Trio Framework for Secure Online Transaction Using Visual Cryptography

Khadija Kaousar M A

MTECH in Computer Science and Engineeringg
Dr. Ambedkar Institute of Technology
Bangalore, India
khadija.kaousar@gmail.com

***Abstract*-** Nowadays as online transaction are becoming very common, a numerous number of attacks are been designed each day. Among them, phishing is the most popular attack. Phishing is a technique of hosting fake website in an attempt to get personal confidential information such as passwords, credit card information from unsuspecting victims for identity theft, financial gain and other fraudulent activities. As the phishing is becoming a serious threat for the online transaction. I present a preventive mechanism to overcome the phishing by the use of biometric along with the combination of visual cryptography. Image captcha along with the OTP helps us identify the fake website. This approach also authenticates the user. Biometric authentication systems are used to authenticate users. The use of steganography preserves the whole of integrity.

***Index Terms*-** biometrics, image captcha, iris, phishing, steganography, visual cryptography

I. Introduction

Due to a substantial increase in internet content and resources, coupled with the evolution of communications, surfing social network sites and online transaction are nowadays becoming very common and there are various attacks are designed for these. In these types of various attacks, phishing is identified as a major security threat and new innovative ideas are arising for this by each passing second. Phishing is a form of online identity theft that aims to steal sensitive information such as online banking passwords and credit card information from users. Phishing scams have been receiving extensive press coverage because such attacks have been escalating in numbers and sophistication. One definition of phishing is given as “it is a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication”. Another definition of phishing, states that it is “the act of sending an email to a user falsely claiming to be an established legitimate enterprise into an attempt to scam the user into surrendering private information that will be used for identity theft”. Identity theft can be described as “a crime in which the impostor obtains key pieces of information such as Social Security and driver's license numbers and uses them for his or her own gain”. Phishing [1] attacks rely upon a mix of technical deceit and social engineering practices. In the majority of cases the phisher must persuade the victim to intentionally perform a series of actions that will provide access to confidential information. In all cases the phisher must impersonate a trusted source (e.g. the helpdesk of their bank, automated support response from their favorite online retailer, etc.) for the victim to believe. To date, the most successful phishing attacks have been initiated by email – where the phisher impersonates the sending authority (e.g. spoofing the source email address and embedding appropriate corporate logos). For example, the victim receives an email supposedly from support@mybank.com (address is spoofed) with the subject line 'security update’, requesting them to follow the URL www.mybank-validate.info (a domain name that belongs to the attacker – not the bank) and provide their banking PIN number.
In order to combat phishing attacks, many solutions have been proposed, such as HTTPS/TLS [6] or Sign-In Seal [9]. Sign-In Seal requests users to upload a picture and to save authentication information in cookies. The browser will show the picture when user logs in the server next time. The disadvantage of Sign-In Seal is that it is ineffective when the cookies are deleted or the user changes computers then visits the website again. On the other hand, HTTPS/TLS uses the X.509 certificate to identify the server. In such a way, verification of the server certificate is demanded, which is a complicated process and is inconvenient for users. In addition, there are also many B/W lists, for instance, that detect phishing websites in APWG [2]. However, the new phishing website will be not immediately detected since it is not recorded in a B/W list. Even though laws prohibit phishing attacks, attacks are still inevitable. As a result, it is nearly impossible to be sure whether computer that is connected to the internet can be considered trustworthy and secure or not. Phishing scams are also becoming a problem for online banking and e-commerce users. The question is how to handle applications that require a high level of security. So here I introduce a new method which can be used as a safe way against phishing which is named as "Trio Framework for Secure Online Transaction Using Visual Cryptography". During the authentication, the server authenticates to the users, but sensitive information about users need aren’t transferred to the server. In this approach website cross verifies its own identity and proves that it is a genuine website (to use bank transaction, E-commerce and online booking system etc.) and by the use of biometric user proves its identity to the server and this make both the sides of the system secure as well as an authenticated one.
This paper is organized as follows: Section II deals with the related work using Visual Cryptography and biometric authentication and Section III & IV presents the current and proposed Methodologies. Section V presents the implementation and Section VI deals with Results and Discussions. Section VII contains the conclusion.

II. Related Work

In this section, the related techniques that include VSS [5], CAPTCHA [7], BIOMETRIC SYSTEM, OTP, and STEGANOGRAPHY are reviewed respectively as follows:

A. Visual Secret Sharing

Cryptography is the art of sending and receiving encrypted messages that can be decrypted only by the sender or the receiver. Encryption and decryption are accomplished by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the message. Naor and Shamir [5] introduced the visual cryptography scheme (VCS) as a simple and secure way to allow the secure sharing of images without any cryptographic computations. This scheme is referred to as the *k*-out-of-*n* VCS which is denoted as (*k*,*n*)VCS. Given an original binary image, it is encrypted in *n* images, such that

$T = S_{h1} \cdot \; S_{h2} \cdot \; S_{h3} \cdot \; \ldots\ldots\ldots\ldots\ldots \; S_{hn}$ (1)

where Å is a Boolean operation, S_{hi}, h_i Î 1,2,….*k* is an image which appears as white noise, *k* d” *n*, and *n* is the number of Noisy images. It is difficult to decipher the secret image *T* using individuals S_{hi}'s . The encryption is undertaken in such a way that *k* or more out of the *n* generated images are necessary for reconstructing the original image *T* . In the case of (2, 2)VCS, each pixel *P* in the original image is encrypted into two sub pixels called shares. For biometric privacy, here 2-out-of-2 scheme is given .In this scheme for sharing a single pixel p, in a binary image Z into two shares A and B is illustrated in Table I.

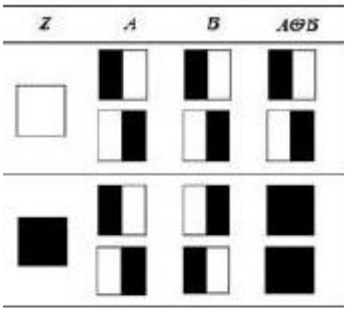

Table I: encoding a binary pixel p into share A&B

If p is white, one of the first two rows of Table 1 is chosen randomly to encode A and B. If p is black, one of the last two rows in Table 1 is chosen randomly to encode A and B. Thus, neither A nor B exposes any clue about the binary color of p. When these two shares are superimposed together, two black sub pixels appear if p is black, while one black sub-pixel and one white sub-pixel appear if p is white as indicated in the rightmost column in Table 1. Based upon the contrast between two kinds of reconstructed pixels can tell whether p is black or white.

B. CAPTCHA

Nowadays attackers usually use robot software to simulate user's behavior. For example, hackers may register the same server with different accounts or execute repeatable action. As a result, the system would be occupied for heavy loading. CAPTCHA [7] is the technique that uses rotating, resizing, distorting, truncating, noise and variant to interfere with pictures with words. CAPTCHA can prevent attackers from using Optical Character Recognition (OCR) technique to identify the words. Only human can recognize those words on CAPTCHA image through Human Visual System (HVS). By using CAPTCHA, it is easy to determine whether a user participating in the process that recognizes the words on CAPTCHA image. CAPTCHA is usually used in free email registration, message postings, and e-commerce systems to prevent robot software.

C. Biometric Authentication

Since biometric information need not be memorized, biometric-based authentication currently has become popular and widely used to differentiate legitimate user from pretender. The biometric person authentication technique based on the human iris is well studied to be applied in any access control system requiring a high level of security. In this paper a system for personal verification based on iris patterns is presented. Iris recognition technology combines computer vision, pattern recognition, statistical inference, and optics. Its purpose is real-time, high confidence recognition of a person's identity by mathematical analysis of the random patterns that are visible within the iris of an eye from some distance. Because the iris is a protected internal organ whose random texture is complex, unique, and stable throughout life, it can serve as a kind of living passport or password that one need not remember but can always present. Because the randomness of iris patterns has very high dimensionality, recognition decisions are made with confidence levels high enough to support rapid and reliable exhaustive searches through national-sized databases. The algorithms for iris recognition were developed at Cambridge University by John Daugman [4].The verification algorithm, which consists of image processing to obtain iris information, iris normalization, feature extraction, and person verification. Filters are used for feature extraction. From such result iris bit template sequence is encoded. Then the Hamming distance is calculated from the iris template, which gives the estimate of the match in the verification process. Since biometric information need not be memorized, biometric-based authentication currently has become popular and widely used to differentiate legitimate user from pretender.

D. One-Time Password

In password-based authentication system, the server checks whether the password entered by the user is the same as saved one. User's personal information would be misused if the password is stolen. In order to address this issue, OTP is proposed. OTP can only be used once, and there's no relation between any two OTPs. On the other hand, if the attacker captures the OTP this time, she/he cannot login the server by reply attack. Moreover, the attacker cannot get any sensitive information about the user from intercepting OTP.

E. Steganography

Steganography [11] is art of hiding information inside information. Steganography can be applied to different types of media including text, audio, image, video, etc. However, text steganography is considered to be the most difficult kind of steganography due to the lack of redundancy in text as compared to image or audio . In our process the pin number of the user is hidden into the user iris template which avoids the weak links of the biometric system.

III. Current Methodology

In the current scenario as shown in the Fig. 1, when the end user wants to access his confidential information online (in the form of money transfer or payment gateway) by logging into his bank account or secure mail account, the person enters information like username, password, credit card no. etc. on the login page. But quite often, this information can be captured by attackers using phishing techniques (for instance, a phishing website can collect the login information the user enters and redirect him to the original site). There is no such information that cannot be directly obtained from the user at the time of his login input. And user has no way of making sure the website is authenticate or not.

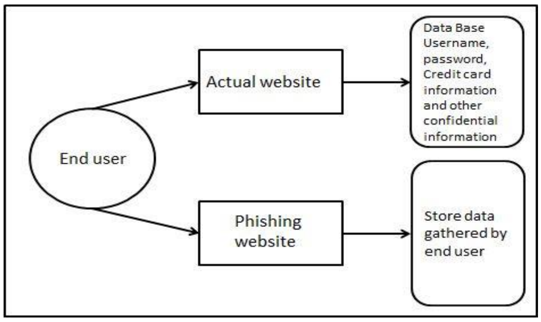
End user
Actual website
Phishing website
Data Base Username, password, Credit card information and other confidential information
Store data gathered by end user

Fig.1 Current scenario

IV. PROPOSED METHODOLOGY

For phishing detection and prevention, we are proposing a new methodology to detect the phishing website. Our methodology is based on the Anti-Phishing Image Captcha and OTP validation and biometric verification scheme using visual cryptography and steganography. It prevents password and other confidential information going to fake websites and also verify the user to the genuine website.

The proposed approach can be divided into twophases:

A. Enrollment Phase

B. Login Phase

The notations used throughout the paper are listed as follows:

EI$_i$*:* input eye image of the user

UD$_{i:}$ an unique identity of user

PC$_{i,}$: a unique pincode of user

VC(.): visual cryptography function.

VAR(.): variation of pincode generation function

A. *Enrollment Phase*

If a user visits a website first time, the user must register at the server. Assume that the connection between the user and the server in the registration is in a secure channel .Firstly the user details is asked such as username, date of birth, user phone number, email id, location. And then the user's eye image is scanned and a template is derived. Server generates a unique pincode and userID, and stores this along with other details in the database at the time of registration at the database of the secure website. The variations of pin code is generated which is the combination of pincode and details provided by the user. Meanwhile the iris image is steganographed with pincode and then shares are generated. Out of the two share only one share1 is stored at the database and other share2 is discarded. The userID, pincode and its variation are sent to the user. The user details, pincode and its variation, share1are stored in the actual database of any confidential website as confidential data. The pincode variations are used to verify the website during login phase. Figure 2 shows the enrollment stage .

Enrollment process is depicted as:

1)User→Server: *name,details, EI*$_{i,,}$

The user will make a registration request as follows:

1-1) input the name

1-2) Scan the input eye image .EIi

1-3)details such as date of birth, location, phone number, mail

2) Server→User: UD$_{i,}$*PC*$_{i,}$

Upon receiving the registration request from the user, the server performs the following tasks:

2-1) Output the userID UD$_{i,}$ pincode *PC*$_i$

2-2)Steganography the EIi with the *PC*$_i$ and generate the shares VC(EIi). Discard the share2.

2-3)Compute variation of *PC*$_i$ *VPC*$_i$=VAR(*PC*$_{i,}$details)

2-4) Record IDi, *PC*$_i$ *VPC*$_{i,}$share1 .

2-5) send the IDi, *PC*$_i$ *VPC*$_i$ to the user.

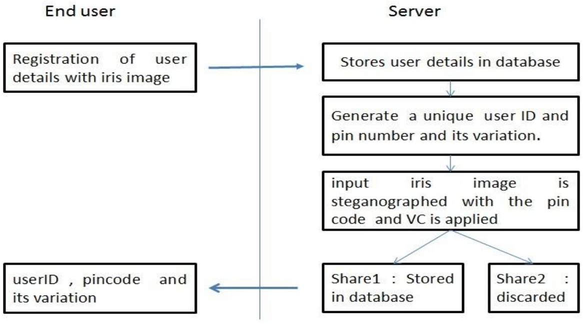
End user
Server
Registration of user details with iris image
Stores user details in database
Generate a unique user ID and pin number and its variation.
input iris image is steganographed with the pin code and VC is applied
Share1 : Stored in database
Share2 : discarded
userID , pincode and its variation

Fig.2 Enrollment Stage

B. *Login Phase*

1-1) WEBSITE VERIFICATION

When the user logs in, user inputs his/her userID. And then user is asked to input the OTP which is sent to the user's registered phone or mail. Website cross check the OTP send by user with its own if it matches ,it produces a captcha whose text will be one of the variations of pincode. User checks this pincode text on captcha and verifies the pincode is the valid one and enters the text present in it. If valid it can be confirmed that website is genuine. User text is crossed check with the input text. If same then it can be concluded that user is not a machine. The end user can confirm whether the website is genuine or fake by 1. By receiving the OTP to its mail or phone since only genuine website will be having this information 2. The variations of pincode are unique and are known only to user and genuine website. If the website is fake, then it'll fail in the above steps. Even by not sharing single personal details , user is still able to verify the website is fake or genuine .hence even if the website is phished , user loses no personal details and can successful know the identity of the website . Only when the user has the confident in the website he/she preform the next step.

*1-2)*USER AUTHENTICATION

User is asked to input the redundant data present in the captcha. Pincode is generated by removing the redundant data as specified by the user from the captcha .User's eye image is scanned and given as input to the website. The input iris image is steganographed with the generated by pincode. As result of performing VC on the image, share1 and share2 are generated .share1 is discarded. The share2 and the stored share1 of the user are overlapped and the input iris image is obtained. Now desteganographing is done and the pincode is generated. This pincode and stored pincode of the user is compared. If it matches then user is a authenticate or else fake. If authenticate one then user is successfully logged in.

Figure 3 clearly explains the login phase

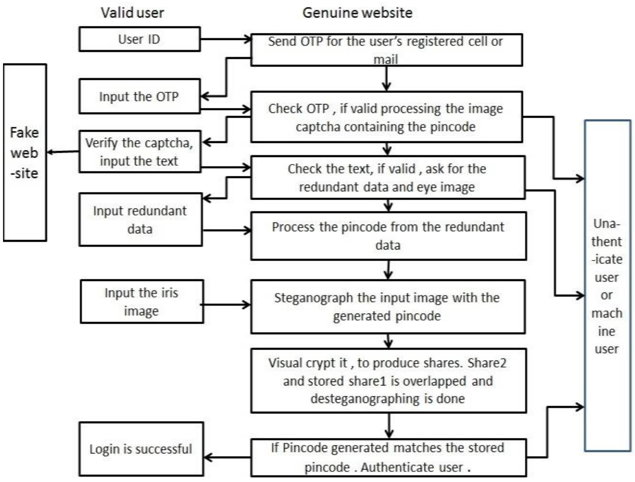
Valid user
Genuine website
User ID
Send OTP for the user's registered cell or mail
Fake web -site
Input the OTP
Check OTP , if valid processing the image captcha containing the pincode
Verify the captcha, input the text
Check the text, if valid , ask for the redundant data and eye image
Input redundant data
Process the pincode from the redundant data
Una- thent -icate user or mach ine user
Input the iris image
Steganograph the input image with the generated pincode
Visual crypt it , to produce shares. Share2 and stored share1 is overlapped and desteganographing is done
Login is successful
If Pincode generated matches the stored pincode . Authenticate user .

Fig.3 Login Stage

IV. Conclusions

This paper has introduced an anti-phishing user and website mutual authentication scheme.it is worthwhile to note that this methodology achieve three propose. 1st user won't disclose any of personal details until it hasn't confirmed that the website is genuine or fake. If the website is a phishing website, then in that situation it won't be able to send the OTP and as well as can't display the image captcha for the specific user due the fact the captcha is generated by the help of details and the unique pincode

Second propose cross validates the website that the user is not a robot. The image captcha is readable by human users alone and not by the machine. So by using the image captcha technique, no machine based attacks are possible. Third propose, by the use of biometric website can validate the authentication of the user identity. With the steganography the weak links of the biometric system is avoided.

Acknowledgment

I gratefully acknowledge the contributions of M.Naor and A.Shamir for their work in the field of visual cryptography. And John Daugman of cambridge university for the algorithm for iris recognition. I would like to thank Dr. Siddaraju Prof & HOD Mr.Nithya E Assoc.Prof. of Dr.A.I.T, Bangalore for their encouragement.

References

[1] Ollmann G., the Phishing Guide Understanding & Preventing Phishing Attacks, NGS Software Insight Security Research

[2] APWG, Jun. 2011, Available at http://www.antiphishing.org/report_phishing.html

[3] Visual Cryptography Wikipedia http://en.wikipedia.org/wiki/Visual_cryptography

[4] J. Daugman. How iris recognition works. Proceedings of 2002 International Conference on Image Processing, Vol. 1, 2002

[5] M.Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT, 1994, pp. 1–12

[6] A. O. Freier, P. Karlton, and P. C. Kocher, "The SSL protocol version 3.0," Jun. 2010, Available at http://tools.ietf.org/html/draft-ietf-tlsssl-version3-00

[7] L. von Ahn, M. Blum, N. Hopper, and J. Langford, "Telling humans and computers apart automatically," Communications of the ACM, vol. 47, no. 2, pp. 56–60, Feb. 2004

[8] CAPTCHA: Using Hard AI Problems For Security Luis von Ahn1, Blum1, Nicholas J. Hopper1, and John Langford.

[9] Nitin, V. K. Sehgal, D. S. Chauhan, M. Sood, and V. Hastir, "Image based authentication system with sign-in seal," Proc. the World Congress on Engineering and Computer Science, pp. 263–266, 2008

[10] A Text-Graphics Character CAPTCHA for Password Authentication Matthew Dailey Chanathip Namprempre

[11] Jithesh, Dr. A. V. Senthil Kumar Multilayer information hiding – A blend of steganography and Visual Cryptography

[12] N. K. Ratha, J. H. Connell, R. M. Bolle Enhancing security and privacy in biometrics – based authentication systems

Authors

Khadija Kaousar M A, pg scholar in computer science and engineering, Dr.Ambedkar Institute of Technology, Bangalore,India . Khadija.kaousar@gmail.com