

# Secure Transactions in E-Banking using Visual Cryptography

**Subodh Kumar**, M.Tech Scholar, Department of Computer Science & Engineering, Kanpur Institute of Technology, Kanpur, India.  
**Akhilesh Pandey**, Assistant Professor, Department of Computer Science & Engineering, Kanpur Institute of Technology, Kanpur, India

**Abstract**—For protecting the digital information, researchers have proposed various security techniques. Security techniques can be made more powerful by storing the sensitive data in a distributed way. Traditional security techniques take more computational time in comparison to visual cryptography techniques. Visual Cryptography is perceived and studied as a perfect combination of secret sharing and digital image processing.

The use of computers and internet has become so pervasive so it influences all the banking sectors. Security has become the most important aspect in today's banking transaction system because banks are committed to provide secure core banking services to their customers. To achieve this goal authenticity of the users is required i.e. only the authorized users can take part in the transaction. Regarding this purpose banks uses Biometrics based authentication systems but due to avoidable malicious activities database of the banking system is no longer secure. Smart hackers can fetch biometric details of customers from the bank's database and later can use it for fake transactions. To avoid all this catastrophic things Visual cryptographic technique is used. Visual Cryptography is an efficient encryption scheme in which information hide inside the images and decrypted only by human visual system. The prime objective of this thesis work proposes a secure XOR operation based visual cryptography and image processing technique to secure banking transaction. In our proposed method using Steganography, our system becomes more secure and efficient.

**Index Terms**—Visual Cryptography, Steganography, Image Processing, Secret Sharing Scheme, Banking System

## I. INTRODUCTION

The Digitalization has the greatest potential to alter the way we live. In today's era of the digitalized world, security is an important concern. Security problems start to become apparent when information is being delivered from node to node over the network. The number of threats has been increasing at a wider rate, therefore, strong security techniques need to be deployed. Cryptography [4-8] is one of the prime techniques for providing information security. In traditional cryptographic methods, enormous computational power and complicated algorithms are common, taking much time and money to encode and decode a secret message. Generally, in banking sector Biometrics based authentication is used. Biometrics based authentication system operates by obtaining raw biometric data (e.g., Face image, Fingerprints etc.) from the subject, extracting feature set from the raw data and comparing the feature set against the blueprint stored in the database in order to authenticate the subject or to verify claimed identity. Security of any institute/organization depends on underlying design technology middle-ware and most of on the design of the database. Every transaction spatial or temporal has impact on the database. Therefore hackers always try to hack the database. The banking system while offering web enable core services major issue is authentication of the user. Many techniques are used for this purpose i.e. Password based authentication, Smart card based authentication, Biometric based authentication system. All these techniques are required to maintain database hence vulnerable for hacking. Database contains private information therefore there is possibility of privacy loss.

Visual Cryptography [1-3] is a secret sharing scheme that takes secret image as input(i.e. Printed, Handwritten) encrypts the input image into a set of other images called shares in such a way, if shares are printed on transparencies and superimposed or staked over one another original secret is revealed. Simplest form of visual cryptography or visual secret sharing scheme considers binary image as input and deals with each and every pixel independently.[10]

To encode a pixel of the secret image, we split the secret pixel into  $n$  versions in such a way that if all  $n$  versions are printed on transparencies and superimposed the original secret pixel is revealed. This process has to be applied for entire secret image. Consequently  $n$  shares of original secret image are ready, to reveal the secret print the shares on transparencies and superimpose them. A method uses XOR operation based Visual Cryptography and image processing techniques to ensure authentication as well as security of the information stored in the bank database. In our proposed method using Steganography, our system becomes more secure and efficient. [15]

## II. LITERATURE REVIEW

Various literature related to progressive collapse of the building structures are studied and brief review is presented below. This section presents a brief summary of the Visual Cryptography and its uses in Banking System. For safeguarding the cryptographic systems keys G. Blakely [11] and A. Shamir [12] in 1979 independently developed  $(t, n)$ - secret sharing scheme, it mean that if at least  $t$  out of  $n$  shares are combined in a particular manner the secret can be revealed. If less than  $t$  shares are available, then secret cannot be revealed. G. Blakely secret sharing scheme is based on vector space and A. Shamir secret sharing scheme is based on polynomial interpolation.

Visual Cryptography is secure technique for detecting fake websites and phishing attacks caused by it. It is method of sending and receiving the messages that can be decrypted only by sender and receiver. Naor and Shamir [1] introduced this technique as simple and secure way of sharing secret image as password.

There are two parts in this technique viz. Encryption decryption and image share generation. The encryption and decryption of message is done by simple mathematical algorithm. The second important part in this scheme is share generation of the image. VCS is a cryptographic technique that encrypts of visual information such that decryption can be performed using the human only.

Naor and Shamir [1] formally defined and put forward the visual cryptography scheme for secret sharing. Since then research on the VC has flourished to become a subject to various research directions. There are many types of VC and each of these schemes has its own emphasis on application in practice. The operation of dividing a VC secret image into shares has been focused on the areas of being applied to different types of the secret such as gray scale and color images. In this chapter initially, basic knowledge of secret sharing and VC has been introduced to address the previous achievements. Several contributions to the literature have been discussed according to different variants of VC scheme suggested in the literature.

The OR-based VCS suffers from the low quality of the reconstructed image. It cannot be improved beyond a certain level in most of the scheme. Tuyls et al.[13] suggested a VCS scheme based on the polarization of light where the Boolean XOR is used as underlying mathematical operation.

It is done by inserting a liquid crystal layer into a liquid crystal display (LCD). In comparison with OR-based schemes where a participant has to carry a number of transcripts to update the shares, in an XOR-based VCS a person has to carry just a device that has a display.

For recovering the secret image the liquid crystal layers have to be stacked together. Moreover, due to the rapid advancement of technology, these devices are getting cheaper. In the suggested scheme for XOR [13] the authors constructed a XOR based (n,n) -VCS and proved that a XOR based VCS is equivalent to a binary code.

In general, XOR- based VCS are non-monotone i.e., if a qualified set of parties can recover the secret image it does not necessarily hold that every superset is able to recover the secret image. The main difference between these two models of visual cryptography lies in the fact that the OR model captures strong access structures but in the XOR model due to the randomness of the XOR operation, it is not possible to satisfy monotone properties However, and we can solve this problem with a slight modification in the definition of XOR scheme.

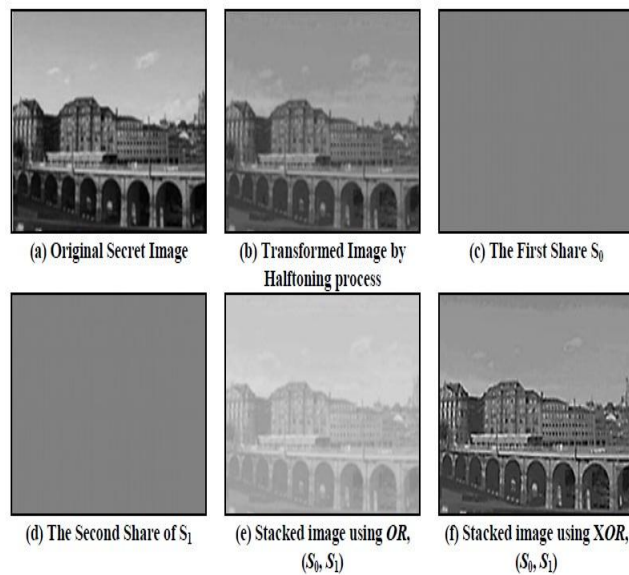


Figure 1: Process of XORing operation on VCS









Pixel	Shares	Basis Matrix	
White	  S1      S2	$M_0 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$	←Row1
	  S1      S2	$M_0 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$	←Row2
Black	  S1      S2	$M_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$	←Row3
	  S1      S2	$M_1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$	←Row4

Figure 2: (2, 2)-VCS Scheme

The security conditions for both the models are same, but the difference lies in the contrast condition. Naor and Shamir's [1] original suggestion has been extended in the 2-out-of-2 secret sharing scheme by using a half toning technique. It also extends basic visual cryptography a step further by supporting other variants of images.

### III. VISUAL CRYPTOGRAPHY

Cryptography has a long and fascinating history within the security domain. Handling of sensitive images carrying confidential information is of prime concern in several departments such as sharing the maps over the internet in the military and in many others commercial sectors. To handle the security problems of sensitive images, various image secret sharing schemes have been evolved. One of the techniques named as Visual cryptography (VC) has been developed by Naor and Shamir [1] in the year 1995 to handle secret sharing for images.

VC is an approach in which a secret image containing confidential visible information is encrypted in a perfectly secure way such that the decryption can be performed directly by the human visual system (HVS), without the assistance of computers. VC allows encrypting any visual information such as printed text, handwritten notes, and pictures. It eliminates complex computation during decryption process, and the images can be restored by doing stacking operation on its shares. It combines the feature of perfect ciphers creation and secret sharing in cryptography. Secret image is usually divided into two or more pieces known as shares. When the required number of shares, print on transparencies and then superimposed, the secret images get recovered.

Naor et al. [1] introduced the technique of VC in which the binary image is decomposed into  $n$  number of shares. Figure 1.1 shows an example of share creation and recovery of a secret image using visual cryptography. In the scheme of  $(k, n)$ , shares when stacked over one another reveals the original secret image. Naor scheme is quite suitable for a binary image. The shares created in the original image are determined by randomly selecting pairs of sub-pixel matrices for black and white pixels [2]. VC scheme suggested by Naor et al. [1] requires no computer participation in any situation for decryption. Visual cryptography combines the notion of the perfect secret with a random image for the purpose of secret sharing [3]. The next section describes the common characteristics of VC schemes.

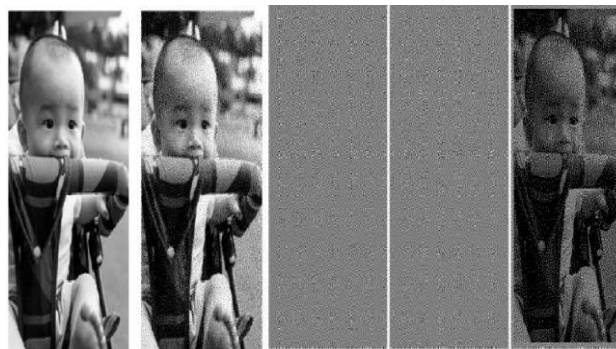


Figure 3: Original image, Halftone, Share-1, Share-2 and Decrypted image

### IV. STEGANOGRAPHY

Steganography aims at hiding digital information into covert channels so that one can conceal the information and prevent the detection of the hidden message [15]. Steganalysis is the art of discovering the existence of hidden information whereas steganalytic systems are used to detect whether an image containing a hidden message. By analyzing various image features between stego-images (image contain hidden messages) and cover images (images containing no hidden messages), a steganalytic system is able to detect stego-images.

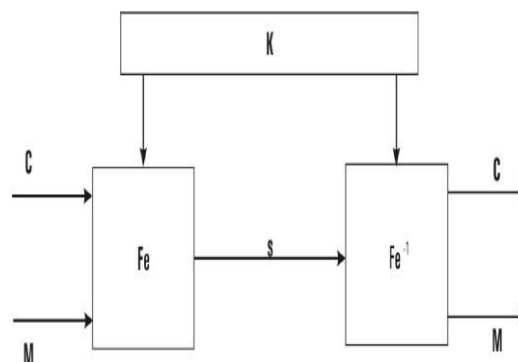


Figure 4: A Steganographic model

The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message. Technically, in simple words “steganography means hiding one piece of data within another”.

Modern steganography uses the opportunity of hiding information into digital multimedia files and also at the network packet level. Hiding information into a media requires the following elements [15].

The cover media ( $C$ ) that will hold the hidden data

- The secret message ( $M$ ) may be plain text, cipher text or any type of data
- The stego function ( $Fe$ ) and its inverse ( $Fe^{-1}$ )
- A stego-key ( $K$ ) or password used to hide and unhide the message.

The stego-function operates over cover media and the message (to be hidden) along with a stego-key to produce a stego media ( $S$ ). The scheme of steganography operation is shown Figure 4.

Steganography and cryptography are used in data hiding. Cryptography is the science of protecting data by scrambling so that nobody can read it without given methods or keys; it allows an individual to encrypt data so that the recipient is the only person able to decipher it. Steganography is the science of obscuring the message into a host object (carrier) with the intent of not drawing suspicion to the context in which the message was transferred. Steganography and cryptography are efficient partners in spite of functional differences. It is common practice to use cryptography with steganography.

## V. METHODOLOGY

Banking system provides the facility of having joint account and operates jointly or individually. In case of individual operation it does not mean to have joint account but it provides flexibility to the members of joint account to operate individually. In some cases socially it is not secure[17].

Suppose A and B have joint account and at later time A gets adverse to B and wish to withdraw all the money from the account. In this case B is cheated by A. In the proposed method it is ensure that transaction is only possible when both the users are available. It also ensure that nobody can misuse the information stored in the database because Shares are random noise like images and nobody can get any clue from a single share even he apply enormous amount of computing power and time. In the proposed method gray images of both the user are taken as input and processed for further use.

Overall process is divided into two phases: Encryption phase and Decryption phase.

### A. Encryption Phase

Encryption phase is further divided into Preprocessing, Image Fusion, and Hide text in Image (Steganography), Secret Image and Share Generation. It is shown in Figure 5.

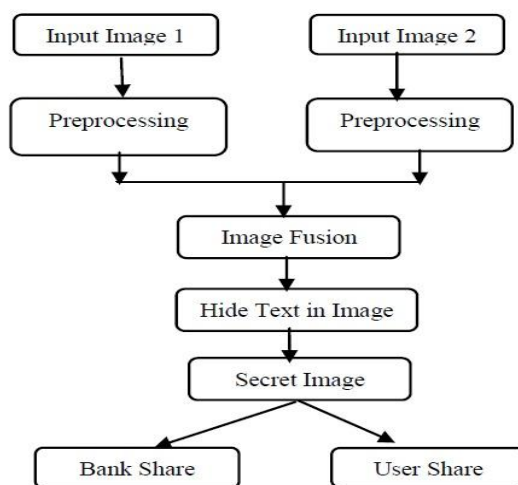


Figure 5: Encryption phase

#### Preprocessing

At the time of registration for joint account user A and user B have to present the face image to the bank. Respective authority preprocesses and generates joint identity of the users A and B. This joint identity of the users A and B is called secret image.

#### Image Fusion

Image fusion refers to the process of combining two or more images into one composite image, which integrates the information contained within the individual images [39]. The result is an image that has a higher information content compared to any of the input images. The goal of the fusion process is to evaluate the information at each pixel location in the input images and retain the information from that image which best represents the true scene content or enhances the utility of the fused image for a particular application. Image fusion is a vast discipline in itself, and refers to the fusion of various types of imagery that provide complementary information. Image fusion combines two or more registered images of the same object into a single image that is more easily interpreted than any of the originals.

#### Hide text in Image (Steganography)

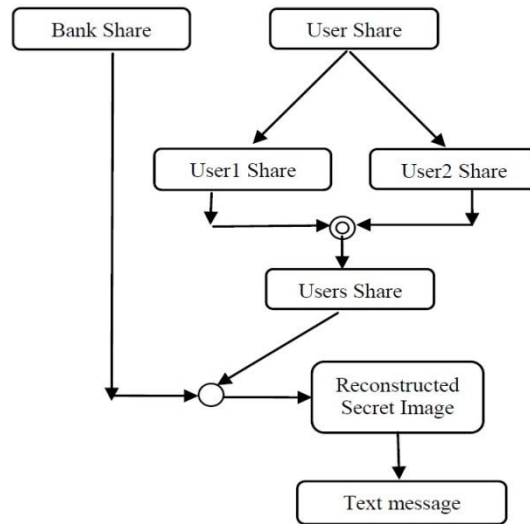
Image files can hide text without their size being affected too much. It's called steganography, and it allows you to hide text in images without anyone from knowing.

#### Share Generation

Secret image is fed as input to the share generation process. Two share are generated for the secret image using (2,2)-VCSXOR. One share is called as Bank which is kept in bank database, and other is called Users share and further divided using the same scheme into two share share1 and share 2, share1 is given to user A and share2 to the user B [18].

**B. Decryption Phase**

When users have to perform the transaction they have to provide their shares to the bank. Bank performs the XOR operation between the user's shares and generates the Users share. To reconstruct the secret image XOR operation is performed between Users share and Banks share. This process reconstructed the secret image, which is as same as secret image because of associative nature of XOR operation. It is shown in Figure 6.



**Figure 6:**Decryption Phase

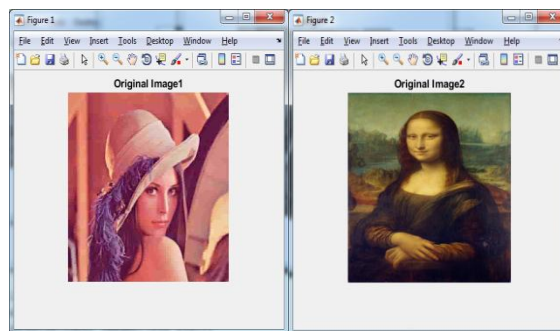
In decryption phase convert to reconstructed secret image to original text.

**VI. RESULTS AND ANALYSIS**

Various activities viz. preprocessing, conversion of images from gray image to black and white, creation of shares, reconstruction of the secret is also performed using the functions defined in the image processing tool box. Initially users image are considered gray and resize to make the size of both the user images same.

The proposed has been implemented with steganography and results have been verified with images.

**1. Original Images**



**Figure 7:**Original Images

**2. Original gray scale images**

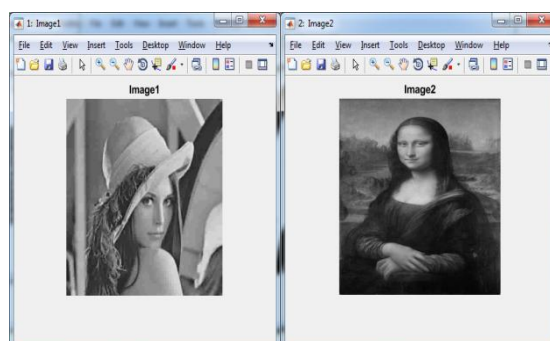


Figure 8:Original gray scale images

3. Preprocessed Images

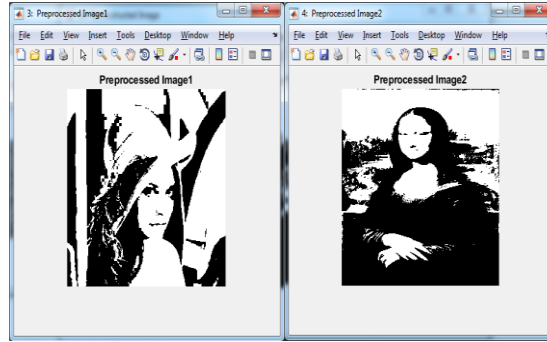


Figure 9:Preprocessed Images

4. Concatenated Image

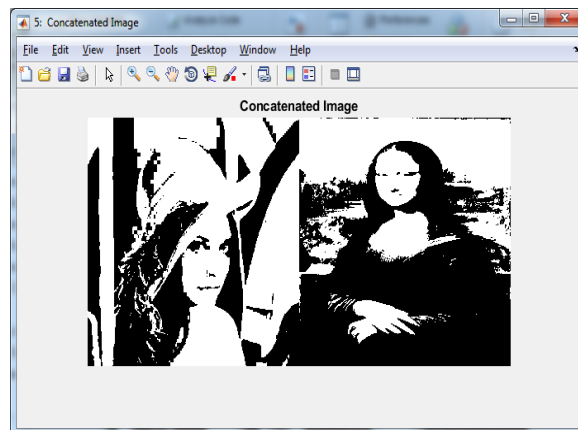


Figure 10:Concatenated Images

5. Secret Image:it contains a hidden text message in image as ( email id is xyz123@gmail.com and password is 12345 )

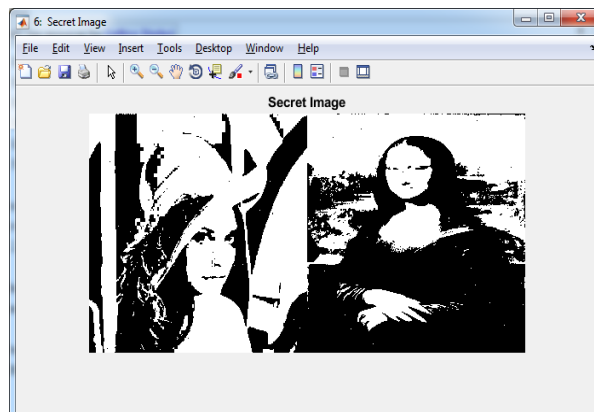
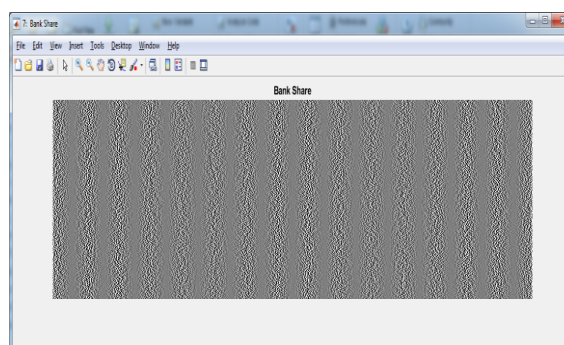


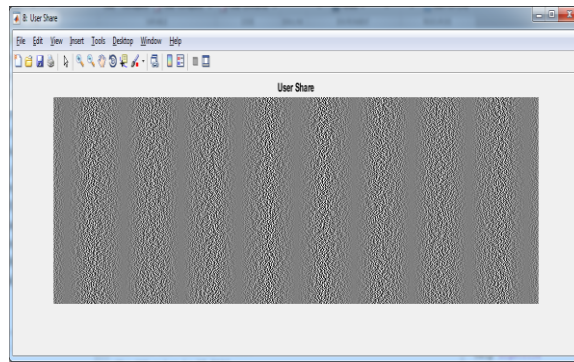
Figure 11:Secret Images

6. Bank Share



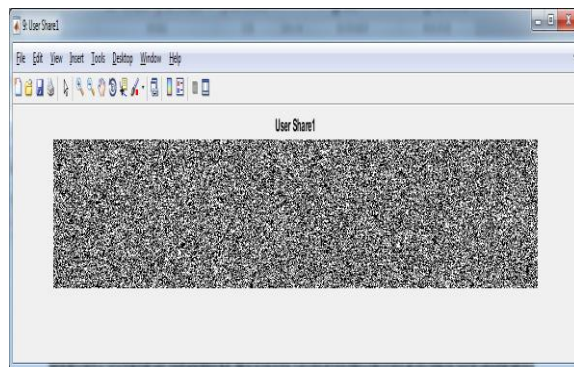
**Figure 12:Bank Share Image**

### 7. User Share

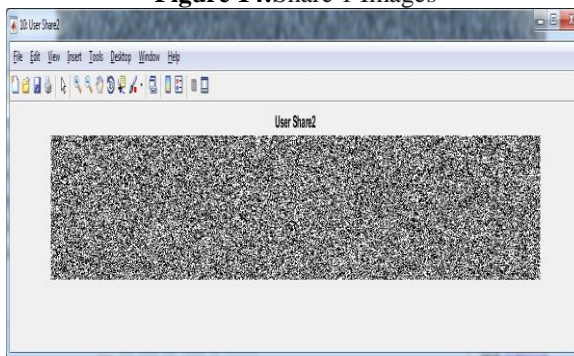


**Figure 13:User Share Image**

The User Share is again divided into User Share1 and User Share2.



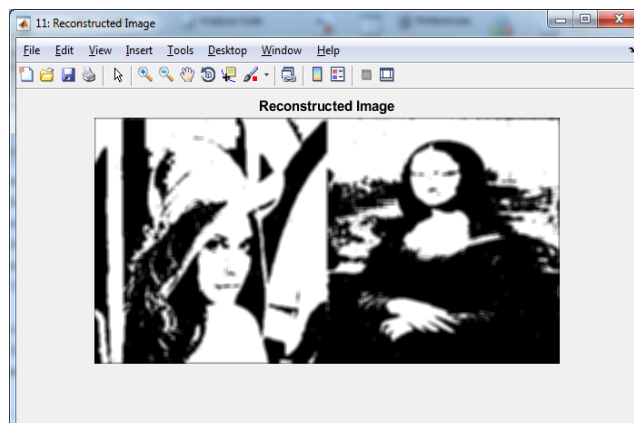
**Figure 14:Share 1 Images**



**Figure 15:Share 2Images**

### 8. Reconstructed Image

Finally we get reconstructed image and the text message



**Figure 16:Reconstructed Image**

The text message is completely decoded and displayed as below, (email id is xyz123@gmail.com and password is 12345) It can be seen that the inserted text message and decoded text message are same. It will allow user to login and start banking online.

Figure 7 and Figure 8 are original images and gray images taken as input while Figure 9 is preprocessed binary images obtained from gray images Figure 8 respectively. Figure 10 showed as concatenated image and Secret image as shown in Figure 11 is obtained from the Figure 9. After that Secret image Figure 13 is divided into user shares Figure 14 and 15. Figure 12 is a bank share image. Reconstructed secret image as shown in Figure 16 is obtained by using the shares Figure 11, Figure 12 and Figure 13.

## VII. CONCLUSION

In this method original image is secured by decomposing it into n shares. This work mainly focuses on issues related to the identity theft and customers data security in the joint account transaction. For secure Banking Transaction in joint account operation this work proposed a method that is based on (2, 2)-VCS-XOR with Hide text in Image (Steganography). Experimental results show that reconstructed secret image is same in size and quality of the original secret image.

## References

- [1] M. Naor and A. Shamir, —Visual Cryptography,| Advances in Cryptology ,EUROCRYPT-94, LNCS-950, pp. 1–12, Springer, Berlin, Heidelberg, 1994.
- [2] B. W. Leung, F. Y. Ng, D. S. Wong, —On the security of a visual cryptography scheme for color images,| Pattern Recognition Journal, Elsevier, Vol. 42, no. 5, pp. 929-940, May, 2009.
- [3] S. K. Das and B. C. Dhara, —An image secret sharing technique with block based image coding,| , 2015 Fifth International Conference on Communication Systems and Network Technologies, pp. 648-652, April, 2015.
- [4] C.Y. Wang, N.S. Shiao, H.H. Chen, and C.S. Tsai, —Enhance the visual quality of shares and recovered secret on meaningful shares visual secret sharing,| in Proceedings of the 4th International Conference on Uniquitous Information Management and Communication - ICUIMC '10, 2010.
- [5] F. Liu and W. Yan, Visual Cryptography for Image Processing and Security : Theory, Methods, and Applications, 2nd edition, Springer, 2015.
- [6] M. Naor and B. Pinkas, —Visual authentication and identification,| Advances in Crypto, Crypto-97, LNCS-1294, pp. 322–336, Springer, Berlin, Heidelberg, 1997.
- [7] D. Chaum, —Secret-ballot receipts: true voter-verifiable elections,| IEEE Security & Privacy Magazine, vol. 2, no. 1, pp. 38–47, Jan. 2004.
- [8] H. Luo, J.-S. Pan, Z.-M. Lu, and B.-Y. Liao, —Watermarking-Based Transparency Authentication in Visual Cryptography,| in Seventh International Conference on Intelligent Systems Design and Applications (ISDA 2007), pp. 609–616, 2007.
- [9] R.J. Hwang, —A Digital Image Copyright Protection Scheme Based on Visual Cryptography,| Tamkang Journal of Science and Engineering, vol. 3, no. 2, pp. 97–106, Sep. 2000.
- [10] F. Liu and W. Q. Yan, —Various Problems in Visual Cryptography,| in Visual Cryptography for Image Processing and Security, pp. 23–61, Springer International Publishing, 2014.
- [11] G.R. Blakley, “Safeguarding cryptographic keys,” Proc. of the National Computer Conference 1979, vol. 48, pp: 313–317, 1979.
- [12] M. Naor and A. Shamir, “Visual cryptography, in Workshop on the Theory and Application of Cryptographic Techniques, pp: 1–12, Springer, 1994.
- [13] S. Roy, P.Venkateswaran, “Online Payment System using Steganography and Visual Cryptography,” Proceedings of IEEE Students’ Conference on Electrical, Electronics and Computer Science, 2014.
- [14] V. Suruthikeerthana1 , Dr. S.Uma , “An Extended Visual Cryptography With Dynamically Authenticated Error Avoidance Scheme For Bank Applications”, International Journal Of Research In Computer Applications And Robotics, vol 4, no. 4, pp: 15-23, 2016.
- [15] R.Anderson and F. Petitcolas, “On the limits of steganography” IEEE Journal of Selected Areas in Communications, Vol. 16, No. 4, May 1998.
- [16] NielsProvos, Peter Honeyman, ”Hide and Seek: An Introduction to Steganography,” IEEE computer society,2003.
- [17] Akhilesh Pandey, Amitash ” Digital watermarking for image using 3-level DWT and PSO algorithms” International Journal of Advanced Research and Technology” Volume (7) Issue (2) June 2019.
- [18] Akhilesh Pandey, Nisha Pal, Dr Dinesh Goyal ” A Survey on MRI Brain Image Segmentation Technique” International Journal of Advance Engineering, Management and Science” Volume (2) Issue (12) December 2016.