A Novel Approach on Secure Data Transfer for General Transactions using Secret Sharing Scheme

J. Sharmila
Assistant Professor,Dept.of CSE
Anil Neerukonda Institute of Technology and Sciences
Visakhapatnam

Jagadish Gurrala
Assistant Professor,Dept. of CSE
Anil Neerukonda Institute of Technology and Sciences
Visakhapatnam

ABSTRACT
In the last two decades, the researchers were targeted on the various issues in any general transactions was getting ambiguity in Information Technology domain because of its challenging nature and all overlapping purchases through selling goods during online shopping in government sector. Visual Cryptography gives us the best framework for all services where all authenticated mobile devices through legitimate users get linked and sharing secret keys with goods details with more security. In the paper, each Mobile get acquainted with this proposed framework to enable source to destination goods delivery among users who subscribed in the online shopping cart. Actual Customers want to shop any item from Flipcart, Amazon with unique purchase and selling their belonging without having gray item available in the network is possible through virtual shopping. In the paper to fill gap between old shopping framework and new framework through this techniques by supplementing new techniques inside mobile shopping. Therefore the .legitimate customer gets benefitted while shopping.

General Terms
Visual secret sharing, general Shopping, visual cryptography

Keywords
Network Security, Tamper resistance.

1. INTRODUCTION
Traditionally, Image processing is a process of converting the pixel intensities into binary 0's and 1's through computer to analyse information inside image using DCT algorithm or JPEG algorithm. A image is made up of a finite number of intensity, color and contrast elements, each of which has some particular location and use. These elements are known as picture elements or image elements simply called pels and pixels.

In visual cryptography phenomenon, a sender or Dealer wish to transmits the secret image which is divided into shares and it holds hidden information which is gained by different participants in the group activity. When all of these shares are aligned and stacked together, they tend to expose the secret image information to the receiver or participant. Earlier VC scheme, the secrecy of the share is not maintained due to any other fake shares can easily insert or modified remain to be continuing challenges. To solve this security issues, a secure share creation scheme constructed by a (k, n) VC scheme has been developed. Once the shares are created,. In this process,k shares of n participants and key bind together to give the resultant shares are called the encapsulated shares[1]. Consequently, the secret image information cannot be retrieved from any one transparency via human visual perception. These scheme offers better security for shares and also reduces the fraudulent shares of the secret image. Further, the experimental results and analyses that the proposed scheme can effectively fill the gap between old Framework using VC scheme and New Framework of VC encrypt the image with the fast execution speed and minimized PSNR value.

The combination of visual cryptography with the public key encryption ends in high security while transmitting the image [5]. The solution of the innovative technique for keeping dishonesty at bay is the acceptance of several secret images in such a way that each qualified subsets will expose the relative secret image only, leaving the other secret images unfamiliar to the prospective hawkers[6].

Image sharing using VC defines a scheme which is similar to that of general secret sharing [Shamir 1979]. In (k, n) image sharing, the image that carries the secret is split up into n pieces and the decryption is totally unsuccessful unless at least k pieces are collected and superimposed. A Visual Cryptography Scheme (VCS) provides a mechanism by which physically superimposing the pieces (known as shares) of an image is able to completely recover the secret.

The combination of visual cryptography with the public key encryption ends in high security while transmitting the image [5]. Image sharing using VC defines a scheme which is similar to that of general secret sharing [Shamir 1979].

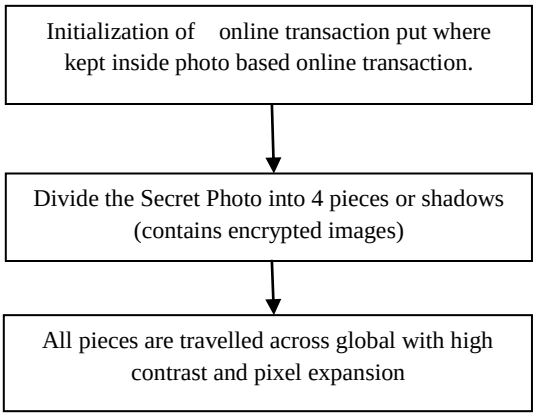


Fig 1: Justification of E-Shopping cart using Visual Cryptography

The rest of this paper is organized as follows. In section 2 discussed literature review is presented. In section 3 focuses on related work and simulation setup and running a scenarios were discussed in section 4. In section 5 the results of the performance evaluation are discussed. Conclusion & Future work is given in section 6.

.

2. LITERATURE SURVEY

Visual cryptography is a cryptographic technique proposed by Moni Naor and Adi Shamir in 1979[12].This cryptographic technique encrypts the images into number of meaningless shares which are Xeroxed into transparencies and only after combining all the shares generated from the image , the original image is retained. If the information is concealed, the adversaries may not be distorted the data. The way to proper and secure transmission of the data becomes a challenging issue. Cryptographic techniques afford the confidentiality and security by reducing the prospect of adversaries [1]. One of the most widely used type of information sharing or secret sharing is the visual secret sharing for voters authentication. Without involving any complex computations, decode the secret biometric face image visually by superimposing a qualified subset of shares through the visual secret sharing method. In the context, there exist Boolean operation of the secret image sharing that overcomes the drawback of low visual quality and pixel expansion created by the VSS [2]. Visual cryptography is a special secret sharing technique that means it is dissimilar from usual cryptography, for the reason that it does not require complex computation to decrypt[3]. In the modern public key cryptography, factors decomposition hassles dependent on huge numbers are habitually employed, the classic example being the RSA cryptography. In visual cryptographically the generated image shares are encrypted by using RSA algorithm.

2.1 PROBLEM STATEMENT

Preserving the voters data (e.g., face images) stored in a cloud has become of paramount importance. This work [6] explores the possibility of using visual cryptography for imparting privacy to voters database data such as fingerprint images, iris codes, and face images. In the case of baby faces or a private face image is dithered into four host face images (known as shares) that are stored in four isolated virtual servers in cloud such that the private image can be revealed only when four shares are simultaneously available; at the same time, the individual share images do not reveal the identity of the private image.

A series of experiments on the MATLAB tool to confirm the following testimonies:

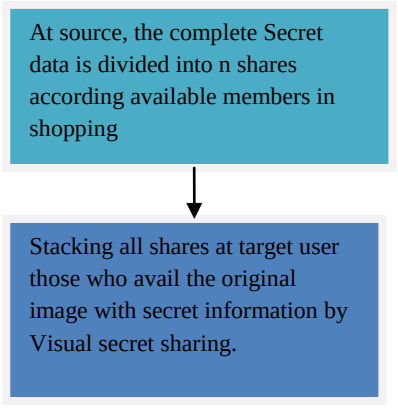
1) The possibility of hiding a private face image in four host face images;
2) The successful matching of face images reconstructed from the shares;
3) The inability of shares to reveal the identity of the private face image;
4) Using different pairs of host images to encrypt different samples of the same private face; and
5) The difficulty of cross-database matching for determining identities. A similar process is used to de-identify fingerprint images and iris codes prior to storing them in a central database.

3. EXISTING PROTOTYPE

3.1 Visual Secret Sharing model

At originator, a user wish to dispatch private face images is to be divided into four shares requires for distribution of pieces or called shares in which all parts of secret data is get dispersed. At receiver all the pieces of a private face image to receive the details of pieces by using visual cryptography schemes contains stacking operation to reduce the transmission bandwidth bottlenecks. In fig 2. The entire process is discussed the process in prototype. Secret sharing is an important concept in modern cryptography.

Often, it is desired that only a certain group of people can recover the secret. The concept of secret sharing was independently introduced by Shamir and Blakley in 1979. Secret sharing becomes indispensable whenever secret information needs to be kept collectively by a group of participants in such a way that only a qualified subgroup is able to reconstruct the secret. An example of such a scheme is a k-out-of-n threshold secret sharing in which there are n participants holding their shares of the secret and every k ($k \leq n$) participants can collectively recreate the secret while any k-1 participants cannot get any information about the secret [4-7]. The need for secret sharing arises if the storage system is not reliable and secure. Secret sharing is also eminently useful if the owner of the secret does not trust any single person.



.

Fig 2: prototype for secret sharing

3.2 Security Analysis

To analyse the security of the 2-out-of-2 VCS, the dealer (sender) randomly chooses one of the two pixel patterns (black or white) from the Table 1. for the shares S1,S2,S3,S4. The pixel selection is random so that the shares S1,S2,S3 and S4 consist of equal number of black and white pixels. Therefore, by inspecting a single share, one cannot identify the secret pixel as black or white. This method provides perfect security. The two participants can recover the secret pixel by superimposing the two shared subpixels. If the superimposition results in two black subpixels, the original pixel was black; if the superimposition creates one black and one white subpixel, it indicates that the original pixel was white.

Let us assume that the binary secret image consists of m x n bits. In the case of k-out-of-n VCS, each share consists of mn bits. Thus, there are 2^{mn} possible combinations. If an intruder takes one microsecond to generate and check one combination, then it takes (k-1) * 2^{mn} *10^{-6} seconds to break the secret for a k-out-of-n VCS, where m and n are the number of rows and columns of the secret image. Consider the binary secret image consisting of 20 bits (2x10). In the case of 3-out-of-4 VCS, each share consists of 20 bits. Thus there are 2^{25} possible combinations. If an intruder takes one microsecond to generate and check one combination, then it will take $2*2^{25} * 10^{-6}$ seconds ~ 12.5 years to reconstruct the secret image. By using recursion, the security of the visual cryptography scheme can be greatly improved.

4. PROPOSED SECRET SHARING METHOD

In the research progress, authors find out gap between past technique and present techniques. It is found that some calculation are needed at receiver by finding our original image from pixels. In the proposed methodology, there is combination of original image and piece of image. Authors tried a lot to get the original image by finding ways in the algorithm. In the mobile shopping general transaction operation, the entire task is to be divided into 3 modules according to tamper proof of goods.

Step1: construction of share from Original image of bar code of item in shopping using (1,1) scheme

Step 2: During construction, Subdivide the Original Image into 2 sub pixels according black line and white lines defined in the Barcode in equal portions.

Step 3: Key is generated for sending the sub images (shares) to the target people to whom the data is received.

Step 4: finally the keys are sending along with share to destination where the secret data is revealed at receiver according to the what sender and receiver agrees on the key management..

4.1 Construct the Share from Original Image

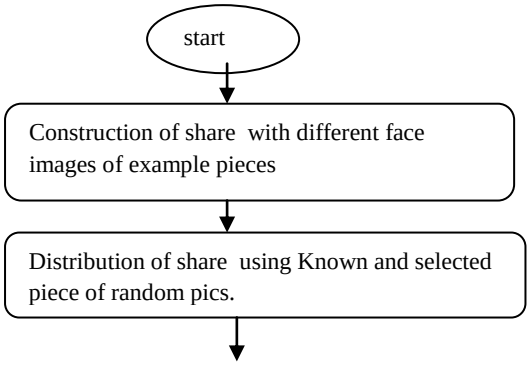
In the process, the total image taking from file 128* 120 size BMP secret data(Baby image)(D) is to be send for transforming into set of sub images(shares) where secret data is hidden whenever all shares are combined together. In this regard, the original image is getting divided into 4 encrypted shares according RSA and DES algorithms.

Fig 3: Secret Image

Share1 share 2 share3 share 4

These shares(piece of secret image) in fig 4 to be converted into binary format using DCT and then send it to receivers desk.

The following framework is proposed on this concept.



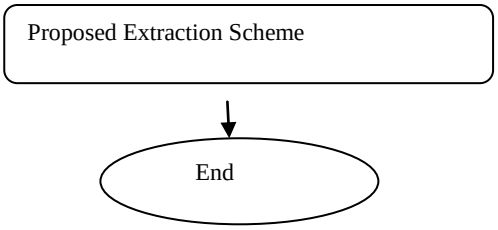


Fig 4: Proposed model

4.2 Proposed Distribution of share:

In this stage, total secret D (e.g., the safe combination) and in which non-mechanical solutions (which manipulate this data) are also allowed. Our goal is to divide D into 4 pieces $D_1 \ldots . D_4$ in such a way that:

(1) Knowledge of any 4 or more D_i pieces makes D easily computable.

(2) Knowledge of any 3 or fewer D_i pieces leaves D completely undetermined (in the sense that all its possible values are equally likely).

Such a scheme is called a (4, 4) threshold scheme. Efficient threshold schemes can be very helpful in the management of cryptographic keys. In order to protect data we can encrypt it, but in order to protect the encryption key we need a different method (further encryptions change the problem rather than solve it). The most secure key management scheme keeps the key in a single, well-guarded location (a computer, a human brain, or a safe). This scheme is highly unreliable since a single misfortune (a computer breakdown, sudden death, or sabotage) can make the information inaccessible. An obvious solution is to store multiple copies of the key at different locations, but this increases the danger of security breaches (computer penetration~ betrayal, or human errors).

4.3 Proposed Extraction Scheme

In the extraction phase fig 5 all pieces are received by concern party those who wants to that copy. In this process the pieces of different image shares are to be segregated together to form original baby image. In the voters database where share1 taken from 4th user and share 2 taken from 2nd user, share 3 taken from 1st user and share 4 taken from 3rd user.

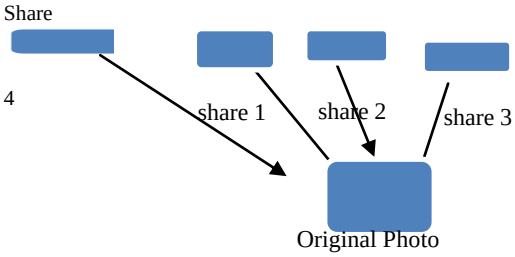


Fig 5. Illustration of Extraction Process

Hence all pieces are gets delivered to destination without distortion even intruders are intervened.

n= want to Searching the resource that is available in the Shopping cart.Initially Dealer (DL) wants to sell the resource to the group of reliable participants (P) through mobile

shopping where all participants can utilize the resources through Visual secret sharing.

By using a (k, n) threshold scheme with n = 2k- 1 we get a very robust key management scheme: We can recover the original key even when ⌊n/2⌋ = k- 1 of the n pieces are destroyed, but our opponents cannot reconstruct the key even when security breaches expose ⌈n/2⌋ = k- 1 of the remaining k pieces.

4.4 Aspect Ratio of proposed method

In the original image contains pixel is to be expanded into big pixel through secret sharing process. In the MATLAB tool, authors observed that baby image with visual secret sharing concept is embed and after deliver extract the image. In table 1. Observed the details from simulation of proposed scheme using MATLAB

Table 1. Observations after share division from original image

Given Image	**Before Share Quality**	**After Share Quality**
Baby with visual secret sharing	0.8	0.5
Baby (visual secret sharing)	**0.8**	**0.7**

5. CONCLUSION

The authenticated user presents their shares across network for general transaction needs many things. These shares are stacked and encrypted to get the original image. The original image is reconstructed by adding the transparencies. During adding the shares appropriately for each sub-pixels of share 1 and share 2 by the process, authors are ready the pair of secret portion of image and existing algorithm discussed above vague idea.

But other pixels which represent the grey image are randomly distributed. To avoid this noise, the technique of post-processing is applied on this image.

6. ACKNOWLEDGMENT

Our sincere thanks to the Dr.R.Sivaranjani, Professor & HoD of CSE who have contributed towards development of the research work.

7. REFERENCES

[1] "Visual cryptography. in Proceedings of Advances in Cryptology", Moni Naor and Adi Shamir,EUROCRYPT 94, LNCS Vol. 950, pages 1- 12. Springer - Verlag, 1994

[2] D. R. L. Prasanna, L. Jani Anbarasi and M. Jenila Vincent "A Novel Approach for Secret Data Transfer using Image Steganography and Visual Cryptography" ICCCS'11, February 2011.

[3] Piyush Marwaha and Paresh Marwaha "Visual Cryptographic Steganography In Images" Second International conference on Computing, Communication and Networking Technologies. 2010.

[4] Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. "Digital image steganography: Survey and analysis of current methods" Signal processing, Vol. 90(3), pp. 727-752, 2010.

[5] Kaur, S., Kaur, A., & Singh, K. "A survey of image steganography" IJRECE, Vol. 2(3), pp. 102-105, 2014.

[6] Anbarsi LJ, Kannan S. Secured secret color image sharing with steganography. In: Recent Trends In Information Technology ICRTIT.2012;44-48.

[7] P.Sanyasi Naidu,Reena Kharat,2016,"Secure Authentication in online voting system using multiple Image secret sharing, springer verilog, 2016.