© 2019 IJSRST | Volume 6 | Issue 2 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology
DOI : 10.32628/IJSRST196278

A Review on Implementation Visual Cryptography and Steganography

Pranay Kalamkar[1], Mrunali Gaikwad[1], Sumit Gore[1], Dhananjay Sonule[1], Prof. Vidya Bodhe[2]

[1]BE Scholar, Department of Information Technology, Abha Gaikwad Patil College Engineering, Mohagoan, Nagpur, Maharashtra, India

[2]Assistant Professor, Department of Information Technology, Abha Gaikwad Patil College Engineering, Mohagoan, Nagpur, Maharashtra, India

ABSTRACT

Online Banking is an arrangement of administrations gave by a group of organized bank offices. Bank clients may access their funds from any of the part branch or workplaces via internet. The real issue in Internet Banking is the authenticity of the user. Because of unavoidable hacking of the databases on the web, it is hard to believe on the security of the data on the web. To take care of this issue of verification, we are proposing a mechanism which is hybrid of data hiding and visual cryptography. This paper proposes a review on visual Cryptography and Steganography techniques and presenting a new approach for handling the transaction key of a user where the key will be embedded into an a image and later the image will be divided into two shares. At the point when two shares are made, one is put away in the Bank database and the other is kept by the client or sends to picture server. The client needs to introduce the offer amid the majority of his exchanges. This offer is stacked with the main offer to get the first Transaction key. The Correlation technique is utilized to take the choice on acknowledgment or dismissal of the yield and validate the client.

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

I. INTRODUCTION

Today, most applications are just as secure as their basic framework. Since the configuration and innovation of middleware has enhanced consistently, their location is a troublesome issue. Therefore, it is quite difficult to make certain whether a PC that is associated with the web can be viewed as dependable and secure or not. The inquiry is the way to handle applications that require an abnormal state of security, for example, center saving money and web managing an account. In a center saving money framework, there is a shot of experiencing manufactured mark for exchange. Furthermore, in the net saving money framework, the secret key of client might be hacked and abused. In this way security is still a test in these applications. Here, we propose review on a system to secure the client data and to keep the conceivable fraud of marks and secret key hacking.

Web Banking has been well known among youthful Internet-astute individuals for a long time, its notoriety is required to become quickly as Internet use becomes globally and individuals find the numerous focal points that it gives. Be that as it may, it might have its own disadvantages. In a center managing an account framework there is a shot of experiencing manufactured mark for exchange. In a net managing an account framework secret key of the client might be hacked and abused. Online exchanges are these days turn out to be extremely normal and there are different assaults exhibit behind this. In these sorts of different assaults, phishing is distinguished as a noteworthy security risk. Phishing tricks are likewise turning into an issue for internet saving money and e-business clients. The question is the way to handle applications that require an abnormal state of security. Phishing is a type of online data fraud that intends to take touchy data, for example, web based keeping money passwords and Mastercard data from clients. One meaning of phishing is given as "it is a criminal action utilizing social designing procedures. Phishers endeavor to falsely get touchy data, for example, passwords and charge card points of interest, by taking on the appearance of a reliable individual or business in an electronic correspondence". Here we will utilize a portion of the methods to secure the client data and to keep the conceivable phony of secret word hacking. The idea of picture handling a steganography and visual cryptography is utilized. Steganography is the workmanship and exploration of composing shrouded messages in a manner that nobody separated from planned beneficiary knows the presence of the message. Unique message is being covered up with a transporter to such an extent that the progressions so happened in the bearer are not detectable. In steganography computerized pictures can be utilized as a transporter to conceal pictures. Joining mystery picture with a bearer picture gives the concealed picture, the shrouded picture is hard to recognize without recovery, and the vast majority of the steganography procedure are either three or four contiguous pixels around an objective pixel. While the proposed system can use at above all else eight contiguous neighbors with the goal that impalpability esteem becomes greater and the partitioning it into a shares. Add up to number of shares to be made is relying upon the plan picked by the bank. At the point when two shares are made one is put away in the bank database and the other one is kept by the client. The client needs to exhibit the share amid the greater part of his exchange. This impart is stacked to the primary share to get the first picture. At that point interpreting technique is utilized to take the shrouded secret word on acknowledgment or dismissal of the yield and validate the client. The visual cryptography (VC) is a technique for encoding a mystery picture into shares with the end goal that stacking an adequate number of shares uncovers the mystery picture.

The idea of picture preparing and an enhanced visual cryptography is utilized. Picture preparing is a strategy of handling an information picture and to get the yield as either enhanced type of the same picture and/or qualities of the info picture. Visual Cryptography (VC) is the technique for encoding a mystery key into shares with the end goal that, stacking an adequate number of shares uncovers the mystery key.

Naor and Shamir presented a straightforward yet flawlessly secure way that permits mystery sharing with no cryptographic calculation, named as Visual Cryptography Scheme (VCS). Essentially, Visual Cryptography Scheme is an encryption strategy that utilizations combinatorial methods to encode mystery composed materials. The thought is to change over the composed material into a picture and encode this picture into n shadow pictures. The deciphering requires just selecting some subset of these n pictures, making transparencies of them, and stacking them on top of each other. The most straightforward Visual Cryptography Scheme is given by the accompanying setup. A mystery picture comprises of a gathering of highly contrasting pixels where every pixel is dealt with freely. To encode the mystery picture, we split the first picture into adjusted renditions (called as shares) with the end goal that every pixel in an offer now subdivides into n high contrast sub-pixels. To decipher the picture, a subset S of those n shares are picked and replicated on partitioned transparencies. On the off chance that S is a qualified subset, then stacking every one of these transparencies will permit visual recuperation of the mystery.

II. RELATED WORK

A) Cryptography

The word cryptography is taken from two Greek words which signify "mystery composing". Cryptography is the way toward scrambling the first content by adjusting and substituting the first content, masterminding it in an apparently unintelligible arrangement for others. Cryptography is a successful approach to secure the data that is transmitting through the system correspondence ways. Cryptology is the science that arrangements about cryptography and cryptanalysis. Cryptography is the methodology of sending the messages subtly and safely to the goal. Cryptanalysis is the technique for getting the installed messages into unique writings. By and large, cryptography is exchanging information from source to goal by modifying it through a mystery code. The cryptosystems utilizes a plaintext as information and create a figure content utilizing encryption calculation taking mystery key as information.

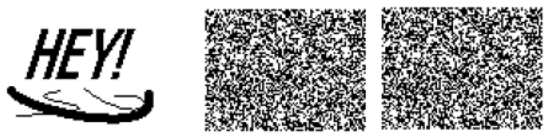
B) Visual Cryptography

Visual cryptography is a cryptographic technique which allows visual information (Image, text, etc.) to be encrypted in such a way that the decryption can be performed by the human visual system without the aid of computers. Image is a multimedia component sensed by human.

C) Techniques for Visual Cryptography

Visual cryptography, the most striking components of this approach is that it can be recuperation mystery picture with no calculation. It abuses human visual framework to peruse the mystery message from some covering offers, therefore conquering inconvenience of complex calculation required in the cryptography. In [19] author presented a basic however flawlessly secure way that permits mystery sharing with no cryptography calculation named as a visual cryptographic plan. The issue of scrambling composed material (printed content, manually written notes, pictures and so on) in a splendidly secure manner which can be specifically by the human visual framework. The thought is to change over the composed material into a picture and encode this picture into n shadow pictures. The deciphering requires just selecting some subset of these n pictures, making transparencies of them and stacking them on top of each other.

- Level 1 concealing utilizing Visual Cryptography



Secret Data share 1 share 2

- Super Imposing Share1 and Share2 to Form the Original Secret Data

The secret Information

The first inspiration was to protect cryptographic keys from misfortune. One of the best known procedures to ensure the information is cryptography. it is a specialty of sending and accepting scrambled messages that can be unscrambled just by the sender or the beneficiary Encryption and decoding are expert by utilizing scientific calculations as a part of such a route, to the point that nobody yet the expected beneficiary can unscramble and read the messages. Visual Cryptography Scheme is a cryptographic strategy that considers the encryption of visual data with the end goal that decoding can be performed utilizing the human visual framework. We can accomplish this by one of the accompanying access structure plans.

1.(2,2) Threshold VCS conspire This is a least difficult limit plot that takes a mystery message and encodes it in two distinct shares that uncover the mystery picture when they are overlaid. No extra data is required to make this sort of get to structure.

2. (2, n) Threshold VCS conspire this plan scrambles the mystery picture into n shares with the end goal that when any two (or more) of the shares are overlaid the mystery picture is uncovered. The client will be provoked for n, the quantity of members.
3. (N, n) Threshold VCS conspire this plan encodes the mystery picture to n shares with the end goal that when all n of the shares are consolidated will the mystery picture be uncovered. The client will be provoked for n, the quantity of members.
4. (k, n) Threshold VCS conspire This plan encodes the mystery picture to n shares to such an extent that when any gathering of in any event k shares are overlaid the mystery picture will be uncovered. The client will be incited for k, the Threshold,, and n, the quantity of members.

On account of (2, 2) VCS, every pixel P in the first picture is encoded into two sub pixels called offers. Fig.1 signifies the shares of a white pixel and a dark pixel. Take note of that the selection of shares for a white and dark pixel is arbitrarily decided (there are two decisions accessible for every pixel). Neither one of the shares give any insight about the first pixel since various pixels in the mystery picture will be scrambled utilizing autonomous arbitrary decisions. At the point when the two shares are superimposed, the estimation of the first pixel P can be resolved. On the off chance that P is a dark pixel, we get two dark sub pixels; on the off chance that it is a white pixel, we get one dark sub pixel and one white sub pixel.

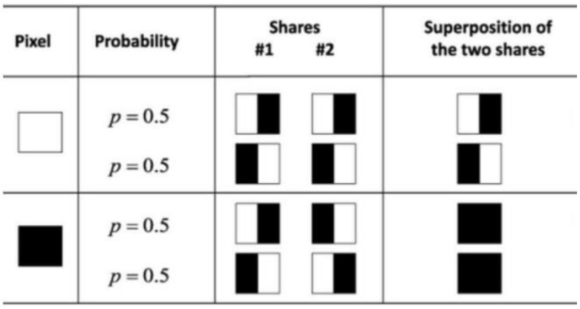


Fig 1. Illustration of 2-out-of-2 VCS scheme with 2 subpixels construction [19].

- Adjustment Technique

Proposed technique considered two consecutive pixels as the one time input in the source image and as a result there shall be four cases in input. These are as 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 references these are:
(i) Hamming weight of every block in each share should be the same.
(ii) Hamming weight of a black block will be greater than the other blocks in the stacked shares.
Let N is the number of participants (i.e no. of account holders). m=integer part of (n/2), where n= number of 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 four possible cases of input pixels:
(i) Black and Black: In this case arrangement of black pixels in the output block will be different from other blocks. This ensures that after stacking the shares,

Hamming weight of the stacked black blocks will become greater than the other blocks.

(ii) Black and White: Here the all the black pixels will be kept together from the first position of the output block.

(iii) White and Black: Where the all the black pixels will be kept together from the last position of the output block.

(iv) White and White: All black pixels will be kept together in the output block.

Now if the number of pixels in the input image is odd then the last pixel will be kept as it is in the shares.

Because the output media of visual cryptography are transparencies, we treat the white pixels of black-and- white images as transparent. Typically, the black-and-white visual cryptography decomposes every pixel in a secret image into 2×2 block in the two transparencies. According to the rules in fig1, when a pixel is white the method chooses one of the two combinations for white pixels in fig1. To form the content of the block in the two transparencies when a pixel is black it chooses one of the other two combinations. Then the characteristics of two stacked pixels are black and black is black, white and black is black, and white and white is white. Therefore , when stacking two transparencies, the blocks corresponding to black pixels in the secret images are full black, and those corresponding to white pixels are half-black and half-white which can be seen as 50% of grace pixels.

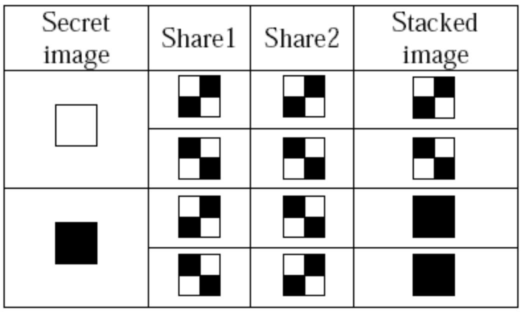


Fig 2. Sharing and Stacking Scheme of Black and White Pixels [19]

D) Comparison of various visual cryptography schemes:

Many research papers have been published using this approach, starting from a binary image moving to grayscale image and finally employing it to color images. Though with each subsequent research paper the quality of the recovered image improved. Detail of various visual cryptography schemes is given in table 4.1 below. One of the promising approaches for color images is proposed by in [7], the proposed technique involves splitting an image into multiple shares.

E) Steganography

Steganography is the act of hiding a record, message, picture, or video inside another document, message, picture, or video. The word steganography joins the Greek words steganos (στεγανός), signifying "secured, disguised, or ensured", and graphein (γράφειν) signifying "composing".

The initially recorded utilization of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography, camouflaged as a book on enchantment. By and large, the shrouded messages have all the earmarks of being (or are a piece of) something else: pictures, articles, shopping records, or some other cover content. For instance, the concealed message might be in imperceptible ink between the noticeable lines of a private letter. A few executions of steganography that do not have a common mystery are types of security through lack of clarity, while key-subordinate steganographic plans stick to Kerckhoffs' principle.

The benefit of steganography over cryptography alone is that the planned mystery message does not draw in thoughtfulness regarding itself as a protest of examination. Obviously noticeable encoded messages—regardless of how unbreakable—excite intrigue, and may in themselves be implicating in nations where encryption is illegal. Thus, while cryptography is the act of securing the substance of a message alone, steganography is worried with hiding the way that a mystery message is being sent, and in addition hiding the substance of the message.

Steganography incorporates the disguise of data inside PC records. In computerized steganography, electronic interchanges may incorporate steganographic coding within a vehicle layer, for example, a record document, picture record, program or convention. Media documents are perfect for steganographic transmission on account of their huge size. For instance, a sender may begin with a harmless picture record and conform the shade of each 100th pixel to compare to a letter in the letter set, a change so unpretentious that somebody not particularly searching for it is probably not going to notice it.

F) Least Significant Bits Technique for Steganography[4]

Today, when converting an analog image to digital format, we usually choose between three different ways of representing colors:

- 24-bit color: every pixel can have one in 2^24 colors, and these are represented as different quantities of three basic colors: red (R), green (G), blue (B), given by 8 bits (256 values) each.
- 8-bit color: every pixel can have one in 256 (2^8) colors, chosen from a palette, or a table of colors.
- 8-bit gray-scale: every pixel can have one in 256 (2^8) shades of gray.

LSB insertion modifies the LSBs of each color in 24-bit images, or the LSBs of the 8-bit value for 8-bit images.

Example:

The letter 'A' has an ASCII code of 65(decimal), which are 1000001 in binary.

It will need three consecutive pixels for a 24-bit image 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:

*1000000**1**.1010010**0**.1011010**0**,*
*1011010**0**.1111001**0**.1011011**0**,*
*1110011**0**.1011001**1**.00110011*

(The values in **bold** are the ones that were modified by the transformation)

The same example for an 8-bit image would have needed 8 pixels:

10000000, 10100100, 10110101, 10110101, 11110011,
10110111, 11100111, 10110011

Then their values after the insertion of an 'A' would have been:

*1000000**1**, 1010010**0**, 1011010**0**, 1011010**0**, 1111001**0**,*
*1011011**0**, 1110011**0**, 1011001**1***

III. PROBLEM DEFINATION

In a core banking system, there is a chance of encountering forged signature for transaction. In the net banking system, the password of customer may be hacked and misused. Thus Security is still a challenge in these applications. Here, we propose a technique to secure the customer information and to prevent the possible forgery of signatures and password hacking.

IV. LITERATURE REVIEW

In [1], new strategy is proposed, that utilizations content based steganography and visual cryptography, which minimizes data sharing amongst shopper and online shipper however empower effective store exchange from customer's record to vendor's record subsequently shielding purchaser data and avoiding abuse of data at dealer side. The strategy proposed is particularly for E-Commerce however can without much of a stretch be reached out for online and also physical managing an account.

In [3] proposes a novel procedure which endeavors to fathom all the above issues in steganography. In the proposed strategy, rather than substitutions we are utilizing the idea of matches between mystery information and cover picture. What's more, we additionally utilize the idea of altered recurrence for every character in English. The proposed technique is lossless, has limitless payload limit, has key size which is just around 10 to 20 rate of the message estimate and has enhanced security.

In [4], an information concealing plan by basic LSB substitution is proposed. By applying an ideal pixel alteration procedure to the stego-picture acquired by the basic LSB substitution strategy, the picture nature of the stego-picture can be significantly enhanced with low additional computational unpredictability. The most pessimistic scenario mean-square-mistake between the stego-picture and the cover-picture is determined. Trial comes about demonstrate that the stego-picture is outwardly vague from the first cover-picture. The acquired results additionally demonstrate a noteworthy change as for a past work.

In [5], the sender is concealing the information which is to send to the beneficiary as pictures. The picture is a blend of the content which is gotten from the two procedures of the content steganography which has been inferred before. The two procedures utilized are Reflection Symmetry and the Vedic Numeric technique. The sender sends the information into apportioned shape or we can say the information which is sent by the sender is parceled into 2 sections and separate-isolate part is sent to the two procedures. We are doing this as though the entire content is sent to one procedure or Vedic strategy it will expend more memory. In this way, the content in the wake of being prepared by the two procedures is joined to shape an entire content and after that the content is changed over into picture by the different techniques or calculations ex. LSB, network augmentation. In this way, the content is changed over into picture that is sent to the recipient. The model proposed in [6] considers the affectability and covering conduct of the human visual framework by method for a nearby isotropic complexity measure and a concealing model. We look at the addition of this watermark in luminance pictures and in the blue channel of shading pictures. We likewise assess the vigor of such a watermark regarding its installing thickness. Our outcomes demonstrate that this approach encourages the addition of a more powerful watermark while safeguarding the visual nature of the first. Moreover, we show that the most extreme watermark thickness by and large does not give the best identification execution.

In [8] paper, a procedure using picture preparing has been proposed utilizing Steganography and visual cryptography, and afterward partitioning it into shares. In this venture the message or the content document is taken as a contribution from the client who needs to get implanted in the picture record. The picture document can be of the expansions .jpg or .png. The message process is computed utilizing the MD5 calculation and this is affixed with the message. The annexed message is then encoded utilizing the AES calculation. The mystery enters utilized as a part of the AES calculation is scrambled utilizing the RSA calculation. The affixed scrambled message is inserted in the picture utilizing the minimum huge piece calculation. The encoded picture is transmitted. The secret word must be given before transmitting the picture document. At the beneficiaries side the watermarked picture record is taken as the information. The message in the picture record is removed utilizing the LSB calculation. The removed message is separated into the process and the message part. The message process is figured for the message and is contrasted and the got one. In the event that they are similar then message is said to be verified.

V. PROPOSED SYSTEM

Our project proposes a technique of processing a secret key of a customer and then dividing it into shares. When two shares are created, one is stored in the Bank database and the other is kept by the customer.

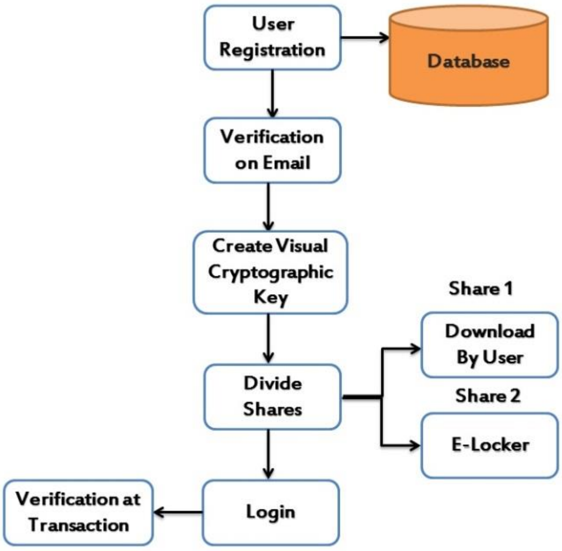


Fig 3. System Architecture

The customer has to present the share during all of his transactions. This share is stacked with the first share get the original secret key. The Correlation method is used to take the decision on acceptance or rejection of the output and authenticate the customer.

VI. CONCLUSION

This system uses Colour Image Visual Cryptography for password protection and it is not able to break this protection with present technology. This system will be a boon for the Core Banking Application and the bank customers are feeling free from the password hacking problems. Once this system is deployed in web Server, all the computer in the network can able to access this application through browser without any software installation in their computer.

VII. 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 and Electrical 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 and Communication 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 Advanced Engineering, vol. 3, no. 6, pp. 80-84, June 2013

[9]. C. Hegde , Manu S , P. Shenoy , Venugopal K R , L M Patnaik, “Secure Authentication using Image 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, “Visual Cryptographic Applications”, International Journal 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 Banking Application”.

[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 Of Steganography And Visual Cryptography,”

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

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

Cite this article as :

Pranay Kalamkar, Mrunali Gaikwad, Sumit Gore, Dhananjay Sonule, Prof. Vidya Bodhe, "A Review on Implementation Visual Cryptography and Steganography", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 6 Issue 2, pp. 420-428, March-April 2019. Journal URL : http://ijsrst.com/IJSRST196278