ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

CONQUERING OF ONLINE BANKING FRAUD ACTIONS USING SECURITY IMAGES

P.Jancy Alfina[1],M.Kavitha[1] ,K.Keerthika[1], Mrs.V.Blessy Selvapriya[2]

1. Under Graduate Students, Department of Computer Science and Engineering, Kings Engineering College, India 2.Assistant Professor, Department of Computer Science and Engineering, Kings Engineering College, India

Abstract

This paper presents a new approach for providing limited information only that is necessary for fund transfer during online shopping thereby safeguarding customer data and increasing customer confidence and preventing identity theft. 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. Phishing is an attempt by an individual or a group to thieve personal confidential information such as passwords, credit card information etc from unsuspecting victims for identity theft, financial gain and other fraudulent activities.The use of images is explored to preserve the privacy of image captcha by decomposing the original image captcha into two shares that are stored in separate database servers such that the original image captcha can be revealed only when both are simultaneously available; the individual sheet images do not reveal the identity of the original image captcha. Once the original image captcha is revealed to the user it can be used as the password. Several solutions have been proposed to tackle phishing.

INTRODUCTION

The main objective of this project is to safeguard customer data and prevent phishing attack during online banking by using visual cryptography and steganography.

A brief survey of related work in the area of banking security based on steganography and visual cryptography is presented in this section. A customer authentication system using visual cryptography is presented in but it is specifically designed for physical banking. A captcha based authentication system for core banking is proposed in but it also requires physical presence of the customer presenting the share. Proposes a combined image based steganography and visual cryptography authentication system for customer authentication in core banking.

A new method is proposed, that uses text based steganography and visual cryptography, which minimizes information sharing between consumer and online merchant but enable successful fund transfer from consumer's account to merchant's account thereby safeguarding consumer information and preventing misuse of information at merchant side. The method proposed is specifically for E-Commerce but can easily be extended for online as well as physical banking.Identity theft is the stealing of someone's identity in the form of personal information and misuse of that information Online banking is the retrieval of product information via the Internet and issue of purchase order through electronic purchase request, filling of credit or debit card information and shipping of product by mail order or home delivery by courier. Identity theft and phishing are the common dangers of online banking. In 2012 consumer information was misused for an average of 48 days as a result of identity theft.

Phishing is a criminal mechanism that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. In 2ndquarter of 2013, Payment Service, Financial and Retail Service are the most targeted industrial sectors of phishing attacks.Secure Socket Layer (SSL) encryption prevents the interception of consumer information in transit between the consumer and the online merchant. However, one must still trust merchant and its employees not to use consumer information for their own purchases and not to sell the information to others.

VISUAL CRYPTOGRAPHY

The best vital techniques to protect data is cyptography. It 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.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

Visual Cryptography Scheme is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. We can achieve this by one of the following access structure schemes.

1.(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.

2.(2,n) Threshold VCS scheme-This scheme encrypts the secret image into n shares such that when any two(or more) of the shares are overlaid the secret image is revealed. The user will be prompted for n, the number of participants.

3.(n,n) Threshold VCS scheme-This scheme encrypts the secret image to n shares such that when all n of the shares are combined will the secret image be revealed. The user will be prompted for n, the number of participants.

4.(k,n) Threshold VCS scheme- This scheme encrypts the secret image to n shares such that when any group of at least k shares are overlaid the secret image will be revealed. The user will be prompted for k, the Threshold and n, the number of participants.

EXISITING SYSTEM

In this existing system security images are often used as part of the login process on internet banking websites .It can help foil phishing attacks.If a phishing website mimics a real one in all ways except that it does not show the users chosen security images , vigilant user might notice the absence of the security image and refuse to login.

Security images are often used as part of the login process on internet banking websites, under the theory that they can help foil phishing attacks. Previous studies, however, have yielded inconsistent results about users ability to notice that a security image is missing. This paper describes an online study of 482 users that attempts to clarify to what extent users notice and react to the absence of security images. The majority of our participants (73%) entered their password when we removed the security image and caption. We found changing the appearance and other characteristics of the security image generally had little effect on whether users logged in when the security image was absent. Additionally, we subjected the passwords created by participants to a password-cracking algorithm and found that participants with stronger passwords were less likely (64.7% vs 80.1%) to enter their passwords when the security image was missing.

PROPOSED SYSTEM

Proposed System, Visual Cryptography (VC), technique based on visual secret sharing used for image encryption. Secure Socket Layer (SSL) encryption prevents the interception of consumer information in transit between the consumer and the online merchant. In this project , a new method is proposed, that uses text based steganography and visual cryptography, which minimizes information sharing between consumer and online merchant. VCS is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. HMAC Algorithm is used 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 validation scheme using visual cryptography.

Advantages

1. It prevents password and other confidential information from the phishing websites.
2. Shoulder surfing attack can be overcome using this methodology.
3. Data integrity –assurance that data received are exactly as sent by an authorized entity.

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 validation scheme using visual cryptography. It prevents password and other confidential information from the phishing websites.

The proposed approach can be divided into two phases:

A. Registration Phase
B. Login Phase

A.REGISTRATION PHASE

In the registration phase, a key string is asked from the user at the time of registration for the secure website. The key string can be a combination of alphabets and numbers to provide more secure environment. According to the key given by the user this string is concatenated with randomly generated string in the server and an image captcha is generated. So the new image captcha is processed behind.

The image captcha is divided into two shares by (k,n) visual cryptography scheme such that the image captcha is divided according to black and white pixels. Then one of the share is kept with the user and the other share is kept in the server. The user's share and the original image captcha is sent to the user for later verification during login phase. The image captcha is also stored in the actual database of any confidential website as confidential data. Because the image captcha is used as the password later.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

Registration process with sequence of encryption is depicted in fig.1

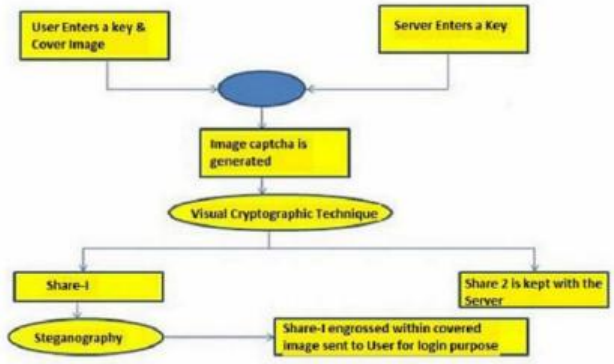
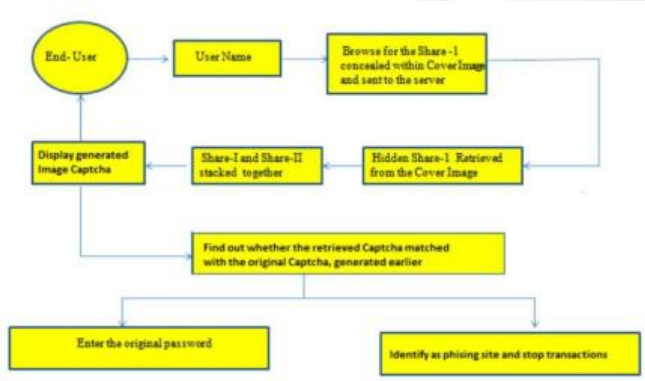


Fig.1 Registeration Phase

B. LOGIN PHASE

When the user logs in by entering his personal information for using his account, then first the user is asked to enter his user id. Then the user is asked to enter his share which is kept with him. This share is sent to the server where the user's share and share which is stored in the database of the website for each user, is stacked together to produce the image captcha. The image captcha is displayed to the user. Here the end user can check whether the displayed image captcha matches with the captcha created at the time of registration. The end user is required to enter the text displayed in the image captcha and this can serve the purpose of password and using this, the user can log in into the website. Using the user id and image captcha generated by stacking two shares one can verify whether the website is genuine/secure website or a phishing website and can also verify whether the user is a human user or not.



TECHNIQUES USED

k-n Secret Sharing Visual Cryptography Scheme

An image is taken as input. The image would be divided (n) number of shares to reconstruct the image (k). The division is achieved by the following algorithm.

ENCRYPTION PROCESS

Step I: Take an image IMG as input and calculate its width (w) and height (h).

Step II: Take the number of shares (n) and minimum number of shares (k) to be taken to reconstruct the image where k must be less than or equal to n. Calculate RECONS = (n-k)+1.

Step III: Create a three dimensional array IMG_SHARE[n][w*h][32] to store the pixels of n number of shares. k-n secret sharing visual cryptographic division is done by the following process.

```
for i = 0 to (w*h-1)
{
  Scan each pixel value of IMG and convert it into 32 bit binary string let PIX_ST.
      for j = 0 to 31
       {   if (PIX_ST.charAt(i) =1){
           call Random_Place (n, RECONS)
           }
           for k = 0 to (RECONS−1)
           {
              Set IMG_SHARE [RAND[k]][i][j] = 1
           }
       }
}
```

Step IV: Create a one dimensional array IMG_CONS[n] to store constructed pixels of each n number of shares by the following process.

```
for k1 = 0 to (n-1)
{ for k2 = 0 to  (w*h-1)
  { String value= “”
     for k3 = 0 to 31 {
        value = value+IMG_SHARE [k1][k2][k3]
      }
     Construct alpha, red, green and blue part of each pixel by taking consecutive 8 bit substring starting from 0. Construct pixel from these part and store it into IMG_CONS[k1] [4].
     }
  Generate image from IMG_CONS [k1][1] [8].
}
```

subroutine int Random_Place(n, RECONS)

```
{ Create an array RAND[RECONS] to store the generated random number.
  for i = 0 to (recons-1)
```

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

```
                {
                Generate a random number within n, let
  rand_int.  [9] if (rand_int is not in RAND
  [RECONS])
    RAND [i] = rand_int
 }
return RAND [RECONS]
}
```

DECRYPTION PROCESS

ALGORITHM

Step 1: Step 1: Input number of shares to be taken(k), height(h),width (w) of each share.
Step 2: Create two dimensional array share[k][w*h] to store the pixel value of each share.
Step 3: Create one dimensional array final[w*h] to store the final pixel values of the image to be performed by OR operation.
Step 4:Scan each pixel value of the image share and store the value in share[i][j].
Step 5: Generate image from final[w*h].

SCREENSHOTS

CONCLUSION

In this paper, a payment system for online shopping is proposed by combining text based steganography and visual cryptography that provides customer data privacy and prevents misuse of data at merchant's side. The method is concerned only with prevention of identity theft and customer data security. In comparison to other banking application which uses steganography and visual cryptography are basically applied for physical banking, the proposed method can be applied for E-Commerce with focus area on payment during online shopping as well as physical banking.

REFERENCES

[1] Jihui Chen, Xiaoyao Xie, and Fengxuan Jing, "The security of shopping online," Proceedings of 2011 International Conference on Electronic and Mechanical Engineering and Information Technology (EMEIT), vol. 9, pp. 4693-4696, 2011.

[2] Javelin Strategy & Research, "2013 Identify Fraud Report," https://www.javelinstrategy.com/brochure/276.

[3] Anti-Phishing Working Group (APWG), "Phishing Activity Trends Report,2013,"http://docs.apwg.org/reports/apwg_trends_report_q2_2013.pdf

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

[8] Jaya, Siddharth Malik, Abhinav Aggarwal, Anjali Sardana, "Novel Authentication System Using Visual

Cryptography," Proceedings of 2011 World Congress on Information and Communication Technologies, pp. 1181- 1186, Mumbai, India, 2011.

[9] K. Thamizhchelvy, G. Geetha, "E-Banking Security: Mitigating Online Threats Using Message Authentication Image (MAI) Algorithm," Proceedings of 2012 International Conference on Computing Sciences (ICCS), pp. 276 – 280, 2012.

[10] S. Suryadevara, R. Naaz, Shweta, S. Kapoor, "Visual cryptography improvises the security of tongue as a biometric in banking system," Proceedings of 2011 2nd International Conference on Computer and Communication Technology (ICCCT), pp. 412 – 415, 2011.