ISSN 2395-1621

Secure Transaction :An Credit Card Fraud Detection System Using Visual Cryptography

[#1]Prajakta Akole, [#2]Nikita Mane, [#3]Komal Shinde, [#4]Prof. Swati A. Khodke

[1]prajaktaakole@gmail.com
[2]niksmane.07@gmail.com
[3]komalshinde1440@gmail.com
[4]swatikhodke@gmail.com

[#123]Deparment of Computer Engineering
[#4]Prof. Department of Computer Engineering
JSPM's
BSIOTR, Wagholi, Pune, India.

ABSTRACT

Rapid progress in the electronic commerce technology, the use of credit cards has increased. As credit card becomes the most accepted mode of payment for both online as well as regular purchase, cases of credit card fraud also rising. The application for the credit cards is depended on internet. The applications in above cases found fraud and is a specific case of identity crime. Credit Card Fraud is the most common, prevalent and costly crime in existence these days. A multilayered detection system which is entirely data-mining based and they deal with real social relationships and finds spikes in duplicates and finally assigns doubtful scores which help in identifying the fake. However, this has certain limitations. A new system is been proposed by using Visual Cryptography to Generate OTP for efficient and to reduce economic losses. The system is totally concerned with credit card application fraud detection by performing the process of visual cryptography and grey scales We propose an credit card fraud detection system that utilizes Visual Cryptography to Generate OTP for efficient transaction and to reduce economic losses. The system is totally concerned with credit card application fraud detection by performing the procedure of visual cryptography and grey scales to overwhelm the disadvantage mentioned previously in the existing systems.

Keyword: **Credit Card Fraud, Visual Cryptography, Security, Grey Scales, Thresholding, OTP.**

ARTICLE INFO

Article History

Received :18th October 2015

Received in revised form :

18th October 2015

Accepted : 22th October , 2015

Published online :

23th October 2015

I. INTRODUCTION

In present world carrying heavy cash is not easily manageable and even risky too. Therefore, for better safety and convenience credit cards are used. A credit card is a payment card issued to users as a system of payment. Credit card is the plastic card which gives approval to the buyers to purchase goods by borrowing money from the financial institution within the given eligible maximum value. Credit Card is also known as plastic money. It is a payment card issue to users as a system of payment. It permits the cardholder to pay for goods and services based on the holder's promise to get hold of them. The issuer of the card creates a rotating account and grants a line of credit to the consumer from which the user can borrow cash for payment to a merchant or as a cash advance to the user. Now days,credit card transaction and online money transfer have been improved rapidly. Therefore, there is threat from third party or unauthorized party accessing secret information has been an still existing concern for the data communication experts. With the rapid advance in the system topology, multimedia data can be transmitting over the Internet conveniently. In order to deal with the security issue of credit card transaction, we are in need of an appropriate secure method of transaction by which we can secure our transaction over the internet. With the help of OTP generation by Visual Cryptography using share generation, the transaction can be securely done over the internet.[1]

Credit card fraud detection system allows users to perform transaction securely using an OTP. The term one-time password (OTP) is an automatically generated numeric or alphanumeric string of characters that authenticates the user for a single transaction or session. An OTP is more safe than a static password, especially a user-created password, which is typically weak. OTPs may replace confirmation login information or may be used in addition to it, to add another layer of security. OTP tokens are typically pocket-size fobs with a small screen that displays a number. The number changes every 30 or 60 seconds, depending on how the token is configured.

In this paper, we propose an credit card fraud detection system based on the concept of Visual Cryptography for OTP [1].Visual cryptography is a cryptographic method which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a automatic operation that does not require a computer.

Visual Cryptography (VC) is one of the encryption method that is used to encrypt secret images in such a way that it can be decrypted by the individual visual system if the correct key images are used. The technique was first proposed by Moni Naor and Adi Shamir [2] in 1994. According to them Visual Cryptography is a method of encrypting a undisclosed image into shares such that stacking a adequate shares of secret image reveal the original image. Shares are usually binary images presented in transparencies. Unlike, when compared to presented traditional cryptographic methods,Visual Cryptography needs no complicated calculation for recovering the secret image. The decryption method is to merely stacking the shares and view the original (secret) image that appears on the stacked shares. The method Visual Cryptography is being used for secret transfer of images in military, hand written documents, text images.[1]

In section II, we describe system components and workflow. We then describe the proposed access control system in section III. System implementation and results are given in section IV, and section V concludes this paper.

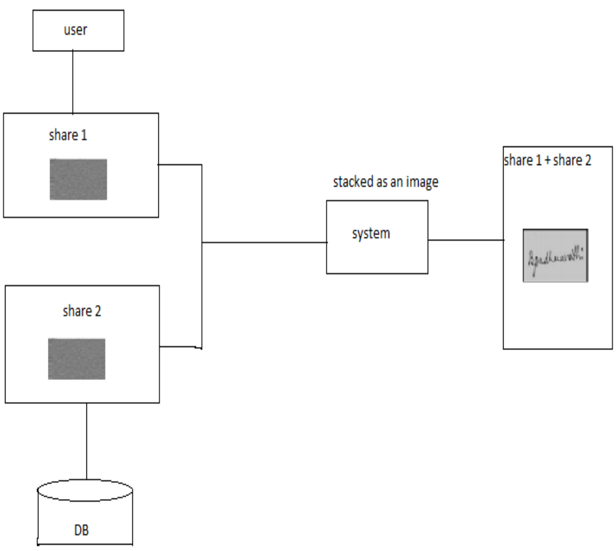

Fig1. Visual Cryptography applied in system.

II. VISUAL CRYPTOGRAPHY

Steganography is the art of hiding of a message within another so that hidden message is indistinguishable. The key concept behind steganography is that message to be transmitted is not detectable to casual eye. Text [4], image [5], video [6], audio [7] are used as a cover media for hiding data in steganography. In text steganography, message can be hidden by shifting word and line [4], in open spaces [8], in word sequence [9]. Properties of a sentence such as number of words, number of characters, number of vowels, position of vowels in a word are also used to hide secret message. The advantage of preferring text steganography over other steganography techniques is its smaller memory requirement and simpler communication [10]. Visual Cryptography (VC), proposed by Naor et al. in [11], is a cryptographic technique based on visual secret sharing used for image encryption. Using k out of n (k, n) visual secret sharing scheme a secret image is encrypted in shares which are meaningless images that can be transmitted or distributed over an untrusted communication channel. Only combining the k shares or more give the original secret image.

III.SYSTEM COMPONENTS AND WORKFLOW

A. The following subsections describe methods for OTP generation using visual cryptography.

1. Gray Scale

In a (8-bit) grayscale image all picture element has an assigned intensity that ranges from 0 to 255.A grey scale image is unlike from black and white image since a grayscale image also includes shades of grey distant from unadulterated black and pure white color. Grayscale images are generally required for image processing.To transform a colour image into gray scale we use gray scaling algorithm. Each colour pixel is described by a triple (R, G, B) intensities for red, green and blue, we have to map that to a single number giving a grayscale value.

Calculate grayscale component

$$(R + G + B) / 3$$

Fig 2. Color – Grayscale

Steps for RGB to Grey Scale alteration:

– Traverse through entire input image array.
– Examine each pixel color value (24-bit).

– Split the color value into each R, G and B 8-bit values
–Calculate the grayscale part (8-bit) forgiven R, G and B pixels using a alteration formula.
–Compose a 24-bit pixel value beginning 8-bit gray scale value.
– Store the new value at same place in output

2. Thresholding of Image

Thresholding is the simplest process of image segmentation. From a grayscale image, thresholding can be used to create binary images i.e. image with just black or white colors. It is usually used for feature extraction where required features of image are transformed to white and everything else to black. (or vice-versa). It is an image processing technique for converting a grayscale to a binary image based upon a threshold value. If a pixel in the image has a gray level value which is less than the threshold value, the corresponding pixel in the resultant image is set to be black.
Otherwise, if the gray scale value of the pixel is greater than or equal to the threshold intensity, the resulting pixel is set to be white. Thus creating an image with only 2 colors. Image Thresholding is very useful for keeping the significant part of an image and getting rid of distorted image caused by noise. This holds true under the assumption that a reasonable threshold value is chosen.

Steps for Thresholding Image:

– Traverse through entire input image array.
– Examine each pixel color value (24-bit) and alter it into grayscale.
– Calculate the binary output pixel value (black or white) based on existing threshold.
– Store the new value at same position in output image.

```
Thresholding Logic
GS = (r+g+b) / 3; // grayscale
if(GS < th) {
pix = 0; // pure black
}else {
pix = 0xFFFFFF; // pure white
}
```

Fig 3. Grayscale – Threshold

3. Visual Cryptography

It is a kind of secret sharing scheme that focuses on sharing secret images. The basic idea of the visual cryptography scheme is to split a secret image into number of random shares (printed on transparencies) 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 the shares.
Visual Cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Both transparent images or layers are required to reveal the information.
4. Share Generation (2,2) Threshold VCS scheme:- This is a simplest threshold scheme that takes a secret message and encrypts it in two different shares that reveal the secret image when they are overlaid. No additional information is required to create this kind of access structure.
In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares. Fig. 2 denotes the shares of a white pixel and a black pixel. Note that the choice of shares for a white and a black pixel is randomly determined (there are two choices available for each pixel). Neither share provides any clue about the original pixel since different pixels in the secret image will be encrypted using independent random choices. When the two shares are superimposed, the value of the original pixel P can be determined. If P is a black pixel, we get two black sub pixels; if it is a white pixel, we get one black sub pixel and one white sub pixel.

IV. PROPOSED SYSTEM

In the Proposed System Sign In from the Client PC after successful verification Browse products and services, select service then enter the credit card detail. The credit card data is entered which is send to the server to process request received from the client. Mining is done to check the credit card details entered are checked with previous transactions done through credit card. On successful verification request is processed. The credit card details found suspicious then Generate OTP.

In the proposed system for secure transaction OTP is generated, image of OTP is created and gray scaling is done on the image after that thresholding of image is done to reduce the complexity to store the image data. Generate the share of the thresholded image the shares are send to the customer purchasing the products through mail and other share is sent on the User Interface.

The share received from the mail is uploaded and both the shares are superimposed to generate the OTP image. The original OTP image is verified with the OTP image gendered after superimposition of shares if the images are successfully verified then process the transaction or else lock the account.

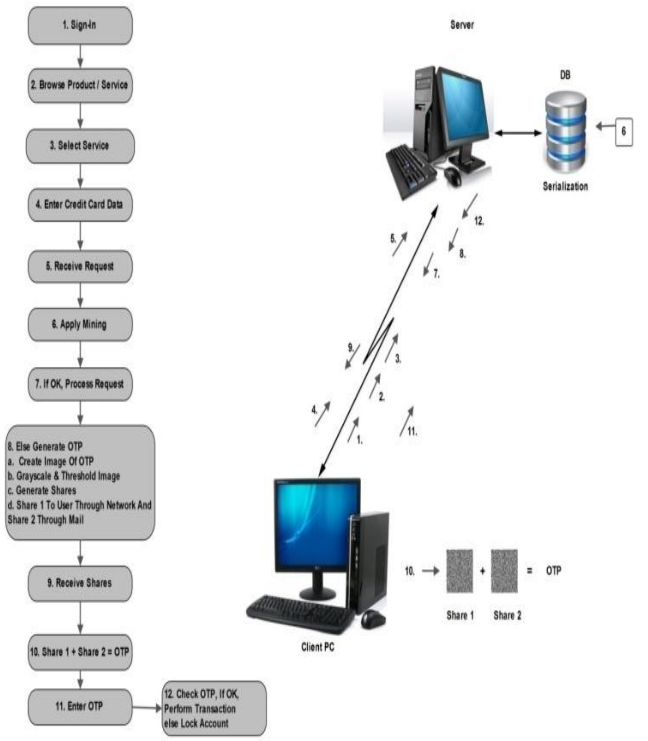

Fig 4. System Workflow

V. ADVANTAGES AND APPLICATION

Advantages:

- Minimize the Credit Card Fraud.
- Safeguarding customer data
- Increasing customer confidence
- Preventing identity theft.

Application:

- Biometric security
- Watermarking
- Steganography
- Remote electronic voting
- Bank customer identification

VI. CONCLUSION

In this paper, we have proposed an Credit Card fraud detection system based on the concept of OTP generation using Visual Cryptography [1]. The proposed system utilizes Visual Cryptography to generate OTP using share generation to overcome the disadvantage exhibited by the credit card fraud detection system using threshold value calculation. This system has been introduced as a trade off balance between security and convenience. If the level of security increases, the level of convenience decreases and vice versa. This is true as a secure system typically is a complex system and requires complex algorithms which will eventually sacrifice the convenience. An insecure system, on the other hand, performs simple algorithm, thus convenience is dominant.

REFERENCE

[1]"A Secure Visual Cryptography Scheme for Sharing Secret Image using RSA" International Journal of Innovative Research in Computer and Communication Engineering ,Vol. 3, Issue 4, April 2015.

[2]Divya James.; Mintu Philip.;"A Novel Anti Phishing framework based on Visual Cryptography", in Proceedings of Power, Signals, Controls and Computation (EPSCICON), 2012.

[3]M. Naor and A. Shamir "Visual Cryptography". Advances in Cryptology EUROCRYPT "94. Lecture Notes in Computer Science, (950):1–12, 1995.

[4] Jack Brassil, Steven Low, Nicholas Maxemchuk, Larry O'Gorman,"Hiding Information in Document Images," Proceedings of the 1995 Conference on Information Sciences and Systems, Johns Hopkins University, pp. 482-489, 1995.

[5] J. Chen, T. S. Chen, M. W. Cheng, "A New Data Hiding Scheme in Binary Image," Proceeding of Fifth International Symposium on Multimedia Software Engineering, pp. 88-93, 2003.

[6] Hu ShengDun, U. KinTak, "A Novel Video Steganography Based on Non-uniform Rectangular Partition," Proceding of 14th International Conference on Computational Science and Engineering, pp. 57-61, Dalian, Liaoning, 2011.

[7] Daniel Gruhl, Anthony Lu, Walter Bender, "Echo Hiding," Proceedings of the First International Workshop on Information Hidding, pp. 293-315, Cambridge, UK, 1996.

[8] Walter Bender, Daniel Gruhl, Norishige Morimoto, A. Lu, "Techniques for Data Hiding," IBM Systems Journal, Vol. 35, Nos. 3 & 4, pp. 313- 336, 1996.

[9] K. Bennet, "Linguistic Steganography: Surevey, Analysis, and Robustness Concerns for Hiding information in Text," Purdue University, Cerias Tech Report 2004—2013.

[10] J.C. Judge, "Steganography: Past, Present, Future," SANS Institute, November 30, 2001.

[11] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptograhy: EUROCRYPT'94, LNCS, vol. 950, pp. 1–12, 1995

