

Visual Cryptography Based Safe Transactions in E-Banking System

Rajat Mishra, M.Tech Scholar, Department of Computer Science & Engineering, Bhabha Institute of Technology, Kanpur, India.
Anamika Tiwari, Assistant Professor, Department of Computer Science & Engineering, Bhabha Institute of Technology, Kanpur, India

Abstract—Researchers have suggested various security strategies for protecting the digital information. Security strategies can be made more efficient by centralized storage of the sensitive data. Compared with the visual cryptography techniques, conventional security techniques require more computational time. Visual cryptography is viewed as a natural combination of secret communication and digital image processing and is studied.

Computer and internet use has become so omnipresent that it impacts all banking sectors. Security has become the most important feature of today's banking transaction system as banks are dedicated to providing their clients with safe core banking services. It is important to achieve this target authentication of the users, i.e. only the approved users can participate in the transaction. Biometrics-based authentication systems are used for this purpose, but the banking system database is no longer safe due to inevitable malicious activities. Smart hackers will capture biometric customer information from the database of the bank and then use it for fake transactions later. Visual cryptographic technique is employed to prevent all these disastrous issues. Visual Cryptography is an effective encryption scheme in which information hides inside images and is only decrypted by the visual system of humans. The prime objective of this thesis work proposes a visual cryptography and image processing technique focused on secure XOR operation to secure banking transaction. Our proposed approach, using steganography, makes our system safer and more effective.

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

I. INTRODUCTION

Digitalisation has the biggest ability to transform our way of life. Security is a major concern in today's digitalised world era. As information is transmitted from node to node over the network, security concerns begin to become apparent. There has been an rise in the number of threats at a broader pace and effective protection measures need to be used. Cryptography[4-8] is one of the prime methods for providing protection of information. Huge computational power and complicated algorithms are popular in traditional cryptographic methods which take a lot of time and money to encrypt and decode a secret message. In general, Biometrics based authentication is used in the banking sector. Biometrics-based authentication system operates by collecting raw biometric data (e.g. face picture, fingerprints etc.) from the subject matter, extracting the feature set from the raw data and comparing the feature set against the blueprint stored in the database to authenticate the subject matter or check the stated identity; Any institution / organization's security depends on the underlying middle-ware architecture technology, and much of it on the database design. Could spatial or temporal activity has impact on the database. But hackers are still trying to crack the database. The banking mechanism that allows core services when providing the web is the user's authentication. For this end other methods are used i.e. Authentication based on passwords, authentication based on smart cards, authentication based on biometrics. To keep the database vulnerable for hacking, all these techniques are needed. Database includes private information and loss of privacy is possible.

Visual Cryptography [1-3] is a secret sharing scheme that takes a secret image as input (i.e. typed, handwritten) encrypts the input image into a collection of other images called shares in such a way that shares are typed on transparencies and superimposed or staked on each other. Simplest visual cryptography or visual secret sharing scheme considers binary image as data, and deals separately with each and every pixel[10].

To encrypt a pixel of the secret image, we divide the secret pixel into n versions in such a way that the original secret pixel is exposed when all n versions are printed on transparencies and superimposed. For the entire hidden picture this procedure must be implemented. Then n shares of original secret picture are able to show and superimpose the secret printing of the shares on transparencies. A system uses Visual Cryptography and image processing techniques based on XOR operations to ensure both authentication and security of the information stored in the bank database. Our device becomes more secure and efficient in our proposed method of using Steganography. [15]

II. LITERATURE REVIEW

Different literature relating to the progressive collapse of the building structures is reviewed and a brief review is given below. This section provides a brief overview of Visual Cryptography in the Banking System and its uses. To secure cryptographic device keys G. Blakely and A. Shamir[12] established independently (t, n) - a secret sharing scheme in 1979, it means that the secret can be exposed if at least t out of n shares are combined in a specific way. If there are less than t shares available, then the secret can not be revealed. G. Blakely's scheme of hidden sharing is based on vector space and a. Shamir's scheme of hidden sharing is based upon polynomial interpolation.

Visual Cryptography is a reliable technique used to detect fake websites and phishing attacks triggered by them. It is method of sending and receiving messages which can only be decrypted by sender and receiver. This technique was introduced by Naor and Shamir[1] as a easy and safe way of sharing secret image as password.

This technique has two sections to it, viz. Decryption access, and generation of image sharing. Email encryption and decryption is achieved through a simple mathematical algorithm. The second significant aspect of this scheme is image creation sharing. VCS is a cryptographic technique that encrypts visual information in such a way that decryption can be carried out only through the person.

The visual cryptography scheme for secret sharing was formally described by Naor and Shamir[1] and put forward. Work on the VC has since flourished to become a focus for different directions of study. There are several types of VC and each of these schemes places its own focus on practical implementation. The process of splitting a secret VC image into shares concentrated on the areas to be applied to different secret forms such as gray scale and color images. Specific knowledge of secret communication and VC was initially presented in this chapter to discuss the previous achievements. Many contributions to the literature were discussed as indicated in the literature according to different variants of the VC scheme.

The OR-based VCS suffers from the image reconstructed being of poor quality. For most of the scheme it can't be changed above a certain point. Tuyls et al.[13] proposed a VCS scheme based on light polarization, where the Boolean XOR is used as the mathematical underlying operation.

It is achieved by adding a layer of liquid crystals into a set of liquid crystals (LCD). Compared to OR-based schemes where a individual has to carry a number of transcripts to update the shares, a person has to carry only a computer that has a display in an XOR-based VCS.

The liquid crystal layers have to be stacked together for the recovery of the secret image. In fact, these machines are becoming cheaper because of the rapid development in technology. The authors constructed an XOR-based (n, n) -VCS in the suggested scheme for XOR[13] and proved that an XOR-based VCS is equivalent to a binary code.

Generally speaking, XOR-based VCS is non-monotonous, i.e. if a qualified collection of parties can recover the secret image, it does not automatically hold that each superset can recover the secret picture. The key difference between these two models of visual cryptography is that the OR model captures strong access structures but it is not possible to satisfy monotonous properties in the XOR model due to the randomness of the XOR operation, however, and we can solve this problem with a minor change in the XOR scheme definition.

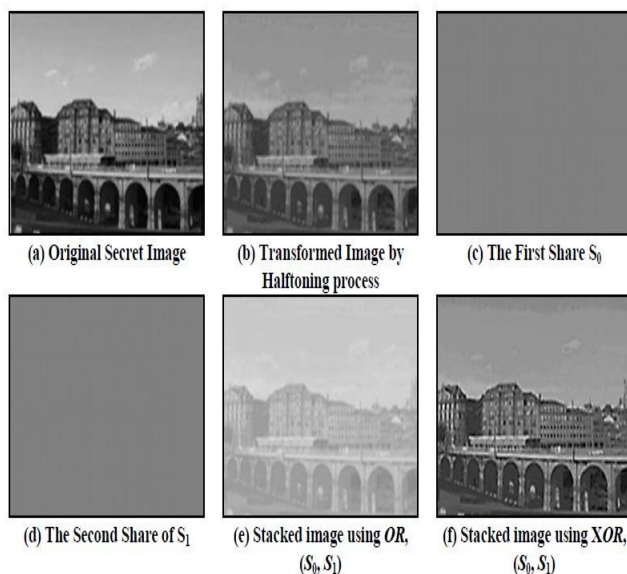


Figure 1: Process of XORing operation on VCS









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

Figure 2: (2, 2)-VCS Scheme

The security conditions are the same for both versions but the distinction lies in the state of contrast. In the 2-out-of-2 hidden sharing scheme, the original suggestion of Naor and Shamir[1] has been expanded by the use of a half toning technique. This also expands the basic visual cryptography by supporting other image variants a step further.

III. VISUAL CRYPTOGRAPHY

Within the security domain cryptography has a long and interesting history. The management of classified photos that contain proprietary information is of primary concern in many agencies, such as the exchange of maps in the military and several other commercial sectors over the internet. Numerous hidden image sharing systems have been developed to manage the security issues of sensitive pictures. Naor and Shamir[1] created one of the techniques called Visual Cryptography (VC) in 1995 to manage hidden image sharing.

VC is an method in which a hidden image containing sensitive visible information is encrypted in a completely safe fashion, so that the decryption can be carried out directly by the human visual system (HVS) without computer assistance. VC enables some visual information to be encrypted, such as printed text, handwritten notes, and photographs. During the decryption process it removes complex computation, and the images can be restored by stacking operation on its shares. This incorporates the trait of making flawless ciphers and exchanging secrets in cryptography. In general, the hidden picture is divided into two or more parts known as shares. The hidden images are retrieved when the appropriate number of shares is printed on transparencies and then superimposed.

Naor et al.[1] implemented the VC technique where the binary image is broken down into n number of shares. Figure 1.1 provides an example of using visual cryptography to build and retrieve a hidden image by sharing. The initial hidden picture is shown in the (k, n) scheme, when stacked over one another. Naor scheme suits perfectly with a binary image. The shares generated in the original image are calculated by selecting sub-pixel matrix pairs randomly for black and white pixels[2].

The VC scheme suggested by Naor et al.[1] does not require any code involvement for decryption in any case. For the purposes of secret exchange, visual cryptography blends the notion of the ideal secret with a random image[3]. The next section explains the features common to VC schemes.

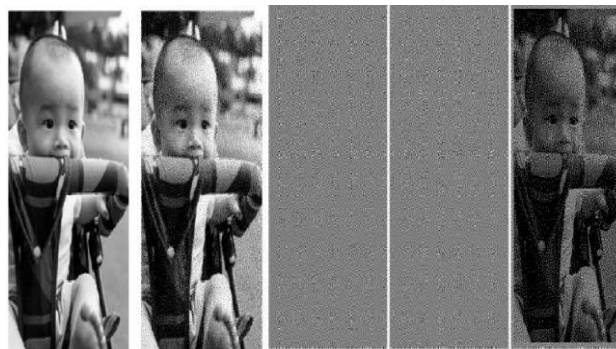


Figure 3: Original image, Halftone, Share-1, Share-2 and Decrypted image

IV. STEGANOGRAPHY

Steganography seeks to encrypt coded information in secret networks so that the information can be dissimulated and the concealed message can not be detected[15]. Steganalysis is the art of discovering the presence of secret content, whereas steganalytic systems are used to detect what a hidden message image contains. By analyzing different image characteristics between stego-images (image contains hidden messages) and cover images (images without hidden messages), a steganalytic device can detect stego-images.

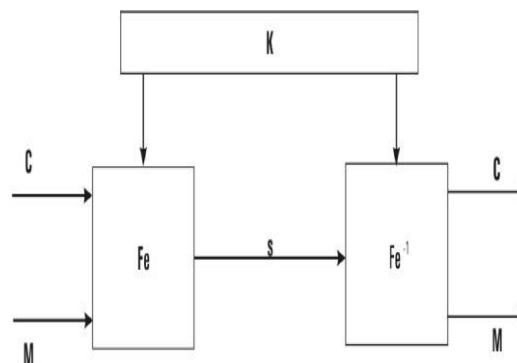


Figure 4: A Steganographic model

Steganography 's purpose is to conceal a secret message inside a cover-media in such a way that others are unable to detect the existence of the hidden message. Technically, "steganography means hiding in another piece of data." Modern steganography makes use of the ability to conceal information in digital multimedia files and at network packet level as well. The following elements are needed when hiding information in a media [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 works over the cover media and the message (to be hidden) along with a stego-key to create a stego media (S). The steganography process scheme is shown in Figure 4. Steganography and cryptography is used in hiding data. Cryptography is the science of data protection through encoding so that no one can decode it without specific methods or keys; it allows an individual to encrypt data so that only the receiver can interpret it. Steganography is the practice of obscuring the message into a host entity (carrier) in order not to attract attention to the context in which the message was being transmitted. Despite functional differences steganography and cryptography are productive partners. Steganography use of cryptography is standard practice.

V. METHODOLOGY

The banking system includes the mechanism for collective account keeping and functions either independently or together. For the case of an individual operation, it does not mean having a joint account but it provides freedom to work independently to the participants of the joint account. In some cases it is not socially safe.

Suppose A and B have a joint account and A is hostile to B and wants to remove all the money from the account at a later time. In this scenario A cheats B. It is ensured in the proposed method that transaction is possible only when both users are available. It also guarantees that no one can abuse the data stored in the database as shares are random noise like pictures and no one can get any information from a single share even if they apply enormous computing power and time. Gray images of both users are taken as input and processed for further use in the proposed system. The ultimate process is split into two phases: phase of encryption and phase of decryption.

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.

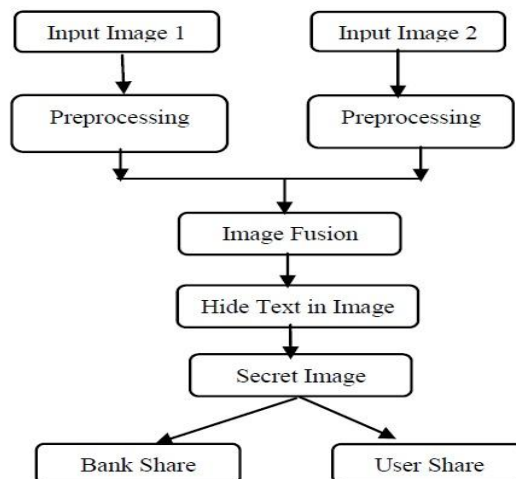


Figure 5: Encryption phase

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 in each image[39]. The effect is an image with a higher quality of information compared to any one of the input images. The purpose of the fusion process is to evaluate the information in the input images at each pixel location and retain the information from that image which best represents the true content of the scene or improves the usefulness of the fused image for a specific application. Image fusion is a vast discipline in itself, which refers to the fusion of various types of images that provide complementary details. Image fusion incorporates two or more existing images of the same object into one image that is easier to view than either of the originals.

Hide text in Image (Steganography)

Image files can cover text without impacting too much on their size. Steganography is named, and it helps you to cover text in pictures without anyone noticing.

Share Generation

Hidden image is fed as input for the process of generating the share. For the secret image two shares are generated using (2,2)-VCSXOR. Another share is called as a bank that is held in the bank database and another is called user share and further divided into two share share1 and share 2, share1 is given to user A and share2 to user B using the same scheme.

B. Decryption Phase

When users are required to perform the transaction they must provide the bank with their shares. Bank performs the XOR operation between the shares of the user and produces the share of Users. XOR operation is performed between Users share and Banks share to reconstruct the secret picture. This method recovered the secret image, because of the associative existence of XOR operation, which is the same as secret image. This is shown in Figure 6.

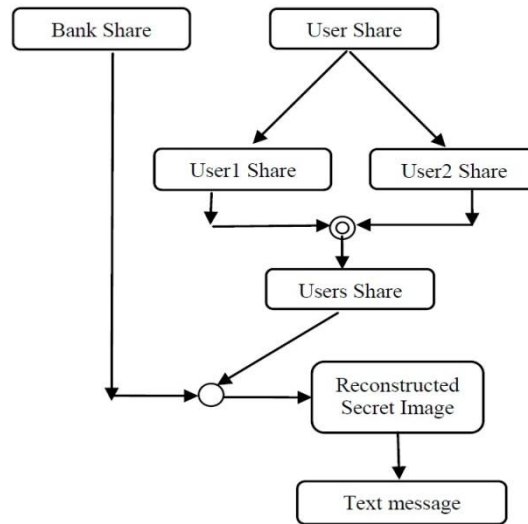


Figure 6:Decryption Phase

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

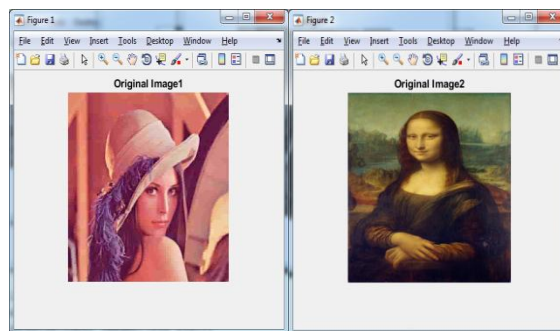


Figure 7:Original Images

2. Original gray scale images

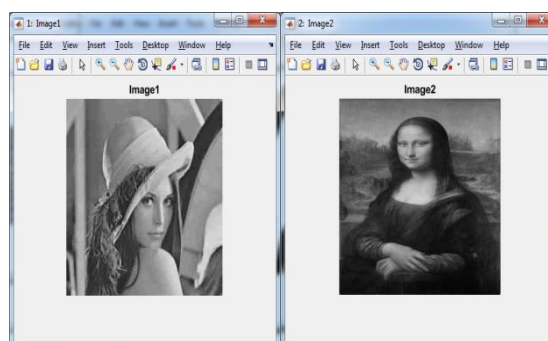


Figure 8:Original gray scale images

3. Preprocessed Images

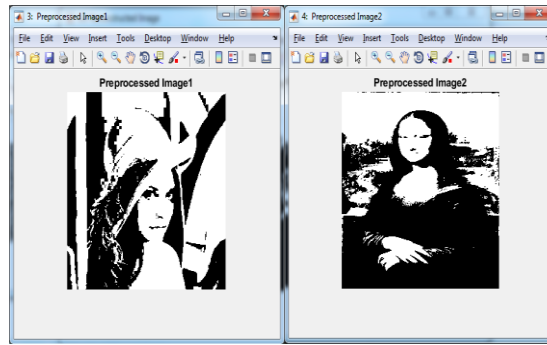


Figure 9:Preprocessed Images

4. Concatenated Image

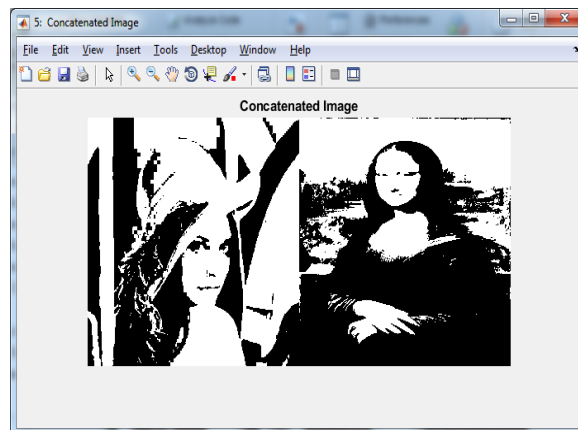


Figure 10:Concatenated Images

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

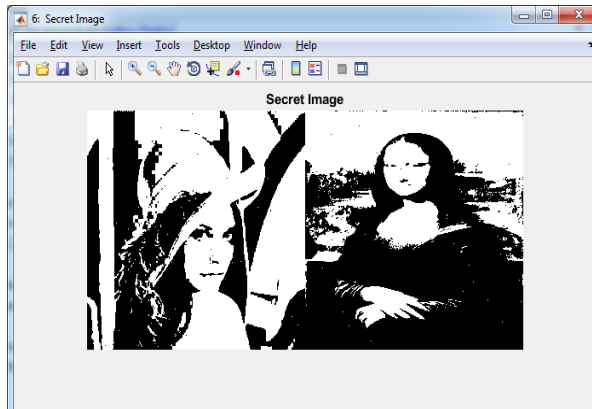


Figure 11:Secret Images

6. Bank Share

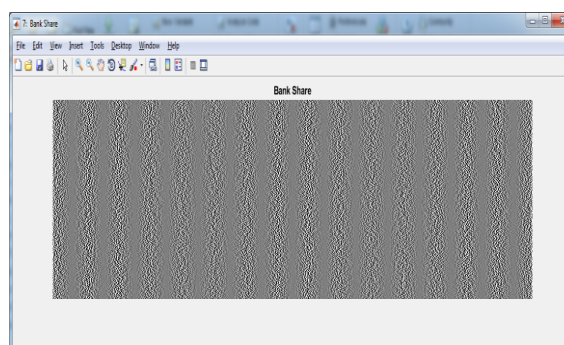


Figure 12:Bank Share Image

7. User Share

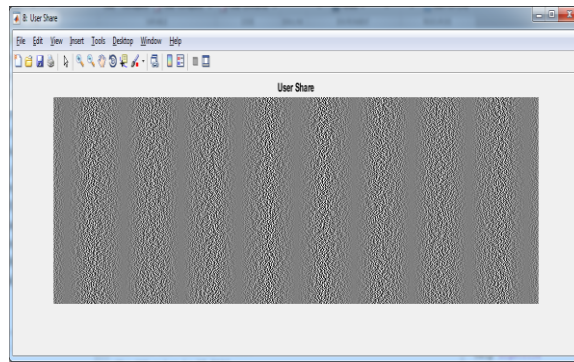


Figure 13:User Share Image

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

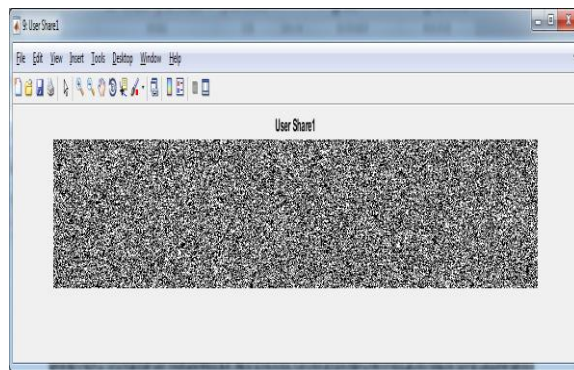


Figure 14:Share 1 Images

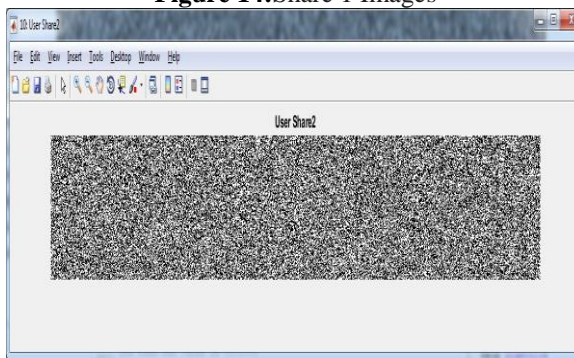


Figure 15:Share 2Images

8. Reconstructed Image

Finally we get reconstructed image and the text message

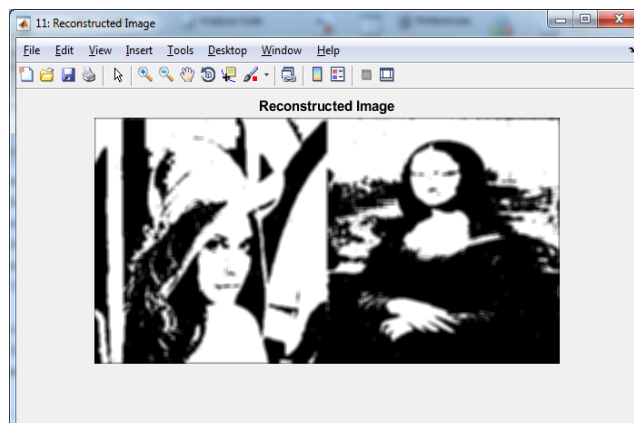


Figure 16:Reconstructed Image

The text message is completely decoded and shown as below (the email I d is rajat123@gmail.com and the password is 09876) The inserted text message and the decoded text message are similar. It will allow users to sign in and start online banking. Figure 7 and Figure 8 are initial and gray images taken as input while Figure 9 is pre-processed binary images derived from gray images respectively Figure 8. Figure 10 shown as a concatenated image, which is obtained from Figure 9 as shown in Figure 11. Figure 13 is split into user shares after the Hidden picture Figure 14 and 15. Figure 12 is an picture of a bank-share. Reconstructed hidden picture is obtained using the shares Figure 11, Figure 12 and Figure 13 as shown in Figure 16.

VII. CONCLUSION

Original image in this system is preserved by decomposing it into n shares. This research focuses primarily on issues related to identity fraud and data protection for consumers in the joint account transaction. This work proposed a method which is based on (2, 2)-VCS-XOR with Hide text in Image (Steganography) for safe banking transaction in joint account service. Experimental findings show the reconstructed secret image of the original secret image is the same in size and consistency.

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 Conference1979, 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.