ISSN:2320-0790

An International Journal of Advanced Computer Technology

A Comprehensive Study on Visual Cryptography

Malyala Sravya Lakshmi[1], Gadi Lava Raju[2]

1 post P.G student of Andhra university dept of (CSC) and lecturer at Aditya Degree College Kakinada E.G.Dt, Andhra Pradesh INDIA.

2. Post P.G. Student of JNTU-K dept of (CSE) and lecturer at Aditya Degree College Kakinada E.G.Dt, Andhra Pradesh, INDIA.

ABSTRACT: This article is a deal with the Review study of visual cryptography there is a need for study. The information helps the mathematician, computer engineers, Academicians' and researchers for better understanding of data whenever it is required. So for this a study is made on the basis of secondary data. Cryptography in the study of mathematical techniques related aspects of information security such as confidentialities, data security, entity authentication, but it is not only the means of providing information security, rather one of the techniques. Visual cryptography is a new technique which provides information security which uses simple algorithm unlike the complex, computationally intensive algorithms used in other techniques like traditional cryptography. This technique allows Visual information like pictures, text. to be encrypted in such a way that their decryption can be performed by the human visual system, without any complex cryptographic algorithms. . In this paper we provide an overview of the emerging Visual Cryptography (VC) and related security. Research work done in this area.

Key Words: Algorithm, Mathematical, Security, Techniques.

I. Introduction

Naor and Shamir introduced Visual Cryptography in 1994. Visual cryptography technique allows the visual information to be encrypted in such a way that their decryption can be performed by human visual system. Security has become an inseparable issue as Information Technology is ruling the world now this technique encrypts a secret image into shares such that stacking a sufficient number of shares reveals the secret image. Shares are usually presented in transparencies The associated secret sharing problem and its physical properties such as contrast, pixel expansion and color were extensively studied by researchers worldwide.

1.1 Various types' cryptography:

The basic model of Visual Cryptography assumes that the secret message consists of black and white pixels. Each secret pixel is either divided into two subpixels or four subpixels. These subpixels form the shares for the secret message. There are different or similar subpixel pattern based on the secret pixel according to the inferred structure can be described in the form of m×n Boolean matrix S = [sij] where sij=1 iff the jth subpixel of the ith share is black. These subpixels are then printed on transparent sheets so that overlapping the transparent sheets reveals the secret message. The gray level value of this combination of shares is equal to the Hamming Weight H(V) of the "or" ed m-vector V. The gray level is visualized as black if H(V) ≥ d and white if

H(V)≤ d-α.m for some fixed threshold 1≤d≤m and relative difference . . Different kinds of Visual Secret Sharing Schemes existing are: (n, n) Visual Secret Sharing Scheme (k, n) Visual Secret Sharing Scheme (n, n) Visual Secret Sharing Scheme is where the secret is divided into a total of n shares and all the n shares are overlapped to get visually read the secret message. (k, n) Visual Secret Sharing Scheme is where the secret is divided into n shares and any k or more of these shares when overlapped reveals the secret. (k, n) Visual Secret Sharing Scheme consists of two collections of n×m Boolean matrices C0 and C1. When a white pixel is shared, any one of the matrices out of the collection in C0 is chosen. And when a black pixel is desired to be shared, anyone matrix out of all in the collection in C1 is considered. The following conditions are to be satisfied to reveal the secret in a (k, n) Visual Scheme using the above matrices. For ant S in C0, the "or" V of any k of the n rows satisfies H(V)≥ d.

1.2 [Ateni01] is a type of cryptography which e[i]ncodes a number of images in the way that when the images on transparencies are stacked together, the hidden message appears without a trace of original images. The decryption is done directly by the human visual system with no special cryptographic calculations. This paper presents a system which takes three pictures as an input and generates two images which correspond to two of the three input pictures. The third picture is reconstructed by printing the two output images onto transparencies and stacking them together. While the previous researches basically handle only binary images, this paper establishes the extended visual cryptography scheme suitable for natural images. Generally, visual cryptography suffers from the deterioration of the image quality. This paper also describes the method to improve the quality of the output images. The trade-off between the image quality and the security are discussed and assessed by observing the actual results of this method. Furthermore, the optimization of the image quality is discussed.

II. Objectives of the study:

1. Visual Cryptography schemes
2. Usage of visual cryptography

III. Earlier studies on focused study area

3.1 Embedded Extended Visual Cryptography Schemes:

Visual cryptography scheme (VCS) is a kind of secret sharing scheme which allows the encoding of a secret image into n shares that distributed to n participants. The beauty of such scheme is that a set of qualified participants is able to recover the secret image without any cryptographic knowledge and computation devices. Extended visual cryptography scheme (EVCS) is a kind of VCS which consists of meaningful shares (compared to the random shares of traditional VCS). In this paper, we propose a construction of EVCS which is realized by embedding random shares into meaningful covering shares, and we call it the embedded extended visual cryptography scheme (embedded EVCS). Experimental results compare some of the well-known EVCS's proposed in recent years systematically, and show that the proposed embedded EVCS has competitive visual quality compared with many of the well-known EVCS's in the literature. Besides, it has many specific advantages against these well-known EVCS's respectively. Visual Cryptography (VC) was first introduced by Moni Noar and Shamir at Eurocrypt'94. 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. To encode a secret employing a (2, 2) VC Scheme, the original image is divided into two shares such that each pixel in the original image is replaced with a non-overlapping block of two or four sub-pixels. . Anyone who holds only one share will not be able to reveal any information about the secret. To decode the image, each of these shares is xeroxed onto a transparency. Stacking both these transparencies will permit visual recovery of the secret. Visual Cryptography scheme. There are several schemes of encoding the pixels of the secret image. In our scheme, each pixel in the secret image is broken into four sub pixels. A white pixel is shared into two identical blocks of four sub-pixels. A black pixel is shared into two complementary blocks of four sub-pixels., illustrates this scheme of encoding one pixel into four pixels in a (2, 2) VC scheme. All the pixels

in the original image are encrypted similarly using this scheme. These shares can be either Vertical or Horizontal or Diagonal Share. [ii]The Visual cryptography scheme (VCS) is a secure method that encrypts a secret image by breaking it into shares. A distinctive property of VCS is that one can visually decode the secret image by superimposing shares without computation. The project presents an approach for embedding visual cryptographically generated image shares in the host images to provide authentication for the VC shares and makes these secret shares invisible by embedding them into host images. The secret shares generated from VC encryption are watermarked into some host images using digital watermarking. Digital watermarking is used for providing the double security of image shares. The share is embedded into the host image in frequency domain using Discrete Cosine Transform (DCT). In frequency domain, the obtained marked image must be less distorted when compared to the original image. Thus secret shares are not available for any alteration by the adversaries who try to create fake shares. Every pixel of the binary VC share is invisibly embedded into the individual block of the host image. The process of watermark extraction necessitates only the watermarked image and it does not require the original host image. The scheme provides more secure and meaningful secret shares that are robust against a number of attacks like blurring, sharpening, motion blurring etc. Visual cryptography (VC) is a method of encrypting a secret image into shares such that stacking a sufficient number of shares[iii] reveals the secret image. Shares are usually presented in transparencies. Each participant holds a transparency. Most of the previous research work on VC focuses on improving two parameters: pixel expansion and contrast. we studied the cheating problem in VC and extended VC. We considered the attacks of malicious adversaries who may deviate from the scheme in any way. We presented three cheating methods and applied them on attacking existent VC or extended VC schemes. We improved one cheat-preventing scheme. We proposed a generic method that converts a VCS to another VCS that has the property of cheating prevention. The overhead of the conversion is near optimal in both contrast digression and pixel expansion. Visual cryptography scheme is one of the most secure techniques for privacy protection[iv], that allow the encryption of secret image or data by transferring it into the secure share and such a scheme is able to recover the secret image or data without any computation devices. In today's era security of that transmitted data is most important problem because network technology is greatly advanced and lot's of information is transmitted via the internet. Visual cryptography scheme allow encoding the original message to hide its meaning and decode it to reveal the original message. Also encoding of information in the number of shares and distributed to number of participants, which decrypt information without any cryptographic knowledge. The shares are sent through different communication channels from sender to receiver so that the probability of getting sufficient shares by the intruder minimized. But the shares may arise suspicion to the hacker's mind that passed information is secret. We can encrypt original image using a key to provide more security to this scheme. This makes visual cryptography scheme a completely secure scheme.

IV. Usage of visual cryptography:

a) Usage for banking sectors:

(2, n) visual cryptographic scheme has been proposed which may be useful in Banking [v]operations in the "either or survivor" mode where n is the number of generated shares, from which n-1 is the number of account holders in an account and one share should be kept to the bank authority. In this technique one account holder should stack his/her share with the share of the bank authority and the secret image for user authentication will be revealed. In this technique two consecutive pixels are taken as the one time input for the share generation process. This technique generates shares with less space overhead compared to existing techniques and may provide better security. It is also easy to implement like other techniques of visual cryptography.

With the evolution in the world of internet, it has become prone to several online attacks and the most common attack is phishing. Phishing is an act of fraudulently acquiring confidential and sensitive information about the user, such as[vi] banking password or credit card number, by pretending to be

a trustworthy entity. Victims are tricked into providing such information by a combination of spoofing techniques and social engineering. we have proposed a new technique named as "An Enhanced Anti-Phishing Framework Based on Visual Cryptography". An image based authentication using Visual Cryptography is implemented. Our proposed methodology uses visual cryptography to preserve the privacy of the randomly chosen image by decomposing the image into two shares. These two shares are for that particular session. The trusted server stores unique keys for the users required for decryption of the share. The original image is obtained at the user end only when both the user and the server under test are registered with the trusted server. Using this method the user can determine whether the site is safe or unsafe to carry out his transaction.

b). Print and Scan applications:

VC is a cryptographic technique that ensures the security of images by dividing a secret image into random shares, which makes the image data unreadable. Then decryption is performed by superimposing the shares, without any special computational power. Intuitively, VC can be categorized as: secret sharing scheme [1] for monochrome images and extended VC (EVC) [2] for [vii]color images. both schemes of VC have been exploited to hide image where image security is essential, such as Bangla text document, hand-written signature, biometric authentication (e.g. human face) etc. These can be exercised in offices for deed, in banking sector for financial document and in examination or election system for authentication respectively. Moreover a minor modification of EVC which can be applied for color image also has been presented

Visual Cryptography is a special type of encryption technique which is used to hide the information and data in images. In this technique the decryption process is done without any complex cryptographic computation. The encrypted data is decrypted using Human Visual System (HVS). This is the benefit of the[viii] visual secret sharing scheme. The encryption technique requires a cryptographic computation to divide the image into a number of parts or we can call it shares. We divide the image into n number of shares. In this paper we have proposed a new k-n secret sharing visual cryptographic scheme for black and white images in which encryption of the image is done by using Random Number generator. This k-n secret sharing scheme uses at least a group of k shares out of n shares to reveal the secret information and less of it will not reveal any information.

Visual cryptography is not much in use in spite of possessing several advantages. One of the reasons for this is the difficulty of use in practice. The shares of visual cryptography are printed on transparencies which need to be superimposed. However, it is not very easy to do precise superposition due to the fine resolution as well as printing noise. Furthermore, many visual cryptography applications need to [ix]print shares on paper in which case scanning of the share is necessary. The print and scan process can introduce noise as well which can make the alignment difficult. In this paper, we consider the problem of precise alignment of printed and scanned visual cryptography shares. Due to the vulnerabilities in the spatial domain, we have developed a frequency domain alignment scheme. We employ the Walsh transform to embed marks in both of the shares so as to find the alignment position of these shares. Our experimental results show that our technique can be useful in print and scan applications.

V. Conclusions

1. Cryptographic schemes, which can decode concealed images without any cryptographic computations. The scheme is perfectly secure and very easy to implement.

2. Visual Cryptography is a special kind of cryptographic scheme where the decryption of the

Encrypted secret is done by the human vision and not by complex mathematical calculations. Visual Cryptography deals with any secrets such as printed or pictures, etc. These secrets are fed into the system in a digital (image) form. The digital form of the secrets is then divided into different parts based on the pixel of the digital secret. These parts are

called shares. The shares are then overlapped correctly to visualize the secret.

3. In this paper we have tried to solve the theoretical problem associated with the use of visual cryptography. Many VC Applications involve printing the share on the paper channel.

4. print and scan technique needs to be developed for recovering the secret image. However, precise alignment at high resolutions is then a problem. We therefore propose the use of the Walsh transform to embed alignment marks in the transform domain. These marks are used as guides to precisely align the shares automatically. Our experimental results point to the viability of the use of VC for print and scan applications.

5. Focus on the applications of visual cryptography on the 2D bar code.

REFERENCES:

[1]. mizuho nakajima,yasushi yamaguchi. extended visual cryptography for natural images.

[2]. Jagdeep Verma, Dr.Vineeta Khemchandani, A Visual Cryptographic Technique to Secure Image Shares, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 1,Jan-Feb 2012, pp.1121-1125.

[3]. Chih-Ming Hu and Wen-Guey Tzeng Cheating Prevention in Visual Cryptography, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 16, NO. 1, JANUARY 2007 pp 36-47.

[4]. Nayan A. Ardak Prof. Avinash Wadhe, Visual Cryptography Scheme for Privacy Protection, International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 2026-2029.

[5]. A (2, n) visual cryptographic technique for banking applications, Jayanta Kumar Pal, J. K. Mandal2 and Kousik and Dasgupta, International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4, October 2010, pp:118-127.

[6]. Gaurav Palande, Shekhar Jadhav, Ashutosh Malwade, Vishal Divekar, Prof. S. Baj, March 2014 An Enhanced Anti-Phishing Framework Based on Visual Cryptography, International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-3),

[7]. Md. Tanbin Islam Siyam, Kazi Md. Rokibul Alam and Tanveer Al Jami, An Exploitation of Visual Cryptography to Ensure Enhanced Security in Several Applications, *International Journal of Computer Applications (0975 – 8887) Volume 65– No.6, March 2013*.

[8]. Puja Devi Rana*, Anita Singhrova**, Suman Deswal, Design and Implementation of K-Split Segmentation Approach for Visual Cryptography, International Journal of Scientific and Research Publications, Volume 2, Issue 8, August 2012 1 ISSN 2250-3153,

[9]. *Wei-Qi Yan, Duo Jin, Mohan S Kankanhalli,* visual cryptography for print and scan applications.