Visual Cryptography-Methods and Applications Survey

Kajal RK Pandey
SRTTC's Faculty of Engineering

Abstract— Cryptography is a technique used for encryption of data (pictures, text, etc.) which involves key to decrypt the data encrypted which can only be done by desired recipient. It depends on type of key used to decrypt it that is private or public key. It was created for security purpose, but the key used in this can act as a major loophole sometimes. To overcome this, there is a technique called visual cryptography which does not use key. It can only be decrypted by human eye. In this paper proposed information is about visual cryptography methods and schemes.

Key words: Halftone, Pixel, Segment, Secret sharing, Security, Visual cryptography

I. INTRODUCTION

Visual cryptography was introduced by Naor and Shamir at EUROCRYPT '94[1]. It is used to encrypt written material (printed text, handwritten notes, pictures, and many more) in a perfectly secure way. The decoding is done by the human visual system directly. Plain text is as an image. Encryption involves creating "shares" of the image which in a sense will be a piece of the image. Give the shares to the respective holders. Decryption is a process involving bringing together all the shares for superimposition in an appropriate combination and then decoded only to human visual system.

So basically it involves dividing the image into two parts:
Key: a transparency
Cipher: a printed page

Separately, they are random noise. Combination reveals an image.

II. LITERATURE SURVEY

A. *Visual cryptography Methods:*

1) *Pixel Based Visual Cryptography:*

In [1], it is proposed that each pixel is divided into two sub-pixels; so that any one of them does not give information about original image. For this it uses K out N secret sharing system. In this images are divided into N shares which are further distributed to K holders. To recover original image respective holders has to superimpose all K shares. K-1 shares cannot be used to retrieve original data as any one share or K-1 share cannot be used to get original image.

In this white pixel and black pixel are divides into two shares creating two choices of generating shares [1]. Here every pixel is sub-divided into 4 sub-pixels so that to get original image we have to superimpose all the shares.

Here, each black pixel is divided into black or white or white and white pixel. Whereas each white pixel is divided into black or white or black and black pixel. Suppose there is an image, whose shares are created namely S1 and S2; when they are superimpose we get original image. Neither one of them reveal original image.

In these 2 out of 2 sharing system is used [1]:

1) To get S we have to; S1 XOR S2.
2) S1 and S2 have binary values (0, 1)

0 XOR 0=0
0 XOR 1=1
1 XOR 0=1
1 XOR 1=0

Here, black pixel is represented by 1 and white as binary digit 0[1].

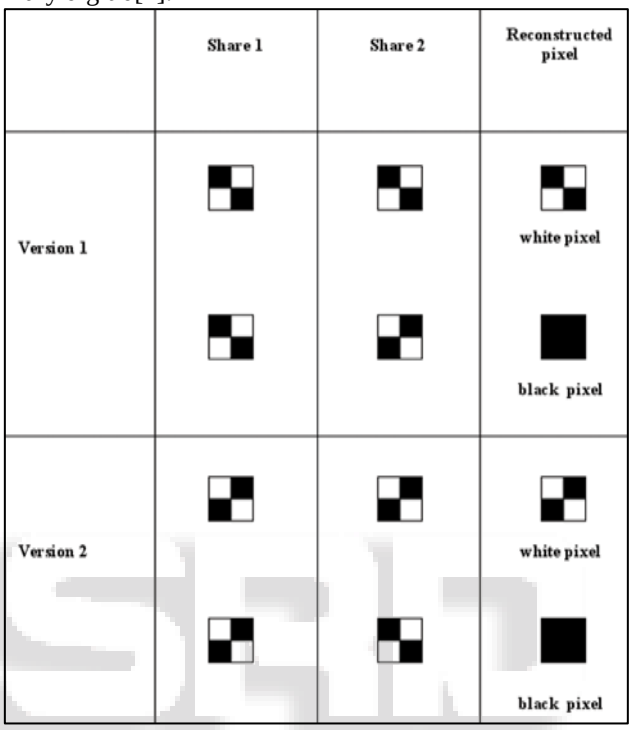

Fig. 1: Pixel based cryptography

2) *Segment Based Visual Cryptography:*

In [1], it is proposed that shares are based on segments rather than pixel. It is used to represent 0-9 and A-Z type of images to be encrypted. Here smallest unit of encryption is not pixel but segments. It is used for messages which represent in numbers and literals. In this it uses seven bars; 4 vertical and 3 horizontal. Like pixel based visual cryptography each segments is divided into shares, here each segment is divided into shares like S1 and S2. Selected segment is highlighted; rest is merged with respective background color. Follows same (n, k) visual cryptography technique.

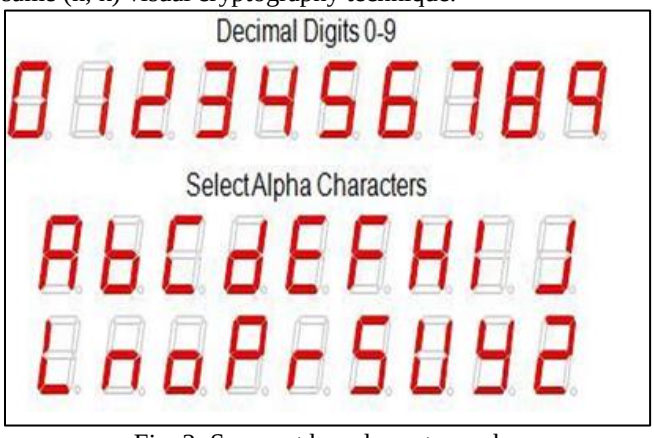

Fig. 2: Segment based cryptography

B. Visual Cryptography Scheme:

1) Black and white visual cryptography scheme:

In [2], it is proposed that encoding scheme to share a binary image is done by dividing it in shares. In black and white image cryptography, if pixel is black one of the two shares of second part of table 1 is selected and if white pixel one of the shares of table 1 of top part is selected. Further it performs encryption process by following basic (n, k) visual cryptography scheme.

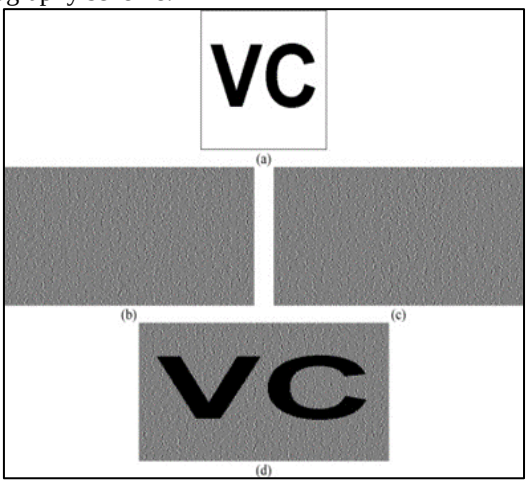

Fig. 3: Black and white visual cryptography scheme

2) Gray Scale Image cryptography scheme:

In this [2], it is explained that to encode an image it uses (2, 2) VC scheme .Here it uses dithering technique which is used to create illusions of the color that are not present actually. The reduction size of decrypted image compared to technique is obtained but quality depends upon the halftone image. Here half-toning means a process of generating a binary pattern of black and white dots from an image is called as half-toning. Gray-scale image is changed into approximate binary image or Halftone image having pixel value 0 and 1 [2]. After that same method of 2 out of 2 virtual cryptography scheme is applied to get shares. And then original image can be reconstructed by superimposition of these shares.

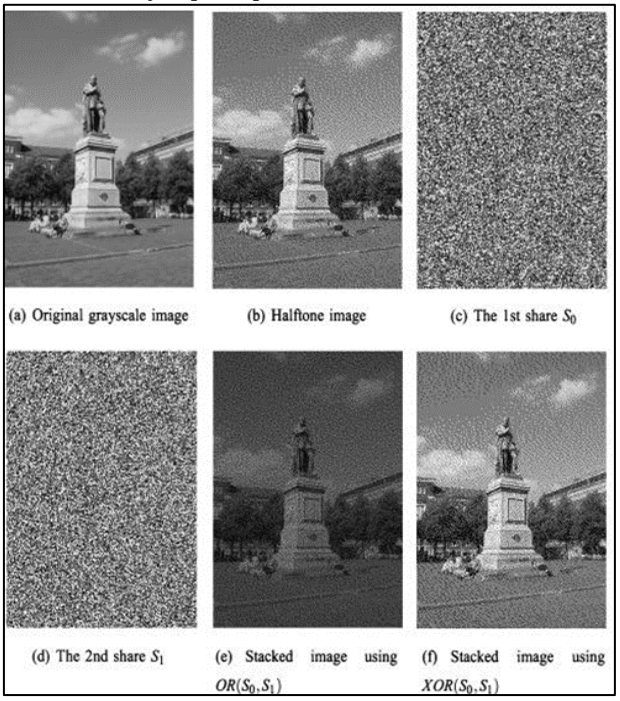

Fig. 4: Gray Scale Image cryptography scheme

3) Color visual cryptography scheme:

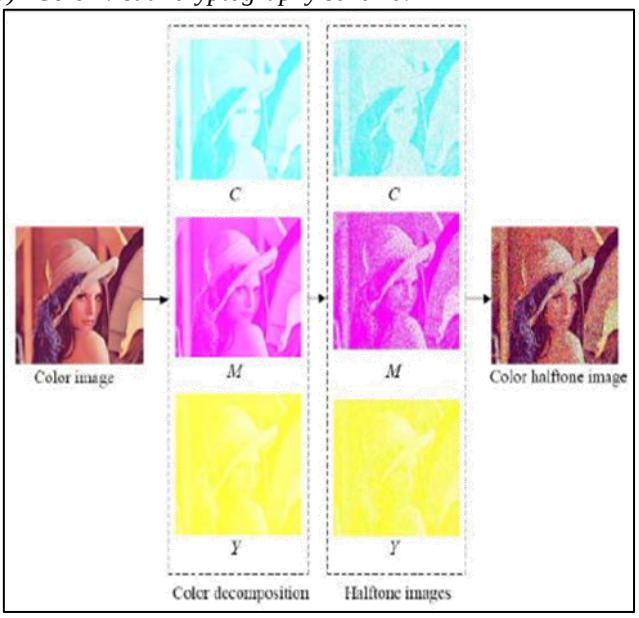

Fig. 5: Color visual cryptography scheme

A secret image which needs to be used for any confidential data can be decomposed into three monochromatic colors. Further this decomposed image is converted into binary image and then it is encrypted using further normal secret sharing system. In decryption the recovered binary image are inverse halftones and then superimposed to get secret color image.

Color half-toning:

We can do color channel splitting first and then do gray-scale half-toning for each shares

SPLIT CMY Half toning

$I \text{ ------} \square\ [I^c I^m I^Y] \text{-----} \square\ [I^c_{hft}, I^m_{hft}, I^Y_{hft}]$

Or we can do color half-toning first followed by splitting.

Color halftoning Split CMY

$I \text{ ----------} \square\ [I_{hft}] \text{ -------} \square\ [I^c_{hft}, I^m_{hft}, I^Y_{hft}]$

After this, each shares are created according to (2,2) VC scheme to be distributed among holders .For decryption OR operation is performed to stack up shares to get original image.

III. PROPOSED TECHNOLOGY:

Visual cryptography is a cryptographic technique which allows visual information (pictures, text) to be encrypted in such a way that decryption can only be performed through normal human visual system.

Visual cryptography is performed by dividing image into encrypted N shares given to K holders, which can only be decrypted by stacking all shares. No K-1 holders can reveal or decrypt original image.

When customer wants to do a transaction it might be futile sometimes or not stable that is sometimes there are chances of getting hacked. So to reduce the chances of it, visual cryptography is used to create shares of transaction key. When a customer wants to do the transaction of money ,they must submit their one time transaction key share which with combined together with one time generated transaction details share can allow access to that customer to do further process.

1) Customer fills in details of transaction.
2) According to type of transaction that is cheque or cash shares are generated which is divided to respective sender ,receiver and the bank worker who is involve in that transaction process.
3) Customer that is sender has to first submit its share with bank worker performing transaction .This step can only pass on transaction money and details to receiver.
4) Receiver has to superimpose their share to get transaction details.

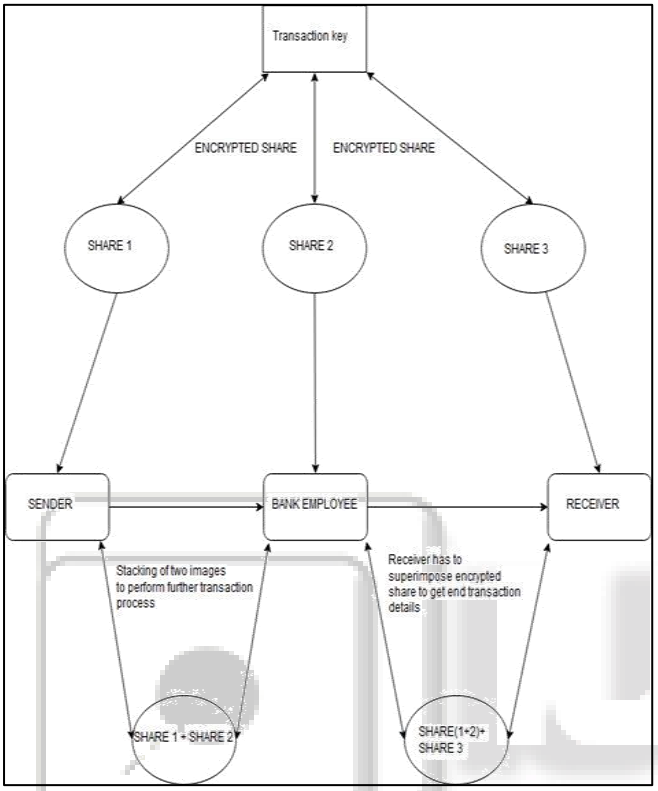

Fig. 6: Proposed system architecture

IV. PERFORMANCE ANALYSIS PARAMETER OF VIRTUAL CRYPTOGRAPHY:

Parameters recommended by researchers to analyze performance of virtual cryptography scheme are as follows [3]:

1) Security:

It satisfies the security parameter if no shares reveal information about original image. And also no K-1 share reveal original image.

2) Accuracy:

This parameter is satisfied if the reconstructed image does not compromise on quality criteria.

3) Contrast:

Contrast 'a' is the relative difference in weight between combined shares that come from a white pixel and a black pixel in original image. [3].

4) Pixel Expansion:

It refers to number of sub-pixel in divided shares that represents a pixel of original image. These parameters are taken into consideration when there is loss in resolution than original image.

5) Image format:

Visual cryptography should support encryption on binary, gray-scale and color images.

6) Shares generated:

Hackers treat shares generated from original image as critical information. So, If random looking shares are mixed with original image shares, hackers interest might be reduced. [3]

7) Computational complexity:

In this total numbers of operators are required to generate n shares and also to reconstruct original image.

V. APPLICATIONS

A. In Online Banking [4]:

To minimize the information sent to the online merchant, steganography and visual cryptography to produce online payment system. Password is hidden in cover text with the help of steganography technique and placed below account number. A snapshot is taken to create shares; one share given to respective customer while other is saved in database. When customer comes for payment, they have to submit their own copy of share combined with merchant shares to get password and other details.

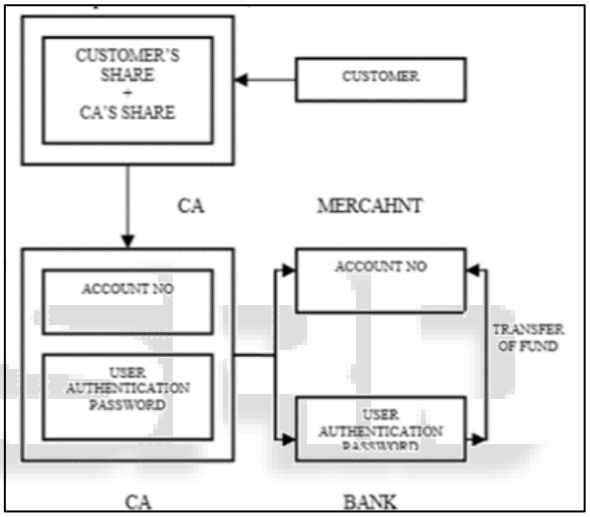

Fig. 7: Payment System

B. Anti-phishing framework [4]:

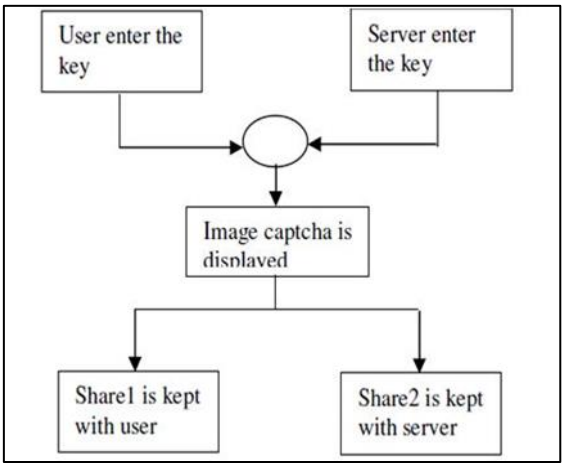

Fig. 8: System architecture

Fake websites are created to get information about user personal details like credit cards number, address and many more. To avoid this we can use shares. Here Shares are created , one share is given to user while other to server .If user wants to access a site ,they will give their share to be superimposed with server share to verify that website is fake or not.

C. Watermark:

Current system on visual cryptography can be used to protect watermark of any association, company or brand. It can be done so to protect original watermark of respective holder from getting copied or distributed by creating it's given shares to respective holders.

VI. FUTURE SCOPE

1) Visual cryptography in Videos.
   Currently, there is also need to encrypt videos by reliable means so that to avoid crimes like piracy. Visual cryptography can be used to de so creating shares to be distributed among holders.
2) Visual cryptography in remote electronic voting.

VII. CONCLUSION

In this paper, a thorough study of visual cryptography methods and applications is presented. Security issues comes under consideration when their contains confidential information. As this method contains no key, it is unbreakable compared to normal cryptography. Visual cryptography have changed through time from traditional creation of shares to modern ways of encryption where traditional visual cryptography deals with creation of shares out of binary image and modern cryptography Gray-scale and color images.

In near future it can be used combined with other techniques to secure the encryption process.

REFERENCES

[1] Rizwan Shaikhv ,Shreyas Siddh, Tushar Ravekar ,Sanket Sugaonkar,"Visual Cryptography Survey International Journal of Computer Applications "(0975 – 8887) Volume 134 – No.2, January 2016
[2] A.Shilpa 2 , J.R.Vijayalakshmi 3 "A Survey On Visual Cryptography Techniques M.Siva Kumar" 1 , International Journal of Application or Innovation in Engineering & Management (IJAIEM) ISSN 2319 – 4847
[3] Lavesh G. Tambe "Survey of Visual Cryptography methods" International Journal of Infinite Innovations in Technology ISSN:2278-9057 IJIIT|Volume-III|Issue-I|2013-2014 July|Paper-11 Reg. No.:20140611|DOI:V3I1P11
[4] F. M. Mursi*, 2 May Salama, 3 Manal Mansour] "Visual Cryptography Schemes: A Comprehensive Survey "Mona international Journal of Emerging Research in Management &Technology sISSN: 2278-9359 (Volume-3, Issue-11)
[5] Naor, M. and A. Shamir. "Visual cryptography, Advances in cryptology." Eurocrypt '94 Proceeding LNCS, 950:1–12, 1995.
[6] Verheul, E.R. and H.C.A.van Tilborg. "Constructions and properties of k out of n visual secret sharing schemes. Design Codes and Cryptography

