# An Innovative Crypto-Stego Technique for Secure and Privacy-Preserving on Reliable Transmission Data

Harikrishna Bommala[*,†], Seelam Sai Satyanarayana Reddy[†]

*KG Reddy College of Engineering & Technology, Moinabad, Hyderabad, Telangana, India.*

## Abstract

In this day's data communication became too much risk factor that there are so many third-party persons are getting an unauthorized access to get the details of the communication, which will affect the security and privacy. Even though we are applying so many data security techniques and privacy techniques simultaneously the unauthorized access mechanism's also developing so secure and privacy communication became more concern and to achieve that previously vernal cipher method, it had a disadvantage that depending on number of input characters that much number of keys are need to generate. To overcome this method and to achieve the secure and privacy preserving communication without getting any unauthorized access that may lead to modification of data so we are proposed technique that provides modern methods inclusive of modified Zig-Zag, modified rail fence, crossover and XOR operations without key similarly, statistics is embedded in picture with none deformation the parameter evaluation along with MSC and PSNR displaying higher outcomes than existing algorithm. In the proposed work an efficient LSB primarily based photo steganography is provided. The proposed technique ensures there's no fundamental adjustments are done where secret message is embedded into cover adjustments.

## Keywords

Data security, zig-Zag, RailFence, cryptography, data transmission, stegnography

## 1. Introduction

To prevent unauthorized parties from deciphering private communications, cryptography involves the construction and analysis of secret procedures [1]. Steganography refers to the process of secretly transmitting data by embedding it in another file, message, picture, or video. The expanding capabilities of modern communications call for a fresh approach to security, particularly in the realm of wireless laptop networks [2]. Network protection is turning into extra crucial as the amount of information being exchanged on the net is increasing safety necessities are necessary both at the very last consumer level and at the organization degree, mainly because of the massive utilization of non-public computer systems, networks, and the internet with its worldwide availability [3]. Historically, people have prioritized the following computational security features: privacy, identity, verification, no-repudiation, integrity, and availability [4]. As a consequence, the industry of secret document storage has developed

*ACI'23: Workshop on Advances in Computational Intelligence at ICAIDS 2023, December 29-30, 2023, Hyderabad, India*

[*] Corresponding author.

[†] These authors contributed equally.

haribommala@gmail.com (H. Bommala); saisn90@gmail.com (S. S. S. Reddy)
0000-0002-9932-6152 (H. Bommala); 0000-0002-2985-3555 (S. S. S. Reddy)

dramatically. A new approach to information concealment is also necessary because of the rapid growth of the publishing and broadcasting generation.

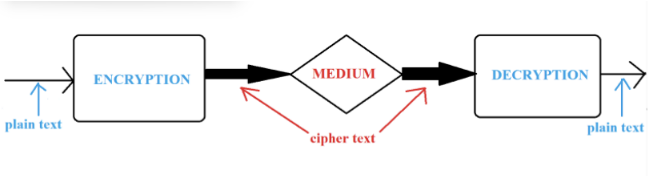


**Figure 1:** Basic flow diagram of cryptography technique

Unauthorized duplication of music, video, and other material that is only available in digital form raises concerns about copyright protection [5]. The music, film, book, and software publishing businesses are particularly hard hit by the nuisance of unlawful copying. To get around this problem, assessment remarks might be sent to the output record using hidden data buried in the digital medium [6] no longer be easily removed unless a unique technique is used [7]. Data security may be achieved in several ways [8] one is cryptography as shown in fig 1. The sender uses an encryption key [9] to scramble the message, the scrambled message is broadcast via an unsecured public channel, and the unique, unencrypted message can be reconstructed only if the recipient has the appropriate decryption key. The second method is called steganography, and it involves concealing a message inside another message such that its very existence is concealed [10]. They adapt rapidly to varying levels of illumination in photos of everyday scenes when it comes to size and variety, LPs just can't be mistaken for anything else in a photograph [11]. Few machine learning methods are proposed to detect network attacks [12, 13].

## 2. Related Work

Data security, confidentiality, information integrity, authentication, and non-repudiation are all relevant to modern cryptography, which is the practice and study of techniques for secure communication in the face of adversarial behavior [14] Present-day cryptography lies at the crossroads of the fields of mathematics, computer technology, electrical engineering, communication technology, and physics [15] packages of cryptography contain digital commerce, chip-primarily based charge playing cards, virtual currencies, computer passwords, and military communications [16] In times past, cryptography was almost identical with encryption, the process by which data is transformed from a legible country into incomprehensible gibberish [17] to prevent unauthorized parties from reading encrypted messages, the sender only provides the decryption method to the intended recipients. Alice (”A”) is the sender, Bob (”B”) is the intended receiver, and Eve (”eavesdropper”) is the adversary, in the cryptography literature [18]. The emergence of computers during World War II and the usage of rotor cipher machines during World War I have both contributed to the complexity and breadth of cryptographic techniques [19] as of late, cryptography has relied heavily on mathematical concepts and computer technology exercises to develop cryptographic algorithms that are very difficult for any opponent to crack in reality [**?** ] While it may be conceivable to disrupt a well-designed system in theory, doing so in reality is very unlikely to succeed. This kind of system is called ”computationally cozy” if it is well-designed; nevertheless, theoretical developments (such as improvements in integer factorization techniques) and faster computer technology need that such designs be constantly reevaluated and, if necessary, updated. The only-time pad and other statistically secure but computationally insecure systems are far more difficult to employ in reality than the best theoretically breakable but computationally comfortable techniques [20] The proliferation of cryptography has given rise to a slew of statistical age jail issues. Because of its potential for use in espionage and sedition, several countries have treated cryptography like a weapon, restricting or outright banning its use and export. Some countries have passed legislation making [21] it possible for law enforcement to demand the surrender of encryption keys for data relevant to an investigation. Digital media copyright infringement challenges and online rights management both rely heavily on cryptography. Steganography technique as shown in fig 2 is a means of hiding mystery info inside (or even on top of) an in any other case commonplace, non-secret document or other medium to stay away from discovery.

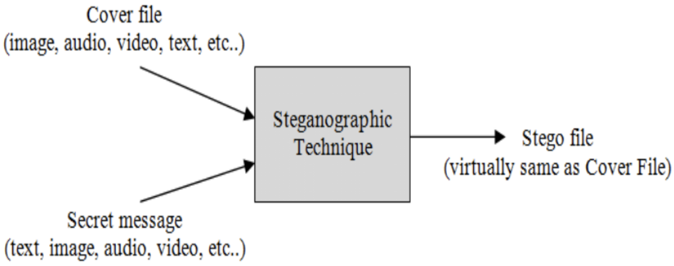

Cover file
(image, audio, video, text, etc..)
Steganographic Technique
Stego file
(virtually same as Cover File)
Secret message
(text, image, audio, video, etc..)

**Figure 2:** Basic process of steganography technique

The fig 2 dispatches can use steganography to hide textual content, video, pics, or maybe audio statistics. It’s a useful bit of know-how, limited handiest by the kind of medium and the writer’s imagination.

## 3. Proposed System

The proposed work that concentrates on techniques which are used to overcome the existing disadvantages [21] the existing system that uses the symmetric key cryptography to transfer the data [22] but in the proposed work there is no keys that are used to encrypt the clear text. The proposed work as shown in fig. 3 that performs two main phases called data encryption and embedding process for encryption and reverse process called decryption [23].

### 3.1. Data Encryption

The goal of encryption in cryptography is to ensure that only authorized parties have access to a message or piece of information. The only thing encryption does is make it so an eavesdropper can’t understand what’s being said. The plaintext of a message or other piece of information is encrypted using an encryption algorithm and a cipher to produce a version of the message

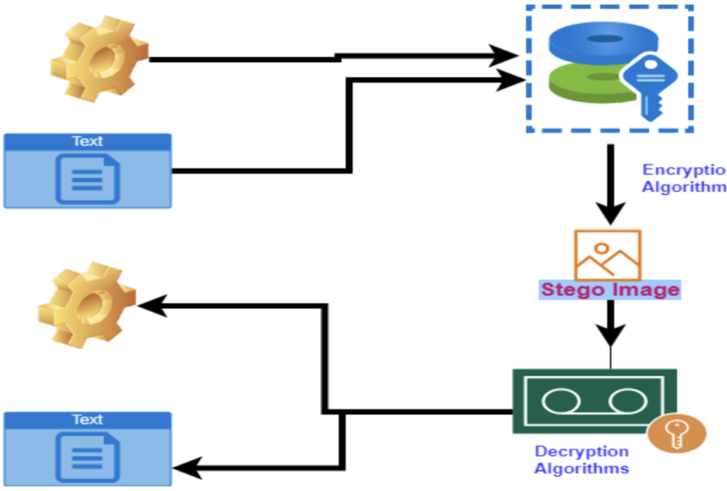


**Figure 3:** Architecture of proposed system

known as ciphertext [21] Both public-key and symmetric-key cryptography are not required to encrypt documents. Instead, we suggest a scheme where the document is encrypted without the usage of a key. If you want to ensure the highest level of security, you shouldn't use the same passphrase to guard your private key as you do the keyless procedure that drives the keyless cipher [24] When it is not necessary to share the password with anybody else, keyless encryption is a great way to keep sensitive data safe. Encrypting a file using a keyless cipher is possible by selecting this menu item. There were four stages of encryption and four stages of decryption in the suggested technique for encrypting work files. The four-step encryption procedure is a methodical, multi-stage scheme that employs four novel techniques. Z-scan, a tweaked rail fence, a cross-over, and a xor operation are the new techniques.

## 3.2. Modified Zig-Zag

Scan In order to no uniformly quantize N*N DCT coefficients, zigzag scanning is used [25]. This coding scheme is based on transforms. The energy is concentrated in the lower coefficients and is dispersed in a radial pattern around the origin. The end result is a one-dimensional sequence in which the vast majority of the coefficients are zero after a critical threshold is passed. When encoding a non-zero coefficient, the category/run length encoding first counts the number of consecutive zeroes in the scanned sequence. Both sym1 and sym2 are based on the number of zeros before the nonzero coefficient, whereas sym1 is based on the magnitude of the coded coefficient. Therefore, the DCT coefficients are ordered in an efficient fashion for the category/run coding phase by use of zigzag scanning. The zigzag operation on binary integers has been described up to this point.

But in this proposed work actually perform on decimal numbers (ASCII of Plain text). The system that uses this operation to make original text to somewhat disturbed text.Zig-zag scan used because to group low frequency coefficients in top of vector. Zig-zag scan matrix range

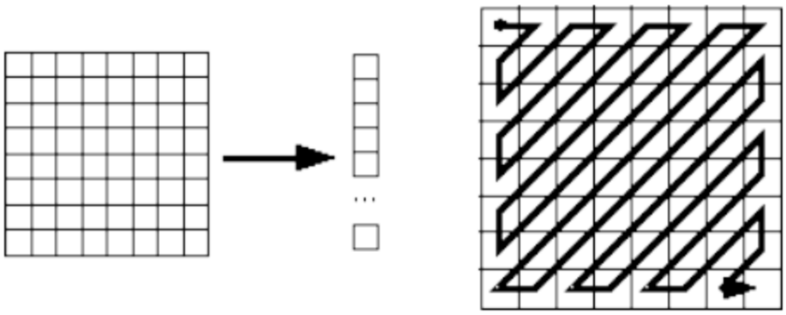


Figure 4: 8*8 zigzag scan matrix

that can defined in two ways such as 4*4 and 8*8 as shown in fig. 4. By performing this scan method, it generates intermediate cipher text1. Maps 8*8 to a 1*64 vector Maps 4*4 to a 1*16 vector.

### 3.3. Modified Rail Fence

1. Data is organized just like as wave form, in this form there exist two levels of values.
2. Second level values are followed by first level values which creates first stage of intermediate cipher2.
3. In the next step split the intermediate cipher into two parts and align them as rail fence structure.
4. Again, perform the actual rail fence process to get as usual original text.

Fig. 5 shows the basic approach of Rail Fence method.

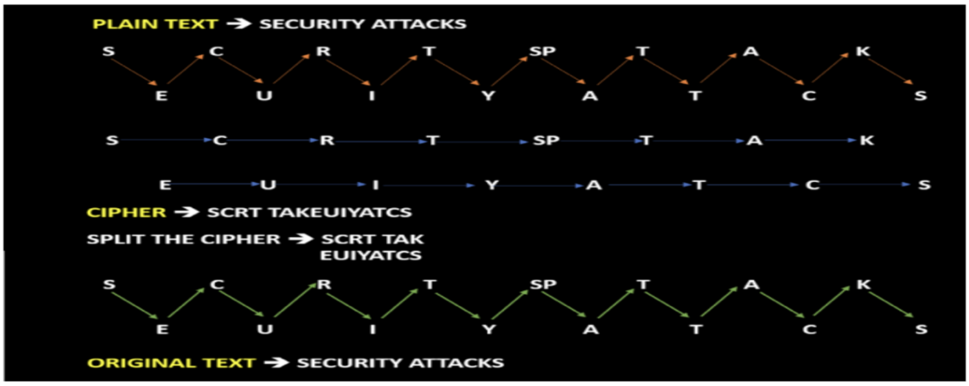

PLAIN TEXT → SECURITY ATTACKS
S C R T SP T A K
E U I Y A T C S
S C R T SP T A K
E U I Y A T C S
CIPHER → SCRT TAKEUIYATCS
SPLIT THE CIPHER → SCRT TAK
EUIYATCS
S C R T SP T A K
E U I Y A T C S
ORIGINAL TEXT → SECURITY ATTACKS

Figure 5: Modified Rail Fence

### 3.4. Modified Crossover

Reproduction and genetic crossover are likened to the crossover operator. In this more than one parent is chosen and one or more off-springs are generated utilizing the genetic material of the parents. It's important to keep in mind that the GA Designer has the option of implementing a problem-specific crossover operator in addition to these fairly general ones. To convert an original matrix into an intermediate cipher3, the proposed work offers a novel crossover technique as shown in fig. 6.

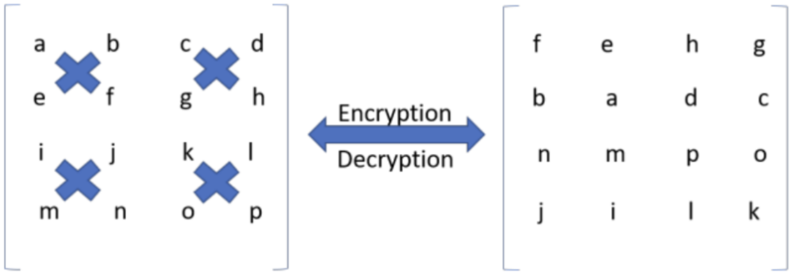


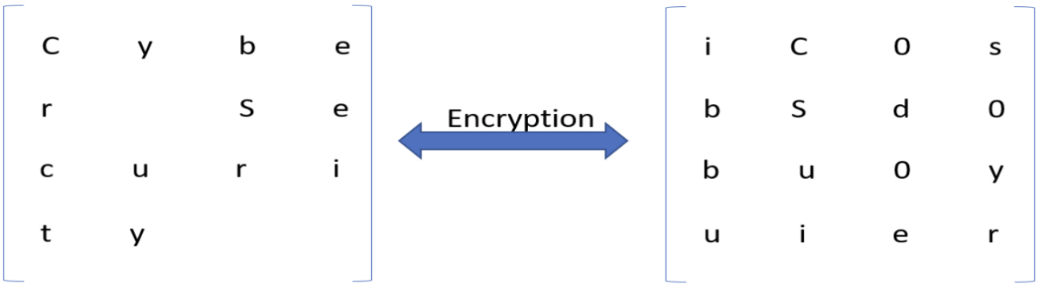
**Figure 6:** 4 x 4 matrix Crossover

### 3.5. XoR Operation

The only two possible numbers in a computer are zero and one, hence all computations are performed using the binary system. Everything on a computer, including numbers, letters, pictures, and videos, is saved and displayed in this way.We shall restrict ourselves to integers for this exercise. All computers first transform integers supplied by the user into a binary representation of the number before carrying out any calculations. Fig. 7 shows the basic encryption process to convert original message into cipher message.

**Encryption Algorithm**

Step 1: Read the text file.
Step 2: Convert each character in the file into corresponding ASCII value.
Step 3: Construct the corresponding data into 4*4 matrices.
Step 4: Each 4*4 block performs the following methods one by one
Step 4.1: Modified 4*4 Zig-Zag scan
Step 4.2: Modified Rail fence
Step 4.3: Crossover
Step 4.4: XOR operation
Step 5: Embed the result of XOR into individual RGB planes.



$$\begin{bmatrix} C & y & b & e \\ r & & S & e \\ c & u & r & i \\ t & y & & \end{bmatrix} \xleftrightarrow{\text{Encryption}} \begin{bmatrix} i & C & 0 & s \\ b & S & d & 0 \\ b & u & 0 & y \\ u & i & e & r \end{bmatrix}$$

**Figure 7:** Original message (left) to Cipher message (right)

## 3.6. Decryption Algorithm

Step 1: Extract the RGB pixels from the stegoimage.
Step 2: Convert each pixel into corresponding ASCII value.
Step 3: Construct the corresponding data into 4 x 4 matrices.
Step 4: Each 4 x 4 block performs the following methods one by one
Step 4.1: XOR operation
Step 4.2: Crossover
Step 4.3: Modified Rail fence
Step 4.4: Modified 4*4 Zig-Zag scan
Step 5: Decrypted plain.txt file will be created.

**Table 1**
Time complexity for existing and proposed

| File size | Existed | Proposed |
|---|---|---|
| 1KB | 285 | 221 |
| 5KB | 370 | 277 |
| 10KB | 360 | 301 |
| 15KB | 395 | 318 |
| 20KB | 720 | 587 |

**Table 2**
PSNR values for existing and proposed

| File size | Existed | Proposed |
|---|---|---|
| 1KB | 4.4881 | 7.297 |
| 5KB | 4.856 | 7.8978 |
| 10KB | 4.8787 | 7.6931 |
| 15KB | 4.7568 | 7.6589 |
| 20KB | 4.6564 | 7.6129 |

## 4. Conclusion

In an efficient LSB based image steganography is presented. The planned method ensures there is no major changes are accomplished where secret message is embedded into cover changes. The secret message has been generated with innovative method such as 4*4 zig-zag, crossover and modified rail fence. When compared with existing it is taking more time for embedding the data. In the parameter analysis PSNR values are high when compared with existing, which means there is no major changes in cover image. Further this work may be extended for audio and video by keeping PSNR as higher values.

## References

[1] J. Wang, C. Yang, P. Wang, X. Song, J. Lu, Payload location for JPEG image steganography based on co-frequency sub-image filtering, Int. J. Distrib. Sens. Netw. 16 (2020) 155014771989956.

[2] N. Alanizy, A. Alanizy, N. Baghoza, M. AlGhamdi, A. Gutub, 3-LAYER PC TEXT SECURITYVIA COMBININGCOMPRESSION, AES CRYPTOGRAPHY2LSB IMAGE STEGANOGRAPHY, jreas 03 (2018) 118–124.

[3] R. Biswas, I. Mukherjee, S. K. Bandyopadhyay, Image feature based high capacity steganographic algorithm, Multimed. Tools Appl. 78 (2019) 20019–20036.

[4] A. V. Srinivas, S. S. S. Reddy, A novel approach for excavating communication using taxonomy and outline mechanisms, in: 2021 Sixth International Conference on Image Information Processing (ICIIP), IEEE, 2021.

[5] A. Jan, S. A. Parah, B. A. Malik, M. Rashid, Secure data transmission in IoTs based on CLoG edge detection, Future Gener. Comput. Syst. 121 (2021) 59–73.

[6] W. Z. Khan, M. Y. Aalsalem, M. K. Khan, Q. Arshad, Data and privacy: Getting consumers to trust products enabled by the internet of things, IEEE Consum. Electron. Mag. 8 (2019) 35–38.

[7] A. Alsaidi, K. Al-lehaibi, H. Alzahrani, M. AlGhamdi, A. Gutub, Compression multi-level crypto stego security of texts utilizing colored email forwarding, J. Comput. Sci. Comput. Math. (2018) 33–42.

[8] K. Hari, J. Bommala, N. Venkata Rao Yanamadni, S. Dr, Survey on machine learning with cloud technology preserving privacy: Risks and keys, Solid State Technology 64 (2021).

[9] V. Madaan, D. Sethi, P. Agrawal, L. Jain, R. Kaur, Public network security by bluffing the intruders through encryption over encryption using public key cryptography method, in: Advanced Informatics for Computing Research: First International Conference, ICAICR 2017, Jalandhar, India, March 17–18, 2017, Revised Selected Papers, Springer, 2017, pp. 249–257.

[10] A. Kumar, I. Fister Jr, P. Gupta, J. Debayle, Z. J. Zhang, M. Usman, Artificial Intelligence and Data Science: First International Conference, ICAIDS 2021, Hyderabad, India, December 17–18, 2021, Revised Selected Papers, Springer Nature, 2022.

[11] N. A. Loan, N. N. Hurrah, S. A. Parah, J. W. Lee, J. A. Sheikh, G. M. Bhat, Secure and robust

digital image watermarking using coefficient differencing and chaotic encryption, IEEE Access 6 (2018) 19876–19897.

[12] R. Shanker, P. Agrawal, A. Singh, M. W. Bhatt, Framework for identifying network attacks through packet inspection using machine learning, Nonlinear Engineering 12 (2023) 20220297.

[13] R. Shanker, V. Madaan, P. Agrawal, Fss-part: Feature grouping subset model for predicting network attacks, SN Computer Science 5 (2023) 94.

[14] B. O. Al-Roithy, A. Gutub, Remodeling randomness prioritization to boost-up security of RGB image encryption, Multimed. Tools Appl. 80 (2021) 28521–28581.

[15] A. Jan, S. A. Parah, B. A. Malik, A novel laplacian of gaussian (LoG) and chaotic encryption based image steganography technique, in: 2020 International Conference for Emerging Technology (INCET), IEEE, 2020.

[16] A. K. Singh, B. Kumar, S. K. Singh, S. P. Ghrera, A. Mohan, Multiple watermarking technique for securing online social network contents using back propagation neural network, Future Gener. Comput. Syst. 86 (2018) 926–939.

[17] K. A. K. Patro, B. Acharya, A novel multi-dimensional multiple image encryption technique, Multimed. Tools Appl. 79 (2020) 12959–12994.

[18] N. Ayub, A. Selwal, An improved image steganography technique using edge based data hiding in DCT domain, J. Interdiscip. Math. 23 (2020) 357–366.

[19] M. Hussan, S. A. Parah, S. Gull, G. J. Qureshi, Tamper detection and self-recovery of medical imagery for smart health, Arab. J. Sci. Eng. 46 (2021) 3465–3481.

[20] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, S. W. Baik, Image steganography using uncorrelated color space and its application for security of visual contents in online social networks, Future Gener. Comput. Syst. 86 (2018) 951–960.

[21] F. S. Hassan, A. Gutub, Novel embedding secrecy within images utilizing an improved interpolation-based reversible data hiding scheme, J. King Saud Univ. - Comput. Inf. Sci. 34 (2022) 2017–2030.

[22] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. S. Ho, K.-H. Jung, Image steganography in spatial domain: A survey, Signal Process. Image Commun. 65 (2018) 46–66.

[23] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, S. W. Baik, Image steganography using uncorrelated color space and its application for security of visual contents in online social networks, Future Generation Computer Systems 86 (2018) 951–960.

[24] F. S. Hassan, A. Gutub, Novel embedding secrecy within images utilizing an improved interpolation-based reversible data hiding scheme, Journal of King Saud University-Computer and Information Sciences 34 (2022) 2017–2030.

[25] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. Ho, K.-H. Jung, Image steganography in spatial domain: A survey, Signal Processing: Image Communication 65 (2018) 46–66.

[26] S. Sai Satyanarayana Reddy, G. Sowmya, V. B. Reddy, B. D. Kumar, A. Kumar (Eds.), Deep CNN Based Whale Optimization for Predicting the Rice Plant Disease in Real Time, ????