ISSN:0975-9646

Visual Cryptography Scheme for Privacy Protection

Nayan A. Ardak Prof. Avinash Wadhe

Dept. of Computer science and Engineering
G.H. Raisoni College of Engineering
Amravati, India

***Abstract*— Visual cryptography scheme is one of the most secure techniques for privacy protection, 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.**

***Keywords*—** visual cryptography scheme, secret share, privacy protection

I. INTRODUCTION

Privacy protection is very important in today's world where personal information, images are generally sharing to each other through the network. When we are sharing information on internet number of outsiders or intruder try to hack it before receive that information by receiver.

So, protect the information from hackers visual cryptography scheme is used. Visual cryptography was introduced as a technique allowing the visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be carried out by human visual system, without the aid of computers visual cryptography find applications in various sectors such as E-voting for giving encrypted receipts.

Visual cryptography scheme is propose by Naor and Shamir. Visual cryptography is the scheme used for the secrete share of image in that secret share the original image is divided into number of shares and that share is distributed to same number of participants as each to one. That secret image is recoverable only when participant share their secret. VCS splits secret image into random shares which separately reveals no information about the secret image other than the size of the secret image .The secret image can be reconstructed by stacking shares. It supports OR operation for decryption. It satisfies the following two conditions:

1. Qualified subset of shares can recover the secret image.
2. Any forbidden subset of shares cannot obtain any information about the secret image other size of the image.

Visual cryptography encodes a secret binary image into n shares of random binary patterns. The secret image can be visually decoded by superimposing a qualified subset of transparencies, but no secret information can be obtained from the superposition of a forbidden subset. By engaging a cryptographic encryption technique involving pixel shuffling and inter changing their position to create the ciphered image, this proposed method makes it difficult for decryption of the image without prior knowledge of the algorithm and the secret key used. Secret shared key and visual cryptography are two distinct types of cryptography. In this paper a method is proposed which combines visual cryptography with shared secret key for the encryption and the decryption process.

This paper has the following structure: section II is about literature survey, section III is on the survey on visual cryptography techniques for the encryption and the decryption process of the digital images, section IV presents analysis of technique employed to come out with a ciphered image for the encryption process. Section V conclusion of the visual cryptography scheme for protecting information, and section VI reference.

II. LITERATURE SURVEY

Noar and Shamir [1] proposed a cryptographic technique which allows visual information (e.g. printed text, handwritten notes and pictures) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. Visual cryptography scheme eliminates complex computation problem in decryption process, and the secret images can be restored by stacking operation.

Sharma and Rao [2] Visual Cryptography authentication for Data Matrix Code in Identity cards.

Data Matrix Code is used to address the authenticity and security of the vital information of the owner such as credit card number, contact number, address or even photograph. Data Matrix Code is an optical, machine readable representation of data which uses the vertical dimension to store and retrieve information.

Vinodhini and Ambarasi [3] proposed a method for authentication based on Visual Cryptography using

CAPTCHA. CAPTCHA stands for Completely Automated Public Turing test to tell Computers and Humans Apart.

Jing Dong [4] proposed biometric watermarking for protecting biometric data and templates in biometric systems. The scheme suggest protection of iris templates by hiding them in cover images as watermarks (iris watermarks), and protection of iris images by watermarking them.

James and Philip [5] proposed phishing attack prevention using a framework. The framework supports complete web application security with respect to phishing attacks. The proposed framework has two phases. In the first phase, a new user registers himself. While making registration the web application chooses an image then it is converted into two share images.

Verheul and Van Tilborg [6] proposed Colored secret images can be shared with the concept of arcs to construct a colored VCS. In colored VCS one pixel is converted into m sub pixels, and each sub pixel is further divided into c color regions. In each sub pixel, there is exactly one color region is colored, and other color regions are black. The color of one pixel depends on the interrelations between the stacked sub pixels.

Fang and Lin [7] proposed a progressive visual secret sharing (PVSS) scheme that demonstrated when more shares are stacked progressively, the recovery of the secret image will be clearer and clearer. Although Fang and Lin's method could achieve a progressive effect, their adoption of expanding pixels meant that more storage space is needed.

Nakajima and Yamaguchi [8] presented a scheme for encrypting a natural image pixel expansion made the share images nine times larger than the original image.

Thien and Lin [9] proposed a pixel non-expansion method that could produce a meaningful share-image but a computer was needed to decrypt the secret image, losing the advantage of visual cryptography which is decryption directly by the human eye.

Chen and Tsao [10] first proposed a user-friendly random grid visual secret sharing (Friendly RGVSS) method which achieved the goal of producing meaningful share-images and pixel non-expansion, but their method still had many restrictions. In that method, pixels are taken from the secret image and the cover image to generate the needed share-images.

III. SURVEY ON VISUAL CRYPTOGRAPHY TECHNIQUE

Security has become an inseparable issue not only in the fields strictly related to secure communications but fields that have anything to do with storage of data as well. Visual Cryptography is the study of mathematical techniques related aspects of Information Security which allows Visual information to be encrypted in such a way that their decryption can be performed by the human visual cryptography system, without any complex algorithms. Secret sharing was developed by Adi Shamir in 1979 for the concept of visual cryptography. He stated that dividing of secret image into *n* pieces and easily reconstructed from any *k* pieces. Encryption protected our data but key use for encryption it not be protected. Hence he introduce the concept of secrete share. According to Shamir, the scheme is *k* out of *n* secret sharing scheme. There are number of technique use for the privacy protection of the data some of the technique is as follows which encrypt and decrypt the data to protect it using the secret share.

3.1 Error Diffusion

Error diffusion is simple method used to improve the quality of image by removing the error from the image. The quantization error at each pixel is filtered and fed back to a set of future input samples. Fig. 1 shows a binary error diffusion diagram where represents the pixel of the input grayscale image, is the sum of the input pixel value and the "diffused" past errors, is the output quantized pixel value. Figure 1 contain the error filter which filter the error to gives us the original image.

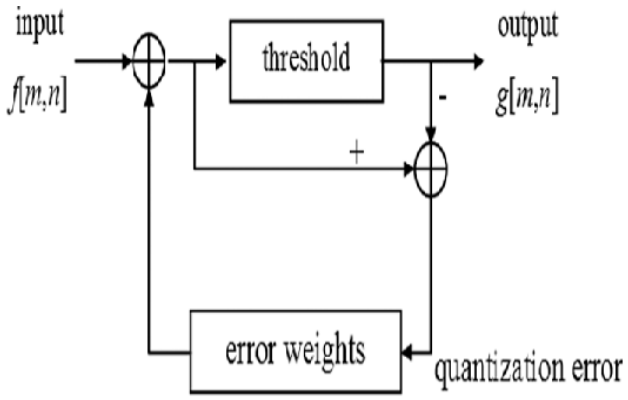

Fig. 1 error diffusion technique

In error diffusion method the error value is distributed on a fractional basis to the neighboring pixels. In this case, the error is computed and added to the pixel right of the current pixel that is being processed. The proposed privacy scheme in visual cryptography via error diffusion technique just shares the error values to neighboring pixels. So that it makes the binary image to achieve some effect as gray image. The error values are computed serially for each pixel.

3.2 Expansion less share

Visual cryptography encrypts secret information into two pieces called as shares. These two shares are stacked together by logical XOR operation to reveal the original secret. Hierarchical visual cryptography encrypts the secret in various levels. The encryption in turn is expansion less. The original secret size is retained in the shares different levels. In this paper secret information is encrypted at two different levels. Out of hierarchical visual cryptography generated the four share. To form the key share any three shares are collectively taken. All shares generated are meaningless it gives no information by visual inspection. Its performance analysis is also based upon various categories of secrets.

In earlier work of visual cryptography, we encrypted the secret with the expansion ratio of 1:4 and later 1:2. The

expansion indicates that if original secret is of size AXB then with expansion ratio 1:4 the shares have size 4AX4B and with expansion ratio 1:2 the shares reflected are found to be of size 2AX2B. Due to this expansion hierarchical encryption of secret gets affected. During encryption using hierarchical visual cryptography initially secret is encrypted using 1:2 expansion ratios giving two shares S1 and S2. If S1 and S2 are encrypted with the same expansion ratio independently then the resultant four shares are again expanded forms of S1 and S2.

3.3 Image captcha base authentication technique

For the anti-phishing there are two phases registration and authentication in the registration phase, User enters a key, server enters a key and then captcha image is generated. The image is divided into two shares in such a way that the shares when stacked together should restore the original captcha[7].

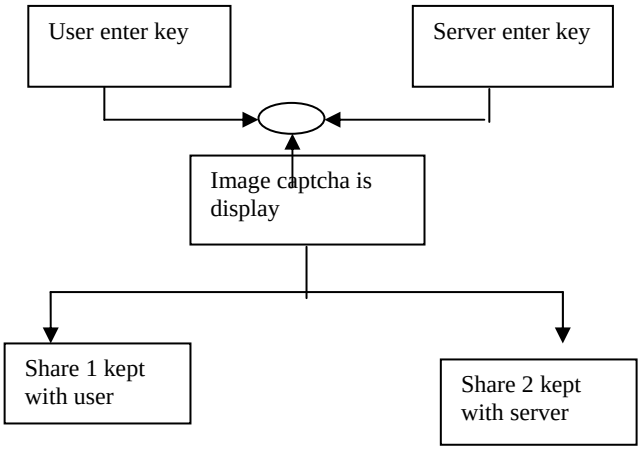

Fig. 2 Registration phase

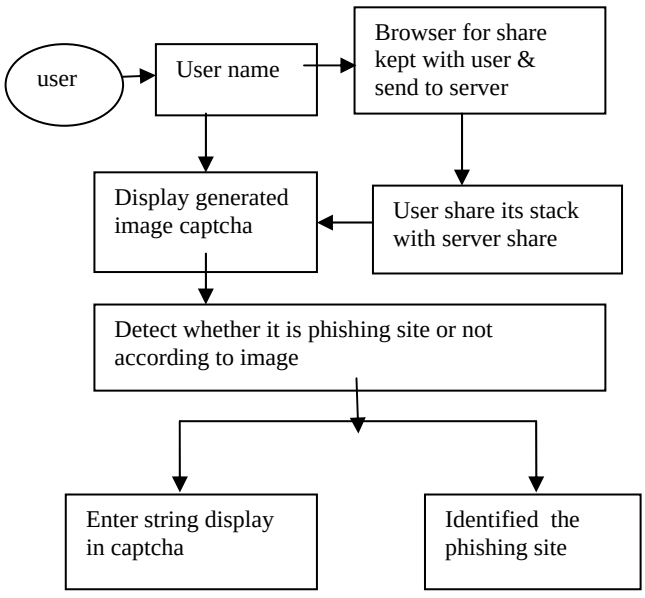

Fig 3. Login Phase mechanisms for anti-phishing.

In the login phase actual authentication takes place. The authentication process is built in such a way that it can detect any kind of phishing attack. In fact it can prevent fishing attack. When the user logs in by entering his confidential information for using his account, then first the user is asked to enter his username (user id).Then the user is asked to enter his share which along with him. This share is sent to the server where the user's share and this shares which are stored in the database of the website for each user, to produce the image captcha we stack it together. The image captcha is displayed to the user.

3.4 Compression random share

The secret shares are generated by using the random permutation of a pre selected basis matrix. The process of the encryption is implemented on the basis of the number of the required secret shares. These parameters are: I – Secret Image, N – Number of secret shares to be generated from I. Share – Encrypted image created using I. To encrypt the secret image a well known LZW compression technique is used. It is a lossless compression algorithm suggested by Abraham Lempel, Jacob Ziv, and Tery Welch published in 1984 it has been improved by many of the researchers to get best results from it.

This algorithm is implemented in following steps

Step1: Create the dictionary that contains all the strings of one character.

Step2: Find a string W with longest length that matches to give input.

Step3: Produce the index for W in the dictionary to give output and eliminate W from the input.

Step4: Append W followed by the next character in the given input to the dictionary.

Step5: Repeat from Step2. Until finished.

Decoding is a very simple process by reading a value from the encrypted input and producing the related string form the generated dictionary. During this the next value from the input is obtained and added to the dictionary by concatenation of the string and the first character of the string accessed by decoding the next value.

IV. ANALYSIS OF VISUAL CRYPTOGRAPHY TECHNIQUE

4.1 Error Diffusion has the tendency to enhance edges in an image. When an image has a transition from light to dark the error diffusion algorithm tends to make the next generated pixel be black. Dark to light transitions tend to result in the next generated pixel being white. This causes an edge enhancement effect at the expense of gray level reproduction accuracy. This results in error diffusion having a higher apparent resolution. This is especially beneficial with images with text in them. So, that the text in the image become sharper and makes more readable. In both secret share generation and decryption part, or operation is used, which makes the scheme very simple.

4.2 The huge expansion in shares affects the space complexity. While superimposing the shares of hierarchical visual cryptography, the larger

transparencies are required. Expansion-less hierarchical visual cryptography is the solution to reduce this expansion in the shares. The requirement of this proposed method is that the secret should be in binary form i.e. black and white passwords, signatures, handwritten text etc. Before encrypting, the original secret is mapped into the size which is multiple of *4*. Before encrypting the secret, it is normalized.

4.3 Anti-phishing technique preserve the privacy of captcha. It achieves this by dividing the original image into two shares which are to be stored in different databases. The decryption is possible only when adversaries can provide both shared at a time. The individual shares can't reveal the original captcha. It prevents password and other confidential information from the phishing website. It is also useful to prevent the attacks of phishing websites on financial web portal, banking portal, online shopping market.

4.4 It provides a safe and secure transmission as it involves multiple manipulations for encryption and so is it with decryption. This System provides a simple user interface to process images. Furthermore, the proposed system is very easy to use and anybody can use this system without having any cryptographic knowledge. It also does not provide the reduction of the size of the covering shares in any way. It is a lossless compression algorithm.

V. CONCLUSION

This paper many visual cryptography technique are used for privacy protection such as Expansion less share, Image captcha base authentication technique, Compression random share and error diffusion for visual quality improvement. Error diffusion is used to construct the shares such that the noise introduced by the preset pixels are diffused away to neighbors when encrypted shares are generated. It is obvious that there is a tradeoff between contrast of encryption shares and the decryption share, however, we can recognize the colorful secret messages having even low contrast. Image captcha base authentication, anti-phishing methodology proposed in. It is nothing but visual cryptography in which image captcha is used to prevent identity theft. Encryption at each level o HVC is expansion less. A share generated out of VC represents the same size of secret. This techniques is more effective in providing security from illicit attacks.

REFERENCES

[1] Mr.A.Duraisamy, Mr.M.Sathiyamoorthy, Mr.S.Chandrasekar, "Protection Of Privacy In Visual Cryptography Scheme Using Error Diffusion Technique", IJCSN, Vol 2, Issue 2, April 2013 ISSN (Online) : 2277-5420

[2] Anushree Suklabaidya, G. Sahoo, " Visual Cryptographic Applications", IJCSE, Vol. 5 No. 06 Jun 2013, ISSN : 0975-3397

[3] P.S.Revenkar, Anisa Anjum, W .Z.Gandhare, "Secure Iris Authentication Using Visual Cryptography", IJCSIS, Vol. 7, No.3, 2010, ISSN 1947-5500

[4] Mounika Reddy.M, Madhura Vani.B, "A Novel Anti Phishing Framework Based On Visual Cryptography", IJARCCE,Vol. 2, Issue 9, September 2013 ISSN (Online) : 2278-1021

[5] L. N. Pande, Niraj Shukla, "Visual Cryptography Schemes Using Compressed Random Shares", International Journal Of Advance Research In Computer Science And Management Studies, Volume 1, Issue 4, September 2013, ISSN: 2321-7782 (Online)

[6] Young-Chang Hou , Zen-Yu Quan, "Progressive Visual Cryptography With Unexpanded Shares", IEEE Transactions On Circuits And Systems For Video Technology, Vol. 21, No. 11, November 2011

[7] Young-Chang Hou, Shih-Chieh Wei, And Chia-Yin Lin," Random-Grid-Based Visual Cryptography Schemes",

[8] Mrs. A.Angel Freeda, M.Sindhuja, K.Sujitha, "Image Captcha Based Authentication Using Visual Cryptography", IJREAT, Volume 1, Issue 2, April-May, 2013 ISSN: 2320 - 8791

[9] Pallavi Vijay Chavan, Dr. Mohammad Atique , Dr. Latesh Malik, "Design And Implementation Of Hierarchical Visual Cryptography With Expansionless Shares" IJNSA, Vol.6, No.1, January 2014