Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7765899

TEXT DATA SECURITY THROUGH HYBRID METHOD USING VISUAL CRYPTOGRAPHY AND IMAGE STEGANOGRAPHY 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: Modern society puts a great deal of importance on digital communication, thus keeping it hidden is crucial. Many modern softwares are web-based, and users increasingly rely on social networking sites like Facebook, Twitter, and others. The data must be secured against unauthorized access and usage since it is distributed over unsecured channels. Since the information is sent across unsecured channels, it is crucial to prevent unauthorized access to and use of the data. Although there has been a significant amount of research done in the past, most of it has not taken into account the need for strong hybrid security concerning secret text. The two techniques most commonly used to prevent unwanted access to sensitive text data are visual cryptography and image steganography. These two techniques' unique merits, nevertheless, are not secure enough for the contemporary era. There may be some vulnerability as a result. If visual cryptography is combined with image steganography, it is feasible to use both algorithms together to obtain high levels of information security. This study presented a hybrid security method for hiding secret text that combines visual cryptography and LSB image steganography. Colour image steganography is used to hide shares in other cover images and cover up secret text in cover images. For splitting the cover image into two shares, use visual cryptography. The secrecy, trustworthiness, and effectiveness of covert communications are considerably improved by these security protocols. The accuracy of the received text data is calculated in terms of MSE and correlation coefficient by comparing the transmitted and received text data, even if there isn't a parameter to indicate the level of security attained by utilizing cutting-edge methods. To evaluate the effectiveness of the suggested methodology, the time required at the transmitter and receiver ends is also evaluated. The MATLAB environment is used in the implementation to show how the proposed method has increased resilience when taking steganalysis into account.

Keywords: *Encryption, Decryption, Cryptography, Steganography*

I. INTRODUCTION

Information hiding is a new field of study that includes steganography, watermarking, fingerprinting, and copyright protection for digital media [1]. A hidden message can be concealed within another message using steganography. One of the three principles of computer security, along with integrity and availability, is secrecy, which can be maintained with the help of steganography. Steganography is significant because it hides the fact that the secret it is attempting to protect even exists. Attackers pose a threat because they want to damage or gain access to assets by exploiting their weaknesses. The task of the attacker is made more challenging by steganography because the asset's very existence is concealed [3]. It is now necessary to combine steganography with encryption to create an impenetrable data-hiding system in order to transfer some critical data from one computer to another [8].

Cryptography: A secret technique is transformed into cypher text via cryptography, often known as secret writing, and communicated to a recipient who subsequently decrypts the cypher text into plain text. Symmetric key cryptography and asymmetric key cryptography are two different categories of cryptography.

Cryptography is utilized in information security on many different levels. It is difficult to read the data without a key to decode it. The data keeps its integrity while in transit and storage.

Cryptography also goes by the name of cryptology. Key pairs in cryptography enable senders and receivers to verify one another. There are various methodologies which are used for the data protection during cryptography. Some of the methodologies are explained below and shown in figure 1:

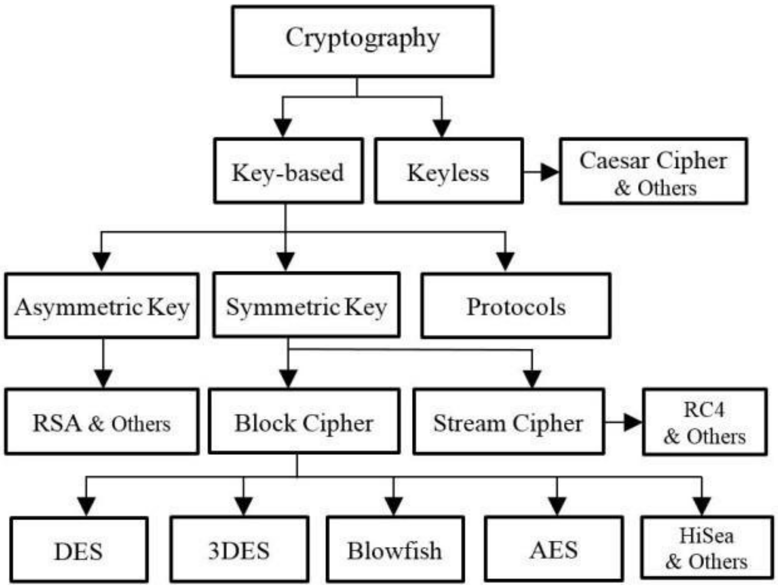


Fig 1: Classification of Cryptography and its techniques

Cryptography-centric data protection techniques:

Cryptographic encryption has shown to be the most effective way of data security. Modern encryption helps meet today's cybersecurity needs. Global cybersecurity uses these four cryptographic approaches.

- **Triple Data Encryption Standard (3DES) :**

Block cipher 3DES is a contemporary cryptography standard. Similar to 3DES, Data Encryption Standard uses keys with a 56-bit length. The Triple Data Encryption Standard is unique in that it uses symmetric key encryption with three keys of size 56 bits. A 56-bit key becomes a 168-bit key after three encryptions.

Although it takes longer than other encryption methods, the data is safer as a result. Because the approach uses shorter block lengths, competent hackers can decrypt and use crucial data more easily. Financial organizations and businesses employ this encryption method, as before. Electronic payments often use it.

- **Twofish**

Blowfish inspired Twofish, a block cipher. It is a symmetric block cipher with 128-256-bit blocks. The approach works best with low-end devices and CPUs. Like AES, it encrypts plain text into cipher text in rounds. Unlike AES, encryption rounds are continuous. Encryption rounds to sixteen regardless of key size.

This cryptographic method is more flexible since you may control key configuration and encryption speed. You can slow down encryption and speed up key configuration. Twofish encryption can be used as often as desired without a licence.

- **Advanced Encryption Standard (AES):**

AES is a secure form of encryption. The block cipher, used for symmetric encryption, fixes data points one at a time using blocks of a predetermined size. AES encrypts data in bulk, unlike other approaches. One AES variant is stream ciphers. AES-256, AES-192, and AES-128 all employ key bits. For encryption assignment, key bit encrypts blocks of 128–256 bits. There are 10, 12, and 14 rounds in 128-bit, 192-bit, and 256-bit encryption, respectively. AES symmetric key encryption requires sharing the key to access encrypted data. The U.S. government protects secret data with AES. This encryption technique is present in a lot of hardware and software products.

- **RSA:**

RSA, named after its creators Ron Rivest, Adi Shamir, and Len Adelman, uses public-key cryptography to send data across an unreliable network. Asymmetric cryptography algorithms use both the private and public keys. The public key is the later one; the former key should never be disclosed. This cryptography requires both keys to decrypt data. Keys can encrypt and decode data.

RSA factors integers from enormous prime numbers, making it secure. Key size increases algorithm security. Most RSA keys are 1024–2048 bits. Despite the increased key size, the encryption approach is faster.

Steganography: Steganography, also referred to as cover writing, is a method for masking a hidden message. This method aids in maintaining the secrecy of a message. It is fairly challenging to use and comprehend. In steganography, the data's structural integrity is preserved. It can be found in audio, video, or visual media.

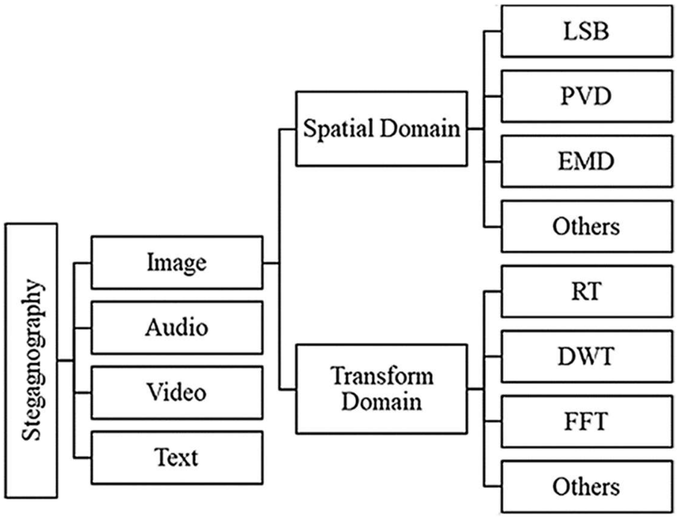


Fig 2: Classification of Steganography and its techniques

Images, videos, and audio files that contain sensitive information can be protected using steganography techniques. Although it is frequently employed in pictures, steganography is typically written in characters with hash marks. In any case, steganography makes it easier for illegal viewers to watch protected materials while also protecting them against piracy. Steganography is intended to be concealed from a third party, in contrast to cryptography, which is intended to be opaque to an unauthorized third party. In addition to having to be found, which is a demanding task in and of itself, the secret data also needs to be encrypted, which can be challenging. One form of steganography is watermarking, which conceals copyright information in a watermark by placing files on top of each other that are difficult to see. This provides copyrighted media with an additional degree of security and aids in preventing fraud. Along with them, there are various methodologies that are used for data hiding during steganography. Some of the methodologies are explained below:

Least Significant Bit (LSB): The most well-known image steganography algorithm is LSB insertion. It entails altering the image's LSB layer. This method stores the message as random noise in the lower-left corner of every pixel. Therefore, altering them has no discernible effect on the image.

Pixel Value Differencing (PVD): The most well-known image steganography algorithm is PVD. The image should be divided into various blocks, each of a certain size. By hiding data in a block, the difference between two pixels is calculated and changed to a new value.

Real Time (RT) Steganography: It is used in the technology of video streaming. While the video is being streamed to another side, the application has the ability to communicate any hidden data (text, binary, etc.) inside the video.

Discrete Wavelet Transform (DWT) Steganography: In DWT-based steganography techniques, the cover image's wavelet coefficients are changed to embed the hidden message. Recently, a DWT-based technique for picture data concealing has been presented, which embeds the cover image's CH band with the hidden message.

As may be shown in table No. 1, there are a few key distinctions between steganography and cryptography.

Table 1: Steganography vs. Cryptography

Factors	**Steganography**	**Cryptography**
Explanation	Cover Writing is referred to as steganography.	Secret writing is referred to as cryptography.
Aim	Maintain communication security	Enable data protection
Integrity	The data's structure has not changed.	Data structures can be changed.
Attack	Steganalysis is the name for an attack in steganography.	Cryptanalysis is the term for an attack in cryptography.
Key	Optional, but when used, improves security	Essential requirement
Data Visibility	No	Yes
Failure	Once secret information has been unlocked, anyone can use the data.	If you have access to the decryption key, the original message can be recovered by deciphering the ciphertext.

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

II. LITERATURE REVIEW

Numerous academics have conducted numerous studies in the past to attempt to address the problem of concealing information while it is being transmitted from the sender to the receiving end. With the help of keywords like encryption, decryption, cryptography, and steganography, the most recent literature was searched. Amin et al. (2003) introduced an image steganographic system employing the LSB technique in their examination of the literature. The use of LSB as a carrier on a digital image, however, has advantages and disadvantages. As a result of how simple it is to integrate the message bits directly into the cover picture's LSB plane, LSB is used in a lot of applications. Another benefit is its perceptual transparency, which makes it impossible for the human eye to detect modifications made to the cover image [1]. Wang and Wang develop tools that can, to some extent, survive both visual and statistical attacks (2004). The secret message can still be extracted by the intended recipient by compensating for changes that result in detectable artefacts after embedding [2]. Juneja and Sandhu discussed robust image steganography in 2009 using LSB (Least Significant Bit) insertion and RSA encryption [3]. The idea of combining encryption with steganography was first presented by Narayana and Prasad in 2010. In addition, a fresh algorithm was suggested to get around steganalysis. The suggested approach offered a higher degree of similarity between the cover and stego images, which also produces a better imperceptibility [4]. Marwaha & Marwaha suggested a complex data encryption system in 2010. It combines the benefits of cryptography, steganography, and multimedia data concealment. However, when data is incorporated in an image, the colour frequencies of the image shift predictably. To avoid this predictability, the authors suggested using multiple cryptography, in which the data is encrypted inside of a cypher and the cypher is hidden within a multimedia image file in encrypted format [5].

Usha et al. (2011) suggested an encryption system that incorporates data concealment, steganography, and cryptographic algorithms. The communication is encrypted twice as opposed to using a single level of data encryption [6]. A fresh approach to integrate data in colour photographs was put forth by Bharti and Soni (2012). This technique demonstrates that it can conceal more data than other techniques while maintaining imperceptibility [7]. In a QR CodeTM, Dey et al. (2012) encode a hidden message. The MSA algorithm's randomization mechanism is employed to generate the embedded QR Code [8]. Abikoye et al. (2012) offer a data concealing system based on audio steganography and cryptography to protect data flow between the source and destination. The LSB (Least Significant Bit) steganography method is used to encode the message within the audio file [9]. Gupta et al. (2012) used the Rivest, Shamir, Adleman (RSA) algorithm and the Diffie Hellman method to encrypt the data [10]. Saeed created a novel method producing colour images in the DCT domain based on text encryption and chaotic steganography (2013) [11]. By using DCT, the original image (cover image) is transformed from the spatial domain to the frequency domain.

Reddy et al. (2013) came up with the concept of merging steganography and cryptography to increase system security by enabling secure communication between two parties. Both encryption and decoding were accomplished using the DES encryption algorithm [12]. In order to create a high security model, Saraireh (2013) combined Steganography and cryptography. The data is encrypted using the filter bank cypher. A symmetric block cypher with great levels of security, scalability, and performance is the filter bank cypher. Using Discrete wavelet transform, encrypted data can be embedded in the cover picture [13]. The Blowfish algorithm was proposed by Sharma et al. (2013) as a method of information encryption. Later, the data was concealed using the LSB method [14]. Thangadurai and Devi released a survey in 2014 outlining how LSB-based picture steganography is understood and how it can be applied to different file formats [15]. Islam et al. (2014) described a method in which a new Steganography methodology is being developed to conceal significant amounts of data in Bitmap images using a filtering-based algorithm that employs MSB bits [16]. In their 2014 paper, Vegh and Miclea proposed a way for maintaining data security and secrecy by combining steganography and cryptography, two of the most popular security techniques. Additionally, they strengthened the overall security of the cyber-physical system and ensured confidentiality by using hierarchical access to information [17].

Kour and Verma (2014) "examined numerous studies on steganography techniques and found that LSB is the most popular steganography approach." In their work, several researchers have also employed techniques including water marking, distortion, spatial, ISB, and MSB, which have produced a potent method for securely transmitting information [18]. Joshi and Yadav (2015) introduced a brand-new technique for spatial domain image steganography using a blend of grayscale images and encryption. To conceal the message and its meaning, respectively, steganography and cryptography are utilised [19]. Mishra and Bhanodiya (2015) noted that although the LSB approach is the most used technique, it has a number of downsides like lowering image quality and arousing suspicions. As a result, they recommended that embedding on the edge area be used to better conceal data" [20]. A novel method of steganography that disguised the data behind an HTML file with a smaller cover size than the one currently used was proposed by Dubey et al. (2015) [21]. Singh and Kaur (2015) proposed a two-layer approach to data security, where the first layer encrypts data using the Advance Encryption Standard Algorithm and the second layer encodes it using the Least Significant Bit image steganography method [22]. Sheth and Tank (2015) provided an overview of the several types of steganography and its traits [23]. In order to improve the data's security, Saleh et al. (2016) suggested combining cryptography and steganography techniques. High embedding capacity and high-quality stego pictures were provided by the suggested technique [24]. By integrating cryptography and Steganographic security, Saritha et al. (2016) created a model with a high level of security. The authors employed the Symmetric XOR algorithm for cryptography and the Sequential algorithm for steganography [25]. Data communication between an IoT device and a home server uses an integrated strategy of lightweight cryptography and steganography (Simple LSB Substitution), and data transport between a home server and an IoT device uses a proposed MSB-LSB Substitution technique. Das and Das (2016) proposed this security scheme to address both of the aforementioned problems.

Sajisha and Mathew (2017) created a new data security technique by combining DNA steganography and AES (Advanced Encryption Standard) cryptography. The secret communication is protected by multiple layers of security using this novel technology [27]. In their 2017 paper, Bangera et al. proposed a method that combines steganography and cryptography to provide multilayer security. A better level of security is offered by the dual audio steganography technique combined with the suggested RSA cryptographic algorithm [28]. In their 2018 paper, Saxena et al. proposed a security method for private data that combines three techniques: first, wavelet-based image compression, which reduces the size of the private image; second, symmetric key cryptography, which encrypts the private image; and third, least significant bit (LSB) steganography, which embeds encrypted data into the private image. Yahya (2019) concentrated on the creation of data-hiding methods for secret data transmission using digital images as the cover medium [30]. In comparison to earlier implementations, Sharma et al. (2019) proposed a novel method for image steganography that is substantially more secure. It makes use of certain standard steganography methods and incorporates them with cryptography and neural networks to make it difficult to crack [31].

III. PROPOSED METHODOLOGY

This study introduced a hybrid security technique that hides the secret text using visual cryptography and LSB image steganography. To conceal shares in other cover images, color image steganography is employed and cover up secret text in cover images. For splitting the cover image into two shares, use visual cryptography. The secrecy, trustworthiness, and effectiveness of covert communications are considerably improved by these security protocols. The accuracy of the received text data is calculated in terms of MSE and correlation coefficient by comparing the transmitted and received text data, even if there isn't a parameter to indicate the level of security attained by utilizing cutting-edge methods. To evaluate the effectiveness of the suggested methodology, the time required at the transmitter and receiver ends is also evaluated. The MATLAB environment is used in the implementation to show how the proposed method has increased resilience when taking steganalysis into account.

To understand the working of the proposed method, a suitable block diagram is given below:

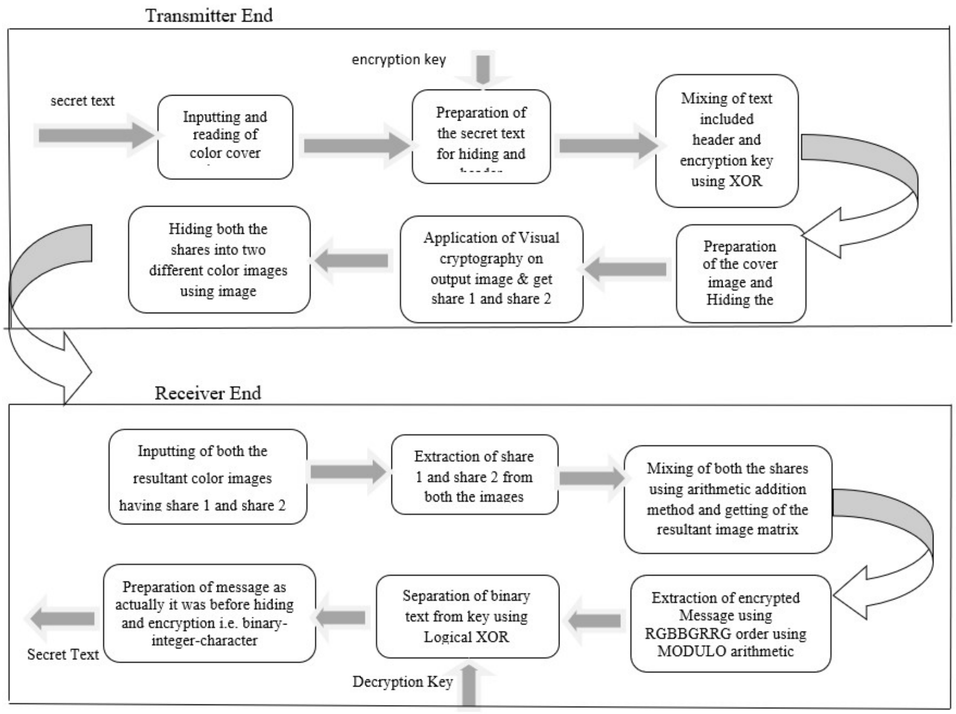

Transmitter End
encryption key
secret text
Inputting and reading of color cover
Preparation of the secret text for hiding and
Mixing of text included header and encryption key using XOR
Hiding both the shares into two different color images using image
Application of Visual cryptography on output image & get share 1 and share 2
Preparation of the cover image and Hiding the
Receiver End
Inputting of both the resultant color images having share 1 and share 2
Extraction of share 1 and share 2 from both the images
Mixing of both the shares using arithmetic addition method and getting of the resultant image matrix
Preparation of message as actually it was before hiding and encryption i.e. binary-integer-character
Separation of binary text from key using Logical XOR
Extraction of encrypted Message using RGBBGRRG order using MODULO arithmetic
Secret Text
Decryption Key

Fig 3: Block diagram for the suggested technique

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

Transmitter End

Inputting and reading of color cover images to hide the text.

1. Inputting and reading the secret text
2. Preparation of the secret text and a header for keeping essential information (type and size of text).

   - The transformation of text into corresponding ASCII Integer Values.
   - Calculating the message's length or the text message's character count.
   - Making a heading that will be in the text message.
   - Place the Header at the message's start.
   - Calculate the message size for header encoding.
   - If there are less than 4 lines of text, pad the header with zeros.
   - Horizontal Concatenation of Headers and Messages.

3. Inputting and reading the cover image.
4. Preparation of the cover image and Hiding the secret text using LSB steganography.

- Initializing some Counters, i.e., rm, gm, and bm.
- Calculate the 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.

- Use the image channel-wise (RGBBGRRG) Order to conceal the data points. Logical AND and OR operations are used to hide encoded secret data bits along columns that traverse the target binary coversheet image from left to right.
- Picking bits of secret messages 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

5. Determining whether or not the image has ended. The next step is to move to the next column and reset the pattern to the first row. You never know when you'll get there, so you have to check this every time you increment the rm/gm/bm .

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

7. Hiding both shares in two distinct 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 three separate variables to each layer matrix, red, green, and blue.
5. Recovering the Header Set from the final image.
6. Initializing the rm, gm, and bm Counters for the recovery procedure.
7. Analysis of header by determining the text data Dimensions from Header Values.
8. Extract the encrypted Message from the resultant image using RGBBGRRG order using MODULO arithmetic.
9. Determining if we've reached the image's end or not. After that, we must switch to the subsequent column and restart the top row of our pattern. We must check this EVERY time after increasing the rm, gm, and bm counters because we have no idea when we will arrive at this stage
10. Separation of binary text from header using horizontal de-concatenation.
11. Converting binary to integer and integer to a character using ASCII values in order to prepare the message to be displayed as it is, before hiding and encryption.
12. Writing the message that was extracted to the TXT file 12.
13. Computation of performance assessment matrices i.e. MSE, correlation coefficient, and Computational time.

IV. EXPERIMENTAL RESULTS AND DISCUSSIONS

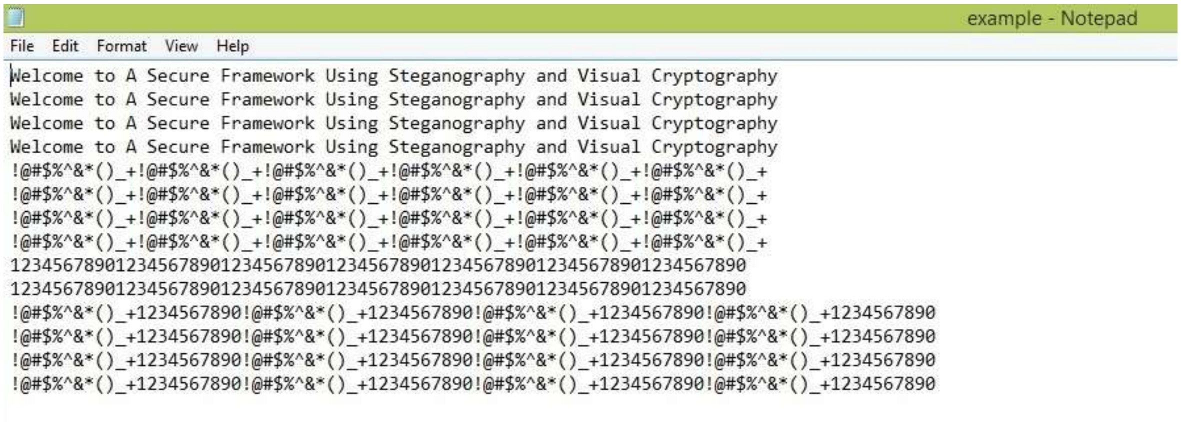
This research presented a hybrid security technique that uses LSB image steganography and visual cryptography to conceal the secret text. Color image steganography is used to hide shares in other cover images and cover up secret text in cover images. For splitting the cover image into two shares, use visual cryptography. The secrecy, trustworthiness, and effectiveness of covert communications are considerably improved by these security protocols. The accuracy of the received text data is calculated in terms of MSE and correlation coefficient by comparing the transmitted and received text data, even if there isn't a parameter to indicate the level of security attained by utilizing cutting-edge methods. To evaluate the effectiveness of the suggested methodology, the time required at the transmitter and receiver ends is also evaluated. The MATLAB environment is used in the implementation to show how the proposed method has increased resilience when taking steganalysis into account.

To assess the viability of the suggested approac, a significant number of special characters, digits, and characters have been employed in the secret Text, whose content is purposefully maintained unpredictably. The images below display the results of each important stage.

Firstly the input cover color image is inputted to cover the secret Text.

Fig 4: Input cover color image

Next, the secret Text is inputted having 2KB size. The secret Text's content is intentionally kept random, and a significant amount of special characters, numbers, and characters have been used to test the efficiency of the proposed method.



```
Welcome to A Secure Framework Using Steganography and Visual Cryptography
Welcome to A Secure Framework Using Steganography and Visual Cryptography
Welcome to A Secure Framework Using Steganography and Visual Cryptography
Welcome to A Secure Framework Using Steganography and Visual Cryptography
!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+
!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+
!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+
!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+
1234567890123456789012345678901234567890123456789012345678901234567890
1234567890123456789012345678901234567890123456789012345678901234567890
!@#$%^&*()_+1234567890!@#$%^&*()_+1234567890!@#$%^&*()_+1234567890!@#$%^&*()_+1234567890
!@#$%^&*()_+1234567890!@#$%^&*()_+1234567890!@#$%^&*()_+1234567890!@#$%^&*()_+1234567890
!@#$%^&*()_+1234567890!@#$%^&*()_+1234567890!@#$%^&*()_+1234567890!@#$%^&*()_+1234567890
!@#$%^&*()_+1234567890!@#$%^&*()_+1234567890!@#$%^&*()_+1234567890!@#$%^&*()_+1234567890
```

Fig 5: Secret texts to be hidden

Initial ASCII Integer Values that are comparable to the inputted Text are then created. After that, a header is developed to go with the text message. The header, which is placed purposefully before the text, carries crucial information like 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 cover image's binary counterpart is then generated. Using image channel-wise (RGBBGRRG) Order, the prepared secret text is then hidden behind each cover image layer. By employing 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. One by one, the components of the secret messages are selected, and the corresponding component of the cover picture is modified specifically.

- If the secret text corresponding bit is 0, change using the logical AND operation.
- If the secret text corresponding bit is 1, change using the logical OR operation.

Using visual cryptography, the cover image is split into two shares, share1 and share2. The following figures 3 and 4 display both shares.

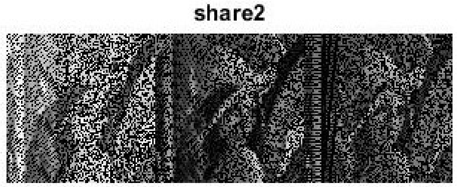


Fig 6: Share 1 extracted after visual cryptography

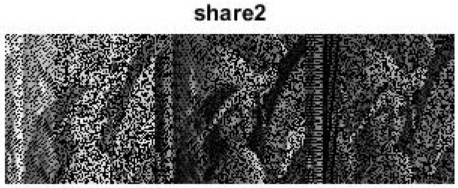


Fig 7: Share 2 extracted after visual cryptography

Using the sequential learning algorithm of image steganography, the shares are concealed in two distinct color cover images. As both claims are to be given to the receiver with an additional degree of security, this is done on purpose. Figures 5 and 6 show the cover pictures for shares 1 and 2, respectively.

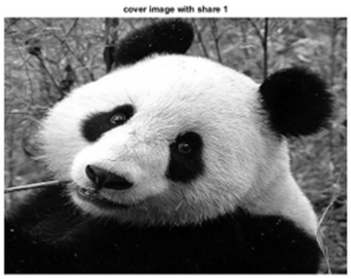


Fig 8: Cover image with Share 1

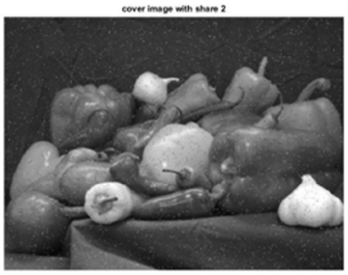


Fig 9: Cover image with Share 2

The recipient side receives both cover images. Using a reverse image steganography technique known as sequential decoding, the shares, i.e., share 1 and share 2, are recovered from both cover images.

The mathematical addition method is used to combine both extracted shares, and the resulting image matrix is calculated. The resultant matrix, known as Share12, is shown in the figure. low.

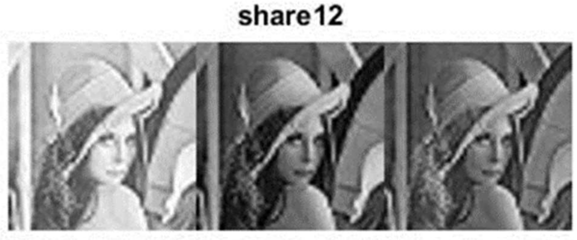
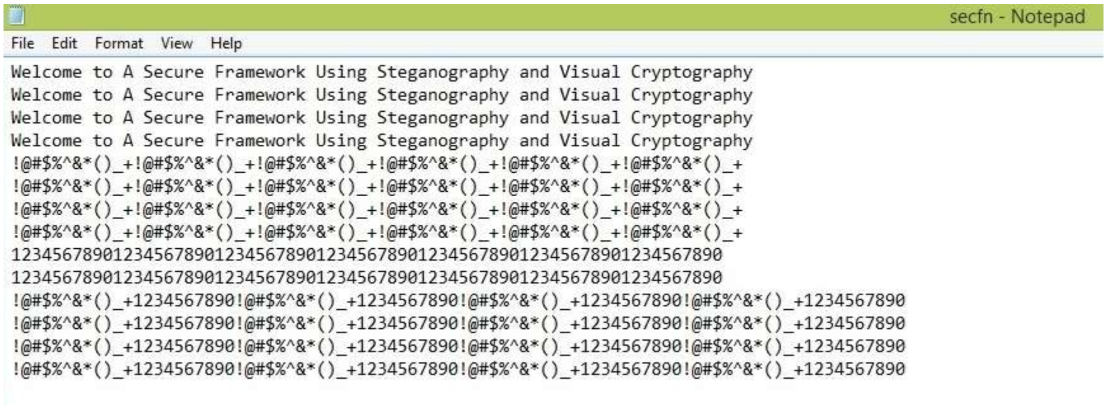


Fig 10: combinations of both shares

To determine the text data sizes, the Header Set from the resulting image must first be retrieved. From the resultant image, the encrypted message is retrieved using RGBBGRRG order and modulo arithmetic.   The next step is to get the message ready to be displayed, which involves converting binary to integer and integer to a character using ASCII values (as before concealing and encrypting). In figure 8, the extracted Text is shown.



```
Welcome to A Secure Framework Using Steganography and Visual Cryptography
Welcome to A Secure Framework Using Steganography and Visual Cryptography
Welcome to A Secure Framework Using Steganography and Visual Cryptography
Welcome to A Secure Framework Using Steganography and Visual Cryptography
!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+
!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+
!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+
!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+!@#$%^&*()_+
1234567890123456789012345678901234567890123456789012345678901234567890
1234567890123456789012345678901234567890123456789012345678901234567890
!@#$%^&*()_+1234567890!@#$%^&*()_+1234567890!@#$%^&*()_+1234567890!@#$%^&*()_+1234567890
!@#$%^&*()_+1234567890!@#$%^&*()_+1234567890!@#$%^&*()_+1234567890!@#$%^&*()_+1234567890
!@#$%^&*()_+1234567890!@#$%^&*()_+1234567890!@#$%^&*()_+1234567890!@#$%^&*()_+1234567890
!@#$%^&*()_+1234567890!@#$%^&*()_+1234567890!@#$%^&*()_+1234567890!@#$%^&*()_+1234567890
```

Fig 11: Extracted secret text at the receiver end

The accuracy of the received text data is calculated by comparing the transmitted and received text data, even if there is no parameter to show the level of security attained using the proposed methodology and comparing it with cutting-edge approaches. Additionally, it computes how long it will take the proposed method to hide and extract at the transmitter and receiver ends, respectively. Both factors might be used as evaluation criteria to determine whether the proposed method is effective. To show all the input and output parameters at once, a table is created.

Table 2: 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	example.txt (2 KB)	Lena.jpg (7 KB)	Panda.jpg (124 KB)	fruit.jpg (94 KB)	2 KB	0	1	10.0469	10.5625
2	thesis.txt (2 KB)	Panda.jpg (6 KB)	fruit.jpg (94 KB)	Lena.jpg (99 KB)	2 KB	0	1	9.0625	8.3445
3	project.txt (2 KB)	fruit.jpg (8 KB)	Lena.jpg (99 KB)	Panda.jpg (124 KB)	2 KB	0	1	11.2969	11.3525

A bar chart has also been created to help you comprehend the values of the computational time performance assessment parameter (at the receiver and transmitter end). Figure 9 and Figure 10 provide an analysis of the computing time at the transmitter and reception ends, respectively.

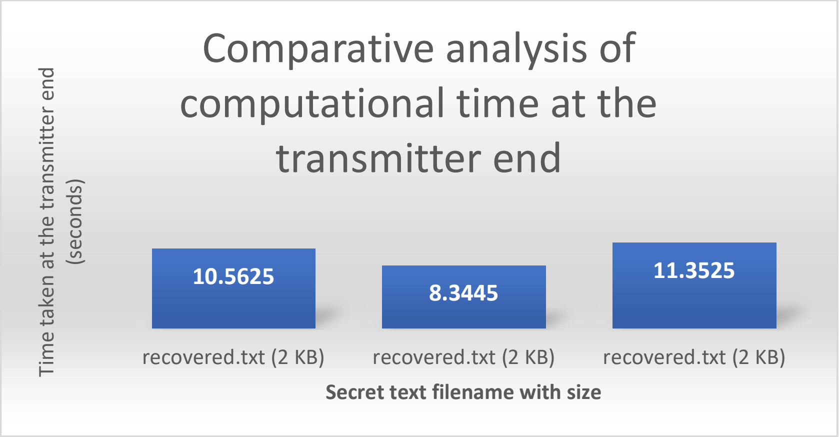


Fig 12: Comparative analysis of computational time at the transmitter end

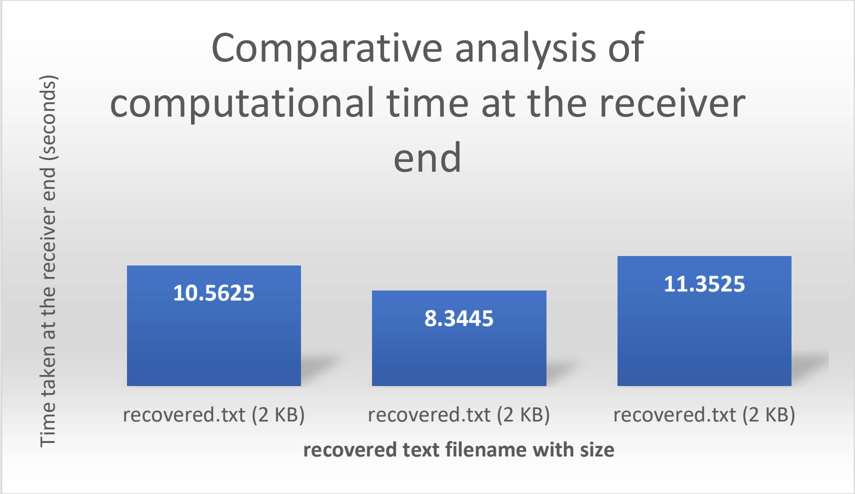


Fig 13: Comparative analysis of computational time at the receiver end

The aforementioned table and both bar graphs clearly show how successful the suggested method is. The calculated values of the performance evaluation parameters demonstrate that the proposed hybrid technique creates no error and complete consistency between the extracted and input text. The proposed process incorporates two security steps for concealing the secret Text, which is the first thing that stands out. Despite this, the proposed method generates flawless, perfectly matching content. The second item that stands out is the need that the cover image used to conceal the share or Text to be greater than the value being concealed.

Additionally, there is little delay between the transmitter and receiver ends. The proposed method performs too quickly, taking not more than 11 seconds (including manual image and text selection and putting up the file name) to hide the Text and not more than 11 seconds (including manual image and text selection and putting up the file name) to extract the Text, despite the two steps involved in doing so.

V. CONCLUSION AND FUTURE SCOPE

This proposed research presents a hybrid approach to text data security. The suggested approach hides the secret Text in two stages and extracts it in two steps. Examining the experimental results from the section before, it was found that the suggested strategies work well. The suggested hybrid approach produces perfect concordance between the extracted and input text and no errors, according to the estimated values of the performance assessment parameters. Additionally, processing the text data only takes a short period at both the transmitter and receiver ends. Despite requiring two stages, the proposed technique works too rapidly, taking no longer than 11 seconds to hide the Text and no longer than 11 seconds to extract the Text (including manual image and text selection and putting up the file name).

Future iterations of the proposed work might be enhanced by encrypting the inputted text before embedding it in the cover image. The degree of security would increase from two levels to three as a result.

REFERENCES

1. Amin, M. M., Salleh, M., Ibrahim, S., Katmin, M. R., & Shamsuddin, M. Z. I. (2003, January). Information hiding using steganography. In *4th National Conference of Telecommunication Technology, 2003. NCTT 2003 Proceedings.* (pp. 21-25). IEEE.
2. Wang, H., & Wang, S. (2004). Cyber warfare: steganography vs. steganalysis. *Communications of the ACM*, *47*(10), 76-82.
3. Juneja, M., & Sandhu, P. S. (2009, October). Designing of robust image steganography technique based on LSB insertion and encryption. In *2009 International Conference on Advances in Recent Technologies in Communication and Computing* (pp. 302-305). IEEE.
4. Narayana, S., & Prasad, G. (2010). Two new approaches for secured image steganography using cryptographic techniques and type conversions. *Signal & Image Processing: An International Journal (SIPIJ) Vol*, *1*.
5. Marwaha, P., & Marwaha, P. (2010, July). Visual cryptographic steganography in images. In *2010 Second international conference on computing, communication and networking technologies* (pp. 1-6). IEEE.
6. Usha, S., Kumar, G. S., & Boopathybagan, K. (2011, December). A secure triple level encryption method using cryptography and steganography. In *Proceedings of 2011 International Conference on Computer Science and Network Technology* (Vol. 2, pp. 1017-1020). IEEE.
7. Bharti, P., & Soni, R. (2012). A new approach of data hiding in images using cryptography and steganography. *International Journal of Computer Applications*, *58*(18).
8. Dey, S., Mondal, K., Nath, J., & Nath, A. (2012). Advanced steganography algorithm using randomized intermediate QR host embedded with any encrypted secret message: ASA_QR algorithm. *International Journal of Modern Education and Computer Science*, *4*(6), 59.
9. Abikoye Oluwakemi, C., Adewole Kayode, S., & Oladipupo Ayotunde, J. (2012). Efficient data hiding system using cryptography and steganography. *International Journal of Applied Information Systems IJAIS411 pp. 6*, *11*.
10. Gupta, S., Goyal, A., & Bhushan, B. (2012). Information hiding using least significant bit steganography and cryptography. *International Journal of Modern Education and Computer Science*, *4*(6), 27.
11. Saeed, M. J. (2013). A new technique based on chaotic steganography and encryption text in DCT domain for color image. *Journal of Engineering Science and Technology*, *8*(5), 508-520.
12. Reddy, V. L., Subramanyam, A., & Reddy, P. C. (2013). A Novel Approach for Hiding Encrypted Data in Image, Audio and Video using Steganography. *International journal of computer applications*, *69*(15).
13. Saraireh, S. (2013). A secure data communication system using cryptography and steganography. *International Journal of Computer Networks & Communications (IJCNC) Vol*, *5*.
14. Sharma, M. H., MithleshArya, M., & Goyal, M. D. (2013). Secure image hiding algorithm using cryptography and steganography. *IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN*, *13*(5), 1-6.

15. Thangadurai, K., & Devi, G. S. (2014, January). An analysis of LSB based image steganography techniques. In *2014 International Conference on Computer Communication and Informatics* (pp. 1-4). IEEE.
16. Islam, M. R., Siddiqa, A., Uddin, M. P., Mandal, A. K., & Hossain, M. D. (2014, May). An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography. In *2014 International Conference on Informatics, Electronics & Vision (ICIEV)* (pp. 1-6). IEEE.
17. Vegh, L., & Miclea, L. (2014, May). Enhancing security in cyber-physical systems through cryptographic and steganographic techniques. In *2014 IEEE International Conference on Automation, Quality and Testing, Robotics* (pp. 1-6). IEEE.
18. Kour, J., & Verma, D. (2014). Steganography techniques–A review paper. *International Journal of Emerging Research in Management & Technology*, *3*(5), 132-135.
19. Joshi, K., & Yadav, R. (2015, December). A new LSB-S image steganography method blend with Cryptography for secret communication. In *2015 Third International Conference on Image Information Processing (ICIIP)* (pp. 86-90). IEEE.
20. Mishra, R., & Bhanodiya, P. (2015, March). A review on steganography and cryptography. In *2015 International Conference on Advances in Computer Engineering and Applications* (pp. 119-122). IEEE.
21. Dubey, R., Saxena, A., & Gond, S. (2015). An innovative data security techniques using cryptography and steganographic techniques. *IJCSIT) International Journal of Computer Science and Information Technologies*, *6*(3), 2175-2182.
22. GNDU RC, J. (2015). Dual layer security of data using LSB Image steganography method and AES encryption algorithm. *International Journal of Signal Processing, Image Processing and Pattern Recognition*, *8*(5), 259-266.
23. Sheth, R. K., & Tank, R. M. (2015). Image steganography techniques. *International Journal Of Computer Engineering And Sciences*, *1*(2), 10-15.
24. Saleh, M. E., Aly, A. A., & Omara, F. A. (2016). Data security using cryptography and steganography techniques. *International Journal of Advanced Computer Science and Applications*, *7*(6).
25. Saritha, M., Khadabadi, V. M., & Sushravya, M. (2016, October). Image and text steganography with cryptography using MATLAB. In *2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)* (pp. 584-587). IEEE.
26. Das, R., & Das, I. (2016, September). Secure data transfer in IoT environment: Adopting both cryptography and steganography techniques. In *2016 Second International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)* (pp. 296-301). IEEE.
27. Sajisha, K. S., & Mathew, S. (2017, April). An encryption based on DNA cryptography and steganography. In *2017 International Conference of Electronics, Communication and Aerospace Technology (ICECA)* (Vol. 2, pp. 162-167). IEEE.
28. Bangera, K. N., Reddy, N. S., Paddambail, Y., & Shivaprasad, G. (2017, May). Multilayer security using RSA cryptography and dual audio steganography. In *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)* (pp. 492-495). IEEE.

29. Saxena, A. K., Sinha, S., & Shukla, P. (2018). Design and development of image security technique by using cryptography and steganography: a combine approach. *International Journal of Image, Graphics and Signal Processing*, *10*(4), 13.
30. Yahya, A. (2019). Introduction to steganography. In *Steganography Techniques for Digital Images* (pp. 1-7). Springer, Cham.
31. Sharma, K., Aggarwal, A., Singhania, T., Gupta, D., & Khanna, A. (2019). Hiding data in images using cryptography and deep neural network. *arXiv preprint arXiv:1912.10413*.