International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869 (O) 2454-4698 (P), Volume-3, Issue-7, July 2015

A Review Paper on Visual Cryptography Technique

Pooja Maan, Mrs. Raman Chawla

***Abstract*— With the coming era of electronics commerce, there is an urgent need to solve the problem of ensuring information safety in today's increasingly open network environment. The encrypting technologies of traditional cryptography are usually used to protect information security. Visual cryptography is an emerging cryptography technology. It is a special cryptographic technique where decryption is done by an authorized user by simply overlaying the shares. It uses the characteristics of human vision to decrypt encrypted images. It needs neither cryptography knowledge nor complex computation. For security concerns, it also ensures that hackers cannot observe any clues about a secret image from individual cover images. So, there is a need to design a method by which a binary image could me encrypted and decrypted easily in a secure manner. This paper provides a review of the visual cryptography.**

***Index Terms*— visual Cryptography, secret sharing, Information Sharing, Shares.**

I. INTRODUCTION

Cryptography refers to the study of mathematical techniques and related aspects of Information security like data confidentiality, data Integrity, and of data authentication. Cryptography as the study of secret (crypto) writing (graphy) can be defined as the science of using mathematics to encrypt and decrypt data back. Cryptography is the art of achieving security by encoding messages to make them non-readable. It is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis [6].

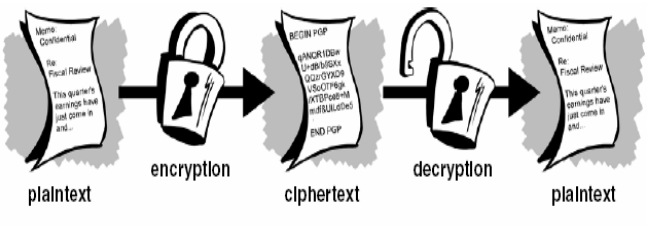

Figure.1 General Block Diagram of Cryptography [6]

Pooja Maan, Computer Science and Engineering, N.C. College of Engineering, Israna Panipat, India
Mrs. Raman Chawla, Computer Science and Engineering, N.C. College of Engineering, Israna Panipat, India

Visual cryptography

Visual cryptography, introduced by Naor and Shamir in 1995 [1], is a new cryptographic scheme where the ciphertext is decoded by the human visual system. Hence, there is no need to any complex cryptographic computation for decryption. The idea is to hide a secret message (text, handwriting, picture, etc…) in different images called shares or cover images. When the shares (transparencies) are stacked together in order to align the subpixels, the secret message can be recovered. The simplest case is the 2 out of 2 scheme where the secret message is hidden in 2 shares, both needed for a successful decryption. This can be further extended to the k out of n scheme where a secret message is encrypted into n shares but only *k* shares are needed for decryption where $k \leq n$. If *k*-1 shares are presented, this will give no information about the secret message.

Unlike conventional cryptographic methods, VC needs no complicated computation for recovering the secret. The act of decryption is to simply stack shares and view the Secret image that appears on the stacked shares [2].

Table1.Naor and Shamir's scheme for encoding a binary pixel into two shares [4]

Pixel	Probability	$Share_1$	$Share_2$	$Share_1 \otimes Share_2$
□	50%	■□	■□	■□
	50%	□■	□■	□■
■	50%	■□	□■	■■
	50%	■□	■□	■■

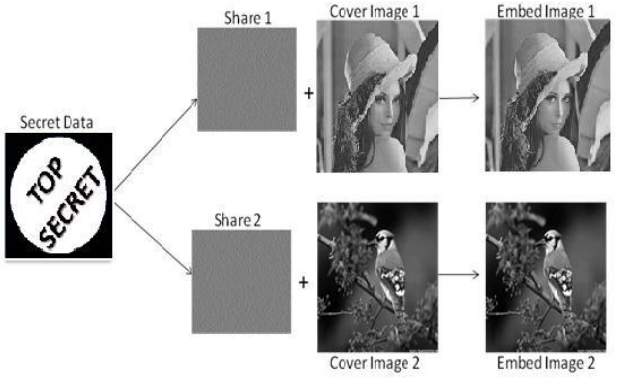

Figure 2: Secret Data Embedding Process using Visual Cryptography [5]

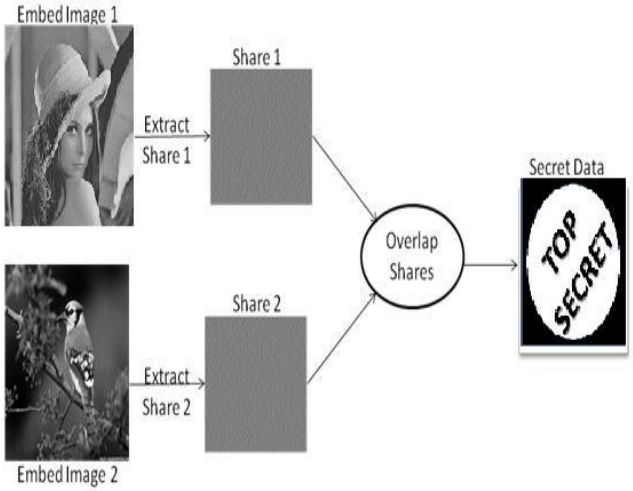

Figure 3: Data Extracting Process using Visual Cryptography [5]

II. Access Structure of Visual Cryptography

To encode the image, original image is split into n modified versions referred as shares. It involved breaking up the image into n shares so that only someone with all n shares could decrypt the image by overlaying each of the shares over each other. Practically, this can be done by printing each share on a separate transparency and then placing all of the transparencies on top of each other. Decoding can be done by simply stacking subset s of those n shares. In their technique n-1 shares reveals no information about the original image [2]. Figure 1 depicts the working of Visual Cryptography.

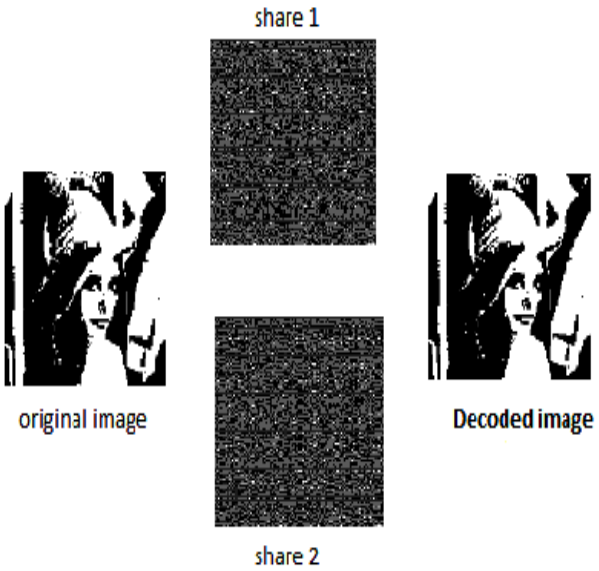

Figure 4: Working of Visual Cryptography

III. VCS Algorithms

VCS Scheme normally involves two algorithms:

- Algorithm for creating shares
- Algorithm for combining shares

Algorithm for creating shares:

This algorithm divides secret image into n number of shares. The shares created by this algorithm will be in unreadable format such that it is impossible to reveal secret image. Single share cannot reveal the secret image. If these individual shares are transmitted separately through communication network, security is achieved.

Algorithm for combining shares:

This algorithm reveals the secret image by taking the number of shares as input. Some algorithm may take all shares as input and some other algorithm may take subset of shares as input. Decryption is done by merging shares which has taken as input [2].

IV. Visual Cryptography Based Image Watermarking Schemes

Watermarking in images can be done both in spatial and transform domains. Spatial domain techniques though computationally less complex, are less resilient to attacks. Transform domain techniques, on the other hand, are more robust in comparison to spatial domain techniques since they modify the coefficients of the transform of the pixel values. Discrete wavelet transform (DWT), discrete cosine transform (DCT) and discrete Fourier transform (DFT) based transformed domain techniques have been found to be more robust than spatial domain techniques particularly in attacks like lossy compression, rescaling, rotation, noise addition etc [7].

V. Visual Cryptography Based Video Watermarking Schemes

A video is nothing but a sequence of images yet image watermarking techniques cannot be directly applied to videos owing to their three dimensional characteristics. In addition to their special preprocessing techniques, the temporal nature of videos has to be taken into account [7]. Redundancy between frames and a large volume of data makes it all the more difficult to perform watermarking in videos. Some common forms of attack on videos are frame swapping, frame averaging, frame dropping, statistical analysis, interpolation etc. which are unknown to the domain of image watermarking. Inter- video collusion attacks and intra-video Collusion attacks are also issues which need to be addressed. Real time implementations of video watermarking techniques are generally much more complex than that of image watermarking which becomes an important issue.

Video watermarking schemes are used for various video applications such as copyright protection, copy control, fingerprinting, broadcast monitoring, video authentication, enhanced video coding etc.

Some traditional video watermarking schemes attempt to embed an entire watermark image within each video frame or within random video frames to give the appearance of a hidden watermark to the casual observer.

VI. Applications of Visual Cryptography

- ***QR Code application***

The block diagram of QR Code application is shown in fig 5.

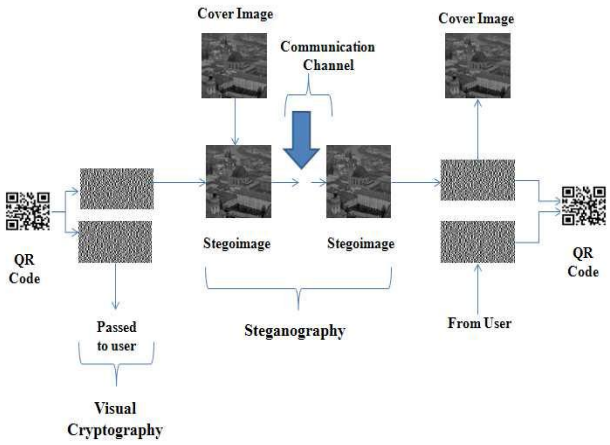

Fig. 5: Visual Cryptography and Steganography for QR code application [3]

- ***Banking application***

The block diagram of banking application is shown in fig 6. In banking application, the bank logo or key image is divided into multiple shares using visual cryptography for colour images. Then each share is hidden into bank customer image or cover image using steganography technique. Then at the time of access of particular joint account by multiple account holders extract each customer share using extraction technique of steganography and overlap the customer shares to get bank logo or key image. Then comparison can be made with certain threshold and then decision can be taken whether access is allowed or is denied. Depending on presence of number of customers the access permissions are given using k out of n visual cryptography schemas for colour images.

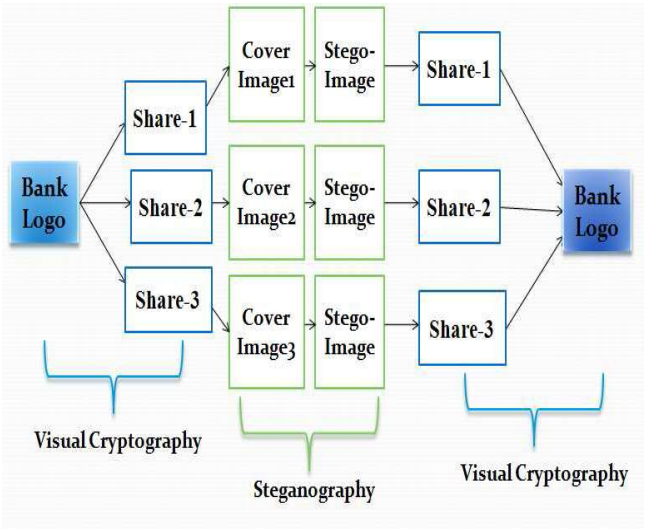

Fig. 6: Visual cryptography and Steganography for banking application [3]

VII. CONCLUSION & FUTURE SCOPE

Cryptography is the art of achieving security by encoding messages to make them non-readable. It is the science of using mathematics to encrypt and decrypt data. Visual cryptography is the current area of research where lot of scope exists. Currently this particular cryptographic technique is being used by several countries for secretly transfer of hand written documents, financial documents, text images, internet voting etc. It provides one of the secure ways to transfer images on the Internet. The main advantage of visual cryptography is that it exploits human eyes to decrypt secret images with no computation required. Visual cryptography is used in many applications like bank customer identification, biometric security & remote electronic voting etc. In this paper we have reviewed about visual cryptography & its various applications.

REFERENCES

[1] R.Youmaran, A. Adler, A. Miri "An Improved Visual Cryptography Scheme for Secret Hiding" 23rd Biennial Symposium on Communications, 2006. PP. 330-333.

[2] Ranjan Kumar H S, Prasanna Kumar H R, Sudeepa K B and Ganesh Aithal, "Enhanced Security System using Symmetric Encryption and Visual Cryptography", International Journal of Advances in Engineering & Technology ©IJAET, Vol. 6, Issue 3, pp. 1211-1219, July 2013, ISSN: 22311963.

[3] Omprasad Deshmukh , Shefali Sonavane "Multi-Share Crypt-Stego Authentication System". IJCSMC, Vol. 2, Issue. 2, February 2013, pg.80 – 90.

[4] Thottempudi Kiran1, K. Rajani Devi, " A Review on Visual Cryptographic Scheme", Journal of Global Research in Computer Science, Volume 3, No. 6, June 2012, ISSN-2229-371X.

[5] Mr. Abhay Sharma, Mrs. Rekha Chaturvedi, Mr. Naveen Hemrajani, Mr. Dinesh Goyal, "New Improved and Robust Watermarking Technique based on 3rd LSB substitution method",International Journal of Scientific and Research Publications, Volume 2, Issue 3, March 2012 , ISSN 2250-3153.

[6] P.Arunagiri, B.Rajeswary, S.Arunmozhi and K.Priethamje vithya "A Steno Hiding Using Camouflage Based Visual Cryptography Scheme" International Journal of Power Control Signal and Computation (IJPCSC) Vol. 2 No. 1.PP. 1-5.

[7] Adrita Barari , Sunita Dhavale "An Overview of Visual Cryptography based Video Watermarking Schemes: Techniques and Performance Comparison" Proc. of Int. Conf. on Advances in Computer Science, AETACS, Association of Computer Electronics and Electrical Engineers, 2013