IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Review of Visual Cryptography and Steganography Implementation

Ms. Y. Tresa [1]
Assistant Professor
Department of Computer Science
Sri Ramakrishna College of Arts and Science for Women
Coimbatore, Tamilnadu, India – 641044

Dr. D. Hema [2]
Assistant Professor
Department of Computer Science
Sri Ramakrishna College of Arts and Science for Women
Coimbatore, Tamilnadu, India – 641044

Abstract: Online banking is a collection of services offered by a number of centralised bank offices. Customers of the bank can use the internet to access their funds from any of the participating branches or offices. The legitimacy of the user is the underlying problem with online banking. It is difficult to imagine that data on the web is secure given the inescapable hacking of online databases. We are suggesting a solution that is a combination of data concealing and visual cryptography to address this verification issue. This paper offers a review of visual cryptography and steganography techniques while also introducing a novel method for handling a user's transaction key in which the key is first embedded in a picture and then split into two parts. When two shares are created, one of them is stored in the bank's database and the other is either maintained by the client or sent to a photo server. In most of his interactions, the client must introduce the offer. To obtain the initial Transaction key, stack this offer with the primary offer. The correlation technique is used to decide whether to accept or reject the yield and to verify the client.

Keywords : Information Security, Steganography, Visual Cryptography, Online Shopping

I. Introduction

These days, the majority of applications are just as secure as their foundation. Their location is a problematic issue because middleware configuration and innovation have continually improved. As a result, it might be challenging to determine whether a PC connected to the internet can be trusted and secure. The question is how to handle applications that need a high level of security, including centre money management and web account management. There is a chance of encountering fabricated mark for exchange in a central saving money framework. Furthermore, the client's secret key could be compromised and used inappropriately in the online financial system. In this approach, security in these applications continues to be tested. Here, we recommend an evaluation of a system to protect customer data, prevent potential mark fraud, and prevent secret key hacking.

Web banking has long been popular among young, Internet-savvy people, and as Internet use spreads worldwide and more people discover its many benefits, its popularity is only expected to grow. Whatever the case, it can have drawbacks of its own.

There is a chance of encountering fake mark for exchange in a centre controlling an account framework. It is possible to hack and misuse a client's secret key when maintaining an account on the internet. Online transactions have been increasingly common in recent years, and several assaults can be seen as the cause of this.

Phishing is acknowledged as a significant security issue in various kinds of diverse attacks. Phishing scams are also becoming a problem for online shoppers and e-commerce customers. The issue is how to handle applications that demand an unusually high level of security. Phishing is a type of online data fraud that aims to steal sensitive information from users, such as their Mastercard information and online banking passwords. Phishing is described as "a criminal act using social engineering techniques" as one definition. By pretending to be a trustworthy person or organisation in an electronic contact, phishers try to fraudulently obtain sensitive data, such as passwords and credit card numbers. Here, we'll use a few techniques to protect user data and prevent any fake attempts at password stealing. Visual cryptography and photo handling as a steganography are used.

Steganography is the art and science of creating hidden messages in such a way that no one other than the intended recipient is aware of their existence. A transporter obscures the unique message to the point that the progressions that have occurred in the bearer are undetectable. Computerised images can be used as a transporter in steganography to hide photographs. The concealed picture is created by joining a mystery image with a bearer image; the shrouded image is difficult to decipher without recovery; and the majority of the steganography process is made up of three or four consecutive pixels surrounding an objective pixel. The proposed approach, however, can make use of at least eight contiguous neighbours in order to increase impalpability value and divide it into shares. The total number of shares that will be made will depend on the plan that the bank chooses. When two shares are created, one is stored in the bank's database and the other is retained by the client. Throughout the majority of his exchange, the client must display the share. To obtain the first image, this share is stacked to the first share. Then, in order to confirm the client, interpretation approach is used to get the covert hidden word on whether to accept or reject the yield. A mystery picture is encoded using the visual cryptography (VC) approach so that it can be decoded by stacking a sufficient number of shares.

It makes use of the notion of picture preparation and improved visual cryptography. The process of treating an information image and obtaining the output as either an improved version of the same picture or attributes of the info picture is known as picture preparation. A mystery key is encoded using the Visual Cryptography (VC) method so that it can be decoded by stacking a sufficient number of shares.

A simple yet completely safe method, known as the Visual Cryptography Scheme (VCS), was introduced by Naor and Shamir. It allows secret sharing without requiring any cryptographic calculations. In essence, the Visual Cryptography Scheme is an encryption approach that uses combinatorial techniques to encode materials that are secretly created. The idea is to turn the composed content into a picture and then encode that picture into n shadow pictures. Simply choosing a subset of these n images, turning them into transparencies, and stacking them on top of one another is all that is needed to read them. The accompanying configuration provides the simplest straightforward Visual Cryptography Scheme. A mystery image is made up of a collection of pixels with sharp contrast in which each pixel is used at random. In order to encode the mystery image, we divide the original image into modified versions (referred to as shares), so that each share now consists of n high contrast sub-pixels for each pixel. A subset S of those n shares is chosen and replicated on partitioned transparency in order to decipher the image. If S is a valid subset, then stacking each of these transparency will enable visual recovery of the enigma.

II. RELATED WORK

A) Cryptography

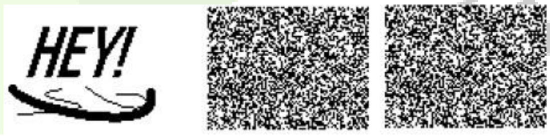
The words "cryptography" and "mystery composing" are both derived from two Greek words. By modifying and substituting the initial content and arranging it such that it appears incoherent to others, cryptography is a method for securing the initial content. A successful method for securing data transmission over system communication channels is cryptography. The science of cryptanalysis and cryptography is known as cryptology. The technique of conveying communications discretely and securely to the target is known as cryptography. The process of converting implanted messages into original writings is known as cryptanalysis. Generally speaking, cryptography involves manipulating information through a secret code and transmitting it from source to target. The cryptosystems use a plaintext as input and generate a figure using encryption calculations with a mystery key as input.

B) Visual Cryptography

Visual cryptography is a cryptographic method that enables visual information (images, text, etc.) to be encrypted in a way that the human visual system can execute the decryption without the assistance of computers. A human may detect images as a part of multimedia.Techniques for Visual Cryptography

The most striking feature of visual cryptography is its ability to recover a mystery image without any calculations. It takes advantage of the human visual system to decipher the secret message from some covering offers, eliminating the discomfort of the difficult calculations needed for cryptography. In [19] The author described a straightforward yet completely safe method—referred to as a visual cryptographic plan—that allows secret sharing without requiring any cryptography calculations. the problem of securely scrambling constructed material (printed text, handwritten notes, photos, etc.) in a way that can be recognised only by the human visual system. The idea is to turn the assembled material into an image and then encode that image into n shadow images. Choosing a subset of these n images, turning them into transparencies, and stacking them on top of one another are all that is needed to read them.

- Level 1 concealing utilizing Visual Cryptography



Secret Data share 1 share 2

- Super Imposing Share1 and Share2 to Form theOriginal Secret Data

The secret Information

The first motivation was to safeguard cryptographic keys from bad luck. Cryptography is one of the most well-known methods for ensuring the information. transmitting and receiving scrambled communications that can only be decoded by the sender or the beneficiary is its speciality. Nobody other than the intended beneficiary can decode and decrypt the messages because to the skilled decoding and encryption techniques used as part of this method.

In order to execute a decoding operation using the human visual framework, the Visual Cryptography Scheme considers the encryption of visual data. One of the access structure plans that is included will help us do this.

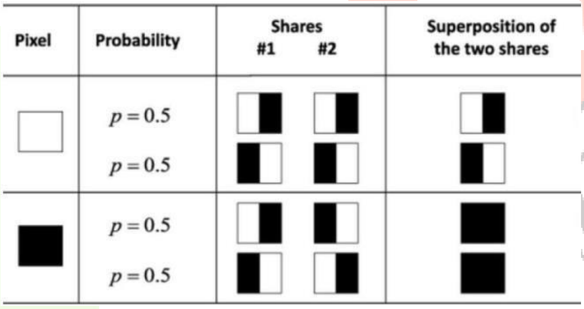
1.(2,2) VCS Threshold conspiracy This least-complex limit plot encodes a secret message into two separate shares that, when put together, reveal the secret image. To create this kind of get to structure, no other information is needed.

2. (2, n) VCS Threshold conspiracy The purpose of this strategy is to reveal the mystery picture when any two (or more) of the shares are overlapped. It divides the mystery image into n shares. The number of members, n, will irritate the client.

3. (N, n) VCS Threshold conspiracy The purpose of this approach is to encrypt the mystery image to n shares so that it may be decoded after all n shares are aggregated. The number of members, n, will irritate the client.

4. (k, n) Threshold VCS plot The mystery picture is so thoroughly encoded into the n shares in this scheme that it will be revealed when any collection of, say, k shares is superimposed. The client will be asked for n, the number of members, and k, the threshold.

5. On account of (2, 2) VCS, In the first image, each pixel P is divided into two smaller pixels called offers. The percentages of a white pixel and a dark pixel are shown in Figure 1. Be aware that the allocation of shares for a white and a dark pixel is chosen at random (each pixel has two choices). Due to the fact that different pixels in the mystery picture will be scrambled using autonomous arbitrary decisions, neither of the shares provides any information regarding the initial pixel. The estimation of the first pixel P can be resolved at the location where the two shares are superimposed. We obtain two dark subpixels in the unlikely event that P is a dark pixel, and one black subpixel and one white subpixel in the unlikely event that P is a white pixel.



Pixel	Probability	Shares #1	Shares #2	Superposition of the two shares
□	$p = 0.5$	◨	◨	◨
	$p = 0.5$	◧	◧	◧
■	$p = 0.5$	◨	◧	■
	$p = 0.5$	◧	◨	■

Fig 1. Illustration of 2-out-of-2 VCS scheme with 2subpixels construction [19].

- Adjustment Technique

The proposed method took two consecutive pixels as the source image's single input, hence there must be four input situations. These areas follows:

(i) Black and Black, (ii) Black and White, (iii) White and Black, (iv) White and White

To develop a (2, n) visual cryptographic scheme two things are considered as major point of referencesthese are:

(i) Each block in each share should have the same hamming weight.

(ii) A black block will have a heavier hamming weight than the other blocks in the stacked shares.

Let N is the number of participants (i.e no. of accountholders). m=integer part of (n/2), where n= numberof total shares. The bank authority has to select the value of n, such that the relation nCm _ min{(N+1)} (where C represents the combination operation) holds. Hamming weight of each block of each share (H) = Integer part of (nCm)/2; Now Let us consider the fourpossible cases of input pixels:

(i) Black and Black: In this scenario, the output block's placement of the black pixels will differ from other blocks. This ensures that after stacking the shares,Hamming weight of the stacked black blocks willbecome greater than the other blocks.

(ii) Black and White: The initial location of the output block is where all the black pixels will be stored together.

(iii) White and Black: where all of the black pixels from the output block's previous position will be maintained together.

(iv) White and White: In the output block, all black pixels will be retained together.

The final pixel will be left in its current state in the shares if the input image's pixel count is odd. We treat the white pixels of black and white images as transparent since the output media of visual cryptography are transparencies. Typically, a secret image's pixels are broken down into two 22 blocks using black-and-white visual cryptography. When a pixel is white, the algorithm selects one of the two possibilities for white pixels in Fig. 1 in accordance with its principles. When a pixel is black, it selects one of the other two possibilities to create the block's content in the two transparencies. Then, white and black is black, white and white is white, and black and black is black are the properties of two stacked pixels. As a result, when stacking two transparencies, the blocks that correspond to dark pixels in the secret images are fully black, and the blocks that correspond to white pixels are split 50/50 in colour, or half black, half white.

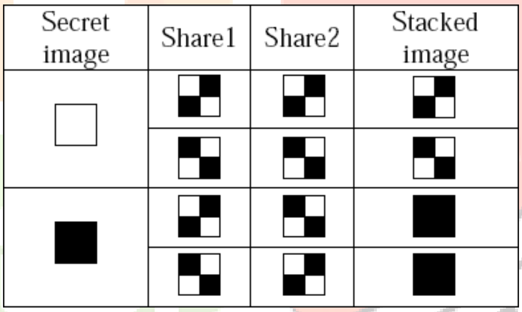


Fig 2. Sharing and Stacking Scheme of Black andWhite Pixels [19]Comparison of various visual cryptography schemes:

This method has been used in numerous research publications; it starts with a binary image and progresses to a grayscale image before being applied to colour images. Although the quality of the reconstructed image got better with each new research publication. Table 4.1 below provides details on various visual cryptography systems. [7] suggests one of the most promising methods for colour photos; the suggested method is dividing an image into numerous portions.Steganography

Steganography is the practise of concealing one message, record, image, or video inside another message, record, image, or video. The Greek terms steganos (v), which means "secured, disguised, or ensured," and graphein (), which means "composing," are combined to form the word steganography.

In 1499, Johannes Trithemius used the term for the first time in his Steganographia, a book about magic disguised as a dissertation on cryptography and steganography. The hidden messages typically appear to be (or are parts of) something else, such as images, articles, shopping lists, or other cover content. For example, the secret message could be written in barely discernible ink between the obvious lines in a private letter. While key-subordinate steganographic schemes adhere to Kerckhoffs' concept, a few steganographic executions that lack a unifying mystery are examples of security by obscurity.

The advantage of steganography over cryptography alone is that the intended secret message does not call attention to itself as a defence against scrutiny. No matter how impenetrable, clearly visible encoded messages arouse suspicion and may even be implicating in countries where encryption is prohibited. As a result, while steganography is concerned with concealing both the method and content of a message's transmission, cryptography focuses solely on protecting the message's content. Steganography involves hiding data in computer records. Electronic interchanges may include steganographic coding as part of a vehicle layer in computerised steganography, such as a record document, picture record, programme, or convention. Due to their enormous size, media documents are ideal for steganographic transmission. For instance, a sender might start with a neutral picture file and adjust the colour of every 100th pixel to correspond to a letter in the letter set, a change so subtle that someone who isn't looking for it probably won't see it.

C) Least Significant Bits Technique forSteganography[4]

Today, we often select one of three methods for portraying colours when converting an analogue image to digital format:

- 24-bit colour: Each pixel can contain up to 224 colours, which are represented as various shades of the three primary colours red (R), green (G), and blue (B), each of which has 8 bits (256 values).
- 8-bit colour: Each pixel can have one of 256 (28) different colours, selected from a palette or colour table.
- 8-bit grayscale allows for 256 (28) shades of grey per pixel.

In 24-bit or 8-bit pictures, LSB insertion affects the LSBs of each colour, or the LSBs of the 8-bit value.

Example:
The ASCII code for the letter 'A' is 65 (decimal), which corresponds to the binary value 1000001.
It will need three consecutive pixels for a 24-bitimage to store an 'A':
Let's say that the pixels before the insertion are:

10000000.10100100.10110101,
10110101.11110011.10110111,
11100111.10110011.00110011
Then their values after the insertion of an 'A' will be:

10000001.10100100.10110100,
10110100.11110010.10110110,
11100110.10110011.00110011
(The values in bold are the ones that were modifiedby the transformation)
The same example for an 8-bit image would haveneeded 8 pixels:

10000000, 10100100, 10110101, 10110101, 11110011,
10110111, 11100111, 10110011
Then their values after the insertion of an 'A' wouldhave been:

10000001, 10100100, 10110100, 10110100, 11110010,
10110110, 11100110, 10110011

III. PROBLEM DEFINATION

A falsified signature for a transaction could appear in a core banking system. The customer's password in the online banking system may be stolen and used inappropriately. Therefore, security in these applications continues to be a challenge. Here, we offer a method for protecting client information, guarding against signature fraud and password hacking, among other potential threats.

IV. LITERATURE REVIEW

In [1], a new approach is suggested that makes use of content-based steganography and visual cryptography. This strategy minimises data sharing between online shoppers and shippers while enabling efficient store exchange from customers' records to vendors' records, protecting buyer data and preventing data abuse at the dealer side. The approach suggested is specifically for e-commerce, although it may easily be used to both online and offline account management.

In [3], a novel method is put out in an effort to understand all the aforementioned steganography problems. Instead of using substitutions, the suggested technique makes use of the notion of matches between the mystery information and cover image. Additionally, we use the concept of changed recurrence for every English character. The suggested method features better security, an unlimited payload limit, a key size that is only about 10 to 20 percent of the message estimation, and lossless operation.

A basic LSB substitution method for information concealment is put forth in [4]. The stego-picture's picture quality can be considerably improved with minimal additional computing effort by applying an optimal pixel alteration technique to the stego-picture obtained by the fundamental LSB substitution strategy. The mean-square error between the cover picture and the stego picture is calculated in the most negative circumstance. Trial results show that the stego-picture is superficially ambiguous from the initial cover- image.The obtained results also show a significant shift from previous work.

The sender in [5] is hiding the information that will be sent to the beneficiary as images. The image is a composite of the content obtained from the two methods of content steganography that have previously been deduced. The Vedic Numeric Method and Reflection Symmetry are the two methods used.The sender divides the information into two portions and sends each segment separately to the two processes. This is known as sending the information in an apportioned shape. We are taking this action because if the entire content were given to a single procedure or Vedic technique, more memory would be used. Thus, after being prepared by the two processes, the content is combined to form a full content, which is then brought into focus by various techniques or calculations, such as LSB or network augmentation. The recipient receives a picture that has been converted from the original content in this way. The model suggested in [6] uses a neighbouring isotropic complexity measure and a concealing model to take the affectability and covering behaviour of the human visual framework into account.

We examine the inclusion of this watermark in shading images' blue channel and luminance images. We also evaluate the strength of the watermark based on how thick it is when installed. Our findings show that this strategy promotes the addition of a stronger watermark while preserving the aesthetic appeal of the first. Additionally, we demonstrate that the best identification execution does not typically result from the most extreme watermark thickness.

In [8] work, a method for producing pictures with Steganography and visual cryptography, then dividing them into shares, has been proposed. In this project, the client's message or content document is accepted as a contribution and used to create the image record. The image file may have the extensions.jpg or.png. The MD5 computation is used to compute the message process, which is attached to the message. Then, the message that was annexed is encoded using the AES algorithm. The RSA computation is used to scramble the secret keys used in the AES calculation. The attached scrambled message is added using the minimum huge piece calculation to the image. The encoded image is sent over the air. Before sending the photo document, the secret word must be disclosed. The watermarked image record is used as the information on the beneficiaries' side. The LSB computation is used to delete the message from the picture record. The procedure and the message parts of the deleted message are separated. The message's message process is calculated, then compared to the one that was really received. If they resemble one another, the message is considered to have been validated. This defence using modern technology. The Core Banking Application will benefit from this approach, and bank customers no longer have to worry about password hacking issues. Once this system is installed on a web server, every machine connected to the network can access it using a browser without needing to install any software.

V. PROPOSED SYSTEM

Our project proposes a technique of processing a customer's secret key, then dividing it into shares. When two shares are established, one is maintained by the customer and the other is stored in the bank's database.

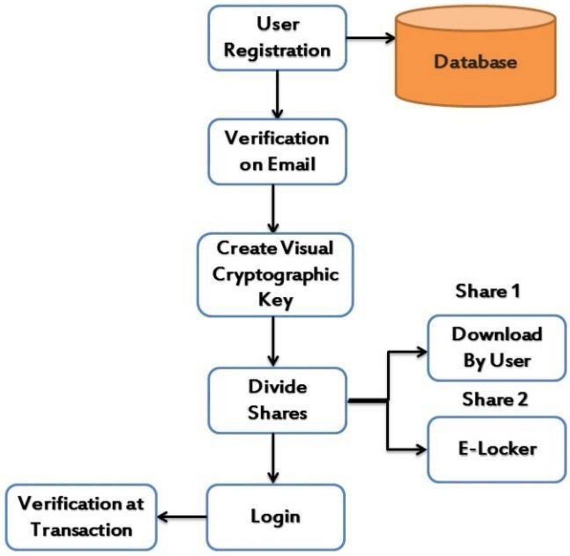


Fig 3. System Architecture

Each time the customer transacts, the share must be presented. The original secret key is given to this share together with the first share. The Correlation technique is used to decide whether to accept or reject the output and to verify the customer's identity.

VI. CONCLUSION

This method uses Colour Image Visual Cryptography to secure passwords, and it is currently technologically impossible to defeat this security. The Core Banking Application will benefit from this approach, and bank customers no longer have to worry about password hacking issues. Once this system is installed on a web server, every machine connected to the network can access it using a browser without needing to install any software.

REFERENCES

[1]. S. Roy, P. Venkateswaran, “Online Payment System using Steganography and Visual Cryptography”, IEEE Conference on Electrical,Electronics and Computer Science, vol. 6, no. 2,pp. 88-93, 2014

[2]. M. Suresh, B. Domathoti, N. Putta, “Online Secure E-Pay Fraud Detection in E-Commerce System Using Visual Cryptographic Methods”, International Journal of Innovative Research in Computer and Communication Engineering ,vol. 3, no. 8, pp. 7519-7525, August 2015.

[3]. Rahna E, V. Govindan, “A Novel Technique For Secure, Lossless Steganography With Unlimited Payload And Without Exchange Of Stegoimage”, International Journal of Advances in Engineering & Technology, vol. 6, no. 3, pp. 1263-1270, July 2013.

[4]. S. Chan, L. Cheng, “Hiding data in images by simple LSB substitution”, Pattern Recognition, pp. 469– 474, August 2004.

[5]. C. Shrivastava1, T. Verma, “A Survey on Various Techniques for Generating Image Steganography with Improved Efficiency”, International Journal of Advanced Research in Computer Engineering & Technology , vol. 4, no. 3, pp. 1005-1009, March 2015

[6]. M. Kutter, S. Winkler, “A Vision-Based Masking Model for Spread-Spectrum Image Watermarking”, In proceedings International Conference on Computing, Electronics andElectrical Technologies, pp. 313-336, 2004.

[7]. Jaya, Siddharth Malik, Abhinav Aggarwal, Anjali Sardana, “Novel Authentication System Using Visual Cryptography,” Proceedings of 2011 World Congress on Information andCommunication Technologies, pp. 1181-1186,Mumbai, India, 2011.

[8]. P. Vaman, C. Manjunath, Sandeep , “Integration of Steganography and Visual Cryptography for Authenticity”, International Journal of Emerging Technology and AdvancedEngineering, vol. 3, no. 6, pp. 80-84, June 2013

[9]. C. Hegde , Manu S , P. Shenoy , Venugopal K R , L M Patnaik, “Secure Authentication usingImage Processing and Visual Cryptography for Banking Applications”, In proceedings of 16th International Conference on Advanced Computing and Communications, pp. 65- 72,2013

[10]. A. Suklabaidya, G. Sahoo, “VisualCryptographic Applications”, InternationalJournal on Computer Science and Engineering, vol. 5, no. 06, pp 455-464, June 2013

[11]. R. C. Gonzalez and R. E. Woods," Digital Image Processing” Upper Saddle River, NJ: Prentice- Hall, 2006.

[12]. S.Premkumar and A.E.Narayanan, “New Visual Steganography Scheme for Secure BankingApplication”.

[13]. H. Wang and S. Wang, "Cyber warfare Steganography vs. Steganolysis," Commun. ACM, vol. 47, no. 10, pp. 76-82, 2004.

[14]. X. Zhang and S. Wang, "Steganography using multiple base notational system and human Vision sensitivity," IEEE Signal Processing Letters, vol. 12, pp. 67-70, Jan. 2005.

[15]. M. Shirali-Shahreza, "Steganography in MMS," in Multi topic Conference, 2007. INMIC 2007. IEEE International, 2007, pp. 1-4.

[16]. Aggelos Kiayias and Yona Raekow, “Efficient Steganography with Provable Security Guarantees”

[17]. T. Morkel, J.H.P. Eloff and M.S. Olivier, “An Overview of Image Steganography”

[18]. Chandramathi S, Ramesh Kumar R, Suresh R, and Harish S,”An overview of visual cryptography”

[19]. Moni Naor, Adi Shamir,” visual cryptography”

[20]. Jithesh K, 2dr. A V Senthil Kumar, “Multi- Layer Information Hiding -A Blend OfSteganography And Visual Cryptography,”

[21]. Young-Chang Hou, “Visual cryptography for color images,”

[22]. https://en.wikipedia.org/wiki/Online_banking# Attacks