A Secure Visual Cryptographic Scheme based on Two Level Sharing

Urvashi Yadav
MTech
Mody University of Science and Technology,
Laxmangarh, Sikar, India

Nisheeth Saxena
Assistant Professor, Faculty of Engineering and Technology
Mody University of Science and Technology,
Laxmangarh, Sikar, India

ABSTRACT
Visual cryptography allows the information to be encrypted using an encoding system. It does not require a computer to decode. Two transparent images are used in Visual Cryptography. One image contains the secret information and the other image contains random pixels. It is impossible to reveal the secret information from one of the images as both transparent images are required to retrieve the information. In this paper, we are working on the security of visual cryptography. Here we purpose a new scheme called three level sharing. In this case, we enhance the security of an image by dividing into shares and then after sub shares. For this purpose, stamping algorithm is used**.**

Keywords
Visual Cryptography, Stamping Algorithm, Pixel Sharing, Security, images

1. INTRODUCTION
Visual cryptography is a cryptographic technique which allows visual information to be encrypted in such a way that the decryption can be performed by humans. Cryptographic scheme can decode concealed images without any cryptographic computations. This scheme is use to extends the visual variants up to their secret sharing problem. In this case, dealer provides a transparency to each n user, any k of them can see the image by stacking their transparencies, but any k -1 of them gains no information about it.

Many years ago, Naor and Shamir [1] described a new (k; n) visual cryptographic scheme using black and white images, where the dealer encodes a secret image into n participants. In the given scheme, shared secret information can be revealed without any cryptographic computations. In order to share a secret black and white image, the concept of their scheme is to transform one pixel into two sub-pixels and divide each sub-pixel into two color regions. The sub-pixels are represented as half white and half black.

In the Visual secret sharing scheme, the secret picture is shared among many users. Hence the picture is divided into n number of transparencies. In this case, if total numbers of transparencies are placed together than the image become visible. If any share or we can say transparency is missing from the total numbers of transparencies than it is not visible to user.

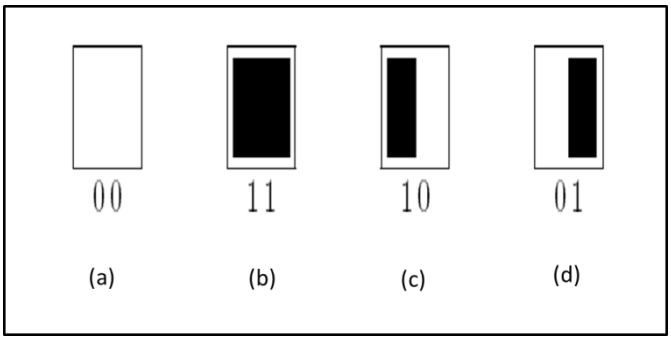

Figure 1: Different types of pixels along with the representation.

In the case (a), white pixels are shown whereas in case (b) black pixels are shown. In case(c) LB pixel are shown and in case (d) RB pixel are shown. In the figure 1, different types of pixels are represented. The first is a white pixel, the next is a black pixel, and the last two are grey pixels. In case of grey pixels the black and white portions are different.

Visual Secret Sharing scheme uses mathematical secret sharing but when implements in hardware, should be printed on transparencies. Once it is created, it requires no technology or algorithm, and however resolution and contrast is lost as well.

Basic concept of 2-out-of-2 VC scheme [2]
Visual cryptography scheme where 2 shares are generated from the original secret image and by stacking together the secret is reveal. This is the basic step of the technique, however if we create equal to or more than 2 shares and if some or all of them staked to reveal the secret image is called visual secret sharing. Figure 2 shows the basic behind this scheme.

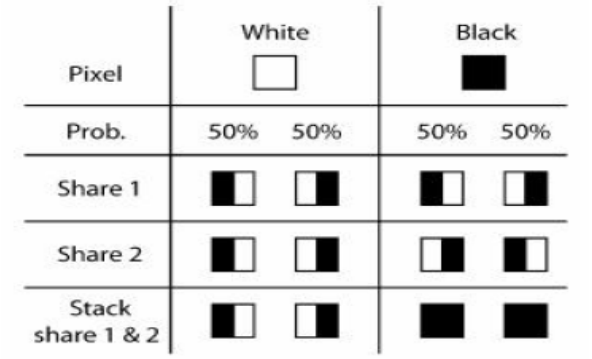

Figure 2: Basic concept of 2-out-of-2 VC scheme

In this concept one white or black pixel will divide into two sub pixels. This can be shown with the help of the above

figure in which the pixel division is done. It states that the shares 1 and 2 are stacked together and gets the result in the form of complete black or gray. Because of this when we stacked the shares the white in original secret image become gray in the stacked result.

2. LITERATURE REVIEW

Rao *et al* [3] discuss about the security in visual cryptography. In the visual cryptography, the secret image consists of a collection of black and white pixels. A row in a matrix corresponds to sub-pixels of a pixel, where 1 denotes the black sub-pixel and 0 denotes the white sub-pixel. Each pixel of the original image will be encoded into pixels; each pixel will consists of sub-pixels on each share. Since a matrix constitutes only one pixel for each share. For security reasons, the number of matrices must be huge. For short description and easy realization of the VC construction, we do not construct and directly. Each white pixel in the original image is split into two of the same small blocks that have half white and black pixels. When these two blocks are overlapped on each other, they line up exactly, and results in a light-colored block. Each black pixel in the original logo is split into two complementary small blocks. When these blocks are overlapped, the result is a complete black box. Encryption methods are one of the popular approaches to ensure the integrity and confidentiality of the protected information. However one of the vital vulnerabilities of encryption techniques is protecting the information from being exposed.

Justin *et al* [4] discuss about the color visual cryptography algorithm. Visual Cryptography is a special type of encryption technique. It is used to hide information in images. The decryption of the images can be performed by the human vision, if the correct key images are used. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet. In the visual cryptography, image is divided into several parts. Each part is decrypted to share the secret information behind it. Traditional Visual Cryptography suffers from share identification problem. Extended visual cryptography is the solution for this problem. In the extended visual cryptography a cover image is add in each share. In this paper, author proposes a general approach to solve the problems, like pixel expansion and share identification. This approach can be used for color secret images. The advantage of the proposed scheme is the encryption phase is not only applicable to extended VCS but also to traditional VCS to construct shares without any pixel expansion.

Kester [5] discuss about the visual cryptographic encryption technique for securing medical images. Medical information of patients are sensitive and needed to be protect during storage. Hence the usage of cryptography in the protection of such data is very crucial. In cryptography, encryption processes are used in transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge. Visual cryptography encodes a secret binary image into various shares of random binary patterns. The secret image can be decoded visually by superimposing a qualified subset of transparencies, but no secret information can be gained from the superposition of a forbidden subset. Digital encryption of medical images before transmission and storage is proposed as a way to effectively provide protection of patient information. This paper presented a visual cryptographic technique for encrypting of medical images before transmission or storage of them.

Chhabra [6] discuss about the visual Cryptographic Steganography in Images. Cryptography involves converting a message text into an unreadable cipher, whereas steganography embeds message into a cover media and hides its existence. Visual steganography is one of the most secure forms of steganography used today. It is most commonly implemented in image files. Both these techniques are combined together to achieve higher levels of security, but there is a need of a highly secure system to transfer information over any communication media minimizing the threat of intrusion. In this paper, author proposed an advanced system of encrypting data that combines the features of cryptography and steganography along with multimedia features of data hiding. Steganography is the art of secret communication. Its goal is to transmit a message hidden inside another visible message. Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is applied. Visual Cryptography uses two transparent images. One image contains the secret information and the other image contains the random pixels. In the visual cryptography, each pixel of the images is divided into smaller blocks. There are always the same numbers of white and black blocks. If a pixel is divided into two parts one will be white and the other will be black block. If the pixel is divided into four equal parts then there will be two white and two black blocks.

Verma *et al* [7] discuss about the visual cryptography of secret sharing images. Visual cryptography scheme is a secure method that is used to encrypt the secret image by breaking it into shares. Shares are binary images that are presented in transparencies. Each participant holds a transparency or we can say share. The visual cryptography needs no complicated computation for recovering the secret. The visual cryptographic scheme can visually decode the secret image by superimposing shares without computation. In this paper, author uses the digital watermarking in visual cryptography. Digital watermarking is used for providing the double security of image shares. Every pixel of the binary visual cryptography share is embedded into the individual block of the host image. The method of watermark extraction necessitates only the watermarked image and it does not require the original host image. Watermarking can be divided into Non blind, Semi-Blind and Blind schemes based on the requirements for watermark extraction or detection. The secret shares are protected from attacks of cheating. The decryption will be same as it is done in the visual cryptographic model.

Zhang *et al.* [8]: In the VSS schemes the gray scale images are used. It is also known as the chromatic images. The pixel block is used as encoding method. The encoding method is proposed in this paper. In this paper, a novel multi pixel encoding method is used. it is a new method that is used in the visual cryptography. It helps to encode more than one pixel in each run. The efficiency of the encoding is very low. In this paper, author presents a new approach which helps in multi pixel encoding. During the scanning period, the length of encoding at one run is equal to the pixel that met during this period of time. In this paper, the main focus is on the access structure and the chromatic images. These images are used without any pixel expansions. It provides the high efficiency for encoding the images.

Yan *et al.* [9]: In this paper, visual cryptography is a secret sharing scheme which is used for the extended images. Visual cryptography contains distinguish characteristics. It has the ability of secret restoration; it can't use the computation results. The visual cryptography is difficult in use of practice. The shares of visual cryptography are printed on transparencies. In the visual cryptography the noise distortion is the big issue. Many visual cryptography applications used the shares in this case, the scanning of the shares is compulsory. The print and scan operations can create the noise. It also makes the alignment very difficult. Here, author discussed the various problems like precise alignment of printed and scanned visual cryptography shares. In this case, the frequency domain alignment scheme is developed.

3. PROPOSED WORK

Advances in the cryptographic secure data embedded imaging technology has led to an exponential growth in the Number of digital images that needs to be acquired, analysed, classified, stored and Retrieved in medical centres. As a result, cryptographic secure data embedded image classification and retrieval has recently gained high interest in the scientific community. Despite of many trials, the proposed solutions are still far from being sufficiently accurate for real-life implementations. It's a given - disaster will strike your cryptographic secure data embedded imaging data at some point in time. No matter how good your IT network is, some types of disaster cannot be prevented, including such natural occurrences as hurricanes and floods. In this thesis, we are working on the security of image. Here we are going to divide an image into two different shares. Then these shares are further divide into sub shares. This is comes under the encryption process.

While in case of decryption process, we have to select all these shares to decrypt an image. If any of the share is missing, it will not show the original image. For this purpose, we are going to use pixel sharing and stamping algorithm. The stamping algorithm is used for overlapping whereas pixel sharing is help in divide the image into several segments. To solve the problem of image data security, we use the stamping algorithm and share pixel images. As stamping algorithm, sticks extra black pixels on shares. In this case, the stuck black pixels are appearing on the regions where the shared pixels are white in colour and cover pixels are black in colour. There are two major issues present in this algorithm.

1. It preserves the security property of i-shares.
2. It keeps the contrast of reconstructed images as high as possible.

In the given image i.e. Figure 3, we take one image as input and create the shares of this image. After that we make the sub shares of these shares. Then we overlap these shares with the help of stamping algorithm and then an output image is generated after this process. This image is same as the previous one.

Algorithm used for the generation of the shares:

Step1:- Pixel S_{ij} with position i and j is the input called original pixel.

Step2:- Apply pixel reversal i.e. $S_{ij}' = 255 - S_{ij}$.

Step3:- Use random number from 0.1 to 0.9 to reduce S_{ij}' randomly.

Step4:- Take the difference of S_{ij}' with original pixel S_{ij} .

Step5:- Use random number to reduce reversed value of S_{ij}' randomly.

Step6:- Apply pixel reversal i.e. $S_{ij}'' = 255 - S_{ij}'$

Step7:- Store in matrix as image called share 1.

Step8:- Take the difference of two random number generators with original pixel S_{ij}''.

Step9:- Apply pixel reversal i.e. $S_{ij}''' = 255 - S_{ij}''$.

Step10:- Store S_{ij}''' in matrix as image called share 2.

Step11:- Repeat point 1 to 10 for all pixels from original image (i.e. matrix of original image)

Given is the flow chart of the proposed methodology.

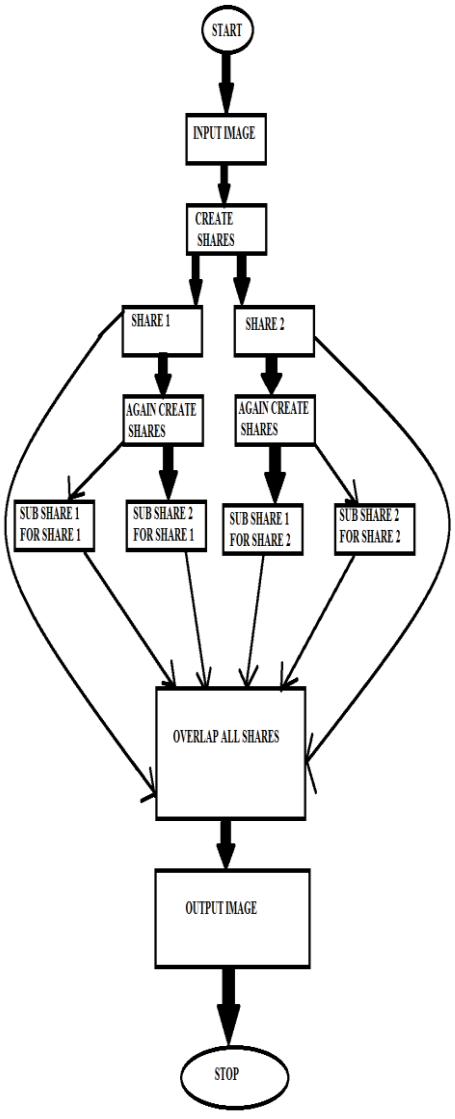

Figure 3: Proposed Schema

4. RESULTS AND DISCUSSIONS:

In this case, we do the three level sharing securities in the visual cryptography. Here we create the shares of an image and after that sub shares of these images are generated. By selecting all these shares we can get the image as an output.

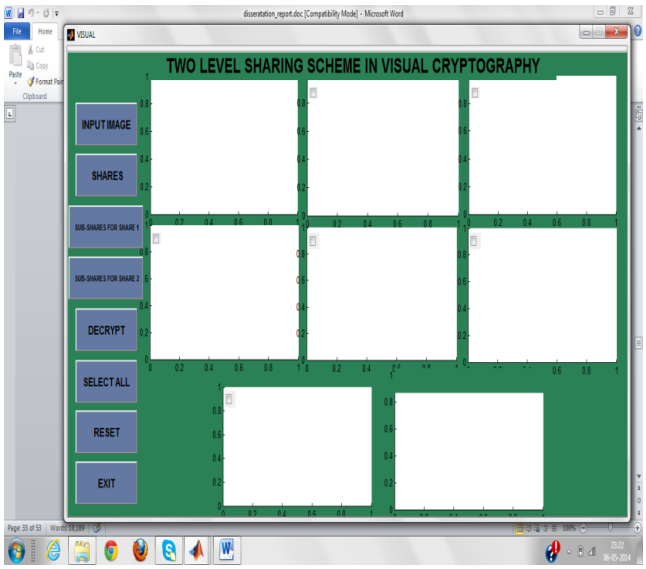

Figure 4: Implementation Snapshots

Here in this case, a GUI is shown. There are the buttons named input image, shares, sub-shares for share 1, sub-shares for share 2, decrypt, select all, reset, exit. All the butons perform their function with respective to their names. With the help of the input button we can upload the image.

On clicking on the input button, a pop-up window will open that will ask for the address of the required image. It helps in taking the input of an image by the user. The user can easily find the image by giving the address .

Input Image:

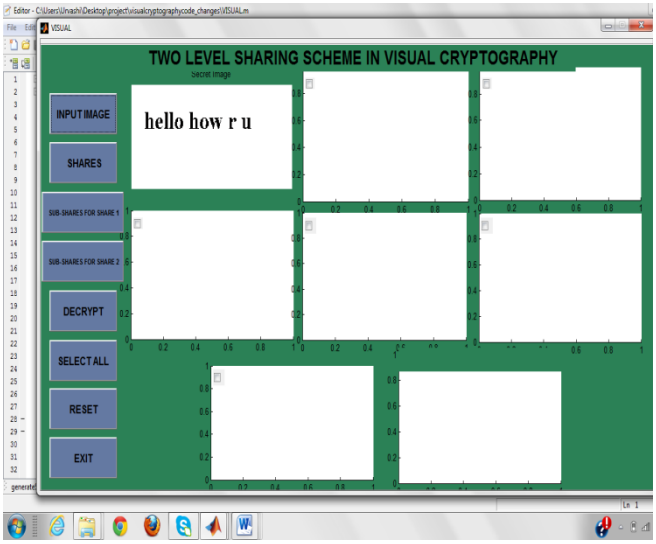

Figure 5: Implementation Snapshots

Here we upload the image, that we want to decrypt. Here we upload a image by just click on it.

Share Generation:

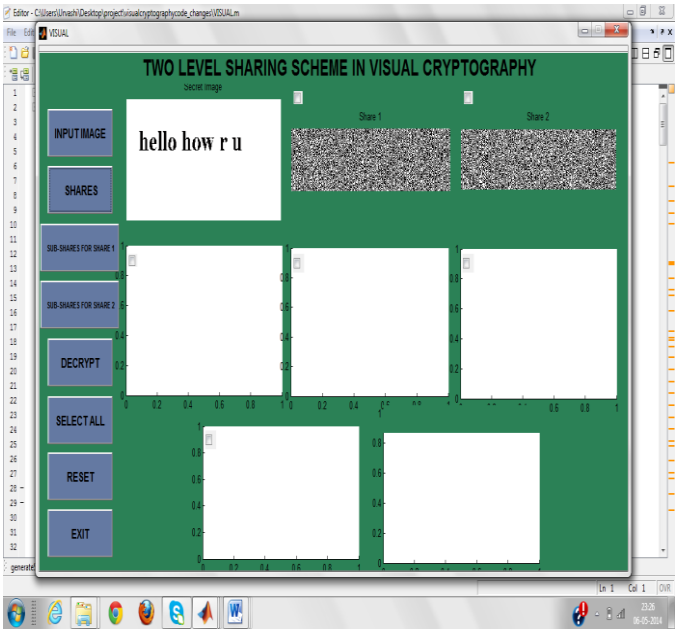

Figure 6: Implementation Snapshots

Now, by clicking on the shares button, two shares will be generated. The shares are in such a way that either of the share will reveal no information of the secret image.

Here when we click on share image. Two shares of images are created. It is defined as share 1 and share 2.

Creation of Sub-Shares:

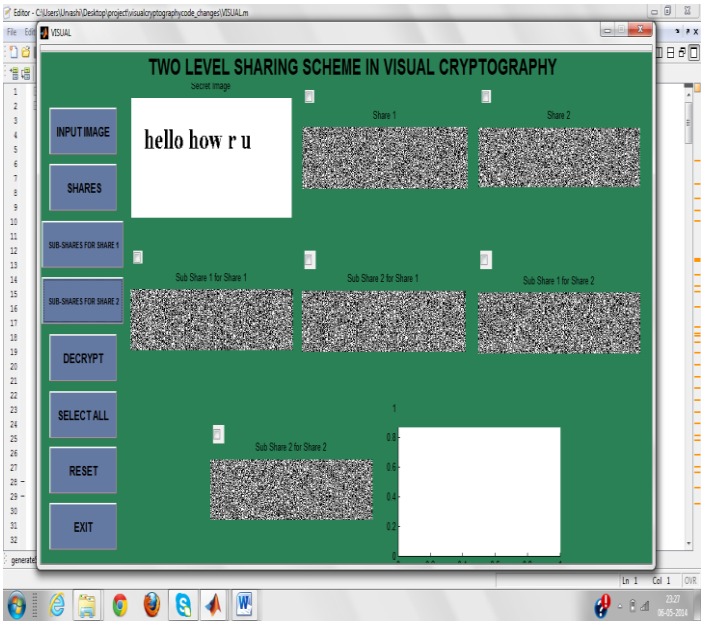

Figure 7: Implementation Snapshots

Here when we click on the button named sub share for share 1, Two shares of the share 1 are created. It can defined as sub share 1 for share 1 and sub share 2 for share 1. And when we click on sub share for share 2. Two sub shares of images are created. It is defined as sub share 1 and sub share 2. Now all the shares and the sub shares of the shares are shown in the fig. at their respective places. After generating the shares then

we have to decrypt the image to reveal the secret image or to show the message written in the image.

Decryption of Image:

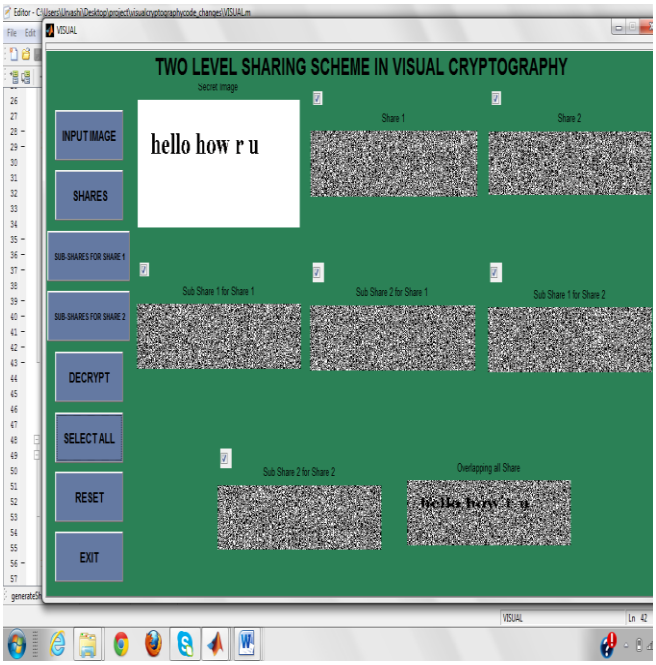

Figure 8: Implementation Snapshots

In this case, it show the decryption message after selecting all the parts. In this case, we have selected all the shares by clicking on the check mark provided on the left corner of the each share. We can also selct all the shares instantly with the help of the select all button. This button ticks all the boxes at once and no need to select each share separately. Depending on the user, how he wants to select the shares. After selecting the shares when we click on the decrypt button the it will overlap all the shares on one another to reveal the secret image. And hence, it shows the decryption of the image. The decrypted image is named as ”overlapping all shares”. The quality of the image will be degraded a little.

The method is applied on the other image as well, the results is shown in the next given figure 9.

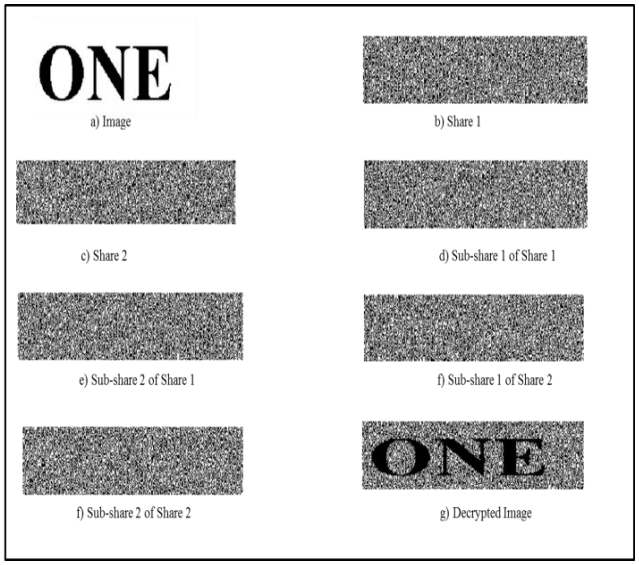

Figure 9: Implementation Snapshots

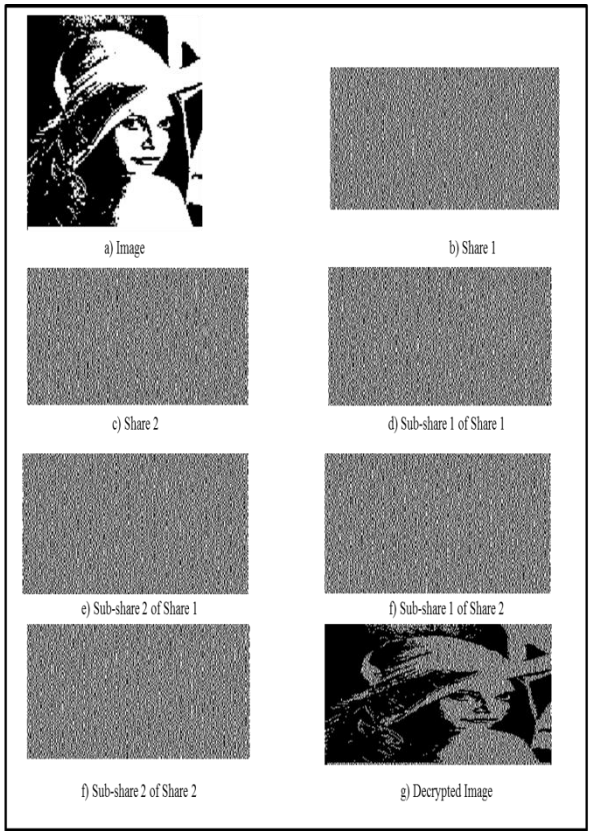

Figure 10: Implementation Snapshots

5. CONCLUSION

This paper describes how the work of the visual cryptography is done. It shows how an image can be decrypted very securely without any need of computation algorithm for decryption. Decryption can be done by overlapping the shares on each other or by human vision. The shares of an image are generated in such a way that all the shares that are stacked together are able to reveal the image as decrypted image. No other means of decryption is done. The shares of an image are generated, and then the sub shares of the shares are generated. This provides much security to the shares. All the shares are compulsory for decryption that is why there will be no meaningless shares. All the shares are meaningful as each share has the information that is required at the time of decryption.

6. REFERENCES

[1] M. Naor, A. Shamir, in: A. De Santis (Ed.), “Visual Cryptography, Advances in Cryptology: Eurpocrypt’94”, Lecture Notes in Computer Science, Vol. 950, Springer, Berlin, 1995.

[2] Shamir, “How to share a secret,” *Common. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[3] R Yadagiri Rao Secure Visual Cryptography , International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 1 Jan 2013 Page No. 265-303.

[4] Juby Justin1 and Giss George, An Extended Color Visual Cryptography Algorithm for General Access Structures International Journal for Advance Research in Engineering and Tecnology,2013.

[5] Quist-Aphetsi Kester, MIEEE, A Visual Cryptographic Encryption Technique for Securing Medical Images, International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 6, June (2013) 496.

[6] Neha Chhabra, Visual Cryptographic Steganography in Images, IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.4, April 2012 , Manuscript received April 5, 2012 Manuscript revised April 20, 2012.

[7] Jagdeep Verma, Dr.Vineeta Khemchandani, A Visual Cryptographic Technique to Secure Image Shares, Jagdeep Verma, Dr.Vineeta Khemchandani / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 1,Jan-Feb 2012, pp.1121-1125 1121.

[8] Haibo Zhang, Xiaofei Wang, Wanhua Cao, Youpeng Huang, "Visual Cryptography for General Access Structure Using Pixel-block Aware Encoding", Journal of Computers, Vol. 3, No. 12, December 2008.

[9] Wei-Qi Yan, Duo Jin, Mohan S Kankanhalli, "Visual Cryptography for Print and Scan Applications", Circuits and Systems, ISCAS, Proceedings of the 2004 International Symposium on (Volume: 5), 2004.