ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

ATM Pin Transfer Using Visual Cryptography

Swati R. Shete, Prof. Yogini C. Kulkarni,

M.TECH. (I.T.) Student, Dept. of I.T., Bharati Vidyapeeth University, College of Engineering, Pune, India

Assistant Professor, Dept. of I.T., Bharati Vidyapeeth University, College of Engineering, Pune, India

ABSTRACT: The one of the Enhanced process which is nothing but visual cryptographic scheme which offers to encrypt private information in such pattern that the Human Visual System can see an original data without any algorithmic decryption, which redirects to original private information without being use of any computer peripherals. In this Technique protected Image is rending into different forms called as shares and after overlapping of these files or shares, we can get the original image.

KEYWORDS: Visual Cryptography, Computer peripherals, shares, Internet.

I. INTRODUCTION

Visual Cryptography is an effective, simple & fast mechanism which is help us to provide the security protection whenever we are going to transfer the important or sensitive data between sender and receiver. Using this technique, the recipient can't change the source and also maintains the authenticity or security of the document.

Visual cryptography considers a financial document or data that is ATM PIN number which is stored into an image that is bitmap file. This file is divided into part one and part two. Using an E-mail, these parts are distributed to the recipients. If the recipient wants to regain the original data then the recipient should have the respective subset of files or shares. [1]

In previous visual cryptography, the recovered images are much darker than the original images or the decoded images are being burry and that's why this method is not widely used. But in this proposed system, this problem is removed and the original document is reproduced or recovered very precisely. [1]

In 1994 NAOR and SHAMIR[1] presented a new cryptography which is referred as one of the method for encryption of notes which are written by hands, any pictures or any graphical black and white or color images and also of the text which is hidden in a graphical image. [1]

As this process is extremely faster with no computational peripherals as well as efficient technique which will guarantee the safety of Secret information. Visual Cryptography enables new way to protect the secret data which is needed to be hidden from unknown persons. Many systems failed to deliver the similar mechanism as Visual Cryptography. That's why this technique has been used and implemented from many years.

A. WHY TO USE VISUAL CRYPTOGRAPHY?

- To overcome the limitation of long-established Cryptography.
- Simple to Implement.
- Decryption Algorithm not required.
- Lower cost and no Computer high power required.
- Removes Graying effect.

B. *Definition of Cryptography*

Cryptography is a technique in which plaintext is encrypted into cipher text and cipher text is decrypted into plaintext with the help of the algorithms at both the end.

DOI: 10.15680/ijircce.2015.0305049

C. *Limitation of Cryptography*

If we want to decrypt the encrypted code then we should have sufficient knowledge about the decryption algorithms which may requires complex and computational calculations. To avoid this we can use Visual Cryptography which does not requires computational and complex algorithms at the decryption end and we can visualize original data by human eye.

II. Related work

This paper explains the VC Scheme which is the way to transfer the financial documents. The author has explained the fundamental or core model of VC [2, 2] Scheme which includes the encoding of secret message into two files. After overlapping of these two files we will get the original secret message. The human visual system can do the decoding process. The techniques such as resizing, post receipt threshold are used to remove the gray effect problem. The increased disk space requires [1]. The paper [2] is divided into three sections. First section gives details of important parameters such as expansion of pixels which is denoted by small letter m and the relative difference between white and black pixels in reconstructed image which is denoted by symbol α. So if m is decreased then quality will be increase but it leads to security problem. Second section describes different types of Visual Cryptography such as VC for general access, VC scheme for gray level, Recursive Threshold VC scheme, Extended VC Scheme for natural images, Halftone VC Scheme, VC scheme for colour images, Progressive VC scheme and Segment based VC scheme [2]. Third section explains to maintain security, we can increase the number of pixel expansion and number of share parameters but this affects the resolution of recovered image. The [3] paper describes the survey of Visual Cryptography for color data. The only disadvantage of this scheme is multiple shares should be created to share large amount of sensitive or confidential data. In [4] paper the author described VC [2, n] scheme may be useful for banking application. To implement VC [2, n] scheme the two important things are mentioned as every block of each share have same Hamming Weight. In [5] author has been described basic VC scheme of binary or monochrome images as well as Color VC Scheme for CMY/RGB or grey scale images using different techniques such as error diffusion, digital halftoning and wavelet which are used to convert the color image into gray and then we can apply basic VC scheme.

III. Visual Cryptography

Visual Cryptography is the simple method which provides the security to an ATM PIN while transferring it from bank to an account holder. Figure 1 depicts the one of the example of Visual Cryptography and through which we can understand the functionality or working or the concept behind the visual cryptography. We can achieve this by using the different schemes which are explained as follows:-

1. *Visual cryptographic [2, 2] scheme*: - It is the simple scheme in which an input image is divided into part one and part two. The two parts or shares are placed on one another and the original image can be recovered. [
2. *Visual cryptographic [2, N] scheme*: - The input file is divided into the 'N' number of parts or shares in such a way that after overlapping of any two or more shares, the original image can be regained.
3. *Visual cryptographic [N, N] scheme*: - The original or secret image or file is encrypted or divided into N number of files or shares and after overlapping of all that N number of files or shares, we can obtain the original image or file.
4. *Visual cryptographic [K, N] scheme*: - An input data file is encrypted into number which is greater than two parts which is denoted by letter 'N'. So we can overlap or put only the 'K' number of parts on one another and we can get output image [4].

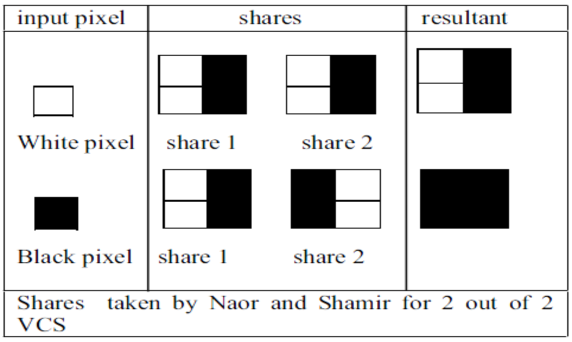

Fig. 1. Example of NAOR and SHAMIR (2,2) VCS

A. *(2, 2) Visual Cryptography Scheme (Proposed VC Scheme)*

In this model the 2 which is placed at first position denotes the minimum number of share images or files which are required to obtain an original image. Similarly the 2 which is placed at the second position denotes how many number of shares that we want to generate.

The following Fig. 2 which is helpful to understand the [2, 2] VC scheme [3].

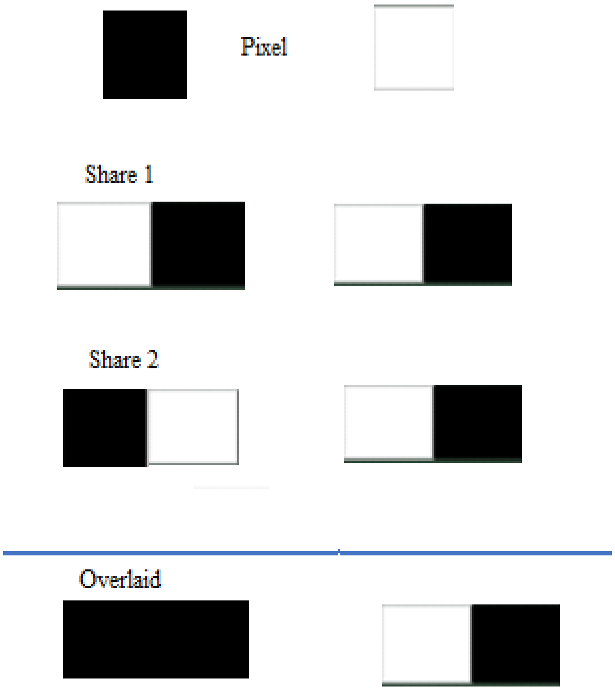

Fig. 2. (2,2) VC Scheme

The VC model is depends on the following matrices which are considered as basic matrices which covers the whole model. The whole model of this scheme can be explained by two basic or fundamental matrices and out of that one matrix is used for black pixel and another matrix is used for white pixel.

The basic or fundamental matrices of VC [2, 2] scheme are as follows:

$$B1=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad B0=\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$$

In the basic matrix, the black color means an element one and the white color means an element zero. The first row of basic matrix corresponds to the first part and second row of basic matrix corresponds to the second part which explains the process of rending the pixels from an input image into first and second share. In this scheme the first 2 tells us that how many minimum number of share images are required to obtain an original image. The two which is placed at second position denotes the total number of parts that we want to generate [5].

As earlier we have discussed that the VCS model not requires the computing peripherals to regenerate the original data and simply we can take printout of share1 and share2 on different transparencies and after overlapping of these two transparencies we will get an original image. This happens because of used properties of basic or fundamental matrices and overlapping or decryption process is an easy method in which simply we have to perform Boolean-OR operation by our human eye without the computer. Since input as black pixel generates two black pixels and after overlapping of white pixel produces one white and one black pixel which will result into darker data than original data because of extra pixels which are having black color.

B. *Properties of VCS model*

- *Pixel Expansion (m)***-:** To copy a single pixel from an original image as a combination of pixels in share1 and other combination of pixels into another share2 and this process is called as pixel expansion. The following Fig. 3. Shows the expansion process of pixels [5].

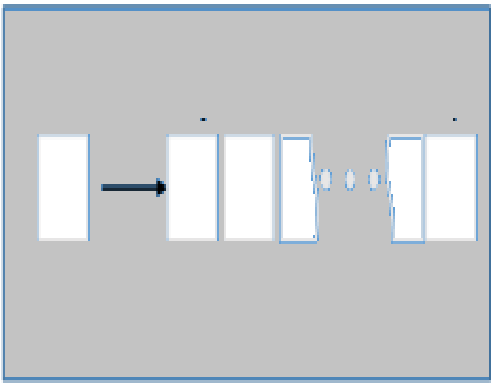

Fig. 3. Pixel Expansion process

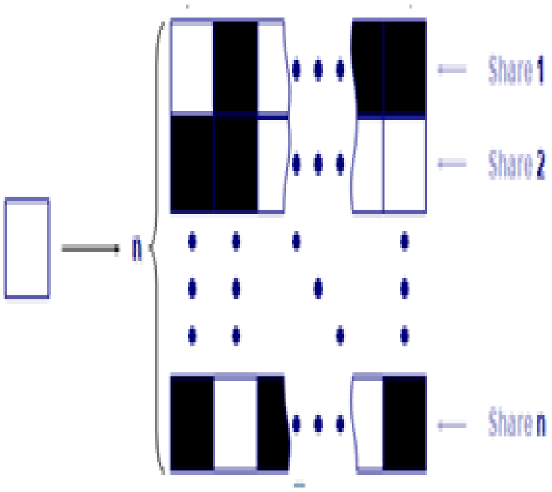

Fig. 4. Pixel Expansion for n shares

C. *Generating shares with OR operation :* Consider 1 = Black pixel & 0 =White pixel

A	B	A OR B
0	0	0
0	1	1
1	0	1
1	1	1

D. *Overlaying Shares with XOR operation :* Consider 1 = Black pixel & 0 =White pixel

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

IV. SECURING DATA IN BANKING SECTOR

Consider an example where Customer want an ATM Card of any bank suppose Bank of Maharashtra. For that purpose he needs to apply for ATM card in the respective bank. Then after some process bank transfers the ATM PIN number to the customer via postal services which leads to breach in the security systems. If PIN number which is transferred from the bank falls in hands of any unauthorized person then he may take advantage of it and he may misuse of it. So to avoid such scenarios and to protect ATM PIN number from such attack Visual Cryptography is used. In this paper I am representing the methodology as "ATM PIN transfer using visual Cryptography" & we can use it in banking Sector.

The following Fig. 5. Shows the pictorial flow of VC scheme.

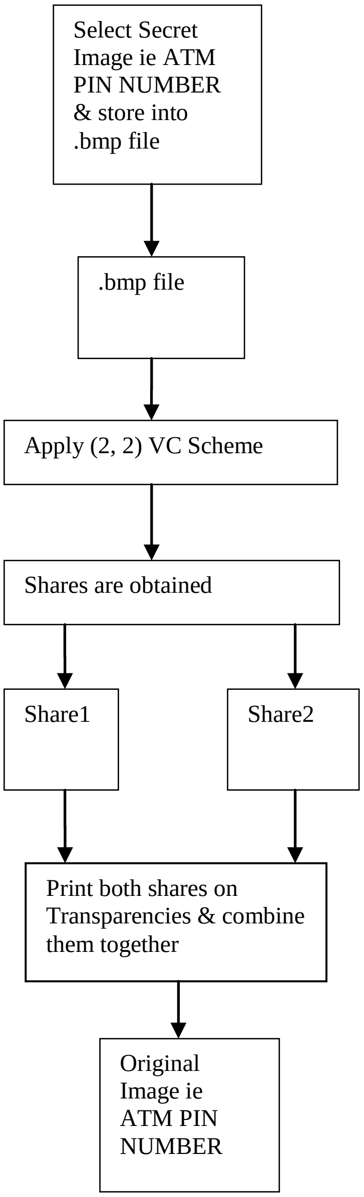
Select Secret Image ie ATM PIN NUMBER & store into .bmp file
.bmp file
Apply (2, 2) VC Scheme
Shares are obtained
Share1
Share2
Print both shares on Transparencies & combine them together
Original Image ie ATM PIN NUMBER

Fig.5. (2, 2) VC Scheme for Banking Sector

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

III. SIMULATION AND RESULTS

Fig.1. represents an original image in .BMP file format which is called as secret image. Fig. 2 and Fig. 3 represents two shares generated which are not visible. Fig. 4. Represents the output as recovered image after stacking of generated shares.

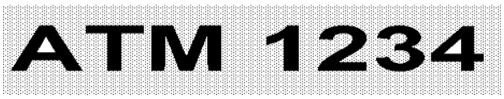

Fig. 1. Original (.BMP) Image

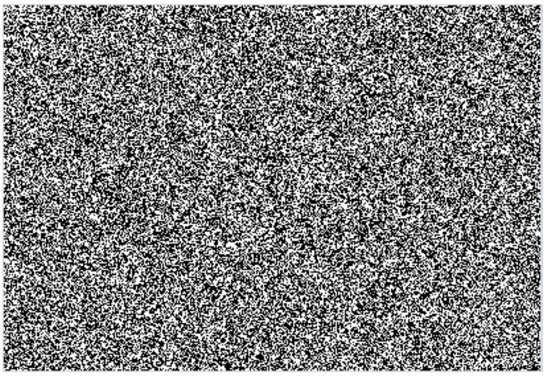

Fig. 2 Share 1

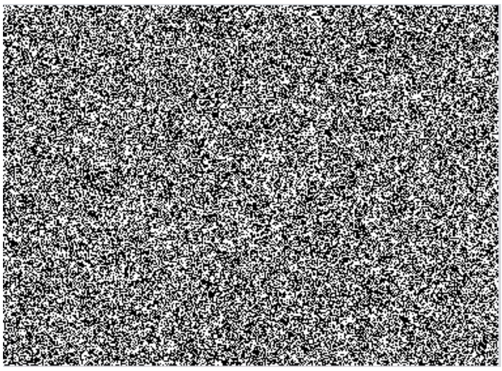

Fig. 3.Share 2

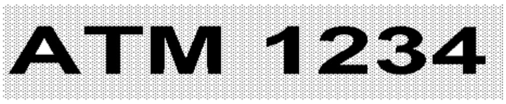

Fig. 4. Recovered Image

IV. CONCLUSION AND FUTURE WORK

We can secure Information in an image using Visual Cryptography into which an image is dividing into two shares & after Stacking we can visualize it by Human eye without any complex cryptographic Algorithm at the Decryption end. We are avoiding the distortion and the greying effect. It is used for various purposes but we are focusing on the banking application. In this the ATM PIN NUMBER image which is a BMP file is encrypted and shares are generated and after overlapping of these two shares we can recover our original image that is ATM PIN NUMBER.

Table 1: Feature, algorithm and future scope [4]

Features	Algorithm	Future Scope
Visual Cryptographic Scheme	(2.2)VC	(2,n)
Applicability in Bank sector	Maximum One Account holder	Maximum n customers
Expansion of Pixels	4times	Not Fixed

Input Number of Pixels	1	2

REFERENCES

1. L. W. Hawkes, A. Yasinsac, C. Cline, “An Application of Visual Cryptography to Financial Documents”, Florida State University, 2008.
2. Chandramathi S., Ramesh Kumar R., Suresh R., and Harish S, “An Overview of Visual Cryptography”, 2010.
3. P. S. Revenkar, Anisa Anjum, W. Z. Gandhare, “Survey of Visual Cryptography Schemes”, Government College of Engineering, Aurangabad, April 2010.
4. Jayanta Kumar Pal, J. K. Mandal and Kousik Dasgupta, “A (2, N) Visual Cryptographic Technique For Banking Applications”, Kalyani Government Engineering College, West Bengal, India, OCT 2010.
5. Sagar Kumar Nerella, Kamalendra Verma Gadi, RajaSekhar Chaganti, “Securing Images /using Colour Visual Cryptography and Wavelets.

BIOGRAPHY

MS. Swati Ramchandra Shete is a student of Master of Technology (M. Tech.) in Information Technology Department, Bharati Vidyapeeth University College of Engineering, Pune, and Bharati Vidyapeeth Deemed University under the guidance of **Prof. Yogini Kulkarni.** She received Bachelor of Engineering in I. T. (B.E. I. T.) degree in 2006 from PDVVP COE, Ahmednagar. Her research interests are Information Security, Software Engineering etc.