brief comparison study is made under varying kinds of attacks in Tab. 5. The results exhibited that the EIS-DHT technique has accomplished proficient results with the minimal MSE and RMSE values and maximum PSNR and normalized correlation coefficient (NCC) values. Under the Erosion attack, the EIS-DHT technique has offered an MSE of 127.0332, RMSE of 11.2709, PSNR of 27.0916 dB, and NCC of 0.9625. In line with, under the Gaussian Noise attack, the EIS-DHT approach has obtainable an MSE of 47.0116, RMSE of 6.8565, PSNR of 31.4088 dB, and NCC of 0.9998. Likewise, under the Dilation attack, the EIS-DHT method has existed an MSE of 137.1452, RMSE of 11.7109, PSNR of 26.7590 dB, and NCC of 0.9614. Meanwhile, under the S&P noise attack, the EIS-DHT manner has offered an MSE of 160.1414, RMSE of 12.6547, PSNR of 26.0858 dB, and NCC of 0.9997. Additionally, under the Speckle attack, the EIS-DHT method has offered an MSE of 317.1320, RMSE of 17.8082, PSNR of 23.1184 dB, and NCC of 0.9982. At last, under the Poisson noise attack, the EIS-DHT methodology has accessible an MSE of 117.8354, RMSE of 10.8552, PSNR of 27.4180 dB, and NCC of 1.0000. The experimental analysis ensured that the EIS-HDT technique has found to be an effective tool to accomplish secure data transmission in IIoT environment.

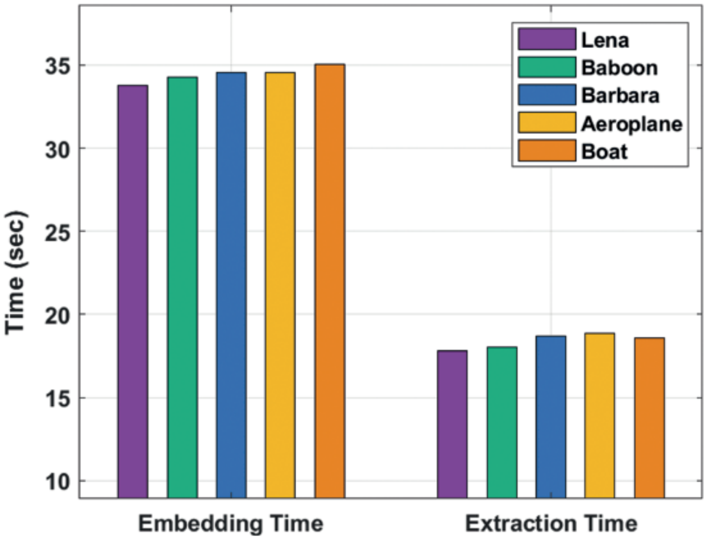


Figure 6: Execution time analysis of EIS-DHT method

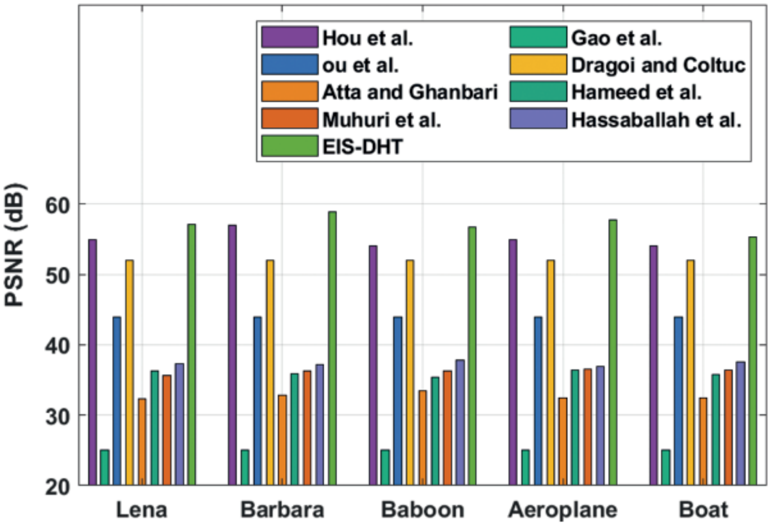


Figure 7: PSNR analysis of EIS-DHT model with existing techniques

Table 4: Performance of existing with proposed EIS-DHT method on different images (512 ∗ 512)

Methods	PSNR (dB)				
	Lena	Barbara	Baboon	Aeroplane	Boat
Hou et al.	55.00	57.00	54.00	55.00	54.00
Gao et al.	25.00	25.00	25.00	25.00	25.00
Ou et al.	44.00	44.00	44.00	44.00	44.00
Dragoi et al.	52.00	52.00	52.00	52.00	52.00
Atta et al.	32.27	32.89	33.44	32.45	32.47
Hameed et al.	36.32	35.91	35.40	36.41	35.72
Muhuri et al.	35.68	36.34	36.28	36.61	36.43
Hassaballah et al.	37.26	37.25	37.81	36.92	37.52
EIS-DHT	57.09	58.91	56.78	57.82	55.33

Table 5: Results analysis of EIS-DHT with existing techniques under different attacks

Type of attacks	MSE	RMSE	PSNR	NCC
Erosion	127.0332	11.2709	27.0916	0.9625
Gaussian noise	47.0116	6.8565	31.4088	0.9998
Dilation	137.1452	11.7109	26.7590	0.9614
S&P noise	160.1414	12.6547	26.0858	0.9997
Speckle noise	317.1320	17.8082	23.1184	0.9982
Poisson noise	117.8354	10.8552	27.4180	1.0000

4 Conclusion

In this study, an efficient EIS-DHT technique has been developed for secure communication in IIoT environment. The EIS-DHT technique can be designed to hide the secret image into the cover image to accomplish secrecy. The presented model involves different stages of operations such as channel extraction, decomposition, QBWO based optimal pixel selection, encryption, and embedding process. The QBWO algorithm derives an objective function to design an image steganography technique in such a way that the MSE gets minimized and PSNR gets maximized. For examining the improved data hiding performance of the EIS-DHT technique, a set of experimentation were carried out and the results are examined based on distinct metrics. The experimental outcomes stated the supremacy of the EIS-DHT technique over the other existing techniques and ensure maximum security. As a part of future scope, the performance of the EIS-DHT technique can be improved by the use of hybrid metaheuristics for optimal pixel selection.

Acknowledgement: This work was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, under grant No. (D-336-611-1443). The authors, therefore, gratefully acknowledge DSR technical and financial support.

Funding Statement: This research work was funded by Institution Fund projects under Grant No. (IFPRC-215-249-2020) Therefore, authors gratefully acknowledge technical and financial support from the Ministry of Education and King Abdulaziz University, DSR, Jeddah, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] R. J. A. Cabrera, C. A. P. Legaspi, E. J. G. Papa, R. D. Samonte and D. D. Acula, "HeMatic: An automated leukemia detector with separation of overlapping blood cells through image processing and genetic algorithm," in *2017 Int. Conf. on Applied System Innovation, ICASI 2017. Proc.: IEEE*, Sapporo, Japan, pp. 985–987, 2017.

[2] Y. J. Choi, H. J. Kang and I. G. Lee, "Scalable and secure internet of things connectivity," *Electronics*, vol. 8, no. 7, pp. 752, 2019.

[3] K. Wang, Y. Wang, Y. Sun, S. Guo and J. Wu, "Green industrial internet of things architecture: An energy-efficient perspective," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 48–54, 2016.

[4] Z. Bi, L. D. Xu and C. Wang, "Internet of things for enterprise systems of modern manufacturing," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1537–1546, 2014.

[5] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[6] S. Dowling, M. Schukat and H. Melvin, "A ZigBee honeypot to assess IoT cyberattack behaviour," in *2017 28th Irish Signals and Systems Conf. (ISSC)*, Killarney, Co Kerry, Ireland, pp. 1–6, 2017.

[7] M. H. Eldefrawy, N. Pereira and M. Gidlund, "Key distribution protocol for industrial internet of things without implicit certificates," *IEEE Internet Things Journal*, vol. 6, no. 1, pp. 906–917, 2019.

[8] P. Mell and T. Grance, "The nist definition of cloud computing," *National Institute of Standards and Technology*, vol. 53, no. 6, pp. 50, 2009.

[9] A. Acar, H. Aksu, A. S. Uluagac and M. Conti, "A survey on homomorphic encryption schemes: Theory and implementation," *ACM Computing Surveys*, vol. 51, no. 4, pp. 1–35, 2018.

[10] S. Xiang and J. He, "Database authentication watermarking scheme in encrypted domain," *IET Information Security*, vol. 12, no. 1, pp. 42–51, 2018.

[11] J. Feng, L. T. Yang, R. Zhang and B. S. Gavuna, "Privacy-preserving tucker train decomposition over blockchain-based encrypted industrial iot data," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 7, pp. 4904–4913, 2021.

[12] Q. Li, Y. Yue and Z. Wang, "Deep robust cramer shoup delay optimized fully homomorphic for iiot secured transmission in cloud computing," *Computer Communications*, vol. 161, pp. 10–18, 2020.

[13] Z. Xia, L. Jiang, X. Ma, W. Yang, P. Ji *et al.,* "A Privacy-preserving outsourcing scheme for image local binary pattern in secure industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, pp. 629–638, 2020.

[14] K. Lin, X. Xu and H. Gao, "TSCRNN: A novel classification scheme of encrypted traffic based on flow spatiotemporal features for efficient management of IIoT," *Computer Networks*, vol. 190, pp. 107974, 2021.

[15] P. W. Khan and Y. Byun, "A Blockchain-based secure image encryption scheme for the industrial internet of things," *Entropy*, vol. 22, no. 2, pp. 175, 2020.

[16] A. K. Bairagi, R. Khondoker and R. Islam, "An efficient steganographic approach for protecting communication in the internet of things (IoT) critical infrastructures," *Information Security Journal: A Global Perspective*, vol. 25, no. 4–6, pp. 197–212, 2016.

[17] J. H. Horng, S. Xu, C. C. Chang and C. C. Chang, "An efficient data-hiding scheme based on multidimensional mini-suDoKu," *Sensors*, vol. 20, no. 9, pp. 2739, 2020.

[18] F. S. Hassan and A. Gutub, "Efficient reversible data hiding multimedia technique based on smart image interpolation," *Multimedia Tools and Applications*, vol. 79, no. 39–40, pp. 30087–30109, 2020.

[19] M. Hassaballah, M. A. Hameed, A. I. Awad and K. Muhammad, “A novel image steganography method for industrial internet of things security,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7743–7751, 2021.

[20] U. Ambika, R. L. Biradar and V. Burkpalli, “Encryption-based steganography of images by multiobjective whale optimal pixel selection,” *International Journal of Computers and Applications*, pp. 1–10, 2019. http://doi.org/10.1080/1206212X.2019.1692442.

[21] K. S. Sarath and S. Sekar, “Black widow optimization algorithm: Optimal designing and modelling and of llc resonant converter,” *Journal of Computational Mechanics, Power System and Control*, vol. 3, no. 1, pp. 31–41, 2020.

[22] A. H. Jassem, A. T. Hashim and S. A. Ali, “Enhanced blowfish algorithm for image encryption based on chaotic map,” in *2019 First Int. Conf. of Computer and Applied Sciences (CAS)*, Baghdad, Iraq, pp. 232–237, 2019.

[23] X. Zhang, L. Wang, Y. Niu, G. Cui and S. Geng, “Image encryption algorithm based on the h-fractal and dynamic self-invertible matrix,” *Computational Intelligence and Neuroscience*, vol. 2019, pp. 1–12, 2019.

[24] A. G. Weber, “The USC-SIPI image database version 5,” *USC-SIPI Report*, vol. 315, no. 1, 1997.