An RGB Color Image Steganography Scheme by Binary Lower Triangular Matrix

Shiv Prasad, Arup Kumar Pal, and Soumya Mukherjee

***Abstract*— Steganography is an area where researchers focus on how to develop novel hiding techniques that are aided by the mathematical or computational model. In order to conceal the secret bits in a cover image, the imperceptible property and embedding payload capacity must be maintained. In most of the developed methods, some selective least significant bits (LSBs) of each pixel of the cover image is modified to hide the data which may lead to substantial distortion in the stego-image especially when the payload size is large. Therefore, to attain the trade-off between payload capacity and image quality, the authors have devised a binary lower triangular matrix-based secret message embedding process in which data can be hidden in the color pixel. In this secret message embedding process, the secret data is embedded aided by the binary lower triangular matrix. The formulated mathematical model for the secret message embedding process has ensured a secure embedding technique with reduced aberration on the stego-image. The proposed steganography scheme is preserving significant visual quality while emphasizing the security aspect by adopting an indirect data-hiding mechanism in contrast to the conventional mechanism. Furthermore, for the betterment of the visual properties of the stego-image, we have generically extended the formulation and tested it to check the visual quality. The empirical results of the proposed steganography scheme depict outcomes satisfactorily for the RGB color images. Researchers can explore and apply this novel data-hiding scheme in different data communication applications.**

***Index Terms*— Color image steganography, covert communication, matrix-based data hiding, stego-image.**

I. INTRODUCTION

INFORMATION technology grows manifolds in the last two decades, and the Internet becomes a backbone medium for the exchange of information among users situated in different parts of the globe. As the Internet becomes a public medium and accessible by one and all, it becomes a precursor of the threat of information security from a confidentiality, integrity, and authenticity perspective. As cybercrimes imperil the secrecy and authenticity of data [1], it becomes imperative to deal with the security threats to ensure that data should be accessible as well as perceptible only by the authorized users. In order to maintain the sanctity of data and to mitigate unauthorized access, the confidentiality of data plays a crucial role. Confidentiality ensures secure transmission of data over a public medium between the sender and receiver. Confidentiality can be attained by means of cryptography and steganography.

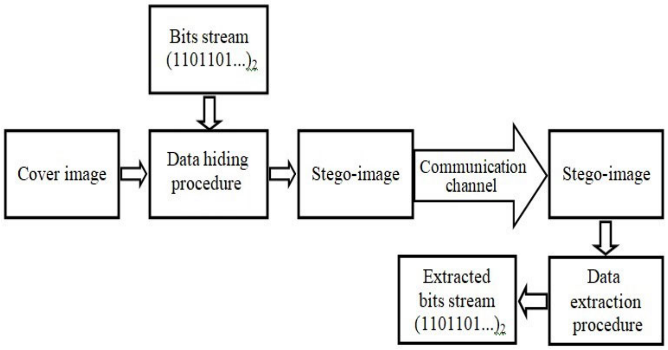
Bits stream (1101101...)$_2$
Cover image
Data hiding procedure
Stego-image
Communication channel
Stego-image
Data extraction procedure
Extracted bits stream (1101101...)$_2$

Fig. 1. Secret bits stream communication using image steganography scheme.

In cryptography, the actual texts of information are converted into cipher text i.e. the text without a meaning. On the other hand, steganography is a covert way of communication where actual data becomes a hidden entity veiled by some other information. Steganography conceals confidential information into meaningful digital cover media (i.e. image, video, and audio) to constitute meaningful imperceptible data which is known as a stego-media. In the image steganography technique, a secret bits stream is embedded into a cover image using some mathematical or computational model. Generally, these secret bits are inserted by some mechanisms, and this cover image and secret bits together formed a stego-image which must be indistinguishable from the cover image. This stego-image is sent over a communication channel, further received and secret bits are extracted by authorized user, deploying proper extraction process. Fig. 1 depicts the steganography mechanism where secret bit stream is employed in the cover image to generate stegoimage. In this technique at the first step, the sender selects a meaningful cover image in which a secret bit-stream is embedded into it by adopting a suitable data-hiding mechanism. This newly formed image which contains a secret bit-stream is called a stego-image. Further, this stego image is sent by the sender into the communication channel where it is difficult for any eavesdropper to suspect the presence of any secret message. In the last step, the receiver's end receives the stego-image and extracts the secret bitstream from the stego-image by deploying a proper data extraction procedure.

Manuscript received 1 October 2021; revised 23 September 2022 and 30 January 2023; accepted 7 March 2023. Date of publication 14 April 2023; date of current version 7 July 2023. The Associate Editor for this article was H. Huang. *(Corresponding author: Shiv Prasad.)*

The authors are with the Department of Computer Science and Engineering, Indian Institute of Technology (Indian School of Mines), Dhanbad, Jharkhand 826004, India (e-mail: psad.shiv@gmail.com).

Digital Object Identifier 10.1109/TITS.2023.3264467

As in steganography [2], [3], data flows in hidden form, so it becomes beyond suspicion for an unauthorized user to differentiate between the cover image and covert data. Among several steganography schemes, LSB based technique is widely exercised for its grater effectiveness as well as higher simplicity. Like, Chan and Cheng [4] have designed a secret data embedding technique into the digital images using LSB substitution in which, secret data are implanted into the cover image's least significant bits. T.-C Lu [5] suggested interpolation-based image steganography technique based on modulus function along with re-encoding approach, which directly hides the secret data and records the position of the altered pixel in order to produce the stego-image. In this method, secret bits are replaced with the cover image bits located at the least significant positions. i.e., present at LSB positions permanently by the secret message bit streams. It is common practice to hide up to three bits of the message into each grayscale cover pixel to maintain tradeoff between capacity and visual quality. Apart from that, the conventional data-hiding techniques found in the literature are not appropriate to hide secret data in color images. Since it causes significant color distortions. Further, color image steganography is suffering from the limitation of less bit embedding capacity and maintaining imperceptibility and quality of the stego-image. Our motivation is to add the secret data with a novel data-hiding technique that is more applicable to RGB color images.

Several researchers have suggested deploying the matrix embedding technique on different steganography approaches. Fridrich and Soukal [6] have proposed a large embedding payload-based matrix embedding technique, which has enhanced the hiding payload/capacity into the stego-media. It has enhanced the number of bits concealed per embedding modification. Mao [7] has suggested a steganography scheme with a fast algorithm for matrix embedding. The fast-embedding algorithm is utilized to search coset leader for hiding secret data with the help of Hamming code along with random linear code. Li et al. [8] designed a matrix-based steganography scheme, to embed a larger payload into the matrix. The parity check matrix is considered as the public key matrix in the data embedding technique which would be intimated to the both sender and receiver. Banerjee and Jana [9] have devised red, green and blue color components-based data hiding technique through (7, 4) Hamming code. In this technique, the cover image is divided into 3×3 block size and each block secret data is inserted into four bit-plane slicing of color component. Yang and Wang [10] presented a smart pixel adjustment based color image steganography scheme with two-color pixels block. Qin et al. [11] introduced a novel color image steganography scheme that utilized pixel vector cost, which has composition of color components in the same spatial position, as embedding units. The embedding capacity is adaptively fixed to every three color components. Carvajal-Gamez et al. [12] introduced an image steganography scheme based upon color local complexity estimation, which is immune to visual decrement and provides a greater hiding payload. It has exploited the cover image to supply a settlement between the hiding payload and the stego-image visual quality. Chowdhuri et al. [13] designed a secure steganographic scheme based upon compressed color image utilizing the properties of discrete cosine transform which has effective uses for various multimedia applications as its functionalities are based upon the shared secret key technique. Sabeti et al. [14] proposed an integer wavelet transform (IWT) using a genetic algorithm, where IWT is employed on each block of the cover image, later genetic algorithm is used to select high frequency coefficients to hide the data. This technique is suitable against any kind of steganoanalysis attack and retains the visual quality. Biswas and Bandyapadhay [15] designed a robust steganography technique utilizing a 2D-DCT and genetic algorithm. In this proposed method, at the first step, image pixels are sampled and later genetic algorithm is employed for optimized embedding secret bits. Hsieh and Wang [16] introduced a steganography technique where a constructive steganographic algorithm is deployed to generate example-based weighted color transfer instead of modifying the cover image. This technique possesses the high capacity of bit embedding techniques with better fidelity and robustness. Zhu et al. [17] proposed a robust image steganography technique based on inverse interpolation. In this proposed technique, an inverse interpolation technique is deployed to prevent data losses over the lossy channel. In this proposed technique authors solved the problem of intersectional blocks during the inverse interpolation process. Liu et al. [18] introduced an adversarial embedding method for enhancing the steganography technique. In order to achieve this, a new adversarial embedding scheme for image steganography is introduced to determine the directions of cost modifications, multiple gradients of the cover image have been combined and stego image is generated. Lu et al. [19] introduced robust JPEG steganography based on autoencoder combined with the adaptive Bose-Chaudhuri-Hocquenghem (BCH) encoding technique, which prevents loss and damage of secret data during transmission over a lossy medium. Here, BCH autoencoder is used for maintaining a relation between before and after compression and encoding is exploited to decrease the error rate. Further, in literature several steganography schemes [20], [21], [22] have been studied where secret data are initially enciphered by a standard cryptography technique and subsequently obtained enciphered messages embedded into the cover media. Our other objective in this work is to maintain a greater degree of security. Therefore, this kind of approach is more effective without combining any conventional cryptography with steganography techniques to achieve the desired goal.

A. Contribution

From the various literature survey, it has been found that most of the research works related to steganography has been suffering from the limitations of less bit capacity or maintaining imperceptibility and preserving quality. In this work, we have suggested a secure and enhanced RGB color image steganography. The proposed method hides the bits of secret data into each RGB color cover pixel by means of a binary lower triangular matrix (BLTM). The BLTM of dimension $A_{k\times k}$ has embedded k-bits of the secret data into the LSB position of R, G, and B color channels. In the contributions of the proposed work, BLTM, $A_{k\times k}$ is used for improving the bits embedding capacity without losing the visual quality of RGB color stego-image. The proposed technique developed an excellent and secure RGB color image steganography scheme, which exhibits the proper visual quality of color stego-images with a greater degree of security. The main contributions of the proposed technique are presented here:

- A secure RGB color image steganography scheme provides a higher degree of visual quality of the stego-image.
- This approach preserves the visual quality, and the level of bits embedding capacity compare to other color image steganography schemes because the secret data embedding process is carried out using BLTM.
- This technique is generic and can be applied to any kind of BLTM.

B. Organization

The remaining part of the paper is systematized as lower triangular matrix presented in section II. Section III illustrates the operation of secret image embedding and extraction of the proposed work. Section IV demonstrates experimental outcomes with comparisons of performance and evaluation of the proposed scheme. Finally, the conclusion is drawn of the proposed work in section V.

II. Lower Triangular Matrix

The lower triangular matrix, $A_{k\times k}$ is a square matrix in which all elements above the main diagonal are 0. The lower triangular matrices are given below:

$$A_{k\times k}=\begin{bmatrix} a_{1,1} & 0 & 0 & 0 & . & . & . & 0\\ a_{2,1} & a_{2,2} & 0 & 0 & . & . & . & 0\\ a_{3,1} & a_{3,2} & a_{3,3} & 0 & . & . & . & 0\\ . & . & . & . & . & . & . & 0\\ . & . & . & . & . & . & . & 0\\ . & . & . & . & . & . & . & 0\\ a_{k,1} & a_{k,2} & a_{k,3} & . & . & . & a_{k,k-1} & a_{k,k} \end{bmatrix}$$

where, $a_{i,j}$ are non zero component of the matrix with j ≤ i.

III. Proposed Method

Notations used in the proposed work are given in Table I In this proposed method, k secret bits are employed into RGB color cover pixel utilizing the binary lower triangular matrix (BLTM) of size $A_{k\times k}$. Here, the k signifies the number of embedding bits to the cover pixel, and accordingly, the matrix will be selected. Some typical BLTM of dimension $A_{2\times2}$, $A_{3\times3}$, $A_{4\times4}$ are depicted in Fig. 2 accordingly. Here in Fig. 2, $C_1, C_2, C_3\ldots$ are 1^{st}, 2^{nd}, 3^{rd}, ... column number from right to left in the binary lower triangular matrices.

In this proposed technique, the secret bits stream is embedded by exploiting the nature and attributes of matrix. So, with the help of BLTM, a standard array has been created. The role of this array is that the encrypted message represented as a δ vector which is mapped to another substituted vector denoted as V_n. The construction of the V_n vector is derived tactically from the column vector (i.e. C_i, where i=1 to k) from the BLTM matrix $A_{k\times k}$, with the exception δ is a zero vector, then V_n is also a zero vector.

TABLE I

Notations and Definitions

Notation	Definition
$A_{k\times k}$	BLTM of dimension $k\times k$
BLTM	The binary lower triangular matrix
C_1, C_2, C_3...	From right to left in BLTM 1^{st}, 2^{nd}, 3^{rd}.. columns
CC	Coefficient correlation
Diff.	Difference
FPR	False positive rate
FNR	False negative rate
NC	Normalized cross-correlation
δ	Encrypted secret message bits
HVQ	Human visual quality
k	Number of bits.
m	Secret message bits
m_k	The length of the secret message bits stream
RGB	Red, green, and blue color components
V_n	The new binary bits vector is generated with respect to columns
v_c	The cover vector
v_s	The stego-vector
$\mathcal{X}$	XOR columns number from right to left in BLTM
SDc	Standard deviation of cover image
SDs	Standard deviation of stego-image

$$A_{2\times2}=\begin{array}{cc} C_2 & C_1\leftarrow\\ \left[\begin{array}{c}1\\1\end{array}\right. & \left.\begin{array}{c}0\\1\end{array}\right]\end{array},\; A_{3\times3}=\begin{array}{ccc} C_3 & C_2 & C_1\leftarrow\\ \left[\begin{array}{c}1\\1\\1\end{array}\right. & \begin{array}{c}0\\1\\1\end{array} & \left.\begin{array}{c}0\\0\\1\end{array}\right]\end{array},\; A_{4\times4}=\begin{array}{cccc} C_4 & C_3 & C_2 & C_1\leftarrow\\ \left[\begin{array}{c}1\\1\\1\\1\end{array}\right. & \begin{array}{c}0\\1\\1\\1\end{array} & \begin{array}{c}0\\0\\1\\1\end{array} & \left.\begin{array}{c}0\\0\\0\\1\end{array}\right]\end{array},\ldots, A_{k\times k}$$

Fig. 2. BLTM are as: $A_{2\times2}$, $A_{3\times3}$, $A_{4\times4}$, ..., $A_{k\times k}$.

TABLE II

The Standard Array Based on BLTM of Size $A_{2\times2}$

δ	$\mathcal{X}$	V_n
00	C_0=[00]	00
01	C_1=[01]	01
10	$C_1\oplus C_2$=[10]	11
11	C_2=[11]	10

The value of the V_n, is indirectly depends on value of δ. If the δ vector can be realized or represented with the aid of column vector $A_{k\times k}$ BLTM, then V_n vector value depends on, the number of selected column vectors i.e. C_i. This process can be further elaborated with the help of an example like if $\delta = (110)$ then we construct the V_n from BLTM, of $A_{3\times3}$. We have observed, that $\delta = (110)$ comprises vectors C_3 and C_1 since $\delta = (\ C_3 \oplus C_1)$. So, V_n will be vector of 101, of corresponding to $\delta = (110)$ where the V_n construction is done based on selection of C_3 and C_1 to obtain δ.

After constructing the standard array, the secret message bits embedding process will be realized in pixel-wise of the given RGB color cover image. To embed k bits of secret data, let's consider an RGB color pixel of cover image. The process will start with the selecting of the k bits length of LSB components

TABLE III

THE STANDARD ARRAY BASED ON BLTM OF SIZE $A_{3\times3}$

δ	$\mathcal{X}$	V_n
000	C_0=[000]	000
001	C_1=[001]	001
010	$C_1 \oplus C_2$=[010]	011
011	C_2=[011]	010
100	$C_3 \oplus C_2$=[100]	110
101	$C_3 \oplus C_2 \oplus C_1$=[101]	111
110	$C_3 \oplus C_1$=[110]	101
111	C_3=[111]	100

TABLE IV

THE STANDARD ARRAY BASED ON BLTM OF SIZE $A_{4\times4}$

δ	$\mathcal{X}$	V_n
0000	C_0=[0000]	0000
0001	C_1=[0001]	0001
0010	$C_1 \oplus C_2$=[0010]	0011
0011	C_2=[0011]	0010
0100	$C_3 \oplus C_2$=[0100]	0110
0101	$C_3 \oplus C_2 \oplus C_1$=[0101]	0111
0110	$C_3 \oplus C_1$=[0110]	0101
0111	C_3=[0111]	0100
1000	$C_4 \oplus C_3$=[1000]	1100
1001	$C_4 \oplus C_3 \oplus C_1$=[1001]	1101
1010	$C_4 \oplus C_3 \oplus C_2 \oplus C_1$=[1010]	1111
1011	$C_4 \oplus C_3 \oplus C_2$=[1011]	1110
1100	$C_4 \oplus C_2$=[1100]	1010
1101	$C_4 \oplus C_2 \oplus C_1$=[1101]	1011
1110	$C_4 \oplus C_1$=[1110]	1001
1111	C_4=[1111]	1000

of the color pixel. For example, if we want to embed 3 bits of secret message into the cover pixels, then basically one LSB bit gets selected from each color component (i.e Red, Green, and Blue color components). In our case, we consider v_c=[b_1 b_2 … b_k] as the targeted cover component, where the secret message embedding process will be actualized. Here, the z vector is computed with the aid of v_c vector and $A_{k\times k}$ BLTM matrix as follows:

$$v = {v_c}^T \tag{1}$$

$$z = (A_{k\times k} \times v)^T = (z_1\ z_2 \ldots z_k)_2 \tag{2}$$

Here, the vector z represents a masking vector for enciphering the k bits of secret message i.e. $m = (m_1\ m_2 \ldots m_k)_2$. The message m is masked with z as:

$$\delta = z \oplus m = (em_1\ em_2 \ldots em_k)_2 \tag{3}$$

Here, the vector δ is masked message. Based on V_n, stego vector will be formed as follows.

$$v_s = v_c \oplus V_n \tag{4}$$

where v_s is the stego-vector, v_c is the cover vector of a particular cover pixel.

Mathematically, the secret message bits, m extraction procedure is depicted as:

$$v_T = {v_s}^T \tag{5}$$

$$m = (A_{k\times k} \times v_T)^T \tag{6}$$

Finally, m has been extracted as the original secret message bits.

Example 1: We took first RGB color pixel and decompose R = 123 = $(01111011)_2$, G = 127 = $(01111111)_2$, and B = 135 = $(10000111)_2$ from Fig. 3 and message bits, $m = (110)_2$. Now, extracted the bits from first LSB positions respectively from R, G, and B color components and represented as vector: $v_c = [1\ \ 1\ \ 1]$ and find, $v = {v_c}^T$. Now calculate $z = (A_{3\times3} \times v)^T = (101)_2$. Again, compute, $\delta = z \oplus m = (101)_2 \oplus (110)_2 = (011)_2$. Now, the value of V_n is searched with respect to δ from standard array based on BLTM of size $A_{3\times3}$ in Table III. The stego-vector $v_s = v_c \oplus V_n = (111)_2 \oplus (010)_2 = (101)_2$. From v_s first LSB positions are replaced into R, G and B components respectively. Now stego RGB color components are Rs = 123 = $(01111011)_2$, Gs = 126 = $(01111110)_2$, and Bs = 135 = $(10000111)_2$.

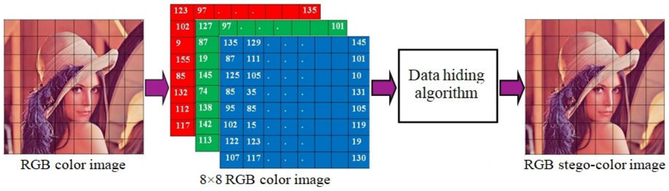

Fig. 3. Proposed data hiding process.

In Fig. 5 secret message embedding procedure has been elaborated. At first, an RGB color image is taken as an input cover image and further each pixel has been decomposed into red, green, and blue color channel. In the second step, selective LSBs are extracted from each color components, and append these as cover vectors, $v_c = [b_1\ \ b_2\ \ b_3]$. In the next step, secret bits are embedded into the cover image components by proposed BLTM method. The whole process will be repeated until all the secret bits are embedded into the cover image. The procedure is depicted in algorithm 1. Fig. 4 and Fig. 5 show the major stages of the secret image hiding procedure.

In the first step, the color stego-image has been given as an input, to extract secret bits from it and further decomposed it

Algorithm 1 Secret Message Embedding Procedure

```
Input : RGB color cover image and binary secret
        image/secret message bits streams.
Output: RGB color stego-image.
Read the RGB color cover image, $I$ with size of
$M \times N \times 3$ and decompose it into R, G, and B color
components respectively.
for $i = 1$ to $M$ do
    for $j = 1$ to $N$ do
        Select, $R = I(i, j, 1)$, $G = I(i, j, 2)$,
        $B = I(i, j, 3)$
        Extracted some selective LSB(s) from R, G, and
        B color components respectively
        Append LSBs of R, G, and B as: cover vector,
        $v_c = [b_1\ b_2\ \ldots\ b_k]$
        Find, $v = {v_c}^T$
        The BLTM is $A_{k \times k}$
        Now $z = (A_{k \times k} \times v)^T$
        Select k-bits of the secret message, $m$
        Compute, $\delta = z \oplus m$
        The value of $V_n$ is searched with respect to $\delta$
        from from standard array based on BLTM of size
        $A_{k \times k}$
        Compute, stego-vector, $v_s = v_c \oplus V_n$
        Modified R, G, and B components based on $v_s$
    end
end
Construct an RGB color stego-image
```

into RGB color stego components. In the next step, selected LSBs are extracted and then secret bits are extracted using BLTM and this process will continue untill the last bit is extracted. Algorithm 2 elaborates the whole process of secret bits extraction.

On the receiver side, Fig. 6 shows the overview of the secret message extraction method using the BLTM technique and Fig. 7, represents the diagram of the secret image extraction method example based using BLTM, $A_{3\times3}$.

Example 2: In the extraction process of secret message bits, from Example 1: stego RGB color components are Rs $= 123 = (01111011)_2$, Gs $= 126 = (01111110)_2$, and Bs $= 135 = (10000111)_2$. Now, extracted first LSB component from Rs, Gs, and Bs stego-color pixel forms the vector as: $v_s = [1\ 0\ 1]$ and find, $v_T = {v_s}^T$. Now, $m = (A_{3\times3} \times v_T)^T = (110)_2$. Finally, secret message bits, $m = (110)_2$

IV. Experimental Results

To conduct the experiments smoothly, $Intel^{\text{ő}}$ $Core^{TM}$ i-5, 10th Gen, processor with 8 GB RAM used with MATLAB 2018b software. We have shown the different experimental results to exhibit the efficacy and correctness of the proposed scheme. At the same time, this section also presents an elaborative discussion on the different findings of the proposed scheme on better security, visual quality, and embedding capability. Here, four commonly used color images by research community are considered as a cover image. Further a secret image, has been considered for different experiments. Later, Fig. 8(a) to 8(d) show the different cover images of size 512 × 512. Next, Fig. 8(e) demonstrates the secret image (i.e., Logo) used for different experiments. Here, all these demonstrated cover images are utilized along with the secret image to perform the proposed embedding scheme. In this

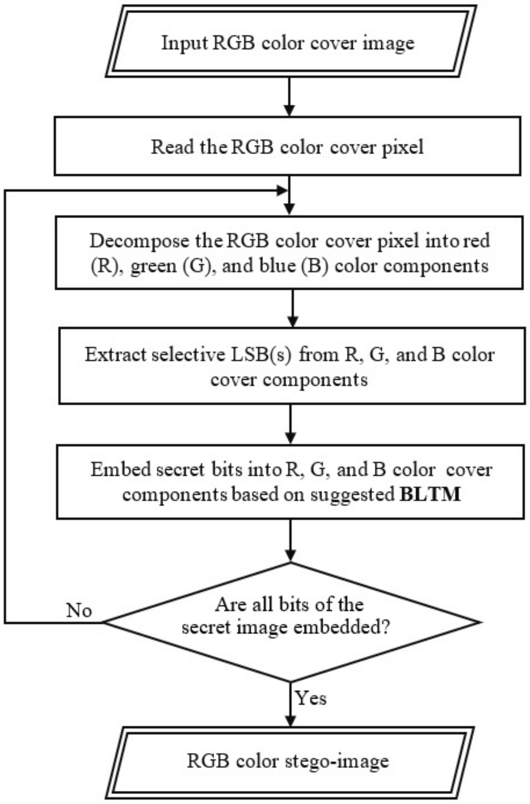
Input RGB color cover image
Read the RGB color cover pixel
Decompose the RGB color cover pixel into red (R), green (G), and blue (B) color components
Extract selective LSB(s) from R, G, and B color cover components
Embed secret bits into R, G, and B color cover components based on suggested **BLTM**
Are all bits of the secret image embedded?
No
Yes
RGB color stego-image

Fig. 4. The overview of the binary secret image embedding procedure.

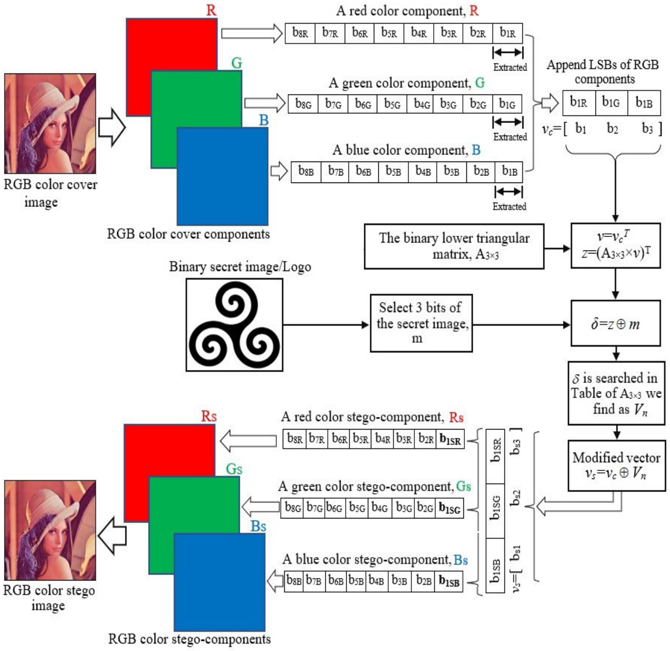
R
A red color component, R
b_{8R} b_{7R} b_{6R} b_{5R} b_{4R} b_{3R} b_{2R} b_{1R}
Extracted
G
A green color component, G
b_{8G} b_{7G} b_{6G} b_{5G} b_{4G} b_{3G} b_{2G} b_{1G}
Extracted
B
A blue color component, B
b_{8B} b_{7B} b_{6B} b_{5B} b_{4B} b_{3B} b_{2B} b_{1B}
Extracted
RGB color cover image
RGB color cover components
Append LSBs of RGB components
b_{1R} b_{1G} b_{1B}
v_c=[b_1 b_2 b_3]
The binary lower triangular matrix, $A_{3\times3}$
$v=v_c^T$
$z=(A_{3\times3}\times v)^T$
Binary secret image/Logo
Select 3 bits of the secret image, m
$\delta=z\oplus m$
δ is searched in Table of $A_{3\times3}$ we find as V_n
Modified vector $v_s=v_c\oplus V_n$
Rs
A red color stego-component, Rs
b_{8R} b_{7R} b_{6R} b_{5R} b_{4R} b_{3R} b_{2R} b_{1SR}
Gs
A green color stego-component, Gs
b_{8G} b_{7G} b_{6G} b_{5G} b_{4G} b_{3G} b_{2G} b_{1SG}
Bs
A blue color stego-component, Bs
b_{8B} b_{7B} b_{6B} b_{5B} b_{4B} b_{3B} b_{2B} b_{1SB}
b_{1SR} b_{1SG} b_{1SB}
v_s=[b_{s1} b_{s2} b_{s3}]
RGB color stego image
RGB color stego-components

Fig. 5. The major steps of the binary secret image embedding procedure.

Algorithm 2 Secret Message Extraction Procedure

```
Input  : RGB color stego-image
Output: The binary secret image/secret message bit streams
Read an RGB color stego-image, $I_s$ with size of $M \times N \times 3$ and decompose it into $R_s$, $G_s$, and $B_s$ color components respectively
for $i = 1$ to $M$ do
    for $j = 1$ to $N$ do
        Select, $R_s = I_s(i, j, 1)$, $G_s = I_s(i, j, 2)$, $B_s = I_s(i, j, 3)$
        Extracted, selective LSB(s) from $R_s$, $G_s$, and $B_s$
        Append LSBs of $R_s$, $G_s$, and $B_s$ as: $v_s = [b_{s1}\ b_{s2}\ \dots\ b_{sk}]$
        Find, $v_T = {v_s}^T$
        The BLTM is $A_{k \times k}$
        Now, $m = (A_{k \times k} \times v_T)^T$
        Finally, secret message bits are $m$
        end
    end
Construct the binary secret image/secret message bit streams
```

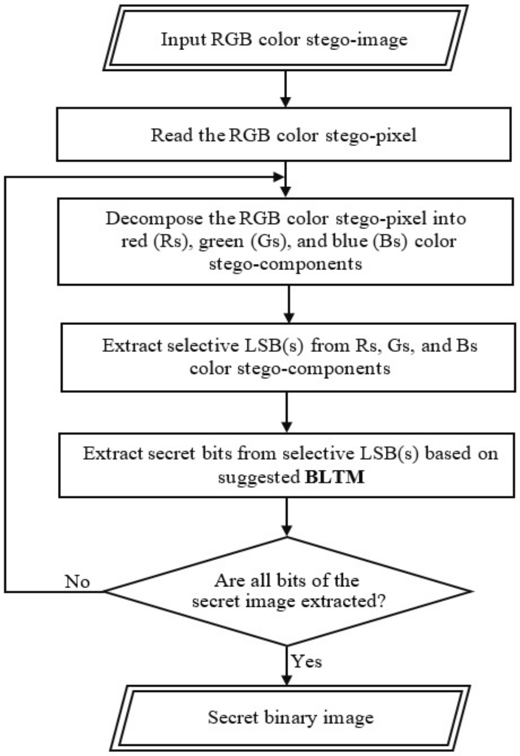
Input RGB color stego-image
Read the RGB color stego-pixel
Decompose the RGB color stego-pixel into red (Rs), green (Gs), and blue (Bs) color stego-components
Extract selective LSB(s) from Rs, Gs, and Bs color stego-components
Extract secret bits from selective LSB(s) based on suggested BLTM
Are all bits of the secret image extracted?
No
Yes
Secret binary image

Fig. 6. The overview of the binary secret image extraction procedure.

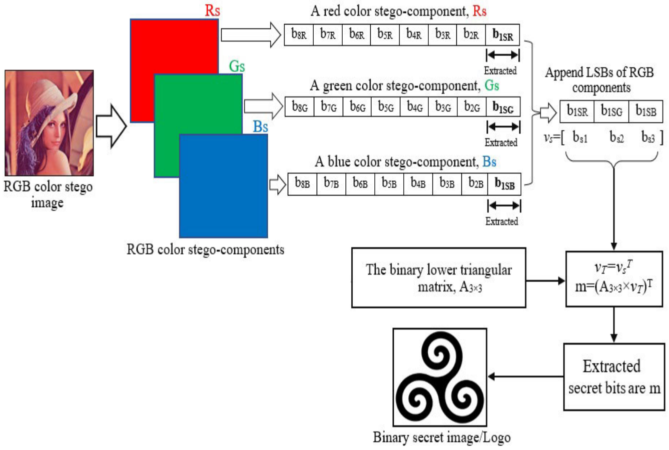
Rs
Gs
Bs
RGB color stego image
RGB color stego-components
A red color stego-component, Rs
b8R b7R b6R b5R b4R b3R b2R b1SR
Extracted
A green color stego-component, Gs
b8G b7G b6G b5G b4G b3G b2G b1SG
Extracted
A blue color stego-component, Bs
b8B b7B b6B b5B b4B b3B b2B b1SB
Extracted
Append LSBs of RGB components
b1SR b1SG b1SB
vs=[bs1 bs2 bs3]
The binary lower triangular matrix, A3×3
vT=vsT
m=(A3×3×vT)T
Extracted secret bits are m
Binary secret image/Logo

Fig. 7. The major steps of the binary secret image extraction procedure.

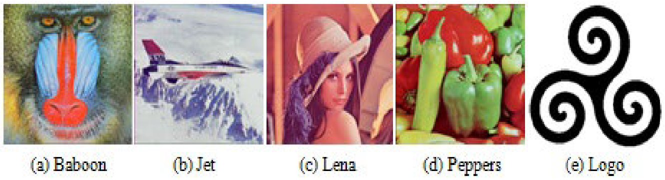
(a) Baboon (b) Jet (c) Lena (d) Peppers (e) Logo

Fig. 8. Original cover images used in the experiment.

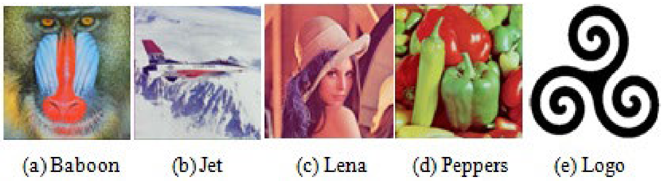
(a) Baboon (b) Jet (c) Lena (d) Peppers (e) Logo

Fig. 9. Stego-images and extracted Logo using $A_{2\times2}$.

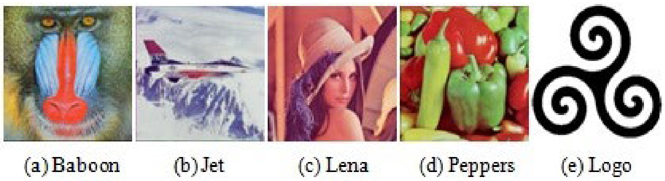
(a) Baboon (b) Jet (c) Lena (d) Peppers (e) Logo

Fig. 10. Stego-images and extracted Logo using $A_{3\times3}$.

paper, the BLTMs of size $A_{2\times2}$ are applied to the 1st positions LSBs of R and G color components, $A_{3\times3}$ is applied to the 1st positions LSBs of R, G, and B color components, and $A_{4\times4}$ is applied to the 1st-2nd-1st positions LSBs of R, G, and B color components respectively. Here, Fig. 9(a-d), Fig. 10(a-d) and Fig. 11(a-d) show the visual outcomes of the proposed scheme (BLTM of dimension $A_{2\times2}$, $A_{3\times3}$, $A_{4\times4}$) in the form of the stego-images. In these figures, it has been observed that the suggested embedding technique has generated decent quality of stego-images. All these stego-images are highly similar to the used original cover images based on human visual perception. Further, Fig. 9(e), Fig. 10(e) and Fig. 11(e) shows the extracted secret image (i.e., Logo). This extracted binary image also similar to the originally used secret binary image. The visual artifact of the stego-images are even significantly less, which can be revealed in Fig. 12. Here, a small cropped region of each stego-image is demonstrated in enlarged form for realizing the acceptability of the visual quality of the stego images.

Next, we have also performed various analysis to check the validation of the potency of the proposed scheme. Here, we have computed the three most widely used evaluation parameters which are image fidelity (IF), peak signal-to-noise ratio (PSNR), and structural similarity index (SSIM).

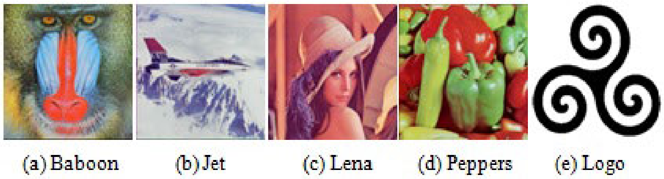

Fig. 11. Stego-images and extracted Logo using $A_{4\times4}$.

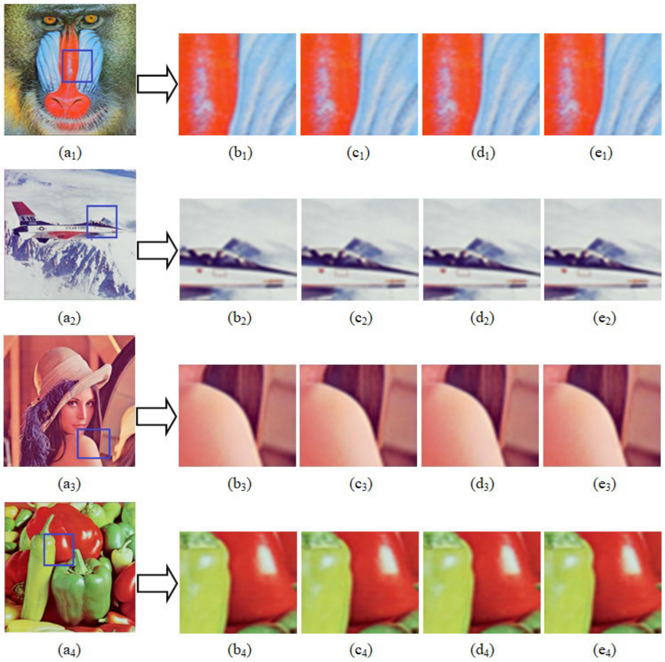

Fig. 12. Baboon, Jet, Lena, and Peppers images:- comparison of visual quality (a_1), (a_2), (a_3), and (a_4) are cover images, (b_1), (b_2), (b_3), and (b_4) are cropped images from the cover images, (c_1), (c_2), (c_3), and (c_4) are cropped images from stego-images using $A_{2\times2}$, (d_1), (d_2), (d_3), and (d_4) are cropped images from the stego-images using $A_{3\times3}$, and (e_1), (e_2), (e_3), and (e_4) are cropped images from the stego-images using $A_{4\times4}$.

TABLE V

Experimental Results in Term of Capacity and PSNR of Proposed Scheme

Images	Using $A_{2\times2}$		Using $A_{3\times3}$		Using $A_{4\times4}$	
	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR
Baboon	524288	52.8923	786432	51.1451	1048576	47.4388
Jet	524288	52.9042	786432	51.1425	1048576	47.4147
Lena	524288	52.9040	786432	51.1490	1048576	47.4480
Pepper	524288	52.9024	786432	51.1395	1048576	47.3707

Among these three parameters, a higher PSNR value shows the obtained stego-images visual quality. The IF value shows the level of accuracy through which the stego-image is produced. Next, the SSIM indicates the resemblance between the reference cover image with the generated stego-image. All these three discussed evaluation parameters are sufficient to establish the validity of the superior functioning of the proposed scheme. From Table V it can be analyzed that the PSNR value is more than 52 dB, when the BLTMs of size $A_{2\times2}$ is deployed on different cover images. PSNR value is more than 51 dB, when BLTMs of size $A_{3\times3}$ is deployed. For BLTMs of size $A_{4\times4}$, the PSNR value is more than 47 dB. Therefore, This proposed scheme ensures a very high PSNR value (which is more than 47 dB) in all cases.

TABLE VI

Experimental Results in Term of IF and SSIM Value of Stego -Images

Images	Using $A_{2\times2}$		Using $A_{3\times3}$		Using $A_{4\times4}$	
	IF	SSIM	IF	SSIM	IF	SSIM
Baboon	0.9987	0.9998	0.9980	0.9997	0.9954	0.9993
Jet	0.9987	0.9994	0.9980	0.9990	0.9977	0.9954
Lena	0.9987	0.9995	0.9980	0.9992	0.9954	0.9982
Pepper	0.9986	0.9993	0.9979	0.9989	0.9950	0.9969

TABLE VII

Experimental Results in Terms of SD of the Proposed Scheme in Stego-Images

Images	SDc of CI	Proposed by $A_{2\times2}$	Proposed by $A_{3\times3}$	Proposed by $A_{4\times4}$
		SDs of SI	SDs of SI	SDs of SI
Baboon	164.9810	164.9913	165.0028	165.0111
Jet	128.5547	128.5653	128.5779	128.5938
Lena	135.9845	135.9956	136.0019	136.0281
Pepper	164.5062	164.5074	164.5141	164.5364

To visualize indistinguishability between the original cover image and stego-image we can evaluate the results of Table VI, where we can find that for all the cover images and for different sizes of BLTM matrix produces IF and SSIM values more than 0.99, which is very high. Further, for more detailed quantitative analysis, we have also computed the standard deviation (SD) for all the cover images as well as for all the stego-images. To visualize the dissimilarity between the cover and the stego-image, the standard deviation is used. Generally, the lower difference values of SD represent the higher visual similarity between these two. Now, the standard deviation is demonstrated in Table VII. In Table VIII, we can see that the SD difference values for most of the cases are near to zero, which reflects the superior execution of the proposed approach in terms of visual quality.

Here, we have also computed the coefficient correlation (CC) values between all the cover and stego-images. Generally, the high CC values (i.e., near to 1) signifies that the generated stego-image possess very high visual quality. Table IX displays the CC values of all cover and stego images. It can be noticed that the CC values are very close to 1. Statistical values presented in Table IX signify the measure of accuracy, and efficiency of the proposed scheme. Some standard classifications for evaluation are computed to analyze the correctness of our scheme in terms of embedded and extracted secret bits. Various classification indicators, such as precession, recall, accuracy, F-measure, FPR, FNR, and NC, are computed.

TABLE VIII
EXPERIMENTAL RESULTS IN TERM OF DIFFERENCE SD OF THE PROPOSED SCHEME

Images	Proposed by $A_{2\times2}$	Proposed by $A_{3\times3}$	Proposed by $A_{4\times4}$
	Diff. of SDs & SDc	Diff. of SDs & SDc	Diff. of SDs & SDc
Baboon	0.0103	0.0218	0.0301
Jet	0.0106	0.0232	0.0391
Lena	0.0111	0.0174	0.0436
Pepper	0.0012	0.0079	0.0302

TABLE IX
EXPERIMENTAL RESULTS IN TERMS OF CORELATION COEFFICIENT OF THE PROPOSED SCHEME

Images	Proposed by $A_{2\times2}$	Proposed by $A_{3\times3}$	Proposed by $A_{4\times4}$
	CC	CC	CC
Baboon	0.9999	0.9999	0.9998
Jet	0.9999	0.9998	0.9997
Lena	0.9999	0.9999	0.9997
Pepper	0.9999	0.9999	0.9998

TABLE X
EXPERIMENTAL RESULTS IN TERMS OF CORRECTNESS OF EXTRACTED MESSAGE

Metrics	Proposed by $A_{3\times3}$			
	Baboon	Jet	Lena	Peppr
Precision	1	1	1	1
Recall	1	1	1	1
Accuracy	1	1	1	1
F-Measure	1	1	1	1
FPR	0	0	0	0
FNR	0	0	0	0
NC	1	1	1	1

The simulation results in Table X show the highest level of correctness of our proposed steganography technique. Further, it can be concluded that our proposed scheme is efficient and superior to various contemporary schemes as demonstrated in Table XI, and XII. Both Table XI and Table XII display a comparative analysis of the proposed technique with other proposed methods by Yang and Wang [10], M. Kalita et al. [3], Banerjee and Jana [9], and P. Chowdhuri et al. [13]. From these analyses, it can be inferred that the proposed technique produces superior results compared to other approaches. In the context of embedding capacity, our method is capable of hiding a significant amount of secret data. At the same time, it has been observed that the PSNR values of the stego images are more than 47 dB in most of the cases. Hence, it can be concluded that our proposed method is having superior performance than the contemporary schemes as demonstrated in Table XI and Table XII.

TABLE XI
COMPARISON RESULTS IN TERMS OF CAPACITY (BITS) VALUES

Scheme Name	Baboon	Jet	Lena	Peppers
	Capacity	Capacity	Capacity	Capacity
Yang & Wang [10]	196608	196608	196608	196608
M. Kilita et al. [3]	800849	789053	795082	789053
Banerjee & Jana [9]	786432	786432	786432	786432
P. Chowdhuri et al. [13]	179457	176541	180942	179657
Proposed by $A_{2\times2}$	524288	524288	524288	524288
Proposed by $A_{3\times3}$	786432	786432	786432	786432
Proposed by $A_{4\times4}$	1048576	1048576	1048576	1048576

TABLE XII
COMPARISON RESULTS IN TERMS OF PSNR

Scheme Name	Baboon	Jet	Lena	Peppers
	PSNR	PSNR	PSNR	PSNR
Yang & Wang [10]	33.29	43.73	41.58	39.43
M. Kilita et al. [3]	40.03	41.62	40.94	40.36
Banerjee & Jana [9]	44.05	45.28	44.04	44.01
P. Chowdhuri et al. [13]	41.23	41.12	42.12	40.12
Proposed by $A_{2\times2}$	52.89	52.90	52.90	52.90
Proposed by $A_{3\times3}$	51.15	51.14	51.15	51.14
Proposed by $A_{4\times4}$	47.44	47.41	47.45	47.37

In this proposed work, we have embedded data in the pixel level of the cover image. In our proposed scheme, the value of z is computed with the aid of the BLTM matrix which is significantly small in size. Therefore, the overall computation cost will be a constant amount of time. Next, searching of v_n will be done on constant time since it is working on a small size of the matrix. Therefore, the computational complexity will be constant for this particular steps. Due to the nested loop in the algorithm to select all R, G, and B color components the complexity will be $O(n^2)$. Thus, the overall complexity will be $O(n^2)$.

V. CONCLUSION

A novel and efficient data hiding scheme based on the binary lower triangular matrix for the color images has been devised in this paper. The proposed scheme is motivated to embed a higher payload into the cover image. However, the limitation of any steganography scheme is, embedding more bits per pixel may cause the quality deterioration of the stego-image drastically. Hence, there is a scope to improve the embedding capacity of the proposed scheme by using suitable error correction mechanisms. Further our work is based on a matrix-based data hiding scheme, researchers may think about a cryptography key-based secret-bit embedding matrix. Again, this data-hiding mechanism can be explored and applied in the field of active forgery. The RGB-based data hiding scheme conceals secret data directly into the color pixels without significant visual quality degradation. The scheme is also appropriate to extract the original content successfully. The scheme exhibits satisfactory results in terms of PSNR as well as payload. Along with that, our proposed technique is impactful in holding the superior visual quality of the stego-image. The technique is simple and novel in terms of embedding procedure. The simulation results and numerical outcomes represented in various tables establish the superiority and validity of the proposed scheme.

References

[1] S. William, *Cryptography and Network Security: Principles and Practices*, 4th ed. London, U.K.: Pearson Education India, 2007.

[2] C.-S. Lu, *Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property*. Taiwan: Idea Group Publishing, 2005.

[3] M. Kalita, T. Tuithung, and S. Majumder, “An adaptive color image steganography method using adjacent pixel value differencing and LSB substitution technique,” *Cryptologia*, vol. 43, no. 5, pp. 414–437, Sep. 2019.

[4] C.-K. Chan and L. M. Cheng, “Hiding data in images by simple LSB substitution,” *Pattern Recognit.*, vol. 37, no. 3, pp. 469–474, Mar. 2004.

[5] T.-C. Lu, “Interpolation-based hiding scheme using the modulus function and re-encoding strategy,” *Signal Process.*, vol. 142, pp. 244–259, Jan. 2018.

[6] J. Fridrich and D. Soukal, “Matrix embedding for large payloads,” *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 3, pp. 390–395, Sep. 2006.

[7] Q. Mao, “A fast algorithm for matrix embedding steganography,” *Digit. Signal Process.*, vol. 25, pp. 3036–3048, Feb. 2014.

[8] X. Li, S. Cai, W. Zhang, and B. Yang, “A further study of large payloads matrix embedding,” *Inf. Sci.*, vol. 324, pp. 257–269, Dec. 2015.

[9] A. Banerjee and B. Jana, “Improving data hiding capacity using bit-plane slicing of color image through (7,4) Hamming code,” in *Information Systems Design and Intelligent Applications*, vol. 672. Singapore: Springer, 2018, pp. 356–367.

[10] C.-Y. Yang and W.-F. Wang, “Block-based colour image steganography using smart pixel-adjustment,” in *Genetic and Evolutionary Computing* (Advances in Intelligent Systems and Computing), vol. 329. Cham, Switzerland: Springer, 2015, pp. 145–154.

[11] X. Qin, B. Li, S. Tan, and J. Zeng, “A novel steganography for spatial color images based on pixel vector cost,” *IEEE Access*, vol. 7, pp. 8834–8846, 2019.

[12] B. E. Carvajal-Gamez, F. J. Gallegos-Funes, and A. J. Rosales-Silva, “Color local complexity estimation based steganographic (CLCES) method,” *Exp. Syst. Appl.*, vol. 40, no. 4, pp. 1132–1142, Mar. 2013.

[13] P. Chowdhuri, B. Jana, and D. Giri, “Secured steganographic scheme for highly compressed color image using weighted matrix through DCT,” *Int. J. Comput. Appl.*, vol. 43, no. 1, pp. 1–12, 2018.

[14] V. Sabeti, M. Sobhani, and S. M. H. Hasheminejad, “An adaptive image steganography method based on integer wavelet transform using genetic algorithm,” *Comput. Electr. Eng.*, vol. 99, Apr. 2022, Art. no. 107809.

[15] R. Biswas and S. K. Bandyapadhay, “Random selection based GA optimization in 2D-DCT domain color image steganography,” *Multimedia Tools Appl.*, vol. 79, nos. 11–12, pp. 7101–7120, Mar. 2020.

[16] K.-S. Hsieh and C.-M. Wang, “Constructive image steganography using example-based weighted color transfer,” *J. Inf. Secur. Appl.*, vol. 65, Mar. 2022, Art. no. 103126.

[17] L. Zhu, X. Luo, Y. Zhang, C. Yang, and F. Liu, “Inverse interpolation and its application in robust image steganography,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 32, no. 6, pp. 4052–4064, Jun. 2022.

[18] M. Liu, W. Luo, P. Zheng, and J. Huang, “A new adversarial embedding method for enhancing image steganography,” *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 4621–4634, 2021.

[19] W. Lu, J. Zhang, X. Zhao, W. Zhang, and J. Huang, “Secure robust JPEG steganography based on AutoEncoder with adaptive BCH encoding,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 31, no. 7, pp. 2909–2922, Jul. 2021.

[20] H. M. Pandey, “Secure medical data transmission using a fusion of bit mask oriented genetic algorithm, encryption and steganography,” *Future Gener. Comput. Syst.*, vol. 111, pp. 213–225, Oct. 2020.

[21] D. Shah, T. Shah, Y. Naseer, S. S. Jamal, and S. Hussain, “Cryptographically strong S-P boxes and their application in steganography,” *J. Inf. Secur. Appl.*, vol. 67, Jun. 2022, Art. no. 103174.

[22] K. S. Rekha, M. J. Amali, M. Swathy, M. Raghini, and B. P. Darshini, “A steganography embedding method based on CDF-DWT technique for data hiding application using Elgamal algorithm,” *Biomed. Signal Process. Control*, vol. 80, Feb. 2023, Art. no. 104212.

Shiv Prasad received the M.C.A. degree from the Kamla Nehru Institute of Technology (KNIT), Sultanpur, India, and the Ph.D. degree from the Department of Computer Science and Engineering, Indian Institute of Technology (Indian School of Mines) Dhanbad, India. He has contributed a number of research papers in several SCI/SCIE and Scopus indexed journals and conference proceedings of international reputes. His main research interests include steganography, watermarking, copy-move forgery detection in digital images, and multimedia security.

Arup Kumar Pal received the B.Tech. degree in computer science and engineering from the Government College of Engineering and Textile Technology, Berhampore, India, in 2006, and the Ph.D. degree in computer science and engineering from the Indian Institute of Technology (ISM) Dhanbad, India, in 2011. He is currently working as an Associate Professor with the Department of Computer Science and Engineering, IIT (ISM) Dhanbad. Before joining this institute, he was a Lecturer with the Department of Computer Science and Engineering, NIT Jamshedpur, from April 2011 to December 2011. He has more than ten years of teaching and research experience. He has contributed over 100 research papers in several journals and conference proceedings of national and international reputes. His main research interests include data compression, multimedia security, and CBIR. He has organized several FDPs in the areas of image processing and cryptography. He has served as an advisor committee member and technical programme committee (TPC) member in various conferences/workshops.

Soumya Mukherjee received the B.Tech. degree in CSE and the M.Tech. degree in computer systems and technology from the West Bengal University of Technology, India. He is currently pursuing the Ph.D. degree with the Department of CSE, Indian Institute of Technology (Indian School of Mines) Dhanbad, India. He is currently working as an Assistant Professor with the Department of CSE (Data Science), Haldia Institute of Technology, Haldia, India. His research interests include steganography, watermarking, and copy-move forgery detection in digital images.