International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 05 July 2023 **Revised:** 25 August 2023 **Accepted:** 15 September 2023*

Secure Framework for Cyber Data Using Cryptographic and Steganographic Algorithms

Bhawna[1], Dr. Sanjay Malik[2],
[1,2] Department of Computer Science and Engineering, S R M University, Sonipat, Haryana, India
[1]bhawnachhabra1983@gmail.com , [2]skmalik9876@gmail.com

Abstract: The e-commerce industry has recently seen enormous growth on a global scale. Due to the rising popularity of online shopping, consumers, businesses, and depository financial institutions are extremely worried about debit/credit card fraud and the protection of personal information. It is essential to prevent unwanted access to and use of the information since it is disseminated over insecure channels. Cryptography and steganography are most frequently employed to avoid unauthorized access to sensitive data. However, the combined qualities of these two approaches are not secure enough in the modern world. It might lead to some vulnerability. It is possible to add additional layers of protection and achieve high levels of information security if visual cryptography is used in conjunction with the abovementioned combination. This research work proposed a multi-level information security framework for cyber data using random public key cryptography for the secret text, color image steganography for concealing secret encrypted text in the cover image, visual cryptography for slicing the cover image into two shares, and image steganography again to hide both the shares into two color images, respectively. These security processes significantly increase the confidentiality, dependability, and efficiency of secret messages. While there isn't a parameter to demonstrate the level of security achieved using cutting-edge techniques, the accuracy of the received text data is calculated in terms of MSE and correlation coefficient by comparing the sent and received text data. To evaluate the effectiveness of the suggested strategy, the time required at the transmitter and receiver ends is also calculated. The MATLAB environment is utilized in the implementation, demonstrating that the suggested system has improved robustness when considering steganalysis.

***Keywords:** Encryption, Decryption, Cryptography, Steganography*

I. INTRODUCTION

High networking expansion leads to a shared culture for exchanging digital photographs. Hackers can easily duplicate and re-distribute digital images. Images must be secured during transmission. Protect credit cards, banking activities, and SSNs. To prevent information theft, various encryption mechanisms exist. In modern Internet days, data encryption plays a key role in safeguarding online data transmissions. The confidential data is encrypted to prevent unauthorized use. As the amount of data transferred daily over the Internet continues to grow, ensuring the safety of the networks involved is more crucial than ever. Cryptography and steganography are two crucial security methods. These two approaches are both commonplace in the field of information security.

Steganography is the process of concealing data in digital media utilizing techniques for embedding messages so that only the sender and the intended recipient(s) can detect their existence. Cryptography is the technique of securely transmitting data over the Internet using cryptographic methods, making it impossible for an adversary to access or steal sensitive or private data. Our research uses sequential encoding, a technique of picture encoding that employs a single scan over the data as opposed to progressive encoding, which employs numerous scans. Sequential decoding is the process of translating received messages into code words of a certain code. There are a variety of prominent mapping methods for communications to code words.

Encoding Process:

The encoding process is carried out at the sender's side. The sender needs to send the data secretly to the receiver. To hide the data from intruders, the concept of cryptography or steganography can be used. But when used individually, one could have single level of security. So, both of the techniques can be used by the sender to have multi-level security. Figure 2 illustrates the encoding process.

The sender hides the information (text to be sent to the receiver) in an image file. This image becomes the secret image. At this point, the sender gets the first level of security. Now the sender uses the concept of visual cryptography to make multiple shares of the secret image. Each share is a noise-like structure. At this point, the sender gets a second level of security. Now the sender uses the concept of image steganography for hiding the shares in different images. At this point, the sender achieves the third level of security. Now, the obtained secret images are sent to the receiver.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *05 July 2023* ***Revised:*** *25 August 2023* ***Accepted:*** *15 September 2023*

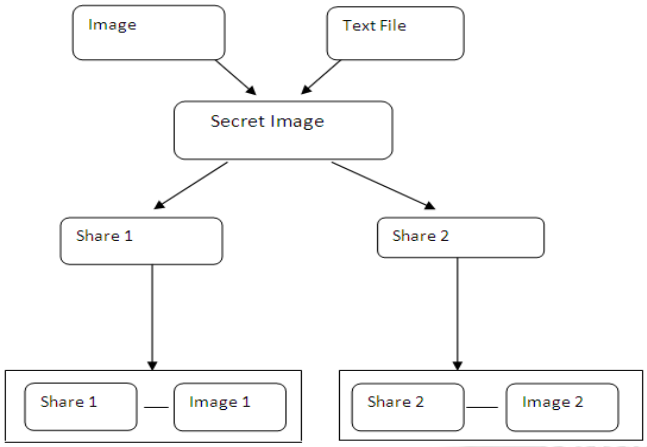

Figure 1: Hiding data and generating shares of image

By using different images for hiding different shares, system can be made much more secure and it will become very difficult for intruders to find out the information.

Decoding Process:

At the receiver's end, the decoding procedure is completed. The receiver receives the two secret images (carrying the information) sent by the sender. The receiver needs to apply the decryption process to obtain the secret text. In the first step, the decryption process of image steganography is applied to extract the hidden shares from the received secret images. Then the extracted shares need to be overlapped in order to obtain the original secret image containing the hidden text. For this, the receiver applies the Bit ORing on the obtained extracted shares. The secret text is then extracted from the received secret image by the recipient using the steganography decryption procedure. The entire decoding procedure is depicted in Figure 2.

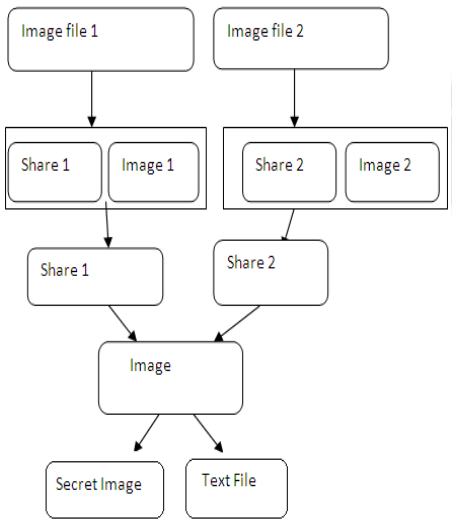

Figure 2: Extracting hidden data from shares

- Decrypt both image files. After decoding the images, we will obtain the hidden shares of the image. They are in encrypted form (encrypted by visual cryptography).
- The obtained shares can then be decrypted without the use of any complex computation. We only need to superimpose these shares on one another so that we will get the original image, containing the hidden information (for that XOR operation is used).

This research paper includes the preceding notable points: (i) a review of past studies that are relevant in section-2; (ii) a description of the methods to be used in section-3; (iii) results in section-4; and (iv) Section-5 contains the conclusion derived from the current research.

II. LITERATURE REVIEW

Various scholars have done a lot of studies in the past to try to tackle the challenge of hiding the information while transferring from the sender to the receiver end. The current literature was searched using e-learning websites, selection criteria, e-learning websites selection techniques, MCDM concept, methodologies, and their implementation in diverse application areas. In their literature analysis, John Justin and Manimurugan (2012) concentrated mostly on the many types of encryption algorithms currently in use. The authors also concentrated on double encryption, chaos-based encryption, information encryption, and picture encryption approaches. This paper analyses the security concerns with the performance parameters utilized in encryption operations [1]. Steganography was discussed by Patel et al. in 2013. Sensitive information can be concealed in any kind of media using steganography, which allows for its secure transmission through communication networks. The authors provided a summary of several information-hiding methods used in steganography as well as an analysis of how these methods have evolved through time [2]. According to a survey conducted by Rahmani et al. (2014), both steganography and cryptography, which both guarantee security, fall short in one way or another when it comes to covering all security criteria. Additionally, a brand-new algorithm was put up that would adhere to all security standards and fulfil steganography's requirements [3].

Almuhammadi and Al-Shaaby (2017) also carried out a comparison between steganography and cryptography. Additionally, the authors classified these techniques and contrasted them in terms of the encryption algorithm, the steganography technique, and the file format utilized to conceal the information [4]. In order to create a hybrid system, Taha et al. (2019) set out to evaluate several strategies to combine steganographic and cryptographic algorithms. While cryptography modifies the transmission format, steganography hides the existence of a secret message

[5]. Information security pioneers Anudini et al. (2021) created cloud computing. The military, healthcare, education, and finance use cloud computing for on-demand internet computing. Cloud computing is efficient, scalable, accessible, backup, and recoverable. The authors described combining blowfish symmetric key cryptography and Elliptic-Curve Cryptography (ECC) as a hybrid cryptosystem to perform double encryption to safeguard data [6]. For encrypted photos, Puech et al. (2008) presented a reversible data-hiding approach. The authors outlined each stage of the suggested procedure and illustrated plots of the local standard deviations to examine various findings [7]. Although Babaei's (2013) trustworthy data encryption method (OTP) is theoretically impenetrable for the encryption and decryption process, it has significant drawbacks [8].

Bouslimi et al. (2016) proposed a revolutionary technique that permits embedding a message inside an encrypted image that may be recovered regardless of whether the image is encrypted. The suggested method relies on applying a "pre-watermark," or predetermined watermark, on the image before the encryption process in order to do this. The process usually continues with adding or removing messages to or from the encrypted image. Due to the influence of this data-hiding technique on the "pre-watermark," after the decryption process, we can access the message in the spatial domain. As a result, the watermark processing process is independent of the encryption key knowledge, and the only thing needed to embed the message and extract it from the encrypted or decrypted image is the watermarking key information. Message embedding/extraction techniques are totally independent from encryption/decryption procedures reciprocally [9]. Haque et al. (2017, October) proposed the use of identity-based encryption to create a feasible and effective hierarchical architecture for UAV networks. Additionally, the authors suggested a selective encryption strategy to decrease overheads and a data-hiding mechanism to improve message secrecy [10].

A brand-new technique for concealing information within an image was presented by Abbood et al. (2018). By spreading the secret text throughout the entire image and randomly assigning bits to each row, this technique generates a new sequence of enigmatic and challenging steps. then hiding the bits in that row using a unique reverse technique. The LSB approach was created in order to make it more challenging to conceal the pixel. The results show how effective and secure the procedure is, and they also increase the security of hidden information [11]. For homomorphic encrypted pictures, A novel reversible data-hiding method was presented by Wu et al. in 2019. By implementing data concealing in the homomorphic encryption domain, user privacy and data security are protected. In addition, by executing data embedding in two stages, the hidden data can be retrieved in the encrypted domain and after image decryption, respectively. As a result, it is possible to select the right algorithm for the message that will be transmitted [12]. In 2020, Baagyere et al. presented an end-to-end steganographic and cryptographic method using genetic algorithms and residue number systems on text and images for digital communication. The proposed approach encrypts and decrypts images, with the encrypted image serving as a text cover (also encrypted). The proposed system can be fully implemented to include the encryption of the stego image or partially implemented to only implement the steganography element, allowing the transmission of a stego image with hidden text. At this stage, the message's existence and content are concealed from outsiders [13].

The protocol for elliptic Galois cryptography was introduced by Khari et al. in 2019. In this protocol, private information obtained from several medical sources was encrypted using a cryptography approach. The encrypted data was then steganographically embedded into a simple image using the Matrix XOR encoding technique. The suggested method additionally optimises the selection of cover blocks inside the image using an optimization algorithm called Adaptive Firefly [14].

Three control random parameters are used in Hashim et al(2019, .'s October) novel steganography technique based on Bit Invert System (BIS). Henon Map Function is used to guide the random selection process (HMF). Affine cypher and the Huffman algorithm were employed to decrease the amount of data that needed to be encrypted before it could be embedded for high payload capability [15]. A medical image dataset was used to test the proposed protocol by Abd-El-Atty et al. (2020), and in terms of security, visual quality, high resistance to data loss assaults, high embedding capacity, etc., the findings were outstanding, establishing the suggested scheme as a legitimate technique for successful medical image steganography[16]. Rajesh et al. (2020) were able to show that even astronomically vast amounts of data can fit inside of a small image by using the new Huffman coding approach in the Image Steganography. The ciphertext was first compressed using Huffman Coding, and then replaced with the data from the previous phase using the LSB method of image steganography. Python was used by the authors to implement the analysis, and the results of improved compression enable networks to carry massive volumes of data more easily [17].

Nunna et al. (2020, March)'s suggested a method that provides two levels of data protection by combining steganography and cryptography. The objective of this

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 05 July 2023 **Revised:** 25 August 2023 **Accepted:** 15 September 2023*

research is to develop a new technique for data encryption using the XOR operation and embedding encrypted data in a picture using a user-selected key [18]. In order to secure and verify a connection between two devices/gadgets utilizing sound, Datta et al. (2021) suggested using a number of techniques without the use of human pin verification. To send data by embedding it inside a file, this steganographic module uses two-stage encryption with two separate encryption methods. For this system's comparison of the resulting file size, a number of encryption techniques and their combinations are used. Both of these systems produce high accuracy and secure connectivity, which results in a long-term communication ecology [19].

Wahab et al(2021) 's evaluated and discussed the RSA method for encrypting and decrypting the secret file with two distinct picture compression algorithms. Several types of image compression techniques are evaluated in accordance with several criteria, such as compression ratio, compression duration, compression speed, Saving Percentage, MSE, PSNR, and structural characteristics [20]. Gaikwad et al. (2014) introduced the steganographic approach for concealing hidden messages of various sizes in video files. Techniques for compression and encryption have been used. When a secret file is huge, it is first compressed before being hidden via LSB steganography. For purposes of encryption and decryption, the password is utilized in secret [21]..

III. THE METHODOLOGY:

This research work proposed a multi-level information security framework for cyber data using random public key cryptography for the secret text, color image steganography for concealing secret encrypted text in the cover image, visual cryptography for slicing the cover image into two shares, and image steganography again to hide both the shares into two color images, respectively. These several security processes significantly increase the degree of confidentiality, dependability, and efficiency for secret messages. While there isn't a parameter to demonstrate the level of security achieved using cutting-edge techniques, the accuracy in terms of MSE and correlation coefficient of the received text data is calculated by comparing the sent and received text data. Also, the time taken at the transmitter and receiver end is calculated to assess the performance of the proposed method. The implementation uses the MATLAB environment, demonstrating that the suggested system has improved robustness when taking steganalysis into account.

To undersand the working of the proposed method, a suitable block diagram is given below.

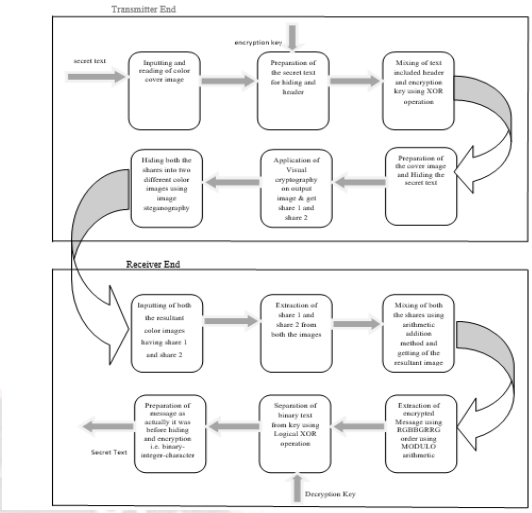

Figure 3: Block diagram of the proposed method

Here are the steps for the implementation of the proposed methodology.

Transmitter End

1. Inputting and reading of color cover images to hide the text.
2. Inputting and reading the secret text.
3. Inputting the encryption key between 0 to 255.

4. Preparation of the secret text and header

- The transformation of text into corresponding ASCII Integer Values.
- Calculating the message's length or the text message's character count.
- Creating a header to be sent with the text message.
- Zeros are padded in the header if there are fewer than four rows of text.
- Horizontal concatenation of the Message and header.
- Conversion of text and header into binary equivalent.
- Mixing of text including header and encryption key using XOR operation.

5. Preparation of the cover image and Hiding the secret text

- Initializing some Counters, i.e., rm, gm, and bm.
- Calculate the encoded Message's size and assign it to a Variable. This variable indicates the number of iterations to be run further.
- Initialization of a loop according to the size of the encoded Message.
- Hide the data points using image channel-wise (RGBBGRRG) Order. Using logical AND and OR operations, conceal the secret data bits that have been encoded along the columns that move from left to right across the binary target cover image.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 05 July 2023 **Revised:** 25 August 2023 **Accepted:** 15 September 2023*

- Picking bits of secret Message one by one and making a particular change in the corresponding bit of the cover image
  - Change using logical AND operation if secret image corresponding bit is 0
  - Change using logical OR operation if the secret image corresponding bit is 1

6. Determining whether or not the image's end has been reached. After that, we must change to the subsequent column and restart the pattern from the top row. We must check this each time we raise the rm, gm, and bm counters because we have no idea when we will arrive at this stage.

8. Application of Visual cryptography on the resultant cover image and getting its shares, i.e., share 1 and share 2.

9. Hiding both the shares into two different color images using image steganography, i.e., sequential encoding method.

Receiver End

1. Inputting of both the final resultant color images having share 1 and share 2.
2. Extraction of share 1 and share 2 from both the images respectively using a reverse image steganography process i.e., sequential decoding method.
3. Mixing both shares using the arithmetic addition method and getting the resultant image matrix.
4. Assigning each layer matrix's red, green, and blue colors to three distinct variables.
5. Inputting of the key for text extraction.
6. Recovering the Header Set from the resulting image.
7. Initializing the rm, gm, and bm Counters for the recovery operation.
8. Analysis of header by determining the text data Dimensions from Header Values.
9. Extract the encrypted Message from the resultant image using RGBBGRRG order using MODULO arithmetic.
10. Determining whether or not the image has ended. The next step is to travel to the subsequent column and reset our pattern to the first row. We must check this EVERY time after increasing the rm/gm/bm counter because we have no idea when we will arrive at this point.
11. Using the logical XOR procedure, binary text and the key are separated.
12. Before hiding and encrypting the message, it is prepared to be displayed as-is, which involves converting the binary data to an integer and the integer to an ASCII character.
13. Writing decrypted Message to. TXT File.
14. Computation of performance assessment matrices i.e. MSE, correlation coefficient, and Computational time.

IV. RESULTS

This research work proposed a multi-level information security framework for cyber data using random public key cryptography for the secret Text, color image steganography for concealing secret encrypted Text in the cover image, visual cryptography for slicing the cover image into two shares, and image steganography again to hide both the shares into two color images, respectively. These several security processes significantly increase the degree of confidentiality, dependability, and efficiency for secret messages. Although there isn't a parameter to illustrate the amount of security attained using the suggested method and compare it to cutting-edge techniques, the correctness of the received text data is calculated in terms of MSE and correlation coefficient by comparing the sent and received text data. Also, the time taken at the transmitter and receiver end is calculated to assess the performance of the proposed method. The MATLAB environment is used in the implementation, demonstrating that the suggested system has improved robustness when considering steganalysis.

The secret Text's content is intentionally kept random, and a significant number of special characters, numbers, and characters have been used to test the efficiency of the proposed method. The output of each substantial step is shown below in the images.

Firstly, the input cover color image is inputted to cover the secret Text with a public encryption key between 0 to 255.

Figure 4: Input cover color image

Next, the secret Text is inputted having 1KB size. In order to evaluate the effectiveness of the suggested method, a sizable number of special characters, digits, and characters have been employed in the secret Text, whose content is purposefully maintained random.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 05 July 2023 **Revised:** 25 August 2023 **Accepted:** 15 September 2023*

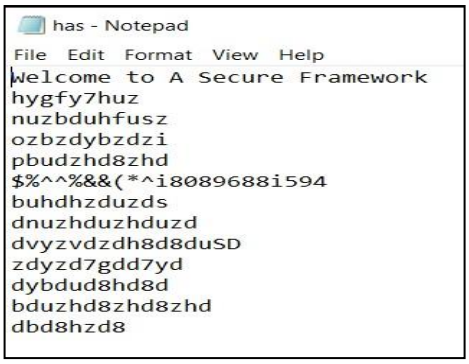

Figure 5: Secret texts to be hidden

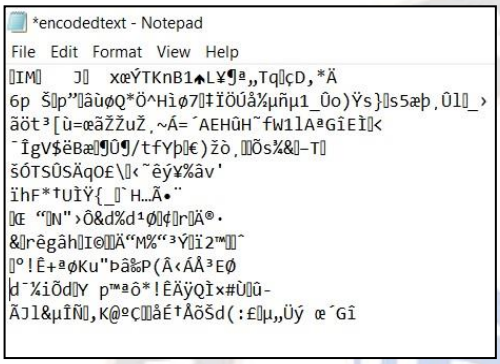

Figure 6: Encrypted secret text

The inputted Text is first converted into equivalent ASCII Integer Values. The text message is then prepared with a header. The header is intentionally inserted before the Text and contains essential details such as the Text's length and whether it is Text or not. After this, the ASCII converted Text and header into its binary equivalent code. The binary equivalent code is mixed with the XOR operation's encryption key. Figure 6 demonstrates the encrypted Text.

After then, the cover image is transformed into its binary counterpart. The encoded Text is then hidden beneath each cover image layer using image channel-wise (RGBBGRRG) Order. By using logical AND and OR operations, the secret data bits are concealed along the columns that go from left to right via the binary target cover image. The bits of the secret message are picked one by one and made a particular change in the corresponding bit of the cover image

- Change using logical AND operation if secret text corresponding bit is 0
- Change using logical OR operation if secret text corresponding bit is 1

Using the visual cryptography technique, the cover image is sliced into two shares i.e., share 1 and share 2. Both the shares are shown in figures 7 and 8 below.

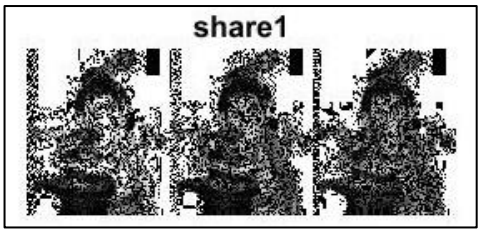

Figure 7: Share 1 extracted

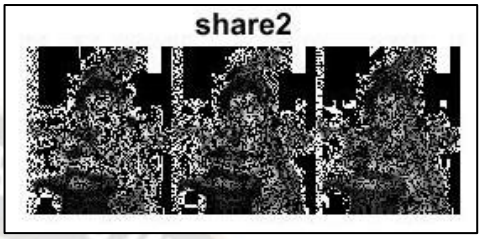

Figure 8: Share 2 extracted

The shares are hidden into two separate color cover images using the image steganography method, i.e., the sequential encoding method. This is done intentionally as both the claims are to be sent to the receiver with an extra layer of security. Both the cover images are sent to the receiver side. The shares, i.e., share 1 and share 2, are extracted from both images using a reverse image steganography process, i.e., sequential decoding. Both the extracted shares are mixed using the arithmetic addition method, and a resultant image matrix is computed. The resulting matrix is named Share12 and is depicted below.

Figure 9: combinations of both shares

After the secret key for the text extraction is inputted. First, the Header Set from the resultant image is recovered to determine the text data dimensions. The encrypted message is extracted from the resulting image using RGBBGRRG order using modulo arithmetic. The binary Text is extracted from the key using a Logical XOR operation. At last, the message to be shown is prepared (as before hiding and encryption), i.e., binary to integer and integer to the character as per ASCII values. The extracted Text is shown below in figure 10.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 05 July 2023 **Revised:** 25 August 2023 **Accepted:** 15 September 2023*

Figure 10: extracted secret text at the receiver end

While there isn't any parameter to demonstrate the level of security achieved using the proposed method and compare it with state-of-the-art techniques, the accuracy of the received text data is calculated by comparing the sent and received text data. Also, the time the proposed approach takes to hide and extract at the transmitter and receiver end is computed, respectively. Both factors could be used as evaluation criteria to determine whether the suggested strategy is effective. To show all the input and output parameters at once, a table is created.

Table 1: comparative analyses of the inputted Text with different sizes, cover image, extracted text size, received text error and similarity, and the time taken at the transmitter end and receiver end

S. No.	Secret Text with size	Cover image with size	Cover image with size for share 1	Cover image with size for share 2	Extracted Text size	Received text error (MSE)	Received text similarity (Cross-Correlation)	Time taken at the transmitter end (seconds)	Time taken at the receiver end (seconds)
1	Tag.txt (1 KB)	Lord.jpg (3 KB)	Lilly.jpg (33 KB)	Slice.jpg (40 KB)	1 KB	0	1	10.0469	8.4375
2	Example.txt (2 KB)	Lord.jpg (3 KB)	Lilly.jpg (33 KB)	Slice.jpg (40 KB)	1 KB	0	1	10.0625	7.8906
3	Extent.txt (3 KB)	Lord.jpg (3 KB)	Lilly.jpg (33 KB)	Slice.jpg (40 KB)	1 KB	0	1	10.2969	7.7234

To understand the values of performance assessment parameter computational time (at receiver and transmitter end) a bar chart has also been prepared. the comparative analysis of the computational time at the transmitter end is given in figure 8 and that at the receiver end is given in figure 9.

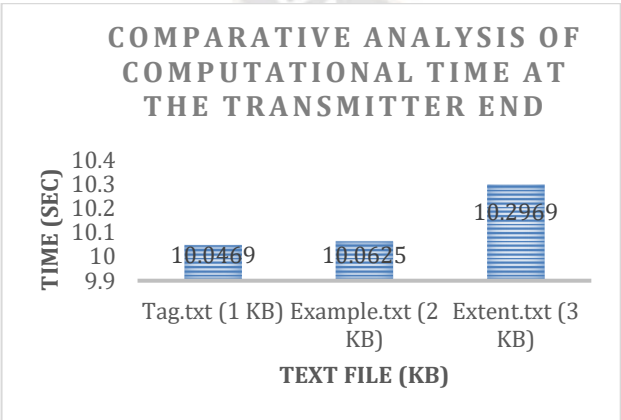

Figure 11: Comparative analysis of computational time at the transmitter end

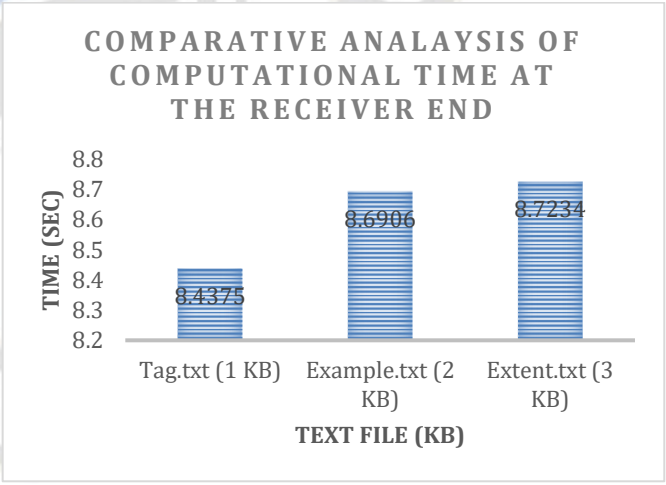

Figure 12: Comparative analysis of computational time at the receiver end

After observing the above table and both the bar charts, it is clear that the proposed methods are working efficiently. The computed values of performance assessment parameters directly depict that the proposed hybrid method produces zero error and hundred percent similarities between inputted and extracted Text. The first noticeable thing is that the proposed process involves four security steps for hiding the secret Text. Despite this, the proposed method produces a hundred

percent similar text with no error. The second noticeable thing is that the cover image required to hide the share or Text must be more significant than the quantity to be hidden.

Also, the time taken at the transmitter and receiver end is meager. Despite the four steps involved in hiding the Text and the same in extracting the Text, the proposed method is performing too fast, i.e., not more than 11 seconds (including manual image and text selection and putting up the file name) in hiding the Text and not more than 8 seconds (including image and text manual selection and putting up the file name) in extracting the Text.

V. CONCLUSION, IMPLICATIONS, AND FUTURE SCOPE

This research work proposes a multi-level information security framework for cyber data. The secret Text is hidden using the proposed method in four phases, and it is also extracted in four steps. The experimental findings in the preceding section were examined, and it was determined that the proposed approaches are effective. The calculated values of the performance evaluation parameters clearly show that the proposed hybrid technique creates no error and complete concordance between the extracted and input text. Additionally, there is little time consumed at the transmitter and receiver ends for processing the text data. The proposed method performs too quickly, taking less than 11 seconds (including manual image and text selection and putting up the file name) to hide the Text and less than 8 seconds (including manual image and text selection and putting up the file name) to extract the Text, even though both tasks require four steps. The proposed work might be improved in the future by employing neural networks for visual cryptography, which would enable the system to produce highly undetectable secret shares using a specific set of training data that could be created automatically and discarded when the task is finished. Additionally, this could speed up the calculation required to hide and retrieve the Text.

REFERENCES

1. John Justin, M., & Manimurugan, S. (2012). A survey on various encryption techniques. *International Journal of Soft Computing and Engineering (IJSCE) ISSN, 2231*, 2307.
2. Patel, K., Utareja, S., & Gupta, H. (2013). A survey of information hiding techniques. International Journal of Emerging Technology and Advanced Engineering, 3(1), 347-350.
3. Rahmani, M. K. I., Arora, K., & Pal, N. (2014). A crypto-steganography: A survey. International Journal of Advanced computer science and applications, 5(7).
4. Almuhammadi, S., & Al-Shaaby, A. (2017). A survey on recent approaches combining cryptography and steganography. Computer Science Information Technology (CS IT).
5. Taha, M. S., Rahim, M. S. M., Lafta, S. A., Hashim, M. M., & Alzuabidi, H. M. (2019, May). Combination of steganography and cryptography: A short survey. In IOP conference series: materials science and engineering (Vol. 518, No. 5, p. 052003). IOP Publishing.
6. Anudini, A. K. S. A., Gayamini, G., & Weerawardane, T. L. (2021). A Systematic Review on Secure Data Transmission in the Cloud Using Steganographic Techniques and Cryptographic Algorithms.
7. Puech, W., Chaumont, M., & Strauss, O. (2008, March). A reversible data hiding method for encrypted images. In *Security, forensics, steganography, and watermarking of multimedia contents X* (Vol. 6819, pp. 534-542). SPIE.
8. Babaei, M. (2013). A novel text and image encryption method based on chaos theory and DNA computing. *Natural computing*, *12*(1), 101-107.
9. Bouslimi, D., Coatrieux, G., Cozic, M., & Roux, C. (2016). Data hiding in encrypted images based on predefined watermark embedding before encryption process. *Signal Processing: Image Communication*, *47*, 263-270.
10. Haque, M. S., & Chowdhury, M. U. (2017, October). A new cyber security framework towards secure data communication for unmanned aerial vehicle (UAV). In *International Conference on Security and Privacy in Communication Systems* (pp. 113-122). Springer, Cham.
11. Abbood, E. A., Neamah, R. M., & Abdulkadhm, S. (2018). Text in Image Hiding using Developed LSB and Random Method. *International Journal of Electrical & Computer Engineering (2088-8708)*, *8*(4).
12. Wu, H. T., Cheung, Y. M., Yang, Z., & Tang, S. (2019). A high-capacity reversible data hiding method for homomorphic encrypted images. *Journal of Visual Communication and Image Representation*, *62*, 87-96.
13. Baagyere, E. Y., Agbedemnab, P. A. N., Qin, Z., Daabo, M. I., & Qin, Z. (2020). A multi-layered data encryption and decryption scheme based on genetic algorithm and residual numbers. *IEEE Access*, *8*, 100438-100447.
14. Khari, M., Garg, A. K., Gandomi, A. H., Gupta, R., Patan, R., & Balusamy, B. (2019). Securing data in Internet of Things (IoT) using cryptography and steganography techniques. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 50(1), 73-80.
15. Hashim, M. M., Taha, M. S., Aman, A. H. M., Hashim, A. H. A., Rahim, M. S. M., & Islam, S. (2019, October). Securing medical data transmission systems based on integrating algorithm of encryption and steganography. In 2019 7th International Conference on Mechatronics Engineering (ICOM) (pp. 1-6). IEEE.
16. Abd-El-Atty, B., Iliyasu, A. M., Alaskar, H., El-Latif, A., & Ahmed, A. (2020). A robust quasi-quantum walks-based steganography protocol for secure transmission of images on cloud-based E-healthcare platforms. Sensors, 20(11), 3108.
17. Rajesh, P., Alam, M., Tahernezhadi, M., Kumar, T. R., & Rajesh, V. P. (2020). Secure communication across the internet by encrypting the data using cryptography and image steganography. International Journal of Advanced Computer Science and Applications, 11(10).

18. Nunna, K. C., & Marapareddy, R. (2020, March). Secure data transfer through internet using cryptography and image steganography. In 2020 SoutheastCon (Vol. 2, pp. 1-5). IEEE.
19. Datta, D., Garg, L., Srinivasan, K., Inoue, A., Reddy, G. T., Reddy, M. P. K., ... & Nasser, N. (2021). An efficient sound and data steganography based secure authentication system. Comput. Mater. Contin, 67, 723-751.
20. Wahab, O. F. A., Khalaf, A. A., Hussein, A. I., & Hamed, H. F. (2021). Hiding data using efficient combination of RSA cryptography, and compression steganography techniques. IEEE Access, 9, 31805-31815.
21. Gaikwad, D. P., Jagdale, T., Dhanokar, S., Moghe, A., & Pathak, A. (2014). Hiding the Text and Image Message of Variable Size Using Encryption and Compression Algorithms in Video Steganography. International Journal of Engineering Research and Applications (IJERA), 1(2), 102-108.