INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

ATM PIN PROTECTION BY USING HALFTONE VISUAL CRYPTOGRAPHY

APARNA S. KALASKAR[1], DR. H. R. DESHMUKH[2], Z. I. KHAN[3], S. S. THANGAN[3]

1. Dept. of COE, IBSS College of Engineering, Amravati, Maharashtra, India.
2. Prof. & Head, IBSS College of Engineering, Amravati, Maharashtra, India.
3. Assistant Professor, IBSS College of Engineering, Amravati, Maharashtra, India.

Abstract: In this era of technology, ATM card is the essential part of life. To have transaction ATM pin code is compulsory and it must be secure. Pin Code is transferred via Postal Services in envelop which is very easy to reveal that may be unsecure. Visual cryptography encodes a secret binary image (SI) into n shares of random binary patterns. If the shares are xeroxed onto transparencies, 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. Visual quality of the obtained halftone shares is observably better than that attained by any available visual cryptography method known to date. A technique named halftone visual cryptography is proposed to achieve visual cryptography via half-toning. Here in this paper Visual Cryptography approach which is simple, fast and provide privacy protection when sharing sensitive ATM Pin Code. In this ATM Pin Code is divided it into two shares. These shares can be transferred to the recipients via electronic mail or postal. ATM Pin Code can be obtained only when two shares combined together at receiving side by Customer.

Keywords: Visual Cryptography, Shares,Secrete binary image, Protection, Halftone.

Corresponding Author: MS. APARNA S. KALASKAR

Access Online On:

www.ijpret.com

How to Cite This Article:

Aparna Kalaskar, IJPRET, 2014; Volume 2 (9): 181-185

PAPER-QR CODE

INTRODUCTION

This paper focuses on developing a general halftone visual cryptography framework for securing an ATM PIN or any E-commerce transition, where a secret binary image is encrypted into high-quality halftone images, or halftone shares. In particular, the proposed method applies the rich theory of blue noise half-toning to the construction mechanism used in conventional VC to generate halftone shares, while the security properties are still maintained. The same contrast is obtained over the whole decoded image. The halftone shares carry significant visual information to the viewers, such as landscapes, buildings, etc. The visual quality obtained by the new method is significantly better than that attained by extended VC or any other available VC method known to date.

Visual Cryptography approach which is simple, fast and provide privacy protection when sharing sensitive ATM Pin Code. In Visual Cryptography ATM Pin Code is dividing into two bit map file shares. These shares can be transferred to the recipients via electronic mail or postal Services by taking print on transparencies individually.

The new approach consists of system which will be interconnected by bank server. System first take a user data from database and then set a ATM PIN in the from of Image, Then this Image will be divide in two share and only one share will be send to user and second share store in repository. Whenever user want to PIN he will login on site and upload its first share then system will automatically overlapped second share and user get its password or access to transition.

METHOD & MATERIALS:

This process organized as follows. The fundamental principles of visual cryptography based on which halftone visual threshold methods are proposed to construct the simplest two-out-of-two scheme and, further a general access structure scheme.

In our application we are implementing Two-out-of-Two Halftone Visual Cryptography Method to provide security to the PIN of ATM for bank customer. Here Bank User generates the two shares from image of the PIN. Then send one share to the customer (account holder). Then customer send notification about one share to the bank so that bank user knows that customer got one share. After that bank send second share to the Costumer. Shares are supposed to be copied on transparencies and decoding of the secret image is done by stacking the shares physically and customer can easily get his ATM PIN.

Visual cryptography (VC) allows the decoding of concealed images without any cryptographic computation. Particularly in a k-out-of-n visual secret sharing scheme (VSS), a secret image is

cryptographically encoded into n shares. Each share resembles a random binary pattern. The n shares are then Xeroxed onto transparencies respectively and distributed among n participants. The secret images can be visually revealed by stacking together any k or more transparencies of the shares and no cryptographic computation is needed. However, by inspecting less than k shares one cannot gain any information about the secret image, even if infinite computational power is available. Therefore we can use this technique to give security to PIN of ATM for bank customer.

Problem Definition: To provide high security to the bank customer's Personal identification number (PIN) using Halftone Visual cryptography method. In this method we divide encoded secret binary image (SI) into two shares.

1)Bank User: - Bank Use selects customer information from database and enters the PIN of respective customer. Then PIN image is generated by system. Here Bank User generates the two shares from image of the PIN form application. Then send one share to the customer (account holder). Then customer send notification about one share to the bank so that bank user knows that customer got one share.

1) User Registration:-In this module a bank user gets registered to our application with his details and his password. For this he enters all the mandatory information which is require for registration. This information will manipulate into database safely.

2) Login:- Here the registered users are trying to logging in with their registered user name and the password. If the user is authenticated he can successfully logged in otherwise restricted. Random Share Creation:-The message consists of black and white pixels. Each pixel appears in n shares, one for each transparency. The share is a collection of m black and white sub-pixels.

3) Half-toning Greyscale Image:- Half-toning process converts a continuous-tone image (greyscale image) into a binary valued image using algorithms like Error diffusion. Using the secret image and multiple greyscale images, halftone shares are generated such that the resultant halftone shares are no longer random patterns, but take meaningful visual images.

4) Decoding Image:- Shares are supposed to be copied on transparencies and decoding of the secret image involves stacking the shares physically. After that bank send second share to the Costumer. Shares are supposed to be copied on transparencies and decoding of the secret image is done by stacking the shares physically. When bank customer gets both shares he can decode the image and get the PIN.

5) Decoding Image:- Shares are supposed to be copied on transparencies and decoding of the secret image involves stacking the shares physically. After that bank send second share to the

Costumer. Shares are supposed to be copied on transparencies and decoding of the secret image is done by stacking the shares physically. When bank customer gets both shares he can decode the image and get the PIN.

RESULT :-

The shares are of better quality means better secret hiding and hence the quality of the secret image can be traded off for better secrecy.

Error diffusion algorithm is use to achieve improved halftone image quality in each developing a general halftone visual cryptography framework, where a secret binary image is encrypted into high-quality halftone images, or halftone shares.

The shares are of better quality meanbetter secret hiding and hence the quality of the secret image can be traded off for better secrecy. By stacking the two shares bank customer can easily decode the PIN code.

It is time saving application for user. In particular, here method applies the rich theory of blue noise half-toning to the construction mechanism used in conventional VC to generate halftone shares, while the security properties are still maintained. The same contrast is obtained over the whole decoded image. The visual quality obtained by the new method is significantly better than that attained by extended VC or any other available.

In the future work, we will try to provide high security by applying advanced encryption algorithm. We will improve the ATM pin protection Technique for sending a public and private key by using Halftone Visual Cryptography and it will be use in mobile banking by using some special authorized proxy server and also use for storing large database. Our approach is to provide a scheme that will be able to satisfy the user needs and requirements.

CONCLUSION:-

Our study helps for secured ATM PIN using Halftone VC, And also provides a security to E-Commerce transition by Using halftone VC algorithm .In terms of future work, you will improve the same Technique for sending a public and private key by using Halftone VC. Here, a general framework of halftone visual cryptography is proposed. Applying the rich theory of blue noise half-toning into the construction mechanism of conventional VC, the proposed method generates visually pleasing halftone shares carrying significant visual information. The obtained visual quality is better than that attained by any other available VC method known to date. The new method can be broadly used in a number of visual secret sharing applications which require high-quality visual images, such as watermarking, electronic cash, etc.

REFERRENCES:-

1. Zhi Zhau, Member, IEEE, Gonzab R. Arce, Fellow, IEEE and Giovanni Di Crescenzo, "Halftone Visual Cryptography" IEEE Transactions on Image Processing, Vol 15, No.8, August 2006

2. M. Naor and A. Shamir, "Visual cryptography," Adv. Cryptol: EURO- CRYPT, Lecture Notes Comput. Sci., vol. 950, pp. 1 –12, 1995.

3. Visual cryptography II: Improving the contrast via the cover base," in Security in Communication Networks, Lecture Notes in Computer Science. Amalfi, Italy: , 1996, vol. 1189, pp. 197–202.

4. G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," Theoret. Comput. Sci. , vol. 250, no. 1–2, pp. 134–161, 2001.

5. Paper Referred: "ATM pin protection using visual cryptography" by Subodh Bobade, Vishal Mane, Arvind Das, Rahul Dargawat; Dept. of computer engg ,Pune Univ, India.