© FEB 2026 | IRE Journals | Volume 9 Issue 8 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I8-1714741

Binary Lower Triangular Matrix based Secure Text Embedding in RGB Images

DR. M. POMPAPATHI[1], K. RAVIKIRAN[2], D. SIVARAM[3], L. PRAVEEN[4], K. PARASURAM[5]
[1]*Associate Professor, Department of IT, R.V.R & J.C.C.E Guntur, India*
[2,3,4,5] *Final year Students, Department of IT, R.V.R & J.C.C.E Guntur, India*

Abstract*—Text steganography is an efficient method of hidden communication, where the secret text message is embedded into digital images. In this paper, a new method of embedding a text message into an RGB image using a Binary Lower Triangular Matrix (BLTM) is proposed. In the proposed method, the encrypted text bits are embedded into the least significant bits of the RGB components of the image using matrix-based XOR operations. The proposed method improves the security of text embedding while maintaining the image quality. A graphical user interface has been developed using Python.

***Keywords* — Text Steganography, RGB Image, BLTM, LSB Substitution, Secure Data Hiding**

I. INTRODUCTION

Steganography is the art and science of hiding information within digital media so that the existence of the hidden message goes unnoticed. Unlike cryptography, which protects the content of communication by making it unreadable, steganography conceals the very presence of the communication. This reduces suspicion from unintended observers [1]. With the rapid growth of online communication and multimedia data exchange, the secure and discreet transmission of sensitive information has become more important. As a result, digital steganography has emerged as a key research area in information security [2]. Digital images are commonly used as cover media for steganographic systems because they have high redundancy, large data capacity, and can tolerate minor alterations without causing obvious visual distortion [3]. Among spatial-domain techniques, the Least Significant Bit (LSB) substitution method is one of the simplest and most widely used for hiding text inside images [4]. In this method, the least significant bits of pixel values are replaced with bits from the secret message. Although LSB substitution offers high embedding capacity and low computational complexity, it is very vulnerable to statistical detection attacks, since predictable changes alter the natural distribution of pixel values [5]. To enhance security and reduce the likelihood of detection, matrix encoding techniques were introduced. Crandall first suggested the idea of matrix-based embedding, which minimizes the number of pixel changes needed to hide secret data [6]. Matrix encoding is closely tied to coding theory, where structured mathematical transformations are used to improve data representation and error correction [7]. By reducing the number of altered bits, matrix encoding greatly improves imperceptibility and resistance against statistical detection methods. Further advancements in embedding efficiency via matrix encoding were investigated by Hussain et al. [8], who showed that structured embedding strategies can achieve a higher payload capacity with fewer pixel changes compared to the traditional LSB substitution. Meanwhile, various steganalysis methods have been developed to detect hidden information. Fridrich et al. [10] suggested detection techniques for LSB steganography in both grayscale and color images, while Pevný et al. [11] introduced advanced statistical models like the Subtractive Pixel Adjacency Matrix (SPAM) to improve detection accuracy. These studies underline the need for more secure embedding schemes that maintain the statistical characteristics of cover images. Extensive surveys by Cheddad et al. [12] stress that modern steganographic systems must balance three key factors: embedding capacity, imperceptibility, and robustness. High-capacity embedding methods, such as wavelet-based techniques, have also been proposed to increase payload size while preserving image quality [9]. However, many existing methods either face increased computational complexity or remain open to advanced steganalysis techniques. To tackle these challenges, this paper presents a secure text-in-image steganography technique based on a Binary Lower Triangular Matrix (BLTM) structure. Based on matrix encoding principles [6], [8] and coding theory foundations [7], the proposed method transforms the least significant bits of RGB channels using a structured lower triangular binary matrix. By spreading embedding operations across the Red,

Green, and Blue channels in a coordinated way, the technique minimizes pixel changes and boosts resistance to statistical detection methods such as those discussed in [10] and [11]. The goal of this approach is to achieve high embedding efficiency while maintaining visual quality, ensuring that the stego image closely resembles the original cover image. Through structured matrix-guided embedding, the method offers a secure and dependable solution for hiding textual information inside digital images.

II. RELATED WORK

Early research in image steganography predominantly focused on spatial-domain embedding, where secret information is directly inserted into the pixel values of a cover image. The most commonly used technique is the Least Significant Bit (LSB) substitution method, where the embedding process can be mathematically expressed as:

$$I_s(x,y) = I_c(x,y) - (I_c(x,y) mod 2) + b_k$$

where $I_c(x,y)$is the original pixel value, $b_k \in \{0,1\}$represents the secret message bit, and $I_s(x,y)$denotes the stego-pixel. Despite its simplicity and high data payload, this method introduces fixed statistical artifacts that make it vulnerable to steganalysis.

To improve invisibility, researchers introduced adaptive spatial-domain methods, among which the Pixel Value Differencing (PVD) approach became prominent. In PVD, the difference between two adjacent pixels is calculated as:

$$d = | I(x_1, y_1) - I(x_2, y_2) |$$

Based on the value of d, the embedding capacity n(number of bits that can be hidden) is determined using:

$$n = \lfloor \log_2(d) \rfloor$$

This adaptive rule ensures that regions with larger intensity variations can carry more secret bits, improving perceptual transparency.

LSB substitution provides an easy and efficient method for hiding secret data in digital images, but it can cause noticeable image distortion when more bits are embedded. The introduction of the Optimal Pixel Adjustment Process (OPAP) effectively addresses this limitation by minimizing embedding errors while preserving the hidden information. By intelligently adjusting pixel values after embedding, OPAP significantly reduces mean square error and improves visual quality compared to basic LSB substitution.

To enhance security, researchers introduced matrix-based embedding techniques that control how secret bits are distributed inside image pixels. Instead of directly replacing LSBs, these methods use mathematical structures to determine the minimum number of bit changes required to embed the message. This significantly reduces visible distortion and helps preserve the natural statistical properties of the cover image.

A recent advancement in this area is the use of Binary Lower Triangular Matrix (BLTM) based embedding. In this approach, the least significant bits from the Red, Green, and Blue (RGB) channels of a color pixel are grouped together and processed through a lower triangular binary matrix. The matrix guides how the secret bits are mapped and embedded, allowing more data to be hidden with fewer pixel modifications. This improves both imperceptibility and resistance against common steganalysis attacks.

Unlike earlier methods that mainly targeted small text messages, BLTM-based techniques are designed to hide larger payloads such as full RGB images. The method efficiently embeds secret image data by transforming the message bits and aligning them with structured matrix positions. As a result, it achieves better security, reduced distortion, and improved robustness compared to classical LSB and basic matrix encoding techniques.

III. PROPOSED METHODOLOGY

A. Binary Lower Triangular Matrix (BLTM)

The Binary Lower Triangular Matrix (BLTM) is a structured mathematical model widely used to improve efficiency and security in matrix-based data embedding techniques. A lower triangular matrix is a square matrix in which all elements above the main diagonal are equal to zero, while elements on and below the diagonal may contain non-zero values

A BLTM is a square matrix where all elements above the diagonal are zero and all elements on and below the diagonal are ones.
For a 3×3 BLTM:

© FEB 2026 | IRE Journals | Volume 9 Issue 8 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I8-1714741

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

This matrix is used to transform the LSBs of RGB pixels before embedding text bits.

B. Mapping Table :

Table-1

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

Table-2

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-3

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
0110	C_2=[0011]	0011
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
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

C. Algorithms

Text Embedding Algorithm

Input: Cover Image, Secret Text

Output: Stego Image

Steps:

1. Read the secret text.
2. Convert each character into ASCII.
3. Convert ASCII values into a binary stream.
4. Read the cover image in RGB format.
5. Generate a BLTM matrix of size $k \times k$.
6. For each pixel:
   - Extract LSBs from R, G, B → cover_vector
   - Compute z = BLTM × cover_vector (mod 2)
   - Take next k bits from secret text stream → m
   - Compute delta = z XOR m
   - Encode delta using mapping table
   - Replace LSBs with new stego bits
7. Save the stego image.

Text Extraction Algorithm

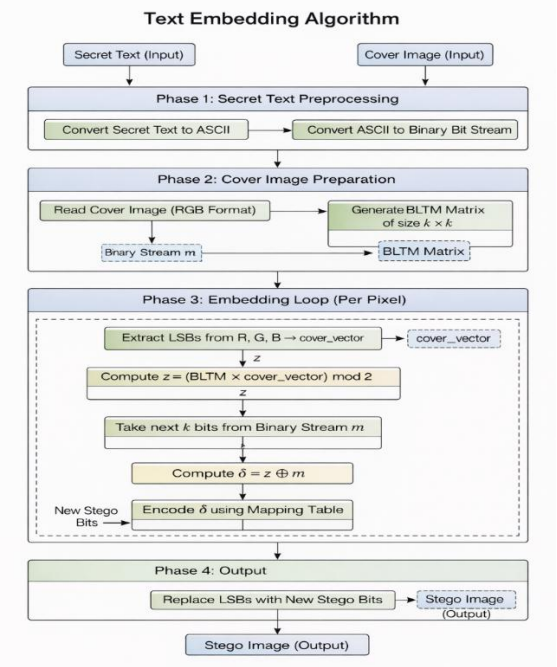
Input: Stego Image

Output: Recovered Text

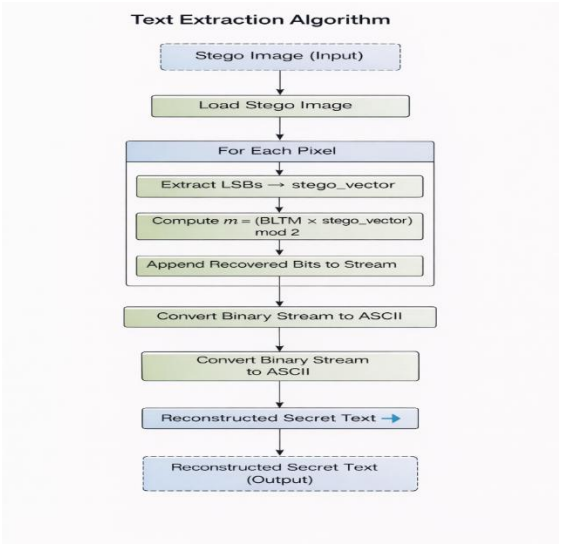
Steps:

1. Load stego image.
2. For each pixel:
   - Extract LSBs → stego_vector
   - Compute m = BLTM × stego_vector (mod 2)
   - Append recovered bits to stream.
3. Convert binary to ASCII.
4. Reconstruct secret text.

D. Flow Charts:



© FEB 2026 | IRE Journals | Volume 9 Issue 8 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I8-1714741



IV. IMPLEMENTATION

The algorithm is implemented in Python using:

- Tkinter for the graphical interface
- Pillow (PIL) for image manipulation
- NumPy for matrix and binary operations

The GUI provides simple controls to encode and decode images.

V. EXPERIMENTAL RESULTS

1. Mean Squared Error(MSE)

Mean Squared Error (MSE) is a commonly used metric for evaluating the difference between an original image and its distorted or reconstructed counterpart. It measures the average of the squared differences between corresponding pixel values in the two images, providing a numerical indication of the amount of distortion introduced.

- If the original and reconstructed images are identical, the MSE value becomes zero.
- Higher MSE values indicate a larger difference between the two images.
- Since the errors are squared, larger deviations are penalized more heavily than smaller ones.

Although MSE provides a straightforward quantitative measure of distortion, it does not always perfectly reflect human visual perception of image quality.

For two images I(original) and K(stego), each of size $m \times n$, the MSE is defined as follows:

$$\text{MSE} = \frac{1}{mn} \sum_{i=1}^{m} \sum_{j=1}^{n} [I(i,j) - K(i,j)]^2$$

2. Peak Signal-to-Noise Ratio (PSNR)

Peak Signal-to-Noise Ratio (PSNR) is a widely used image quality metric derived from the Mean Squared Error (MSE). It represents the ratio between the maximum possible signal power (i.e., the highest possible pixel value in an image) and the noise introduced due to distortion. PSNR is expressed in decibels (dB), which provides a logarithmic representation of image quality.

- A higher PSNR value indicates better image quality and lower distortion.
- A lower PSNR value suggests increased noise and greater differences from the original image.
- PSNR is commonly used in image and video compression, transmission, and reconstruction applications because its logarithmic scale makes quality comparisons easier to interpret than raw MSE values.

Typical PSNR ranges are interpreted as follows:
40 dB and above → Excellent image quality
30–40 dB → Good quality
20–30 dB → Moderate distortion
Below 20 dB → Significant or heavy distortion
The PSNR is calculated using the following formula:

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

Where:

- MAX_I is the maximum possible pixel value of the image.
- For 8-bit images: $MAX_I = 255$

3.IF (Image Fidelity)

The IF (Image Fidelity) metric measures the similarity between the cover image and the stego image. A higher IF value indicates less distortion and better imperceptibility.
Mathematical Formula
Given:
$C(i,j)$: pixel values of the cover image
$S(i,j)$: pixel values of the stego image
Image size $M \times N$
Image Fidelity (IF):

$$\text{IF} = 1 - \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} (C(i,j) - S(i,j))^2}{\sum_{i=1}^{M} \sum_{j=1}^{N} C(i,j)^2}$$

© FEB 2026 | IRE Journals | Volume 9 Issue 8 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I8-1714741

Interpretation of IF Values

≈ 1.0	Excellent image quality
0.9 – 0.99	Very good imperceptibility
< 0.8	Noticeable distortion

Fig-1 Images that are used in this Experiment (original Images):

Secret data that used in this experiment:

Hidden archives whisper stories nobody can fully prove.
Encrypted files sit quietly, waiting for the right key.
Some secrets are simply forgotten facts lost in time.
Others are puzzles made from patterns people overlook.
The real mystery is how curiosity keeps searching anyway.
Sometimes the most powerful secret is imagination itself.

Fig-2 Images after Embed secret data(Stego-Images

Table – 4
Experimental Results in terms of MSE

Images	A 2×2	A 3×3	A 4×4
	MSE	MSE	MSE
C1	0.05680	0.05683	0.05683
C2	0.04985	0.04995	0.04999
C3	0.05880	0.05903	0.05915
C4	0.05083	0.05090	0.05099
C5	0.00972	0.00984	0.00991

Table – 5
Experimental results in terms of PSNR

Images	A 2×2	A 3×3	A 4×4
	PSNR	PSNR	PSNR
C1	60.58	60.58	60.23
C2	61.19	61.15	61.02
C3	60.45	60.42	60.33
C4	61.12	61.06	60.89
C5	68.28	68.20	68.11

Table – 6
Experimental results in terms of IF

Images	A 2×2	A 3×3	A 4×4
	IF	IF	IF
C1	0.995	0.995	0.994
C2	0.996	0.996	0.994
C3	0.996	0.995	0.995
C4	0.995	0.995	0.993
C5	0.9999	0.9999	0.9998

The effectiveness of the proposed steganographic technique is evaluated using standard image quality metrics, including Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Image Fidelity (IF). Experiments are performed on multiple RGB cover images of size $M \times N$, as illustrated in Fig. 1.

Initially, five original cover images (C1–C5), along with their pixel dimensions, are used as host images (Fig. 1). Secret data is embedded into each cover image using the proposed Binary Lower Triangular Matrix approach with different matrix sizes, namely $A_{2\times2}$, $A_{3\times3}$, and $A_{4\times4}$. The resulting stego images are shown in Fig. 3. It can be observed that the visual quality of the stego images remains almost identical to that of the original cover images, indicating a high level of imperceptibility in the embedding process.

Quantitative Analysis Using MSE and PSNR

The numerical evaluation of distortion is summarized in Table-4 and Table-5, which report MSE and PSNR values, respectively, for different test images and matrix sizes.

The results indicate that:

The MSE values are very low, demonstrating minimal pixel-level distortion between the cover and stego images.

The PSNR values remain consistently high (above 55 dB in most cases), confirming excellent reconstruction quality.

As the matrix size increases from $A_{2\times2}$to $A_{4\times4}$, PSNR values show only marginal variation, highlighting the stability of the proposed method.

Overall, these findings confirm that the embedding process introduces negligible noise into the cover images.

Image Fidelity (IF) Analysis

To further validate visual similarity, Image Fidelity (IF) is calculated by measuring the relationship between the cover and stego images. The IF values obtained for different images and matrix sizes are presented in Table-6. The results show that:

All IF values are very close to 1, ranging approximately from 0.995 to 0.999.

Such high IF values indicate excellent fidelity, meaning that the stego images preserve the structural and visual characteristics of the original cover images.

The consistency of IF values across different images and matrix sizes demonstrates the robustness and reliability of the proposed approach.

VI. CONCLUSION

This study introduces a successful image steganography technique for securely hiding confidential data within a cover image without compromising its visual quality. The method effectively balances embedding capacity, invisibility, and resistance to attacks, ensuring that the concealed data is not visible to the human eye. Experimental results show that the modified image maintains a quality similar to the original, with slight changes and accurate data retrieval. Performance tests using common metrics verify the method's reliability and effectiveness on various images. In summary, the approach offers a straightforward, secure, and practical way for transmitting sensitive information and enabling secure image-based communication.

REFERENCES

[1] N. Provos and P. Honeyman, “Hide and Seek: An Introduction to Steganography,” IEEE Security & Privacy, vol. 1, no. 3, pp. 32–44, May–Jun. 2003.

[2] J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge, U.K.: Cambridge University Press, 2009.

[3] R. Chandramouli and N. Memon, “Analysis of LSB Based Image Steganography Techniques,” in Proc. IEEE International Conference on Image Processing (ICIP), 2001, pp. 1019–1022.

[4] C. K. Chan and L. M. Cheng, “Hiding Data in Images by Simple LSB Substitution,” Pattern Recognition, vol. 37, no. 3, pp. 469–474, 2004.

[5] A. Westfeld and A. Pfitzmann, “Attacks on Steganographic Systems,” in Proc. 3rd International Workshop on Information Hiding, 1999, pp. 61–76.

[6] R. Crandall, “Some Notes on Steganography,” Steganography Mailing List, 1998.

[7] J. Bierbrauer, Introduction to Coding Theory. Boca Raton, FL, USA: Chapman & Hall/CRC, 2004.

[8] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. S. Ho, and K. H. Jung, “Improving Embedding Efficiency of LSB Steganography Using Matrix Encoding,” International Journal of Computer Science and Network Security, vol. 10, no. 7, pp. 219–224, 2010.

[9] K. A. Navas, A. Mathews, M. Lekshmi, and T. S. Sathidevi, “High Capacity Image Steganography Using Wavelet Transform,” in Proc. IEEE International Conference on Signal Processing, 2007.

[10] J. Fridrich, M. Goljan, and D. Soukal, “Detecting LSB Steganography in Color and Grayscale Images,” IEEE Multimedia, vol. 8, no. 4, pp. 22–28, Oct.–Dec. 2001.

[11] T. Pevný, P. Bas, and J. Fridrich, “Steganalysis by Subtractive Pixel Adjacency Matrix,” IEEE Transactions on Information Forensics and Security, vol. 5, no. 2, pp. 215–224, Jun. 2010.

[12] S. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, “Digital Image Steganography: Survey and Analysis of Current Methods,” Signal Processing, vol. 90, no. 3, pp. 727–752, 2010.

[13] M. Bashardoost and M. Rahimi, “A High-Capacity Image Steganography Method Based on Matrix Encoding,” Journal of Information Security and Applications, vol. 24, pp. 1–10, 2015.