Visual Cryptographic Proposal for Enhancing Privacy of Image Using Shares Technique

Shalu Rani [1], Dr. Aman Jain [2]
Department of Computer Science
[1] Research Scholar, Singhania University, Jhunjhunu Rajasthan, India
[2] Professor, Maharishi Arvind Institute of Science and Management Jaipur, India

Abstract- *Visual Cryptography is the strategy for cryptography that encodes any visual data, (for example, pictures, text, handwritten and so forth.) such that decryption is finished by utilizing human visual framework without the assistance of computer. Because of quick movement of information trade through web, data security has turned out to be more imperative in information transmission and capacity. Due to very use of images in mechanical process, it is vital to shield the private images information from unauthorized get to. In this paper, the sharing of secret image with third party has been performed in the proposed work and the third party should be trusted. For the security, the third party uses visual cryptography for generating two shares. But theses shares should be transformed into QR code before sending it to various servers and diverse image media used here for the conversion of shares into QR code. The key features of original image are considered for the encryption of the shares to QR code performed by third party. The proof of concept implementation and security analysis of the proposed model is discussed within the paper.*

Keywords- Cryptography, Secret Image, Pixel, QR Code, Shares and Server Database

I. INTRODUCTION

Cryptography is a way through which information can be made invisible to the users by encrypting them. It is the examination and usage of methods to conceal data, or just to protect a message or content from being perused.

Visual Cryptography

Visual cryptography is a viable encryption technique to cover data in images with the end goal that it can be unscrambled by the human vision if the right key image is used. Visual Cryptography Schemes (VCS) is a system of image encryption n novel to shroud the secret data in images. Visual cryptography system was presented by Naor and Shamir in 1994 as an option for conventional cryptography [1]. It uses two or more transient images (called shares). One picture contains arbitrary pixels and the other picture contains the secret information that is hidden. It isn't conceivable to recuperate the secret data from any of the pictures (images). Either transparent images or layers are required to uncover the secret information. In the overlay animation it can be seen by sliding the two layers over each other until the point when they are effectively adjusted and the concealed data appears [2]. It is thought to be a binary image and every pixel is dealt with independently. Every unique pixel shows up in n adjusted renditions (called shares) of the image, one for every transparency. Each offer contains m high contrast sub pixels. Each offer of the sub pixels is imprinted on the transparency in close proximity.

II. VISUAL CRYPTOGRAPHY PROCESS

The process behind VC is to generate shares randomly based on the input date (image) in such way that the outputs can stack together to show the input. Expecting that the message being scrambled is a binary image with p pixels, each of these pixels are separately encoded with a subpixel gathering with s pixels [3]. This permits n shares to be created utilizing these subpixel groupings. Each offer is a gathering of m black and white subpixels. These subpixel groupings are ordinarily square to not contort the angle proportion of the original image [3]. Nonetheless, subpixel groupings that are not square do occur in VC algorithms and the viewpoint proportion of the image is modified appropriately. This structure can be portrayed as a n×m Boolean framework S. The structure of S can be depicted along these lines: S = (sij) m×n where sij = 1 or 0 iff the jth sub-pixel of the ith share is black or white. The imperative parameters of the scheme are [4]:

- m, the quantity of pixels in an share.
- α the relative distinction in the weight between the joined shares that originate from a white and dark pixel in the original image (the loos conversely).
- γ the extent of the accumulation of C0 and C1.
- C0= the sub pixel designs in the shares for a white pixel.
- C1= the sub pixel designs in the offers for a black pixel.

The Hamming weight H (V) of the ored m-vector V is translated by the visual framework as [3]:

- Interpreted as dark if H(V) ≥ d for edge d
- Interpreted as white if H (V) ≤ d-α m for relative distinction α >0
- 1 ≤ d ≤ m.

The offers can be produced in the accompanying way:

- If the pixel of the original binary image is white, randomly pick a similar example of four pixels for the two shares.
- If the pixel of the original image is black, pick a correlative match of examples, the most usually utilized subpixel groupings in VC calculations are appeared in Figure 1. The age of the offers depends on the estimation of the pixel and the likelihood of a subpixel group occurring [3]. A share age conspire relating to k=2 and n=2 is appeared in Figure 2. This is connected to a binary image by allocating the comparing subpixel gathering to the pixels all through the picture. These outcomes in two random offers where the message can't be recognized.

Fig1: Shares most commonly used for Visual Cryptography [5].

As figure 2 portrays a pixel is isolated into four sections, can have six distinct states. On the off chance that a pixel on share 1 has a given express, the pixel on share 2 may have one of two states: indistinguishable or upset to the pixel of offer 1[5]. On the off chance that the pixel of offer 2 is indistinguishable to share 1, the overlaid pixel will be completely black. This is a data pixel.

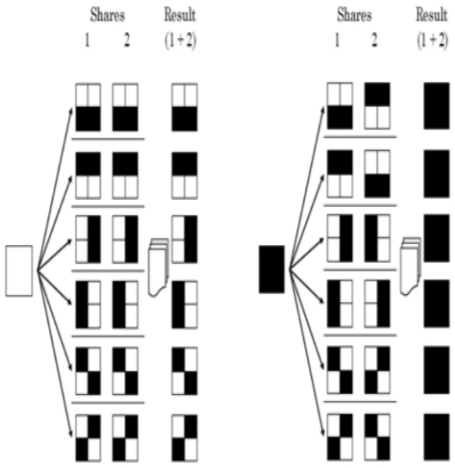

Fig 2: A Share generation scheme corresponding to k=2 and n=2[5].

In the event that the pixel conditions of offer 1 are truly (crypto secure) random, both empty and data pixels of offer 2 will likewise have totally random states [5]. One can't know whether a pixel in share 2 is utilized to make a grey or black pixel, since we require the condition of that pixel in share 1 (which is random) to know the overlay result.

III. ANALYSIS OF VISUAL CRYPTOGRAPHY TECHNIQUE

- Error Diffusion tends to upgrade edges in a image. At the point when a image has a change from light to dark the error diffusion algorithm tends to make the following produced pixel be black. Dark to light changes tend to bring about the following produced pixel being white. This causes an edge enhancement impact to the detriment of gray level multiplication exactness. This outcomes in error diffusion having a higher obvious determination. This is particularly valuable with images with content in them. Along these lines, that the content in the image wind up noticeably more keen and makes more intelligible. In both secret share age and decoding part, or task is utilized, which makes the plan extremely basic [6].

- The gigantic extension in shares influences the space intricacy. While superimposing the offers of dynamic visual cryptography, the greater transparencies are required. Extension less hierarchical visual cryptography is the solution for diminish this development in the offers. The prerequisite of this proposed technique is that the mystery ought to be in binary form i.e. highly contrasting passwords, signatures, handwritten content and so forth [6].

- Anti-phishing system safeguards the privacy of captcha. It accomplishes this by separating the first image into two offers which are to be put away in various databases. The decryption is conceivable just when enemies can give both shared at once. The individual shares can't reveal the first captcha. It forestalls secret word and other private data from the phishing website. It is also useful to prevent the attacks of phishing websites on financial web portal, banking portal, online shopping market.

- It gives a sheltered and secure transmission as it includes numerous controls for encryption as is it with decryption This System provides a simple user interface to process images. Furthermore, the proposed system is very easy to use and anybody can use this system without having any cryptographic knowledge. It also does not provide the reduction of the size of the covering shares in any way. It is a lossless compression algorithm [6].

IV. LITERATURE SURVEY

Yamini Ravella et al. [2017] in this paper, cryptography is the investigation of encoding and decoding the data in secure frame, from unintended recipients. Visual Cryptography is the strategy for cryptography that encodes any visual data, (for example, pictures, text, handwritten and so forth.) such that decryption is finished by utilizing human visual framework without the assistance of computer. Because of quick movement of information trade through web, data security has turned out to be more imperative in information transmission and capacity. Due to very use of images in mechanical process, it is vital to shield the private images information from unauthorized get to. Presently a days images are exchanged over internet and for larger size image it influences transmission speed. Subsequently unique image pressure and decompression systems are utilized essentially to have high data rates. The paper proposes a solution to image security as a fusion of visual cryptography and image compression technique. Discrete cosine transform with visual cryptography enhance the security level of image over internet [7].

Gopal D. Dalvi et al. [2017] in the present time, whole web is coming closer from content data to blended media data. One of the real security concerns is the insurance of this sight and sound information. Picture, which covers the most noteworthy rate of the media information, its assurance is essential. These might incorporate Military Secrets, Commercial Secrets and Information of people. This can be accomplished by visual Cryptography. It is one kind of picture encryption. In current development, most of visual cryptography is embedded a riddle using different offers [8].

Praveen K et al. [2017] in this paper, our extended XOR step development to grey scale images and the correlations with related work is appeared. We also proposed a cheating immune VCS which is applicable to grey level images [9].

Jitendra Saturwar et al. [2017] in this paper analysis of different algorithms are performed which generates meaningful shares. These shares are watermarked with cover images. After transmission of these watermarked images to accepting end, the less than desirable end will extricate the offers from watermarked images and stacking of these removed significant offers will create the original secret image. Blend of Digital watermarking and visual cryptography adds improved security to secret images [10].

Ching-Nung Yang et al. [2017] in this paper, Our (k, n)- RPVCS has k+1) secrecy-level regions and every area can be found within-(n any past locale. This new sort of district designation not just gives more zones in which to conceal the secret contrasted with the no overlapping locales in RIVCS yet in addition gives diverse presentation techniques in dynamic decoding [11].

As¸kın Okkalı et al. [2017] this study proposes a practical, cost-effective and privacy-enhancing visual cryptographic surveillance system solution to independently store multiple shares of the original camera images. A face-detection algorithm determines faces on the original real-time image, and then the determined faces are replaced with random data to protect people's identities. The rest of the images are kept, as it is to be able to follow the acts within the surveillance system. Whenever a suspected act occurs, independent entities in the system may act together to re-compose the original image and identify the suspected person. The proof of concept implementation, attack model and security analysis of the proposed model is discussed within the paper [12].

V. PROPOSED WORK

The sharing of secret image with third party has been performed in the proposed work and the third party should be trusted. For the security, the third party uses visual cryptography for generating two shares. But theses shares should be transformed into QR code before sending it to various servers and diverse image media used here for the conversion of shares into QR code. The key features of original image are

considered for the encryption of the shares to QR code performed by third party.

Shares formation using visual cryptography: The original images are converted into secret images by transforming original image into binary image.

QR code formation from shares using diverse image media: The share image is taken into consideration by encoding it and performs hiding to form QR code. If image is digital or printed then various steps should be performed such as image processing, feature extraction, pixel swapping, encoding and hiding shares by applying QR code.

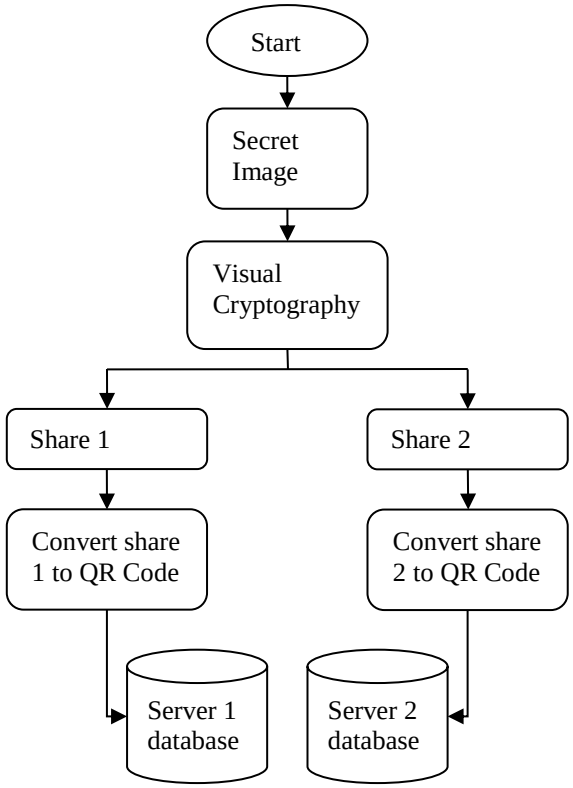

Fig 3: Architecture of Process

Steps for Encoding and Decoding:

Step:1 Initialized a random number and extraction of features performed by this number
Step:2 Features images are initialized ImgF1, ImgF2,...,ImgFn-1
Step:3 Extraction of binary feature matrix for digital image by applying feature extraction algorithm
Step:4 Feature matrix used for pixel swapping for digital image
Step:5 Apply XOR operation is applied on input image I with feature matrix in every colour plane

Steps for hiding share by using QR Code:

The communication threat of shares is secured by using QR code method and various processes are mentioned below:

Step:1 Initialized capacity ratio C and share's information amount Si
Step:2 Conversion of feature matrix into binary string BS
Step:3 BS and C used to remove the information's quantity
Step:4 The starting of string should be equivalent to null otherwise repeat from above step
Step:5 Set numeric string into null
Step:6 The final result generated

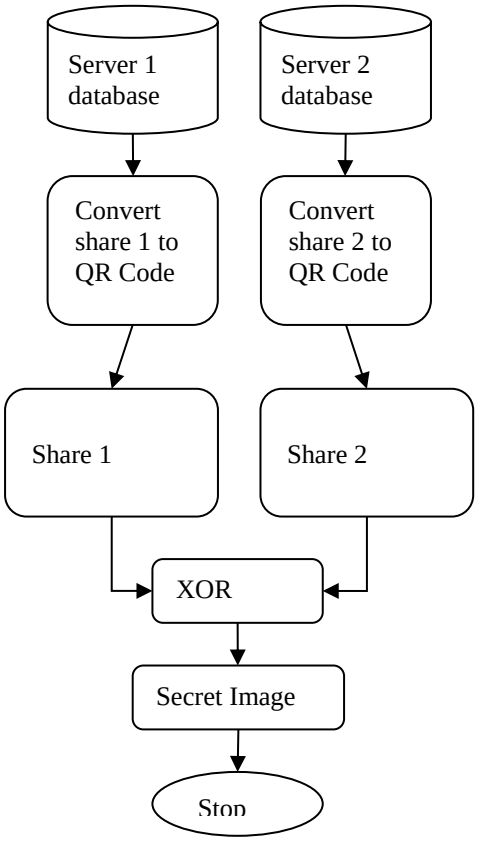

Fig 4: Authentication Procedure

VI. RESULT ANALYSIS

In this result analysis, there is a login process for the creation of shares for secret images. Image is inserted in the system by the admin and creates 2 shares of it. Visual cryptography used for the conversion of shares into QR code with diverse image media. The formation of shares is explained into various steps and appropriate understanding is explained as follows:

Step 1: Login operation performed by the Admin for providing proper authentication.

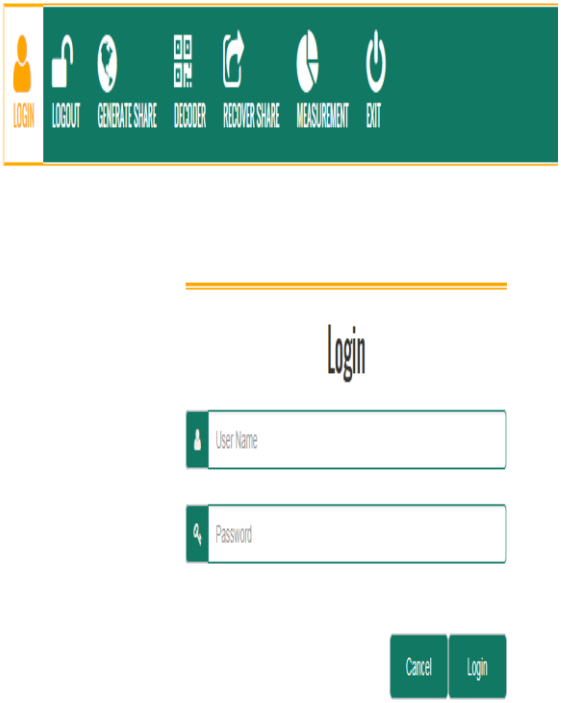

Fig 5: Admin Login

Step 2: Select secret image and form shares by the admin if it is authenticated user and successfully login.

Fig 6: Creation of shares

Step 3: Now digital image and share image are selected for the formation of QR Code.

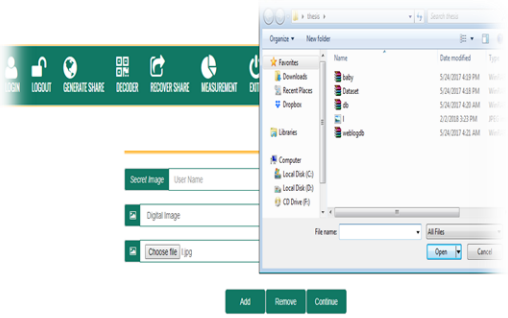

Fig 7: Select Digital images and Share Image

Step 4: Two images are selected and in this step we choose 1st image. Here the particular digital image is added and demonstrated.

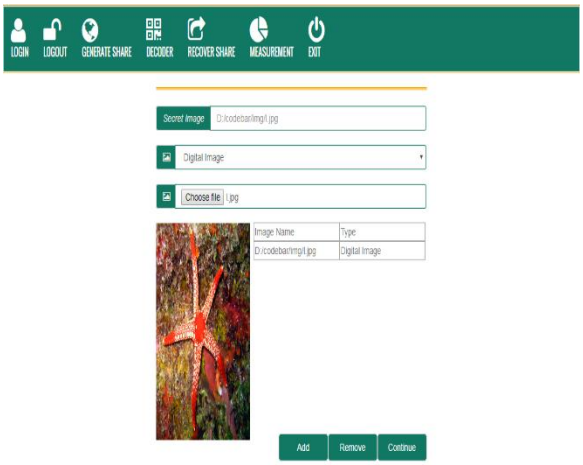

Fig 8: Display Digital Image

Here second digital image will be added and display.

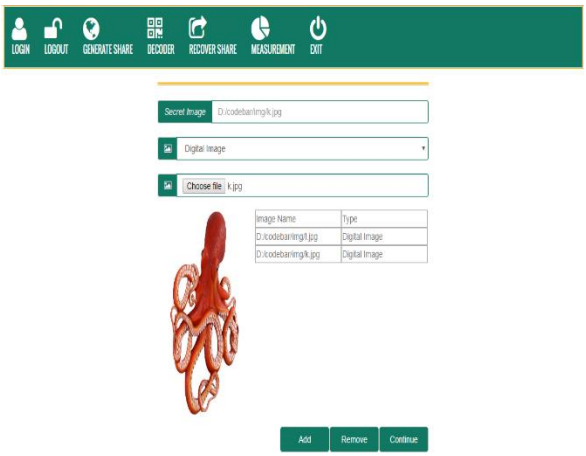

Fig 9: Display second digital image

Share to be converted to QR code is selected

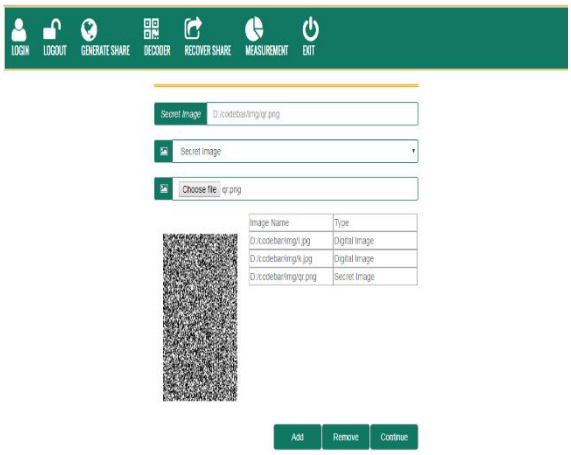

Fig 10: Select Share image

In the below figure it will display the Feature Extraction process from the natural images i.e. digital images. The below figure gives the result of encryption process

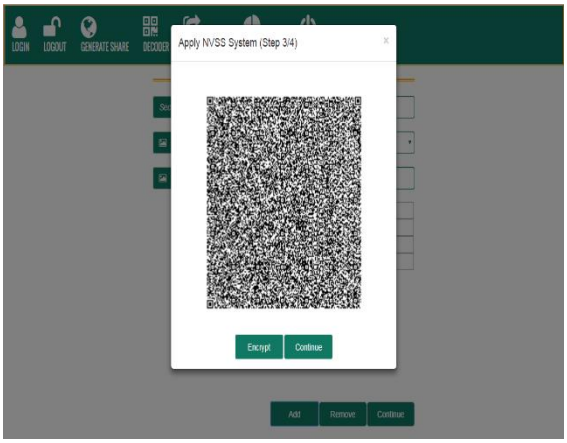

Fig 11: Share like image generated

QR code generation

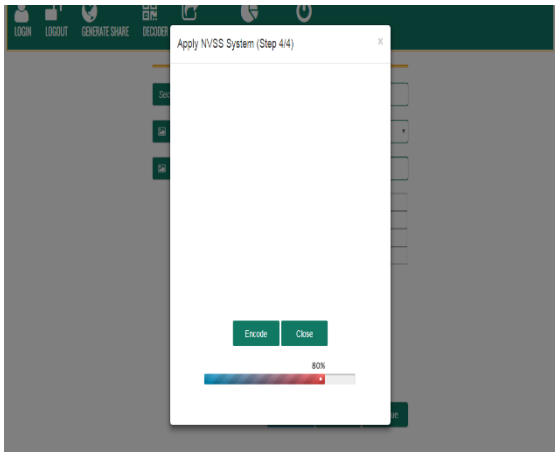

Fig 11: QR code generation

After completing the process of encoding QR code will be display in such as shown in the below snapshot. And the generated QR code will be display as shown in the below.

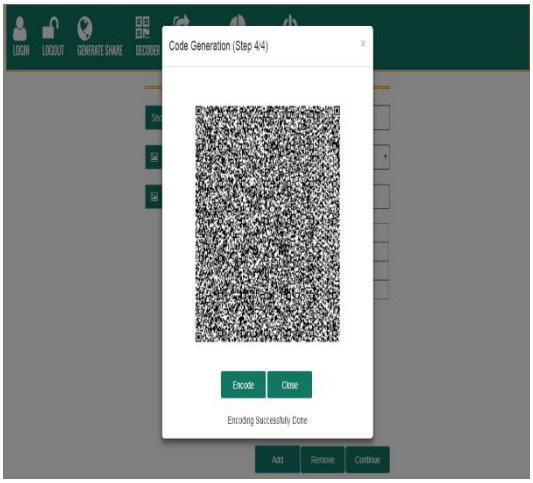

Fig 12: Generated QR code

To recover the private image from QR code, the QR code stored at different database is collected by server. Then reverse process is applied and after sending QR code to the destination database it must have to do the decoding process to get back the image share from QR code. In the below figure it display the decoded QR code to get the share.

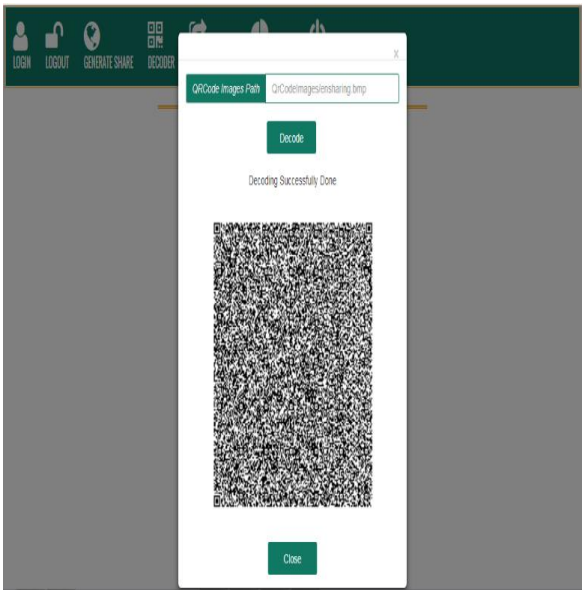

Fig 13: Decode QR Code

After getting share the process of decryption can be done to get the original secrete image. This can be done in below figure. After getting the share at side of decryption process it will require the two digital or printed images to decrypt the share. First select first digital image same as the encoding process.

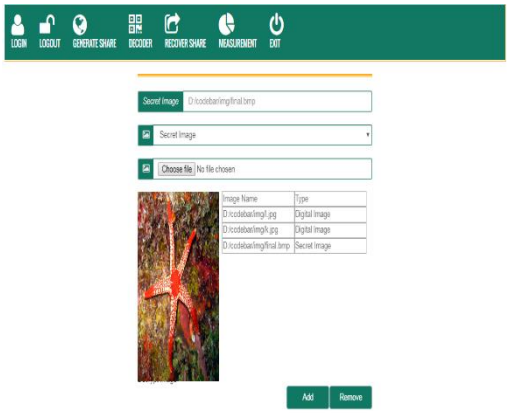

Fig 14: Select digital image for decryption

Here select the second digital image.

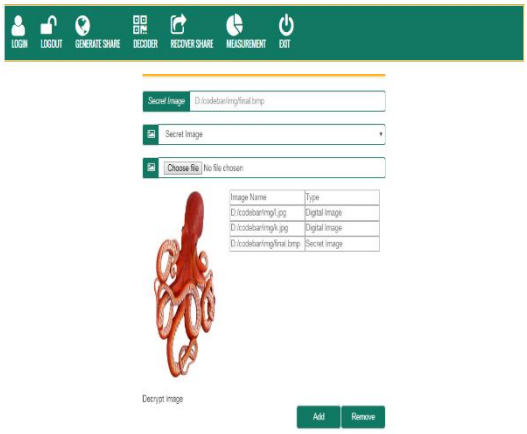

Fig 15: Select second digital image for decryption

Then select the share as the secret image and it will be ready for the decryption process. After completing the process of decryption the original secret share will be recovered from the generated share. The recovered original secret share will be as shown below.

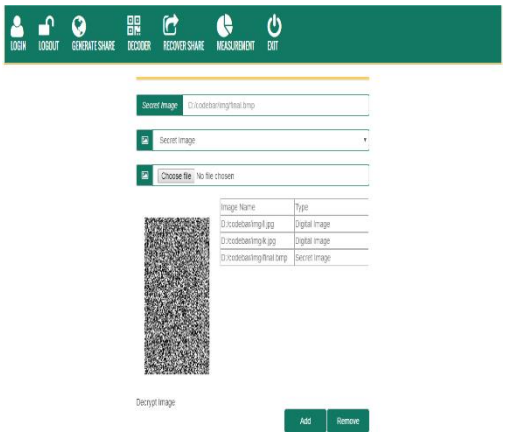

Fig 16 Recovered Share image

VII. CONCLUSION

Cryptography is the investigation of encoding and decoding the data in secure frame, from unintended recipients. VCS is a system of image encryption n novel to shroud the secret data in images. Visual cryptography system was presented as an option for conventional cryptography. It uses two or more transient images. One picture contains arbitrary pixels and the other picture contains the secret information that is hidden. It isn't conceivable to recuperate the secret data from any of the pictures. The paper proposes a solution to image security as a fusion of visual cryptography and image compression technique. Discrete cosine transform with visual cryptography enhance the security level of image over internet

REFERENCES

[1] M. Naor and A.Shamir. (1995). Visual Cryptography", Advances in cryptography EUROCRYFT94, LNCS, vol-950, pp.1-12, 1995.

[2] Mahmoud E. Hodeish,V. T. Humbe. (2014). "State-of-the-Art Visual Cryptography Schemes," International Journal of Electronics Communication and Computer Engineering, vol. 5, pp. 412-420.

[3] Walden, Disa E. A Benchmarking assessment of known visual cryptography algorithms. Diss. Rochester Institute of Technology, 2012.

[4] Lin, Chang-Chou, and Wen-Hsiang Tsai. "Secret image sharing with steganography and authentication." Journal of Systems and software 73.3 (2004): 405-414.

[5] Naor, Moni, and Adi Shamir. "Visual cryptography II: Improving the contrast via the cover base." International Workshop on Security Protocols. Springer Berlin Heidelberg, 1996.

[6] Nayan A. Ardak Prof. Avinash Wadhe "Visual Cryptography Scheme for Privacy Protection" International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 2026-2029.

[7] Yamini Ravella, Dr.Pallavi Chavan "Secret Encryption Using (2, 2) Visual Cryptography Scheme with DCT Compression" International Conference on Intelligent Computing and Control Systems ICICCS 2017.

[8] Gopal D. Dalvi, Dr.D.G.Wakde "Facial Images Authentication In Visual Cryptography Using Sterilization Algorithm" 2017 2nd International Conference for Convergence in Technology (I2CT).

[9] Praveen K and Sethumadhavan M "On the extension of XOR step construction for optimal contrast grey level visual cryptography" 978-1-5090-6367-3/17/$31.00 ©2017 IEEE.

[10] Jitendra Saturwar D.N. Chaudhari "Secure Visual Secret Sharing Scheme for Color Images Using Visual Cryptography and Digital Watermarking" 978-1-5090-3239-6/17/$31.00©2017 IEEE.

[11] Ching-Nung Yang, Chih-Cheng Wu, and Yi-Chin Lin "k out of n Region-Based Progressive Visual Cryptography" 1051-8215 (c) 2017 IEEE.

[12] As¸kın Okkalı Mehmet Tahir Sandıkkaya "Preserving Privacy Using Visual Cryptography in Surveillance Systems" 978-1-5386-0930-9/17/$31.00 c 2017 IEEE.