Visual Secret Sharing Scheme: Visual Cryptography

Pavani Kadem, Divya Kancharkuntla, Vivek Chowdary Vasireddy, Jyothi Kiranmai Sankuru, Pramod Pamarthi
Southeast Missouri State University -Cape Girardeau
{pkadem1s, dkancharkuntla1s, vvasireddy1s, jsankuru1s, pspamarthi}@semo.edu

Abstract *— Secure Data Sharing Using Visual Cryptography is a kind of secret sharing scheme that fixates on sharing secret data. Visual cryptography is the technique used to encrypt texts, images, and many other types of data so that the image will display the decrypted data. In addition to being used for data concealment, image protection, color imaging, and many other domains, visual cryptography is a form of procedure that also appears in file formats, cybercrime, and other methods of data concealment. The encrypted image is split into n pieces so that the information can only be shared with the n people who have access to the n pieces. Any host photos will have encrypted transparency hidden in them before being shared with the target users. This application applies the sharing of single secrete data and multiple secrete data on ebony and white as well as on color images but with a comparative analysis of visual cryptography schemes with all performed.*[1]

Keywords: *Visual cryptography, Pixel, Encryption, Decryption.*
Tools: CrypTool 2.1 — Visual Cryptography

Introduction

One of the finest methods for data protection is cryptography. Visual Cryptography is a cryptographic technique that allows visual information to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. It is a method that only the transmitter or the recipient can use to help send and receive encrypted data. Data will be encrypted and decrypted with the aid of mathematical methods to ensure that only the intended receiver may access the information. A visual cryptography technique enables safe image sharing without the need for cryptographic computations. The usage of optical cryptography techniques are widespread [1,2]. The description of the visual cryptography scheme can only be done using the human optical system, but it is a sort of procedure that will be useful for the encryption of visual data. The visual encryption method used in digital verse enables the machines to decipher the visual data that is stored as coded and illustrative language. Cryptography is one of the most efficient methods available today for safeguarding sensitive and important data as it travels through the networking communication channel. White and black pixels make up the hidden image. White pixels are represented by 0, whereas black pixels are represented by 1.

Problem Formulation

Motivation

The secret image that contains the important data will be hampered during sharing production, and the picture may experience problems as a result of pixel enlargement. There will be some contrast-related issues with the recovered image or hidden data. For this, we came up with an idea by sharing the same information in two different images with one as a duplicate image and one with the original image. This Visual cryptography helps us to use it in many real-world scenarios like Securing military data, securing bank details, and storing them in encrypting messages.

Overshooting dye to the pixel expansion also reduces the overall quality of the host picture or image. A certain organization can recognize a safe digital transfer according to the idea behind visual cryptography. Moreover, critical information can be protected via visual cryptography against cyber-crime violations and the theft of biometric templates.

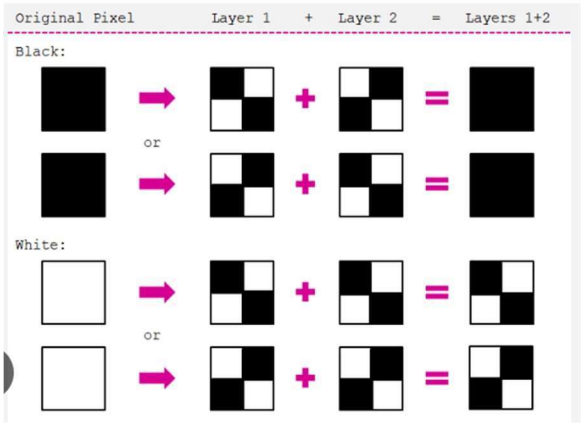


Figure 1: Visual Cryptography

Related Work

First Visual cryptography enrooted by M. Naor and A. Shamir. When shares (images) are merged using OR/XOR operation, the greyed secret image is recovered.

They designed VCS using 4 subpixels, which means one pixel of the original image provokes 4 subpixels in each share. Hence the share size is 4 times the original image.

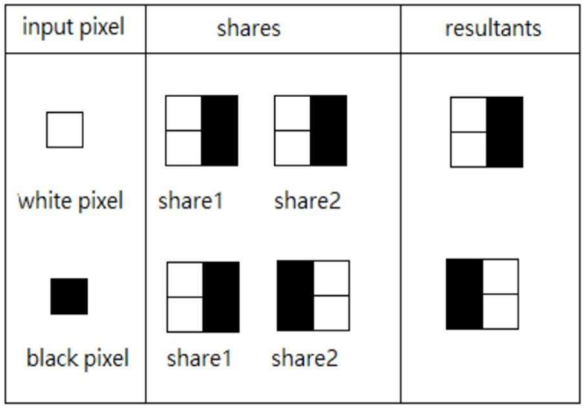


Figure 2: Shares used by Naor andShamir in (2, 2) VCS

Here is some induced share for their (2,2) scheme[5][9] Tai-wen Yue and Chian[13] introduce a modified scheme in which the share dimension is twice of original in a horizontal direction while remaining the same in the vertical direction. Its contrast is the same as Naor and Shamir's 2 out of 2 schemes.

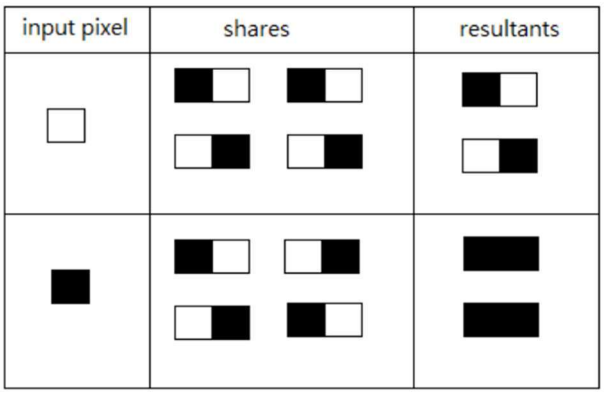


Figure 3: Shares used by Tai-wen andSuchen Chian [8]

D. Jena and S. K. Jena proposed data hiding in halftone images using conjugate ordered dithering DHCOD)[5]. They considered the security of shares [5] in visual cryptography. Firstly, shares are generated using a basic scheme. Then these shares are watermarked [5]with some cover images using DHCOD [5]. The decryption is made by the human visual system. Abhisek Parakh and Subhas Kak proposed a (2, 3) VCS based on a recursive hiding scheme [1],[12]. All the above-mentioned schemes increase the size of shares and loss of visual fidelity.

The following other commercially available tools that share similarities with CrypTool:

1. Crypt: You can drag and drop or open files using Crypt to encrypt them.
2. Cryptext: Cryptext makes it simple to secure your written work and notes. Your messages' content is protected by Cryptext using the AES algorithm.
3. U2F Zero: A USB token that functions with any service that supports U2F, such as Google services, is known as U2F Zero. It is effective for two-factor authentication and occasionally even for password replacement. No need for drivers. Simply plug it in and click on the button
4. Mbed TLS: The GPLv2 or private mbed TLS library is a dual-licensed implementation of the SSL and TLS protocols, along with the necessary support code and corresponding cryptographic algorithms.
5. SecureBlackBox: For software developers, SecureBlackbox is a library (set of parts and classes) that enables secure data transit and storage, digital signature and verification, encryption, and compression.

Design of Experiments

Security Attacks, and Risks Scenario

Visual cryptography techniques were exclusively utilized for black-and-white graphics up to the end of the 1990s. The development of a colored visual cryptography scheme requires ongoing study and work on the part of researchers. The relationships created between the stacked subpixels will determine the hue of the pixels. The actual color-hidden image does not lend itself to the pixel expansion strategy. They want toproduce an image with reduced noise in order to blend a modest notion into the coloredphotos. Schemes for visual cryptography will get rid of the specifics of computing issues during the decryption process [3,4]. The property will produce valuable pictures to meet the demand for the computational load. The Sina Gas Field is not the only place where visual cryptography is applied.

It is applicable to many different things, including voting, bank customer identification, biometric security, and watermarking. Criminals use a variety of techniques, including encryption and other techniques like password encryption, to conceal information from law enforcement. Therefore, it's not necessary to comprehend

how criminals operate to come up with a fix for the problem. Multimedia applications can potentially make use of visual cryptography. Visual cryptography is mostly utilized in the multimedia industry to encrypt or safeguard valuable data.

The ideal encryption system consists of two independent components; the first element primarily entails taking the messages and conjugating them with a key to create anencrypted message. The other half, on the other hand, deals with the conversion of ciphertext into plain text during the decryption process. In this situation, a simple brute attack largely makes use of automation techniques and scripts to try to guess the passwords needed to decrypt the file. By using such automated scripts, simple passwords can be quickly encrypted.

To avoid brute force attacks on their system, the majority of the organization uses a range of small and uppercase alphabets with a combination of numbers and symbols.

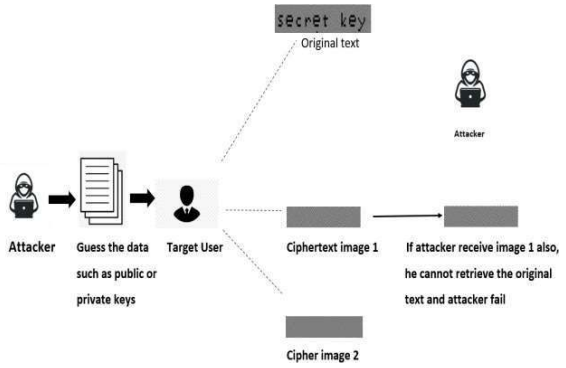


Figure 4: Attack Scenario

Encryption Process

The least significant bit (LSB) from each pixel is mostly used in an encryption procedure to hide unimportant information. The total number of bits chosen from the red, green, and blue pixel colors are all completely different. After the concealing procedure is complete, the images of the other paints will likewise be transformed into red, green, and bite-colored matrices and restored. The red matrix will startthe concealment process, followed by the greenand blue matrices. Every pixel's value is compared to the average of its corresponding colors in the up, down, right, and left directions[7]. The comparison is primarily designed to determine how close neighbors and pixels resemble one another, making it simple to determine the overall amount of concealing bits.

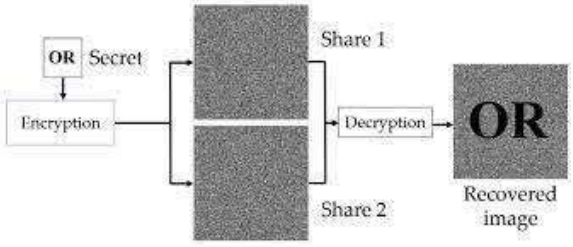


Figure 5 : Encryption and Decryption in CrypTool.

Decryption Process

Each of the three-color matrices is searched in turn during the decryption process, going over the lines of every row and column. Examining the average value will also help determine the number of bits used. In the encryption procedure, the average of

four neighbors will be used as the definition. To create the original message, the canceled values will beseparated and concatenated.

Each of the three-color matrices is searched in turn during the decryption process, going over the lines of every row and column. Examining the average value will also help determine the number of bits used. In the encryption procedure, the average of four neighbors will be used as the definition. To create the original message, the canceled values will beseparated and concatenated.

The personal image, encryption, cover image, data concealing, and host image are all steps in the decryption procedure for the secret picture hidden in the cover image.

The description and the concealed picture are shared during the decryption process for the inverse data hiding from the host image and inverse data hiding to obtain the secret (SHARMA, 2012).

With the aid of strong keys and carrier pictures, encryption primarily entails converting straightforward, readable communications into an unintelligible message version [8]. Decryption, on the other hand, describes the procedure for returning an encrypted, unintelligible message to its original, plain-text format.

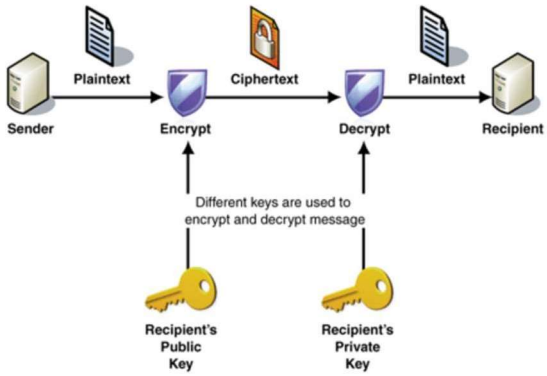


Figure 6: Encryption and Decryption process in Cryptography

A private key is necessary for both the overall encryption and decryption of the data and is what makes them work. The perfect key is created using primal knowledge that can only be known by the senders and receivers of the cryptic messages. In this method, the networking communication system's users' data transfer procedure is made more secure.

Design Diagram

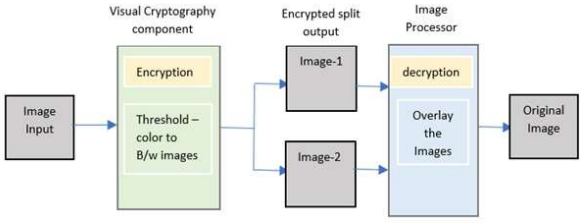


Figure 7: Design diagram of Visual Cryptography using Cryptool.

The above figure shows the process of visual cryptography for a given input into a cryptool. The input can be text or an Image. Once it is connected to the Visual cryptography component, it encrypts the input and splits it into two images. By giving a threshold value, we can convert the color images into black-and-white images. Once the encrypted output is received at the receiver end, the image processor decrypts the encrypted image by overlaying the two output images.

Platform and Tools

CrypTool 2.1 (CT2) is the modern successor of CryptTool 1, a well-known e-learning platform for cryptography and cryptographic analysis. It provides an interface for creating workflows by adding and combining different elements (plugins) in a project. Users can drag deployed components (for input, output, and cryptographic functions) into the workspace and link them together, or use a predefined template. The resulting model can be executed, where the corresponding operations are computed. Some components also have an internal image, called a layout. The plugins in CT2 are programmed in the C# programming language, using the Microsoft .NET framework.

Implementation

Image encoding and decoding

Consider a text image in black and white as the input for encoding. When a color image is binaryized, a binary image is produced. White pixels are denoted by 0, whereas black pixels are

represented by 1. Use larger-size fonts for text images for the best results. Encode every black-and-white pixel in the text image. Replace each black pixel (1) with two subpixels in the secret image; the distribution of the subpixels

for each black pixel will differ between the ciphertext images 1 and 2. The distribution of the subpixels in the ciphertext images 1 and 2 will be the same in the case of a white pixel (zero) in the secret image.

A 100% pure white pixel becomes a 50% white pixel, or half black and half white, in the secret image by swapping out the white pixel for a subpixel that is half white and half black. Consequently, a white pixel in the hidden image is converted to a gray pixel in the combined image (Images 1 and 2). This is the cause of the loss of contrast between the original image and the reconstructed image. The secret message and the ciphertext pictures will both be rebuilt in order to decipher the image.

Open the crypTool 2.1 version and look for visual cryptography to start using the project. Visual cryptography opens in a new window when it is selected. There are the following: plain text, visual cryptography, converters, ImageProcess, ciphertext image 1 and image 2 as well as Image1+ Image 2.

Any text can be used as Plaintext. After selecting plain text, click the Play button located in the page's top header. The images are then generated. The Image visual cryptography follows the same procedure. The input is the only difference. Then, we drag the file input option onto the workspace from the left-side menu. After choosing the input button, the location of the image is fed into the file input.

Algorithm

1. Start
2. Take any encrypted message (text, image, etc.) and convert it to plaintext.
3. Use the visual cryptography encryption method.
4. Expand the pixel size
5. Create images of ciphertext.
6. Store every ciphertext image that was created.
7. Stack each image of the ciphertext.
8. Stop.

Experiment Results

Our findings are based on a visual cryptography system. The submitted image can be of any size and in any format, and the original image is in its binary form in this

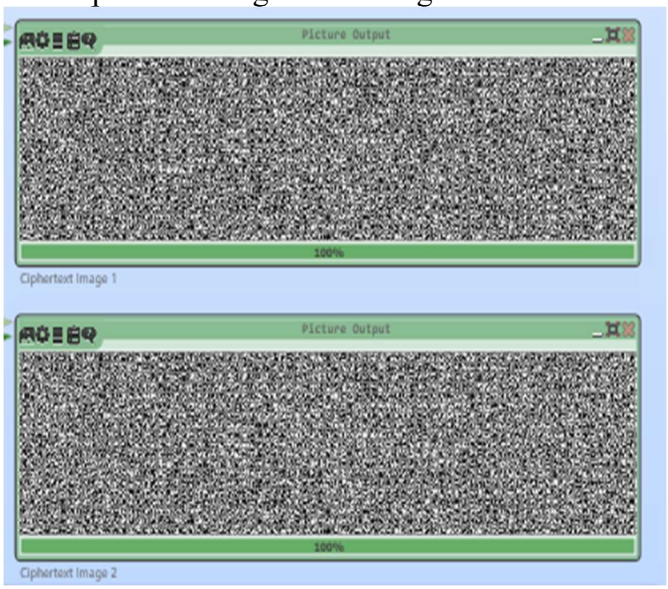
scheme. The built image's contrast can be further enhanced. Setting the Threshold value, which maintains the aspect ratio of the sub-pixels to their respective pixel, can improve the contrast in the experimental results. This threshold improves the quality of the image by maintaining the aspect ratio of the pixel to its subpixel. We must preserve the aspect ratio of the pixel to its subpixels in order to increase the quality of the produced image.

Text:

PlainText: The secret key:7DF9A0C3115FAD9

Visual Cryptography :

The Ciphertext image 1 and image 2 would be:



The whole process can be depicted as:

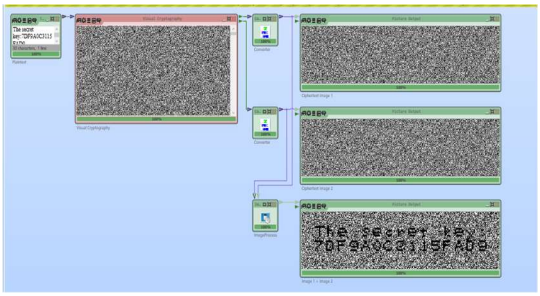


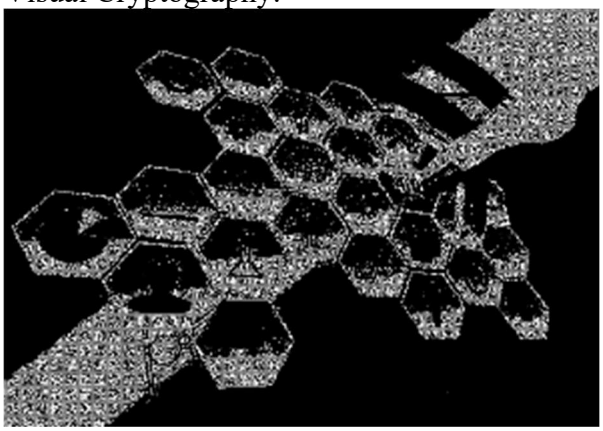
Figure 8(a) Implementation of Visual Cryptography for a text format

The reconstructed image quality can be altered by the threshold value. When the threshold value is higher, the image is sharpened and thus the quality is higher.

Image:

Plaintext (File Input):

Visual Cryptography:



The whole process:

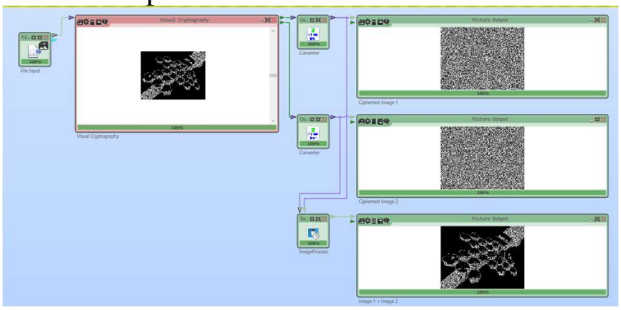


Figure 8(b) Implementation of Visual Cryptography for Image Format

Advantages:

1. Simple to use: Even those without a technical background can easily construct visual cryptography schemes thanks to CrypTool's user-friendly interface.
2. Simple algorithms are sufficient: With the straightforward technique of visual cryptography, messages can be encoded and decoded without the use of complicated algorithms. It is therefore perfect for applications where efficiency and simplicity are crucial.
3. Robustness: Shares that are resistant to visual attacks like rotation, translation, and scaling can be made using visual cryptography.

Visual cryptography does not necessitate the decoding of the encoded information. It's perfect for cases where the parties involved don't want to share their secret keys because of this.

Limitations:

1. Limited capacity: The ability to encode secret information using visual cryptography is limited. The size of the secret message has an exponentially increasing effect on the number of shares needed to encrypt it.
2. Limited security: Stacking and correlation attacks can be used against visual cryptography. The encrypted message's security may be jeopardized as a result.
3. Limited adaptability: The types of communications that can be encoded using visual cryptography are not very diverse. It works best for encoding binary messages, such as graphics in black and white.

Visual cryptography is difficult to employ for encoding huge amounts of information, which limits its practical application. It works best when encoding brief binary messages.

Performance analysis of the visual cryptography schemes

Many new factors are suggested by the researchers in order to assess the overall effectiveness of visual cryptography methods. The two primary parameters proposed by Naorand Shamir are in

conflict with the pixel expansion m. The total number of developed pixels, or "pixel expansion m," is what refers tothe pixels in the primary input image. Also, it will indicate specifics regarding the whole resolution loss from the primary image to the shared image [10]. Another relative weight differential between several combined shares ofthe white and black pixels in an original or print is called contrast. Security, pixel expansion, computing complexity, and accuracy are the main performance indicators. The assurance has been met, thus the disclosed information will show all of the information from the original image. When a few shares are gathered, the original notion won't be shown. Accuracy is regarded as a secret image as well, and the PSNR metric will be used to assess it. The number of operations required to create the set of n shares and alter or restore the original image is what raises concerns about computational complexity. Schemes for visual cryptography should always support several formats, including color and grayscale.

The random-looking stakes in above figure 8 will also seem suspicious, and they are always vulnerable to the other attacks made by attackers in the middle to fill the security issues or gaps; also, many more significant shares will be developed. If the scheme supports only sharing the single secret simultaneously for sharing multiple images, then many claims are to be generated, transferred and maintained.

The table outlines all pertinent information as well as the association of the values obtained from the hidden image and the recovered private vision. As the XOR operations will be carried out and the protected picture will be retrieved throughout the stacking process, it has also produced a negative value. Distinct weights are formed in contrast and are reversed. While comparing the two images, a negative value will also emerge.

The degree of communication and processing complexity was typically used to evaluate cryptographic techniques. The degree to which a cryptographic system performs in a structured environment is influenced by important variables such as processing speed, memory size, energy consumption, and communication overhead [9]. Based on the noted factors, a security system is said to operate at its peak levels if it can achieve the related objectives in terms of service availability, reliability, integrity, confidentiality, and authenticity.

Comparative Analysis

A variety of visual cryptography schemes are presented, and they ultimately depend on the overall aesthetic of a person's appearance and the nature of the connection. Every time a visual cryptography system is employed, it is regarded as a one-time use or non-reusable one-time password.

Comparison

The wang system is explicitly compared in the below table in terms of the overall number of shares, kind of protected picture, size of a share, computational complexity, type of claims, and capability of verification.

Criteria	Wang scheme	Proposed scheme
Total number of shares	N=2	N = 3
Style of the protected image	Greyscale image or the Binary	Binary
Size of share	n	2n
Computational complexity	Low	Lesser
Style of the share	Noise type shares	Noise the shares
Verifying ability	No	Yes

Conclusion/ Outline for the finalworking model

The internet has rapidly expanded into the world's fastest communication system and media. Several companies have found it difficult to keep up with the current dangers and difficulties due to the internet's constant evolution as a communication medium.

The major purpose of the visual cryptography system used to share the secret image is to make the decryption procedure more user-friendly [11,12]. Also, it is a simple procedure that doesn't call for technical expertise. To prevent suspicion

of the secret picture, all the encrypted images are copied into the host image. Inverse data hiding involves receiving a portion of the image from the host image while keeping the hidden concept. A median filter will be used to filter a personal photo to enhance its overall quality.

References :

[1] A. Sharma, "Performance of Error Filters in Halftone Visual Cryptography", International Journal on Cryptography and Information Security, vol. 2, no. 3, pp. 143-159, 2012. Available: 10.5121/ijcis.2012.2313.
Fu Z, Cheng Y, Yu B. Visual cryptography scheme with meaningful shares based on QR codes. IEEE Access. 2018 Oct 8;6:59567-74.
Geeksforgeeks.org(2018,Feb)"Visual Cryptography | Introduc——tion" Available at: https://www.geeksforgeeks.org/visual- cryptography-introduction/ [Acessed on: 05/05/2022]

[2] Ibrahim DR, Teh JS, Abdullah R. An overview of visual cryptography techniques. Multimedia Tools and Applications. 2021Sep;80(21):31927- 52.

[3] K. Uno and H. Dung, "Visual Cryptography by Speckle Pattern Illumination," Journal of the Institute of Industrial Applications Engineers, vol. 4, no. 1, pp. 26-32, 2016. Available: 10.12792/jiiae.4.26.

[4] Kumar T, Chauhan S. Image cryptography with matrix array symmetric key using chaos- based approach. International Journal of Computer Network and Information Security. 2018 Mar 1;10(3):60.

[5] R. K, "Secure Data Transfer: Based on Steganography and Visual Cryptography", International Journal of Engineering and Computer Science, 2017.Available:10.18535/ijecs/v6i5.5.

[6] Rachmawanto EH, Sari CA, Susanto A, Doheir M. A comparative study of image cryptographic method. In2018 5th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE) 2018 Sep 27 (pp. 336-341). IEEE.

[7] Taha MS, Rahim MS, Lafta SA, Hashim MM, Alzuabidi HM. Combination of steganography and cryptography: A short survey. InIOP conference series: materials science and engineering 2019 May 1 (Vol. 518, No. 5, p.052003). IOP Publishing.

[8] Ateniese, G., Blundo, C., De Santis, A., Stinson, D.R.: Visual cryptography for general access structures. Information and Computation 129(2), 86–106 (1996)

[9] Yang, C.N., Chen, T.S.: New size- reduced visual secret sharing schemes with half reduction of shadow size. IEICE Transactions 89-A(2), 620–625 (2006)

[10] Yang, C.N., Chen, T.S.: Visual secret sharing scheme: Improving the contrast of a recovered image via different pixel expansions. In: Campilho, A., Kamel, M.S.(eds.) ICIAR 2006. LNCS, vol. 4141, pp. 468–479. Springer, Heidelberg (2006)

[11] Luo, H., Pan, J.S., Lu, Z.M.: Hiding multiple watermarks in transparencies of visual cryptography. Intelligent Information Hiding and Multimedia Signal Processing 1, 303–306 (2007)

[12] Leung, B.W., Ng, F.Y., Wong, D.S.: On the security of a visual cryptography scheme for color images. Pattern Recognition (August 2008)

[13] CrypTool 2. Wiki for CrypTool 2 developers. url:https://www.cryptool.org/trac/CrypTool2/wiki/WikiStart

[14] CrypTool 2. CrypTool 2 - CrypTool Portal. url: https://www.cryptool.org/ en/cryptool2

Team members	Contributions
Pavani Kadem	Problem formulation,Related work, Design Diagram and IEEE formatting.
Divya Kancharkuntla	Implementation , Experiment and Results.
Pramod Pamarthi	Design of experiments, encryption, and decryption.
Jyothi Kiranmai Sankuru	Abstract , Introduction and Motivation.
Vivek Chowdary Vasireddy	Performance analysis of visual cryptography schemes and conclusion.

Video Link:
https://youtu.be/GuEuxevM0nE