Visual Cryptography and Image Processing Approaches for Enhanced E-Banking Transactions

Kamlesh Kumar Rajpoot, M.Tech Scholar, Department of Computer Science & Engineering, Vishveshwarya Group of Institutions, Gautam Buddh Nagar, India.
Mrs. Madhu Lata Nirmal, Assistant Professor, Department of Computer Science & Engineering, Vishveshwarya Group of Institutions, Gautam Buddh Nagar, India.

Abstract— **Researchers have come up with a range of various security measures in order to preserve the digital information. By storing sensitive information in a manner that is distributed among numerous places, security measures can be tailored to be more effective. Visual cryptography techniques demand substantially less time investment in terms of computing in contrast to more standard security solutions. Visual Cryptography is considered as and investigated as the optimal mix of information sharing in trust with the processing of digital images.**
Because the use of computers and the internet has become so prevalent, it now has an impact on all sections of the banking industry. Because banks have made a commitment to providing their clients with secure core banking services, security has emerged as the single most crucial component of today's system for processing financial transactions. In order to attain this purpose, the legitimacy of the users is vital. This means that only the users who have been authorized authorization to participate in the transaction can do so. In respect to this purpose, banks use authentication systems that are based on biometrics; yet, due to unavoidable hostile activities, the database of the financial system is no longer secure. Hackers with sufficient intelligence can retrieve the biometric details of clients from the bank's database and then use those details to fabricate fake transactions later on. A visual cryptography technique is applied so that all of these fatal scenarios can be avoided. Visual Cryptography is a highly effective method of data encryption in which information is disguised inside visuals and can only be read by the visual system of a human being. The fundamental objective of this thesis work is to propose a secure XOR operation based visual cryptography and image processing approach for the purpose of securing financial transactions. Steganography is going to be implemented in our proposed solution, which will make our system both more secure and more efficient.

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

I. INTRODUCTION

The advent of digitization presents the greatest opportunity for bringing about a change in the way that we live. In this day and age, when everything is moving toward becoming more digitalized, there is a significant concern regarding safety. The vulnerabilities in the network's security become apparent and begin to cause problems with the transmission of data from one node to the next as it moves through the network. It is necessary that stringent safety precautions be taken because the number of possible threats has been increasing at a quicker rate, making it more important than ever to take these precautions. It is of the utmost significance to make use of cryptography [4-8] as one of the key approaches for the protection of sensitive information. Cryptography [4-8] The older methods of cryptography call for a large amount of computing power as well as complicated algorithmic solutions. As a consequence of this, encoding and decoding a secret message can be a laborious and time-consuming process that can also be rather costly. Authentication based on biometric traits is often applied in the financial sector as a standard practise. A biometrics-based authentication system works by first obtaining raw biometric data from the subject (such as an image of their face or their fingerprints, for example), then extracting a feature set from the raw data, and finally comparing the feature set to a blueprint that is stored in the database. This allows the system to authenticate a subject or verify their claimed identity. This is done in order to substantiate the subject's claims regarding their identification or authenticate the subject. The design of the database, in addition to the underlying design technology middleware, is the single most essential aspect in defining the amount of security that can be offered to any particular firm or institution. Each geographical and temporal transaction will have some kind of an effect on the database. Hackers try their hand at breaking into the database on a regular basis because of this. The authentication of the user is a key barrier for the banking system, which, despite the fact that it provides essential services that can be accessed over the web, continues to do so. Several different approaches, including authentication based on passwords, authentication based on smart cards, and authentication based on biometric data, are used in order to achieve this objective. Some of these methods include: As a consequence of the fact that each of these procedures is required for the database to be maintained, it is susceptible to being hacked. Due to the fact that the database stores personal information, there is a possibility that an individual's privacy could be invaded. 1
Visual Cryptography [1-3] is a method for sharing a secret that encrypts the secret image that is used as input (i.e., printed or handwritten) and uses that encrypted image to generate a set of other images that are called shares. This method uses a secret image as input (i.e., printed or handwritten). The shares are encoded in such a way that the original secret can only be decrypted if the shares are printed on transparencies and then staked over one another. This is the only method by which the original secret can be deciphered. The most elementary form of visual cryptography, also known as a visual secret sharing system, starts with a binary image as its input and then processes every single pixel on its own. This is the most basic form of visual cryptography. [10]

s

In order to encode a pixel of the secret image, we first break the secret pixel into n different versions in such a way that the original secret pixel can only be decoded if all n different versions are printed on transparencies and then superimposed on one another. This is done in such a way that the original secret pixel cannot be decoded without all n different versions being printed on transparencies. It is imperative that this process be carried out on the complete confidential photograph. Because of this, n duplicates of the original secret image have been made; in order to solve the mystery, you will need to print the copies on transparency and then superimpose them on each other. Visual Cryptography, which is based on the XOR operation as well as image processing methods, is one method that can be used to authenticate users and maintain the confidentiality of the data that they have entered into the bank's database. This method is just one of several available options. The adoption of steganography, which is the approach that we recommend, using, will cause our system to become both more secure and more effective [15]. Because of the development of the Internet and interactive media contents, such as sound, picture, video, and so on for communicating hidden images or data, security issues should be given significant thought because programmers may use frail connections over communication organization to take data that they required. Currently, security is a major risk in the transmission medium because of these developments. Different picture mystery sharing methods have been developed in order to address the concerns regarding the safety of secret photographs. These plans have given rise to new developments in the field of photography that call for less calculating and less hoarding than their predecessors. Naor and Shamir (1995) came up with the concept of visual cryptography, also known as VC, which enables the encryption of data that is concealed inside a picture's structure. A system known as visual cryptography is one that divides a secret image into n different profits, with each individual profit holding at least one position. A secret picture was broken up into a number of distinct offers with the use of visual cryptography, and each of those offers was then given to one of n different people. Through the accumulation of their n profits, it is possible to unearth the concealed data and make it visible to the human visual framework on the outside. The visual cryptography is also known as secret sharing in other contexts. The most elementary form of visual cryptography splits a mysterious image into two parts, each of which, on its own and without the assistance of anybody else, does not transmit any data. The first riddle can be solved once these two parts have been brought together using techniques that involve superimposing one on top of the other. The field of visual cryptography centres on a select few key areas. To put it simply, it is simple to use, and there is no need to perform any mathematical calculations in order to solve the enigma. People who are not familiar with cryptography are also, in an indirect way, participating in the decoding process. In spite of the fact that the majority of these investigations focused on the preparation of dark shading photographs, only few of them suggested ways for doing so. The majority of the techniques that are utilized on shading photos, for instance, do not bring back the initial picture. The information contained in this paper presents many visual plans and strategies for the secure exchange of data.

II. Literature Review

The following is a brief overview of the numerous pieces of literature that were examined and reviewed in relation to the progressive collapse of the building structures.

This section presents a synopsis of Visual Cryptography as well as its applications in the Banking System in an easy-to-understand format. The (t, n)- secret sharing scheme was separately created in 1979 by G. Blakely [11] and A. Shamir [12] for the aim of securing the keys of cryptographic systems. This indicates that the secret can be uncovered if at least t out of n shares are combined in a particular way; however, it should not be assumed that this will be the case because it is not a given. If there are fewer than t shares available, the secret cannot be revealed. This is the only scenario in which it is permissible. The G. Blakely technique for secretly sharing information makes use of vector space, whereas the A. Shamir scheme for secretly sharing information makes use of polynomial interpolation as its basis.

Visual Cryptography is a technology that may be used to identify fraudulent websites and the phishing efforts that are a direct result of those websites without running the danger of being scammed. It is a system that allows for the sending and receiving of communications, the contents of which can only be understood by the sender of the message and the recipient of the message. Naor and Shamir [1] initially offered this method as an easy and risk-free approach to exchange a secret image as a password. They described it as a method for exchanging a password.

The two parts that make up this method are the process of decrypting data that has been encrypted and the process of producing photographs that may be shared. A straightforward mathematical method is applied in both the process of encrypting a communication as well as decrypting one that has been encrypted. The creation of the image through the utilisation of resources that are communally available is the second fundamental component of this methodology. The VCS is a type of cryptographic technology that encrypts visual information in such a way that the process of decryption can only be carried out by a human being. This makes it impossible for machines to read the encrypted data.

Sejal krishna Gajbhiye, Pooja Gedam, Lavanya Gannamani,Mrunal Deshmukh (2020), In this research, a visual cryptography system that shared two of two secrets was described in order to encrypt colour images. This approach divides the input colour image into two parts in such a way that it is impossible for either of those portions to accurately forecast even a small fraction of the entire original image. By performing an X-OR operation on both pieces, the original image can be reconstructed. The method that has been proposed does not call for complicated mathematical calculations. Therefore, the size of the regained image does not rise any further, and there is an introduction of a negligible quantity of noise. However, the user is able to perceive the structure of the image by superimposing the two halves.

John Blesswin A., Christhu Raj, Rajeev Sukumaran, and Selva Mary G. were the authors of this study (2019), In this research, an Enhanced Semantic Visual Secret Sharing (ESVSS) Scheme was presented. This scheme sends a grayscale secret image to the receiver while simultaneously concealing it with two colour cover images. At the receiving end, the hidden image is pieced back together using a digital stacking technique to piece together the individual shares. The study of the results demonstrates that the ESVSS accomplishes both the goal of achieving security and improving the quality of the rebuilt image. Peak Signal to Noise Ratio (PSNR) up to +39 dB and Mean Square Error decreased to 6 are the metrics that are utilized to evaluate the level of

quality. For the image that was reconstructed, the findings of the Universal Image Quality Index (UIQI) can be recorded at up to 90 percent with only a small amount of processing complexity.

Shital B. Patel and Dr. Vinod L. Desai (2018), In their method for a secure online payment system utilizing Visual Cryptography (VC), used Secure Socket Layer (SSL) encryption to safeguard data between end users and online merchant websites from being stolen. This method protects the client information in order to prevent any fraudulent activity that may occur when making online purchases. When a customer creates an account at a bank, the bank will provide the consumer with a private key, which will then be split into two shares. The other half will be given to the consumer, while the first share will be kept by the bank in its database.

This section provides a high-level overview of Visual Cryptography and its applications in the banking industry. Keys are required for the protection of cryptographic systems. According to G. Blakely [11] and A. Shamir [12], in 1979 they each independently created the (t, n)- secret sharing scheme. This scheme states that the secret can be revealed when at least t shares out of n shares are combined in a specific manner. It is not possible to reveal the secret if there are fewer than t shares available. The secret sharing schemes developed by G. Blakely and A. Shamir are both based on vector space, with the latter employing polynomial interpolation as a base.

Visual cryptography is a safe way for identifying bogus websites and phishing attempts that are perpetrated on them. It is a way of transmitting and receiving communications that can only be decoded by the sender and the recipient themselves. This technique was developed by Naor and Shamir [1] as a simple and secure way of transmitting a secret image as a password with others.

S.Makbul Hussain Proposed Text-Based Steganography Method by G. Mahaboob Basha (2017) The strategy reduces the amount of personal information about customers that is transmitted to online retailers. The presence of a third party CA enhanced the level of security even more because it involved an increasing number of parties in the process. Steganography ensures that the Customer Authentication Provider (CA) does not know the consumer authentication password, hence preserving the privacy of the customer.

Sarita swami and Reshma gulwani (2017), Used a text-based steganography method with a VC code that is based on an Indian root methodology. It provides the store with only the most essential of details. Use CA applications in conjunction with steganography and visual cryptography.

Shemin P.A. and Professor Vipin Kumar K.S. (2015), A technique of electronic payment that makes use of quantum cryptography, visual cryptography, and image steganography is proposed in this study. Following the establishment of an account, the financial institution will provide the customer with a private key as well as one of the shares produced through visual cryptography.

Other shares will continue to be stored in the bank's database. Applying visual cryptography to a photo of text comprising the customer's account number as well as debit and credit card information allows for the generation of a share. Using this share, the customer can now conduct electronic shopping.

By preventing a "man in the middle" attack, the suggested solution that is based on two different cryptographic protocols offers complete and total security. The usage of VC in this system protects the customer's data, and the implementation of quantum cryptography and image steganography eliminates potential security risks such as phishing and identity theft.

The layers of liquid crystal need to be piled one on top of the other before the hidden image can be recovered. In addition, the rapid improvement of technology is resulting in a decrease in the costs associated with these devices. In the proposed method for XOR [13], the authors created an XOR-based (n,n)-VCS and established that an XOR-based VCS is comparable to a binary code. This was done in order to demonstrate the usefulness of the XOR-based VCS.

In general, XOR-based VCS are non-monotone, which means that even if a qualified set of parties is able to recover the secret image, it does not always hold that every superset is able to do so as well. This is because of the way that the secret image is stored. The primary distinction between these two models of visual cryptography lies in the fact that the OR model is able to represent strong access structures, whereas the XOR model is unable to do so due to the randomness of the XOR operation. This makes it impossible for the XOR model to satisfy monotone property requirements. On the other hand, and we are able to resolve this issue by making a little adjustment to the definition of the XOR scheme.

Sayali Vaidya, Shreya Zarkar , Prof. Achal N. Bharambe, Arifa Tadvi,Tanashree Chavan, To identify the phishing website, we have been using the registration Phase and the Login Phase of the Anti-phishing Structure, which is based on the VC and RSA algorithms. Phishing websites can be recognised using Visual Cryptography and the RSA Algorithm.

Aparnaa. K. S., Sathyasundaram. M., and Santhi. P. (2016). Uses Visual Cryptography image, Security image for each client, After that, the image is segmented and used during the submission of the User ID and password, both of which are designed to be input in distinct web sites in order to carry out the image verification. During the first disclosure of the security image that has been stored in the intermediary database, the user is prompted to provide an answer to any one question. Once the user's response has been validated against the security text values stored in the server database, the server reveals the entire security image.

Determine the boundaries of the available Security Images. The system that is being proposed generates security images based on a text that is selected by the user. The text is encoded within a black and white image that has a lower contrast and a higher brightness than normal so that it may be seen by the human eye. Using this technique, the restricted security image notion of the existing system can be delimited.

s

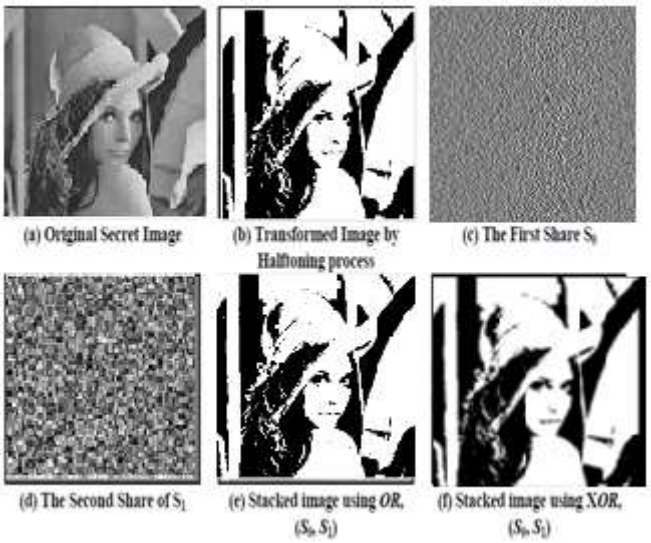

Figure 1: Process of XORing operation on VCS

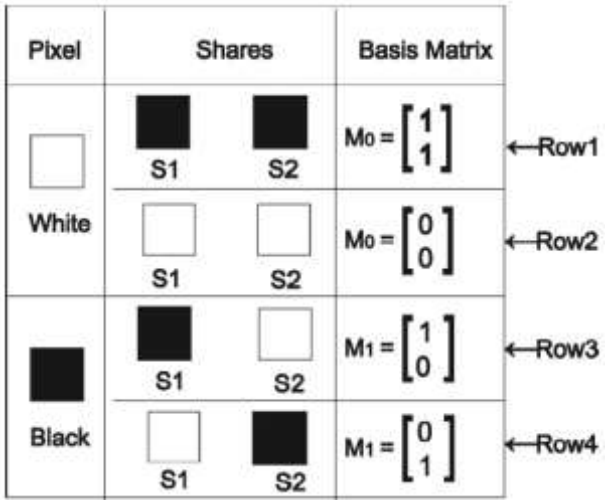

Figure 2: (2, 2)-VCS Scheme

Because of this, the contrast condition is where you'll find the difference between the two models. Since both models have the same safety conditions, this is where you'll find the difference. The fundamental idea that was developed by Naor and Shamir [1] was elaborated upon in the 2-out-of-2 secret sharing scheme by making use of a technique that is known as half toning. In addition to this, it broadens the scope of what is possible with conventional visual cryptography by offering support for an expanded range of image permutations.

III. Visual Cryptography

The term "visual cryptography" refers to a method of encryption that was first introduced by Moni Naor and Adi Shamir in the year 1994. The images are encrypted using this cryptographic method into a number of meaningless shares, which are then Xeroxed into transparency, and the original image is only preserved once all of the shares that were generated from the image have been combined together.

Steganography is the practise of concealing sensitive information within a normal, non-secret file or message in order to avoid being discovered; the sensitive information is then extracted at the location where it is intended to be delivered. The use of encryption as an additional step for hiding or safeguarding data can be supplemented by the use of steganography as an additional step.

Exploring the long and interesting history of cryptography, which is relevant to the realm of security, is something that should be done. The handling of sensitive photos that contain confidential information is a top priority in many different departments, such as the pharmaceutical industry, as well as in many other commercial sectors, such as the military, which uses the internet to share maps. This is also the case in many other government agencies. In order to address the concerns of confidentiality that are raised by images of sensitive subjects, a number of different strategies for image secret sharing have been created. In 1995, Naor and Shamir [1] developed a method that they named Visual cryptography (VC) in order to facilitate the secure transfer of images. [1] The purpose of developing this technique was to facilitate the anonymous exchange of photos.

It is a method in which a hidden image that contains confidential visible information is encrypted in a manner that is fully secure, such that the decryption may be carried out directly by the human visual system (HVS), without the use of computers. VC is capable of encrypting almost any kind of visual information, such as printed text, handwritten notes, and images. It is not necessary to carry out a complicated computation when carrying out the decryption procedure, and the images can be restored

by carrying out an action known as stacking on its shares. It combines the features of producing flawless cyphers with the characteristics of secret sharing in cryptography in order to achieve this. The components of a hidden image, which might number anywhere from two to multiple parts, are collectively referred to as shares. After the necessary number of shares have been printed on transparencies and then layered, the hidden images can be recovered.

The method known as VC, which was created by Naor et al. [1, and which involves decomposing a binary image into a n number of shares, was the first method of its kind to be presented. Visual cryptography is used to produce and retrieve a secret image in this example, which takes place within the setting of a shared network and is depicted in Figure 1.1. In the scheme of (k,n), shares that are stacked atop one another reveal a hidden image that was once concealed from view. When creating a binary image, the Naor scheme is a fantastic option to go with. The shares that are produced in the initial image are selected by first randomly selecting pairs of sub-pixel matrices for black and white pixels [2], and then combining those matrices together.

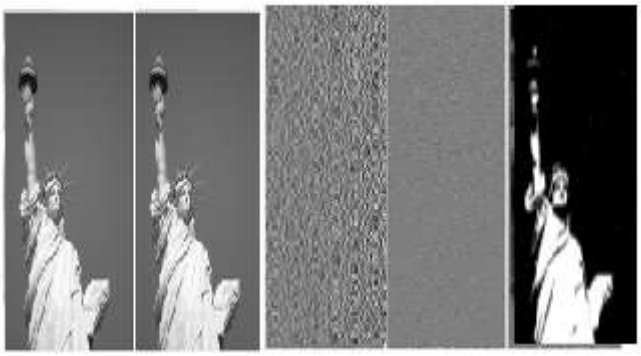

Figure 3: Original image, Halftone, Share-1, Share-2 and Decrypted image

The VC approach that was presented by Naor et al. [1] does not need the assistance of a computer in any circumstance in order to be decrypted. [Citation needed] [Citation needed] Visual cryptography is a form of encryption that makes use of visuals in order to secure secrets. This form of cryptography blends the concept of the ideal secret with that of a random image for the purpose of exchanging secrets [3]. In the following paragraphs, we will talk about the characteristics of VC schemes that are shared by all of them.

It is standard procedure to make use of visual cryptography in order to safeguard the privacy of raw images. It is needed of the vast majority of corporate enterprises to safeguard their information from being made public [4]. The majority of companies are afraid of storing all of their data on a single computer as a result of the increasing interconnectivity of the world brought about by the usage of computers. As a consequence of this, VC offers a procedure that copies the data to several different locations while simultaneously wiping the original. When there is a requirement for the original data, it is possible to reconstruct it using the distributed shares in the exact order that they are needed. There is no way that all of the information can be accessed in a single location at the same time. The following characteristics have contributed to the rise in popularity of visual cryptography among academics and researchers. As a result of these characteristics, visual cryptography has been utilized in a wide variety of security-related fields.

Its major characteristics are unbreakable security, the ability to restore secrets even in the absence of a computing device, and resistance to the effects of lossy compression [5]. The following is a list of additional qualities that visual cryptography includes as well: As a direct consequence of the fact that this method is both uncomplicated and risk-free, visual cryptography has emerged as an important and appealing area of research.

IV. Methodology

The banking system allows customers to work jointly or individually, and it also provides the option of having joint accounts. In the case of individual operation, this does not mean that there is a joint account; rather, it means that the members of a joint account have the ability to operate independently if they so choose. There are situations in which it does not guarantee social security [17].

Imagine that A and B have a joint account, and at some point in the future, A develops a grudge against B and decides they want to remove all of the money from the account. In this scenario, B is the one who is tricked by A. The proposed method ensures that a transaction may only take place if both of the users are present and available at the same time. It also ensures that nobody can exploit the information that is saved in the database because shares are random noise similar to pictures, and nobody can get any clue from a single share even if they apply a large amount of processing power and spend a significant amount of time doing so. In the method that has been suggested, grayscale photographs from both the user and the system are taken as input and then processed for subsequent usage.

The entirety of the procedure can be broken down into two distinct phases: the encryption phase and the 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 4.

s

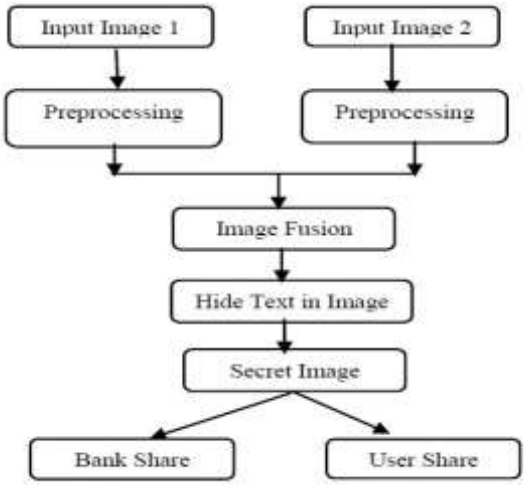

Figure 4: Encryption phase

Preprocessing

When registering for a joint account, users A and B are required to provide the bank with a photo of their faces. The respective authority performs any necessary preprocessing and then generates a combined identity for users A and B. The term "secret image" refers to the combined identities of the users A and B.

Image Fusion

Image fusion is the act of combining two or more photographs into a single composite image, which combines the information that is present within the separate images [19]. Image fusion is also known as image merging. The end product is an image that is superior in terms of the amount of information it contains than any of the input photos. The purpose 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 either best represents the true scene content or enhances the utility of the fused image for a specific application. This evaluation and retention of information is done in order to achieve the goal of the fusion process. The term "image fusion" refers to the process of combining different kinds of imagery in order to obtain information that is not available from any single sort of image alone. Image fusion is the process of combining two or more registered photographs of the same object into a single image that can be understood more quickly than any of the originals. Image fusion can also be used to create composite images.

Hide text in Image (Steganography)

Image files have the ability to conceal text without significantly increasing their file sizes. The process is known as steganography, and it enables users to conceal text within images without letting anybody else know about it.

Share Generation

The input for the process of sharing the secret image is the secret image itself. Using (2,2)-VCSXOR, two shares of the secret image are generated and distributed. One of the shares is known as the Bank share, and it is recorded in the bank's database. The other share is known as the Users share, and it is further divided using the same system into two shares known as share1 and share 2. Share1 is distributed to user A, and share2 is sent to user B [18-20].

B. Decryption Phase

When it comes time for users to carry out the transaction, they will be required to hand over their shares to the bank. The user's share is produced after the XOR operation between the bank's shares and the user's share is carried out. A XOR operation is conducted between the users' part and the bank's share so that the secret image can be reconstructed. Due to the associative nature of the XOR operation, the secret image was recreated using this approach and the result is identical to the original secret image. Figure 6 illustrates it for us.

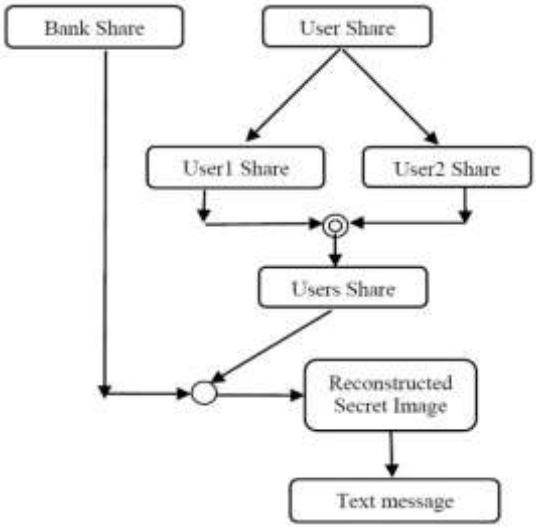

Figure 5: Decryption Phase

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

V. PROPOSED SYSTEM

Steganography is used to transfer digital data across secret channels in order to hide it [15]. This is done to prevent both the information and the hidden message from being detected. Steganalytic systems are the devices that detect whether or not an image contains a message of some sort, whereas steganalysis refers to the act of uncovering concealed information. The term "the art of detecting concealed information" also applies to steganalysis. By comparing numerous visual characteristics between images that contain concealed messages (referred to as "stego-images") and images that do not, a steganalytic system can identify stego-images (referred to as cover images).

In order to achieve the highest possible level of security at the bank, we suggested implementing a new system known as secure online transaction. So The suggested system for online transactions will only provide the merchant with the bare minimum of information. The strategy that has been provided ensures that the adversary will not have access to any relevant information even in the event that their attack is successful.

Customers have the option of opening joint accounts with the bank and conducting business either jointly or alone. When two people share a joint bank account, there is always the possibility that one of them would try to defraud the other by taking all of the money out of the account or doing fraudulent online banking transactions.

The solution that has been offered makes it such that any kind of online banking transaction may only take place if both of the account holders of a joint account are aware of it. It protects against any form of hostile assault, such as phishing and identity theft, among other things. It ensures that nobody can misuse the information that is stored in the database even if they apply as much computing power and time as they possibly can because the shares are random noise like images and they are distributed among three parties. This prevents the attackers from having any idea what is going on. In the method that has been suggested, grayscale photographs from both the user and the system are taken as input and then processed for subsequent usage. Image encryption is accomplished with the help of steganography and visual cryptography in the proposed system. The private keys for the joint account are distributed to both of the account holders [21-22].

The proposed technique for conducting online transactions involves a total of four primary parties: two individuals who hold joint accounts, a bank, and a merchant or retailer.

Before making any purchases online, the joint account holders need to open a bank account individually by giving the bank with their personal information.

When two people open a joint account at the same bank, both of their photographs are taken, scanned, and kept in the bank's database together as a single image.

The total images that include both account holders for the joint account is divided into two parts. One share is entered into the database maintained by the bank, and the other share is partitioned into two further shares before being distributed to the individuals who are listed as joint account holders.

s

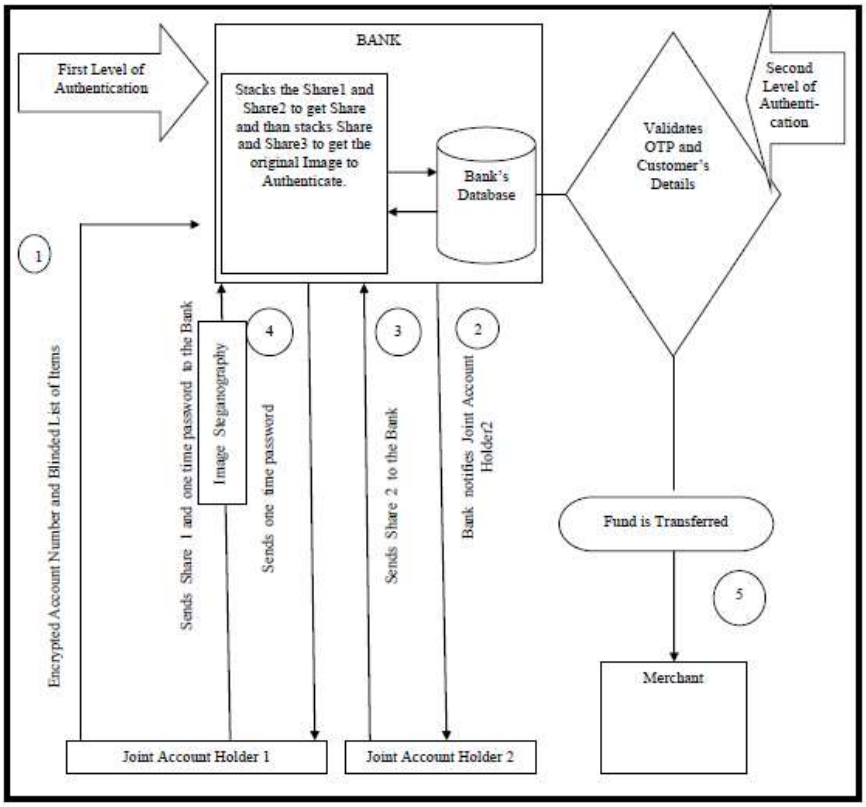

Figure 6: A Proposed System model

The purpose of steganography is to conceal a confidential message within another form of media in such a way that it is impenetrable to those who are not privy to the contents of the covert communication. In a nutshell, "steganography" means concealing one piece of data within another. This definition refers to a technical term. The practice of modern steganography takes advantage of the possibility of concealing information within digital multimedia files as well as at the level of network packets. The following components are necessary for concealing information within a medium [23].
The cover media, the message that has to be concealed, and a stego key are all required for the stego function to work properly so that it can make stego media (S). Figure 7 provides a schematic representation of the steganographic process.

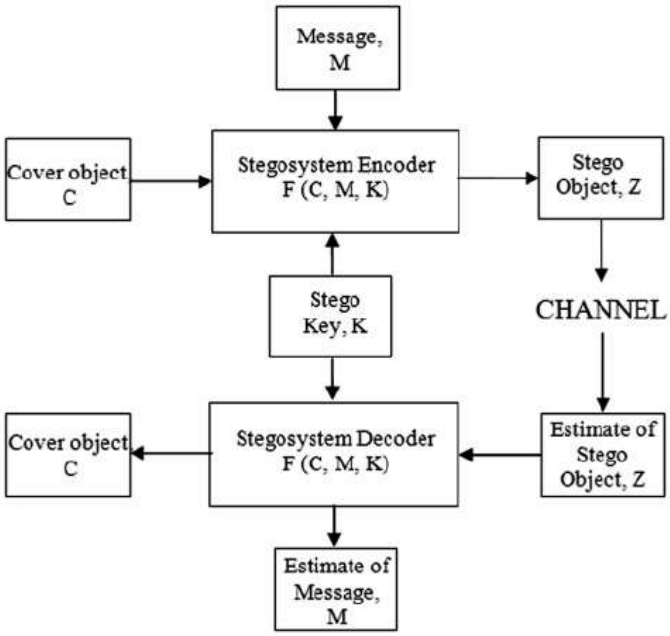

Figure 7: The Steganographic Process

Steganography and cryptography are used in the data concealing process. Using cryptography, one can encrypt data such that only the intended recipient can decrypt it. Cryptography is the study of protecting data by scrambling it in a way that prevents anyone from reading it without being given certain methods or keys [24]. Steganography is the process of hiding a message inside a host item, often referred to as a carrier, in order to avoid being discovered regarding the circumstances of the message's

transit. Despite playing very different functional functions, steganography and cryptography are good working companions. A common technique for data security and concealment uses steganography and encryption.

VI. Results and Analysis

Preprocessing, converting images from greyscale to black and white, creating sharing, and reconstructing secrets are just a few of the activities that the tools included in the image processing toolbox are employed for. To make the user photos comparable to one another, they will initially be greyed out and shrunk to the same size.
The idea was put into practice using steganography, and the veracity of the results was verified using images.

1. **Original Images**

Figure 8: Original Images

2. **Original gray scale images**

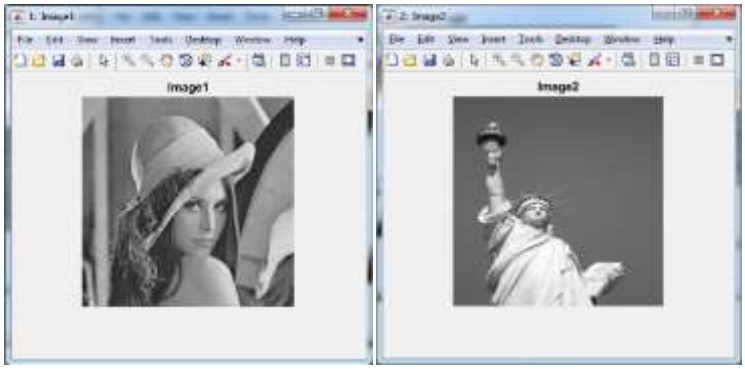

Figure 9: Original gray scale images

3. **Preprocessed Images**
4.

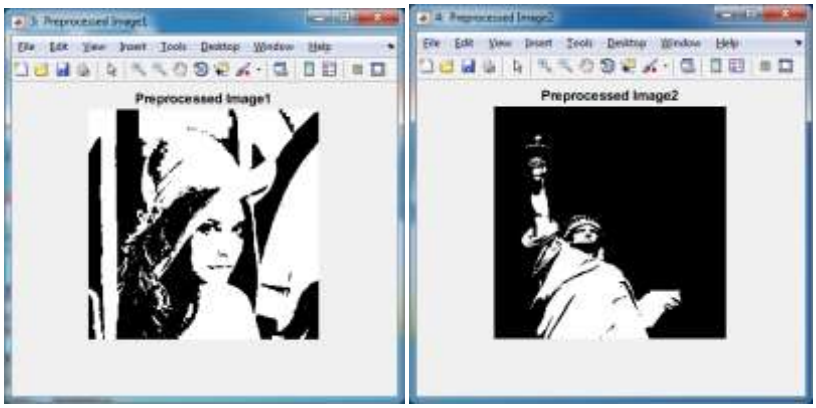

Figure 10: Preprocessed Images

s

5. **Concatenated Image**

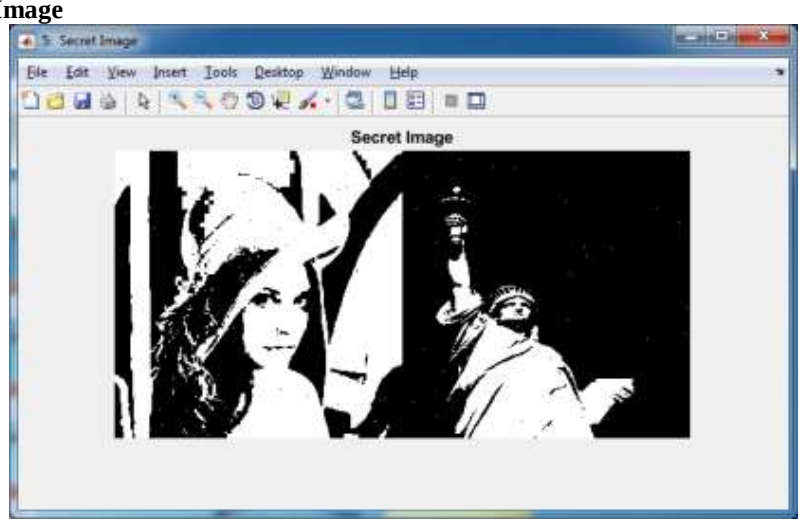

Figure 11: Concatenated Images

6. **Secret Image:** it contains a hidden text message in image as (email id Kamlesh123@gmail.com and password is KKR12345)

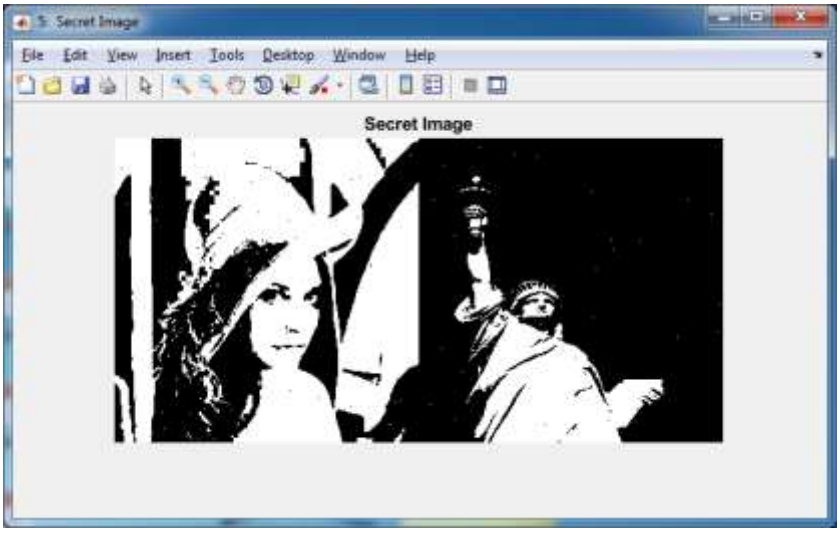

Figure 12: Secret Images

7. **Bank Share**

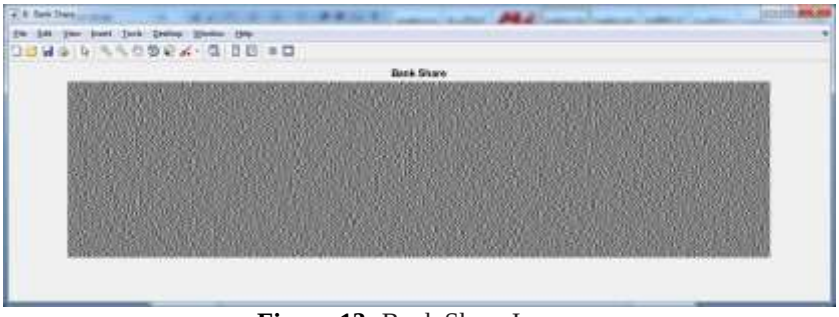

Figure 13: Bank Share Image

8. **User Share**

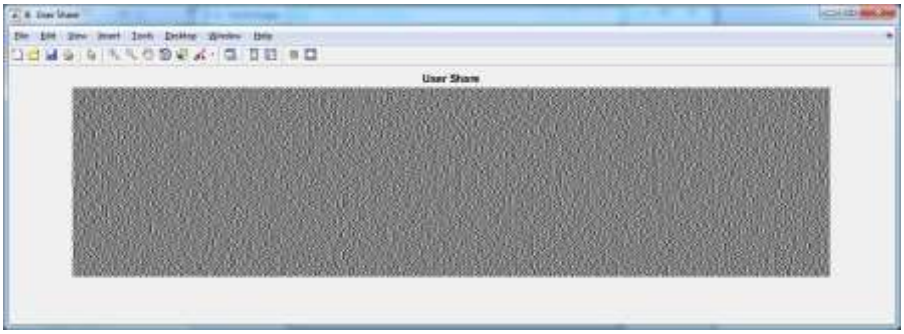

Figure 14: User Share Image

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

Figure 15: Share 1 Images

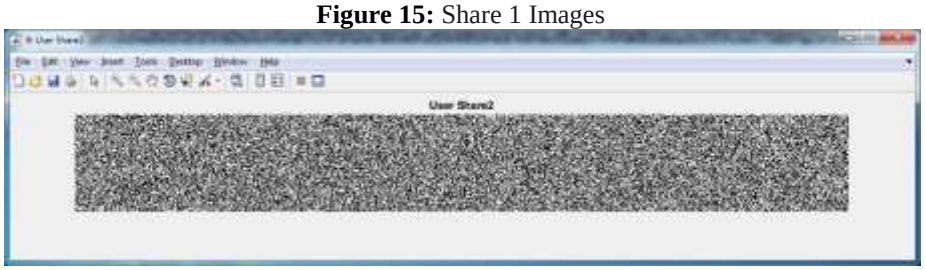

Figure 16: Share 2 Images

9. Reconstructed Image

Finally we get reconstructed image and the text message

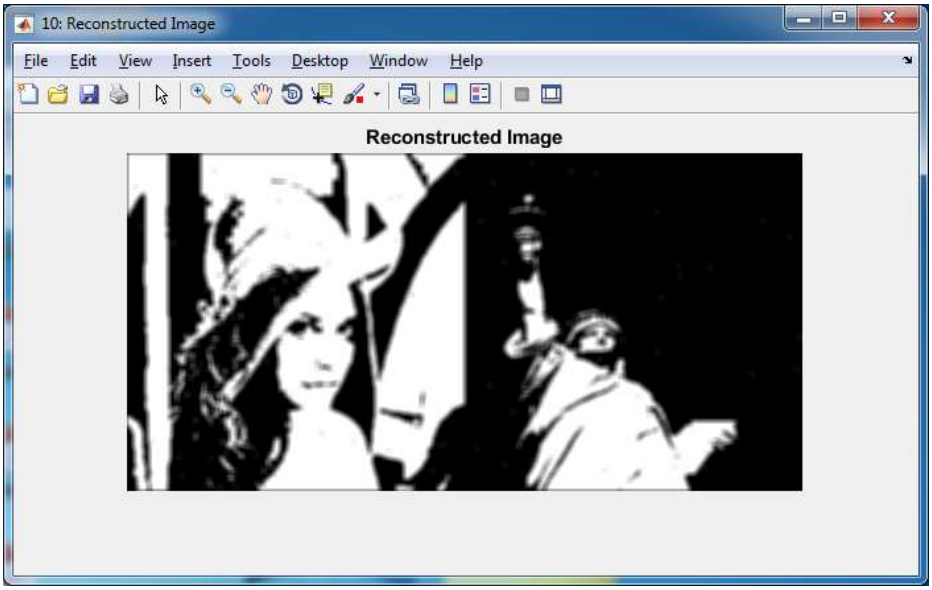

Figure 17: Reconstructed Image

The entire text message has been deciphered, and it has been shown as follows (the email address is Kamlesh123@gmail.com and password is KKR12345). It is clear that the inserted text message and the text message after it has been decoded are identical. Users will be able to log in and begin their online banking with this feature.

Figure 8 and Figure 9 show the original images and grey images that were used as input, respectively, and Figure 10 shows the preprocessed binary images that were produced from the grey images shown in Figure 9. The concatenated image may be seen in Figure 11, and the secret image, which can be seen in Figure 12, can be derived from Figure 10. After that, the user shares are Figure 15 and 16, which are segregated from the secret image Figure 14. The image depicted in figure 13 is a bank share. A reconstructed hidden image, such as the one shown in Figure 16, can be obtained by utilizing the shares illustrated in Figures 12, 13, and 14.

VII. CONCLUSION

In this method, the original image is secured by being divided into several distinct shares. This study primarily focuses on issues related to identity theft and the security of consumers' personal information that arise during joint account activities. In this work, a technique based on (2, 2)-VCS-XOR with Hide text in Image was suggested as a way to guarantee the security of banking transactions in joint account operations (Steganography). The results of the studies show that the reconstructed hidden image is identical in terms of size and quality to the original hidden image.

.

s

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] Sayali Vaidya, Shreya Zarkar , Prof. Achal N. Bharambe, Arifa Tadvi,Tanashree Chavan -- Anti-Phishing Structure Based On Visual Cryptography and RSA Algorithm International Journal of Engineering Trends and Technology (IJETT, 2015)
[17] Aparnaa. K. S., Sathyasundaram. M., Santhi. P. -- Securing Internet Banking with a Two – Shares Visual Cryptography Secret Image International Journal of Engineering Research & Technology (IJERT 2016)
[18] B.Srikanth, G.Padmaja -- Secured Bank Authentication using Image Processing and Visual Cryptography International Journal of Computer Science and Information technology (IJCSIT 2014)
[19] Naveen Kumar Kolli -- Implementation of secure payment transaction using AES encryption with extended visual cryptography (tamucc.edu 2017)
[20] Sarita swami, Reshma gulwani -- Secure E-PAY Using Steganogrphy and Visual Cryptography WRFER International Conference, 2017
[21] Dr.S.Makbul Hussain G. Mahaboob Basha -- Online Payment System using Steganography and Visual Cryptography International Journal & Magazine of Engineering, Technology, Management and Research (www.ijmetmr.com, 2017)
[22] Ms. Shital B Patel & Dr. Vinod L Desai -- Cheating Prevention in E-payment System using Visual Cryptography International Journal of Research and Analytical Reviews (ijrar.com, 2018)
[23] John Blesswin A, Christhu Raj, Rajeev Sukumaran & Selva Mary G -- Enhanced semantic visual secret sharing scheme for the secure image communication (link.springer.com, 2019)
[24] Sejal krishna Gajbhiye, Pooja Gedam, Lavanya Gannamani, Mrunal Deshmukh Mobile Banking App Using Visual Cryptograpy And Steganography International Journal of Scientific Development and Research (IJSDR) (www.ijsdr.org, 2020)