Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.024902
Article

Tech Science Press

Blockchain Enabled Optimal Lightweight Cryptography Based Image Encryption Technique for IIoT

R. Bhaskaran[1], R. Karuppathal[1], M. Karthick[2], J. Vijayalakshmi[3], Seifedine Kadry[4] and Yunyoung Nam[5,*]

[1]Department of Information Technology, PSNA College of Engineering and Technology, Dindigul, 624622, India
[2]Department of Electronics and Communication Engineering, K. Ramakrishnan College of Engineering, Tiruchirappalli, 621112, India
[3]Department of Electronics and Communication Engineering, Kongu Engineering College, Perundurai, 638060, India
[4]Deparmtent of Applied Data Science, Noroff University College, Kristiansand, Norway
[5]Department of Computer Science and Engineering, Soonchunhyang University, Asan, Korea
*Corresponding Author: Yunyoung Nam. Email: ynam@sch.ac.kr

Received: 03 November 2021; Accepted: 17 December 2021

Abstract: Industrial Internet of Things (IIoT) and Industry 4.0/5.0 offer several interconnections between machinery, equipment, processes, and personnel in diverse application areas namely logistics, supply chain, manufacturing, transportation, and healthcare. The conventional security-based solutions in IIoT environment get degraded due to the third parties. Therefore, the recent blockchain technology (BCT) can be employed to resolve trust issues and eliminate the need for third parties. Therefore, this paper presents a novel blockchain enabled secure optimal lightweight cryptography based image encryption (BC-LWCIE) technique for industry 4.0 environment. In addition, the BC-LWCIE technique involves the design of an optimal LWC based hash function with optimal key generation using chicken swarm optimization (CSO) algorithm. Moreover, the CSO algorithm derives a fitness function with the maximization of peak signal to noise ratio (PSNR). The BC-LWCIE technique stores the cryptographic pixel values of the encrypted image in the BCT to ensure secrecy in the IIoT environment. In order to highlight the enhanced security performance of the BC-LWCIE technique, a series of simulations were carried out and the results demonstrated the betterment of the BC-LWCIE technique over the recent techniques.

Keywords: Lightweight cryptography; hash value; blockchain; image encryption; security; industrial iot

1 Introduction

The automation of an industrial system is going to be attained *via* connected cyber physical system (CPS) in Industry 4.0; hence, permitting the production processes and industrial infrastructure for transforming to dynamic and autonomous systems [1]. The entity in these are extremely incorporated networks that should broadcast and perform as smart devices to independently operate with one another and to attain a general objective. Information and communication technology (ICT) is expected to play an important role in sustainable industrialization for supporting social, environmental, and global economic sustainability. IIoT, a conventional CPS, is determined as "computers, machines, and persons assisting smart industrial operation, with an innovative data analytics for transformation business outcome" [2]. IIoT allows the incorporation of internet infrastructure, wireless sensor network (WSN), and transmission protocol using the process assisting smart industrial operation to monitor, analyses, and manage. This internetwork of everything in the production scheme contexts helps in automation of industrial performance and enhances safety, intelligence, and efficiency. The communication layer, application layer, and physical layer form the 3 layers of IIoT infrastructure. The physical layers include physical devices such as sensors, actuators, smart terminals, manufacturing equipment, and datacenters. The communication layers use network technologies, like WSN, 5G, machine-to-machine (M2M) communications, and actuators, for the incorporation of several devices in the physical layers for industrial automation and manufacturing [3]. The computing, control, and networking architectures of the cyber system enable the intelligent operation and networking of the production system. Fig. 1 shows the evolution of industry 4.0.

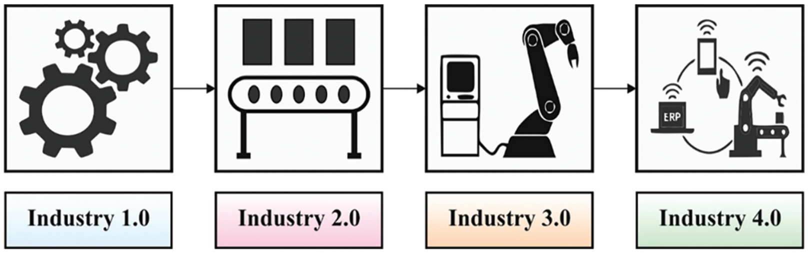


Figure 1: Evolution of industry 4.0

Video and Image surveillances play an important part in IIoT aimed network computing systems. This can be employed for building business intelligence, data management system, realtime analyses, and scientific research [4]. Image sensors based solution helps in work process safety and enhancing maintenance. Additionally, they considerably develop the quality of productivity. Computer vision technologies are employed for the visual quality control and continuous monitoring of production process. Increasing innovative sensors and cameras are employed in the industry [5]. Also, this development brings novel problems like absence of built-in safety. Determining scalability, reliability, and IoT management in this sensor is highly complicated. This novel challenge demands secure and safe device and application with no human interference.

Cyberattacks against automation in the IIoT environments have extensive effects [6]. They could interrupt the process of manufacturing, and sensitive information might be damage. They might contain negative impacts on the quality of product. Also, they could harm humans/property. Present solutions for image encryption don't assist smart industries in which peers are de-centralized. The significance of blockchain in Industry 4.0 applications, like IIoT, is evident [7]. *E.g.*, there has been attempt to make use of blockchain in IIoT safety and in facilitating information storage and collection methods. In another word, blockchain provides a secure, immule and trusted environment for many entities (organizations and individuals) for exchanging assets or data, perform and collaborate transaction. As there is no central controlling authority in the blockchain framework, beforehand a block could be approved for inclusion to the ledger, the contributing nodes should attain a consensus by operating a predetermined consensus approach employed in the blockchain protocols.

This paper presents a novel blockchain enabled secure optimal lightweight cryptography based image encryption (BC-LWCIE) technique for industry 4.0 environment. Besides, the BC-LWCIE technique involves the design of an optimal LWC based hash function with optimal key generation using chicken swarm optimization (CSO) algorithm. Furthermore, the CSO algorithm derives a fitness function with the maximization of peak signal to noise ratio (PSNR). The BC-LWCIE technique saves the cryptographic pixel values of the encrypted image in the BCT to guarantee secrecy in the IIoT environment. For examining the improved secrecy of the BC-LWCIE technique, a comprehensive experimental analysis takes place using benchmark images.

2 Literature Review

Abbas et al. [8] proposed a decentralized data management system for secure and smart transportations which employs blockchain and the IoT in sustainable smart city environments for solving the information susceptibility problems. Intelligent transport mobility systems demand making connected transit systems for ensuring efficiency and flexibility. This study introduces previous knowledge and later provides a Hyperledger Fabric based data structure which supports a trusted, secured intelligent transport systems. Gao et al. [9] proposed a privacy protection identity verification system on the basis of blockchain. The users autonomously generate several identity data, and this identity could be employed for applying identity certificates. Authority uses the ECDSA signature algorithms and RSA encryption algorithms for completing the distribution of identity certificates on the basis of identity data as well as finalize the registering of identity verification *via* intelligent contracts on the blockchain.

In Hu et al. [10], a P2P DE transaction method for the IIoTs has been presented on the basis of blockchain. First, blockchain based peer to peer distributed transaction frameworks was made, *i.e.*, highly appropriate for generalized energy transactions according to a conventional transaction scenario of the IIoTs. With a smart contract and credit value evaluation for ensuring the non-tampering, transparency, and openness of the credit score. Shen et al. [11] proposed secure SVM, *i.e.*, a PPSVM training system through blockchain based encrypted IoT information. They use the blockchain methods for building reliable and secure information exchange platforms amongst several data providers, in which IoT information is encrypted and later listed on a distributed ledger. Also, designed secured building blocks, like secured comparison and secured polynomial multiplication, through applying a Paillier, homomorphic cryptosystem, and create a secured SVM training algorithms that only require 2 communications in an individual iteration, without needing a trusted 3rd party.

Abd El-Latif et al. [12] presented novel encryption and authentication protocols on the basis of QIQW approach. The presented method is used for building a blockchain architecture for secured data transmissions amongst IoT devices. Rather than employing traditional cryptographic hash function, quantum hash function based QIQW is used to link a block of chains. In Li et al. [13], a storage solution and security transmission are presented based on the sensing images for blockchain in the IoT. First, these solutions intellectually sense user's image data and divide this sensed data into smart blocks. Next, various blocks of information are transmitted and encrypted safely *via* smart encryption algorithm. Lastly, storage and signature verification are executed by a smart authentication method.

Banerjee et al. [14] proposed a new blockchain intended fine grained users accessing control systems for data scalability and security in IIoT environments. The presented system support ciphertext and many attributes authority and constant size keys. The collected information using the IoT smart device is encrypted by the CP-ABE and transmit to their adjacent gateway node. Then, the gateway node forms the transaction from the encrypted information from the smart device *i.e.*, employed for creating a partial block. Li et al. [15] make use of blockchain technologies that serve as a secure tamper proof distributed ledger to IoT devices. In the presented approach, they assigned an exclusive ID for all separate devices and recorded them to the blockchain, thus we could validate one another without a central authority. Also, designed an information security method through hashing considerable data (viz., firmware) to the blockchain in which other states changing of the information could be identified instantly.

In Wang et al. [16], a reputation system is presented for encouraging abnormal and normal nodes to partake in network collaboration in an effective means. For guiding the behaviour, credit based incentive approaches were introduced. The punishment and reward factors are developed in the revenue payment function of reputation. The efficacy is that the non-cooperative behaviors are punished, and the cooperative behaviors are rewarded. In Khalid et al. [17], decentralized authentication and access control mechanisms were introduced for lightweight IoT devices and are relevant to various situations. The result attained from the experiment demonstrates an increased efficiency of the presented method than an advanced blockchain based verification method. Velmurugadass et al. [18] construct a Cloud based SDN algorithm, it includes hundred mobile Nodes (IOT devices), open flow switch, and Blockchain based cloud server, controller, investigator, and AS. At first, each user is listed by an AS and attain their secret key from AS based HSO algorithm. In the mobile node, the packet is encrypted with ECIES approach and transmit to the cloud servers.

3 Design of BC-LWCIE Technique

In this study, a new BC-LWCIE technique is derived to accomplish secure image transmission in the Industry 4.0 environment. The BC-LWCIE technique involves three major processes namely LWC based encryption process, CSO algorithm based key generation process, and BCT based secure transmission. The detailed working of these processes is provided in the succeeding sections.

3.1 Process Involved in LWC Based Image Encryption

In the presented method, the image in IIoT is encrypted through the use of LWC-hash function using optimum key provided to the cipher images. The basic approach of images could be viewed as a course of actions of block. The coherent information existing in images is due to the relationships amongst the image modules in a provided yield of course of actions. The presented hash function utilizes the concept of change over an unsustainable measure of digital data to a predetermined measure of data, *via* rolling-out slight improvement in input data feature, bringing on key modifications in yield data. Hash function is used to recognize the image of some length as input, provide a fixed length at fast rate. Additionally, the optimum key arrangement makes use of CSO optimization method in the hash function. The proficiency and security of the images in IIoT are based completely on the inherent ciphers that need confused computation.

The cryptographic hash function [19] licenses one to quickly confirm that any information coordinate stores hash esteem, still make it complex to regenerate the information only in the hash. The presented image security method considers the hash function using 3 characteristics provided in the following need to be satisfied for this study.

Preimage Resistance (PR): This component has pre-indicated yield through unimaginable input function using applicable hash value. *E.g.*, inspiring images I, hash function H and the hash calculation of image security are $H(I)$.

Second Preimage Resistance (SPR): It is computational complex for locating following input that has undistinguishable yield from each predefined data I. Hence the hash calculation of this SPR is $H_1(I) = H_2(I)$ representing that the hash function validation consists of $2n$ work.

Collision Resistance (CR): A hash impacts occur while 2 random images, I_1 & I_2 hash to related esteem. Therefore, the hash esteem is defined as $(I_1) = H(I_2)\ I_1 \neq I_2$. Furthermore, it is suitable for alternating the relation in a hash function and in addition perform multiblock collisions to indicate 2 influencing messages, all comprised of somewhere around 2 blocks.

Cryptographic hash functions are a mathematical model which takes a subjective size of data and encodes it to a fixed size of data, generally closer to 128 bits. Instead of using a hash function with parameter size data, a function using fixed size data is created and used maximum times. Robustness denotes the hashing esteem remains same afterward conventional attacks, that assurance the normal image security.

3.2 Optimal Key Generation Using CSO Algorithm

By using aforementioned procedure, the optimum key is determined using the CSO algorithm with an objective function of maximum PSNR. The assumptions to the fundamental CSO technique is given as follows [20]:

1) In chicken swarm, many groups are available. All the groups have dominant rooster, the combine of hen as well as chick.
2) Due to fitness value computed to individuals from chicken swarm, various individuals with optimum fitness value were utilized as roosters, different individuals with reduced fitness value are utilized as chicks, and the residual individuals are utilized as hens.
3) Assume the number of roosters from the chicken swarm exists *RN*, the amount of hens that exist HN, the amount of chicks that exist CN, and the amount of chick's mothers in MN. The single hen was arbitrarily elected as chick mother from all groups.
4) Afterward, all *G* iterations of this technique depend upon fitness values of individuals, re-define that individuals were utilized as rooster that individuals are utilized as hens and that individual is utilized as chicks.
5) In all groups of population, the hens follow the roosters for finding food and arbitrarily compete with another individual for food. An individual with optimum fitness values from the population is highly possible for obtaining food.

The roosters, hens, and chicks from the chicken swarm utilize distinct place upgrade equations. The equivalent place upgrade equation to the rooster as [21]:

$$x_i^R(t+1) = x_i^R(t)^* \left(1 + N\left(0,\ \sigma^2\right)\right) \tag{1}$$

where R represents the individuals are roosters, $N(0, \sigma^2)$ implies the Gaussian distribution with mean and variance σ^2.The equation to calculate the variance σ^2 as:

$$\sigma^2 = \begin{cases} 1 & if\ f_i < f_k \\ exp\left(\dfrac{(f_k - f_i)}{|f_i| + \varepsilon}\right), & otherwise \\ & i,\ k \in [1, 2,\ \ldots,\ RN],\ k \neq i \end{cases} \tag{2}$$

where ε is utilized for avoiding zero division error, and ε refers the minimum constant from the computer. Combine of i and $k \in [1, 2, \ldots, RN]$ are rooster indices, arbitrarily elected in the rooster group, and i is not equivalent to k. The f_i and f_k signify the fitness value of $i-th$ as well as $k-th$ roosters correspondingly.

The equivalent place upgrades equation to the hens is as:

$$x_i^H(t+1) = x_i^H(t) + S_1^* rand^* \left(x_{r1}^R(t) - x_i^H(t)\right) + S_2^* rand^* \left(x_{r2}(t) - x_i^H(t)\right) \tag{3}$$

$$S_1 = \exp\ ((f_i - f_{r1})/(abs(f_i) + \epsilon)) \tag{4}$$

$$S_2 = \exp\ (f_{r2} - f_i) \tag{5}$$

where *rand* implies the uniform arbitrary number from 0 and 1. R denotes the individuals are rooster. H refers to the individuals are hens. $r1 \in [1, 2, \ \ldots, \ RN]$ is an index of roosters that is $i-th$ hen's group-mate, but $r2 \in [1, 2, \ \ldots, \ RN + HN]$ is an index of chickens (roosters/hens) that is arbitrarily selected in the swarms. $r1$ is not equivalent to $r2$.

The equivalent place upgrade equation to the chicks is as follows:

$$x_i^C(t+1) = x_i^C(t) + FL*\left(x_m^H(t) - x_i^C(t)\right) \tag{6}$$

where m implies the chick mother index from the $i-th$ group, C defines the individual as chick, H refers the individuals were hens, and FL represents the uniform arbitrary number from 0 and 2.

3.2.1 Encryption Process

Consider 256-pixel plain images based on the matrix with rows and columns when the pixel values are in range of zero and 255. According to this, the hash values are made for the supposed input images. It is mathematically given as follows

$$HASH\ (En(Image,\ opt\_pu_k),\ H_k) = H(image,\ H_k)$$

$$HASH\ (En(Image,\ opt\_pu_{k1}), H_k)\ = HASH(En(Image,\ opt\_pu_{k2}),\ H_k) \tag{7}$$

In Eq. (7), pu_{k1}, pu_{k2} denotes optimum encryption key and using this, the images are separated into blocks; every dimension 16×16. Afterward separating, there would be overall 256 blocks. It uses several averages while encrypting distinct input images with similar series on the basis of hash function.

3.2.2 Decryption Process

The optimum private keys are made by the diffusion method. The security of cipher must depend on the decryption key, pr_{k1}, pr_{k2} because an adversary could improve the plain images in the observed cipher images when get pr_{k1}, pr_{k2}.

$$Decrypted\ Image\ = Decrypt\ (\overline{C}) \tag{8}$$

$$HASH\ (Dec) = C \oplus mod\ (H_k + Cipher,\ 256) \oplus pr_{k1}, pr_{k2} \tag{9}$$

The decryption method is managed as a minimum of one cryptographic key. Generally, the key utilized to the process of decryption and representation isn't really undistinguishable, based on the architecture used.

3.3 Blockchain Technology for Security

In IIoT scheme, private blockchain systems have emerged. In this method, the admin could form the non-endorser and endorser peers. As the sensors don't have several energy resources to operate the mining method, few nodes act as authenticator nodes. This node attains a consensus for adding novel blocks to the chain. The accountability of nodes in a network is to endure the replication of a blockchain. Also, peer/node is accountable to process the transaction. In IIoT network, the node is electricity/battery powered device which carries out data collection and transmission. The nodes in the blockchain integrate state databases, distinct blocks, smart contracts, and policies [22]. The structure of the blockchain is given in Fig. 2.

In the permitted blockchain, few nodes are stated as endorser nodes using the system administrators. This peer could confirm the transaction. The entire method begins with the image sensor nodes that can be any devices that task is to take an image. The image would be transmitted to various nodes interconnected with the blockchain. Once validated by this node, this would become a portion of the chain. The end users could access the needed images through the hashed transaction ID of certain images.

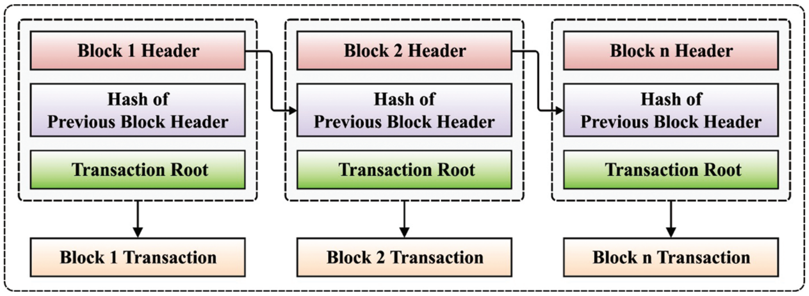


Figure 2: Structure of blockchain

4 Performance Validation

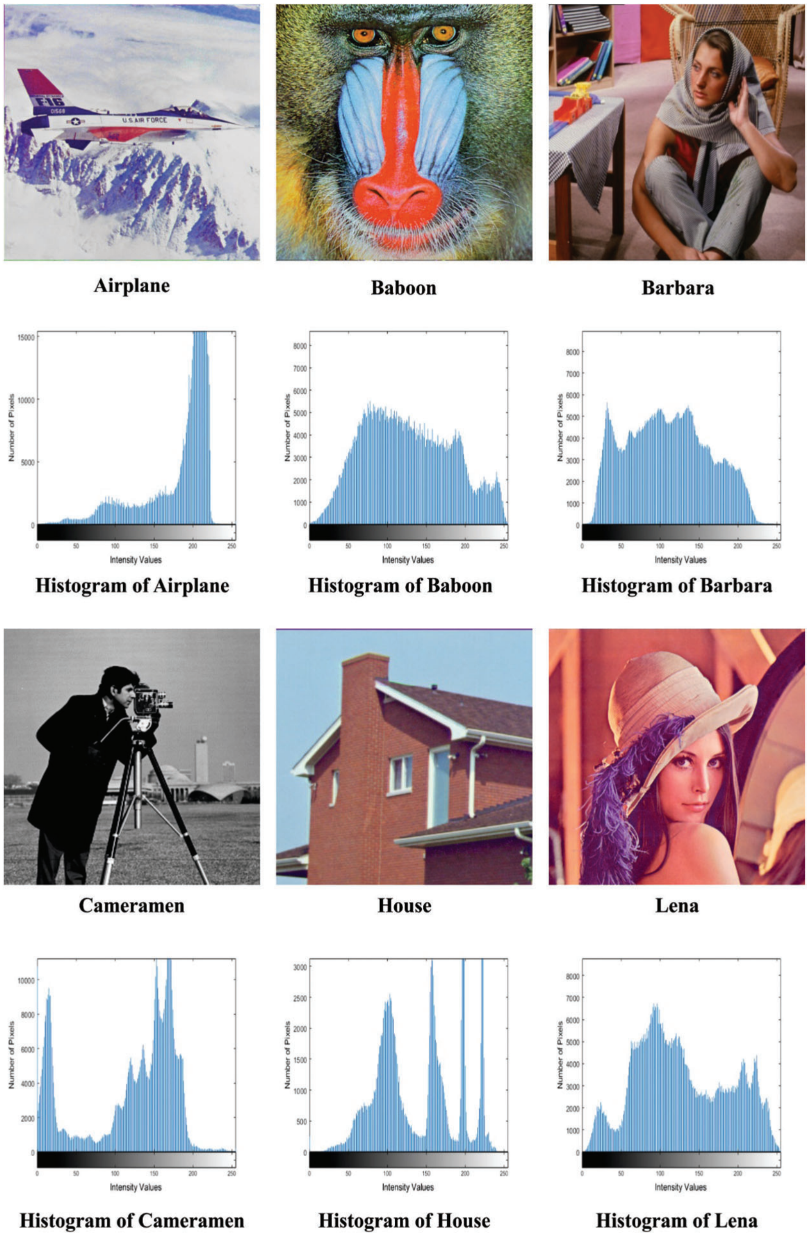
This section investigates the performance of the BC-LWCIE technique on the benchmark test images. In addition, the results are inspected interms of different performance measures. Fig. 3 shows the sample set of original images along with the histogram.

Fig. 4 illustrates the sample visualization results of the BC-LWCIE technique. Fig. 4a shows the original set of input images and the encrypted images are demonstrated in Fig. 4b. The figure has shown that the encrypted images do not reveal any useful data.

Tab. 1 examines the performance of the BC-LWCIE technique interms of MSE. The results ensured that the BC-LWCIE technique has accomplished effective outcomes with minimal MSE. For instance, with Lena image, the BC-LWCIE technique has resulted in a minimum MSE of 0.027 whereas the HF, HCS, and HECS techniques have attained a maximum MSE of 5.390, 1.269, and 0.073. Simultaneously, with Baboon image, the BC-LWCIE approach has resulted in a minimal MSE of 1.475 whereas the HF, HCS, and HECS methods have reached a higher MSE of 42.760, 8.890, and 3.095. Concurrently, with Airplane image, the BC-LWCIE approach has resulted in a minimum MSE of 0.053 whereas the HF, HCS, and HECS manners have gained an increased MSE of 5.080, 1.269, and 0.156.

A comprehensive PSNR analysis of the BC-LWCIE technique with existing techniques takes place in Tab. 2 and Fig. 5. The results exhibited that the BC-LWCIE technique has accomplished effective outcomes with the higher PSNR of 63.82dB whereas the HF, HCS, and HECS techniques have obtained a reduced PSNR of 40.81dB, 47.10dB, and 59.52dB respectively. Moreover, the results showcased that the BC-LWCIE method has accomplished effective results with the maximum PSNR of 46.44dB whereas the HF, HCS, and HECS techniques have gained a lower PSNR of 31.82dB, 38.64dB, and 43.22dB correspondingly. Furthermore, the results demonstrated that the BC-LWCIE manner has accomplished effective outcomes with superior PSNR of 60.89dB whereas the HF, HCS, and HECS methodologies have achieved a decreased PSNR of 41.78dB, 46.13dB, and 56.20dB correspondingly.

A brief NPCR analysis of the BC-LWCIE method with existing manners takes place in Tab. 3 and Fig. 6. The results outperformed that the BC-LWCIE technique has accomplished effective outcomes with the higher NPCR of 99.570% whereas the HF, HCS, and HECS approaches have gained the least NPCR of 79.753%, 81.280%, and 99.221% correspondingly. Likewise, the results exhibited that the BC-LWCIE algorithm has accomplished effective outcomes with the superior NPCR of 99.230% whereas the HF, HCS, and HECS techniques have obtained a minimum NPCR of 79.753%, 92.350%, and 98.076% correspondingly. Also, the results exhibited that the BC-LWCIE manner has accomplished effectual outcomes with the higher NPCR of 99.340% whereas the HF, HCS, and HECS techniques have reached a lower NPCR of 79.372%, 82.807%, and 98.839% correspondingly.



Airplane

Baboon

Barbara

Histogram of Airplane

Histogram of Baboon

Histogram of Barbara

Cameramen

House

Lena

Histogram of Cameramen

Histogram of House

Histogram of Lena

Figure 3: Original images and its histogram

A detailed security level (SL) analysis of the BC-LWCIE algorithm with existing approaches takes place in Tab. 4 and Fig. 7. The outcomes demonstrated that the BC-LWCIE manner has accomplished performance results with increased r SL of 96.74% whereas the HF, HCS, and HECS techniques have obtained a reduced SL of 80.75%, 85.55%, and 93.14% respectively. Besides, the results portrayed that the BC-LWCIE technique has accomplished effective outcomes with the maximal SL of 89.52% whereas the HF, HCS, and HECS manners have achieved a lesser SL of 71.16%, 80.35%, and 85.15% respectively. Eventually, the results showcased that the BC-LWCIE technique has accomplished effectual outcomes with the superior SL of 97.81% whereas the HF, HCS, and HECS methodologies have obtained a reduced SL of 90.74%, 92.74%, and 94.34% correspondingly.

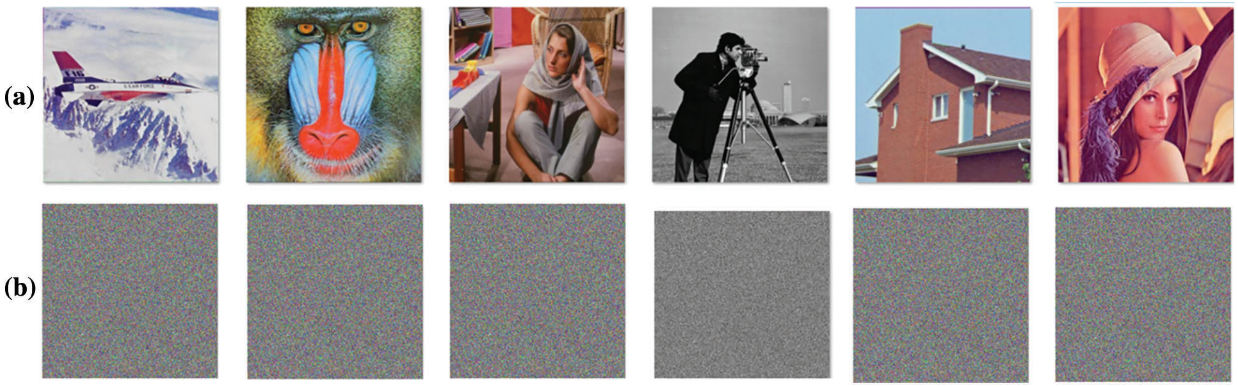


Figure 4: Sample results (a) original images (b) encrypted images

Table 1: MSE analysis of BC-LWCIE model with different images

	Mean square error			
Images	HF model	HCS model	HECS model	BC-LWCIE
Lena	5.390	1.269	0.073	0.027
Barbara	97.490	8.420	0.738	0.256
Baboon	42.760	8.890	3.095	1.475
House	6.740	4.830	0.296	0.126
Airplane	5.080	1.269	0.156	0.053
Cameraman	4.320	1.585	0.063	0.019

Table 2: PSNR analysis of BC-LWCIE model with different images

	PSNR (dB)			
Images	HF model	HCS model	HECS model	BC-LWCIE
Lena	40.81	47.10	59.52	63.82
Barbara	28.24	38.88	49.45	54.05
Baboon	31.82	38.64	43.22	46.44
House	39.84	41.29	53.42	57.13
Airplane	41.07	47.10	56.20	60.89
Cameraman	41.78	46.13	60.14	65.34

Tab. 5 examines the comparative analysis of BC-LWCIE model interms of encryption time (ET) and decryption time (DT). Fig. 8 inspects the performance of the BC-LWCIE manner with respect to ET. The outcomes make sure that the BC-LWCIE manner has accomplished effectual results with the lesser ET. For instance, with Lena image, the BC-LWCIE technique has resulted in a reduced ET of 0.17s whereas the HCS and HECS methods have attained a higher ET of 0.21s and 0.19s.

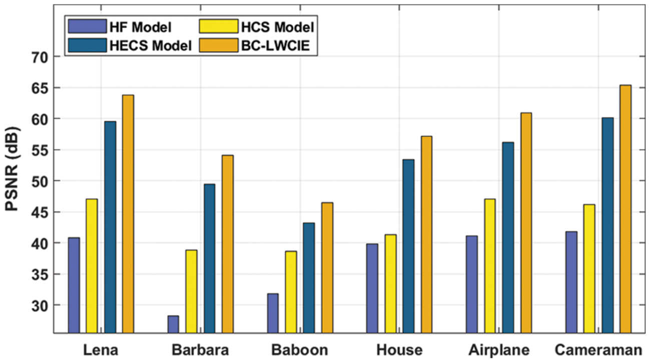


Figure 5: PSNR analysis of BC-LWCIE model with varying images

Table 3: NPCR analysis of BC-LWCIE model with different images

	NPCR (%)			
Images	HF model	HCS model	HECS model	BC-LWCIE
Lena	79.753	81.280	99.221	99.570
Barbara	69.065	79.372	96.549	97.260
Baboon	79.753	92.350	98.076	99.230
House	82.044	89.296	95.786	96.890
Airplane	79.372	82.807	98.839	99.340
Cameraman	69.828	88.533	98.458	99.470

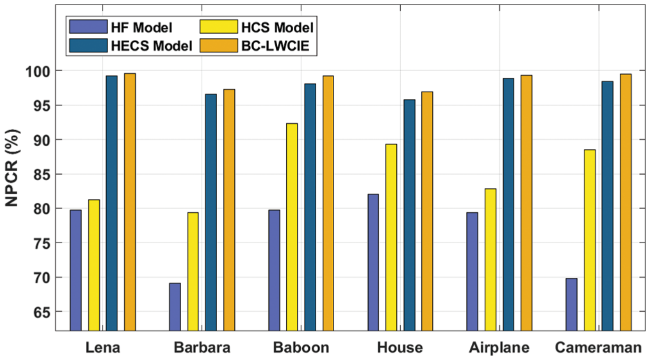


Figure 6: NPCR analysis of BC-LWCIE model with distinct images

At the same time, with Baboon image, the BC-LWCIE technique has resulted in a minimum ET of 0.18s whereas the HCS and HECS approaches have gained a maximum ET of 0.29s and 0.22s. Simultaneously, with Airplane image, the BC-LWCIE system has resulted in a minimal ET of 0.18s whereas the HCS and HECS techniques have obtained an increased ET of 0.39s and 0.21s.

Table 4: Security level analysis of BC-LWCIE model with different images

	Security level (%)			
Images	HF model	HCS model	HECS model	BC-LWCIE
Lena	80.75	85.55	93.14	96.74
Barbara	81.95	83.95	87.94	92.35
Baboon	71.16	80.35	85.15	89.52
House	78.35	81.95	89.94	96.79
Airplane	90.74	92.74	95.94	97.81
Cameraman	85.95	91.94	94.34	96.58

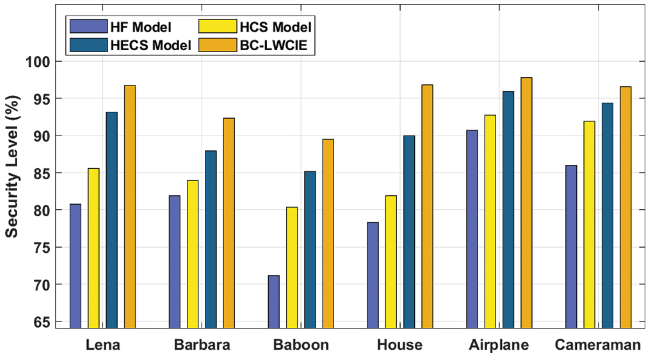


Figure 7: Security level analysis of BC-LWCIE model

Table 5: Comparative analysis of BC-LWCIE model with existing techniques

Images	Encryption time (s)			Decryption time (s)		
	HCS model	HECS model	BC-LWCIE	HCS model	HECS model	BC-LWCIE
Lena	0.21	0.19	0.17	0.19	0.22	0.17
Barbara	0.33	0.29	0.25	0.24	0.3	0.21
Baboon	0.29	0.22	0.18	0.17	0.36	0.14
House	0.48	0.38	0.35	0.33	0.44	0.29
Airplane	0.39	0.21	0.18	0.32	0.41	0.28
Cameraman	0.44	0.27	0.24	0.42	0.52	0.37

Fig. 9 examines the performance of the BC-LWCIE technique interms of DT. The outcomes demonstrated that the BC-LWCIE approach has accomplished effectual outcomes with the reduced DT. For instance, with Lena image, the BC-LWCIE technique has resulted in the least DT of 0.17s whereas the HCS and HECS techniques have attained a maximum DT of 0.19s and 0.22s. Then, with Baboon image, the BC-LWCIE technique has resulted in a lower DT of 0.14s whereas the HCS and HECS techniques have reached a superior DT of 0.17s and 0.36s. Eventually, with Airplane image, the BC-LWCIE technique has resulted in a least DT of 0.28s whereas the HCS and HECS methods have reached a higher DT of 0.32s and 0.41s.

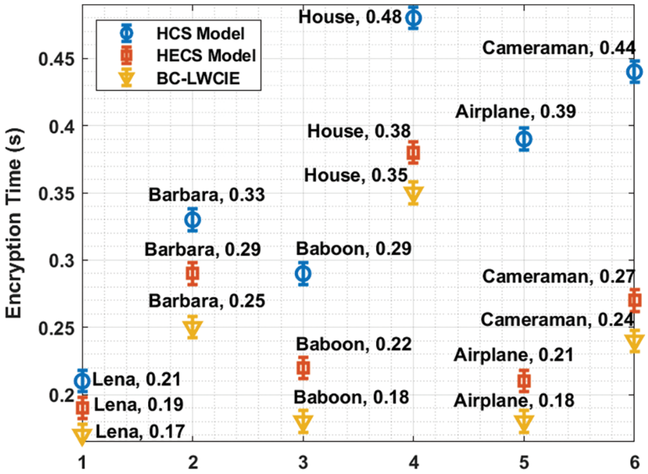


Figure 8: ET analysis of BC-LWCIE model with different images

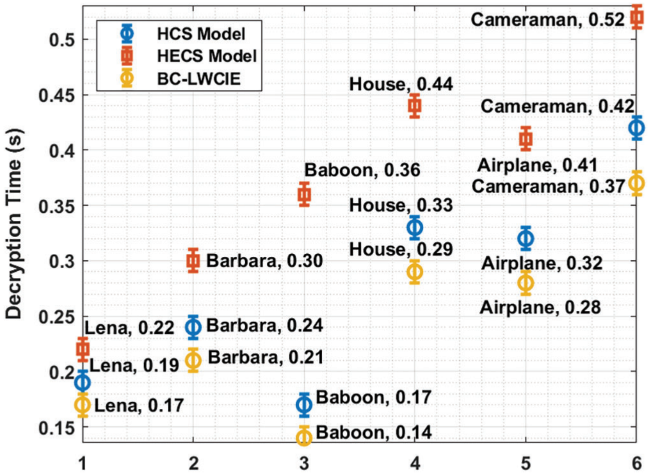


Figure 9: DT analysis of BC-LWCIE model with different images

5 Conclusion

This paper has presented an effective BC-LWCIE technique for secure image transmission in the industry 4.0 environment. The presented BC-LWCIE technique has derived an optimal LWC based hash function with CSO based key generation process. Besides, a fitness function involving the maximization of PSNR is derived by the CSO algorithm. Furthermore, the BC-LWCIE technique stores the cryptographic pixel values of the encrypted image in the BCT to guarantee secrecy in the IIoT environment. For examining the improved secrecy of the BC-LWCIE technique, a comprehensive experimental analysis takes place using benchmark images. The experimental results highlighted the superior performance of the BC-LWCIE technique over the recent techniques. In future, the security performance of the BC-LWCIE technique can be improved by the use of attribute based encryption and digital signature approaches.

Funding Statement: This research was supported by a grant of the Korea Health Technology R&D Project through the Korea Health Industry Development Institute (KHIDI), funded by the Ministry of Health & Welfare, Republic of Korea (grant number: HI21C1831) and the Soonchunhyang University Research Fund.

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

References

[1] T. Alladi, V. Chamola, R. M. Parizi and K. R. Choo, “Blockchain applications for industry 4.0 and industrial iot: A review,” *IEEE Access*, vol. 7, pp. 176935–176951, 2019.

[2] F. Shrouf, J. Ordieres and G. Miragliotta, “Smart factories in Industry 4.0: A review of the concept and of energy management approached in production based on the Internet of Things paradigm,” in *2014 IEEE Int. Conf. on Industrial Engineering and Engineering Management*, Selangor, Malaysia, pp. 697–701, 2014.

[3] M. Weyrich and C. Ebert, “Reference architectures for the Internet of Things,” *IEEE Software*, vol. 33, no. 1, pp. 112–116, 2015.

[4] 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.

[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] D. Miller, “Blockchain and the Internet of Things in the industrial sector,” *IT Professional*, vol. 20, no. 3, pp. 15–18, 2018.

[8] K. Abbas, L. A. Tawalbeh, A. Rafiq, A. Muthanna, I. A. Elgendy *et al.,* “Convergence of blockchain and iot for secure transportation systems in smart cities,” *Security and Communication Networks*, vol. 2021, pp. 1–13, 2021.

[9] S. Gao, Q. Su, R. Zhang, J. Zhu, Z. Sui *et al.,* “A Privacy-preserving identity authentication scheme based on the blockchain,” *Security and Communication Networks*, vol. 2021, no. 8, pp. 1–10, 2021.

[10] W. Hu and H. Li, “A blockchain-based secure transaction model for distributed energy in Industrial Internet of Things,” *Alexandria Engineering Journal*, vol. 60, no. 1, pp. 491–500, 2021.

[11] M. Shen, X. Tang, L. Zhu, X. Du and M. Guizani, “Privacy-preserving support vector machine training over blockchain-based encrypted iot data in smart cities,” *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7702–7712, 2019.

[12] A. A. A. E. Latif, B. A. E. Atty, I. Mehmood, K. Muhammad, S. E. V. Andraca *et al.,* “Quantum-inspired blockchain-based cybersecurity: Securing smart edge utilities in iot-based smart cities,” *Information Processing & Management*, vol. 58, no. 4, pp. 102549, 2021.

[13] Y. Li, Y. Tu, J. Lu and Y. Wang, “A security transmission and storage solution about sensing image for blockchain in the internet of things,” *Sensors*, vol. 20, no. 3, pp. 916, 2020.

[14] S. Banerjee, B. Bera, A. K. Das, S. Chattopadhyay, M. K. Khan *et al.,* “Private blockchain-envisioned multi-authority CP-ABE-based user access control scheme in IIoT,” *Computer Communications*, vol. 169, no. 6, pp. 99–113, 2021.

[15] D. Li, W. Peng, W. Deng and F. Gai, “A blockchain-based authentication and security mechanism for IoT,” in *2018 27th Int. Conf. on Computer Communication and Networks (ICCCN)*, Hangzhou, China, pp. 1–6, 2018.

[16] E. K. Wang, Z. Liang, C. M. Chen, S. Kumari and M. K. Khan, “PoRX: A reputation incentive scheme for blockchain consensus of IIoT,” *Future Generation Computer Systems*, vol. 102, no. 99, pp. 140–151, 2020.

[17] U. Khalid, M. Asim, T. Baker, P. C. K. Hung, M. A. Tariq *et al.,* “A decentralized lightweight blockchain-based authentication mechanism for IoT systems,” *Cluster Computing*, vol. 23, no. 3, pp. 2067–2087, 2020.

[18] P. Velmurugadass, S. Dhanasekaran, S. S. Anand and V. Vasudevan, “Enhancing blockchain security in cloud computing with iot environment using ecies and cryptography hash algorithm,” *Materials Today: Proceedings*, vol. 37, pp. 2653–2659, 2021.

[19] K. Shankar and M. Elhoseny, “An optimal lightweight cryptographic hash function for secure image transmission in wireless sensor networks,” in *Secure Image Transmission in Wireless Sensor Network (WSN) Applications*. Cham: Springer, pp. 49–64, 2019.

[20] X. B. Meng, Y. Liu, X. Gao and H. Zhang, “A new bio-inspired algorithm: Chicken swarm optimization,” in *Proc. of Int. Conf. in Swarm Intelligence*, Cham, Switzerland, Springer, pp. 86–94, 2014.

[21] J. Wang, Z. Cheng, O. K. Ersoy, M. Zhang, K. Sun *et al.,* “Improvement and application of chicken swarm optimization for constrained optimization,” *IEEE Access*, vol. 7, pp. 58053–58072, 2019.

[22] M. T. Yang, B. X. Zhou, S. Dong, N. Lin, Z. G. Li *et al.,* “Microgrid power market design and dispatch optimization supported by blockchain,” *Electric Power Automation Equipment*, vol. 39, no. 12, pp. 155–161, 2019.