ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

ATM PIN Transfer Using Visual Cryptography (Implementation)

Ms. Swati Shete[1], Prof. Y. C. Kulkarni[2]

Student of M.Tech., Dept. of I. T., Bharati Vidyapeeth Deemed University College of Engineering, Pune, India.

Asst. Prof. Information Technology, Bharati Vidyapeeth Deemed University College of Engineering, Pune, India.

Abstract: The Visual Cryptography is simple technique to encrypt the confidential data in such way that decryption process can be done by human eye. The purpose of this paper is to study (2, 2) VC Scheme with an implementation and experimental results.

Keywords: Cryptography, Encrypt, Decryption, VC Scheme.

I. Introduction

The steps to understand how visual cryptographic scheme functions are explained as follows:

- To store original data that is ATM PIN number into a bitmap file.
- To generate shares that is to divide the original file into two files which is also called as share1 and share2.
- To overlap or put these two shares that is share1 and share2 on one another, so we can recover original image.
- Then we can take printout of share1 and share2 on transparencies and we can put them on each other and we can regain or regenerate the original or data.

The each and every pixel from original image is expanded into smaller subparts which can be considered as blocks. The number of white and black blocks is always same. If the pixel is going to divide into two parts then it will divide into one white and one black pixel.

Then we can ready to generate or produce the two layers or shares. Out of these two layers, layer 1 is nothing but transparent layer which includes the random pixels. The layer 2 is also same except the black color pixels when overlapped. The state of these pixels is exactly opposite to the pixels which are present in layer 1. In this example, each pixel is going to rend into four subparts. To rend pixel, we can rend it into two rectangular subparts or into circles.

II. Proposed System

The proposed is explained with the topics such as objectives, proposed algorithm, an example and conclusion and experimental results An easy way to comply with the conference paper formatting requirements

A. Objectives

- To provide security to an ATM PIN number while transferring it from bank to an account holder.
- To learn and understand the basic model of (2, 2) VC scheme.
- To learn how can we overcome the limitations of traditional cryptography?
- At the same time to maintain security and quality of original data.

B. Proposed Algorithm

- Start
- To open an application/project.
- To login by entering password for verifying authentication.
- Read an input that is ATM PIN number which is stored in monochrome (.BMP) file.
- Create two parts which are called as First and second share respectively which are unreadable.
- To take printouts of created two parts and Xerox them on transparencies.
- Overlap or stack the created two parts on each other that mean we have to perform simple Boolean OR operation.
- Reconstruct or recover an original ATM PIN number from recovered image

C. An Example of (2,2) VC Scheme

In this core model, the 2 which is placed at first position denotes the minimum number of parts which are required to obtain an original image. Similarly the 2 which is placed at second position denotes the number of parts that we want to create.

The core matrices are as follows

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

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

Consider the black pixel to be copy then dealer has to select B1 matrix. Similarly if we want to copy white pixel then we have to select B0 matrix. If we required the random

DOI 10.17148/IJARCCE.2015.4581

output, we have to permute the core matrices to obtain a set of permuted core matrices.

$$C1 = \left\{ \begin{matrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{matrix} \right\}$$

$$C0 = \left\{ \begin{matrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{matrix} \right\}$$

To copy a black pixel, we have to choose randomly one of the matrices from set C1 & first row of selected matrix to be copied in first share and second row in second share. To copy a white pixel, we have to choose randomly one of the matrices from set C0 & first row of selected matrix to be copied in first share and second row in second share. Then we can put first share on other share that means we have to do addition of pixels of first and second share which is called as overlapping or stacking process. After this process, we will get an original data. The following figure shows a flow of an example of Visual Cryptographic scheme for banking applications.

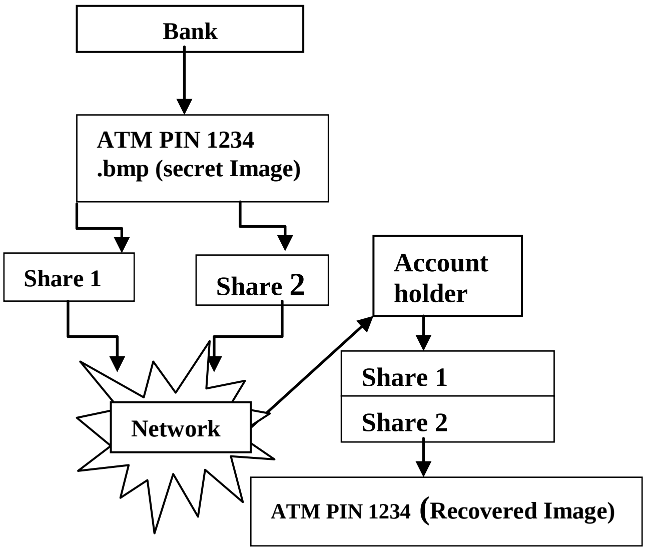


Fig.1. Example of Visual Cryptography for Banking Application

The Fig. 2 to Fig. 5 shows input image, images of two parts or shares and output image.

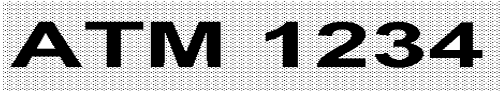


Fig.2. Secret Image (Original Image)

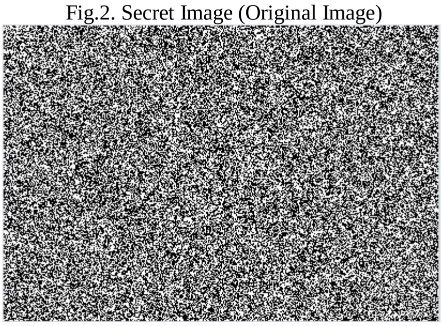


Fig.3. Share 1

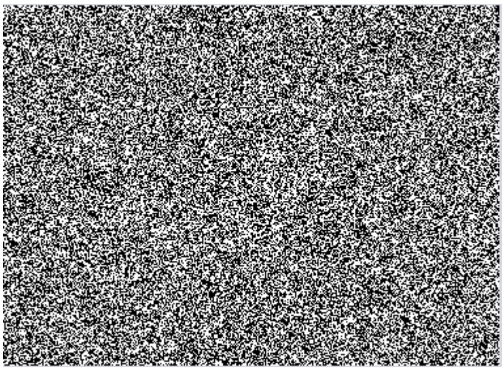


Fig.4. Share 2

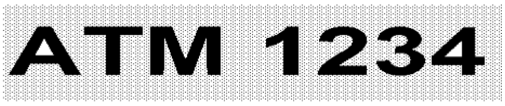


Fig.5. Recovered Image

III. OR OPERATION

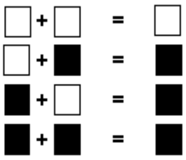
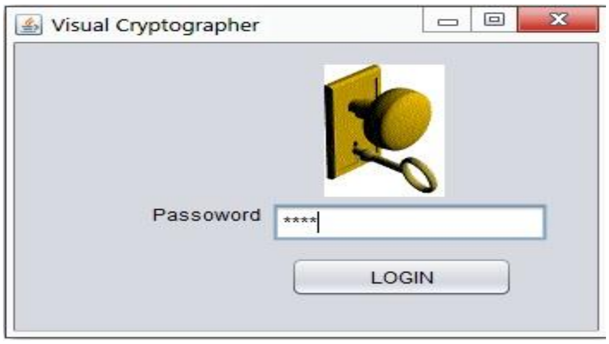


Fig. 6. Boolean OR Operation

IV. EXPERIMENTAL RESULTS



Visual Cryptographer

Password ****

Fig. 7. Login Form

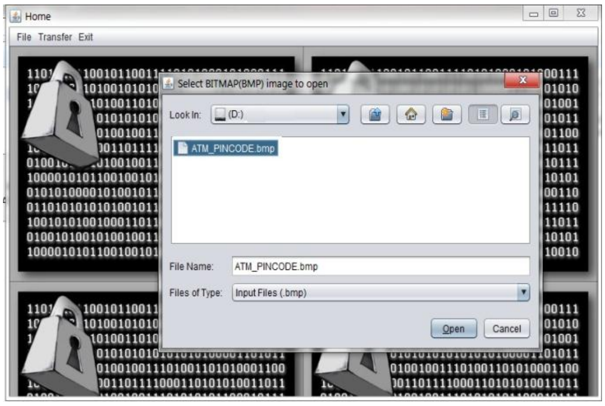
Loading

Progress: 61 % done

99%

Fig. 8. Loading

DOI 10.17148/IJARCCE.2015.4581



Select BITMAP(BMP) image to open

Look In: (D:)

ATM_PINCODE.bmp

File Name: ATM_PINCODE.bmp

Files of Type: Input Files (.bmp)

Open Cancel

Fig. 9. Select Image

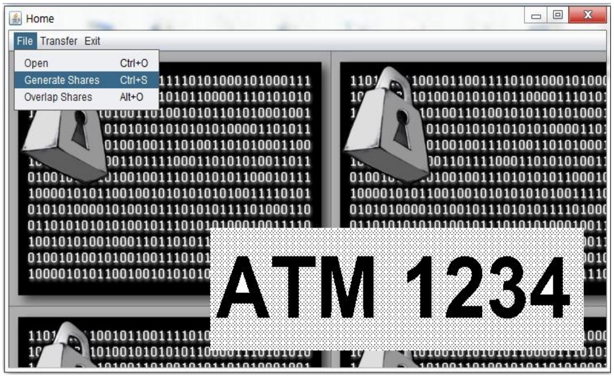


Fig. 10. Generates Shares

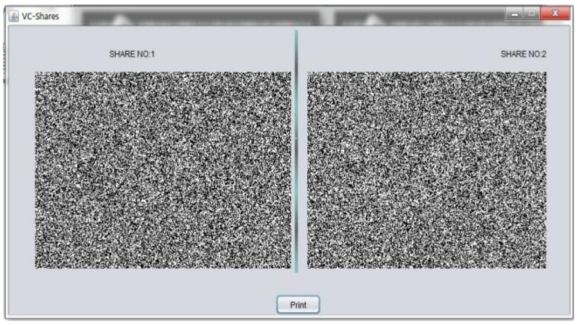


Fig.11 Share 1 and Share 2

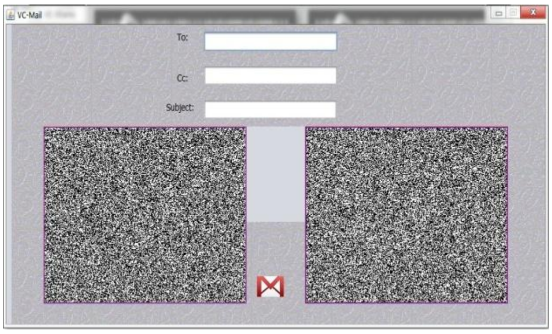


Fig. 12 Transfer of shares via Mail

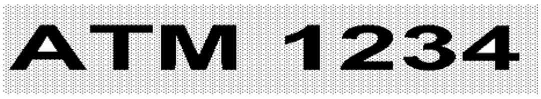


Fig. 13 Output Image

V. CONCLUSION

We can overcome on the limitation of cryptography using visual cryptographic scheme. This scheme does not require any complex and computational algorithms at the decryption and we can visualize original data by human eye.

Also we can use this concept in banking sectors. Bank provides ATM PIN number to customers via postal or courier services and if any unauthorized person will get ATM PIN number then ha can hack the account of customer and ha can misuse it and which will lead to break the security of the systems. So to avoid this or to protect our ATM PIN number, we can use VC scheme.

ACKNOWLEDGEMENT

I sincerely thanks to all authors in reference section. All papers in the reference section are very useful for my proposal. Their concepts, algorithms and techniques are very useful for my PG Dissertation. Also I sincerely thanks to **Prof. S. Z. Gawali** (Head, IT, BVDU, COE, Pune) & my project guide **Prof. Y.C. Kulkarni** (PG Coordinator, IT, BVDU, COE, Pune).

REFERENCES

[1] M. Naor, and A. Shamir, (1994) "Visual Cryptography", Advances in Cryptography-Eurocrypt '94, vis Lecture Notes in Computer Science 950, pp. 1-12.

[2] Tai- Wen Yue and, Suchen Chiang (2000) "A Neural Network Approach for Visual Cryptography", IEEE-INNS-ENNS International Joint Conference on Neural Networks, vol.5.

[3] Naor, M. and A. Shamir, Visual Cryptography, in Advances in Cryptology – Eurocrypt '94, A. De Santis, Ed., Vol. 950 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, pp 1-12, 1995.

[4] D. Jena, and S. K .Jena,(2009) "A Novel Visual Cryptography Scheme", The 2009 International Conference on Advanced Computer Control, pp- 207-211.

[5] Moni Naor and Adi Shamir, "Visual Cryptography", advances in cryptology– Eurocrypt, pp 1-12,1995.

[6] J. K. Pal, J. K. Mandal and K. Dasgupta (2010) "A Novel Visual Cryptographic Technique through Grey Level Inversion (VCTGLI)" *Proceedings of The Second International conference on Networks & Communications*, Chennai, India, pp. 124-133

[7] M. Heidarinejad, A. A. Yazdi,; K.N. Plataniotis, (2008) "Algebraic Visual Cryptography Scheme for Color Images" *IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 1761 – 1764.

[8] G.R Zhi Zhou Arce,. G. Di Crescenzo (2006) "Halftone Visual Cryptography". *IEEE Transactions on Image Processing*. , Volume: 15, Issue: 8pp- 2441-2453.

[9] A. Houmansadr, S. Ghaemmaghami, (2006) "A Novel Video Watermarking Method Using Visual Cryptography" *IEEE International Conference on Engineering of Intelligent Systems*.

[10] P. Geum-Dal,; Y. Eun-Jun,; Y. Kee-Young , (2008) "A New Copyright Protection Scheme with Visual Cryptography", *Second International Conference on Future Generation Communication and Networking Symposia*. pp. 60-63.

BIOGRAPHY

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