Project Report
on

Visual Cryptography

Submitted in the partial fulfillment of the requirements for the award of Degree of B. Tech

By

Aashutosh Sehgal(1606810007)

Abhinav Chaudhary(1606810012)

Aditya Sangwan(1606810027)

Ajay Sharawat(1606810038)

Under the Supervision of:-

Mr.Vishal Jayaswal
(Assistant professor, Department of CSE)

Department of Computer Science & Engineering
Meerut Institute of Engineering and Technology,
Meerut – 250 005

Dr. A.P.J. Abdul Kalam Technical University, U.P., Lucknow

[2016-20]

DECLARATION

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgment has been made in the text.

Signature :AASHUTOSH SEHGAL
Name : Aashutosh Sehgal
Roll No. :1606810007
Date :26/04/2020

Signature :ABHINAV CHAUDHARY
Name :Abhinav Chaudhary
Roll No. :1606810012
Date :26/04/2020

Signature :ADITYA SANGWAN
Name :Aditya Sangwan
Roll No. :1606810027
Date :26/04/2020

Signature :AJAY SHARAWAT
Name :Ajay Sharwat
Roll No. :1606810038
Date :26/04/2020

CERTIFICATE

This is to certify that *Project Report entitled* —*Visual Cryptography A Secure Medium* which is submitted by *Aashutosh Sehgal (1606810007), Abhinav Chaudhary (1606810012), Aditya Sangwan (1606810027), Ajay Sharawat (1606810038)* in partial fulfillment of the requirement for the award of degree B. Tech. in Department of Computer Science Of Dr. A.P.J. Abdul Kalam Technical University, U.P., Lucknow., is a record of the candidate own work carried out by him under my supervision. The matter embodied in this Project report is original and has not been submitted for the award of any other degree.

Date: 26/04/2020

Supervisor: Mr. Vishal Jayaswal
Designation: Assistant professor
CSE dept.

ACKNOWLEDGEMENTS

It gives us a great sense of pleasure to present the report of the B. Tech Project undertaken during B.Tech. Final Year. We owe special debt of gratitude to our guide Prof. (Mr. Vishal Jayaswal), Department of Computer Science, Meerut Institute of Engineering and Technology, Meerut for his constant support and guidance throughout the course of our work. His sincerity, thoroughness and perseverance have been a constant source of inspiration for us. It is only his cognizant efforts that our endeavors have seen light of the day.

We also do not like to miss the opportunity to acknowledge the contribution of all faculty members of the department for their kind assistance and cooperation during the development of our project. Last but not the least, we acknowledge our friends for their contribution in the completion of the project.

LIST OF FIGURES

ABSTRACT

The Project is elaborate description of Visual cryptography using Python Language to distribute the image (here Grey scale and B&W) in two share such the image can be shared secretly between sender and receiver without any unauthorized person getting the hint of what's been shared. In the multimedia Cryptography system, the message will first be encrypted using public key encryption algorithm, and then this encrypted data will be hidden into an image file thus accomplishing both data encoding and hiding. The multimedia data will be used to provide the cover for the information. Cryptography involves converting a message text into an unreadable cipher. On the other hand, Cryptography embeds message into a cover media and hides its existence. Both these techniques provide some security of data neither of them alone is secure enough for sharing information over an unsecure communication channel and are vulnerable to intruder attacks. Although these techniques are often combined together to achieve higher levels of security but still there is a need of a highly secure system to transfer information over any communication media minimizing the threat of intrusion. In this paper we propose an advanced system of encrypting data that combines the features of cryptography, Cryptography along with multimedia data hiding. This system will be more secure than any other these techniques alone and also as compared to Cryptography and cryptography combined systems. Visual Cryptography is one of the most secure forms of Cryptography available today. It is most commonly implemented in image files. However embedding data into image changes its color frequencies in a predictable way. To overcome this predictability, we propose the concept of multiple cryptography where the data will be encrypted into a cipher and the cipher will be hidden into a multimedia image file in encrypted format. We shall use traditional cryptographic techniques to achieve data encryption and visual Cryptography algorithms will be used to hide the encrypted data.

TABLE OF CONTENT

Page No.

CHAPTER -1
INTRODUCTION

Secret information is main topic focused in systems used for communication an effective and secure protection is through encrypting the data. The data must be protected from being tampered by any process going on within the systems. Encryption of data is one of the methods to make sure that integrity and confidentiality of important information is available. The major role of encryption techniques is to prevent exposure of information to unnecessary individuals. Secret image sharing is also an alternative to consider as a solution to problems, especially for long detailed information so called as secret images. Nowadays with the increase in networking industry the transmission of images and other multimedia can be done easily. This use of secret sharing is increased because hackers can find the weak points of a communication system and attack to extract confidential information being transmitted over the network.

Visual cryptography was firstly discovered by Noar and Shamir in 1994. Encryption of a visual information using the cryptography technique such that the decryption is only possible using proper orientation of images or with the right algorithm for overlapping. Transferring multimedia information using Internet is very common these days. Various techniques and methods have been developed to solve the problem of sharing of secret images and these tools can be used to resolve this problem .The splitting of images should be done such that even hacker is able to make available any share but is not able to get any information out of it. In today's scenario of electronic commerce, the need to solve the issue of sharing information safely considering the fact of using network as medium of sharing information. Regular efforts of hackers to gain secret information are done as a result of which there is an urgent need to make both communications medium as well as communication tools and techniques safe and secure. The scheme of visual secretly sharing of the image is to eventually divide it into 'n' total shares. As all 'n' shares are combined, the secret image is created. The benefit of using this technique is that even if the hacker gets 'n-1' shares they would not be able to get the main secret image as all the 'n' shares are required to generate the secret image.

In today’s information age, information sharing and transfer has increased exponentially. The threat of an intruder accessing secret information has been an ever existing concern for the data communication experts. Cryptography is the most widely used techniques to overcome this threat.

Cryptography involves converting a message text into an unreadable cipher. On the other hand, embeds message into a cover media and hides its existence. Both these techniques provide some security of data neither of them alone is secure enough for sharing information over an unsecure communication channel and are vulnerable to intruder attacks. Although these techniques are often combined together to achieve higher levels of security but still there is a need of a highly secure system to transfer information over any communication media minimizing the threat of intrusion. In this paper we propose an advanced system of encrypting data that combines the features of cryptography, along with multimedia data hiding. This system will be more secure than any other these techniques alone and also as compared to cryptography combined systems

Cryptography is the art of “secret communication”. Its goal is to transmit a message (information) hidden inside another visible message. The typical visible message used in many cryptographic systems is a digital image and the embedded message is usually hidden by working in the Fourier domain. The message is first coded by a sequence of small irregular images and then merged inside another image together with many other small images.

Visual cryptography is one of the most secure forms available today. It is most commonly implemented in image files. However embedding data into image changes its color frequencies in a predictable way. To overcome this predictability, we propose the concept of multiple cryptography where the data will be encrypted into a cipher and the cipher will be hidden into a multimedia image file in encrypted format. We shall use traditional cryptographic techniques to achieve data encryption and visual cryptography algorithms will be used to hide the encrypted data. Visual cryptography is a cryptographic technique which allows visual information to be encrypted in specific a way that decryption becomes a mechanical operation that does not require a computer. The idea was about producing image shares of a given secret image in a way that the image shares appear meaningless.

Recovery of the image can be done by superimposing specified number of share images and, hence, the decoding process requires no special hardware or software and can be simply done by the human eye. Visual cryptography is a little more advantageous for implementation, while compared to conventional cryptography schemes, since the decryption process does not need any computation. Further, the image based information becomes more secure, since only the intended recipient can reveal the true meaning of the decrypted image. Suppose the data (image) D is divided into n shares. D can be constructed from any k shares out of n shares. Complete knowledge of (k-1) shares reveals no information about D. So, k out of n shares is necessary to reveal secret data. For example: let 6 thieves share a bank account but they do not trust each other. The thieves split up the password for the account in such a way that any 3 or more thieves working together can have access to account, but not less than 3.

CHAPTER -2

LITERATURE REVIEW

The main operation of Visual Cryptography is based on the use of binary inputs. As the binary data is displayed transparent when imprinted on screen that is transparent itself. Smaller blocks are used to divide every pixel of the secret image. Same numbers of black and white blocks are present in the image or the blocks. Only 1 black and 1 white block is there if any of pixel is split into two parts. And so on goes on if pixel gets split in 4 parts ,2 black and 2 white blocks are formed out of it . Fig 1 shows an example for division into 2x2 blocks and Fig 2 is superimposed image.

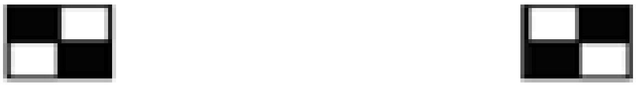


Figure 1: Two 2 × 2 pixel blocks

Figure 2: Superimposed Image

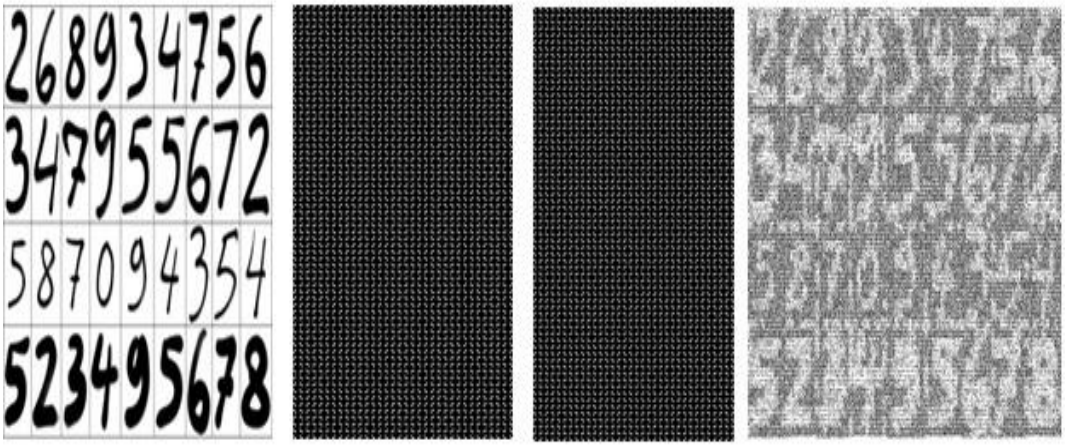
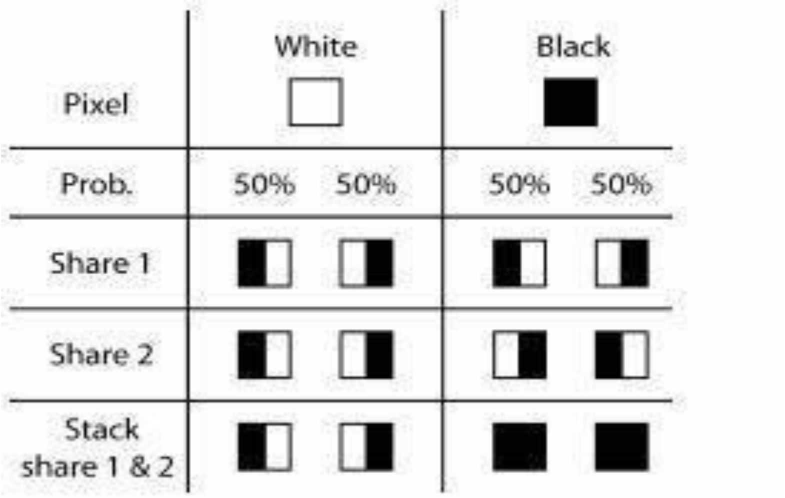


Fig-3: Example of Visual Cryptography

Visual secret sharing is the most simple out of problems of messages that comprise of black and white pixels and each pixel is handled separately. 'n' modified shares are generated for each original pixel that appears , one for each transparency . 'm' black and white sub-pixels are formed for each share , they are imprinted as close pattern to each other such that visual system create a median of the separate black as well as white versions. Structure that is formed by shares and contribution can be explained by Boolean matrix which is (nxm) and S is expressed [sij] where *sij* -> 1 and when the jth pixel is black in transparency. The framework is almost similar to the Naor and Shamir whereas the important difference that their framework that divides into 'n' shares of binary secret image. The 'm' sub pixels are used to explain each pixel of image. Black and white schema of visual cryptography is illustrated by a Boolean matrix of the form 2(n x m) where (S0 and S1). Main image i.e. white pixel image is represented using S0 and but if main image is black then S1 is used instead. Representation of white and black pixel is done by 0 and 1 respectively in the technique of visual cryptography .Various visual cryptography techniques are used example: 2 / 2, 2 / n, n / n and k / n. The 2 / 2 is the widely taken in use to explain the Visual Cryptography schema.

The 2 / 2 Visual Cryptography technique S1 and S0 is expressed as

.



Pixel	White □		Black ■	
Prob.	50%	50%	50%	50%
Share 1	◧	◨	◧	◨
Share 2	◧	◨	◨	◧
Stack share 1 & 2	◧	◨	■	■

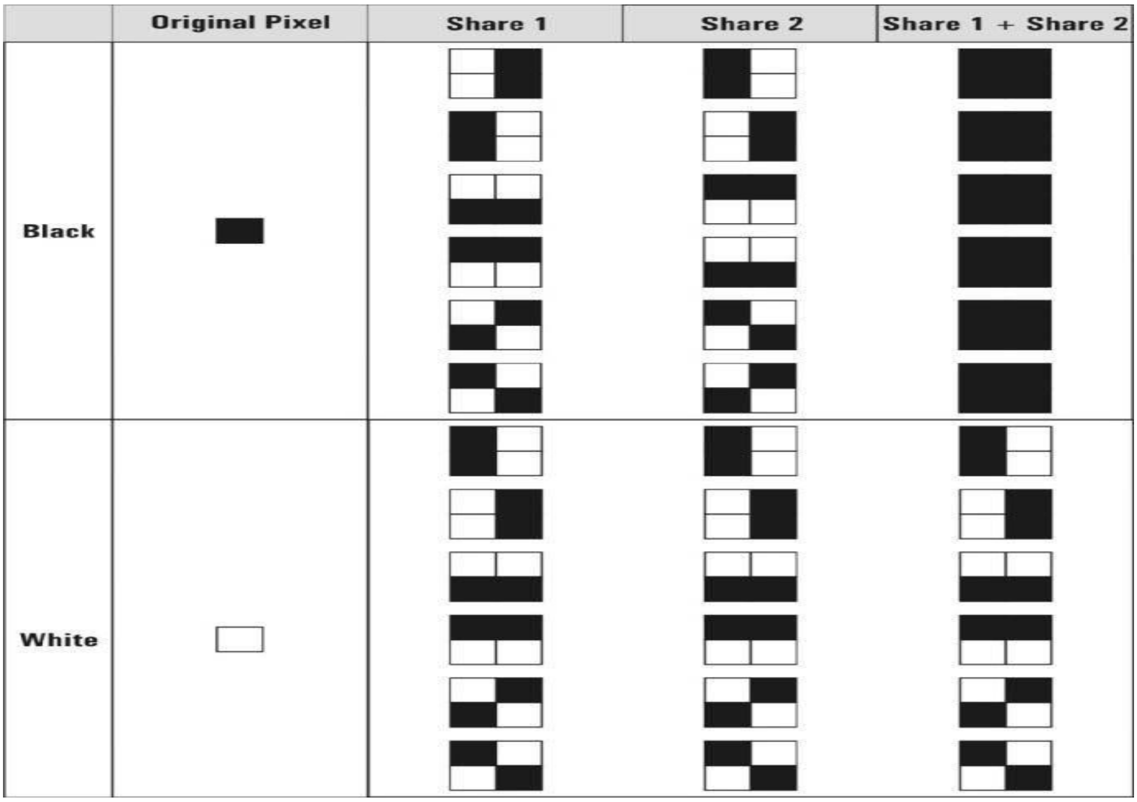
Fig-4: Formation of 2 by 2 VC schema

Two different Q0 and Q1 matrices. We select the matrix Q0 to give a white pixel and the matrix Q1 is used give a black pixel. The very initial row of selected matrix is for the share S1 and the row after the is for the share S2.

The encoding of every pixel of the main image into two sub pixel is the disadvantage and if main image sized S x S is positioned by share and is sized as S X2S. Due to the distortion present we take 4 sub pixel as design layout. Also the expansion of pixel is 2 by 2 pixels.

$$S0 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix} S1 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

Fig-5: Illustration of 2 X 2 Visual Cryptography technique using a layout design of 4 sub pixel



CHAPTER -3

Basic Overview on Cryptography

Cryptography involves converting a message text into an unreadable cipher.

A large number of cryptography algorithms have been created till date with the primary objective of converting information into unreadable ciphers The two types of algorithms that will be discussed are

- Joint Key Cryptography (Symmetric Key Cryptography): Uses a single key for both encryption and decryption
- Public Key Cryptography (Asymmetric Key Cryptography): Uses one key for encryption and another for decryption

1.1 THE JOINT KEY CRYPTOGRAPHY (Symmetric key cipher)

It uses a common key for encryption and decryption of the message. This key is shared privately by the sender and the receiver. The sender encrypts the data using the joint key and then sends it to the receiver who decrypts the data using the same key to retrieve the original message. Joint key cipher algorithms are less complex and execute faster as compared to other forms of cryptography but have an additional need to securely share the key. In this type of cryptography the security of data is equal to the security of the key. In other words it serves the purpose of hiding a smaller key instead of the huge chunk of message data

.

1.2 THE PUBLIC KEY CRYPTOGRAPHY (asymmetric key cipher)

It is a technique that uses a different key for encryption as the one used for decryption. Public key systems require each user to have two keys – a public key and a private key (secret key). The sender of the data encrypts the message using the receiver's public key. The receiver then decrypts this message using his private key. This technique eliminates the need to privately share a key as in case of symmetric key cipher. Asymmetric cryptography is comparatively slower but more secure than symmetric cryptography technique. The public key cryptography is a fundamental and most widely used technique, and is the approach which underlies Internet standards such as Transport Layer Security (TLS). The most common algorithm used for secret key systems is the Data Encryption Algorithm (DEA) defined by the Data Encryption Standard (DES)

1.3 A HYBRID CRYPTOSYSTEM

It is a more complex cryptography system that combines the features of both joint and public key cryptography techniques. We shall use traditional public key cryptography techniques to covert the message into a cipher. For embedding the cipher into images, a modified joint key technique will be used.

1.4 VISUAL CRYPTOSYSTEM

When the random image contains truly random pixels it can be seen as one time pad and will offer unbreakable encryption. In the overlay animation you can observe the two layers sliding over each other until they are correctly aligned and the hidden information appears. To try this yourself, you can copy the example layers 1 and 2, and print them onto a transparent sheet or thin paper. Always use a program that displays the black and white pixels correctly and set the printer so that all pixels are printed accurate (no diffusion or photo enhancing etc). You can also copy and paste them on each other in a drawing program like paint and see the result immediately, but make sure to select transparent drawing and align both layers exactly over each other.

CHAPTER -4

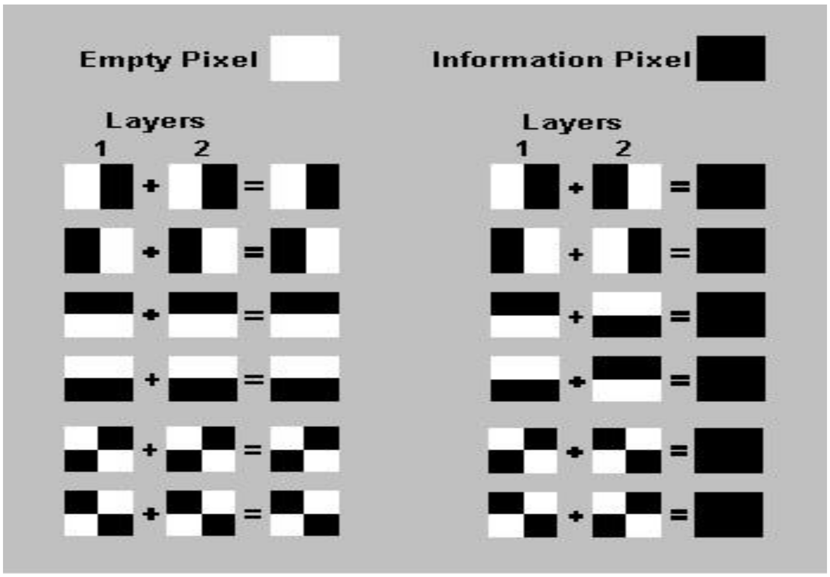
How Visual Cryptography works

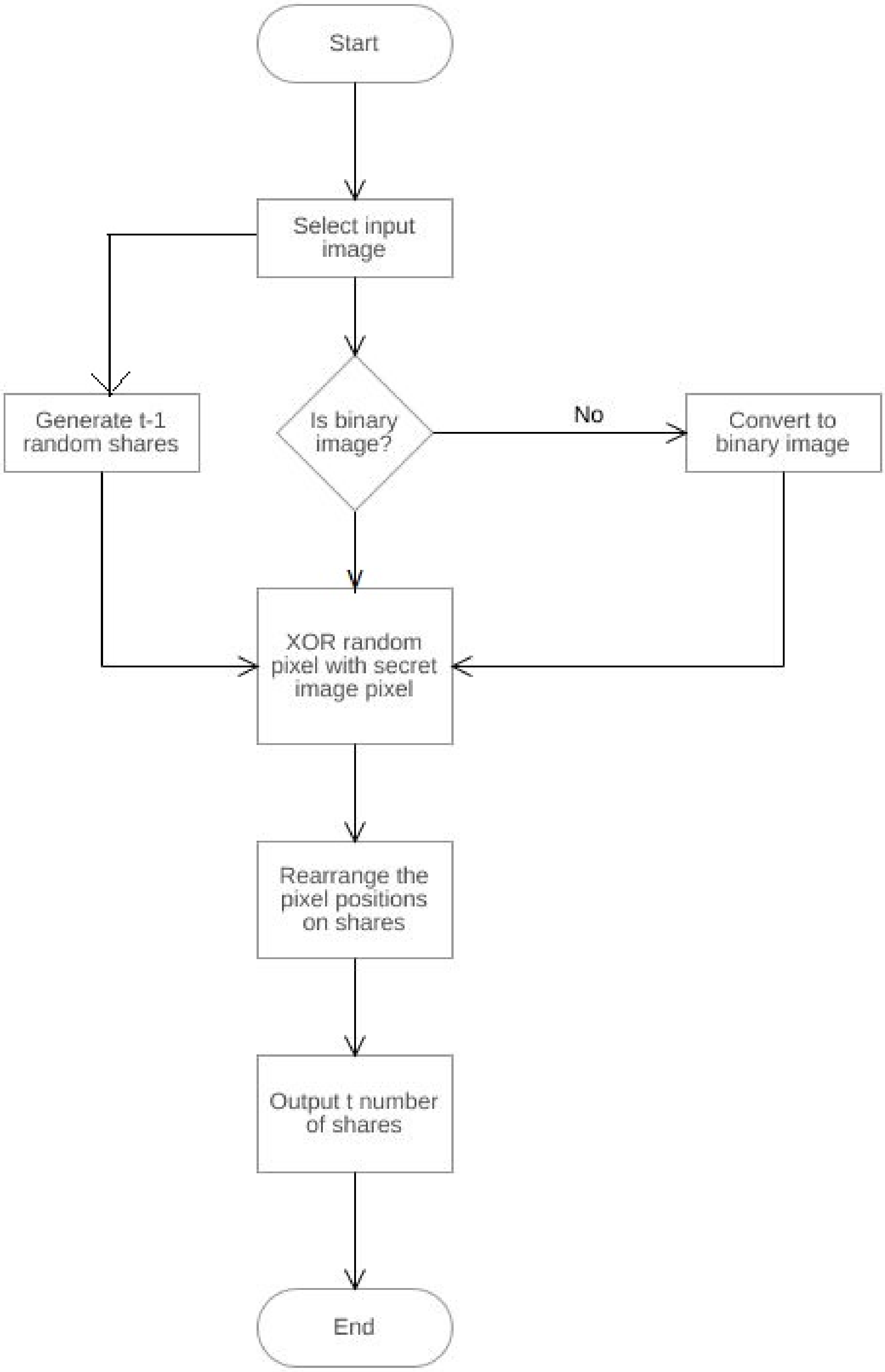
Each pixel of the images is divided into smaller blocks. There are always the same number white (transparent) and black blocks. If a pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal parts, there are two white and two black blocks. The example images from above uses pixels that are divided into four parts.

In the table on the right we can see that a pixel, divided into four parts, can have six different states.

If a pixel on layer 1 has a given state, the pixel on layer 2 may have one of two states: identical or inverted to the pixel of layer 1. If the pixel of layer 2 is identical to layer 1, the overlaid pixel will be half black and half white. Such overlaid pixel is called grey or empty. If the pixels of layer 1 and 2 are inverted or opposite, the overlaid version will be completely black. This is an information pixel.

Fig 6:Multilayer pixel distribution




Start
Select input image
Generate t-1 random shares
Is binary image?
No
Convert to binary image
XOR random pixel with secret image pixel
Rearrange the pixel positions on shares
Output t number of shares
End

Flow chart visual cryptography

We can now create the two layers. One transparent image, layer 1, has pixels which all have a random state, one of the six possible states. Layer 2 is identical to layer 1, except for the pixels that should be black (contain information) when overlaid. These pixels have a state that is opposite to the same pixel in layer 1. If both images are overlaid, the areas with identical states will look gray, and the areas with opposite states will be black.

The system of pixel can be applied in different ways. In our example, each pixel is divided into four blocks. However, you can also use pixels, divided into two rectangle blocks, or even divided circles. Also, it doesn't matter if the pixel is divided horizontally or vertically. There are many different pixel systems, some with better contrast, higher resolution or even with color pixels.

If the pixel states of layer 1 are truly (crypto secure) random, both empty and information pixels of layer 2 will also have completely random states. One cannot know if a pixel in layer 2 is used to create a grey or black pixel, since we need the state of that pixel in layer 1 (which is random) to know the overlay result. If all requirements for true randomness are fulfilled, Visual Cryptography offers absolute secrecy according to the Information Theory.

If Visual Cryptography is used for secure communications, the sender will distribute one or more random layers 1 in advance to the receiver. If the sender has a message, he creates a layer 2 for a particular distributed layer 1 and sends it to the receiver. The receiver aligns the two layers and the secret information is revealed, this without the need for an encryption device, a computer or performing calculations by hand. The system is unbreakable, as long as both layers don't fall in the wrong hands. When one of both layers is intercepted it's impossible to retrieve the encrypted information.

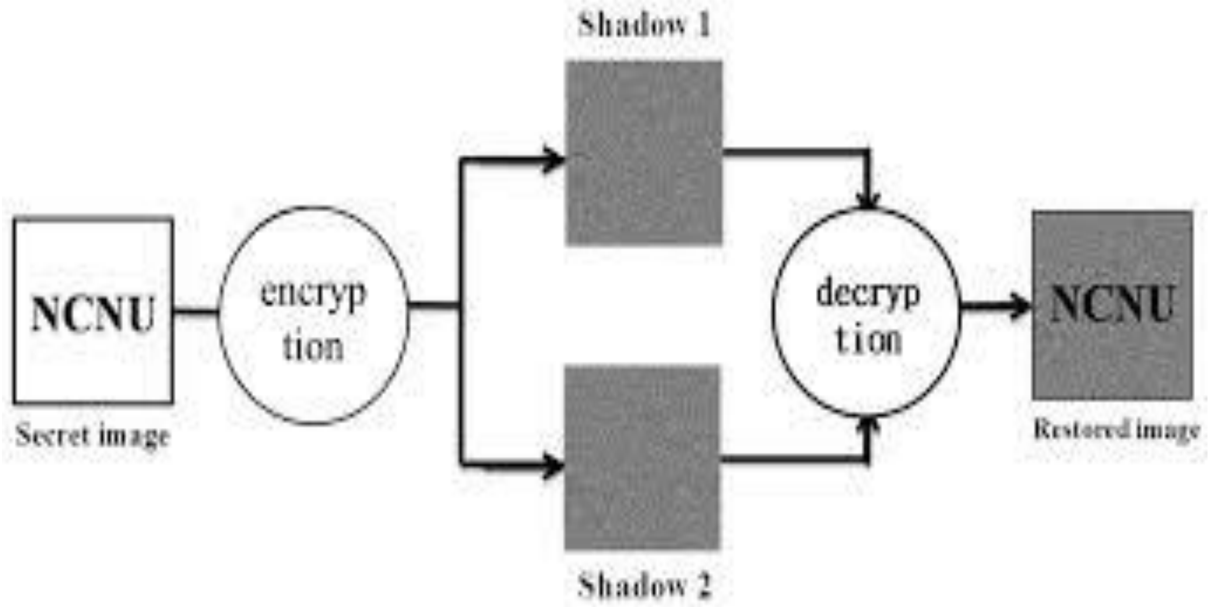


Fig 8: Visual Cryptography Diagram

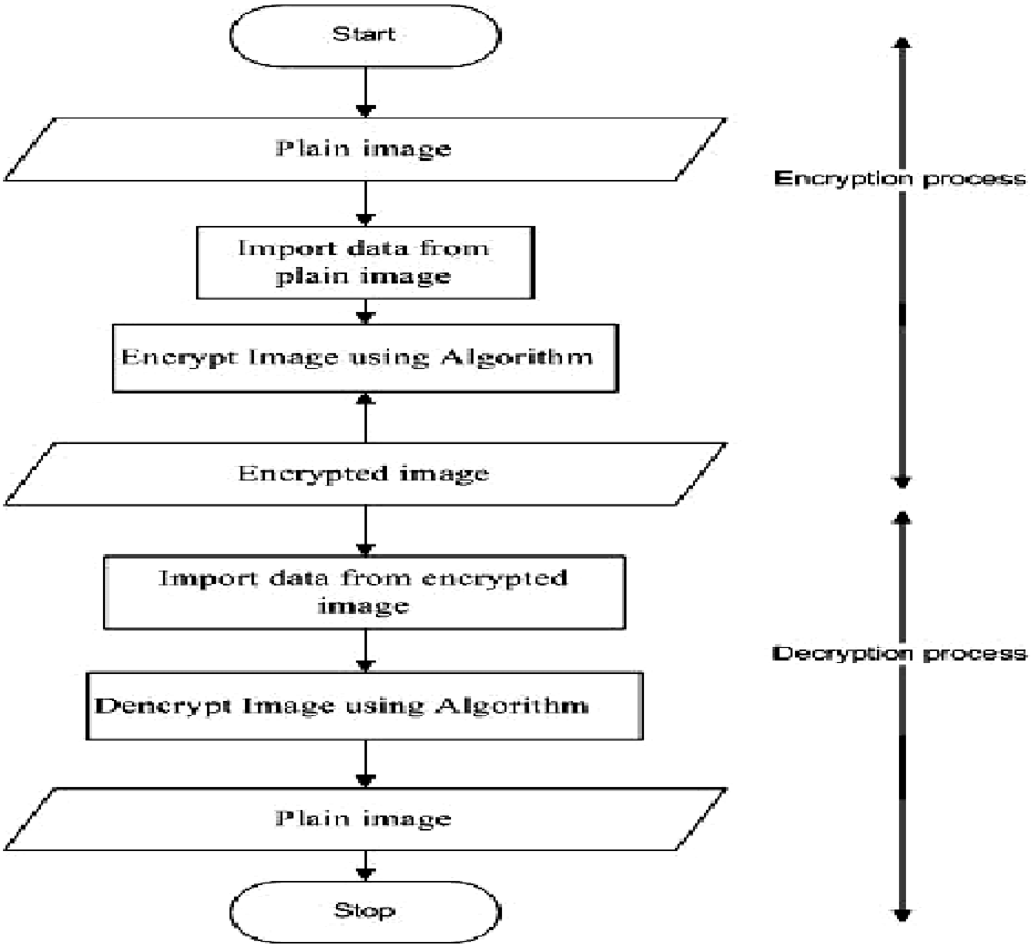


Fig 9: Step by Step Description

Naor and Shamir in 1994 they demonstrated a visual secret sharing plan, where a picture was separated into n imparts so that just somebody to all n shares could decode the picture, while any n 1 shares uncovered no data about the first original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. At the point when all n shares were overlaid, the first picture would show up. There are a few speculations of the fundamental plan including k-out-of-n visual cryptography. Rijimen displayed another 2-out-of-2 VC plot by applying the thought of shading mixture. When two transparencies superimposed on one another with distinctive colors, they lead to raises a third blended shading.

In 2002, Nakajima predicted a new method of extended visual cryptography. This method is for regular images which are used to produce meaningful binary shares .This system works by taking three pictures as an input and generates two images which correspond to two of the three input pictures. The third picture is recreated by printing the two share pictures onto transparencies and stacking them together. By and large, visual cryptography experiences the deterioration of the image quality. In this also describes the method to improve the quality of the output image.

Binary visual cryptography scheme is proposed Houetal in the year 2004, which is applied to gray level images, that a gray level image is transformed into halftone images. The method that uses the density of the net dots to simulate the gray level is called Halftone and transforms an image with gray level into a binary image before processing. Halftone visual cryptography is proposed by the Zhi Zhou et al. In 2006 which produce meaningful and good high quality halftone shares, the generated halftone shares contain the visual information.

CHAPTER -5

k out of k visual cryptography scheme

A common example of k out of k visual cryptography scheme is 2 out of 2 visual cryptography schemes. In (2, 2) Visual Cryptography Scheme, the original image is broken into 2 image shares. In original image , every pixel is represented by non-overlapping block of 2 or 4 sub-pixels in each share. If anyone is having only one share will not be able to reveal any secret information. Both the shares are required to be superimposed to reveal the secret image.

There are many techniques for encoding the pixels of original image. In a technique, in which each pixel in original image is represented by two sub-pixels in each share, while reading the pixels in original image, if a white pixel is encountered, one of the first two rows in Figure given below is selected with probability 0.5, and the shares are assigned 2 pixel blocks as shown in the third and fourth columns in figure given below. Similarly, if a black pixel is encountered, one of the last two rows is selected with probability 0.5, from which a sub-pixel block is assigned to each share. When two shares are superimposed, if two white pixels overlap, the result will be white pixel and if a black pixel in one share overlaps with either a white or black pixel in another share, the result will be black pixel. This implies that the superimposition of the shares represents the Boolean OR function. The last column in Figure given below shows the resulting sub-pixel when the sub-pixels of both the shares in the third and fourth columns are superimposed.

CHAPTER -6

k out of n visual cryptography scheme

In (2, 2) visual cryptography, both the shares are required to reveal secret information. Due to some problem if one share gets lost then the secret information cannot be revealed. So there is a restriction of keeping all the shares secure to reveal the secret information and user can not afford to lose a single share. Naor and Shamir generalized basic model of visual cryptography into a visual variant of k out of n visual cryptography scheme to give.

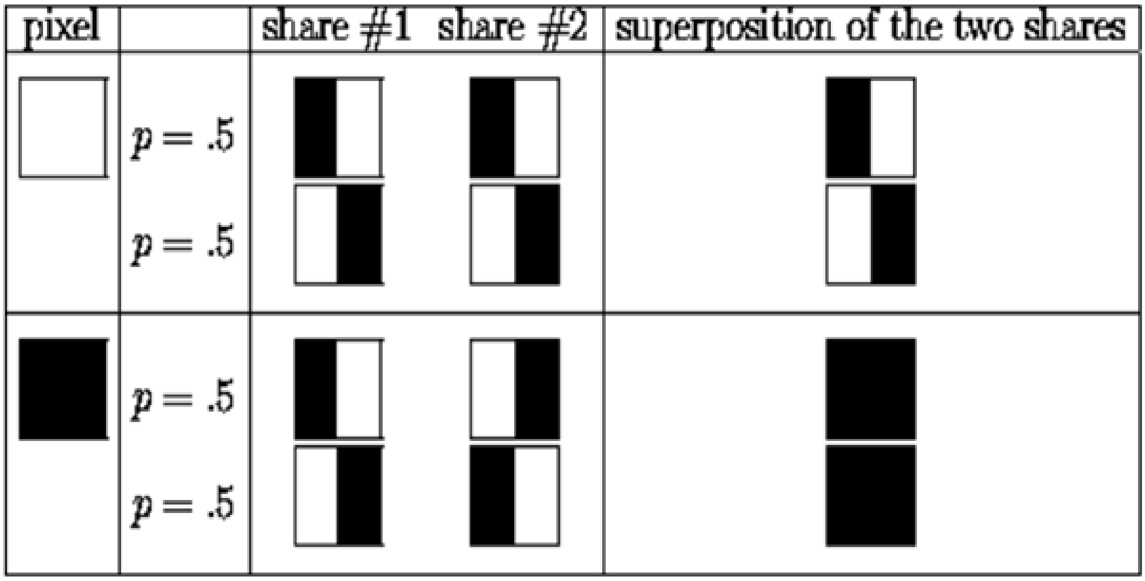


Figure 10: Illustration of a (2, 2) VC Scheme with 2 Sub pixels

Some flexibility to user in (k, n) visual cryptography scheme, n shares can be generated from original image and distributed. Original image is recognizable only if k or more shares superimposed, where value of k is between 2 to n. If less than k shares stacked together, secret original image cannot be revealed. It gives flexibility to user. If user loses some of the shares still secret information can be revealed, if minimum k number of shares is obtained. It also ensures the security as to know the secret information you have to have more than k shares out of n secret shares.

CHAPTER -7

Visual Cryptography Scheme for General Access Structure

In (k, n) visual cryptography scheme, all n shares have equal importance. The secret information can be revealed if any k out of n shares are available. The security of system might get compromised due to this. To beat this issue, G. Ateniese, C. Blundo, A. DeSantis, and D. R. Stinson extended (k, n) visual cryptography model to general access structure. In general access structure scheme, given set of n shares is divided into two subsets namely qualified and forbidden subset of shares as per the importance of shares. Any k shares from qualified subset of shares can reveal secret information, but fewer than k shares from qualified subset of shares can not reveal any secret information. Even k or more shares from forbidden set can not reveal secret information. So, Visual cryptography for general access structure improves the security of system.

Recursive Threshold Visual Cryptography Scheme

In (k, n) visual secret sharing scheme, a secret of b bits is distributed among n shares of size at least b bits each. Since only k out of n shares is needed to reveal secret, every bit of any share conveys at most 1/k bits of secret. It results in inefficiency in terms of number of bits of secret conveyed per bit of shares. To overcome this limitation proposed Recursive threshold visual cryptography. The basic idea behind Recursive threshold visual cryptography is recursive hiding of smaller secrets in shares of larger secrets with secret sizes doubling at every step, and thereby increasing the information, every bit of share conveys to (n-1)/n bit of secret which is nearly 100

Halftone Visual Cryptography Scheme

Halftone visual cryptography uses half toning technique to create shares. Halftone is the reprographic technique. It simulates continuous tone imagery through the use of dots, which may vary either in size, in shape or in spacing. Zhi Zhou et al. proposed halftone visual cryptography .In halftone visual cryptography a secret binary pixel is encoded into an array of sub pixels, called as halftone cell, in each of the n shares. By using halftone cells with an appropriate size, visually pleasing halftone shares can be obtained. It maintains good contrast and security and increases quality of the shares[3].

Visual Cryptography Scheme for Grey images

All previous visual cryptography schemes were only limited to binary images. These procedures were fit for doing operations on just highly contrasting black and white pixels. It is not sufficient for real life applications. Chang-Chou Lin, Wen Hsiang Tsai proposed visual cryptography for gray level images. In this scheme a dithering technique is used to convert gray level image into approximate binary image. Then existing visual cryptography schemes for binary images are applied to create the shares.

CHAPTER -8

Basic Terminology of Cryptography

Computers are used by millions of people for many purposes. such as banking, shopping, military, student records, etc.. Privacy is a critical issue in many of these applications, how are we need to make sure that an unauthorized parties cannot read or modify messages.

Cryptography is the transformation of readable and understandable data into a form which cannot be understood in order to secure data. cryptography refers exactly to the methodology of concealing the content of messages, the word cryptography comes from the Greek word "Kryptos", that means hidden, and "graphikos" which means writing.

The information that we need to hide, is called plaintext , It’s the original text, It could be in a form of characters, numerical data, executable programs, pictures, or any other kind of information, The plaintext for example is the sending of a message in the sender before encryption, or it is the text at the receiver after decryption.

The data that will be transmitted is called cipher text, it's a term refers to the string of "meaningless" data, or unclear text that nobody must understand, except the recipients. it is the data that will be transmitted Exactly through network, Many algorithms are used to transform plaintext into cipher text.

Cipher is the algorithm that is used to transform plaintext to cipher text, this method is called encryption, in other words, it's a mechanism of converting readable and understandable data into "meaningless" data.

The Key is an input to the encryption algorithm, and this value must be independent of the plaintext, This input is used to transform the plaintext into cipher text, so different keys will yield different cipher text, In the decipher side, the inverse of the key will be used inside the algorithm instead of the key.

Computer security it's a generic term for a collection of tools designed to protect any data from hackers, theft, corruption, or natural disaster while allowing these data to be available to the users at the same time. The example of these tools is the antivirus program.

Network security refers to any activity designed to protect the usability, integrity, reliability, and safety of data during their transmission on a network, Network security deals with hardware and software. The activity can be one of the following anti-virus and anti-spyware, firewall, Intrusion prevention systems, and Virtual Private Networks.

Internet Security is measures and procedures used to protect data during their transmission over a collection of interconnected networks, while information security is about how to prevent attacks, and to detect attacks on information-based systems.

CHAPTER -9

Cryptography Goals

By using cryptography many goals can be achieved, these goals can be either all achieved at the same time in one application, or only one of them.

These goals are:

1. **Confidentiality:** it is the most important goal, that ensures that nobody can understand the received message except the one who has the decipher key.

2. **Authentication:** it is the process of proving the identity, that assures the communicating entity is the one that it claimed to be. This means that the user or the system can prove their own identities to other parties who don't have personal knowledge of their identities.

3. **Data Integrity:** It ensures that the received message has not been changed in any way from its original form. The data may get modified by an unauthorized entity intentionally or accidently. Integrity service confirms that whether data is intact or not since it was last created, transmitted, or stored by an authorized user. This can be achieved by using hashing at both sides the sender and the recipient in order to create a unique message digest and compare it with the one that received.

4. **Non-Repudiation:** it is mechanism used to prove that the sender really sent this message, and the message was received by the specified party, so the recipient cannot claim that the message was not sent. For example, once an order is placed electronically, a purchaser cannot deny the purchase order, if non-repudiation service was enabled in this transaction.

5. **Access Control:** it is the process of preventing an unauthorized use of resources. This goal controls who can have access to the resources, If one can access, under which restrictions and conditions the access can be occurred, and what is the permission level of a given access.

CHAPTER -10

Data Encryption

A data encryption is a random string of bits created explicitly for scrambling and unscrambling data. Data encryption is designed with algorithms intended to ensure that every key is unpredictable and unique.

Cryptography uses two types of keys: symmetric and asymmetric. Symmetric keys have been around the longest; they utilize a single key for both the encryption and decryption of the cipher text. This type of key is called a secret key. Secret-key ciphers generally fall into one of two categories: stream ciphers or block ciphers. A block cipher applies a private key and algorithm to a block of data simultaneously, whereas a stream cipher applies the key and algorithm one bit at a time.

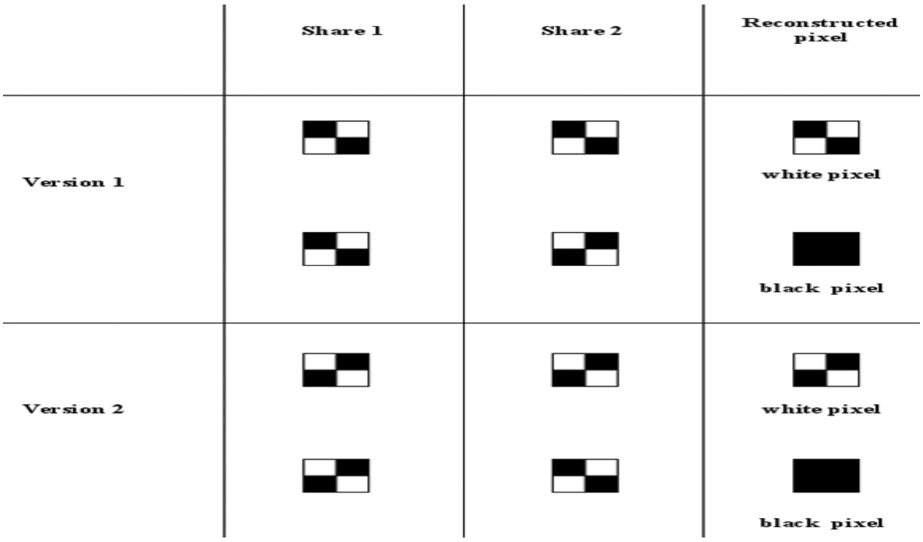
Most cryptographic processes use symmetric encryption to encrypt data transmissions but use asymmetric encryption to encrypt and exchange the secret key. Symmetric encryption, also known as private key encryption, uses the same private key for both encryption and decryption. The risk in this system is that if either party loses the key or the key is intercepted, the system is broken and messages cannot be exchanged securely.

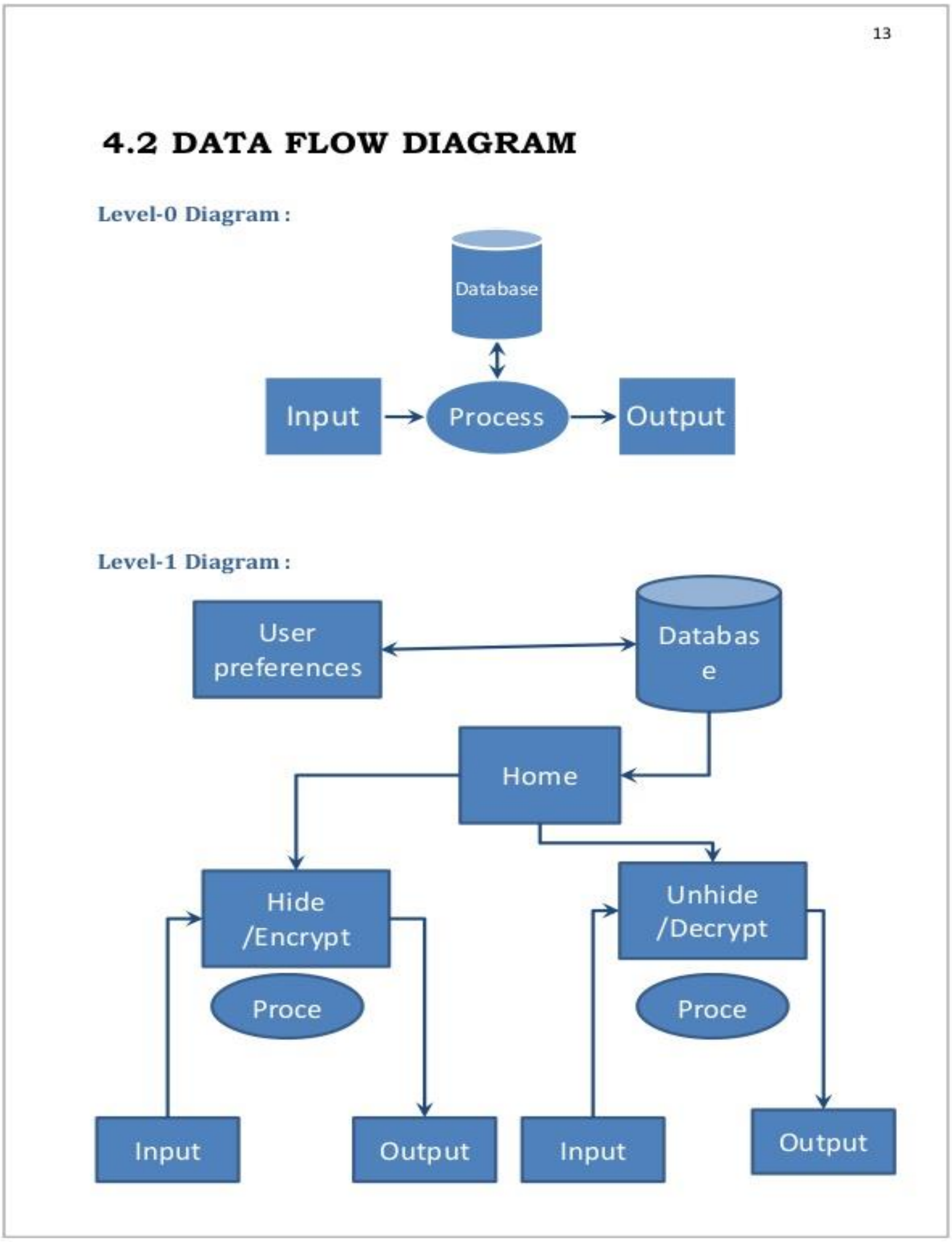
CHAPTER -11

Data Decryption

One of the foremost reasons for implementing an encryption-decryption system is privacy. As information travels over the World Wide Web, it becomes subject to access from unauthorized individuals or organizations. Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys. Encryption is the process of translating plain text data (*plaintext*) into something that appears to be random and meaningless (*cipher text*). Decryption is the process of converting cipher text back to plaintext.

Figure 11: Different Pixel Splitting





13

4.2 DATA FLOW DIAGRAM

Level-0 Diagram :

Level-1 Diagram :

Fig 12: DFD level 0 and level 1

CHAPTER -12

PROPOSED ALGORITHM

Basis matrices

Any black-and-white visual cryptography scheme can be described using two n x m Boolean matrices S0 and S1, called basis matrices, to describe the sub pixels in the shares. The basis matrix S0 is used if the pixel in the original image is white, and the basis matrix S1 is used if the pixel in the original image is black. The use of the basis matrices S0 and S1 can have small memory requirements (it keeps only the basis matrices S0 and S1), and it is efficient (to choose a matrix in C0 or C1) because it only generates a permutation of the columns of S0 or S1.

Basically, the two basis matrices S0 and S1 should satisfy the following. Definition:

1.A k-out-of-n visual cryptography scheme with parameters 1 d m and ¿ 0 can be constructed from two n x m Boolean matrices S0 and S1 if the following three conditions are met:

The OR m-vector V of any k of the n rows in S0 satisfies H (V) d .m. The OR m-vector V of any k of the n rows in S1 satisfies H (V) d. For any set r1, r2, . . . , rt 1,2,. . .,n with t ¡ k, the t x m matrices obtained by restricting S0 and S1 to rows r1, r2,, rt, are equal up to a column permutation.

where H (V) is the hamming weight (the number of one's) of the m-vector V of any k of the n rows, m is the pixel expansion and is the relative difference. The conditions (1) and (2) related to contrast in a reconstructed image and condition (3) related to security. Relative-Difference:

Let H (S0) and H (S1) be the hamming weight corresponding to the basis matrices S0 and S1 . Then relative difference () is defined as:

$\alpha = (H(S1)H(S0))/m$

Contrast:

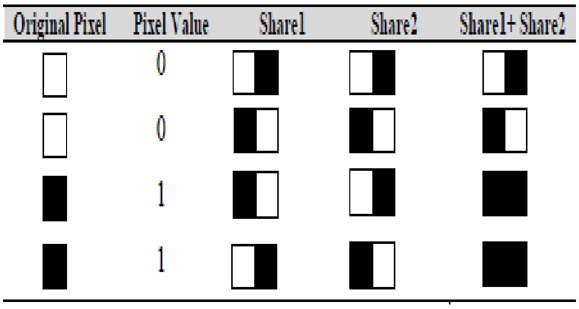
Let be the relative difference and m be the pixel expansion. The formula to compute contrast in different VCS is:

$\beta = \alpha.m, \beta \geq 1$

The basic idea of visual cryptography can be best described by considering a 2-out-of-2 VCS.

Construction of 2 out of 2 VCS

Let us consider a binary secret image S containing exactly m pixels. The dealer creates two shares (binary images), S1 and S2, consisting of exactly two pixels for each pixel in the secret image. If the pixel in S is white, the dealer randomly chooses one row from the first two rows of the figure 3 given below. Similarly, if the pixel in S is black, the dealer randomly chooses one row from the last two rows of figure 3.



Original Pixel	Pixel Value	Share1	Share2	Share1+ Share2
□	0	◨	◨	◨
□	0	◧	◧	◧
■	1	◧	◨	■
■	1	◨	◧	■

Figure 13: Illustration of a (2, 2) VC Scheme with 2 Sub pixels

To analyze the security of the 2-out-of-2 VCS, the dealer randomly chooses one of the two pixel patterns (black or white) from the Table for the shares S1 and S2.Randomly the pixels are selected so that the shares S1 and S2 consist of equal number of black and white pixels. Therefore, by reviewing a single share, one cannot distinguish the secret pixel as black or white. This technique gives flawless security. By superimposing the two shared sub pixels, the two participants can recover the secret pixel. The original pixel was black, If the superimposition results in two black sub pixels and if the superimposition creates one black and one white sub pixel, it indicates that the original pixel was white[1]. In visual cryptography, the white pixel is represented by 0 and the black pixel by 1. For the 2-out-of-2 VCS, the basis matrices, S0 and S1 are designed as follows:

$$S^0=\begin{bmatrix}1 & 0\\ 1 & 0\end{bmatrix}$$
$$S^1=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$$

Figure 3.2: S0 and S1 matrices

The relative difference and contrast , for the above basis matrices can be computed as:

$\alpha = 1/2$

$\beta = 1$

There are two collections of matrices, C0 for encoding white pixels and C1 for encoding black pixels. Let C0 and C1 be the following two collections of matrices:

$C0 = \pi(S0)\ C1 = \pi(S1)$

where $\pi(S0)$ and $\pi(S1)$ represents the collection of all matrices obtained by permuting the columns of matrices S0 and S1 respectively.

That is, to share a white pixel, the dealer randomly selects one of the matrices in C0, and to

$$C_0 = \left\{ \begin{bmatrix}1 & 0\\ 1 & 0\end{bmatrix}, \begin{bmatrix}0 & 1\\ 0 & 1\end{bmatrix} \right\} \text{ and } C_1 = \left\{ \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} \right\}$$

Figure 3.3

Share a black pixel, the dealer randomly selects one of the matrices in C1. The first row of the chosen matrix is used for share1(S1) and the second row for share 2 (S2). The two shares individually do not reveal the secret message. When we merge the two shares one upon another we can reveal the secret.

Construction of k out of n VCS

In this type of VCS, we are given a secret message. We would like to generate n transparencies so that the original secret message is visible if any k (or more) of them are stacked together but totally invisible if fewer than k transparencies are stacked together. A solution to the k out of n VCS consists of two collection of n*m Boolean matrices C0 and C1. To share a white pixel, the dealer randomly chosen one of the matrices in C1. The chosen matrix defines the color of the m sub pixels in each one of the n transparencies and likewise for black pixels. We apply 2 out of 2 VCS for every share images to create more shares[1].

Our project uses an advance technique of Visual Cryptography where an image is taken and eventually divided as 2 shares. Share 1 also called random share whereas the share 2 is main/key share that contains confidential information. The shares share 1 and share 2 have nothing in common to the secret image. The combination of the shares by XORing generates the secret image. There is no change in the quality of image created and the secret image. This algorithm has efficient recombination property and there is no loss of pixel so far. The use of algorithm is only bound for Black and white images without the loss of pixel.

Algorithm:

Step 1: Generation of random share
Step 2: Generation of key share
Step 3: Combining both the shares to generate secret image

In given step 1: For monochrome image a random share is generated for every pixel that has either 0 or 1 as its value. So, by picking randomly either 1 or 0 the random share would be created. Share size is same as that of the secret image. Different value is generated for each pixel each time a random share is created. Therefore, 2 randomly generated shares of the original image can never be equivalent.

In given step 2: XORing is the technique used to for key share generation where each and every pixel taken from the share randomly created is XORed with each and every pixel of the secret image. No change in size of original image and share can be seen. As it is seen that no 2 randomly generated shares can be same as a result of which no 2 key shares can be same.

In given step 3: XORing of randomly generated share and key share pixel after pixel is done to find the overlapping or resultant image. The result of which is the generation of the desired secret image.

For Monochromatic Images

```
   Algo RaKeOv ( )
 For each pixel j=0 to n
  {
      RaSj = Ra (0-1)
     KeSj = DSj ⊕ SIj
}
SI = DS ⊕ JS
  }
/* SI = Secret Image, DS=Random Share, JS=Key Share*/
```

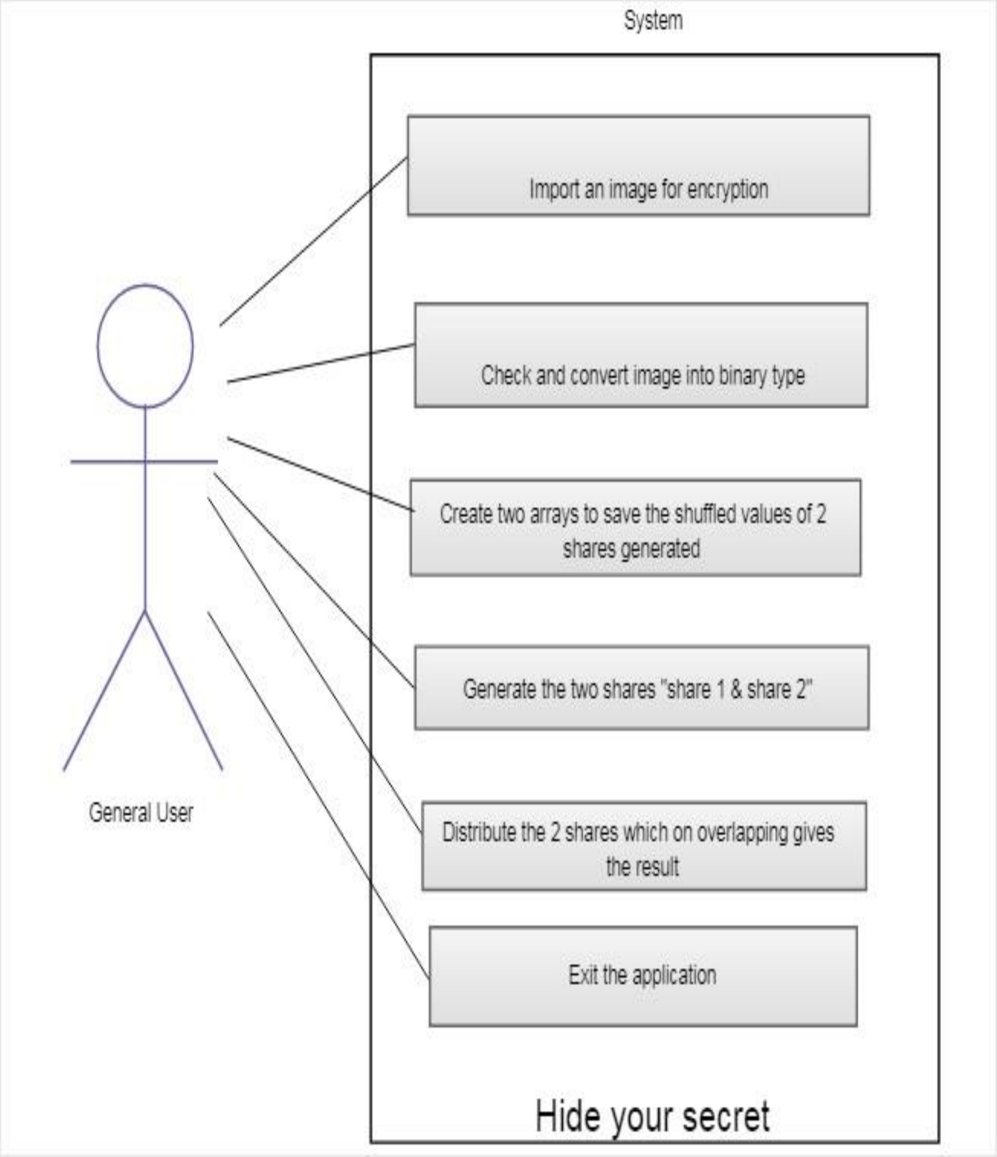

System
Import an image for encryption
Check and convert image into binary type
Create two arrays to save the shuffled values of 2 shares generated
Generate the two shares "share 1 & share 2"
Distribute the 2 shares which on overlapping gives the result
Exit the application
General User
Hide your secret

Fig 14 UML for Visual Cryptography

The visual cryptography scheme is a secure method that encrypts a secret document or image by breaking it into shares. A unique property of visual cryptography scheme is that one can visually decode the secret image by superimposing shares without computation. By taking the advantage of this property, third person can easily retrieve the secret image if shares are passing in the network. This approach is for encrypting visual cryptographically generated image shares using public key encryption. RSA algorithm is used for providing the double security of secret image. This scheme provides more security to secret shares that are robust against number of attacks. .

CHAPTER -13

Methodology

This scheme generates the VC shares using basic visual cryptography model and then encrypt the shares using RSA algorithm so that the shares will be more secure and protected from the malicious adversaries who may try to alter the bit sequence to create fake shares. During the decryption phase the secret shares are extracted by RSA decryption algorithm and stacked to reveal the secret image.

RSA algorithm

RSA is algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm, means there are two different keys. This is also called public key cryptography because one of them is public i.e can be given to everyone. The other key must be kept private. It is based on the fact that finding the factors of a integer is hard. RSA stands for Ron Rivest , Adi Shamir and Leonard Adleman , who first publicly described it in 1978.

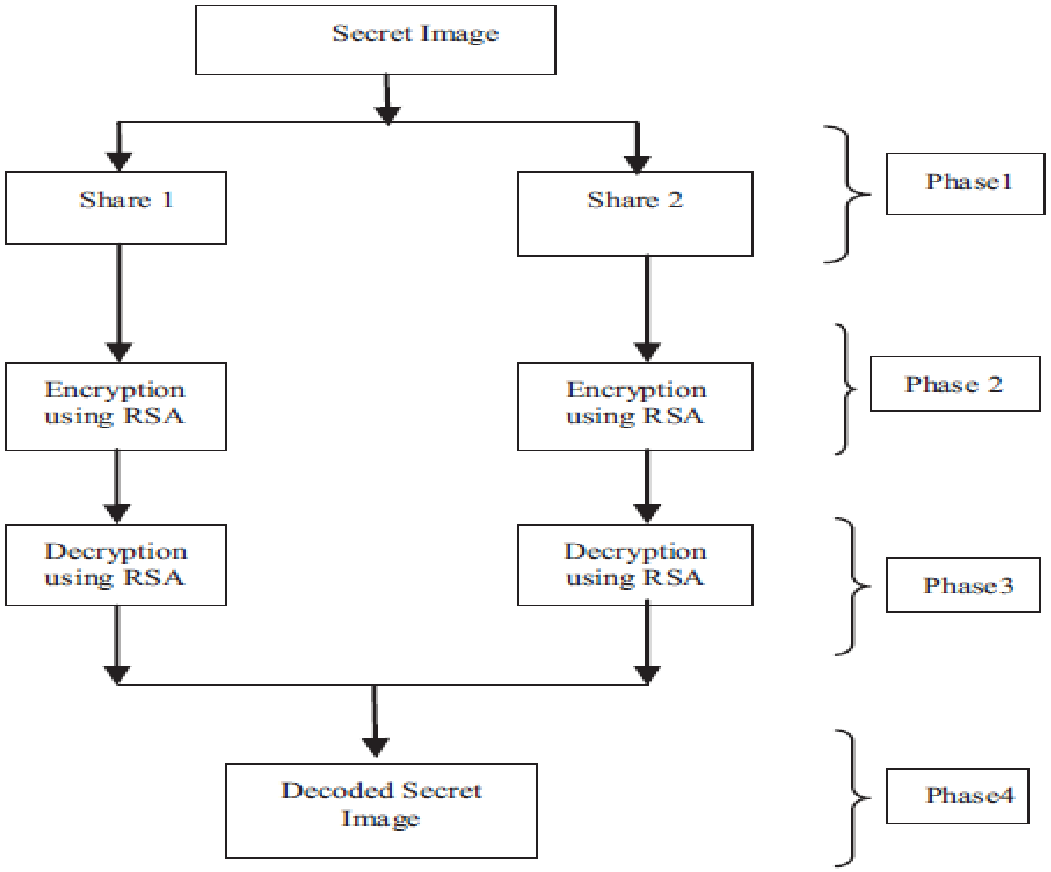


Figure 15: Methodology for public key encryption scheme

Operation

RSA involves a public key and private key. The public key can be known to everyone, it is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key. The keys for the RSA algorithm are generated the fol- lowing way:- 1. Choose two distinctive prime numbers p and q. For security purpose, the integers p and q should be chosen at random and should be of similar bit length. Prime integers can be efficiently found using a primarily test.

2. Compute $n = p * q$

n is used as the modulus for both the public and private keys. It's length usually ex- pressed in bits, is the key length.

3. Compute $\emptyset(n) = \emptyset(p) * \emptyset(q)$

$= (p - 1) * (q - 1)$

$= n - (p + q - 1)$

where, $\emptyset(n)$ is Euler's tontine function.

4. Choose an integer e such that, 1<e<$\emptyset(n)$ and gcd(e,$\emptyset(n)$)=1 that is e and $\emptyset(n)$ are co prime.

5. Determine d as d= e∧-1(mod $\emptyset(n)$) i.e. d is the multiplicative inverse of e(modulo$\emptyset(n)$).

The public key consists of the modulus n and the public(or encryption)exponent e. The private key consists of the modulus n and the private(or decryption) exponent d, which must be kept secret.

Data Encryption

A data encryption is a random string of bits created explicitly for scrambling and unscrambling data. Data encryption is designed with algorithms intended to ensure that every key is unpredictable and unique.

Cryptography uses two types of keys: symmetric and asymmetric. Symmetric keys have been around the longest; they utilize a single key for both the encryption and decryption of the cipher text. This type of key is called a secret key. Secret-key ciphers generally fall into one of two categories: stream ciphers or block ciphers.

A block cipher applies a private key and algorithm to a block of data simultaneously, whereas a stream cipher applies the key and algorithm one bit at a time.

Most cryptographic processes use symmetric encryption to encrypt data transmissions but use asymmetric encryption to encrypt and exchange the secret key. Symmetric encryption, also known as private key encryption, uses the same private key for both encryption and decryption. The risk in this system is that if either party loses the key or the key is intercepted, the system is broken and messages cannot be exchanged securely.

Encryption

One party transmits public key(n,e) to second party and keeps the private key d secret. The second party then wishes to send message M to first party.The second party first turns M into an integer m such that,

$0<m<n$

by using an agreed upon reversible protocol known as a padding scheme. Then compute the cipher text C correspond to, $c=m\wedge e(\text{mod } n)$

This can be done efficiently even for 500 bit numbers, using modular exponential. Then

second party transmits C to first party.

Data Decryption

One of the foremost reasons for implementing an encryption-decryption system is privacy. As information travels over the World Wide Web, it becomes subject to access from unauthorized individuals or organizations. Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys. Encryption is the process of translating plain text data (*plaintext*) into something that appears to be random and meaningless (*ciphertext*). Decryption is the process of converting ciphertext back to plaintext.

Decryption

First party can recover m from C by using private key exponent d via computing

$m=C\wedge d(\text{mod } n)$

given m, first party can never recover the original message M by reversing the padding scheme.

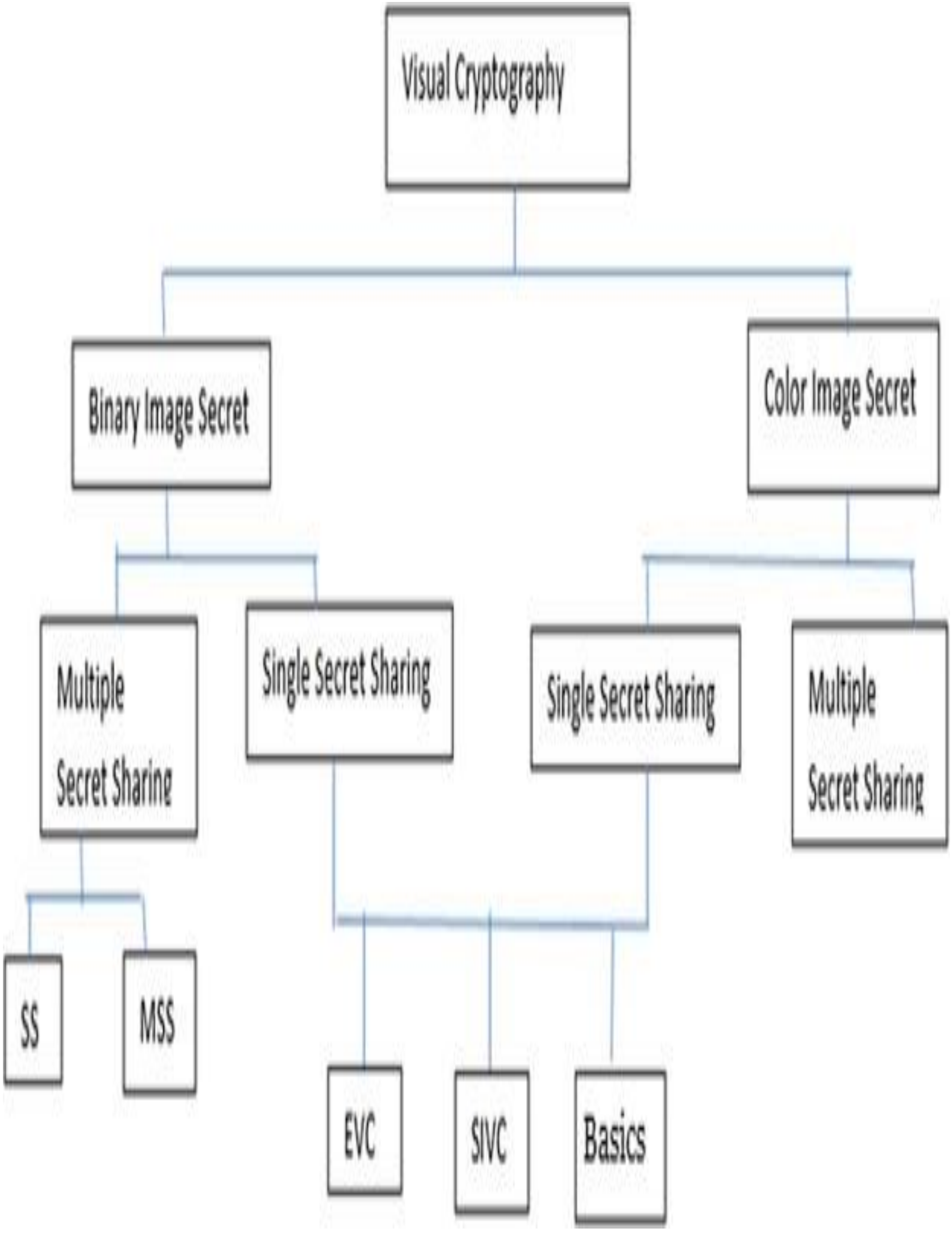


Fig 16: Visual Cryptography subdivision

CHAPTER -14

General Solutions

In the following section, we will be discussing two basic techniques as discussed by (1). The schemes that we will be discussing are as follows

- 2 out of N general scheme - This scheme means that if image is divided into N shares then at least 2 shares are needed to re-compute the image.
- 3 out of N general scheme – This scheme means that if image is divided into N shares then at least 3 shares are needed to re-compute the image.

Before discussing the two schemes, it is very vital to discuss about the basis matrices and the share distribution algorithm.

Basis Matrices – There are 2 matrices, which form the core of the visual cryptography scheme. One is to handle all the white pixels while the other is there to handle all the black pixels.

Share distribution Algorithm

In (1), the share distribution algorithm is defined as follows, For each pixel, do the following

1. Generate a random permutation of the set – {1,2,3,..., m}
2. If P is a black pixel, then apply the permutation to columns of S^1.
3. Else if it is a white pixel, then apply the permutation to columns of S^0.
4. Now each row in the new matrix comprises the m sub pixels of the pixel P in the each share.

The above algorithm makes use of random permutations of the basis matrix. For each pixel a different permutation is used hence *confusion* is introduced. This *confusion* adds to the security of the algorithm.

2 out of N Visual Sharing Scheme

For a (2,n) VCS, the solution is obtained as follows for S^0 and S^1

- S^0 – It is the matrix which has all rows of column 1 set as 1 and all other cells as 0.
- S^1 – It is the identity matrix.

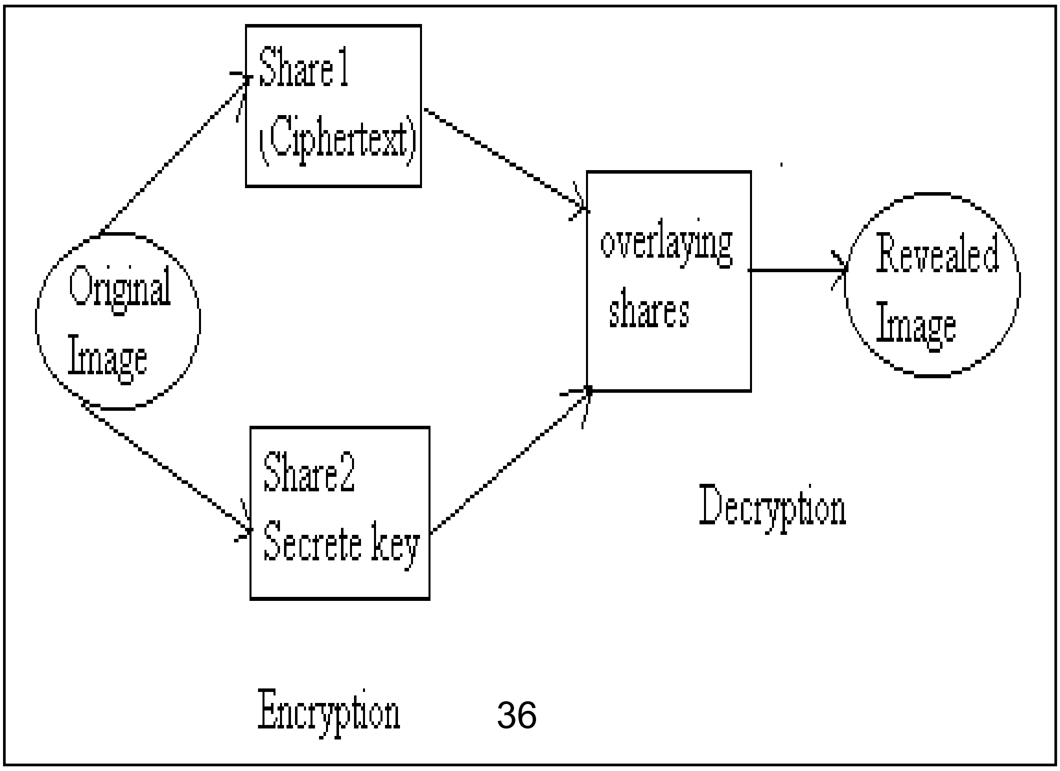
From these S^0 and S^1, the collection C^0 is obtained by all permutations of S^0 and C^1 is the collection of all permutations of S^1.

3 out of N Visual Sharing Scheme

For a (3,n) VCS, the solution is obtained by the following algorithm

- Generate a B matrix, which is of the dimension n x (n-2) containing only 1‟s
- Generate I as Identity matrix of n dimension
- Concatenate B and I to form the n x (2n-2) matrix
- C^0 – All matrices obtained by permuting c(BI)
- C^1- All matrices obtained by permuting BI

Fig 17: 2 out of Two secret sharing scheme



The image is visible only if all subpixels are of the same color, then the value of that pixel in the recomputed image is that color otherwise it is a mix color or black.

Share1 (1st half): 0 1 0 1 0 1 00

Share2 (1st half): 1 0 1 0 1 0 10

----

1 1 1 1 1 1 1 0 = 254

Share3 (1st half) : 0 0 1 0 0 1 00

Share1 (2nd half): 1 1 0 1 1 0 10

----

1 1 1 1 1 1 1 0 = 254

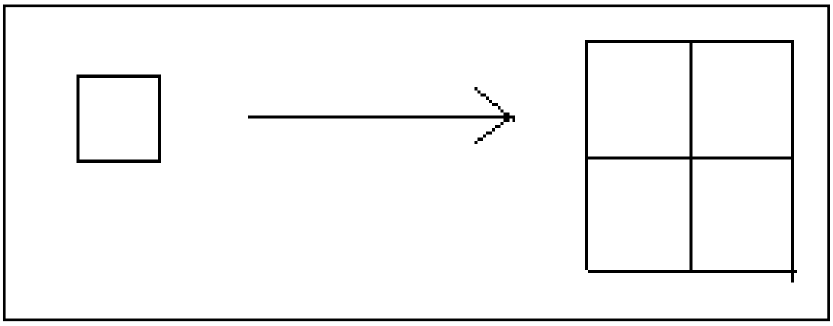
Share2 (2nd half): 1 1 1 0 1 1 10

Share3 (2nd half): 1 0 0 1 0 1 00

----

1 1 1 1 1 1 1 0 = 254

Fig18 : Pixel Expansion



CHAPTER -15

CODE OF THE PROJECT

Code to generate the 2 shares of images:

```
from PIL import Image
import random
import sys

image = Image.open(sys.argv[1])
image = image.convert('1')

outfile1 = Image.new("1", [dimension * 2 for dimension in image.size])
outfile2 = Image.new("1", [dimension * 2 for dimension in image.size])

for x in range(0, image.size[0], 2):
    for y in range(0, image.size[1], 2):
        sourcepixel = image.getpixel((x, y))
        assert sourcepixel in (0, 255)
        coinflip = random.random()
        if sourcepixel == 0:
            if coinflip < .5:
                outfile1.putpixel((x * 2, y * 2), 255)
                outfile1.putpixel((x * 2 + 1, y * 2), 0)
                outfile1.putpixel((x * 2, y * 2 + 1), 0)
                outfile1.putpixel((x * 2 + 1, y * 2 + 1), 255)

                outfile2.putpixel((x * 2, y * 2), 0)
                outfile2.putpixel((x * 2 + 1, y * 2), 255)
                outfile2.putpixel((x * 2, y * 2 + 1), 255)
                outfile2.putpixel((x * 2 + 1, y * 2 + 1), 0)
            else:
                outfile1.putpixel((x * 2, y * 2), 0)
                outfile1.putpixel((x * 2 + 1, y * 2), 255)
                outfile1.putpixel((x * 2, y * 2 + 1), 255)
                outfile1.putpixel((x * 2 + 1, y * 2 + 1), 0)

                outfile2.putpixel((x * 2, y * 2), 255)
                outfile2.putpixel((x * 2 + 1, y * 2), 0)
```

```
          outfile2.putpixel((x * 2, y * 2 + 1), 0)
          outfile2.putpixel((x * 2 + 1, y * 2 + 1), 255)



elif sourcepixel == 255:
       if coinflip < .5:
          outfile1.putpixel((x * 2, y * 2), 255)
          outfile1.putpixel((x * 2 + 1, y * 2), 0)
          outfile1.putpixel((x * 2, y * 2 + 1), 0)
          outfile1.putpixel((x * 2 + 1, y * 2 + 1), 255)

          outfile2.putpixel((x * 2, y * 2), 255)
          outfile2.putpixel((x * 2 + 1, y * 2), 0)
          outfile2.putpixel((x * 2, y * 2 + 1), 0)
          outfile2.putpixel((x * 2 + 1, y * 2 + 1), 255)
       else:
          outfile1.putpixel((x * 2, y * 2), 0)
          outfile1.putpixel((x * 2 + 1, y * 2), 255)
          outfile1.putpixel((x * 2, y * 2 + 1), 255)
          outfile1.putpixel((x * 2 + 1, y * 2 + 1), 0)
          outfile2.putpixel((x * 2, y * 2), 0)
          outfile2.putpixel((x * 2 + 1, y * 2), 255)
          outfile2.putpixel((x * 2, y * 2 + 1), 255)
          outfile2.putpixel((x * 2 + 1, y * 2 + 1), 0)

outfile1.save('out1.jpg')
outfile2.save('out2.jpg')
```

Code to show the result:

```
from PIL import Image
import sys

infile1 = Image.open(sys.argv[1])
infile2 = Image.open(sys.argv[2])
outfile = Image.new('1', infile1.size)

for x in range(infile1.size[0]):
  for y in range(infile1.size[1]):
    outfile.putpixel((x, y), max(infile1.getpixel((x, y)), infile2.getpixel((x, y))))
outfile.show()
```

CHAPTER -16

RESULTS

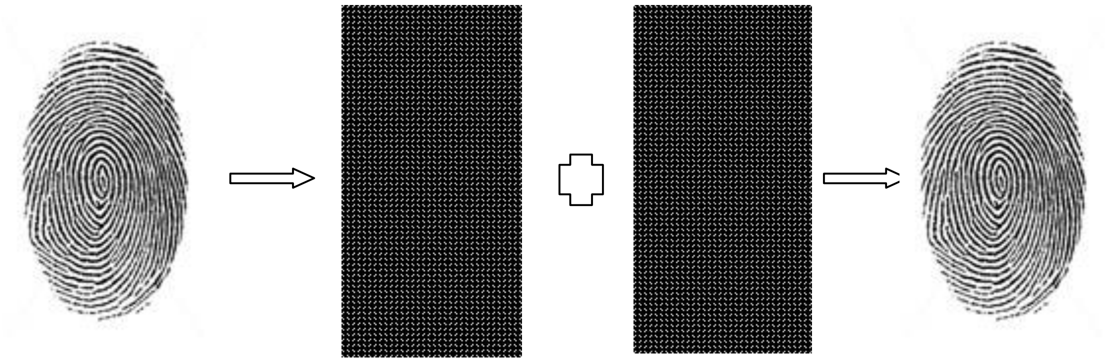
Report of test cases:

The test cases that are discussed above can be seen to have passed

A. 8-bit Gray Scale Image:

Example:

The algorithm has its implementation on gray scale image that is shown in Fig 6. 2 different shares S1 and S2 as shown in Fig 7 and Fig 8 respectively. After overlapping S1 and S2 the resultant image is shown in Fig 9.



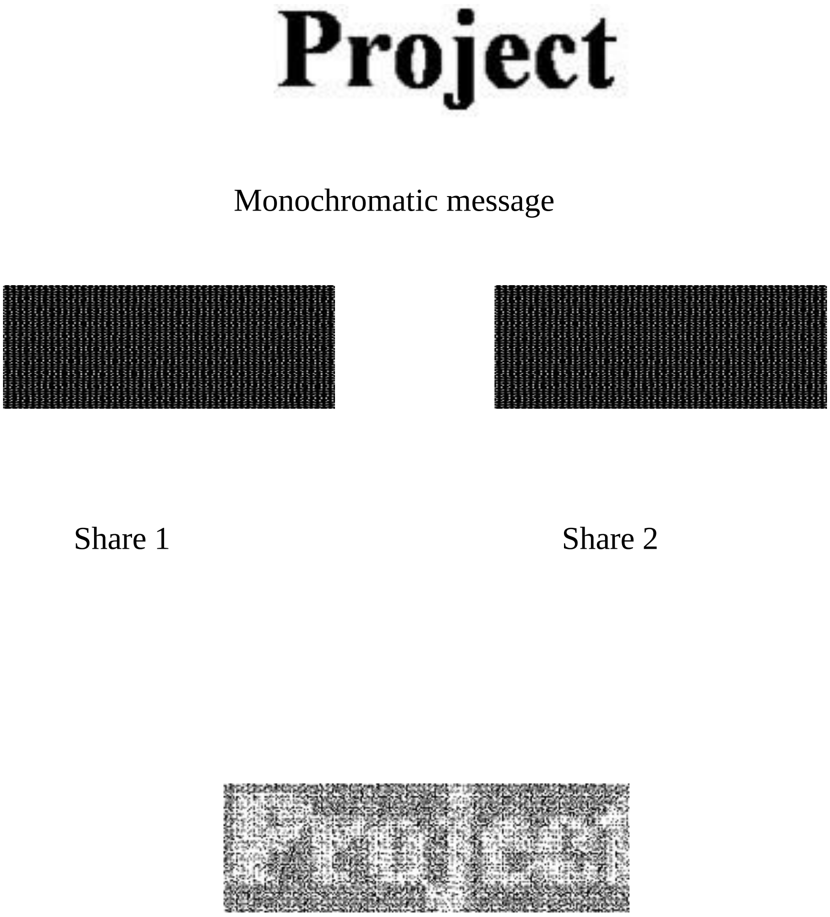
Gray Scale Image Share 1 Share 2 Resultant image

Fig 19 : 8 bit grey scale image result

B. 1-bit Black and White image:

Example:

The algorithm is also tested on B&W image as shown in Fig 10. 2 shares S1 & S2 are shown as Fig 11 & Fig12 . After overlapping S1 and S2 the resultant image is shown in Fig 13.



Monochromatic message

Share 1

Share 2

Resultant image

Fig 20: 1 bit B & W image result

CONCLUSION

The key logic behind the project is the splitting of the original image into two shared images, a randomly generated image and the other one is the key image and the secret image can be easily get back by performing least computation possible.

This project has the following merits:

(a) Retrieval of original image with completeness and integrity.

(b) Storage requirement for each share is same as no pixel expansion takes place.

(c) No quality change of the image.

(d) The logic in project is for gray scale images and B&W images.

Project checks the authentication where access to original image is given only when overlapped using right algorithm and right shares generated for the give image to reveal the original message. The secret image is accessed using combination of both the shares if any one of them is missing then the original or secret cannot be retrieved else if one does not have the right algorithm to overlap the image is not generated.

Visual cryptography is the current area of research where lot of scope exists. In this thesis, we have demonstrated the construction of basis matrices for 2-out-of-n, n-out-of-n, k-out-of-n VCS is demonstrated with examples. Also, using public key encryption, secret shares are made more secure which make secret image shares impossible to be altered by any third party. Visual secret sharing schemes with public key encryption technique ensure us for secure information transformation through a channel.

FUTURE SCOPE

Visual Cryptography has a lot of scope in future for encrypting images. The method used in the project produces the exact image similar to the original image or message to be sent. Randomly generated shares are for the i/p image, this technique is improvised by increasing randomness in shares.

A lot of work has already been done in the field of visual cryptography and technically the technique is sound enough and cryptanalysis is not so easy to do. Though seeing the immense vastness of the visual cryptography, it has not been implemented on a large scale. For example, these days top companies are using biometric sensors to take attendance. But, what they are missing is that most of low scale industries cannot afford the nuisances of a biometric sensor. Hence, using visual cryptography, a low cost solution can be established where multiple secrets are shared between users and the authenticator.

Besides this, a potential work lies in making visual cryptography size invariant, as increasing size of the output images lower the resolution of the images and hence making tougher for humans to decrypt them.

REFERENCES

1. Moni Naor, Adi Shamir,“Visual Cryptography”, Advances in cryptology, 1995

2. M. Naor and A. Shamir,1996. *Visual cryptography ii: Improving the contrast via the cover base*. Theory of Cryptography Library, (96- 07).

3. Sandeep Katta,“Visual Secret Sharing Scheme using Grayscale Images”, Department of Computer Science,Oklahoma State University Stillwater

4. Feng Liu and chuankun Wu.(2011), ‘Embedded Extended Visual Cryptography Schemes’, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 2, pp. 307-322

5. Swarnalata Bollavarapu and Ruchita Sharma-— Data Security using Compression and Cryptography Techniques

6. Kulvinder Kaur and Vineeta Khemchandani. ”Securing Visual Cryptographic Shares using Public Key Encryption”.2013 3rd IEEE International Advance Computing Conference (IACC).

7. https://en.wikipedia.org/wiki/Cryptography

8. https://www.tutorialspoint.com/cryptography/cryptography_tutorial.pdf

9. Ateniese, G.. "Extended capabilities for visual cryptography", Theoretical Computer Science, 20010106

10. Ida Christy, V. Seenivasagam. "Construction of color Extended Visual Cryptographic scheme using Back Propagation Network for color images", 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), 2012

11. Daisy, Annie, J. Arokia Renjith, P. Mohan Kumar, and L. Selvam. "Achieving Secrecy in Visual Secret Sharing Scheme Using Encrypted Images", Journal of Applied Security Research, 2014.

12. www.ijarcsse.com

13. www.ijsrcseit.com

14. Feng, J.-B.. "Visual secret sharing for multiple secrets", Pattern Recognition, 200812

Visual Cryptography - A Secure Medium

Aashutosh Sehgal[1], Abhinav Chaudhary[2], Aditya Sangwan[3], Ajay Sharawat[4], Vishal Jayaswal[5]

[1,2,3,4]*Student, Department of Computer Science and Engineering, Meerut Institute of Engineering and Technology, Meerut, India*

[5]*Professor, Department of Computer Science and Engineering, Meerut Institute of Engineering and Technology, Meerut, India*

***Abstract*: Secret information is main topic focused in systems used for communication an effective and secure protection is through encrypting the data. The data must be protected from being tampered by any process going on within the systems. Encryption of data is one of the methods to make sure that integrity and confidentiality of important information is available. The major role of encryption techniques is to prevent exposure of information to unnecessary individuals. Secret image sharing is also an alternative to consider as a solution to problems, especially for long detailed information so called as secret images. Nowadays with the increase in networking industry the transmission of images and other multimedia can be done easily. This use of secret sharing is increased because hackers can find the weak points of a communication system and attack to extract confidential information being transmitted over the network.**

***Keywords*: Visual cryptography, Security, Secretly data sharing, Visual Cryptography.**

1. Introduction

Visual cryptography was firstly discovered by Noar and Shamir in 1994. Encryption of a visual information using the cryptography technique such that the decryption is only possible using proper orientation of images or with the right algorithm for overlapping. Transferring multimedia information using Internet is very common these days. Various techniques and methods have been developed to solve the problem of sharing of secret images and these tools can be used to resolve this problem. The splitting of images should be done such that even hacker is able to make available any share but is not able to get any information out of it. In today's scenario of electronic commerce, the need to solve the issue of sharing information safely considering the fact of using network as medium of sharing information. Regular efforts of hackers to gain secret information are done as a result of which there is an urgent need to make both communication medium as well as communication tools and techniques safe and secure. The scheme of visual secretly sharing of the image is to eventually divide it into 'n' total shares. As all 'n' shares are combined, the secret image is created. The benefit of using this technique is that even if the hacker gets 'n-1' shares they would not be able to get the main secret image as all the 'n' shares are required to generate the secret image.

2. Literature review

The main operation of Visual Cryptography is based on the use of binary inputs. As the binary data is displayed transparent when imprinted on screen that is transparent itself. Smaller blocks are used to divide every pixel of the secret image. Same numbers of black and white blocks are present in the image or the blocks. Only 1 black and 1 white block is there if any of pixel is split into two parts. And so on goes on if pixel gets split in 4 parts, 2 black and 2 white blocks are formed out of it. Fig. 1 shows an example for division into 2x2 blocks and Fig. 2 is superimposed image.

Figure 1: Two 2 × 2 pixel blocks

Figure 2: Superimposed Image

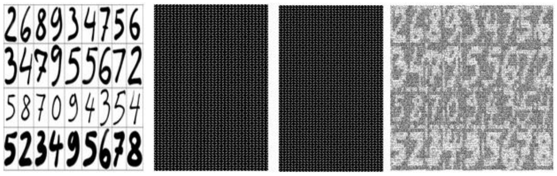


Fig. 3. Example of Visual Cryptography

Visual secret sharing is the most simple out of problems of messages that comprise of black and white pixels and each pixel is handled separately. 'n' modified shares are generated for each original pixel that appears, one for each transparency. 'm' black and white sub-pixels are formed for each share, they are imprinted as close pattern to each other such that visual system create a median of the separate black as well as white versions. Structure that is formed by shares and contribution can be explained by Boolean matrix which is (nxm) and S is expressed [sij], where *sij*->1 and when the jth pixel is black in transparency. The framework is almost similar to the Naor and Shamir whereas the important difference that their framework that divides into 'n' shares of binary secret image. The 'm' sub pixels are used to explain each pixel of image. Black and white schema of visual cryptography is illustrated by a Boolean matrix of the form 2(n x m) where (S0 and S1). Main image i.e.

white pixel image is represented using S0 and but if main image is black then S1 is used instead. Representation of white and black pixel is done by 0 and 1 respectively in the technique of visual cryptography. Various visual cryptography techniques are used eg. 2 / 2, 2 / n, n/n and k/n. The 2/2 is the widely taken in use to explain the Visual Cryptography schema.

The 2/2 Visual Cryptography technique S1 and S0 is expressed as,

$$S0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \quad S1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

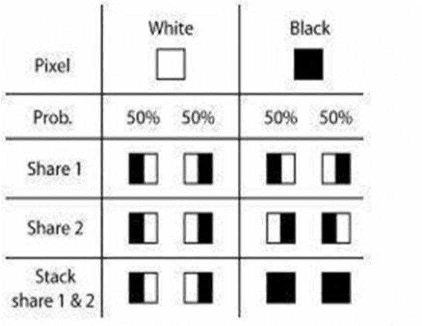


Fig. 4. Formation of 2 by 2 VC schema

Two different Q0 and Q1 matrices. We select the matrix Q0 to give a white pixel and the matrix Q1 is used give a black pixel. The very initial row of selected matrix is for the share S1 and the row after the is for the share S2.

The encoding of every pixel of the main image into two sub pixel is the disadvantage and if main image sized S x S is positioned by share and is sized as S X2S. Due to the distortion present we take 4 sub pixel as design layout. Also the expansion of pixel is 2 by 2 pixels.

$$S0 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix} \quad S1 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

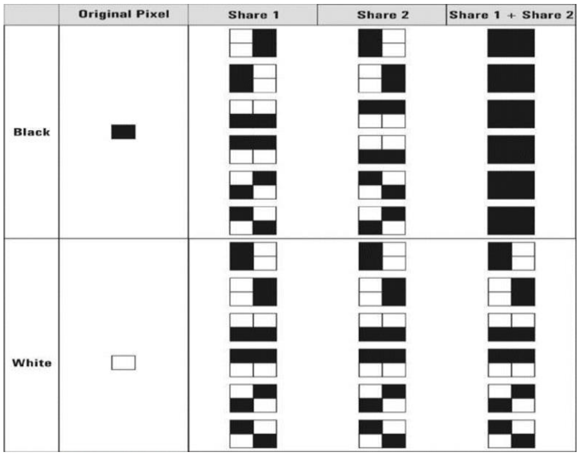


Fig. 5. Illustration of 2 X 2 Visual Cryptography technique using a layout design of 4 sub pixel

3. Proposed algorithm

Our project uses an advance technique of Visual Cryptography where an image is taken and eventually divided as 2 shares. Share 1 also called random share whereas the share 2 is main/key share that contains confidential information. The shares share 1 and share 2 have nothing in common to the secret image. The combination of the shares by XORing generates the secret image. There is no change in the quality of image created and the secret image. This algorithm has efficient recombination property and there is no loss of pixel so far. The use of algorithm is only bound for Black and white images without the loss of pixel.

Algorithm:
Step 1: Generation of random share
Step 2: Generation of key share
Step 3: Combining both the shares to generate secret image

In given step 1: For monochrome image a random share is generated for every pixel that has either 0 or 1 as it's value. So, by picking randomly either 1 or 0 the random share would be created. Share size is same as that of the secret image. Different value is generated for each pixel each time a random share is created. Therefore, 2 randomly generated shares of the original image can never be equivalent.

In given step 2: XORing is the technique used to for key share generation where each and every pixel taken from the share randomly created is XORed with each and every pixel of the secret image. No change in size of original image and share can be seen. As it is seen that no 2 randomly generated shares can be same as a result of which no 2 key shares can be same.

In given step 3: XORing of randomly generated share and key share pixel after pixel is done to find the overlapping or resultant image. The result of which is the generation of the desired secret image.

For Monochromatic Images

```
Algo RaKeOv ( )
 For each pixel j=0 to n
{
       RaSj = Ra (0-1)
       KeSj = DSj ⊕ SIj
}
SI = DS ⊕ JS
 }

/* SI = Secret Image, DS=Random Share, JS=Key Share*/ *
```

4. Results and Discussions

Report of test cases:

The test cases that are discussed above can be seen to have passed.

A. 8-bit Gray Scale Image

Example:

The algorithm has its implementation on gray scale image that is shown in Fig. 6. 2 different shares S1 and S2 as shown in Fig. 7 and Fig. 8 respectively. After overlapping S1 and S2 the resultant image is shown in Fig. 9.

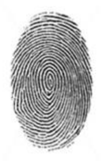


Fig 6. Gray Scale Image

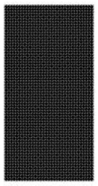


Fig 7. Share1

Fig 8. Share2

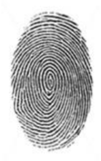


Fig 9. Resultant image

B. 1-bit Black and White image

Example:

The algorithm is also tested on B & W image as shown in Fig. 10. 2 shares S1 & S2 are shown as Fig. 11 and Fig. 12. After overlapping S1 and S2 the resultant image is shown in Fig. 13.

Fig. 10. Monochromatic message

Fig. 11. Share1

Fig. 12. Share2

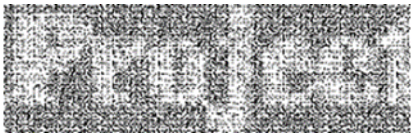


Fig. 13. Resultant image

5. Conclusion

The key logic behind the project is the splitting of the original image into two shared images, a randomly generated image and the other one is the key image and the secret image can be easily get back by performing least computation possible.

This project has the following merits:

a) Retrieval of original image with completeness and integrity.
b) Storage requirement for each share is same as no pixel expansion takes place.
c) No quality change of the image.
d) The logic in project is for gray scale images and B & W images.

Project checks the authentication where access to original image is given only when overlapped using right algorithm and right shares generated for the give image to reveal the original message. The secret image is accessed using combination of both the shares if any one of them is missing then the original or secret cannot be retrieved else if one does not have the right algorithm to overlap the image is not generated.

6. Future scope

Visual Cryptography has a lot of scope in future for encrypting images. The method used in the project produces the exact image similar to the original image or message to be sent. Randomly generated shares are for the i/p image, this technique is improvised by increasing randomness in shares.

References

[1] Moni Naor, Adi Shamir, "Visual Cryptography", Advances in cryptology, 1995.

[2] M. Naor and A. Shamir,1996. Visual cryptography ii: Improving the contrast via the cover base. Theory of Cryptography Library.

[3] Sandeep Katta, "Visual Secret Sharing Scheme using Grayscale Images", Department of Computer Science, Oklahoma State University Stillwater

[4] Feng Liu and chuankun Wu. (2011), 'Embedded Extended Visual Cryptography Schemes', IEEE *transactions on information forensics and security*, vol. 6, no. 2, pp. 307-322.

[5] Swarnalata Bollavarapu and Ruchita Sharma, "Data Security using Compression and Cryptography Techniques."

[6] Kulvinder Kaur and Vineeta Khemchandani, "Securing Visual Cryptographic Shares using Public Key Encryption," 2013 3rd IEEE International Advance Computing Conference (IACC).

[7] https://en.wikipedia.org/wiki/Cryptography

[8] https://www.tutorialspoint.com/cryptography/cryptography_tutorial.pdf

[9] https://en.wikipedia.org/wiki/Cryptography

[10] Ateniese G, "Extended capabilities for visual cryptography", Theoretical Computer Science.

[11] Ida Christy, V. Seenivasagam. "Construction of color Extended Visual Cryptographic scheme using Back Propagation Network for color images", 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), 2012.

[12] Daisy, Annie, J. Arokia Renjith, P. Mohan Kumar, and L. Selvam, "Achieving Secrecy in Visual Secret Sharing Scheme Using Encrypted Images", Journal of Applied Security Research, 2014.

[13] Feng, J. B, "Visual secret sharing for multiple secrets", Pattern Recognition.