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

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— **Image cryptography is a new subject of study that is gaining popularity. For cryptography, a number of different techniques have been developed over time. Many different encryption algorithms have been employed to conceal visual information (images, text, and so on) within images. Visual cryptography is the name given to the concept that the primary notion of encryption is the potential of decryption by the human vision provided the correct key image is utilized.**
Although banks are committed to offering secure core banking services to their consumers, security has emerged as the most crucial factor in today's banking transaction system. Only those users who have been given permission to do so can participate in the transaction, which depends on the users' legitimacy. Banks use biometric, password, and OTP-based authentication systems for this reason, but the database of the banking system is no longer secure owing to avoidable criminal activities like phishing attacks and identity theft. Intelligent hackers can retrieve biometric information about consumers from the bank's database and utilise it later to make fraudulent transactions. To prevent all of these terrible occurrences, the RSA algorithm is utilized coupled with visual cryptography and steganographic approaches. A cryptographic method called visual cryptography enables information to be encrypted in a way that when it is decoded, the information appears as a visual image. In this study, we offer a financial transaction security technique based on visual cryptography, steganography, and image processing.

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

I. INTRODUCTION

The transmission of digital information and data via the Internet is currently taking place at a rate that is significantly quicker than at any point in the history of the network. In recent years, there has been a surge in the popularity of digital media due to the broad availability of international computer networks for the transmission of digital information and data, as well as the high efficiency of these networks. This has led to a broad variety of applications in fields such as education, entertainment, the media, and the military, amongst other areas of application. Digital images, video, and audio have been revolutionised in terms of the ways in which they may be obtained, stored, transported, and manipulated. As a result of advances in technology, personal computers and facilities for establishing computer networks have become both more accessible and more affordably priced. The field of digital multimedia has reaped various benefits as a consequence of the utilisation of innovative methods for the storage, access, and distribution of data. These benefits are essentially the result of attributes such as distortion-free transmission, compact storage, and simplicity of editing [1].
As our reliance on computers at every level of our lives continues to grow, the amount of personally identifiable and sensitive information that is being saved and transmitted on a daily basis through the use of computer systems and networks also continues to grow. This transformation, on the other hand, has brought with it new hazards and criminal activity using computers. According to the growth in the frequency of computer attacks and break-ins, this revolution has brought with it new perils. If vital information is duplicated, then intruders will have a better chance of gaining access to the information they need to get through the system. On the other hand, due to the fact that there is only one copy of this information, in the event that it is lost, there will be no way to retrieve it from the version that was stored previously. Because of this, it is absolutely necessary that information be managed in a reliable and trustworthy manner at all times. In circumstances like these, the exchange of confidential information is quite crucial.
The potential for the greatest shift in the way we live is represented by the advent of digital technology. The problem of ensuring the safety of one's digital assets has taken on a more pressing role since the dawn of the digital age. When information is transmitted from one node to another through a network connection, the existence of potential security flaws becomes immediately apparent. The number of potential dangers is growing at an alarming rate, which makes the deployment of stringent security measures absolutely necessary. The use of cryptography is among the most essential strategies for ensuring the confidentiality of sensitive information. Encoding and decoding a secret message, respectively, both entail a large investment of time and resources due to the fact that traditional encryption methods rely on enormous quantities of processing power and complicated algorithms.
The financial industry is one that frequently makes use of authentication methods that are based on biometric data. In order to authenticate a subject or verify their claimed identity, a biometrics-based authentication system first obtains raw biometric data from the subject (such as an image of their face or fingerprints, for example), then extracts a feature set from the raw data, and finally compares the feature set to a blueprint that is stored in the database. This process is known as "comparing the feature set." Authentication methods that are based on biometric data are becoming more and more popularity. Any institution's or organization's level of safety and protection is directly proportional to the quality of the underlying design technology middleware and, to an even larger extent, the design of the database. Each and every transaction, irrespective of the amount of space or time it covers, has some sort of impact on the database. As a direct consequence of this, hackers make persistent

attempts to breach the database's security. When it comes to the provision of web-based core services, the authentication of the user is one of the most important concerns for the financial system. In order to accomplish this goal, a number of different authentication methods, such as those based on passwords, smart cards, and biometric information, are put into use. Because all of these techniques are necessary for the upkeep of databases, it leaves them open to the risk of being hacked. There is the potential for a violation of privacy because the database contains personal information that could be considered sensitive. 1
Visual Cryptography [1-3], which takes a secret image as input (i.e. printed or handwritten), encrypts the input image into a set of other images called shares in such a way that the original secret is revealed if the shares are printed on transparencies and superimposed or staked over one another in such a way that the original secret is revealed if the shares are printed on transparencies and superimposed or staked over one another in such a way that the original secret is revealed. A binary image is used as the input for the most fundamental form of visual cryptography, which is also known as visual secret sharing. This form of visual cryptography works with each and every pixel in the image separately and independently.
The hidden picture is encoded by dividing each pixel into n different variations, all of which need to be printed on transparencies and then superimposed on the original secret pixel in order to view the hidden picture. It is imperative that this process be adhered to for the entirety of the hidden image. Now that you have n copies of the original secret image, you can unveil it by printing the copies on transparent paper and layering them one on top of the other. In order to guarantee the authenticity of and protect the confidentiality of the data that is kept in a banking institution's database, a solution has been developed that is based on XOR operation-based visual cryptography and makes use of image processing techniques.
At this point in time, a rising trend that can be observed is online banking. As the use of online banking becomes more widespread, the number of attempts to hack into online accounts also rises. Phishing and other forms of online fraud like identity theft are the primary sources of concern for both customers and merchants. Phishing is a form of social engineering that is frequently utilised in order to obtain user data, including login credentials and credit card numbers. It takes place when an attacker poses as a reliable party in order to trick a victim into opening an email, instant message, or text message that the attacker has sent. These phishing assaults prompted a significant number of reports to be filed. It has come to everyone's attention that the quantity and sophistication of these kinds of attacks are both on the rise, along with the number of people shopping online. We need to transfer over to a protection strategy that is even more dependable to ensure that safe networking of transactions can take place so that we can give increased safety against the leaking of confidential information. Clients of online banks have always been the preferred targets of people who engage in phishing attacks, as the account information of these customers can earn them more money in a matter of seconds.
Aside from that, there have been instances involving joint account holders wherein one of the account holders was able to carry out illegal activities by conducting online transactions. This was the situation in some of these instances. In this study, we suggest a new approach for conducting electronic transactions that offers increased safety by making use of cryptographic techniques such as steganography, visual cryptography, and other similar methods. The authentication details of the customer are concealed by visual cryptography, which works by first generating two shares for the joint account holders and then two shares for the bank respectively. The share of the customer is then broken down into two shares, one of which is given to each joint account holder. In order to protect the transmission of the customer's share to the bank, steganography is utilised to combine the customer's share with a single password. Steganography provides this added layer of security.

II. Literature Review

When you conduct a literature review, you are analyzing the information that has already been gathered and coming up with a mix of fresh knowledge and information that has not been gathered before. This section provides a concise explanation of the various research papers that are included in the research papers themselves, in addition to the occurrence of summaries and synthesis of research papers that are included in the research papers.
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.

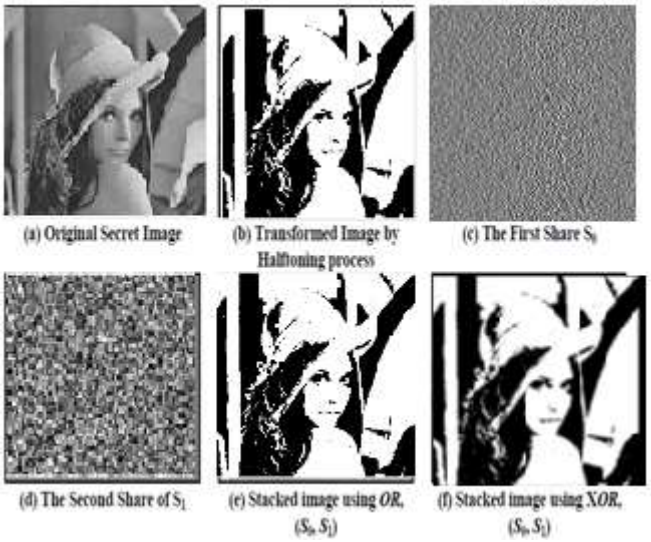

Figure 1: Process of XORing operation on VCS

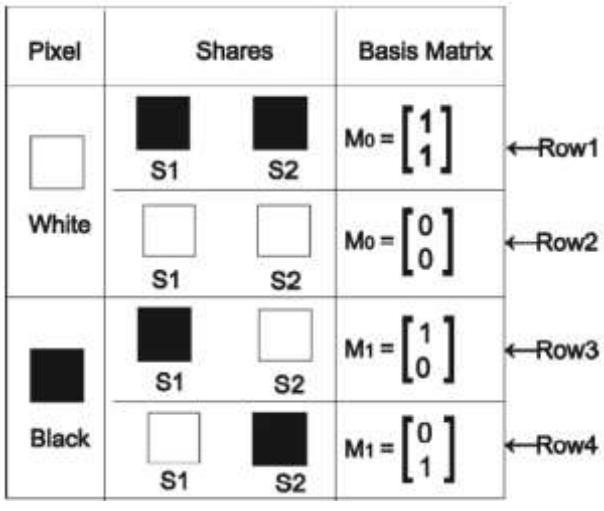

Figure 2: (2, 2)-VCS Scheme

The only thing that differentiates the two models is the contrast condition; other than that, the security criteria for both models are exactly the same. The half toning technique, which was initially presented by Naor and Shamir [1], has been extended in the 2-out-of-2 secret sharing scheme to include the 2-out-of-2 secret sharing scheme. This extension was made possible by the 2-out-of-2 secret sharing scheme. The most fundamental form of visual encryption is expanded upon by including a wider variety of image permutations in the process.

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.

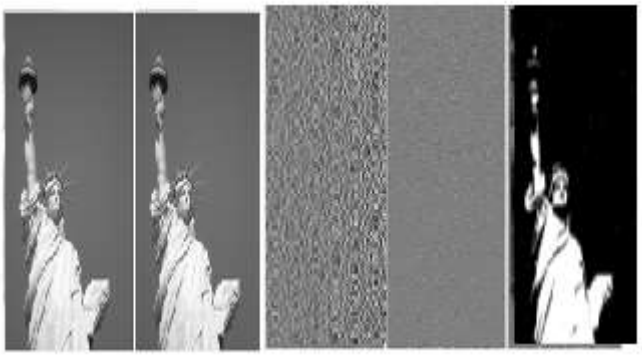

Figure 3: Original image, Halftone, Share-1, Share-2 and Decrypted image

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. VISUAL CRYPTOGRAPHY, AUTHENTICATION AND SHARING

It is now abundantly evident, as a result of the significant amount of progress that has been made in the discussion on venture capital, that the safeguarding of the secret image has a strong relationship with the dependability of venture capital shares. In order to successfully cheat in VC schemes, decryption and analysis of VC shares are requirements. It is feasible that the act of cheating could result in victims being harmed as a result of a fraudulent image being validated and approved by a person. A significant number of researchers have investigated the viability of cheating with VCS and have also provided strategies for securing it against such attacks.

There is a theory that authentication methods, which centre on the exchange of identifiers between two parties, can be utilized to assist in preventing any kind of cheating from taking place. This theory is now under investigation. Two distinct strategies for detecting and preventing cheating have been presented by a number of researchers, among them Tzeng et al. [9]. In the first one, the verification process between the participants is carried out with the assistance of an online trust authority, however in the second one, it is not. A modification to the VC scheme is required for this type of adjustment. This adjustment causes a verification indication to show whenever two shares are stacked on top of each other. The authentication process is considered to have been unsuccessful if the predefined symbols for the stacked VC shares do not display on the stacked VC shares. However, in order to employ this approach, it is required to include additional pixels in the secret.

Another strategy for avoiding dishonesty in academic settings is detailed in Horng and colleagues' [60] article. If the hacker is able to make an accurate observation of the precise distribution of black and white pixels in each of the shares held by honest players, then they will be able to successfully attack and cheat the scheme. It is possible to adopt a mechanism that prevents the attacker from gaining this distribution in order to put a halt to cheating. This can be done. In addition to providing ways for cheating, Hu et al. [14] have additionally provided a solution to the issue. The Tzeng approach additionally incorporated alterations to the Yang system and, as a last step, a brand new cheating prevention strategy with the objective of lowering the total number of additional pixels.

Previous research has attempted a number of different things to trick immune VCS [15], with varying degrees of success. In visual secret sharing systems, Yang et al. developed a method of dividing the secret into two barcodes, which they referred to as the "two barcode approach" [15]. This method was patented by the researchers. Barcodes are a typical kind of cypher, and under certain circumstances, the braille character may be utilized in conjunction with it. Because of the way the pixels are placed in the graphic pattern structure of a barcode, it is difficult for human eyes to differentiate between the black and white pixels that make up a barcode. Traditionally, the information is encoded in one-dimensional barcodes by employing lines that are parallel to one another as the encoding method. Utilizing these symbols in conjunction with the VC blind authentication method is not only possible but also highly recommended.

In order to evaluate the efficacy of a variety of well-known cheating activities and Cheating-prevention Visual Secret-sharing Schemes, the authors Chen et al. and Tsai &Horng investigated and analysed a number of these topics (CPVSS). According to the findings of their research, cheated actions were classified into one of three categories: meaningful cheating, non-meaningful cheating, or meaningful deterministic cheating (see Figure 1). An study of the research challenges in CPVSS is also given, along with a suggestion for a novel cheating prevention system that is superior to earlier schemes in terms of having less stringent security criteria. Both of these are presented in the report.

In order for the process of producing shares all throughout the encoding process to be effective, it should not only be a strong procedure, but it should also be devoid of any kind of trickery. Any time the system generates an artefact of a hidden image in any of the produced shares, it gives up its information to the relevant participant in every one of these different kinds of scenarios. As a consequence of this, the development of secure shares, in conjunction with strategies for the prevention of cheating, will be an endeavour to establish the best possible system for safe VCS.

V. APPLICATIONS OF VISUAL CRYPTOGRAPHY

Visual cryptography has many uses apart from the most obvious one, which is the concealment of information. Some of these uses include access control (like the opening of a bank vault), threshold signatures (like the security of a wallet through multiple devices like bit coins), copyright protection, watermarking, visual authentication (like the validation of tickets), and human identification (among other things). The banking industry, satellite imaging, and commercial applications for protecting biometric data collected on people are just some of the many fields that can make use of visual cryptography's vast variety of applications.

The technique of visual cryptography can be utilised in a manner that is very simple to understand. It is surprising, however, that in the twenty years that have passed since its conception by Naor and Shamir, there have been made only a few ideas for applying it to real-world scenarios. When Naor and Pinkas [6] presented a method for using visual cryptography to protect online transactions against manipulation, Chaum et al. [7] suggested that it could be applied to verifying that an election's outcome was correct. Chaum et al. [7] suggested that it could be applied for verifying that an election's outcome was correct.

The user is given a set of transparencies that are consecutively numbered by the transaction server in order to increase the level of safety associated with online monetary transactions. The server sends a visual message to the user's screen that is encoded using visual cryptography so that the information can be kept secure. This message contains the data associated with the transaction. The user is able to decipher the message hidden inside the image by placing a transparency bearing a particular number on top of the image that has been encoded. screened individual can decipher the message hidden within the picture.

If the server does not receive the right TAN, then it will not proceed with the transaction. If it does receive the correct TAN, then it will. With this approach, the level of protection afforded to financial dealings in the natural world can be improved. In

particular, the usage of the Moiré pattern and watermarking are two applications that are popular among VC users. Moirés patterns are produced when a layer that is to be revealed is stacked on top of an image that consists of forms that are repeated on a regular basis, which results in the formation of a periodic pattern. The Moiré pattern was investigated by researchers, who attempted to implement it into the shares of virtual currencies. The imbedded image may be seen when the shares are separated, and the initial secret can be revealed when the shares are superimposed one on top of the other.

The use of watermarking is yet another use for VC that is frequently put into practise. The process of watermarking is an important tool for hiding and embedding sensitive information in digital files. The implementation of VC in watermarking relies on a basis matrix, just like regular VC does, and the final recovered secret can be noticed through the use of a contrast between white and black colours, just like in traditional VC.

In a manner not dissimilar to this, Luo et al. [8] study the use of watermarks in the context of visual cryptography. Hwang [9] has developed a copyright system for digital photographs that is based on visual cryptography. This system prevents unlawful use of digital photos. It is a highly effective means of preventing cheating when VC-based watermarking is implemented in products; this is especially true in fields that already enjoy the benefits of utilising watermarking.

These recommendations did not result in applications that were utilised for significant reasons as a consequence of impediments such as adjustability, size, and the costs of specialist equipment. However, in the future, the widespread use of visual cryptography in practical applications may be the result of further refinement of the ideas offered in a variety of different methods, as well as the introduction of new ideas. It is conceivable that venture capital could be introduced into the financial industry, such as the banking sector, provided that contemporary picture hatching procedures are utilised in combination with VC. Furthermore, it is essential to do an analysis of the use of shares in the secure printing industry. The scanning of a share into a computer system, followed by the digital superimposition of the linked share, is an alternate method that may be researched.

VI. MERITS OF PROPOSED SYSTEM

- Because there are two different tiers at which shares can be created, the proposed system offers many tiers of security.
- It is impossible to steal a certain number of assaults. There is no clear definition of the total number of attacks that are required to fully mimic someone. This is due to the fact that the shares are split among three different companies and are only disclosed to the customers. Even if the attacker manages to take one of the security photos, it will be of little value to him because images are shared among three different parties, and image steganography is employed during transmission to encrypt the image.
- Method with multiple stages that is based on heuristics The 'Visual cryptography' technique is used to the security image that is encoded by the account number within an image using the 'Steganography' method. This increases the heuristics that are used to verify whether or not the website in question is a phishing site.
- The joint account holders have complete authority over all of the account's internet dealings.

VII. CONCLUSION

The use of critical tools like visual cryptography is essential in order to protect the privacy of images that contain sensitive information. VC, a subfield of secret sharing, has garnered a lot of attention as of late because to the security technique it employs, which takes into consideration both image processing and cryptography factors. The uses of virtual reality appear to be expanding and becoming more applicable in tandem with the development of virtual reality in the fields of dealing with a variety of different forms of secret images. In the context of a joint account transaction, the primary focus of this study is to solve difficulties associated with identity theft and the protection of client data. The use of visual cryptography helps to protect the confidentiality of financial transactions. A method for sharing confidential information is provided by visual cryptography, steganography, and the RSA algorithm. The original image is kept safe using this procedure, which involves decomposing it into n different schemes. In this article, a proposal was made for improved security measures to be offered for phishing attempts, identity theft, and the data of consumers transacting via joint accounts. This study offered a better approach to protect banking transactions using steganography and visual cryptography in addition to the RSA algorithm. The proposed method was intended for use in the context of joint account operations.

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] C.M. Hu and W.G. Tzeng, ―Cheating Prevention in Visual Cryptography,‖ IEEE Transaction on Image Processing, vol. 16, no. 1, pp. 36–45, Jan. 2007.
[16] G. Horng, T. Chen, and D. Tsai, ―Cheating in Visual Cryptography,‖ Design, Codes and Cryptography, vol. 38, no. 2, pp. 219–236, Feb. 2006.
[17] J. Weir and W. Yan, ―Authenticating Visual Cryptography Shares Using 2D Barcodes,‖, In: Shi Y.Q., Kim HJ., Perez-Gonzalez F. (eds) Digital Forensics and Watermarking. IWDW 2011. Lecture Notes in Computer Science, vol 7128, pp. 196–210, Springer, Berlin, Heidelberg, 2012.
[18] Sarita swami, Reshma gulwani -- Secure E-PAY Using Steganogrphy and Visual Cryptography WRFER International Conference, 2017
[19] 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)
[20] 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)
[21] 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)
[22] 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)