An Intelligence System for Visual Cryptography Techniques for E-Banking Transactions

Sumit Yadav, M.Tech Scholar, Department of Computer Science & Engineering, Faculty of Engineering & Technology, Rama University, Kanpur, India
Manisha Verma, Assistant Professor, Department of Computer Science & Engineering, Faculty of Engineering & Technology, Rama University, Kanpur, India

Abstract—**Researchers also suggested a variety of security strategies to secure digital data. By storing sensitive data in a distributed manner, security techniques can be rendered more effective. In contrast to visual cryptography, traditional encryption strategies take longer to compute. Visual cryptography is thought of as a natural blend of secret sharing and digital image processing.**
The use of computers and the internet has become so widespread that it has influenced every aspect of banking. Since banks are dedicated to providing safe core banking services to their customers, security has become the most critical feature of today's banking transaction system. To achieve this goal, users must be authenticated, which ensures that only approved users can participate in the transaction. Banks use biometrics-based authentication systems for this reason, but the banking system's database is no longer safe due to unavoidable malicious activities. Smart hackers can extract biometric information from a bank's database and use it to make fraudulent transactions. To stop any of this, a visual cryptographic technique is employed. Visual cryptography is a powerful encryption scheme in which data is hidden inside images and can only be decrypted by the human visual system. The main goal of this thesis work is to propose a stable XOR operation based visual cryptography and image processing technique for banking transaction security. Our system becomes more stable and effective when we use the Steganography method we propose.

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

I. INTRODUCTION

Digitalization has the biggest potential to transform our habits. Protection is a major concern in today's digitally connected world. When information is sent from one node to another over the network, security issues begin to emerge. Since the number of threats is growing at a faster pace, strong protection strategies are needed. One of the most important strategies for ensuring information security is cryptography [4-8]. Traditional cryptographic methods need a lot of computing power and complicated algorithms to encrypt and decode a secret message, which takes a lot of time and resources. Biometrics-based authentication is commonly used in the banking industry. To authenticate the subject or verify claimed identity, a biometrics-based authentication system obtains raw biometric data (e.g., face picture, fingerprints, etc.) from the subject, extracts feature set from the raw data, and compares the feature set to the blueprint stored in the database. Any institute's or organization's security is based on the underlying design technology middleware and, to a large extent, the database design. Any transaction has an effect on the database, whether it is spatial or temporal. As a result, hackers are constantly attempting to breach the database. While the banking system provides web-based core services, the authentication of the user is a big problem. Password-based authentication, smart card-based authentication, and biometric-based authentication systems are all used for this purpose. All of these techniques are needed to keep a database up to date, making it vulnerable to hacking. Since the database includes private information, there is a risk of privacy breach. 1
Visual Cryptography [1-3] is a secret sharing scheme that takes a secret image as input (i.e. typed, handwritten) and encrypts it into a collection of other images called shares in such a way that the original secret is exposed if the shares are printed on transparencies and superimposed or staked over one another. The simplest type of visual cryptography, also known as visual secret sharing, takes a binary image as input and treats each pixel separately [9].
To encode a pixel of the secret image, we break it into n versions in such a way that the original secret pixel is exposed when all n versions are printed on transparencies and superimposed. This method must be used for the entire secret picture. As a result, n copies of the original hidden image are ready to be printed on transparencies and superimposed to show the secret. To ensure authentication and confidentiality of the information stored in the bank database, a system employs XOR operation-based Visual Cryptography and image processing techniques. Our system becomes more stable and effective when we use the Steganography method we propose [15].

II. LITERATURE REVIEW

A brief overview of the literature related to the progressive deterioration of building systems is presented below.
This section provides a brief overview of Visual Cryptography and its applications in the banking system. G. Blakely [11] and A. Shamir [12] independently introduced the (t, n)-secret sharing scheme in 1979 for safeguarding cryptographic systems keys, which 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, the secret will not be exposed. The secret sharing schemes of G. Blakely and A. Shamir are based on vector space and polynomial interpolation, respectively.
Visual cryptography is a safe method of detecting fake websites and the phishing attacks that result from them. It is a method of transmitting and receiving messages that only the sender and recipient can decrypt. This technique was introduced by Naor and Shamir [1] as an easy and safe way of sharing a hidden image as a password.

This technique has two parts: encryption decryption and image sharing generation. A basic mathematical algorithm is used to encrypt and decrypt messages. The image's share generation is the scheme's second important component. VCS is a cryptographic method for encrypting visual information such that it can only be decrypted by humans.

The visual cryptography scheme for secret sharing was formally described and proposed by Naor and Shamir [1]. Since then, VC research has grown in popularity, becoming a focus for a variety of studies. There are several different forms of VC, each with its own focus on practical use. The operation of splitting a VC secret image into shares has been based on the areas of being applied to various forms of secret images, such as grayscale and color images. To address the previous accomplishments, this chapter first introduces basic knowledge of secret sharing and VC. Several contributions to the literature have been discussed in light of various VC schemes that have been proposed in the literature.

The reconstructed picture of the OR-based VCS is of poor quality. In most of the schemes, it cannot be changed beyond a certain stage. Tuyls et al.[13] proposed a VCS scheme that uses the Boolean XOR as the underlying mathematical operation and is based on light polarization.

A liquid crystal coating is placed into a liquid crystal display to achieve this (LCD). In contrast to OR-based systems, where participants must hold a number of transcripts in order to update their shares, an XOR-based VCS needs only a computer with a monitor.

The liquid crystal layers must be stacked together in order to recover the hidden image. Furthermore, due to rapid technological advancements, these devices are becoming more affordable. The developers of the suggested XOR scheme [13] built an XOR based (n,n) -VCS and proved that an XOR based VCS is equivalent to a binary code.

In general, XOR-based VCS are non-monotone, which means that just because a qualified group of parties can recover the secret image does not mean that any superset can. The key difference between these two visual cryptography models is that the OR model captures strong access structures, while the XOR model cannot satisfy monotone properties due to the randomness of the XOR operation. However, by making a minor change to the description of the XOR scheme, we can solve this problem.

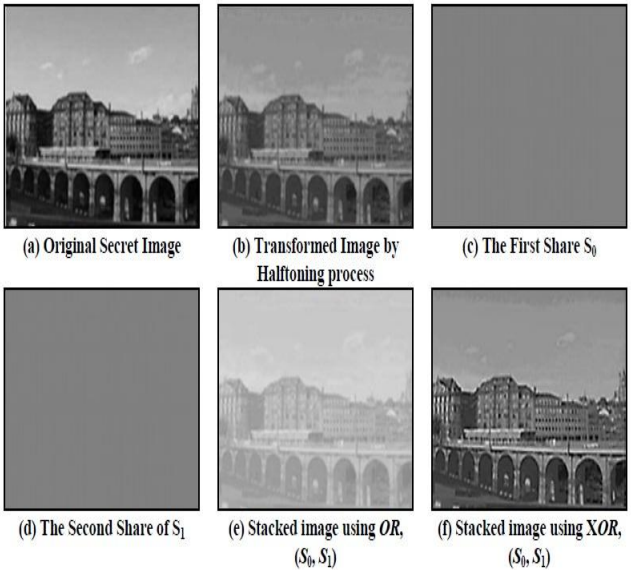

Figure 1: Process of XORing operation on VCS

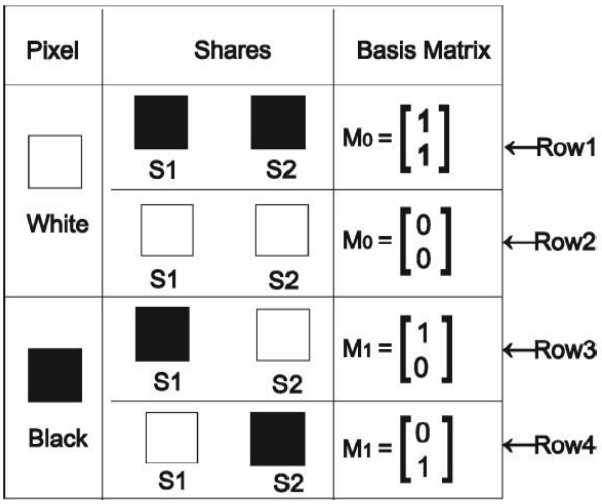

Figure 2: (2, 2)-VCS Scheme

The security conditions for both versions are identical, but the contrast condition differs. The half toning technique has been used to expand Naor and Shamir's [1] original suggestion in the 2-out-of-2 secret sharing scheme. It also goes a step further than basic visual cryptography by supporting other image variants.

III. VISUAL CRYPTOGRAPHY

Within the security domain, cryptography has a long and interesting history. The handling of classified photos containing secret information is a top priority in many agencies, such as the military's distribution of maps over the internet and several other commercial sectors. Various image secret sharing systems have been developed to address the security issues with sensitive images. Visual cryptography (VC) is a technique developed by Naor and Shamir [1] in 1995 to manage hidden image sharing.

VC is a method of encrypting a hidden image containing sensitive visible information in such a way that the decryption can be done entirely by the human visual system (HVS) without the use of computers. Any visual content, such as printed text, handwritten notes, and images, can be encrypted using VC. It removes the need for complex computation during the decryption process, and the images can be restored by stacking the shares. It blends the features of creating perfect ciphers and exchanging secrets in cryptography. The secret image is usually split into two or more shares. The hidden images are retrieved when the requisite number of shares are printed on transparencies and then superimposed.

The technique of VC was introduced by Naor et al. [1], in which the binary image is decomposed into n number of shares. Figure 1.1 depicts an example of using visual cryptography to create a share and recover a hidden image. As shares are stacked on top of one another in the (k,n) scheme, the original hidden picture is shown. For a binary image, the Naor scheme is ideal. The shares generated in the original image are calculated by choosing pairs of sub-pixel matrices for black and white pixels at random [2], whereas the VC scheme proposed by Naor et al. [1] does not require computer involvement in any situation for decryption. For the purpose of secret sharing, visual cryptography incorporates the concept of the perfect secret with a random picture [3]. The following section discusses the different features of VC schemes.

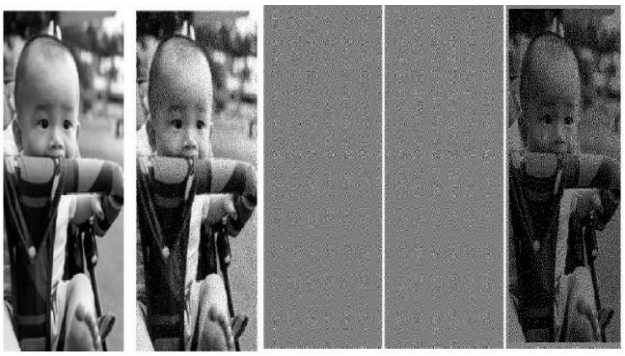

Figure 3: Original image, Halftone, Share-1, Share-2 and Decrypted image

IV. STEGANOGRAPHY

Steganography attempts to hide digital information in secret networks in order to mask the information and avoid the concealed message from being discovered [15]. Steganalytic systems are used to detect whether an image contains a hidden message. Steganalysis is the art of finding hidden information, while steganalytic systems are used to detect whether an image contains a hidden message. A steganalytic device can detect stego-images by comparing different image features between stego-images (images with hidden messages) and cover images (images with no hidden messages).

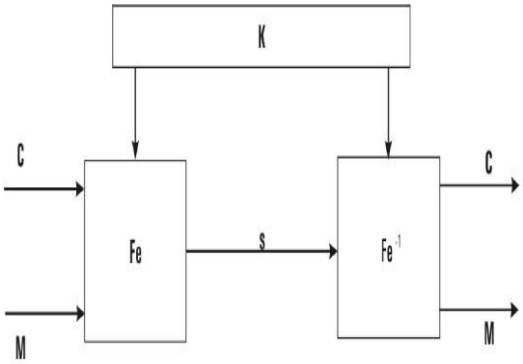

Figure 4: A Steganographic model

The aim of steganography is to conceal a secret message inside a cover-media in such a way that others are unable to detect its existence. In layman's terms, "steganography" simply means "hiding one piece of data inside another." Modern steganography makes use of the ability to hide data in digital multimedia files as well as network packets. The elements needed to hide information in a media are as follows: [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 creates a stego media by combining cover media and the message (to be hidden) with a stego-key (S). Figure 4 depicts the steganography process scheme.
Data is hidden using steganography and cryptography. Cryptography is the science of scrambling data so that no one can decode it without the use of specific methods or keys; it enables a person to encrypt data so that only the receiver can decrypt it. Steganography is the science of obscuring a message into a host object (carrier) such that the context in which the message was transferred is not suspected. Despite their functional differences, steganography and cryptography are effective partners. Cryptography is often used in conjunction with steganography.

V. METHODOLOGY

The banking system allows for the creation of a joint account that can be used jointly or individually. Individual activity does not imply the existence of a joint account, but it does allow joint account participants to work independently. In certain situations, it is not healthy socially[17].
Assume A and B have a joint account, and A becomes enraged with B and wishes to remove all of the funds from the account. In this case, A has deceived B. It is ensured in the proposed method that transactions are only possible when both users are open. It also ensures that no one can misuse the data stored in the database because shares are random noise, similar to images, and no one can extract any information from a single share, even though they use a lot of processing power and time. Gray images of both the user and the proposed approach are used as feedback and processed for further use.
The entire procedure is divided into two stages: Phases of encryption and 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.

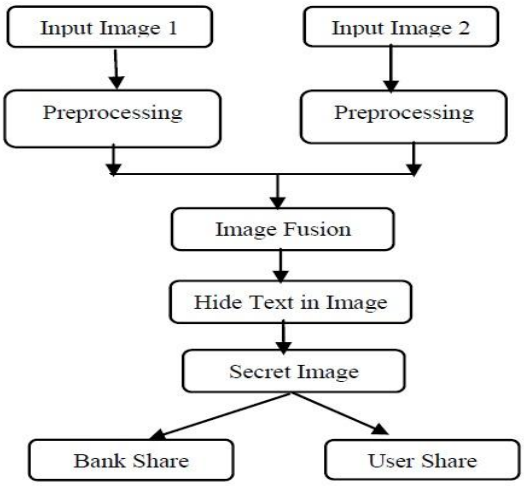

Figure 5: Encryption phase

Preprocessing
User A and user B must show a face picture to the bank while applying for a joint account. Respective authority preprocesses and creates the users A and B's shared identification. The hidden picture refers to the users A and B's combined identity.

Image Fusion
Image fusion is the process of merging two or more images into a single composite image that incorporates the details from the individual images [39]. In comparison to either of the input images, the result is an image with more information content. The fusion process evaluates the information at each pixel position in the input images and retains the information from that image that better reflects the true scene content or improves the utility of the fused image for a specific application. The fusion of different forms of imagery that provide complementary details is referred to as image fusion, which is a large discipline in and of itself. Picture fusion is the process of combining two or more recorded images of the same object into a single image that is easier to view than the originals.

Hide text in Image (Steganography)
Text can be hidden in image files without affecting their size too much. It's a technique known as steganography, and it helps you to conceal text in images without anyone noticing.

Share Generation
The hidden image is fed into the share generation process as an input. Using (2,2)-VCSXOR, two shares are created for the secret picture. One share is known as Bank and is held in a bank database, while the other is known as Users share and is split into two shares, share1 and share 2, using the same system. Share1 is given to user A, and share2 is given to user B [18].

B. Decryption Phase

Users must provide their shares to the bank in order to complete the transaction. The bank produces the Users share by performing an XOR operation between the user's shares. The XOR operation is performed between the Users share and the Banks share to reconstruct the secret picture. Because of the associative nature of the XOR procedure, this method reconstructed the secret image, which is identical to the original secret image. Figure 6 depicts the situation.

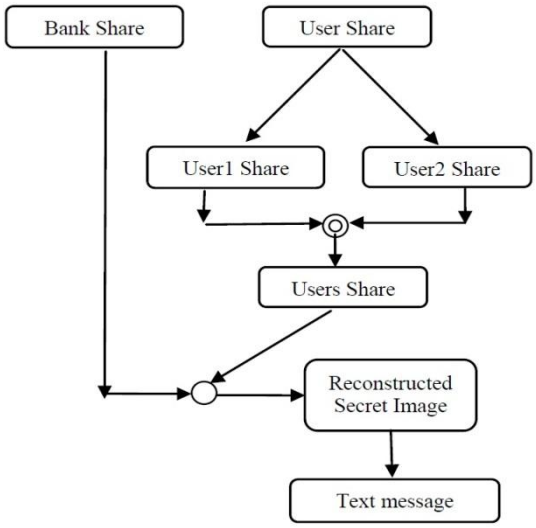

Figure 6: Decryption Phase

Convert the restored hidden image to the original text during the decryption process.

VI. Results and Analysis

The functions described in the image processing tool box are also used to perform various activities such as preprocessing, conversion of grayscale images to black and white, development of shares, and hidden reconstruction. Initially, users' images are grayscale, and they are resized to render all user images the same size.
The proposal was implemented using steganography, and the findings were checked using images.

1. **Original Images**

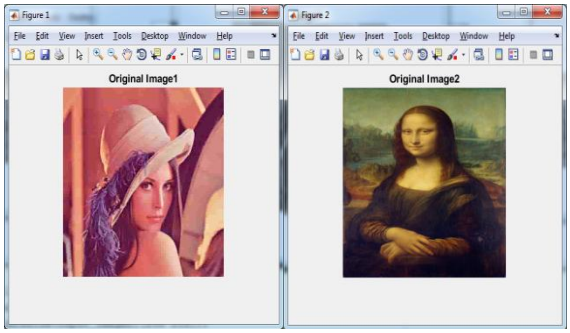

Figure 7: Original Images

2. **Original gray scale images**

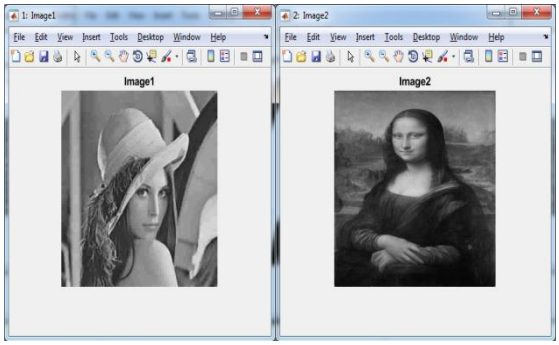

Figure 8: Original gray scale images

3. **Preprocessed Images**

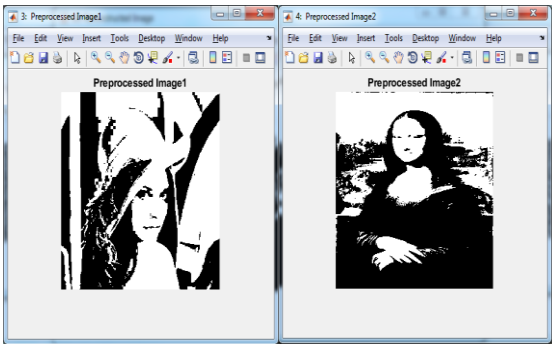

Figure 9: Preprocessed Images

4. **Concatenated Image**

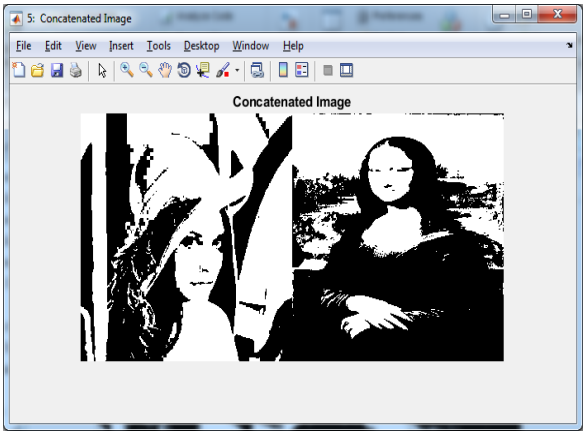

Figure 10: Concatenated Images

5. **Secret Image:** it contains a hidden text message in image as (email id is abc12@gmail.com and password is 09876)

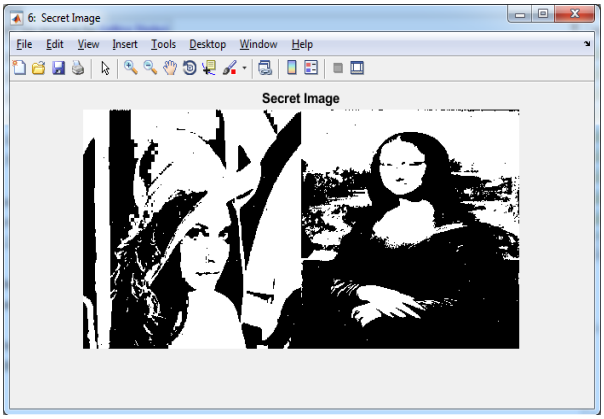

Figure 11: Secret Images

6. **Bank Share**

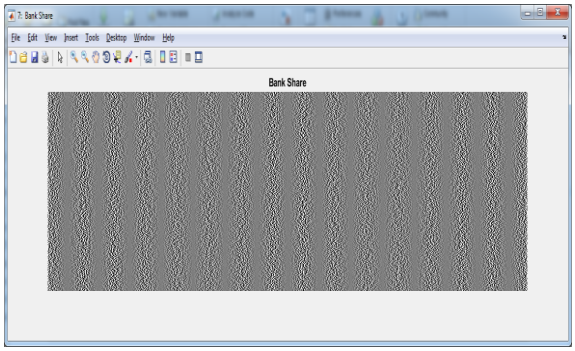

Figure 12: Bank Share Image

7. **User Share**

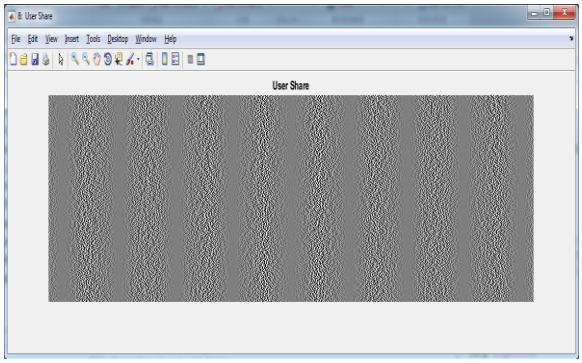

Figure 13: User Share Image

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

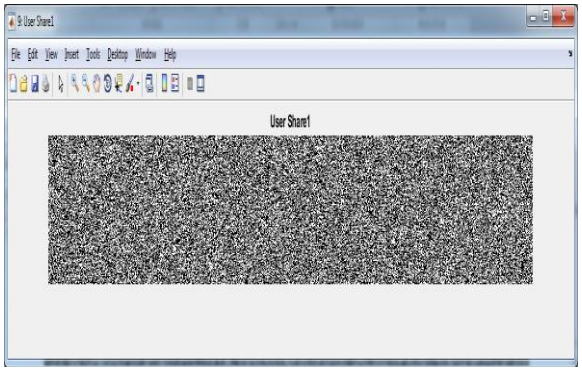

Figure 14: Share 1 Images

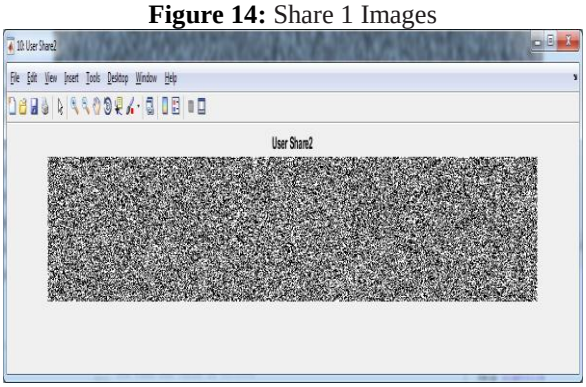

Figure 15: Share 2Images

8. Reconstructed Image

Finally we get reconstructed image and the text message

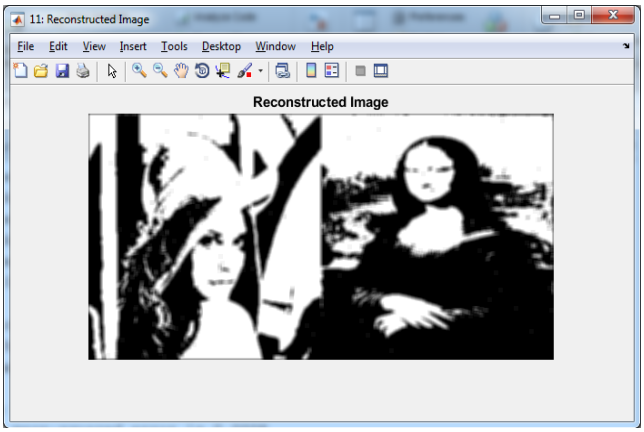

Figure 16: Reconstructed Image

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.

Original images and gray images are used as input in Figures 7 and 8, respectively, while preprocessed binary images are derived from gray images in Figure 8. Figure 10 is a concatenated image, and Figure 11 is the secret image obtained from Figure 9. After that, user shares Figures 14 and 15 are split from the hidden picture Figure 13. A bank share is depicted in Figure 12. The shares Figure 11, Figure 12, and Figure 13 were used to reconstruct the hidden image shown in Figure 16.

VII. CONCLUSION

The original image is protected in this system by dividing it into n shares. This project is specifically concerned with issues of identity fraud and consumer data protection in joint account transactions. This work proposed a method based on (2, 2)-VCS-XOR with Hide text in Image for safe Banking Transactions in joint account operations (Steganography). The restored secret image is the same size and consistency as the original secret image, according to the results of the experiments.

.

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.

[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.