Blockchain Enabled Emperor Penguin Optimizer Based Encryption Technique for Secure Image Management System

Padmavathi U
National Institute of Technology Puducherry
Narendran Rajagopalan (narendran@nitpy.ac.in)
National Institute of Technology Puducherry

Research Article

Keywords: Blockchain, Security, Image transmission, Share creation, Encryption, Optimal key generation

Posted Date: May 28th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-539648/v1

Blockchain Enabled Emperor Penguin Optimizer based Encryption Technique for Secure Image Management System

U. Padmavathi[1], Narendran Rajagopalan[2*]
[1,2] Department of Computer Science & Engineering, National Institute of Technology Puducherry, Karaikal, Puducherry, India.
[1]udayarajepadma@gmail.com, [2]narendran@nitpy.ac.in

Abstract

In recent years, the electronic sharing of digital images faces a major threat to security, as the existing image transmission infrastructure is mainly based on the trust of third parties. At the same time, the available solutions are placed on the cloud based centralized data center, which is expensive, requires large storage area, and security issues regarding the transmission of data over the network. So, it is needed to develop an image management system which enables sharing and storing of digital images effectively. This paper develops novel multiple share creation schemes with block technology for secure image management (MSCCBT-SIM) systems. The MSCCBT-SIM model allows the user to create consensus with no dependencies on central authorities. It involves an MSC which involves share creation and share encryption using emperor penguin optimizer based ElGamal public key cryptosystem (EPO-EPKC). In addition, the blockchain is used as a distributed data storage mechanism to generate a ledger for permitting access to the user and prevent third party access to the encrypted shares. The application of blockchain technology and MSC techniques helps to achieve decentralization, highly reliable, inexpensive, and secure transmission and storage of digital images. In order to validate the effective performance of the MSCCBT-SIM model, a series of simulations take place and investigated the results interms of different measures. The experimental results ensured the better performance of the MSCCBT-SIM model over the state of art methods.

Keywords: Blockchain, Security, Image transmission, Share creation, Encryption, Optimal key generation

1. Introduction

Currently, the amount of data being transmitted over unprotected public networks become considerably increased. The utilization of insecure transmission networks like social media is highly at risk of misusing the data by third-parties. Thus, it is significant to preserve the privacy of information, involving images that are transmitted by insecure networks. There are 2 major challenges based on the sharing of images via open networks. Initially, the size of image data is increasing due to the requirement of higher image quality. It takes a long time to transfer the

image data [1, 2]. This challenge could be conquered by employing compression technique before transmitting the data [3]. Another challenge is the weaker safety of image data since it utilizes an open network for distributing the image data. This issue could be addressed via encrypting the data by an encryption technique. The present solutions for image encryption are not effective in real time when the peers are decentralized. The blockchain offers a whole solution for decentralized devices, and the encryption method is highly protected for crucial applications. Fig. 1 depicts the structure of blockchain.

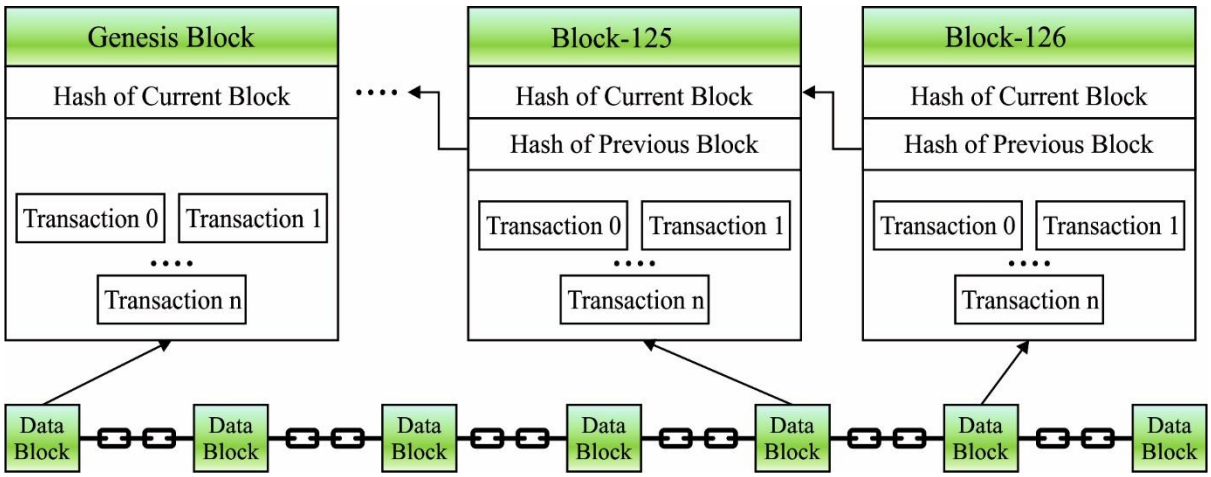


Fig. 1. Structure of Blockchain

Initially, blockchain was established for monetary purposes. At present, it is developing from cryptocurrency and has greater influence over several industries. Its main objective is to remove third-party from money transactions by making a reliable digital currency [4]. A blockchain is a digital ledger, which has a whole history of transactions created on the network. It is a collection of connected blocks that are interconnected by hash values which have been generated over a period of time. Each data on blockchain is constant and could not be altered. A hash recognizes the block and every content, and same as human fingerprint, which is often exclusive. After a block is generated, its hash can be estimated. The alterations within the block can cause the hash to modify. All the blocks comprises the hash of prior block and it efficiently makes a blockchain.

A blockchain is a peer-to-peer network, thus it doesn't have central authorization [5, 6]. All nodes of blockchain obtain an entire copy of the full chain, thus nodes utilize that copy to authenticate that the whole thing is in sequence. Each block is time-stamped, hence it is nearly impracticable to damage the information. If a novel block is generated, it is transmitted to the entire nodes of the chain. Each node authenticates that this block hasn't been damaged and

makes a consensus. There is no central authorization in a blockchain, hence it is a decentralized framework [7]. There are 2 kinds of blockchain namely public, for example, Ethereum and Bitcoin, and next is private that is created particularly for various managements.

Because of the benefits of blockchain technique, maximum reliability, minimum cost, and decentralization, the data stored solution and blockchain are greater compared to conventional data broadcast and centralized stored solution regarding performance, security, and assets usage. As aforementioned, a storage solution and security transmission are presented to sense images for blockchain. This solution is an efficiently withstand the theft and forgery attacks of an image data by adversaries and guarantee that the communication and stored of client data are highly protected. In spite of the overall acceptance that blockchain technique assist rapid and easier auditable interaction and enables the interchange of immutable data between supply chain partner, it takes time for the technique to be employed and revolutionized the supply chain. Presently, several applications of the blockchain is conceptual exposition, and empirical evidence on the implementation of it is restricted. Moreover, several works have been performed on the issues of designing the blockchain in the supply chain, like organization willingness, technical proficiency, scalability, and compatibility with existing systems.

This paper develops novel multiple share creation schemes with block technology for secure image management (MSCCBT-SIM) systems. The MSCCBT-SIM model permits the user to generate consensus with no dependences on central authorities. The MSC scheme involves share creation and shares encryption processes to achieve security. For encrypting shares, emperor penguin optimizer based ElGamal public key cryptosystem (EPO-EPKC) is applied. Moreover, the blockchain is utilized as a distributed data storage mechanism to generate a ledger for permitting access to the user and prevent third-party access to the encrypted shares. The efficiency of the MSCCBT-SIM model is experimented on a different set of benchmark images and examined the results interms of different measures. In short, the paper contribution can be summarized as follows.

- Employ an efficient multiple share creation scheme with block technology for secure image management (MSCCBT-SIM) system.
- Enables the user to generate consensus with no dependences on central authorities.
- Involves share creation and EPO-EPKC based share encryption processes to achieve security.

- Utilizes blockchain as a distributed data storage mechanism to prevent third-party access to the encrypted shares.
- Validate the performance of the MSCCBT-SIM model on benchmark images and examined the results interms of different measures.

The organization of the paper is given as follows. Section 2 discusses the previous works related to the study. Section 3 elaborates the proposed model and section 4 validates the performance of the proposed model. At last, section 5 concludes the study.

2. Literature Review

Jabarulla and Lee [8] proposed a new concept implemented for distributed patient centric image management (PCIM) method which is intended to guarantee security and controlling of person secrecy information without utilizing a focused platform. In this method, it utilized a developing Ethereum blockchain and distributed file system technique named InterPlanetary File System (IPFS). Later, it designed an Ethereum smart contract named the person centric accessing control protocol for allowing the distribute and reliable accessing control strategy.

Alqaralleh et al. [9] implement deep learning (DL) with blockchain supported secured image broadcast and diagnoses method for the IoMT platform. The introduced method consists of several tasks such as data classification, data collection, hash value encryption, and secure transaction. Koptyra and Ogiela [10] presented an image chain a novel technique for connecting images. Unlike other results, the images aren't kept in a blockchain. Rather, they establish the chain by itself. It is understood by storing the information straightaway in graphical files. Thus, the ledger isn't a divided object instead embedded in the image.

The blockchain model is utilized in several areas like industry, medical fields, and smart grid. Gai et al. [11] introduced Privacy enabled Blockchain enabled Transaction (PBT) method to resolve security challenges of energy transaction clients in the smart network. Liang et al. [12] projected a blockchain based secured data broadcast model depending upon an enhanced FaBric framework that is employed to an Industrial IoT for resolving the privacy issues in a blockchain based power grid. Shen et al. [13] presented a blockchain based medicinal encrypted image retrieval method for protecting client image secrecy in the medicinal IoT platform. Initially, this result transfers the image to the hospital's management system via IoT devices. The hospital servers extract distinct kinds of medicinal image features and utilize the image features that exists encryption and kept by Secure Multi-party Computation (SMC) [14].

Li et al. [15] developed the security system for protection and stored of IoT data depending upon blockchain. The result utilizes edge computing to execute data estimation for IoT device and transmits the data to the memory. Additionally, the result utilizes unauthorized encryption technique for establishing an appropriate individuality verification method to blockchain based IoT applications.

Gai et al. [16] integrated the blockchain and edge computing technique and projected a permission blockchain edge model (PBEM-SGN) method which is appropriate for smart networks to resolve 2 significant challenges in smart networks, such as energy security and privacy protection. Guo et al. [17] developed the distributed trusted authentication method depending upon blockchain and edge computing. The method comprises blockchain edge, blockchain network, and physical network layers. Pan et al. [18] implemented and modeled an edge IoT architecture depending upon smart contracts and blockchain. Kim et al. [19] enhanced the Byzantine Fault Tolerance (BFT) consensus technique for lightweight IoT networks depending upon blockchain and presented a storage compression consensus (SCC) method. Shahid et al. [20] presented a lightweight and scalable blockchain architecture for assets controlled IoT sensor device is called as “sensor chai”. Doku et al. [21] developed a method which integrates the blockchain and IoT and mine the network with restricted node assets. The relative research demonstrates that the system contains powerful scalability and effective utilization of assets.

3. The Proposed MSCCBT-SIM Model

Fig. 2 displays the overall working process of proposed MSCCBT-SIM model. The proposed model aims to generate the shares, encrypts them, and then allows blockchain technology to authorize the set of entities in accessing the encrypted shares. The blockchain comprises a set of blocks where every block holds two major parts of data components namely block header and transaction components.

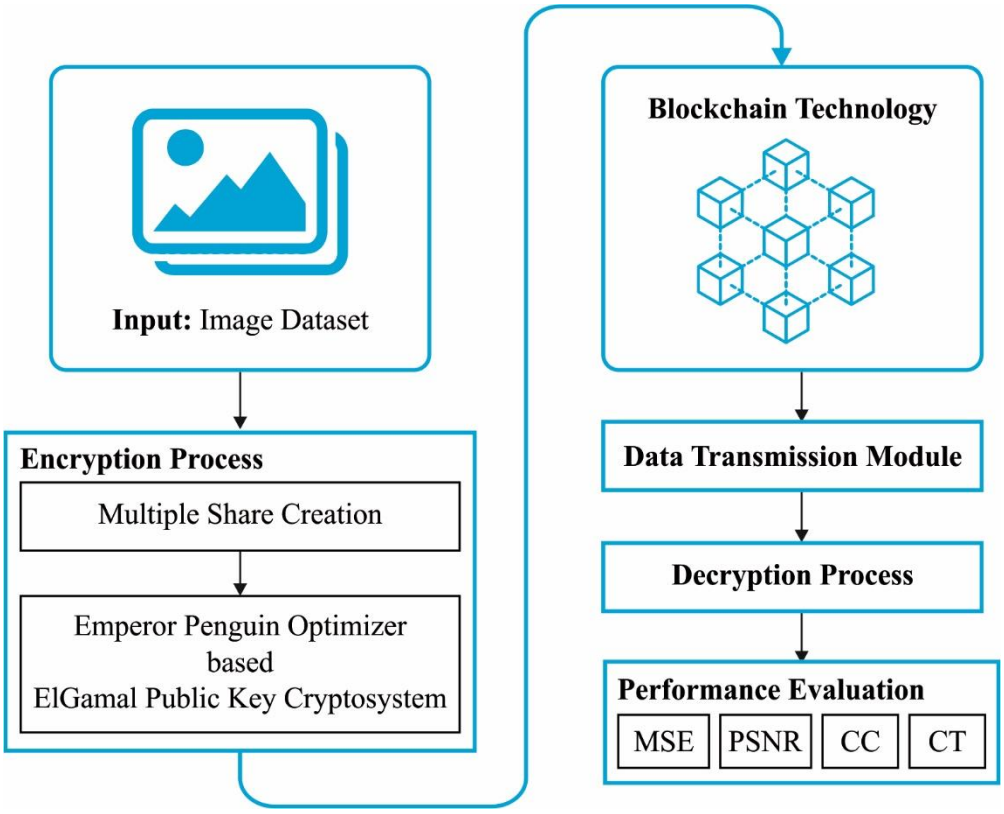


Fig. 2. Working process of MSCCBT-SIM Model

Each block is composed of 2 primary categories of data components. Block header components offer essential metadata needed to create the ordering and integrity of the blockchain. It has the hash of previous block, block identifier, time stamp, and total block size. The next transaction component is a unique data field which distinguishes the blockchain, and its definition completely regulates the type of data that the blockchain structure can stored. The blockchain based image transmission can be defined using the transactions give here. The minimal transaction set obtained for reliable image sharing is defined as follows:

- Define Source: It links the public key to a uniform resource locator (URL).
- Define Study: It generates a source as the creator and a user with a specific unique identifier UID.
- Allow Access: It allows the user to ensure other parties access the encrypted shares from the source endpoint URL.

These 3 kinds of transactions are adequate for the image sharing blockchain for fulfilling the major objective of effective IMS.

3.1. Process involved in MSC Scheme

At this stage, the digital image is fed into the MSC technique and generates a set of multiple shares.

The pixel value of the input image is extracted and RGB would be individually defined as matrix (R_m, G_m, B_m). The matrix size is similar to the input image size (P*Q). The actual pixel value of input image is defined by [22]:

$$Pixel = \sum R + G + B \tag{1}$$

Here, $pixel$ describes the sum of overall values R_m, G_m, and B_m.

Every pixel that appears in the input image could take place in as n transformed manner, called shares. All the shares have a group of subpixels of the RGB image. The R, G, and B shares are based on the pixel values present in the RGB image. The share for RGB is separately denoted as R_s, G_s, and B_s and is defined by.

$$R_s = \int_1^k lim_{k \to 1 ton} R_{ab}$$

$$G_s = \int_1^k lim_{k \to 1 ton} G_{ab}$$

$$B_s = \int_1^k lim_{k \to 1 ton} B_{ab}$$

where a and b denote matrix location, $R_s, G_s \; and \; B_s$ represents shares of RGB, $R_{ab}, G_{ab} \; and \; B_{ab}$ indicates elements of image pixel [23]. Later, the shares are generated dependent on the partition of image as to different parts. The MSC method aims to encrypt the image into many useless share images. The shares don't determine any beneficial data except every share is combined together.

In previous share creation, the basic matrix is essential to be acquired depending upon the number of shares to be made that is predetermined by the client. Moreover, a random key is given regarding the block size of the input image. Commonly, the block size is made to be 4x4/8x8. The number of shares is defined by 2^s, if the $S \geq 2$. In this condition, the amount of basic matrix is two, and the share count is four. The basic matrix is acquired by separating the

RGB values of the pixels by two. The red band shares are generated by XORing the key and basic matrices are given by.

$Rs1 = XR_1 \oplus K_M$

$Rs2 = XR_2 \oplus XR_1$

$Rs3 = XR_2 \oplus Rs1$

$Rs4 = Rs1 \oplus R$

The aforementioned procedure becomes repetitive for other blue and green bands to generate several shares.

Share Reconstruction:

In reconstruction procedure, several shares are combined to create the original actual image. It is given as:

$R = Rs1 \oplus Rs2 \oplus Rs3 \oplus Rs4 \oplus Rs4 \oplus K_M$

$G = Gs1 \oplus Gs2 \oplus Gs3 \oplus Gs4 \oplus Gs4 \oplus K_M$

$B = Bs1 \oplus Bs2 \oplus Bs3 \oplus Bs4 \oplus Bs4 \oplus K_M$

After the shares are reconstructed, the encrypted and decrypted processes utilizing EPKC method, which is applied to all color bands of the reconstructed share. All color bands of image are separated as to blocks before the encrypted and decrypted procedures [24]. The blocks are divided into 4*4 in size. As aforementioned, several shares are created and encryption method is employed on the share. The blocks are portioned to the size of 4*4. From aforementioned processes, several shares are generated and later the EPKC based encryption method is employed on the share.

3.2. Encryption of Shares using EPO-EPKC algorithm

During the share encryption process, the EPO-EPKC algorithm gets executed and encrypts the multiple shares created for every image. The EPKC technique contains 3 important functions such as key generation, encrypt, and decrypt processes. In general, key generation is considered an important part of cryptosystem as it controls the efficiency of whole system. Some additional enhancements raise the usage of this cryptosystem with optimization techniques. Also, it is an

asymmetric key encryption method that utilizes Diffie-Hellman key exchange model. Mostly, this method contains the private key (a random number) $xi \in Zi_{qi'}$ by their respective public key $yi \equiv (gi')^{xi}$ *mod qi*, where gi' defines the generator for Gi_1 with a prime sequence qi'. Since the new contribution, the purposes for optimizing the respective private key using the new EPO algorithm. Also, the encryption message $mi \in Gi_1$ and the public key yi is defined as the pair $ci_1 \equiv (gi')^{ri} modqi$; $ci_2 \equiv yi^{ri} mi \; mod \; qi$, where ri refers the random number [25]. Besides, the decryption ciphertext $\{ci_1, ci_2\}$ and the private key xi is expressed as $mi \equiv ci_2\left(ci_1^{xi}\right)^{-1}$ *mod qi*.

The EPKC technique is determined utilizing the game method with challengers Ci and an adversary Ai.

- Firstly, *Ai* elects two distinct shares as $mi_0, mi_1 \in Gi_1$ and forwards it to Ci'.
- Afterward, this method calculates as Ci' elects $ai \in \{0,1\}$ and $ri_1, xi \in Zi_{qi'}$ randomly and sets $yi \equiv (gi')^{xi}$ *mod qi*, $ci_1 \equiv (gi')^{ri}$ *mod qi* and $ci_2 \equiv (gi')^{rixi} mi_{ai}$ *mod qi*. Moreover, Ci' gives *Ai* as gi', yi, ci_1 and ci_2.
- Calculate challenge as Ci' examines Ai on ai.
- Calculate guessing as Ai gives ai' and forward it returns to Ci'. Now, Ai become success if $ai' = ai$ else fails.

In the aforementioned game, let Ai recognizes gi', $(gi')^{xi}$, $(gi')^{ri}$ and $(gi')^{xiri} mi_{ai}$ so far, Ai could not get access rights to xi and *ri*‘. Here, the success potentiality of probabilistic polynomial-time adversaries Ai to attained ai exactly is trivial enhanced to arbitrary guesses as provided in Eq. (2).

$$Pi\,[ai' = ai] = \frac{1}{2} + negl \tag{2}$$

In Eq. (2), Pi defines success probabilities and $negl$ represents the trivial enhancement. At last, the encrypted share with a better private key is achieved. At this stage, the keys in the EPKC algorithm are chosen optimally with the goal of maximizing the PSNR as the fitness function. The EPO algorithm is used for the selection of the keys and the fitness function can be represented using Eq. (3):

$$Fitness = MAX\{PSNR\} \tag{3}$$

This bio-stimulated technique is initially proposed by Dhiman and Kumar [26] for solving optimization problems. The EPO is stimulated from the emperor penguins' (EPs) huddle attitude, as established from the Antarctic. So, the primary objective is to determine an effectual mover in the swarm mathematically. The distances among EPs $\left(X_{ep}\right)$ are calculated succeeding by its temperature profile (θ'). The productive mover is determined and locations of other EPs are altered for achieving an optimal value. The temperature profile of the EPs is estimated as:

$$\theta' = \left(\theta - \frac{Iter_{\max}}{C - lter_{\max}}\right) \tag{4}$$

$$\theta = \begin{cases} 0 & if R > 0.5 \\ 1 & if R < 0.5 \end{cases} \tag{5}$$

The maximal count of iterations, where C refers the present iteration is demonstrated by $Iter\_max$ and R represents the arbitrary number among $[0,1]$. As EPs usually huddle combined for preserving temperatures, careful safeguard need become for protecting in neighborhood collisions. Therefore, it offers 2 vectors $\left(\vec{U}\right)$ and $\left(\vec{V}\right)$ whose values are computed as:

$$\vec{U} = \left\{M \times \left(\theta' + X_{grid}(accuracy)\right) \times Rand\ 0\right\} - \theta \tag{6}$$

$$\vec{V} = Rand(\,) \tag{7}$$

$$X_{grid}(accuracy) = \left|\vec{X} - \vec{X}_{\text{ep}}\right| \tag{8}$$

Where M defines the parameter for actions set as 2, $\vec{x}$ refers the better solution, $\vec{x}_{ep}$ denotes the positions of other EPs, [0,1] and || signifies the absolute value for *Rand*.

$$\vec{D} = \left|\left\{S\left(\vec{U}\right) \cdot \vec{X}(x) - \vec{V} \cdot \vec{X}_{ep}(x)\right\}\right| \tag{9}$$

$$S\left(\vec{U}\right) = \sqrt{(fe^{-C/v} - e^{-\mathrm{C}})^2} \tag{10}$$

Eqs. (9) and (10) are created for estimating the distance amongst EP and optimal fittest search agent $\left(\vec{D}\right)$. $S()$ depicts the human forces to that the better search agents are led by Eps, e signifying the exponential operation [27]. The control parameters f and v are individuals where the optimal value of f and v is within the [2, 3] and [1.5, 2] range correspondingly. Now, based on better agent attained utilizing Eq. (11), the locations of EPs are upgraded.

$$\vec{X}_{ep}(x+1) = \vec{X}(x) - \vec{U} \cdot \vec{D}_{ep} \tag{11}$$

It is noticeable the parameter ranges selective are corresponding to individuals of the original literature. So, the EPO technique is utilized for achieving better global value with fit concern to operators. Fig. 3 demonstrates the flowchart of EPO technique.

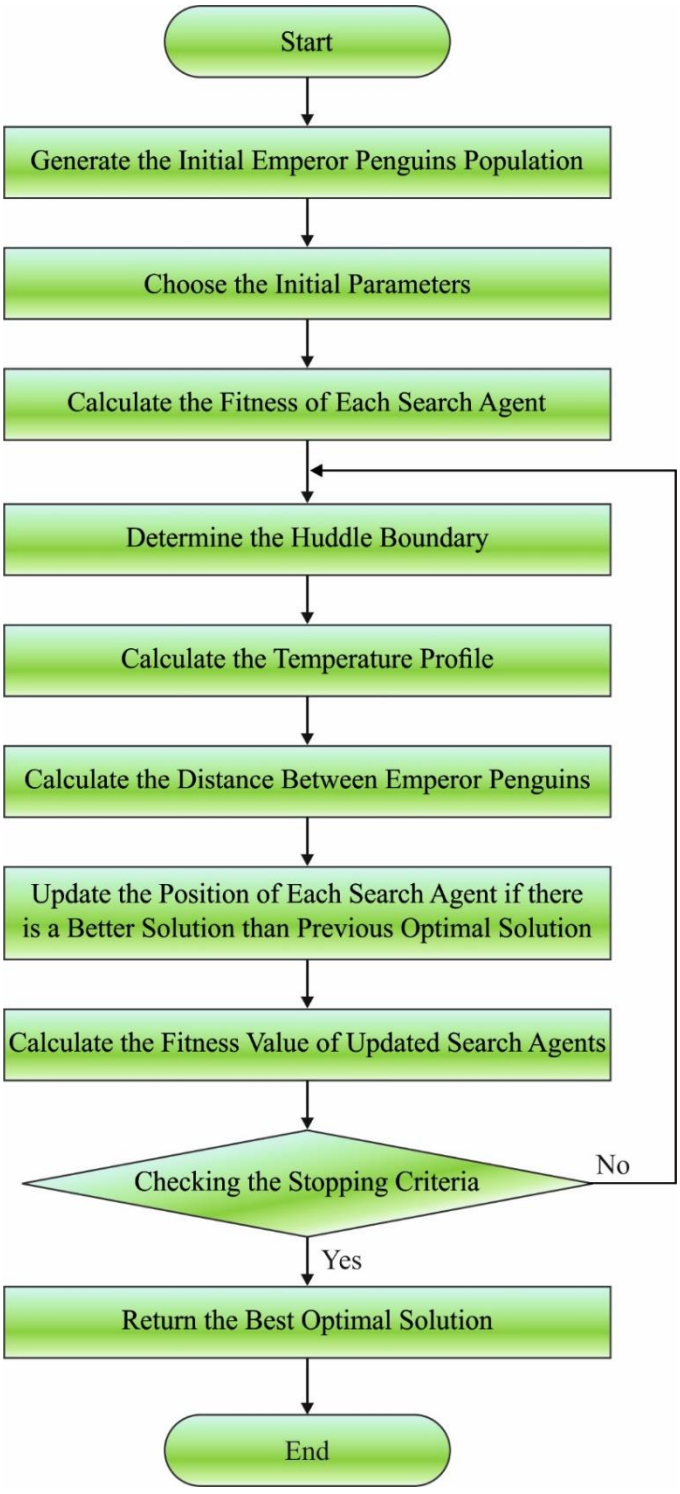


Fig. 3. Flowchart of EPO

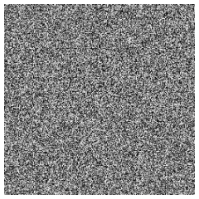
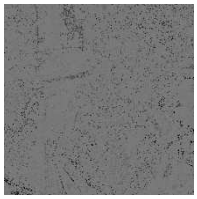
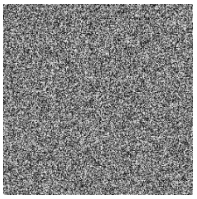
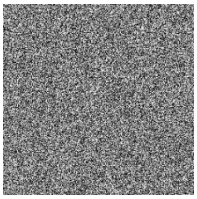
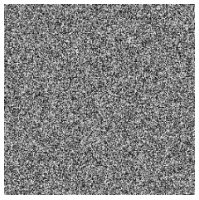
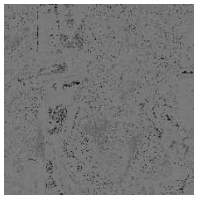
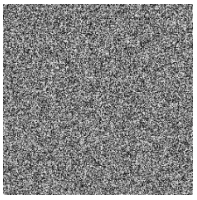
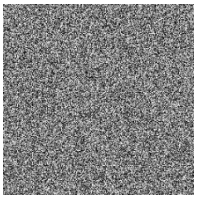
4. Performance Validation

This section validates the performance of the presented method and examines its importance under different aspects. The proposed model is tested using a set of benchmark RGB images. Fig. 4 illustrates the sample images.

Fig. 4. Sample Images

Table 1 illustrates the visualization of multiple shares generated for every band that exists in the applied input image. The shares in row 1 denote the generated shares for 'R' color band, shares in row 2 represent the created shares for 'G' color band, and shares in row 3 signifies the produced shares for 'B' color band. The generated shares are seemed to be meaningless unless all the shares are integrated together.

Table 1 Results of Share Creation Method

Original Image	Share-1	Share-2	Share-3	Share-4
				
				

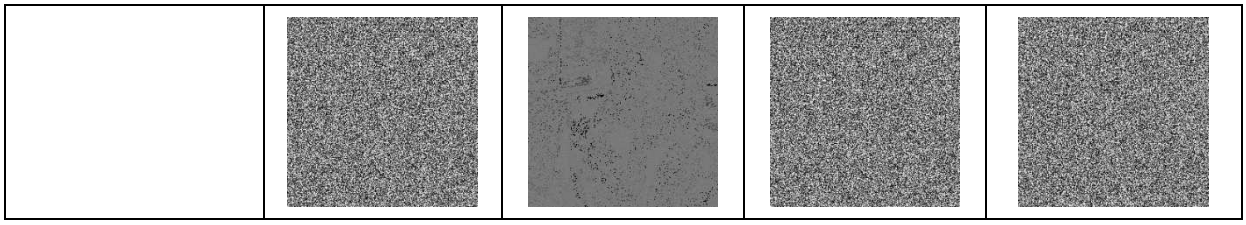
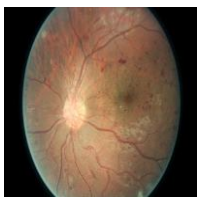
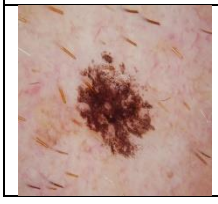
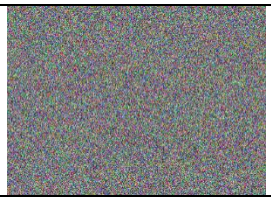


Table 2 investigates the results obtained by the MSCCBT-SIM model for the applied input test images interms of MSE, PSNR, and CC. From the table, it is evident that the MSCCBT-SIM model demonstrated an effective outcome by offering maximum PSNR and CC with minimal MSE values. For instance, on tested input image-1, the MSCCBT-SIM method has obtained an MSE of 0.086, PSNR of 58.786dB, and CC of 0.997. Besides, on tested input image 2, the MSCCBT-SIM technique has reached an MSE of 0.074, PSNR of 59.438dB, and CC of 0.999.

Table 2 Result Analysis of Proposed Method MSCCBT-SIM

Input Image	**Encrypted Image**	**MSE**	**PSNR**	**CC**
		0.086	58.786	0.997
		0.074	59.438	0.999
		0.098	58.219	0.998
		0.064	60.069	0.999
		0.070	59.680	0.999

Next, on tested input image-3, the MSCCBT-SIM model has obtained an MSE of 0.098, PSNR of 58.219dB, and CC of 0.998. Then, on tested input image-4, the MSCCBT-SIM method has attained an MSE of 0.064, PSNR of 60.069dB, and CC of 0.999. Lastly, on tested input image 5, the MSCCBT-SIM methodology has obtained an MSE of 0.070, PSNR of 59.680dB, and CC of 0.999.

Table 3 examines the performance of the MSCCBT-SIM model with other existing methods interms of MSE and PSNR. Fig. 5 illustrates the MSE analysis of the MSCCBT-SIM model with other methods. The figure demonstrated that the MSCCBT-SIM model has obtained improved outcomes with minimal MSE over the other methods. For instance, the MSCCBT-SIM model has required a lower MSE of 0.086 whereas the other methods such as HOCE-ECC, GO-ECC, PSO-ECC, and CS-ECC required an MSE of 0.125, 0.141, 1.145, and 1.278 respectively. Moreover, the MSCCBT-SIM approach has required a lower MSE of 0.098 whereas the other methods such as HOCE-ECC, GO-ECC, PSO-ECC, and CS-ECC required an MSE of 0.119, 0.134, 1.189, and 2.245 respectively. Furthermore, the MSCCBT-SIM model has required a lower MSE of 0.070 whereas the other methods such as HOCE-ECC, GO-ECC, PSO-ECC, and CS-ECC required an MSE of 0.136, 0.138, 1.246, and 2.780 correspondingly.

Table 3 Result Analysis of Proposed MSCCBT-SIM Method with Existing Methods with respect to MSE and PSNR

Test Images	MSCCBT-SIM		HOCE-ECC		GO-ECC		PSO-ECC		CS-ECC	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
Image 1	0.086	58.79	0.125	57.16	0.141	56.64	1.145	47.54	1.278	47.07
Image 2	0.074	59.44	0.127	57.09	0.136	56.80	1.379	46.74	1.974	45.18
Image 3	0.098	58.22	0.119	57.38	0.134	56.86	1.189	47.38	2.245	44.62
Image 4	0.064	60.07	0.145	56.52	0.194	55.25	1.653	45.95	1.907	45.33
Image 5	0.070	59.68	0.136	56.80	0.138	56.73	1.246	47.18	2.780	43.69

Fig. 6 depicts the results analysis of the MSCCBT-SIM model with state-of-the-art approaches interms of PSNR. The figure portrayed that the MSCCBT-SIM technique outperforms the other methods by accomplishing maximum PSNR. For instance, on the input image 1, the MSCCBT-

SIM model has gained a superior PSNR of 58.79dB whereas the HOCE-ECC, GO-ECC, PSO-ECC, and CS-ECC methods offered a lower PSNR of 57.16dB, 56.64dB, 47.54dB, and 47.07dB respectively. Along with respect, on the input image 3, the MSCCBT-SIM model has gained a higher PSNR of 58.22dB whereas the HOCE-ECC, GO-ECC, PSO-ECC, and CS-ECC methods offered a lower PSNR of 57.38dB, 56.86dB, 47.38dB, and 44.62dB respectively. Along with that, on the input image 5, the MSCCBT-SIM model has gained a superior PSNR of 59.68dB whereas the HOCE-ECC, GO-ECC, PSO-ECC, and CS-ECC methods offered a lower PSNR of 56.80dB, 56.73dB, 47.18dB, and 43.69dB respectively.

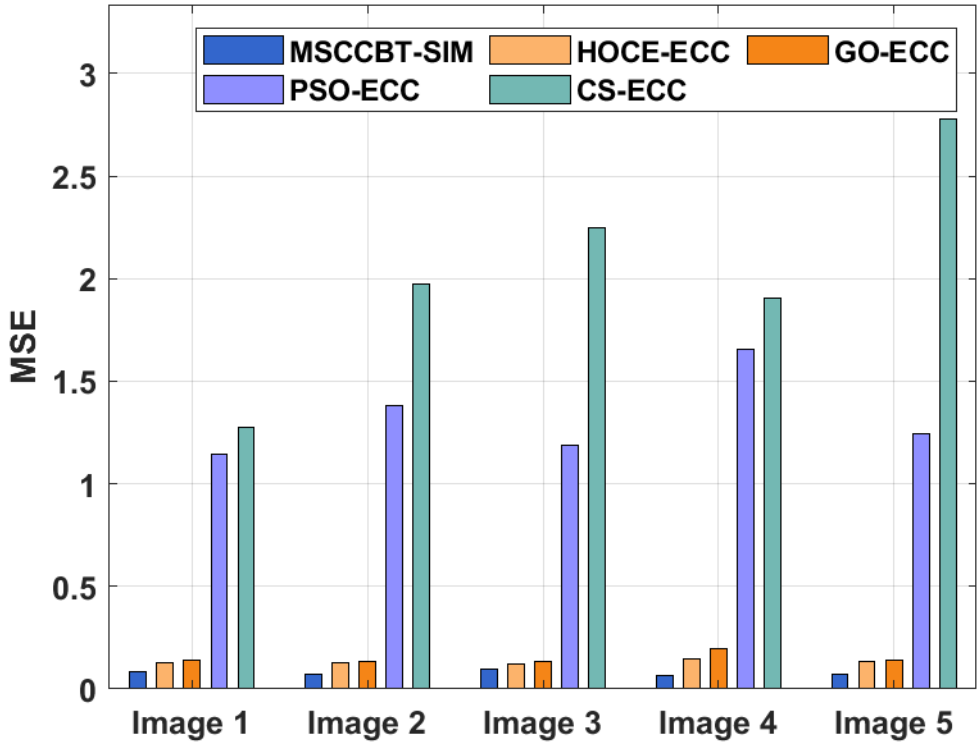


Fig. 5. MSE analysis of MSCCBT-SIM model

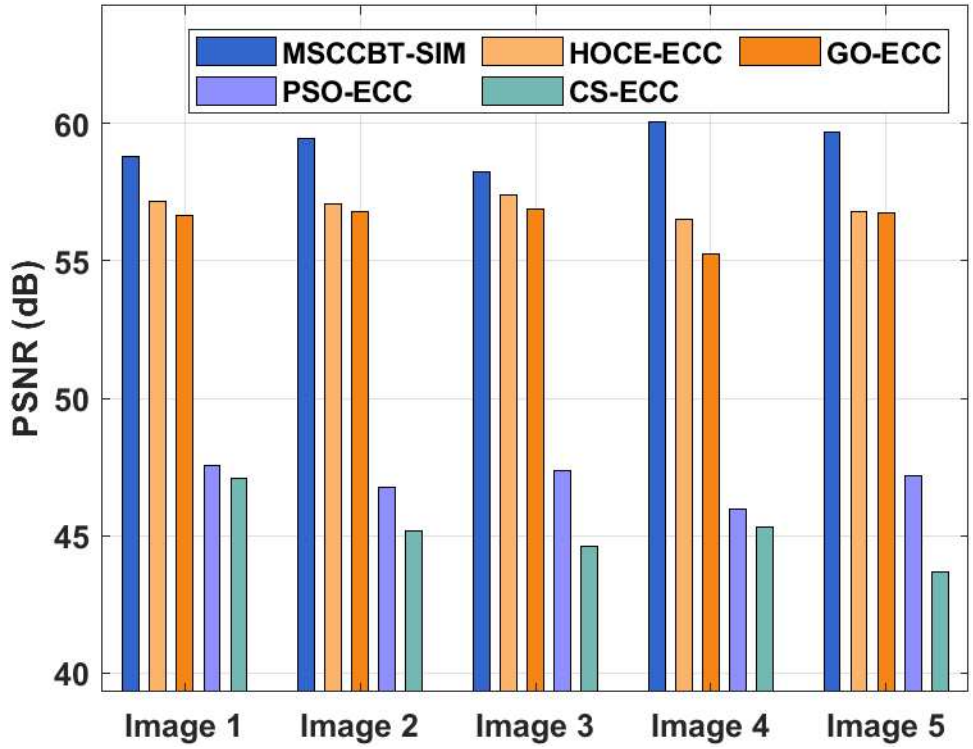


Fig. 6. PSNR analysis of MSCCBT-SIM model

Table 4 Result Analysis of Proposed MSCCBT-SIM Method with Existing Methods in terms of CC

Test Images	**MSCCBT-SIM**	**HOCE-ECC**	**GO-ECC**	**PSO-ECC**	**CS-ECC**
Image 1	0.997	0.995	0.994	0.992	0.990
Image 2	0.999	0.997	0.995	0.994	0.991
Image 3	0.998	0.996	0.994	0.992	0.990
Image 4	0.999	0.997	0.996	0.994	0.993
Image 5	0.999	0.998	0.996	0.993	0.992

Table 4 and Fig. 7 examine the performance of the MSCCBT-SIM model with other existing methods interms of CC. The figure portrayed that the MSCCBT-SIM model outperforms the other methods by accomplishing maximum CC. For instance, on the input image 1, the MSCCBT-SIM model has gained a higher CC of 0.997 whereas the HOCE-ECC, GO-ECC, PSO-ECC, and CS-ECC methods offered a lower CC of 0.995, 0.994, 0.992, and 0.990

correspondingly. Likewise, on the input image 3, the MSCCBT-SIM model has gained a maximum CC of 0.998 whereas the HOCE-ECC, GO-ECC, PSO-ECC, and CS-ECC methods offered a lower CC of 0.996, 0.994, 0.992, and 0.990 respectively. Along with that, on the input image 5, the MSCCBT-SIM model has gained a higher CC of 0.999 whereas the HOCE-ECC, GO-ECC, PSO-ECC, and CS-ECC methods offered a lower CC of 0.998, 0.996, 0.993, and 0.992 respectively.

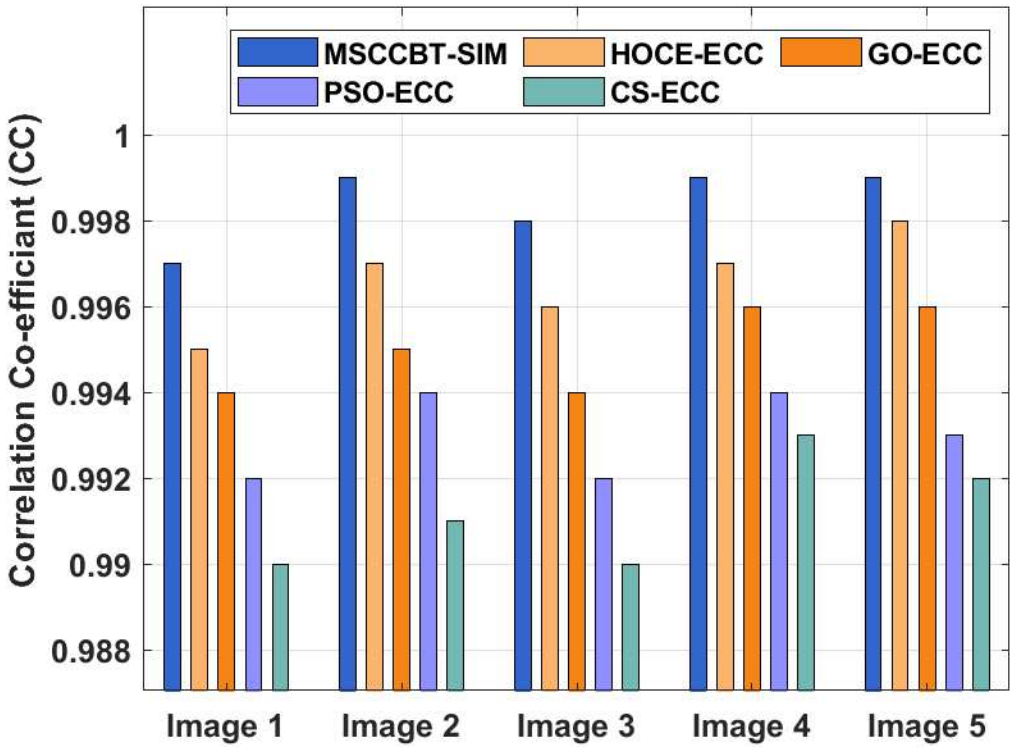


Fig. 7. Result analysis of MSCCBT-SIM model interms of CC

Table 5 validates the results obtained by the MSCCBT-SIM model with existing methods under the existence of salt and pepper attack [28]. Fig. 8 investigates the CT analysis of the MSCCBT-SIM model with other existing techniques on the applied input images. The figure demonstrated that the MSCCBT-SIM model has obtained improved outcomes with minimal CT over the other methods. For instance, the MSCCBT-SIM model has required a lower CT of 0.67minute whereas the other methods such as HOCE-ECC, GO-ECC, PSO-ECC, and CS-ECC required a CT of 0.84, 1.34, 1.45, and 1.67 minutes respectively. Moreover, the MSCCBT-SIM model has required a lower CT of 0.47minute whereas the other methods such as HOCE-ECC, GO-ECC, PSO-ECC, and CS-ECC required a CT of 0.56, 1.89, 1.92, and 2.19 minutes respectively. Furthermore, the MSCCBT-SIM model has required a lower CT of

0.65minute whereas the other methods such as HOCE-ECC, GO-ECC, PSO-ECC, and CS-ECC required a CT of 0.76, 1.63, 2.06, and 2.45 minutes respectively.

Table 5 Result Analysis of Proposed MSCCBT-SIM Method with Existing Methods in terms of Computation Time (Min) and Time of Attack in PSNR (dB)

Computation Time (Min)					
Test Images	**MSCCBT-SIM**	**HOCE-ECC**	**GO-ECC**	**PSO-ECC**	**CS-ECC**
Image 1	0.67	0.84	1.34	1.45	1.67
Image 2	0.54	0.78	1.27	1.83	1.88
Image 3	0.47	0.56	1.89	1.92	2.19
Image 4	0.82	1.03	2.01	2.08	2.31
Image 5	0.65	0.76	1.63	2.06	2.45
Time of Attack in terms of PSNR (dB)					
Test Images	**MSCCBT-SIM**	**HOCE-ECC**	**GO-ECC**	**PSO-ECC**	**CS-ECC**
Image 1	57.35	55.38	54.32	53.29	52.10
Image 2	58.21	54.29	53.07	52.01	51.05
Image 3	56.83	56.13	54.78	53.91	52.00
Image 4	58.61	54.21	53.12	51.08	50.67
Image 5	57.09	53.08	52.91	52.65	50.51

Fig. 9 depicts the results analysis of the MSCCBT-SIM technique with existing approaches interms of PSNR. The figure portrayed that the MSCCBT-SIM model outperforms the other methods by accomplishing maximum PSNR. For instance, on the input image 1, the MSCCBT-SIM model has gained a higher PSNR of 57.35dB whereas the HOCE-ECC, GO-ECC, PSO-ECC, and CS-ECC methods offered a lower PSNR of 55.38dB, 54.32dB, 53.29dB, and 52.10dB correspondingly. Also, on the input image 3, the MSCCBT-SIM method has gained a maximum PSNR of 56.83dB whereas the HOCE-ECC, GO-ECC, PSO-ECC, and CS-ECC

methods offered a lower PSNR of 56.13dB, 54.78dB, 53.91dB, and 52dB respectively. Along with that, on the input image 5, the MSCCBT-SIM model has gained a superior PSNR of 57.09dB whereas the HOCE-ECC, GO-ECC, PSO-ECC, and CS-ECC methods offered a lower PSNR of 53.08dB, 52.91dB, 52.65dB, and 50.51dB respectively.

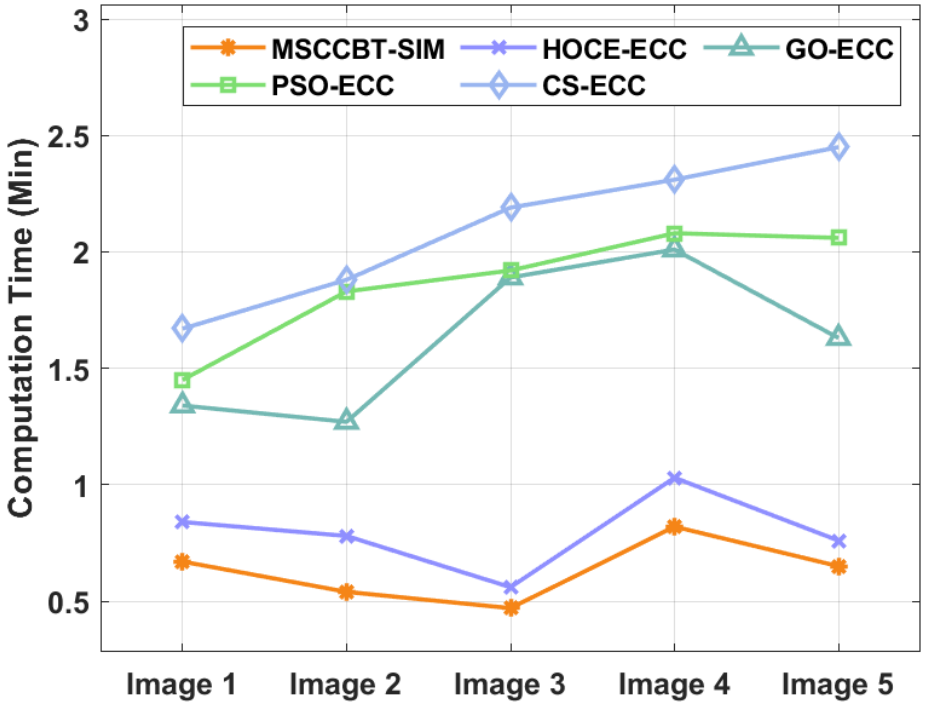


Fig. 8. Computation time analysis of MSCCBT-SIM model

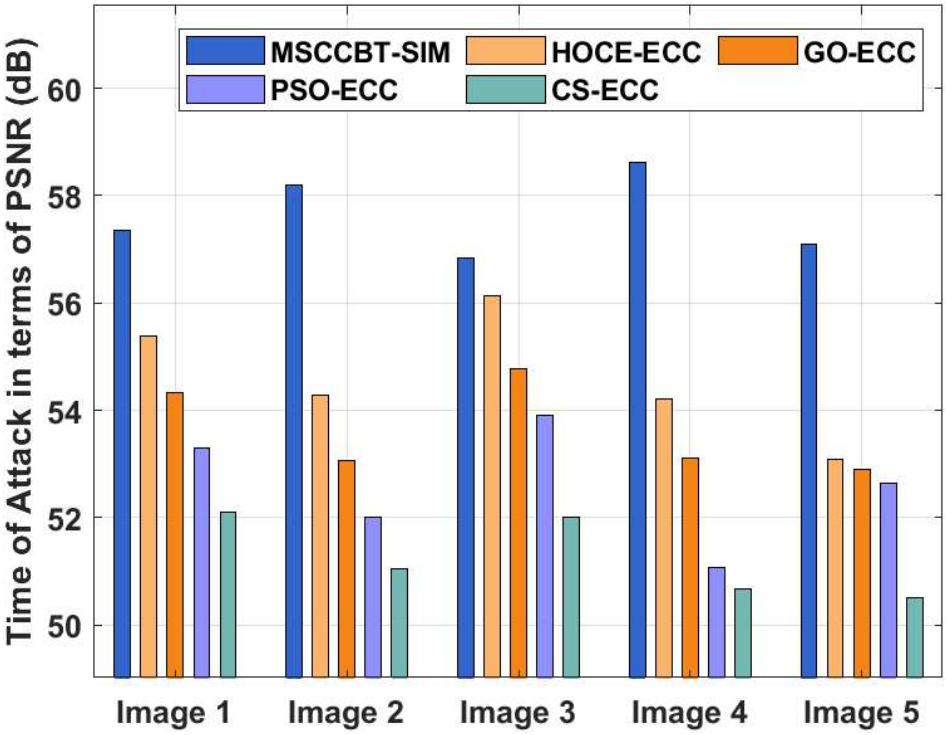


Fig. 9. PSNR analysis of MSCCBT-SIM model with existing techniques

5. Conclusion

This paper has developed a new MSCCBT-SIM model to handle the storage and transmission of images in a secured way. The MSCCBT-SIM model permits the user to generate consensus with no dependences on central authorities. The presented model initially creates multiple shares of images using MSC technique and then encrypts the shares using EPO-EPKC algorithm. Besides, in order to improve efficiency of the EPKC algorithm, the optimal key generation process takes place using EPO algorithm which in turn enhances the visual outcome. The application of blockchain technology and MSC techniques helps to achieve decentralization, highly reliable, inexpensive, and secure transmission and storage of digital images. The efficiency of the MSCCBT-SIM model is experimented on a different set of benchmark images and examined the results interms of different measures. The experimental outcomes make sure the better performance of the MSCCBT-SIM model over the state of art methods. In future, the proposed model can be incorporated into the healthcare sector for secure transmission of images.

Declarations

Funding: No funding is received

Conflicts of interest/Competing interests: The authors have expressed no conflict of interest

Availability of data and material: Not applicable

Code availability: Not applicable

References

[1] Setyaningsih, E., Wardoyo, R. and Sari, A.K., 2020. Securing color image transmission using compression-encryption model with dynamic key generator and efficient symmetric key distribution. *Digital Communications and Networks*.

[2] M. Hamdi, R. Rhouma, S. Belghith, A selective compression-encryption of images based on SPIHT coding and Chirikov Standard Map, Signal Process. 131 (2017) 514–526.

[3] E. Setyaningsih, A. Harjoko, Survey of hybrid image compression techniques, Int. J. Electr. Comput. Eng. 7 (4) (2017) 2206.

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

[5] Lakshmanaprabu, S.K., Mohanty, S.N., Krishnamoorthy, S., Uthayakumar, J. and Shankar, K., 2019. Online clinical decision support system using optimal deep neural networks. Applied Soft Computing, 81, p.105487.

[6] Patel, V., 2019. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health informatics journal*, *25*(4), pp.1398-1411.

[7] Uthayakumar, J., Elhoseny, M. and Shankar, K., 2020. Highly reliable and low-complexity image compression scheme using neighborhood correlation sequence algorithm in WSN. IEEE Transactions on Reliability, *69*(4), pp.1398-1423.

[8] Jabarulla, M.Y. and Lee, H.N., 2021. Blockchain-Based Distributed Patient-Centric Image Management System. Applied Sciences, 11(1), p.196.

[9] Alqaralleh, B.A., Vaiyapuri, T., Parvathy, V.S., Gupta, D., Khanna, A. and Shankar, K., 2021. Blockchain-assisted secure image transmission and diagnosis model on Internet of Medical Things Environment. Personal and Ubiquitous Computing, pp.1-11.

[10] Koptyra, K. and Ogiela, M.R., 2021. Imagechain—Application of Blockchain Technology for Images. Sensors, 21(1), p.82.

[11] Gai, K.; Wu, Y.; Zhu, L.; Qiu, M.; Shen, M. Privacy-Preserving Energy Trading Using Consortium Blockchain in Smart Grid. IEEE Trans. Ind. Inf. 2019, 15, 3548–3558.

[12] Liang, W.; Tang, M.; Long, J.; Peng, X.; Xu, J.; Li, K. A Secure FaBric Blockchain-Based Data Transmission Technique for Industrial Internet-of-Things. IEEE Trans. Ind. Inf. 2019, 15, 3582–3592.

[13] Shen, M.; Deng, Y.; Zhu, L.; Du, X.; Guizani, N. Privacy-Preserving Image Retrieval for Medical IoT Systems: A Blockchain-Based Approach. IEEE Netw. 2019, 33, 27–33.

[14] Li, Y., Tu, Y., Lu, J. and Wang, Y., 2020. A security transmission and storage solution about sensing image for blockchain in the Internet of Things. *Sensors*, *20*(3), p.916.

[15] Li, R.; Song, T.; Mei, B.; Li, H.;Cheng, X.; Sun, L. Blockchain for Large-Scale Internet of Things Data Storage and Protection. IEEE Trans. Serv. Comput. 2019, 12, 762–771.

[16] Gai, K.; Wu, Y.; Zhu, L.; Xu, L.; Zhang, Y. Permissioned Blockchain and Edge Computing Empowered Privacy-Preserving Smart Grid Networks. IEEE Int. Things J. 2019, 6, 7992–8004.

[17] Guo, S.; Hu, X.; Guo, S.; Qiu, X.; Qi., F. Blockchain Meets Edge Computing: A Distributed and Trusted Authentication System. IEEE Trans. Ind. Inf. 2020, 16, 1972–1983.

[18] Pan, J.; Wang, J.; Hester, A.; Alqerm, I.; Liu, Y.; Zhao, Y. EdgeChain: An Edge-IoT Framework and Prototype Based on Blockchain and Smart Contracts. IEEE Int. Things J. 2019, 6, 4719–4732.

[19] Kim, T.; Noh, J.;Cho, S. SCC: Storage Compression Consensus for Blockchain in Lightweight IoT Network. In Proceedings of the 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 11–13 January 2019.

[20] Shahid, A.; Pissinou, N.; Staier, C.; Kwan, R. Sensor-Chain: A Lightweight Scalable Blockchain Framework for Internet of Things. In Proceedings of the 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Atlanta, GA, USA, 14–17 July 2019.

[21] Doku, R.; Rawat, D.; Garuba, M.; Njilla, L. LightChain: on the Lightweight Blockchain for the Internetof-Things. In Proceedings of the 2019 IEEE International Conference on Smart Computing (SMARTCOMP), Washington, DC, USA, 12–15 June 2019.

[22] K. Shankar and P. Eswaran, "RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography," in *China Communications*, vol. 14, no. 2, pp. 118-130, February 2017, doi: 10.1109/CC.2017.7868160.

[23] Shankar, K. and Eswaran, P., 2016. RGB-based secure share creation in visual cryptography using optimal elliptic curve cryptography technique. *Journal of Circuits, Systems and Computers*, *25*(11), p.1650138.

[24] A. F. S. Devaraj *et al*., "An Efficient Framework for Secure Image Archival and Retrieval System Using Multiple Secret Share Creation Scheme," in *IEEE Access*, vol. 8, pp. 144310-144320, 2020, doi: 10.1109/ACCESS.2020.3014346

[25] Kalyani, G. and Chaudhari, S., 2019. Data privacy preservation in MAC aware Internet of things with optimized key generation. *Journal of King Saud University-Computer and Information Sciences*.

[26] Dhiman, G. and Kumar, V., 2018. Emperor penguin optimizer: a bio-inspired algorithm for engineering problems. *Knowledge-Based Systems*, *159*, pp.20-50.

[27] Dhiman, G., Oliva, D., Kaur, A., Singh, K.K., Vimal, S., Sharma, A. and Cengiz, K., 2021. BEPO: a novel binary emperor penguin optimizer for automatic feature selection. *Knowledge-Based Systems*, *211*, p.106560.

[28] Elhoseny, M., Shankar, K., Lakshmanaprabu, S.K., Maseleno, A. and Arunkumar, N., 2018. Hybrid optimization with cryptography encryption for medical image security in Internet of Things. *Neural computing and applications*, pp.1-15.

Figures

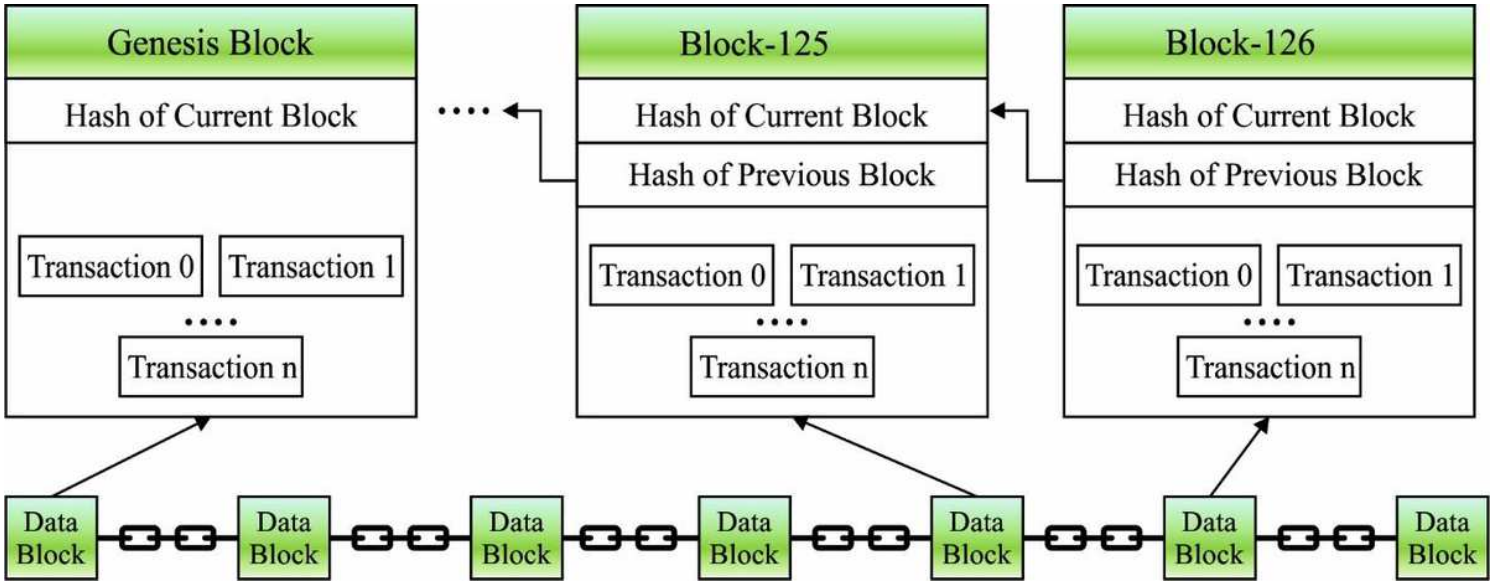


Figure 1

Structure of Blockchain

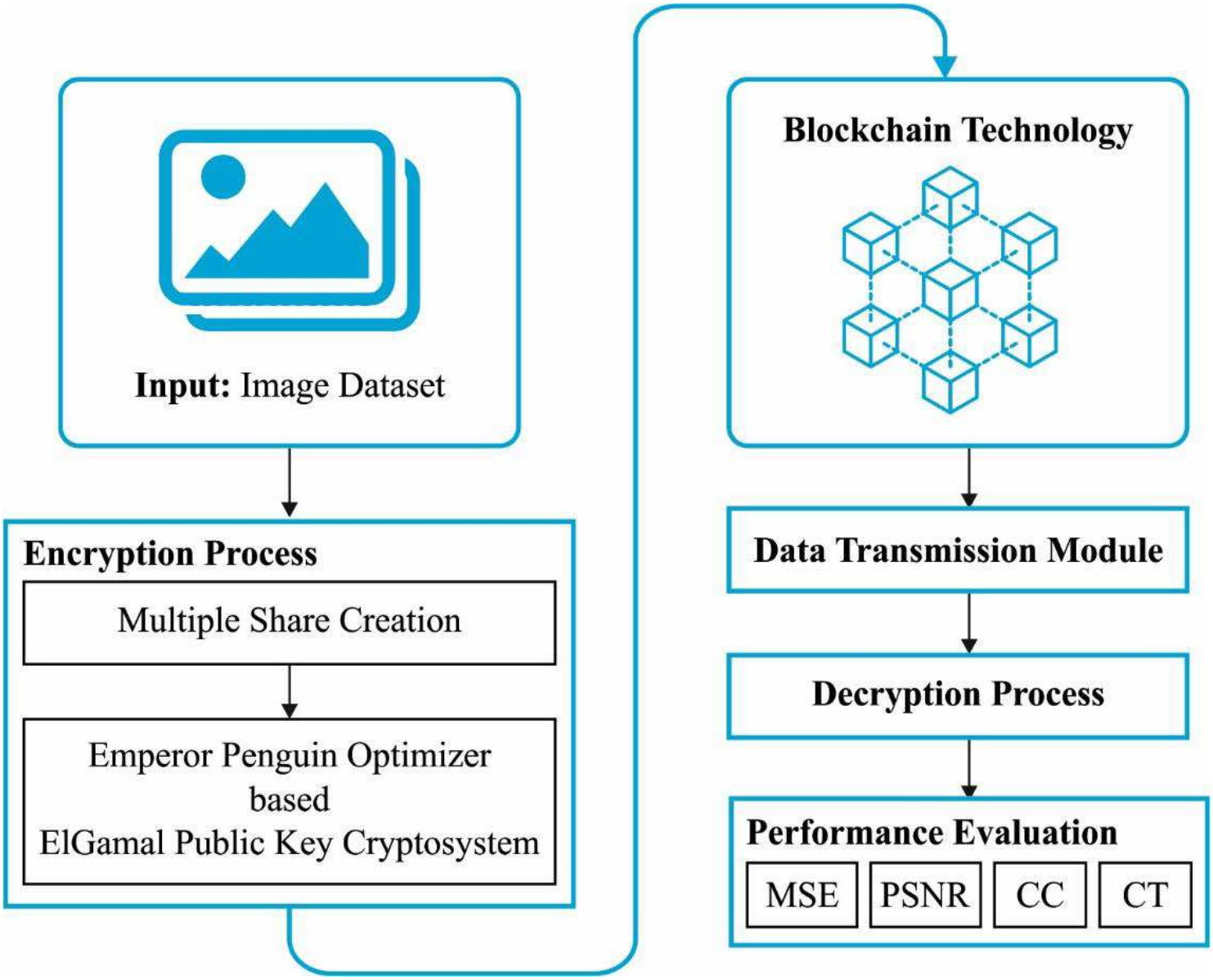


Figure 2

Working process of MSCCBT-SIM Model

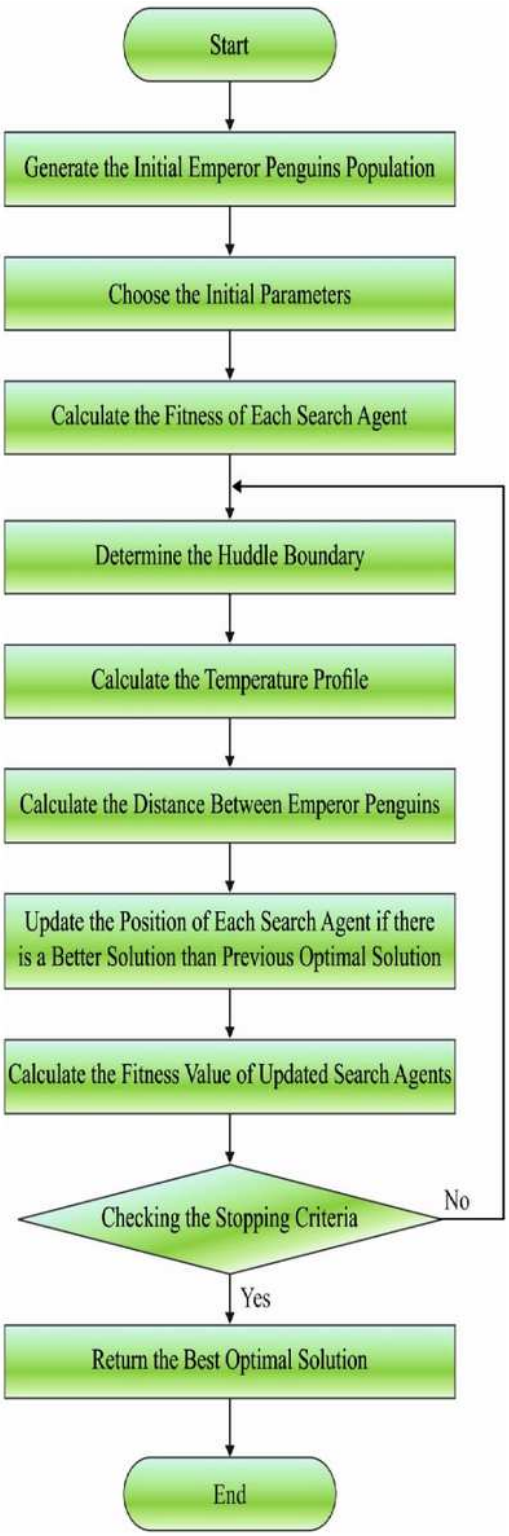


Figure 3

Flowchart of EPO

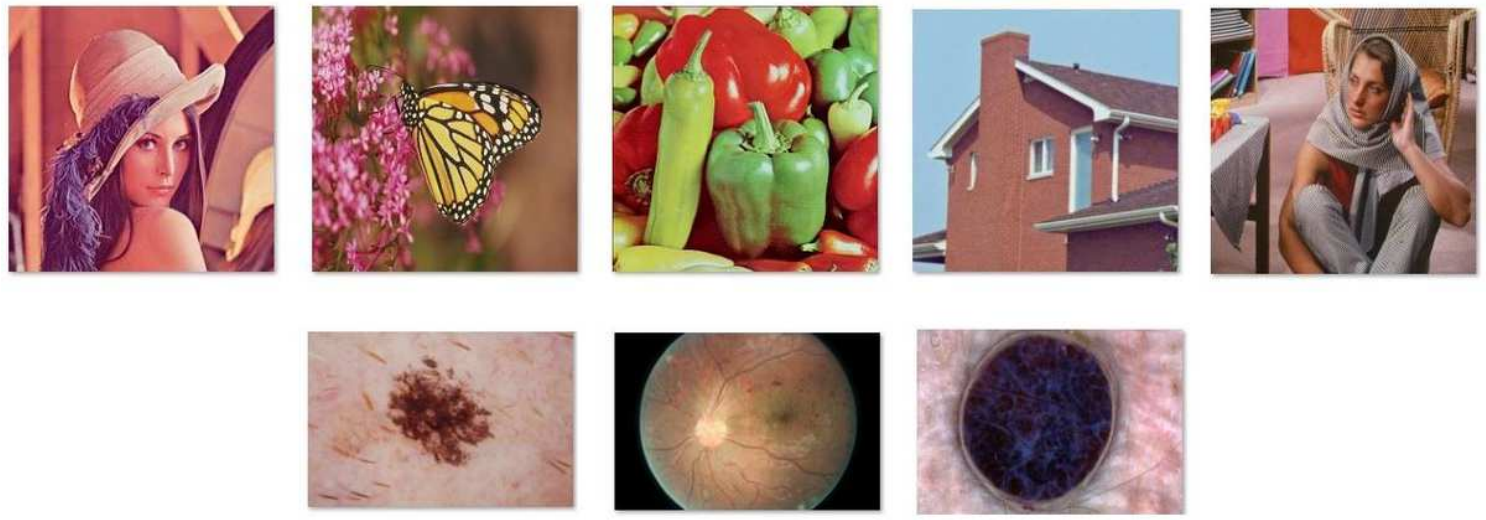


Figure 4

Sample Images

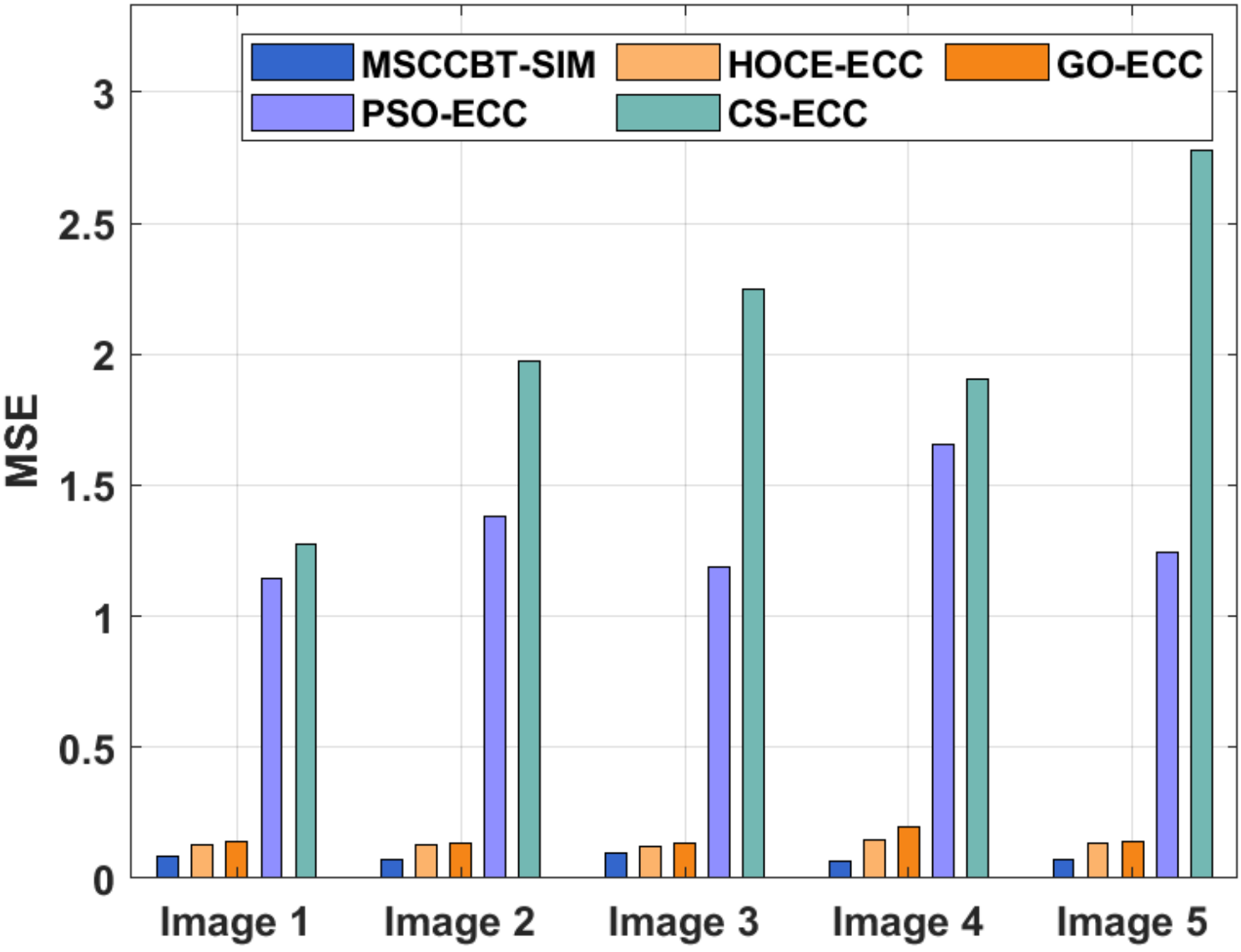


Figure 5

MSE analysis of MSCCBT-SIM model

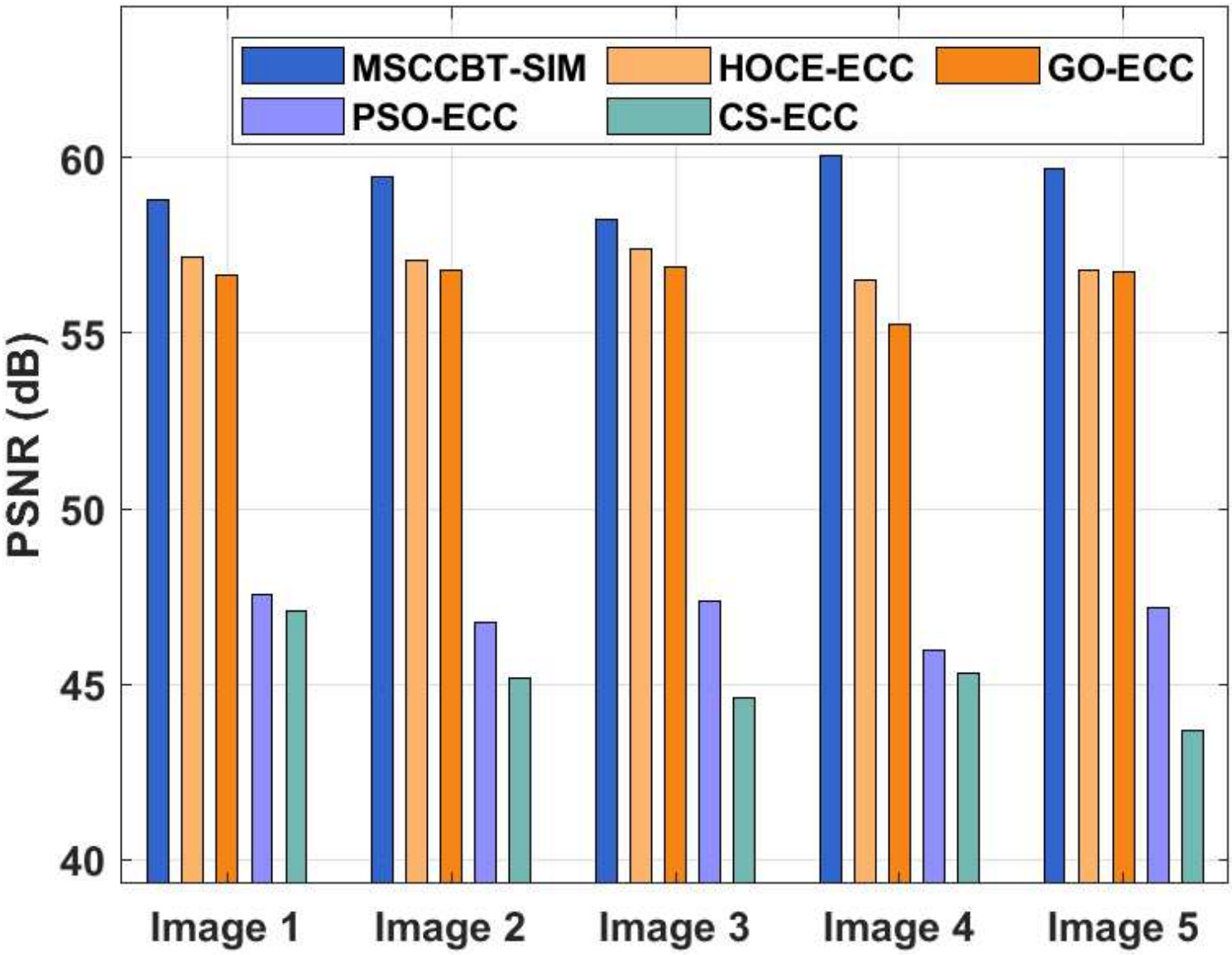


Figure 6

PSNR analysis of MSCCBT-SIM model

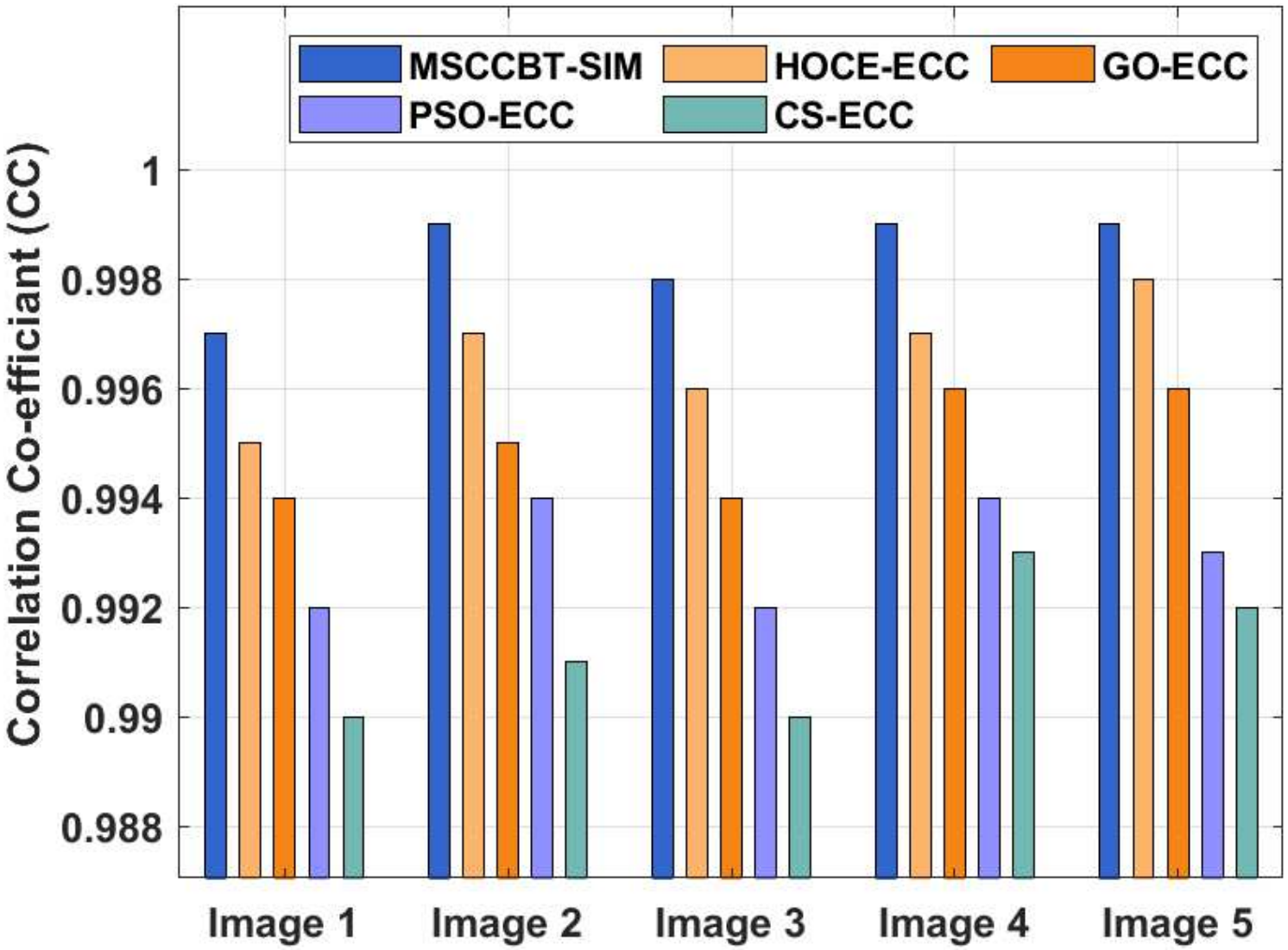


Figure 7

Result analysis of MSCCBT-SIM model interms of CC

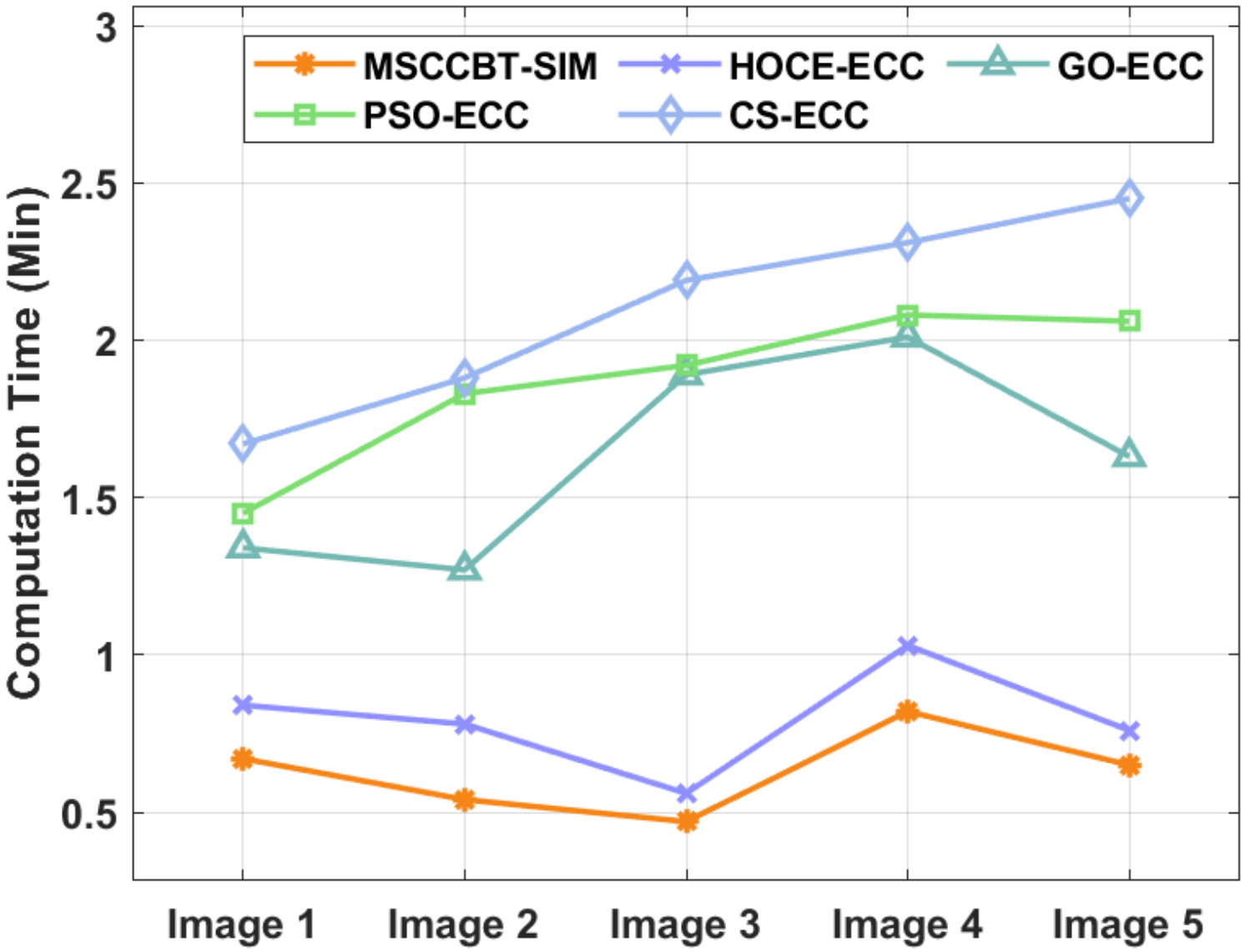


Figure 8

Computation time analysis of MSCCBT-SIM model

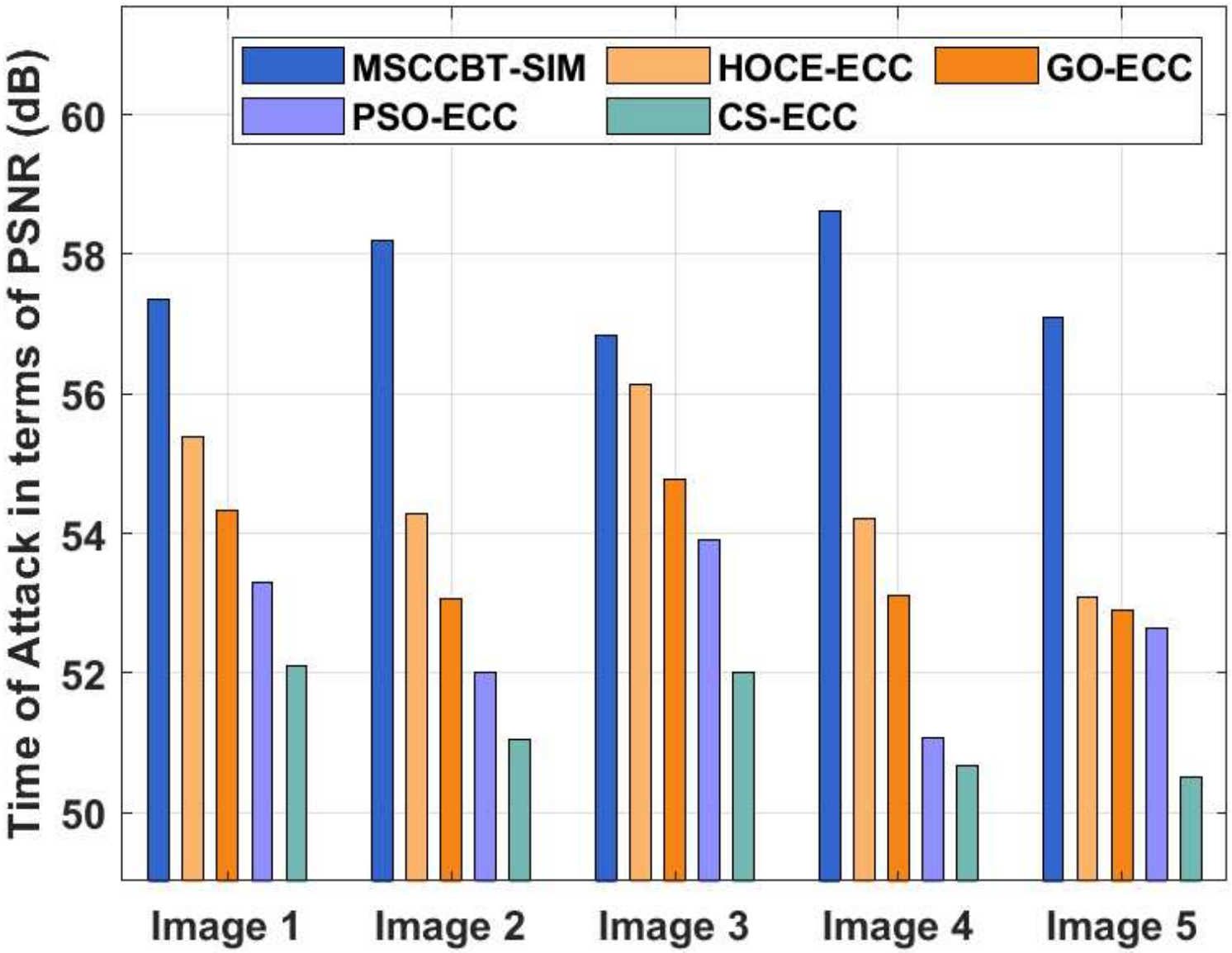


Figure 9

PSNR analysis of MSCCBT-SIM model with existing techniques