PRESERVING USER-PARTICIPATION FOR INSECURE NETWORK COMMUNICATIONS WITH CAPTCHA AND VISUAL SECRET SHARING TECHNIQUE

V.Neela Gandhi,
Department of CSE
Francis Xavier Engineering College
neelagandhiragavi@gmail.com

NadarKeerti Ashok
Department of CSE
Francis Xavier Engineering College
keertinadar24@gmail.coms

Dr.S.Balaji
Professor
Francis Xavier Engineering College
balajiphd@gmail.com

Abstract:
This paper presents a new approach for providing limited information only that is necessary for fund transfer during online shopping thereby conserving 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 secretsharing scheme a secret image is encrypted in shares which are meaningless images that can be transmitted or distributedover an un trusted communication channel.Only combining the k shares or more give the original secret image. Phishingis an attempt by an individual or a group to thieve personal confidential information such as passwords, credit cardinformation from unsuspecting victims for identity theft, financial gain and other fraudulent activities. The use of images is explored to safeguard the solitude 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 individuality of the original image captcha. Once the original image captcha is revealed to the user it can be used as the secret code.Several solutions have been proposed to tackle phishing. In existing they analyze the honey word approach and give some remarks about the security of the system. Furthermore, they point out that the key item for this method is the generation algorithm of the honey words such that they shall be indistinguishable from the correct passwords. Therefore, they propose a new approach that uses passwords of other users in the system for honey word sets, i.e. realistic honey words are provided.

1.Introduction

The main objective of this project is to safeguard customer data and prevent phishing attack during online shopping by using visual cryptography and steganography. A brief survey of related work in the area of banking safety measures 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 signature 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 verification in core banking. In this paper, a new method is planned, that uses text based steganography and visual cryptography, which minimizes information sharing between consumer and online merchant but enable flourishing 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 shopping is the retrieval of product information via the Internet and issue of purchase order through electronic purchase request, filling of recognition 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 shopping for making purchase and opening of bank accounts or arranging credit cards. 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 transfer between the consumer and the online business. However, one must still trust merchant and its employees not to use customer information for their own purchases and not to sell the information to others.

2. Existing system

Phishing web pages are forged web pages that are created by malicious people to imitate Web pages of real websites. Most of these kinds of web pages have high visual resemblance to scam their losses. Some of these kinds of web browsers look exactly like the real one. Victims of phishing web browsers may expose their bank account, password, credit card number, or other important information to the phishing web page owners. It includes techniques such as tricking customers through email and spam messages, man in the middle attacks, installing key loggers and screen captures.

2.1. Demerits

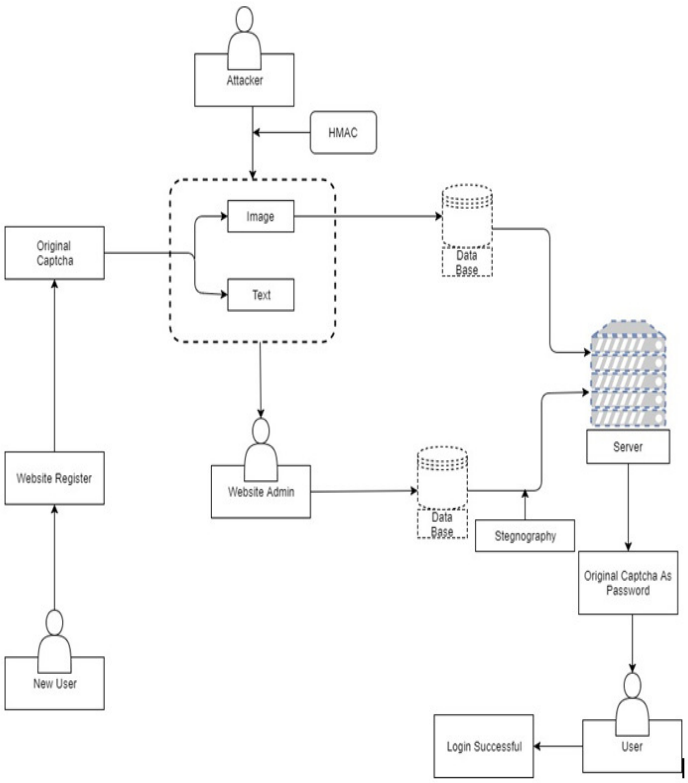
Does not give a friendly environment to encrypt or decrypt the data (images). It supports with only one kind of image format. For example, if it is .jpg, then it supports only that same kind of image format only.It is the most critical measurement to evaluate the effectiveness of a VCS.

2.2 Problem Identification

The problem is that CA does not know to which bank to forward the cover text obtained from combine two shares. It can be solved by adding 9 digit routing or shipment number of bank with client authentication information. Now one share is kept by the customer and the other share is kept in the database of the certified authority. During shopping online, after selection of desired item and adding it to the cart, favored payment system of the merchant directs the customer to the Certified Authority entry.In the portal, shopper submits its individual share and merchant submits its own account details. Now the CA combines its own share with shopper's share and obtains the original image. From CA now, merchant account details, cover text are sent to the bank where customer authentication password is recovered from the cover text. Customer authentication information is sent to the merchant by CA. Upon receiving client authentication password, bank matches it with its own database and after verifying legitimate customer, transfers fund from the customer account to the submitted merchant account. After receiving the fund, merchant's payment system validates receipt ofpayment using customer authentication information.
Phishing is a form of social engineering. Phishing attacks use email or dangerous websites to solicit personal, often financial, information. Attackers may send email seemingly from a reputable credit card company or financial institution that request account information, often suggesting that there is a problem. When users respond with the requested information, attacker can use it to gain access to the accounts.

3. Proposed system

Proposed System, Visual Cryptography (VC), method based on visual secret sharing used for image encryption. Secure Socket Layer (SSL) encryption prevents the interception of customer information in shipment between the consumer and the online merchant. In this paper, a new technique is proposed, that uses text based steganography and visual cryptography,which minimize information sharing between consumer and online merchant.VCS is a cryptographic technique that allows for the encryption of visual information such that decryption can perform using the human visual scheme. HMAC Algorithm is used for phishing detection and prevention. We are proposing a new method to find the phishing website. Our methodology is based on the Anti-Phishing Image Captcha validation system using visual cryptography.It prevents password and other confidential information from the phishing websites. Cryptographic technique: (2, 2)- Threshold VCS scheme(n, n) Threshold VCS scheme, (k, n) Threshold VCS scheme are used in this proposed scheme.The below diagram shows the architecture diagram of our proposed system:

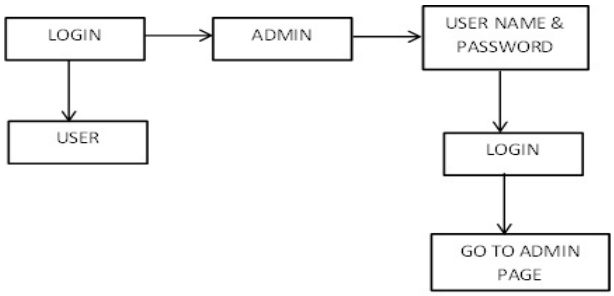


These are the various stages of the project

1. User and admin authentication
2. Captcha encryption
3. Captcha decryption
4. Customer merchant
5. Amount transaction
6. Transfer to fund

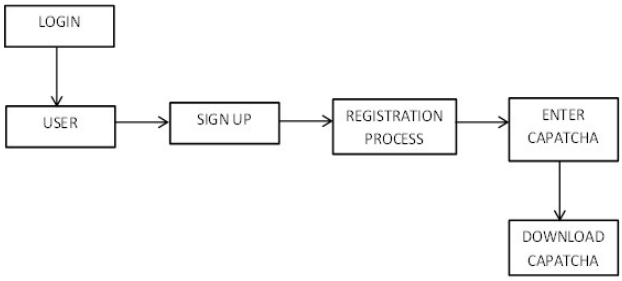
1. User and admin authentication

It performs log on for basic form authentication. User can use these login modules to perform authentication with user ID and password. The logic modules used for authentication with client certificates.



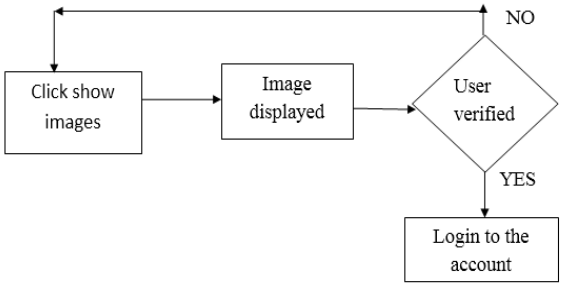
2. Captcha encryption

This module describes the signup form captcha as encrypt and make it as image format to access the user login page for security purpose.



3. Captcha decryption

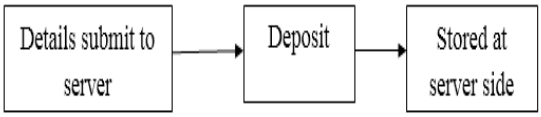
This module prescribes the encrypted captcha image to bind the captcha in data information in stenography image to protect from attacks. From this technique we can hide the user authentication process from hackers.



4. Customer merchant

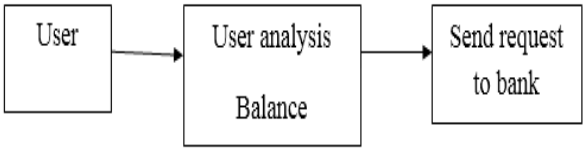
Customer authentication information is sent to the merchant by CA. Upon receiving customer password, bank matches it with its own databases and after verifying, legitimate customer, transfers fund from the customer account to the submitted merchant account.After receiving the fund, merchant's payment system validates receipt of payment using customer authentication information. The problem is that CA does not know to which bank to forward the cover

text obtained from combining two shares. It can be solved by appending 9 digit routing or transit number of bank with customer authentication information.



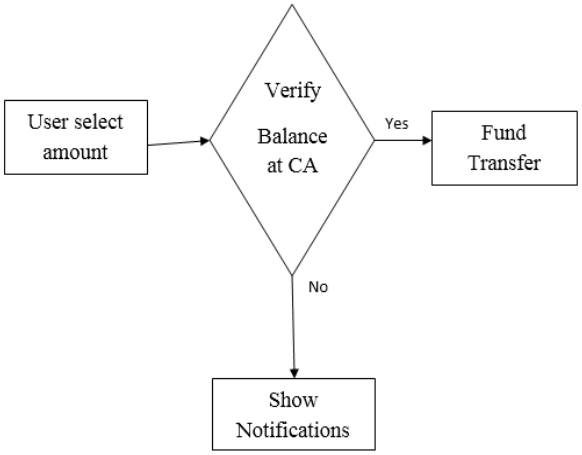
5. Payment Gateway

Consumer selects item from online shopping portal and then is directed to the payment page. Online merchant may have its own payment system or can take advantage of third party payment system such as PayPal, Pay online web moment and others.



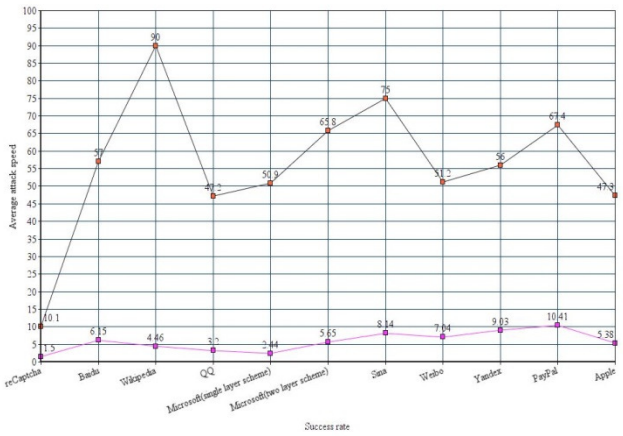
6. Transfer of fund

During online shopping, after selection of desired item and adding it to the cart, preferred payment system of the merchant is directed from the customer to the Certified Authority Portal. In the portal, shopper submits its own share and merchant submit its own account. Consumer selects items from online shopping portal and then is directed to the payment page. Online merchant may have its own payment system or can take advantage of third party payment systems such as PayPal, pay online system, Web Money and others. In the payment portal consumer submit his or her credit. Now one share is kept by the customer and the other share is kept in the database of the certified authority.



4.Discussions

Discussions were made based on the existing system:



The success rate against reCAPTCHA is the lowest, since it uses street views containing house numbers as the Captcha. These complicated street view scenarios make the extraction of a house number extremely difficult, and there is a wide variation in the choice of fonts in real-world house numbers. Both of these reasons explain the lower success rate of our attack**.**

5. Conclusion

In this paper, a payment scheme for online shopping is proposed by combining text based steganography and visual cryptography that provides customer data privacy and prevent misuse of data at merchant's side. The system 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 future method can be applied for E-Commerce with focus region on payment during online shopping as well as physical banking.

6. References

[1] L. Von Ahn, M. Blum, N. J. Hopper, and J. Langford, "Captcha: Using hard ai problems for security," in *Advances in CryptologyłEUROCRYPT2003*. Springer, 2003, pp. 294–311.
[2] L. Von Ahn, M. Blum, and J. Langford, "Telling humans and computers apart automatically," *Communications of the ACM*, vol. 47, no. 2, pp. 56–60, 2004.
[3] E. Bursztein, M. Martin, and J. Mitchell, "Text-based captcha strengths and weaknesses," in *Proceedings of the 18th ACM conference onComputer and communications security*. ACM, 2011, pp. 125–138.
[4] J. Yan and A. S. El Ahmad, "Usability of captchas or usability issues in captcha design," in *Proceedings of the 4th symposium on Usable privacyand security*. ACM, 2008, pp. 44–52.
[5] J. Yan and A. S. E. Ahmad, "Breaking visual captchas with naive pattern recognition algorithms," in *Computer Security Applications Conference,2007. ACSAC 2007. Twenty-Third Annual*, 2007, pp. 279–291.
[6] J. Yan and A. S. El Ahmad, "A low-cost attack on a Microsoft captcha," in *Proceedings of the 15th ACM conference on Computer andcommunications security*. ACM, 2008, pp. 543–554.
[7] C. Kumar, L. Kevin, S. Patrice, Y., and C. Mary, "Computers beat hu-mans at single character recognition in reading based human interaction proofs (hips)," in *CEAS 2005 - Second Conference on Email and Anti-Spam, July 21-22, 2005, Stanford University, California, USA*, 2005.
[8] H. Gao, W. Wang, J. Qi, X. Wang, X. Liu, and J. Yan, "The robustness of hollow captchas," in *Proceedings of the 2013 ACM SIGSAC conferenceon Computer & communications security*. ACM, 2013, pp. 1075–1086.
[9] A. S. El Ahmad, Y. Jeff, and T. Mohamad, "The robustness of googlecaptchas," 2011.
[10] H. Gao, W. Wang, Y. Fan, J. Qi, and X. Liu, "The robustness of "connecting characters togethe" captchas." *J. Inf. Sci. Eng.*, vol. 30, no. 2, pp. 347–369, 2014.
[11] H. Gao, M. Tang, Y. Liu, P. Zhang, and X. Liu, "Research on the security of microsoft's two-layer captcha," *IEEE Transactions on InformationForensics and Security*, vol. 12, no. 7, pp. 1671–1685, 2017.
[12] E. Bursztein, J. Aigrain, A. Moscicki, and J. C. Mitchell, "The end is nigh: Generic solving of text-based captchas." in *WOOT*, 2014.
[13] H. Gao, J. Yan, F. Cao, Z. Zhang, L. Lei, M. Tang, P. Zhang, X. Zhou, X. Wang, and J. Li, "A simple generic attack on text captchas." in *NDSS*, 2016.
[14] K. Chellapilla, K. Larson, P. Y. Simard, and M. Czerwinski, "Building segmentation based human-friendly human interaction proofs (hips)," in *Human Interactive Proofs*. Springer, 2005, pp. 1–26.
[15] A. Algwil, D. Ciresan, B. Liu, and J. Yan, "A security analysis of automated chineseturing tests," in *Proceedings of the 32nd AnnualConference on Computer Security Applications*. ACM, 2016, pp. 520–532.
[16] I. J. Goodfellow, Y. Bulatov, J. Ibarz, S. Arnoud, and V. Shet, "Multi-digit number recognition from street view imagery using deep convolu-tional neural networks," *arXiv preprint arXiv:1312.6082*, 2013.
[17] N. Otsu, "A threshold selection method from gray-level histograms," *Automatica*, vol. 11, no. 285-296, pp. 23–27, 1975.
[18] Y. LeCun*et al.*, "Lenet-5, convolutional neural networks," *URL:http://yann. lecun. com/exdb/lenet*, 2015.
[19] D. C. Ciresan, U. Meier, J. Masci, L. Maria Gambardella, and J. Schmid-huber, "Flexible, high performance convolutional neural networks for image classification," in *IJCAI Proceedings-International Joint Confer-ence on Artificial Intelligence*, vol. 22, no. 1. Barcelona, Spain, 2011,p. 1237.
[20] V. Turchenko and A. Luczak, "Caffe: Convolutional architecture for fast feature embedding," *EprintArxiv*, pp. 675–678, 2014.
[21] D. D'Souza, P. C. Polina, and R. V. Yampolskiy, "Avatar captcha: Telling computers and humans apart via face classification," in *Electro/Information Technology (EIT), 2012 IEEE International Conference on*. IEEE, 2012, pp. 1–6.
[22] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," in *Advances in neural infor-mation processing systems*, 2012, pp. 1097–1105.

[23] G. Mori and J. Malik, "Recognizing objects in adversarial clutter: Breaking a visual captcha," in *Computer Vision and Pattern Recognition,2003. Proceedings. 2003 IEEE Computer Society Conference on*, vol. 1.IEEE, 2003, pp. I–134.

[24] G. Moy, N. Jones, C. Harkless, and R. Potter, "Distortion estimation techniques in solving visual captchas," in *Computer Vision and PatternRecognition, 2004. CVPR 2004. Proceedings of the 2004 IEEE Com-puter Society Conference on*, vol. 2. IEEE, 2004, pp. II–II.

[25] C. Cruz-Perez, O. Starostenko, F. Uceda-Ponga, V. Alarcon-Aquino, and L.Reyes-Cabrera, "Breaking recaptchas with unpredictable collapse: Heuristic character segmentation and recognition," *Pattern Recognition*, pp. 155–165, 2012.