*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 10s*
*DOI: https://doi.org/10.17762/ijritcc.v11i10s.7634*
***Article Received:** 03 June 2023 **Revised:** 29 July 2023 **Accepted:** 11 August 2023*

# Triple Layered Security for Data Hiding Using Steganography and Visual Cryptography

**Bhawna[1], Sanjay Kumar Malik[2]**
[1]Department of CSE, SRM University, Delhi-NCR, Sonipat, Haryana, India,
bhawnachhabra1983@gmail.com
[2]Department of CSE, SRM University, Delhi- NCR, Sonipat, Haryana, India
skmalik9876@gmail.com

**Abstract**—The proposed system makes use of steganographic method along with visual cryptography for hiding data in images and to provide better security. Even though extensive research work has been done previously, but most of the research work gives no robust security for the image that has been encrypted. The method proposed in this paper is capable of hiding some secret message in least significant bits of the original image, thereby hiding the secret message in way to make its detection difficult. The secret image is then under went to visual cryptography algorithm. Thereby, creating shares of the secret image, which are noise like structures. Further, the method proposes to hide these shares in least significant bits of different images so as to create three levels of security for the message. The main objective of the proposed method is to combine the use of data hiding techniques, steganography and visual cryptography algorithms for designing a secure algorithm so that security, reliability and efficiency of secret message can be improved. The framework is implemented in matlab.

## I. INTRODUCTION

Digital images are one of the most important data that is transferred over these networks. Some important solutions of secure communication for data images such as secret key cryptography, watermarking, secret sharing schemes, etc. are presented [19, 20, 21]. Image encryption is applied to secure the communication with digital images. Traditional image encryption schemes encrypt the image based on mathematical algorithms using some keys. Image decryption without the keys is impossible and image data cannot be retrieved correctly. One of the disadvantages of image encryption schemes is that the decryption process requires computing devices.

Focusing on this matter, Naor and Shamir proposed a new cryptographic scheme for binary images called Visual Cryptography (VC) [17]. Contrary to traditional encryption schemes, VC does not have any keys. Visual cryptography is applied to encrypt a binary image into two separate binary images called shares that are apparently random, and reveal no information about the original image. Shares are generated based on the original image pixels values; and Human Visual System (HVS) is the decryption device. To achieve this, encrypted images are generated block by block corresponding to each pixel in the original image. Table 1 illustrates an example of blocks that are used in share images. If the pixel in original image is white, both blocks placed in encrypted images are the same, as well as if the pixel is black, blocks values are adverse. Blocks for both black and white pixels are shown in table 1. Superposing shares results a fully black pixel block for each black pixel in the original image; and a pixel block with black sub-pixels for each white pixel. Using transparency specification and HVS ability, original image is revealed if the encrypted images are superposed correctly

TABLE 1: BLOCKS USED IN SHARES AND STACKING RESULTS

| Secret pixel | White | Black |
|---|---|---|
| Share 1 | | |
| Share 2 | | |
| Stacking result | | |

. Figure 1 illustrates an example of shares obtained for a secret image and the image retrieved after superimposing the obtained shares.

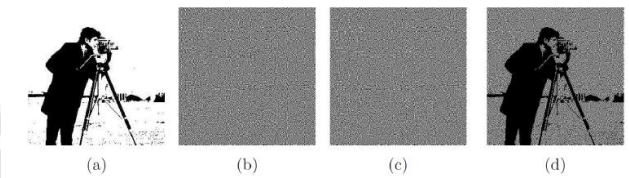



Figure 1: Binary visual cryptography
(a) Cameraman binary image ; (b) Share 1; (c) Share 2; (d) Retrieved image;

Steganography is a technique that is used for hiding the secret by immersing it into an innocuous medium [9]. Steganography was used many years back when messages were hidden on things of everyday use, eg: watermarks on letters, carvings on bottom sides of tables, and other objects. But nowadays this concept has emerged with the dawn of the digital world. It has already been proved in that we can hide data inside different digital files like image, audio, video files [8] in different ways. The main benefit of the method steganography is that just

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 10s*
*DOI: https://doi.org/10.17762/ijritcc.v11i10s.7634*
***Article Received:** 03 June 2023 **Revised:** 29 July 2023 **Accepted:** 11 August 2023*

sender and receiver are aware of the existence of the hidden information; but to all others, the object carrying the hidden information seems like just a normal object.

Unfortunately, when using steganography alone it will be quite easy for an intruder to decrypt the secret message. For image security, both the topics of steganography and visual cryptography have been considered as a distinct one. The use of steganography in combination visual cryptography is a powerful model for providing security to data [7] and adds a lot of challenges in identifying such hidden and encrypted data. A lot of work has been done to provide dual layer security to data[1][2][4][6] but no one gives satisfactory results. To add on security to data we can hide data in three layers.

The main objective of the proposed framework is to improve security, reliability, and efficiency for secret message.

## II. LITERATURE REVIEW

Steganography is a data hiding technique that can use any cover medium to hide the information. In [1] the authors considered text as the secret information. They text was hide using DES encryption algorithm. The key used for encryption was hidden using RSA algorithm. The algorithm provided two layers of security to the secret information. First by hiding the secret using DES algorithm and secondly by hiding the key using RSA algorithm. The algorithm proposed provides high reliability.

Visual cryptography and steganography are both data hiding techniques and abundant research is being done in these areas. In [2] the authors presented a method that combines the concept of steganography and visual cryptography. The secret is encrypted using Matrix embedding method and hamming code method. Shares of secret were generated using Random Grid method. Since there is no pixel expansion using Random Grid method, so secret was completely obtained from the shares. The idea presented by authors can be used in research areas in the field of forensics.

With rise in internet, communication has increased and so is the need of security and privacy , as a lot of confidential information is being shared over internet. In [3] the authors proposed double layer security to data using the concept of visual cryptography and steganography. The authors implemented the work using Matlab. First the hide the secret using visual cryptography to create shares and then in second layer of security they used steganography to embed the share in images. The main advantage of the system obtained is that computation time for decryption is just for one level.

In [4], the authors used the concept of visual cryptography and steganography for hiding the secret. The authors encoded the cover message and encrypted secret message as noise-like structures using (2, 2) VC where concept of digital invisible ink of steganography is used with VC (DIIVC) to hide the secret message. Unlike classical steganography, shares are modified to hide secret message instead of cover image. At receiver side, decryption of shares is performed using conventional Visual Cryptography, which results in poor contrast of the cover image. The receiver decrypts the secret from the obtained cover image by using the proposed algorithm. Finally, using the secret key, the original secret message is revealed.

Cryptography and steganography are two different techniques to hide the data from intruders. No technique is much effective alone and can be compromised. In [6], authors presented a system that provides double layer security to data using DCT steganography and visual cryptography. First layer of security uses visual cryptography and second layer of security is provided using DCT steganography. The proposed method has advantage as it requires computation time for one level only. The method can be used in online transactions and various online contracts.

## III. SYSTEM ARCHITECTURE

For creating the proposed framework, existing methods have been analyzed. There are few techniques that can be used to implement steganography and visual cryptography, both together. From them a superlative technique can be developed by analyzing the existing methods, which are implemented using the known techniques. Each method/technique has got their own pros and cons. Using the existing methods of both steganography and visual cryptography a more effective algorithm can be developed[7], which could be better for sharing the secret information over unreliable network. As, mentioned both steganography and cryptography have pros and cons. Whenever these algorithms are used standalone one could only have single level of security which can easily be broken by eavesdroppers. By combining the features of both visual cryptography and steganography we would have two levels of security. So, by using these two methods together we are hiding the hidden data, which ensures multi level of security**.** So, here we suggest blending of both steganography and visual cryptography. The main virtue of visual cryptography is that there is no computation involved for decryption of the encrypted data. Visual cryptography doesn't work with any key[11]. It can be well perceived through human visual system (HVS). What we require is, only the required number of shares of the original information which are created during encryption. Types of VC schemes differ in pixel expansion and contrast [12].

Previously the technique used for encrypting information is either cryptography or steganography. But here we used both. A lot of work has been done using both techniques but with visual cryptography the image obtained after decryption is distorted[13] so it is not possible to obtain the secret message hidden inside the image. In proposed method we tried to obtain

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 10s*
*DOI: https://doi.org/10.17762/ijritcc.v11i10s.7634*
*Article Received: 03 June 2023 Revised: 29 July 2023 Accepted: 11 August 2023*

the same secret image containing hidden data after applying XOR operation. The algorithm is as follows. Initially, the information which is going to be transmitted over unsecure channel is encrypted using steganography. So there we achieve first level of security. Then the image containing hidden data is encrypted using visual cryptography. This gives second level of security. Finally, the obtained shares are embedded in other images, using steganography. That gives third level of security. Hence multilevel security is achieved.

### *A. 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 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 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.

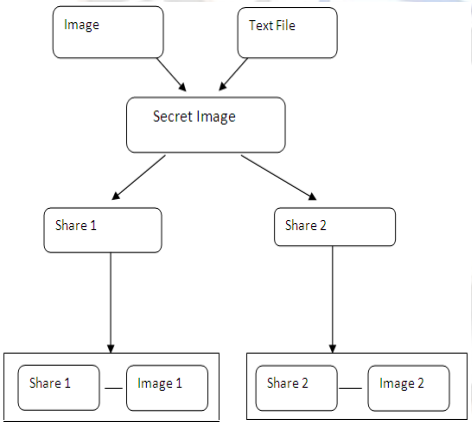



Figure 2: Hiding data and slicing of image

1. Choose Image to be encrypted, say Mi.
2. Choose the text to be hiding.
3. Using the method of text steganography (LSB Method) hide the text file into the image file (Here we get first level of security).
4. The image (Mi) is divided into n shares using visual cryptography (here we get second level of security)
5. Each share will be treated as information.
6. Shares obtained by visual cryptography are hidden inside separate images..
7. Select an appropriate images so that the shares of the original image can be embedded into selected images. Instead of sending the shares immediately they will be embedded into an image or images. (Here we get third level of security).

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.

### *B. Decoding Process*

The decoding process is carried out at receiver's side. 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. At the first step, 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. After this the receiver applies the decryption process of steganography to decode the secret text from the obtained secret image. Figure 3 shows the complete decoding process.

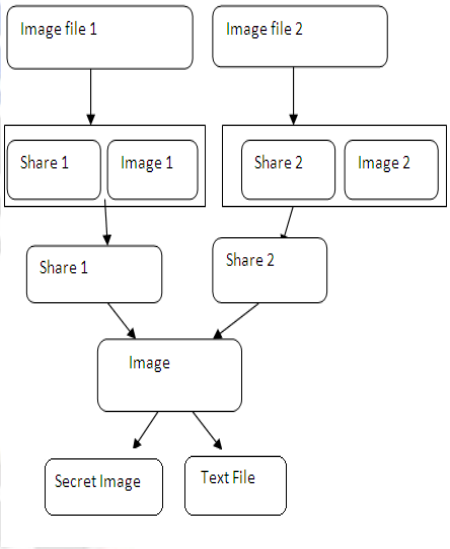



Figure 3: Extracting hidden data from shares

1. 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).
2. The obtained shares can then be decrypted without the use of any complex computation. We only need to super impose these shares on one another so that we will get the original image, containing the hidden information (for that XOR operation is used).

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 10s*
*DOI: https://doi.org/10.17762/ijritcc.v11i10s.7634*
*Article Received: 03 June 2023 Revised: 29 July 2023 Accepted: 11 August 2023*

### *C. Algorithm*

**Function steganography(image, message, key)**

1. Read the image and transform it into grayscale. Resize if needed
2. Read the secret message and transform it into binary format
3. Initialize output image same as input image
4. Fir each pixel of the image perform the following:
   - Transform the pixel to its binary value
   - Read the next bit of the secret message to be hidden
   - Create a temporary variable, temp
   - If the message bit and the LSB of the pixel are same, set temp = 0 else set temp=1
   - Update the pixel of output image as

     output image pixel value=input image pixel value + temp
5. Repeat till all the bits in the message are embedded
6. Write the output image.

**function visual(output)**

1. Read the image.
2. Read the ASCII values of pixels of image and no of rows and columns of image
3. Create share1 and share2 images with same number of rows and columns and with value zero.
4. Read the ASCII value of each pixel of image
5. If the value of pixel is odd then store that pixel in share1 else in share2.[rows , cols] = size(output);

## IV. SYSTEM DESCRIPTION

The sender who wants to send the secret information/message to the receiver initiates the encryption process. The sender firstly applies the encryption process of LSB steganography for hiding the secret information/message inside an image. The sender then uses the concept of visual cryptography to make multiple shares of the secret image obtained at first step. For obatining shares the concept of even odd pixel is applied on the secret image. Then sender applies the concept of LSB steganography for hiding the obtained shares in different images. With this the sender achieves the three level of security. The obtained two secret images are then forwarded to the receiver's side. Figure 4 shows the complete system model.

At the receiver side the reverse process of the one applied by the sender is applied. The receiver receives the two secret images. The reciver firstly decrypts the obtained secret images by applying the decryption process of LSB steganography for obtaining the shares. Next the receiver applies the decryption process of visual cryptography for obtaining the original secret images. For this the receiver alligns the obtained shares by Bit ORing of the shares. Now the receiver has the secret image containing the hidden information/message. The receiver now applies the decryption process of LSB steganography for extracting the hidden secret information/message from the secret image.

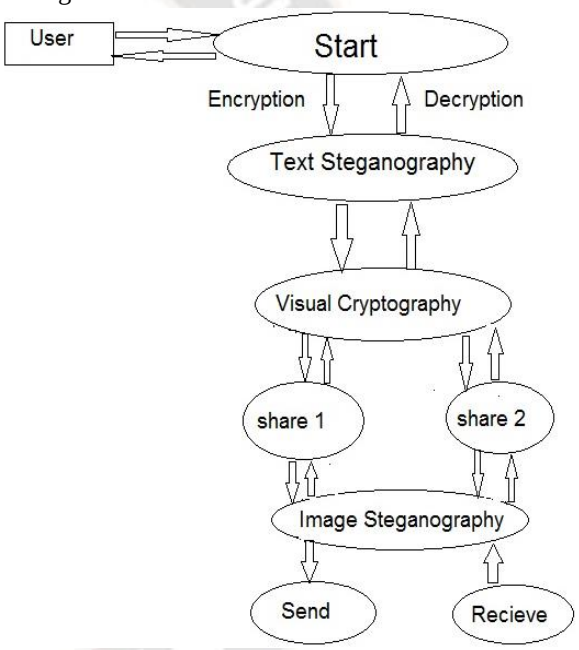



Figure 4: System Model

## V. RESULTS AND DISCUSSIONS

The framework is implemented and data is encrypted successfully. The results are shown in terms of matrix representation of pixel values of images and ASCII values of text file used. Figure 5 – Figure 14 shows the result obtained at different levels and Table 2 depicts the comparison of different sizes of text files and images.

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 10s*
*DOI: https://doi.org/10.17762/ijritcc.v11i10s.7634*
*Article Received: 03 June 2023 Revised: 29 July 2023 Accepted: 11 August 2023*

### *A. Encryption Process*

**a) Data Confidentiality:** Hide data in image

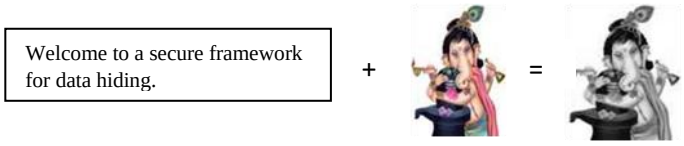



Figure 5: Data Confidentiality

**Secret message**

**87** 101 108 99 111 109 101 32 116 111 32 86
67 83 58 32 65 32 78 101 119 32 83 101
99 117 114 105 116 121 32 70 114 97 109 101
119 111 114 107

+

**Original image** (The actual matrix of image is 100*86*3. For reference here we are showing a part of matrix only.)

**255 255** 255 255 255 255 255 255 255 255 255 255 255
255 255 255 255 255 255 255 255 255 255 255 255 255
255 255 255 255 255 255 255 255 255 255 255 255 255
255 255 255 255 255 255 255 255 255 255 255 255 255
255 255 255 255 255 255 255 255 255 255 255 255 255

=

**Secret image** (The actual matrix of image is 100*86)

**254 255** 254 255 254 255 255 255 254 255 255 254 254
255 254 255 254 255 255 254 255 255 254 254 254 255
255 254 254 254 255 255 254 255 255 254 255 255 255
255 254 255 255 254 255 255 254 255 254 255 255 254
255 255 254 254 254 254 255 254 254 254 254 254 254

**b) Image Slicing (Visual Cryptography)**

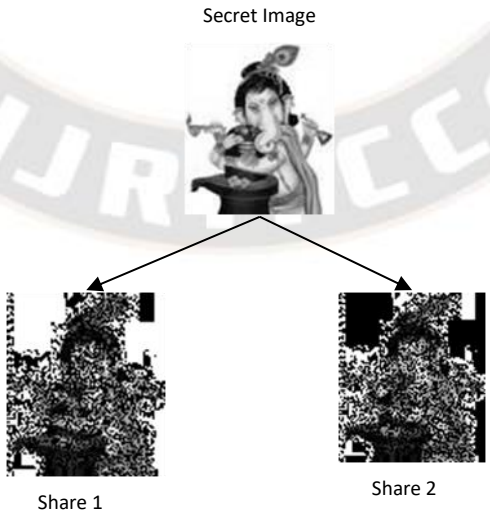



Figure 6: Shares of image

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 10s*
*DOI: https://doi.org/10.17762/ijritcc.v11i10s.7634*
*Article Received: 03 June 2023 Revised: 29 July 2023 Accepted: 11 August 2023*

**Secret image** (The actual matrix of image is 100*86)

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **254** | **255** | 254 | 255 | 254 | 255 | 255 | 255 | 254 | 255 | 255 | 254 | 254 |
| 255 | 254 | 255 | 254 | 255 | 255 | 254 | 255 | 255 | 254 | 254 | 254 | 255 |
| 255 | 254 | 254 | 254 | 255 | 255 | 254 | 255 | 255 | 254 | 255 | 255 | 255 |
| 255 | 254 | 255 | 255 | 254 | 255 | 255 | 254 | 255 | 254 | 255 | 255 | 254 |
| 255 | 255 | 254 | 254 | 254 | 254 | 255 | 254 | 254 | 254 | 254 | 254 | 254 |

=

**Share 1** (The actual matrix of image is 100*86)

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **0** | **255** | 0 | 255 | 0 | 255 | 255 | 255 | 0 | 255 | 255 | 0 | 0 |
| 255 | 0 | 255 | 0 | 255 | 255 | 0 | 255 | 255 | 0 | 0 | 0 | 255 |
| 255 | 0 | 0 | 0 | 255 | 255 | 0 | 255 | 255 | 0 | 255 | 255 | 255 |
| 255 | 0 | 255 | 255 | 0 | 255 | 255 | 0 | 255 | 0 | 255 | 255 | 0 |
| 255 | 255 | 0 | 0 | 0 | 0 | 255 | 0 | 0 | 0 | 0 | 0 | 0 |

**&**

**Share 2** (The actual matrix of image is 100*86)

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **254** | **0** | 254 | 0 | 254 | 0 | 0 | 0 | 254 | 0 | 0 | 254 | 254 |
| 0 | 254 | 0 | 254 | 0 | 0 | 254 | 0 | 0 | 254 | 254 | 254 | 0 |
| 0 | 254 | 254 | 254 | 0 | 0 | 254 | 0 | 0 | 254 | 0 | 0 | 0 |
| 0 | 254 | 0 | 0 | 254 | 0 | 0 | 254 | 0 | 254 | 0 | 0 | 254 |
| 0 | 0 | 254 | 254 | 254 | 254 | 0 | 254 | 254 | 254 | 254 | 254 | 254 |

**c) Hiding share1**


Figure 7: Hiding Share1

**Cover image1** (The actual matrix of image is 240*320*3)

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **244** | **244** | **248** | **253** | **249** | **248** | **253** | **255** | 254 | 255 | 255 | 255 |
| 242 | 242 | 247 | 252 | 238 | 239 | 243 | 246 | 248 | 248 | 252 | 251 |
| 244 | 243 | 249 | 254 | 236 | 239 | 241 | 243 | 243 | 242 | 243 | 243 |
| 246 | 247 | 253 | 255 | 246 | 248 | 250 | 250 | 246 | 242 | 240 | 238 |
| 246 | 246 | 252 | 255 | 254 | 255 | 255 | 255 | 255 | 251 | 248 | 246 |

+

**Share 1** (The actual matrix of image is 100*86)

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **0** | 255 | 0 | 255 | 0 | 255 | 255 | 255 | 0 | 255 | 255 | 0 | 0 |
| 255 | 0 | 255 | 0 | 255 | 255 | 0 | 255 | 255 | 0 | 0 | 0 | 255 |
| 255 | 0 | 0 | 0 | 255 | 255 | 0 | 255 | 255 | 0 | 255 | 255 | 255 |
| 255 | 0 | 255 | 255 | 0 | 255 | 255 | 0 | 255 | 0 | 255 | 255 | 0 |
| 255 | 255 | 0 | 0 | 0 | 0 | 255 | 0 | 0 | 0 | 0 | 0 | 0 |

=

**Secret image containing hidden share1** (The actual matrix of image is 240*320)

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **244** | **244** | **248** | **252** | **248** | **248** | **252** | **254** | 255 | 255 | 255 | 255 |
| 243 | 243 | 247 | 253 | 238 | 238 | 242 | 246 | 248 | 248 | 252 | 250 |
| 245 | 243 | 249 | 255 | 237 | 239 | 241 | 243 | 242 | 242 | 242 | 242 |
| 246 | 246 | 252 | 254 | 247 | 249 | 251 | 251 | 247 | 243 | 241 | 239 |

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 10s*
*DOI: https://doi.org/10.17762/ijritcc.v11i10s.7634*
*Article Received: 03 June 2023 Revised: 29 July 2023 Accepted: 11 August 2023*

**d) Hiding share2**


Figure 8: Hiding Share2

**Cover image2** (The actual matrix of image is 1800*2800*3)

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **205** | **206** | **207** | **206** | **207** | **207** | **207** | **206** | 206 | 208 | 208 | 209 |
| 203 | 204 | 208 | 205 | 206 | 206 | 206 | 207 | 206 | 202 | 201 | 200 |
| 206 | 206 | 209 | 209 | 206 | 204 | 207 | 209 | 206 | 202 | 200 | 199 |
| 204 | 206 | 205 | 206 | 205 | 204 | 204 | 206 | 203 | 202 | 202 | 202 |
| 200 | 204 | 206 | 199 | 206 | 206 | 204 | 200 | 198 | 199 | 201 | 200 |

+

**Share 2** (The actual matrix of image is 100*86)

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **254** | 0 | 254 | 0 | 254 | 0 | 0 | 0 | 254 | 0 | 0 | 254 | 254 |
| 0 | 254 | 0 | 254 | 0 | 0 | 254 | 0 | 0 | 254 | 254 | 254 | 0 |
| 0 | 254 | 254 | 254 | 0 | 0 | 254 | 0 | 0 | 254 | 0 | 0 | 0 |
| 0 | 254 | 0 | 0 | 254 | 0 | 0 | 254 | 0 | 254 | 0 | 0 | 254 |
| 0 | 0 | 254 | 254 | 254 | 254 | 0 | 254 | 254 | 254 | 254 | 254 | 254 |

=

**Secret image containing hidden share2** (The actual matrix of image is 1800*2880)

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **205** | **207** | **207** | **207** | **207** | **207** | **207** | **206** | 206 | 208 | 208 | 208 |
| 202 | 204 | 208 | 204 | 207 | 207 | 207 | 207 | 207 | 203 | 201 | 200 |
| 206 | 206 | 208 | 208 | 206 | 204 | 206 | 208 | 207 | 203 | 201 | 199 |
| 205 | 207 | 205 | 206 | 204 | 204 | 204 | 206 | 202 | 202 | 202 | 202 |
| 200 | 204 | 206 | 198 | 206 | 206 | 204 | 200 | 198 | 198 | 200 | 200 |

### *B. Decryption Process*

**a) Extracting share1 from secret image1:**


Figure 9: Extracting Share1

**Secret image containing hidden share1** (The actual matrix of image is 240*320)

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **244** | **244** | **248** | **252** | **248** | **248** | **252** | **254** | 255 | 255 | 255 | 255 |
| 243 | 243 | 247 | 253 | 238 | 238 | 242 | 246 | 248 | 248 | 252 | 250 |
| 245 | 243 | 249 | 255 | 237 | 239 | 241 | 243 | 242 | 242 | 242 | 242 |
| 246 | 246 | 252 | 254 | 247 | 249 | 251 | 251 | 247 | 243 | 241 | 239 |

↓

**Share 1** (The actual matrix of image is 100*86)

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **0** | **255** | 0 | 255 | 0 | 255 | 255 | 255 | 0 | 255 | 255 | 0 | 0 |
| 255 | 0 | 255 | 0 | 255 | 255 | 0 | 255 | 255 | 0 | 0 | 0 | 255 |
| 255 | 0 | 0 | 0 | 255 | 255 | 0 | 255 | 255 | 0 | 255 | 255 | 255 |
| 255 | 0 | 255 | 255 | 0 | 255 | 255 | 0 | 255 | 0 | 255 | 255 | 0 |

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 10s*
*DOI: https://doi.org/10.17762/ijritcc.v11i10s.7634*
*Article Received: 03 June 2023 Revised: 29 July 2023 Accepted: 11 August 2023*

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 255 | 255 | 0 | 0 | 0 | 0 | 255 | 0 | 0 | 0 | 0 | 0 | 0 |

**b) Extracting share2 from secret image2:**

Secret image2 containing hidden share2 — Extracted share2

**Secret image2 containing** ⟶ **Extracted Share2 hidden share2**

Figure 10: Extracting Share2

**Secret image containing hidden share2** (The actual matrix of image is 1800*2880)

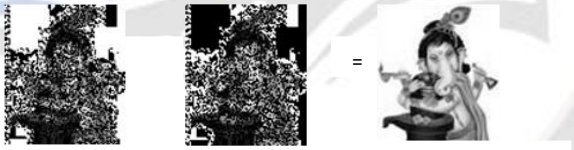
| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **205** | **207** | **207** | **207** | **207** | **207** | **207** | **206** | 206 | 208 | 208 | 208 |
| 202 | 204 | 208 | 204 | 207 | 207 | 207 | 207 | 207 | 203 | 201 | 200 |
| 206 | 206 | 208 | 208 | 206 | 204 | 206 | 208 | 207 | 203 | 201 | 199 |
| 205 | 207 | 205 | 206 | 204 | 204 | 204 | 206 | 202 | 202 | 202 | 202 |
| 200 | 204 | 206 | 198 | 206 | 206 | 204 | 200 | 198 | 198 | 200 | 200 |

↓

**Share 2** (The actual matrix of image is 100*86)

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **254** | 0 | 254 | 0 | 254 | 0 | 0 | 0 | 254 | 0 | 0 | 254 | 254 |
| 0 | 254 | 0 | 254 | 0 | 0 | 254 | 0 | 0 | 254 | 254 | 254 | 0 |
| 0 | 254 | 254 | 254 | 0 | 0 | 254 | 0 | 0 | 254 | 0 | 0 | 0 |
| 0 | 254 | 0 | 0 | 254 | 0 | 0 | 254 | 0 | 254 | 0 | 0 | 254 |
| 0 | 0 | 254 | 254 | 254 | 254 | 0 | 254 | 254 | 254 | 254 | 254 | 254 |

**c) Obtaining the original Secret Image from the extracted shares:**



Extracted share1 — Extracted share2 — = Obtained original secret image

Figure 11: Obtaining Secret Image

**Extracted share1** (The actual matrix of image is 100*86)

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **0** | **255** | 0 | 255 | 0 | 255 | 255 | 255 | 0 | 255 | 255 | 0 | 0 |
| 255 | 0 | 255 | 0 | 255 | 255 | 0 | 255 | 255 | 0 | 0 | 0 | 255 |
| 255 | 0 | 0 | 0 | 255 | 255 | 0 | 255 | 255 | 0 | 255 | 255 | 255 |
| 255 | 0 | 255 | 255 | 0 | 255 | 255 | 0 | 255 | 0 | 255 | 255 | 0 |
| 255 | 255 | 0 | 0 | 0 | 0 | 255 | 0 | 0 | 0 | 0 | 0 | 0 |

**XOR**

**Extracted share 2** (The actual matrix of image is 100*86)

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **254** | **0** | 254 | 0 | 254 | 0 | 0 | 0 | 254 | 0 | 0 | 254 | 254 |
| 0 | 254 | 0 | 254 | 0 | 0 | 254 | 0 | 0 | 254 | 254 | 254 | 0 |
| 0 | 254 | 254 | 254 | 0 | 0 | 254 | 0 | 0 | 254 | 0 | 0 | 0 |
| 0 | 254 | 0 | 0 | 254 | 0 | 0 | 254 | 0 | 254 | 0 | 0 | 254 |
| 0 | 0 | 254 | 254 | 254 | 254 | 0 | 254 | 254 | 254 | 254 | 254 | 254 |

=

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 10s*
*DOI: https://doi.org/10.17762/ijritcc.v11i10s.7634*
*Article Received:* 03 June 2023 *Revised:* 29 July 2023 *Accepted:* 11 August 2023

**Obtained original secret image** (The actual matrix of image is 100*86)

**254 255** 254 255 254 255 255 255 254 255 255 254 254
255 254 255 254 255 255 254 255 255 254 254 254 255
255 254 254 254 255 255 254 255 255 254 255 255 255
255 254 255 255 254 255 255 254 255 254 255 255 254
255 255 254 254 254 254 255 254 254 254 254 254 254

**d) Obtaining the secret message from the secret image :**


Figure 12: Extracting Secret Message

**Obtained original secret image** (The actual matrix of image is 100*86)

**254 255** 254 255 254 255 255 255 254 255 255 254 254
255 254 255 254 255 255 254 255 255 254 254 254 255
255 254 254 254 255 255 254 255 255 254 255 255 255
255 254 255 255 254 255 255 254 255 254 255 255 254
255 255 254 254 254 254 255 254 254 254 254 254 254

↓

**Obtained secret message**

**87** 101 108 99 111 109 101 32 116 111 32 97
32 115 101 32 65 32 78 101 119 32 83 101
99 117 114 105 116 121 32 70 114 97 109 101
119 111 114 107

**e) Comparison of text files containing secret message:**

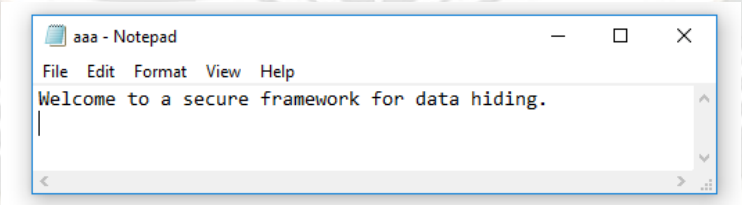



Figure 13: Text file containing secret message at sender's side

**At sender's side : Text file containing secret message**

**87** 101 108 99 111 109 101 32 116 111 32 97
32 115 101 97 117 114 101 32 102 114 97 109
101 119 111 114 107 32 102 111 114 32 100 97
116 97 32 104 105 100 105 110 103 46

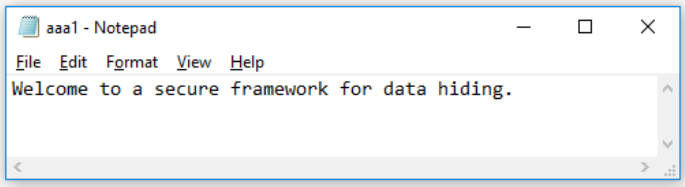



Figure 14: Text file containing secret message at receiver's side

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 10s*
*DOI: https://doi.org/10.17762/ijritcc.v11i10s.7634*
*Article Received: 03 June 2023 Revised: 29 July 2023 Accepted: 11 August 2023*

**At receiver's side : Obtained Text file containing secret message**

**87** 101 108 99 111 109 101 32 116 111 32 97
32 115 101 97 117 114 101 32 102 114 97 109
101 119 111 114 107 32 102 111 114 32 100 97
116 97 32 104 105 100 105 110 103 46

Table 2: Comparison of different sizes of Text files and images

| Cover Image | Text File | Stego File | Share1 | Share2 | Cover Image1 | Cover Image2 | Stego Image1 | Stego Image2 | Retrieve Message |
|---|---|---|---|---|---|---|---|---|---|
| 2.75 KB | 40 Bytes | 9.64 KB | 9.64 KB | 9.64 KB | 19.1 KB | 3338.24 KB | 76 KB | 5058.56 KB | ✓ |
| 2.75 KB | 246 Bytes | 9.64 KB | 9.64 KB | 9.64 KB | 19.1 KB | 3338.24 KB | 76 KB | 5058.56 KB | ✓ |
| 3.34 KB | 40 Bytes | 16.4 KB | 16.4 KB | 16.4 KB | 32.2 KB | 39.5 KB | 250 KB | 333 KB | ✓ |
| 3.34 KB | 246 Bytes | 16.4 KB | 16.4 KB | 16.4 KB | 32.2 KB | 39.5 KB | 250 KB | 333 KB | ✓ |

## VI.CONCLUSION

Steganography and visual cryptography have different uses in the digital and real worlds. There are different methods for steganography and visual cryptography. Each method has its own advantages and power, as well as disadvantages and weaknesses. Certain methods can be compromised easily than others. When both techniques, i.e. steganography and visual cryptography are used together, it is almost impossible for intruders to uncover the encrypted or hidden information. We notice that using an algorithm with a better reconstruction method will allow us to reconstruct shares back into the original, i.e. unaltered image. Till now, visual cryptography has been used along with steganography for hiding the pictorial representation of data and not for hiding the written information. But with the proposed method, written information can be secured and retrieved using these two techniques. This algorithm would present a great area for further exploration which would open up some more venues in the world of data security.

## References

[1] Shreyank N Gowda. Dual Layered Secure Algorithm for Image Steganography. 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT). IEEE 2016.

[2] Aishwarya Nandakumar, P. Harmya, Noopa Jagadeesh, and S.S. Anju. A Secure Data Hiding Scheme Based on Combined Steganography and Visual Cryptography Methods. ACC 2011, Part II, CCIS 191, pp. 498–505, Springer. 2011.

[3] Pallavi B, Vishala I. L. Double Layer Security Using Visual Cryptography and Transform Based Steganography. IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163. pISSN: 2321-7308. Volume: 03 Special Issue: 03.2014.

[4] Yogesh K. Meghrajani, Himanshu S. Mazumdar. Hiding Secret Message Using Visual Cryptography in Steganography. IEEE INDICON 2015.

[5] Souvik Roy and P. Venkateswaran. Online Payment System using Steganography and Visual Cryptography. IEEE. 2014.

[6] M. Wherate, Dr. S. Sherekar, Dr. V. M. Thakre. Two Layer Security Using Visual Cryptography and Steganography. IJARCSSE International Journal of Advance Research in Computer Science and Software Engineering, Vol 5, Issue 4, 2015.

[7] S.M.Poonkuzhali, M.Therasa. Data Hiding Using Visual Cryptography for Secure Transmission. International Journal of Advanced Research in Computer and Communication Engineering. Vol. 4, Issue 4, 2015.

[8] Apurva. S. Mahajan , Prof. Sheetal. G. Khadke. Review on LSB Steganography. International Journal of Computer Science Trends and Technology (IJCST). Vol 3, Issue 2, 2015.

[9] Sumeet Kaur, Savina Bansal, R. K. Bansal. Steganography and Classification of Image Steganography Techniques. IEEE, 2014.

[10] Archana O. Vyas Dr. Sanjay V. Dudul. Study of Image Steganalysis Techniques. International Journal of Advanced Research in Computer Science. ISSN No. 0976-5697, Volume 6, No. 8, 2015.

[11] D. Taghaddos, A. Latif. Visual Cryptography for Gray-scale Images Using Bit-Level. Journal of Information Hiding and Multimedia Signal Processing. SN 2073-4212. Volume 5, Number 1, 2014.

[12] Mr. K. Das, Prof. S. K. Bandyopadhyay. A REVIEW PAPER ON VARIOUS VISUAL CRYPTOGRAPHY SCHEMES. International Journal of Current Research. ISSN: 0975-833X. Vol. 8, Issue, 06, pp.32445-32449, 2016.

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 10s*
*DOI: https://doi.org/10.17762/ijritcc.v11i10s.7634*
*Article Received: 03 June 2023 Revised: 29 July 2023 Accepted: 11 August 2023*

[13] T. Ambritha, J. Poorani Sri, J. Jessintha Jebarani, M. Pradhiba Selvarani. Comparative Study of Various Visual Cryptography Techniques to Analyze the Quality of Reconstruction. International Journal for Research in Applied Science & Engineering Technology (IJRASET). ISSN: 2321-9653. Vol 4 Issue 4, 2016.

[14] Aejaz Farooq Ganai, Farida Khursheed. (2023). Computationally Efficient Holistic Approach for Handwritten Urdu Recognition using LRCN Model. International Journal of Intelligent Systems and Applications in Engineering, 11(4s), 536 –. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2724

[15] Rosziati Ibrahim and Teoh Suk Kuan. Steganography Algorithm to Hide Secret Message inside an Image. Computer Technology and Application 2. pp 102-108, 2011.

[16] Ravikumar M.Raypure, Prof. Vinay Keswani. Implementation For Data Hiding Using Visual Cryptography. International Research Journal of Engineering and Technology (IRJET). Vol: 04 Issue: 07. 2017.

[17] Halim Maulana, Edy Rahman Syahputra. International Conference on Information and Communication Technology. Journal of Physics. 2017

[17] M. Naor, and A. Shamir, Visual cryptography, Proc. of Advances in Cryptology - EUROCRYPT, LNCS 950, Springer, pp. 1-12, 1995.

[18] R. Lukac, and K. N. Plataniotis, Bit-level based secret sharing for image encryption, Journal of Pattern Recognitions, vol. 38, no. 5, pp. 767-772, 2005.

[19] B. Li, J. H. He, J. W. Huang, and Y. Q. Shi, A survey on image steganography and steganalysis, Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, pp. 142-172, 2006.

[20] Z. H. Wang, C. C. Chang, H. N. Tu, and M. C. Li, Sharing a secret image in binary images with veri_cation, Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 1, pp. 78-90, 2008.

[21] A. Latif, and A. R. Naghsh-Nilchi, Digital image watermarking based on parameters amelioration of parametric slant-hadamart transform using genetic algorithm, International Journal of Innovative Computing, Information and Control, vol. 8, no. 2, pp. 1205-1220, 2012.

[22] K. Gurunathan and S. P. Rajagopalan, A stegano - visual cryptography technique for multimedia security, Springer, 2019.

[23] L. Rudraksha and G. Prasad M.N., Advanced Robust Data Hiding Using Visual Cryptography, IEEE, 2019.