Blockchain based security framework for sharing digital images using reversible data hiding and encryption

Denslin Brabin1 · Christo Ananth2 · Sriramulu Bojjagani3

Received: 3 January 2021 / Revised: 16 May 2021 / Accepted: 9 February 2022 / Published online: 21 March 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract
Security is an important issue in current and next-generation networks. Blockchain will be an appropriate technology for securely sharing information in next-generation networks. Digital images are the prime medium attacked by cyber attackers. In this paper, a blockchain based security framework is proposed for sharing digital images in a multi user environment. The proposed framework uses reversible data hiding and encryption as component techniques. A novel high capacity reversible data hiding scheme is also proposed to protect digital images. Reversible data hiding in combination with encryption protects the confidentiality, integrity and authentication of digital images. In the proposed technique, the digital image is compressed first to create room for data hiding, then the user signature is embedded; afterwards the whole image is encrypted. For compression, JPEG lossy compression is used to create high capacity. For encryption, any symmetric block cipher or stream cipher can be used. Experimental results show that the proposed blockchain based framework provides high security and the proposed reversible data hiding scheme provides high capacity and image quality.

Keywords Blockchain · Compression · Encryption · JPEG · Reversible data hiding

✉ Denslin Brabin
denscse@gmail.com

Christo Ananth
dr.christoananth@gmail.com

Sriramulu Bojjagani
sriramulubojjagani@gmail.com

1 Department of Computer Science and Engineering, DMI College of Engineering, Chennai, Tamil Nadu, India
2 Department of Natural and Exact Sciences, Samarkand State University, Samarkand, Uzbekistan
3 Department of Computer Science and Engineering, SRM University-AP, Amaravati, Andhra Pradesh, India
1 Introduction

Next-Generation Networks (NGN) are the next-generation wireless communication systems that will drastically change the progress of the society. Nowadays, the initiation of the Internet of Everything (IoE) has prompted a rush in the volume of data transfer for the current and upcoming networks [13]. Securing these data is an important issue in the networks. Blockchain technology will be an appropriate mean for securely sharing information in communication networks.

A blockchain is a growing list of blocks, called records that are linked and secured using cryptography. A blockchain is a decentralized, distributed, and open ledger that is used to record transactions. Initially it was implemented for crypto currency, called bitcoin later it finds application in different domains like Internet of Things (IoT), E-Governance, Information Sharing, Privacy protection etc. By using blockchain technology, new information is added to a block and is made available to all the users or nodes in a distributed network [8].

Data hiding techniques embed secret data in a digital medium such as text, image audio and video. In the receiving end, secret data can be extracted from the digital medium but the digital medium is distorted, it cannot be recovered to its original format. Data hiding techniques are used for secret communication (Steganography) and copy right protection (Watermarking). The objective of steganography is to embed a secret information inside digital media that should not be potential to notice the secret information by the attacker. The confidentiality of the secret information should be preserved. Watermarking embeds ownership information (watermark) directly in digital media with the objective of copyright protection. The watermark should not be corrupted and integrity should be preserved. Reversible Data Hiding (RDH) techniques embed secret data in a digital medium similar to data hiding, but in the receiving end digital medium can be recovered to its original format after extraction of secret data.

Data hiding in digital images is by far the best method because it is easy to hide secret data in digital images without affecting the visual quality of images. As images are more vulnerable to attack in the cyber world, it needs to be protected. RDH in combination with encryption protects the confidentiality, integrity and authentication of digital images. JPEG (Joint Photographic Experts Group) compression is used to create more room for embedding user secret. Remaining portion of the paper explains about the literature survey, proposed framework, algorithm steps, implementation details and result analysis of the proposed technique.

2 Literature survey

Blockchain technology is being started to use in different fields of applications. Some of the important works on blockchain technology is explored here. The study in [5] explores how blockchain technology is used for detecting frauds in online businesses. Subjective fraud and objective fraud are differentiated in the case of rating fraud and explains the detection of objective fraud effectively using blockchain technology. This study explores the opportunities in designing the reputation system for online businesses by preventing objective frauds using blockchain technology. Dobre et al. [6] proposed an authentication method for JPEG image using blockchain technology. It uses signature based image authentication instead of image processing based or watermarking based authentication. Feature based signature of a digital image is extracted and encrypted, then added to blockchain for authentication. Signature of the
image is protected and it can be verified by using this method, but image content cannot be protected. Application of blockchain technology in securing an energy system is explained in [7]. A complete blockchain based security infrastructure prototype is proposed for energy grid system which is supported by cloud and IoT. Advantages and limitations of the proposed model are also analyzed.

Blockchain based data sharing system is proposed by Zheng et al. [31], which protects the privacy of multi-party data. It uses Paillier cryptosystem to provide data confidentiality. The transaction information of shared data is protected by using Paillier cryptosystem. The proposed model uses different layers: user, data, cloud and blockchain to provide different levels of security. The Paillier cryptosystem along with blockchain technology shall protect secret data effectively. A copyright protection system using blockchain technology and watermarking is proposed in [16]. In the proposed system, blockchain is used to store watermark(copyright) information in a secure manner. Hash value of the image is calculated using perceptual hash function which is used as ID of the image. Then, the watermark is embedded on the image and the watermarked image is stored using Inter Planetary File System(IPFS) instead of centralized servers. Nagasubramanian et al. [17] proposed a method for protecting healthcare records in the cloud using blockchain technology. In the proposed system, Keyless Signature Infrastructure (KSI) is used for securely storing the digital signatures. KSI is not using any key instead it uses a hash value for ensuring the security. Healthcare records are signed and stored in blockchain and can be verified at any time.

An automatic log-in system is proposed in [11] by applying the blockchain theory. Security of the automatic log-in system is maintained using fingerprint recognition function. A user can be authenticated in three platforms: mobile, PC and IoT environment. Blockchain technology is applied to strengthen the security of fingerprint information against tampering or forging. Mehedi et al. [15] proposed a security management mechanism for IoT setup. It uses ethereum which enables to write, deploy, and use smart contracts. A decentralized and fault-tolerant security management mechanism is created for IoT infrastructures. Rakovic et al. [21] explains the combined effect of blockchain and IoT. The issues and challenges induced by the integration of blockchain and IoT are described in this study. It also shows how blockchain is used to construct secure mesh networks of active IoT devices that avoid threats. Ryu et al. [22] proposed an investigation framework for IoT environment. Blockchain technology is used to provide integrity of data in the digital forensics framework. The four categories of blockchain used in the proposed system are investigator, IoT user, IoT device manufacturer and service provider. Application of blockchain technology in E-voting is projected in [29]. Security of the voting procedure is ensured by storing all the votes in blockchain that are linked cryptographically. A synchronized model is designed to verify voting records and to avoid forgery of votes.

Li et al. [14] proposed blockchain based architecture for Vehicular Ad Hoc Network (VANET). It provides deployment of decentralized structure and security. Different algorithms are proposed to protect identity of user and location. Two parameters called k-anonymity and average distance are used to protect vehicular location. Yang et al. [28] proposed a data sharing system for medical data using blockchain technology and attribute cryptosystem. In the proposed system, the medical data are encrypted using attribute-based encryption and stored in the cloud. The medical-related information and storage address are stored in blockchain to ensure the integrity of stored medical data. It combines the benefits of blockchain technology and cloud system. A blockchain based framework for steganography is proposed in [23] that uses dilated Robert’s edge detection to increase the payload embedding capacity. The secret
image is decomposed into frames (blocks) and each frame is considered as one transaction in block chain technology. A shared secret key is used to encrypt the stego-image and the same key is used by the receiver to extract the secret data.

In the past few years some RDH researches were carried out in encrypted domain of digital images. In some works, data hiding is performed in the encrypted image and in other works secret data is embedded first and then image is encrypted. Subramanyam et al. [26] proposed a watermarking technique for encrypted JPEG2000 images. In this technique, the JPEG2000 compressed image is encrypted using stream cipher, then watermarking bits are embedded in less significant bit planes of middle resolutions without affecting image quality. Bouslimi et al. [3] proposed a joint encryption and watermarking scheme for medical images. It uses Quantization Index Modulation (QIM) scheme for watermark embedding and stream cipher or block cipher algorithm for encryption. Abdulla et al. proposed two steganography approaches [1, 2] based on bit-plane manipulation. The first approach increases the embedding capacity by using bit-plane mapping mechanism. Two secret bits are embedded into three LSBs of each pixel in the cover image by using Fibonacci bit-plane mapping. The second approach increases the security by hiding in multiple image planes by using bit-plane index manipulation which increases the undetectability of the stego-image.

Qian et al. [19] proposed a RDH scheme for encrypted JPEG images. In this technique, the image is compressed using JPEG compression, then the JPEG byte streams are encrypted using stream cipher, afterwards the secret messages are embedded by slightly modifying the encrypted JPEG byte stream. Encryption key and data hiding key are used to enhance security. In the receiving side, after decryption and extraction of secret data, original JPEG image can be restored perfectly. Zhou et al. [32] proposed a RDH scheme for digital images in encrypted domain. The digital image is encrypted using steam cipher and the encrypted image act as a cover for data hiding. Data hiding is performed using public key modulation with set of public keys that are selected prior to data hiding. At the receiving side, a two class Support Vector Machine (SVM) classifier is used to extract the secret message and restore the original image. Zhang et al. [30] proposed a RDH scheme for encrypted images using public key cryptography. In this technique, preprocessing is performed to shrink the image histogram, then encryption of the pixels is performed by using public key crypto system such as Paillier and Damgard–Jurik cryptosystems. After encryption, secret message bits are embedded by slightly modifying the cipher pixel values. Because of histogram shrinking, the data embedding process should not cause any overflow/underflow problem.

Huang et al. [9] proposed a RDH scheme for JPEG images based on histogram modification. In this technique, data embedding is performed based on the modification of Discrete Cosine Transform (DCT) coefficients. Only coefficients with values 1 and −1 are selected to embed secret bits and remaining coefficients are unchanged. A location map is used to identify the selected coefficients in the recovery process. Another framework for encryption domain based RDH is proposed in [10]. In this framework, a digital image is divided into sub-blocks and each sub-block is encrypted using a random stream key. Then the encrypted sub-blocks are permuted to preserve the correlation between neighboring pixels. The data hiding is performed using any RDH technique in the permuted image. Here, the RDH scheme is independent of encryption. Jiang et al. [12] proposed an encryption domain based RDH technique for 3D meshes. This technique maps the decimal coordinates of the 3D mesh into integers, and then the integers are converted into bit stream to perform stream cipher encryption. The Least Significant Bits (LSBs) are altered to hide secret data using a data
hiding key. In the receiving side, using the data hiding key and the spatial correlation in the mesh model the secret data is extracted and the original mesh is recovered.

A prediction based RDH scheme for encrypted images is proposed in [18]. In the encoding side, the image is encrypted and secret bits are embedded in Most Significant Bits (MSBs) by substitution instead of LSBs. In the decoding side, the secret bits are directly extracted from the MSBs and the lost MSBs of the encrypted image are recovered by prediction. After MSB recovery the encrypted image is decrypted to get the original image. Shukla et al. [25] proposed a high capacity RDH scheme. The secret message is first compressed using arithmetic coding, and then encrypted using Advanced Encryption Standard (AES) algorithm. After compression and encryption, the secret bits are embedded using LSB substitution and Pixel Value Differencing (PVD). Shin et al. [24] proposed a RDH scheme for encrypted images in which the encrypted images are given as input to data sender and the secret data is embedded by data sender. Encrypted image is divided into four pixel blocks and the different values of two-pixel pairs in each block is used to hide secret data. Xie et al. [27] proposed an improved RDH method for JPEG images by extending Huang et al. [9] method. In this method, frequency coefficients with values in \((1, -1, 2, -2)\) are selected, then secret data is embedded into the selected coefficients by doubling them. A location map is required to identify the selected coefficients. The unselected coefficients are kept as it is. A removable visible watermarking scheme for JPEG image is proposed in [4]. In this scheme, DCT coefficients of cover image is modified in accordance with the DCT coefficients of watermark image. The visibility of the watermark can be adjusted based on different application requirements by modifying the watermarking parameters. Qiu et al. [20] proposed a block based RDH scheme for encrypted images. The secret data and auxiliary data are embedded using integer transformation which is reversible in the receiving end. Lossless compression is applied in the carrier image to create room for data hiding.

In this paper, a blockchain based framework is proposed to protect digital image. Most of the existing blockchain based frameworks provide only authentication and integrity. But the proposed blockchain based framework provides the security services authentication, confidentiality, integrity, access control and availability. A novel reversible data hiding technique in encryption domain is proposed to provide the security services. Only limited amount of secret data can be hidden in digital images by using the existing RDH techniques. In the proposed technique, more secret data bits can be embedded in digital images without affecting the visual quality of the image. JPEG compression is applied before data embedding which makes more room for data hiding.

### 3 Proposed framework

The proposed blockchain based framework is used to protect digital images in a multiuser environment. Users of the framework is divided into three categories as shown in Table 1 to access the digital images. Group A users having all the rights to access the image are called as administrators. Group A users can create an image, hide their signature in the image blocks and also verify other group A users. Group B users are called insiders, they can access the encrypted image and can decrypt the image to view the content of the image. Group C users are completely prohibited from accessing the image; they can only view the traffic. Group C users are called as outsiders.
In the proposed framework, an administrator can create or select an image, and the image is divided into blocks of size $8 \times 8$. Signature of each user of group A is embedded in the image blocks. Block (1, 1) contains the signature of owner of the image. User signature can be embedded into the image blocks using the proposed RDH scheme explained in section 4. The user signature can be XORed with watermarking key before embedding in the image block to enhance the security. Each block of the image contains image information and user signature as shown in Fig. 1. Number of group A users are limited based on the number of blocks in the image. For example, a $512 \times 512$ image contains 4096 blocks of size $8 \times 8$. So maximum 4096 group A users can access the image. Number of Group B and Group C users are unlimited.

Let us consider user-1 creates an image and embeds his signature on the first block of the image. After signing, he will encrypt the entire image and send to other Group A users. Group A users those who are accepting the image and willing to embed their signature, can hide their signature in the image blocks. If majority of Group A users (More than 50% of users) signed the image, then it can be considered as accepted. Each user can verify the owner of the image and the other users who have signed the image. The signed and encrypted images are send to group B users. Group B users can decrypt and view the image. They can verify the owner and other users who have signed the message. Outsiders (Unauthorized users) cannot view the image and verify the users. The user signature consists of following fields as shown in Fig. 2.

1. Date: It is a 3 byte field in the format of DD/MM/YY and 1 byte for each
2. Time: It is 3 byte field in the format of H:M:S and 1 byte for each
3. User ID: It is 2 byte field accepts any integer value between the range of 0 to $2^{16}-1$.
4. User Information: It is a variable length field in which user can provide any information about the user and image.

### 4 Proposed RDH scheme

The proposed high capacity reversible data hiding scheme consists of encoding and decoding portions. The encoding portion consists of three operations compression, embedding and encryption as shown in Fig. 3a. First the image is separated into $8 \times 8$ blocks, and then
compressed using a JPEG lossy compression algorithm to make room for data hiding. During JPEG compression process, operations up to quantization is applied. Then the secret data (user signature) is embedded in the image and finally the image is encrypted using any block cipher (e.g. AES, DES) or stream cipher (e.g. RC4) algorithm to create encrypted stego-image. In digital image, size of each pixel is 8 bits in case of gray scale image or 24 bits for color images. In case of color images, each plane (R, G, B) is separately processed.

![Diagram](image_url)  
**Fig. 1** Information on image blocks

![Table](image_url)  
**Fig. 2** Signature format
According to the JPEG compression algorithm, the digital image \( I \) is divided into \( N \) number of blocks of size \( 8 \times 8 \). Each block is converted from spatial domain into frequency domain using forward DCT. The pixel \( P(x, y) \) of each block is converted into \( F(i, j) \) using DCT.

\[
I = I_1 \| I_2 \| I_3 \| \ldots \| I_N
\]

Then the frequency coefficients are quantized using JPEG quantization Table (Q). After quantization process, the high indexed frequencies become zero. If zig-zag scanning is performed on \( 8 \times 8 \) block of 64 coefficients, the 32 higher end coefficients are zero in most of the blocks. This higher end zero coefficients are the room for data embedding.
Each quantized DCT block consists of 64 coefficients. The nonzero coefficients are signed integers with negative and positive values. These nonzero coefficients are represented as positive number using sign magnitude representation as 8 bits with first bit (MSB) as sign bit and remaining 7 bits as magnitude. For example if the frequency coefficient is 6, it is represented as 00000110 (Integer equivalent is 6), if the coefficient value is −6, it is represented as 10000110 (Integer equivalent is 134). After the sign magnitude representation, every block B consists of 64 positive integer coefficients and each coefficient consists of 8 bits as shown in Eq. (5), where \( b_i \) is sign bit.

\[
B_i = C_1 \| C_2 \| C_3 \| \ldots \ldots \| C_{64}
\]

\[
C_i = b_1 \| b_2 \| b_3 \| b_4 \| b_5 \| b_6 \| b_7 \| b_8
\]

A threshold (T) can be used to denote number of coefficients used in each block for data embedding. This T can be common in all the blocks. For example, if the last 10 coefficients of all the blocks are zero, the threshold value is 10. That means the higher end 10 coefficients of each block are used for embedding user signature. Data embedding is performed by directly replacing the zero coefficients with the data bits of user signature (S). One coefficient is replaced by 8 bits. So if 10 coefficients are used for data embedding in a block, 10 \( \times \) 8 = 80 bits can be embedded in one block. If the image size 512 \( \times \) 512, then 4096 blocks are there. In each block if 80 bits (10 bytes) are embedded, then totally 327,680 bits (40,960 bytes) can be embedded in that image. One block is used to embed the signature of one Group A user. Therefore, in a 512 \( \times \) 512 image, 4096 users can embed their signature. If the threshold value is 20 then user signature of 20 bytes can be embedded in each block. All the bytes (minimum 10; maximum 30; numbered as 1 to 30) of the user signature is embedded in a block of 8 \( \times \) 8 using reverse of Zig-Zag scanning order as shown in Fig. 4. First byte of user signature is embedded on 64th position, second byte is embedded on 63rd position and so on. After embedding user signature in all the blocks, the image is encrypted using block cipher like AES or stream cipher like RC4. The resultant image is called as encrypted stego-image (SI). That is send to the receiver or stored in repository.

\[
T_i = D(B_i, S)
\]

\[
M_i = E(K, T_i)
\]

\[
SI = M_1 \| M_2 \| M_3 \| \ldots \ldots \| M_m
\]

Where,

\[ B_i \] \( i^{th}\) block of quantized image

\[ T_i \] Signature Embedded \( i^{th}\) block

\[ D \] Data hiding function
The algorithm of data embedding can be explained with an example shown in Fig. 5. Consider an image block as shown in Fig. 5a. After converting the original image block pixels into frequency coefficients, the DCT block is produced as shown in Fig. 5b. Figure 5c shows the DCT block after quantization with JPEG default quantization table. Then the negative integers are converted into positive integers using sign magnitude representation as shown in Fig. 5d. Let the threshold T be 20. That means number of coefficients used in each block for data embedding is 20. So 20 byte user signature is embedded on the quantized DCT block. After embedding user signature, the stego-image block looks like Fig. 5e. At last, the stego-image block is encrypted using RC4 algorithm with sample key and the resultant encrypted stego-image is shown in Fig. 5f.

Block diagram of the decoding process is shown in Fig. 3b. In the decoding process, the user signature is extracted from the encrypted stego-image and the JPEG decompressed image is recovered. First the stego-image is divided into \(8 \times 8\) blocks. Then each block is decrypted using decryption function and encryption key. From the decrypted block, the high end coefficients are extracted as user signature based on the threshold T. If the threshold T is 20 then 20 high end coefficient values are extracted as user signature from the decrypted block. After extraction of signature, the 20 pixel values are assigned as zero. Based on sign bit of low end coefficients, the coefficients need to be converted into positive or negative integer. If the sign bit (MSB) is 0, it is a positive integer, otherwise it is a negative integer. For example, if the
frequency coefficient is 6, its binary form is 00000110 and the sign bit is 0. So it is positive integer and the original coefficient value is 6. If the coefficient value is 134, its binary form is 10000110 and the sign bit is 1. So it is negative integer and the original coefficient value is \(-6\). Same way, all the blocks are processed to extract user signature. The extracted user signature need to be XORed with watermarking key to verify signature. Then all the blocks are dequantized and inverse DCT is performed. Finally, all the blocks are combined to recover the JPEG decompressed original image. In the proposed RDH technique the original host image cannot be recovered in its original form, instead JPEG decompressed image is recovered. But human visual system cannot identify any visual artifacts in the recovered image. Group A users can decrypt the stego-image, extract and verify the signature by using encryption key, watermarking key and threshold value. Group B users are holding only
encryption key. So they can decrypt the image to view the content of the image. But they cannot verify the signature. Group C users are completely prohibited from accessing the image because they are not having any key.

5 Results and discussion

The proposed RDH scheme is implemented in MATLAB and tested with different gray scale and color images. The sample digital images Lena, Baboon, Boat, Peppers and Airplane of size $512 \times 512$ are considered as test images. The original image, encrypted stego-image and recovered image of these sample images are shown in Fig. 6. The Peak Signal to Noise Ratio (PSNR) is used to quantitatively measure the quality of the recovered image. The proposed RDH scheme will not produce exact replication of the original image in the decoding phase. Instead it produces JPEG decompressed image which has data loss, but it will not affect the visual quality of the image. For the threshold value 10, image quality of the recovered host images and the JPEG decompressed image are shown in Table 2. PSNR of the recovered image and the JPEG decompressed image are exactly same when the threshold is 10. So the minimum size of the user signature is 10 bytes.

$$PSNR = 10^{\log_{10} \left( \frac{255^2}{MSE} \right)}$$

Where,

- $MSE$ Mean Square Error
- $H$ Height of a digital image
- $W$ Weight of a digital image
- $I$ Host image
- $\tilde{I}$ Processed image

The embedding capacity based on different thresholds is mentioned in Table 3. For every 5 increments in threshold, 163,840 bits (20,480 bytes) embedding capacity is increased. High capacity of 983,040 bits is achieved for the threshold 30 with only fractional variation in image quality. The variation in PSNR value for different thresholds for the sample images are shown in Table 4 and Fig. 7. PSNR value at threshold 0 represents the normal JPEG decompressed image quality with quality factor 50. Up to the threshold value 30, the variation in PSNR between JPEG decompressed image and the image recovered by the proposed technique is less than 1. When we consider the maximum size of the user signature as 30 bytes, there is only fractional variation in PSNR. Thus the proposed RDH scheme provides high capacity and good image quality.

The comparison of proposed technique with the existing JPEG based and/or encryption based techniques is shown in Table 5. For this comparison, JPEG compression quality factor is taken as 50 and Threshold is considered as 15 (Embedding capacity is approximately 50,000 bits). The quality of the recovered image is high in proposed RDH scheme when compared
Fig. 6  Original Image, Encrypted Stego-Image and Recovered Image of sample test images a Lena b Baboon c Boat d Peppers e Airplane
whose JPEG compression based RDH schemes. The embedding capacity is also very high in the proposed scheme. Security evaluation of the proposed blockchain based security framework is shown in Table 6. The five important security services (confidentiality, integrity, authentication, access control and availability) are achieved effectively by the proposed framework.

6 Conclusion

A blockchain based security framework is proposed for protecting digital images in current and next generation networks. It provides different levels of security services to different levels (Three categories) of user in a network when sharing digital images. User signature is embedded in the image block to provide authentication and integrity. User signature of size up to 30 bytes can be embedded in an image block of size $8 \times 8$ and maximum 4096 administrative users can access a $512 \times 512$ image. A high capacity RDH scheme is proposed to embed the user signature in the proposed framework. JPEG compression is used to enhance

### Table 2  PSNR of recovered images

| SL.No. | Image  | PSNR of recovered image | PSNR of JPEG image |
|--------|--------|-------------------------|--------------------|
| 1      | Lena   | 35.78                   | 35.78              |
| 2      | Baboon | 28.49                   | 28.49              |
| 3      | Boat   | 33.49                   | 33.49              |
| 4      | Peppers| 34.84                   | 34.84              |
| 5      | Airplane| 35.99                  | 35.99              |

### Table 3  Embedding capacity

| SL.No. | Threshold (T) | Number of bits |
|--------|---------------|----------------|
| 1      | 5             | 163,840        |
| 2      | 10            | 327,680        |
| 3      | 15            | 491,520        |
| 4      | 20            | 655,360        |
| 5      | 25            | 819,200        |
| 6      | 30            | 983,040        |

### Table 4  PSNR comparison for sample images

| SL.No. | Threshold (T) | Lena | Baboon | Boat | Peppers | Airplane |
|--------|---------------|------|--------|------|---------|----------|
| 1      | 0             | 35.7852 | 28.49 | 33.4953 | 34.8429 | 35.9977 |
| 2      | 5             | 35.7852 | 28.49 | 33.4953 | 34.8429 | 35.9977 |
| 3      | 10            | 35.7838 | 28.49 | 33.4946 | 34.8429 | 35.9977 |
| 4      | 15            | 35.7838 | 28.3392 | 33.4786 | 34.8404 | 35.9797 |
| 5      | 20            | 35.7751 | 27.6752 | 33.2801 | 34.8013 | 35.2695 |
| 6      | 25            | 35.0713 | 26.7786 | 32.0397 | 34.3316 | 34.5921 |
| 7      | 30            | 34.3100 | 25.7363 | 30.8997 | 33.3910 | 33.1168 |
the hiding capacity. Variable length user signature can be embedded in the image blocks because of high capacity. Maximum hiding capacity of 102,400 bytes is achieved with good image quality of about 35 dB. The proposed framework combines blockchain technology,

**Table 5** PSNR comparison of proposed technique with existing techniques

| SL.No. | Threshold (T) | PSNR of different images |
|--------|---------------|--------------------------|
|        | Proposed      | Shin et al. [24] | Xie et al. [27] | Qiu et al. [20] |
| 1      | Lena          | 35.7838        | 34.00          | 33.76          | 32.71          |
| 2      | Baboon        | 28.3392        | 28.02          | 26.52          | --             |
| 3      | Boat          | 33.4786        | 31.44          | 31.61          | 29.61          |
| 4      | Peppers       | 34.8404        | 32.49          | 33.89          | 32.08          |
| 5      | Airplane      | 35.9797        | 31.26          | --             | 29.62          |
reversible data hiding and encryption to provide different security service. Experimental results reveal that the proposed framework helps to share digital images securely in a multi user environment without overheads.

References

1. Abdulla AA, Jassim SA, Sellahewa A (2013) Efficient high capacity steganography technique. Proc SPIE 8755:875508. https://doi.org/10.1117/12.2018994
2. Abdulla AA, Jassim SA, Sellahewa H (2013) Secure steganography technique based on Bitplane indexes. In: IEEE international symposium on multimedia, pp 287–291. https://doi.org/10.1109/ISM.2013.55
3. Bouslimi D, Coatrieux G, Cozic M, Roux C (2012) A joint encryption/watermarking system for verifying the reliability of medical images. IEEE Trans Inf Technol Biomed 16:891–899
4. Brabin DRD, Perinbam JRP, Meganathan D (2020) Watermark visibility adjustable RVW scheme for JPEG images. Wirel Pers Commun 115:187–202
5. Cai Y, Zhu D (2016) Fraud detections for online businesses: a perspective from blockchain technology. Financ Innov 2. https://doi.org/10.1186/s40854-016-0039-4
6. Dobre RA, Preda RO, Oprea CC, Pirmog I (2018) Authentication of JPEG images on the blockchain. In: Proceedings of IEEE international conference on control, artificial intelligence, Robotics & Optimization, pp 211–215
7. Dong Z, Luo F, Liang G (2018) Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems. J Mod Power Syst Clean Energy 6:958–967
8. Elisa N, Yang L, Chao F, Cao Y (2018) A framework of blockchain-based secure and privacy-preserving E-government system. Wirel Netw. https://doi.org/10.1007/s11276-018-1883-0
9. Huang F, Qu X, Kim HJ, Huang J (2016) Reversible data hiding in JPEG images. IEEE Trans Circuits Syst Video Technol 26(9):1610–1621
10. Huang F, Huang J, Shi YQ (2016) New framework for reversible data hiding in encrypted domain. IEEE Transactions on Information Forensics and Security 11:2777–2789
11. Huh JH, Seo K (2019) Blockchain-based mobile fingerprint verification and automatic log-in platform for future computing. J Supercomput 75:3123–3139
12. Jiang R, Zhou H, Zhang W, Yu N (2018) Reversible data hiding in encrypted three-dimensional mesh models. IEEE Trans Multimedia 20:55–67
13. Li B, Fei Z, Zhang Y (2019) UAV communications for 5G and beyond: recent advances and future trends. IEEE Internet Things J 6:2241–2263
14. Li H, Pei L, Liao D, Sun G, Xu D (2019) Blockchain meets VANET: an architecture for identity and location privacy protection in VANET. Peer-to-Peer Netw Appl 12:1178–1193
15. Mehedi SKT, Shamim AAM, Miah MBA (2019) Blockchain-based security management of IoT infrastructure with Ethereum transactions. Iran J Comput Sci 2:189–195
16. Meng Z, Morizumi T, Miyata S, Kinoshita H (2018) Design scheme of copyright management system based on digital watermarking and blockchain. In: Proceedings of IEEE international conference on computer software & applications, pp 359–364
17. Nagasubramanian G, Sakthivel RK, Patan R, Gandomi AH, Sankayya M, Balusamy B (2018) Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Comput & Applic 32:639–647
18. Puteaux P, Puech W (2018) An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images. IEEE Transactions on Information Forensics and Security 13:1670–1681

Table 6  Security evaluation

| Sl. No. | Requirements         | Employed safeguard                       |
|--------|----------------------|------------------------------------------|
| 1      | Confidentiality      | Symmetric encryption                     |
| 2      | Integrity            | Proposed RDH Scheme                      |
| 3      | Authentication       | Proposed RDH Scheme                      |
| 4      | Access control       | Three Categories of Users                |
| 5      | Availability         | Limited according to the user Category   |
19. Qian Z, Zhang X, Wang S (2014) Reversible data hiding in encrypted JPEG bitstream. IEEE Trans Multimedia 16:1486–1491
20. Qiu Y, Qian Z, Zeng H, Lin X, Zhang X (2020) Reversible data hiding in encrypted images using adaptive reversible integer transformation. Signal Process 167:107288
21. Rakovic V, Karamachoski J, Atanasovski V, Gavrilovska L (2019) Blockchain paradigm and internet of things. Wirel Pers Commun 106:219–235
22. Ryu JH, Sharma PR, Jo JH, Park JH (2019) A blockchain-based decentralized efficient investigation framework for IoT digital forensics. J Supercomput 75:4372–4387
23. Sarkar P, Ghosal SK, Sarkar M (2020) Stego-chain: a framework to mine encoded stego-block in a decentralized network. Journal of King Saud University - Computer and Information Sciences. https://doi.org/10.1016/j.jksuci.2020.11.034
24. Shin SH, Jung KH (2018) Reversible data hiding method using meaningful encrypted images. Multimed Tools Appl 77:14841–14857
25. Shukla AK, Singh A, Singh B, Kumar A (2018) A secure and high-capacity data-hiding method using compression, encryption and optimized pixel value differencing. IEEE Access 6:51130–51139
26. Subramanya V, Emmanuel S, Kankanhalli MS (2012) Robust watermarking of compressed and encrypted JPEG2000 images. IEEE Trans Multimedia 14:703–716
27. Xie XZ, Chia-Chen Lin CC, Chang CC (2019) A reversible data hiding scheme for JPEG images by doubling small quantized AC coefficients. Multimed Tools Appl 78:11443–11462
28. Yang X, Li T, Pei X, Wen L, Wang C (2020) Medical data sharing scheme based on attribute cryptosystem and blockchain technology. IEEE Access 8:45468–45476
29. Yi H (2019) Securing e-voting based on blockchain in P2P network. EURASIP J Wirel Commun Netw 137. https://doi.org/10.1186/s13638-019-1473-6
30. Zhang X, Long J, Wang Z, Cheng H (2016) Lossless and reversible data hiding in encrypted images with public-key cryptography. IEEE Trans Circuits Syst Video Technol 26:1622–1631
31. Zheng BK, Zhu LH, Shen M, Gao F, Zhang C, Li YD, Yang J (2018) Scalable and privacy-preserving data sharing based on blockchain. J Comput Sci Technol 33:557–567
32. Zhou J, Sun W, Dong L, Liu X, Au OC, Tang YY (2016) Secure reversible image data hiding over encrypted domain via key modulation. IEEE Trans Circuits Syst Video Technol 26:441–452

Publisher’s note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Denslin Brabin received B.E. and M.E. degrees in Computer Science and Engineering from Manonmaniam Sundaranar University, Tamil Nadu, India in 2002 and 2004 respectively. He received Ph.D. degree in Information and Communication Engineering from Anna University, India in 2018. He has 17 years of teaching experience. Currently he is working as Professor in the Department of Computer Science and Engineering, DMI College of Engineering, Chennai, India. He has published more than 15 research papers in International Journals. His current research interests include Image Processing and Cyber Security.
Christo Ananth got his B.E. Degree in Electronics and Communication Engineering in 2009 and his M.E. Degree in Applied Electronics in 2013. He received his Ph.D. Degree in Engineering in 2017. He completed his Post-Doctoral Research work in Co-operative Networks in 2018. Christo Ananth has almost spent a decade in research, instructing, counseling and down to earth application improvement. His exploration skill covers Image Processing, Co-operative Networks, Electromagnetic Fields, Electronic Devices, Wireless Networks and Medical Electronics. He has published 59 Research Papers in refereed and indexed International Journals. At present, he is a member of 140 Professional and Social-Welfare Bodies over the globe.

Sriramulu Bojjagani is currently working as Assistant Professor in the Department of Computer Science and Engineering, SRM University-AP, Amaravati, Andhra Pradesh, India. He received his Ph.D. from the University of Hyderabad, Hyderabad, India. He is a reviewer for the many reputed journals like IJCS: Wiley, Peer-to-Peer Networking and applications, Telecommunication systems: Springer, IEEE Security & Privacy and IEEE Systems. His research interests include design, testing of mobile payment applications, formal methods for verification of secure mobile protocols, Information security and privacy in IoV (Internet of Vehicles), Cloud Computing and SDN (Software Defined Networks)