

Security for Online Banking Using Captcha

¹S.Snehalatha, ²R.Viji and ³R.Sivasankari,

^{1,2,3}Department of Computer Science and Engineering, G.K.M. College of Engineering and Technology, Chennai, Tamil Nadu, India

Abstract- In the current generation most of the people using bank transaction, fund transfer are being processed through the internet. So the probability to malicious activity are also increased. To overcome this activity Captcha is used in computing to determine whether or not the user is human or robot. In this proposed system Captcha is converted into two images with help of visual cryptography and steganography methods. 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 share 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. A cryptographic technique based on visual secret sharing used for image encryption.

Keywords—Captcha, Visual cryptography, Image encryption, Common Language Runtime (CLR), Security Socket Layer (SSL), Hash-based Message Authentication Code (HMAC).

I. 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 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 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 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. Phishing is a criminal mechanism that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. In 2nd quarter of 2013, payment service, financial and retail service 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.

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.

II. RELATED WORKS

K. Bennet Purdue University "Hiding information in document images". In this paper they proposed how to use spatial information to reliably hide data in document images. The system can be used to discourage unauthorized reproduction and dissemination of either copyrighted documents distributed electronically, or paper copies of confidential executive memoranda. t. s. chen and m. w. cheng, "a new data hiding scheme in binary image". In this paper they proposed how to use the data-embedding algorithm that is based on hamming codes, the proposed scheme embeds authentication information into the cover image with flipping only a small number of pixels. Randomly shuffling the bit-order of the authentication information to be embedded, the information can only be extracted by the designated receiver who has the symmetric key. Jihui Chen and Xiaoyaoxie "The security of shopping online". In this paper they proposed about the characteristics of online shopping and the current development of the main safety problems, and make online shopping related security measures and transactions. The online shopping convenient fast efficient and economic advantages. Manu and P. Deepashenoy, "secure authentication using image processing and visual cryptography for banking applications". In this paper proposes a technique of processing the signature of a customer and then dividing it into shares. Total number of shares to be created is depending on the scheme chosen by the bank. the correlation method is used to take the decision on acceptance or rejection of the output and authenticate the customer.

III. 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 paper, 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, in proposed system 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. cryptographic technique: (2, 2)- threshold vcs scheme, (n, n) threshold vcs scheme, (k/n) threshold vcs scheme are used in this proposed system.

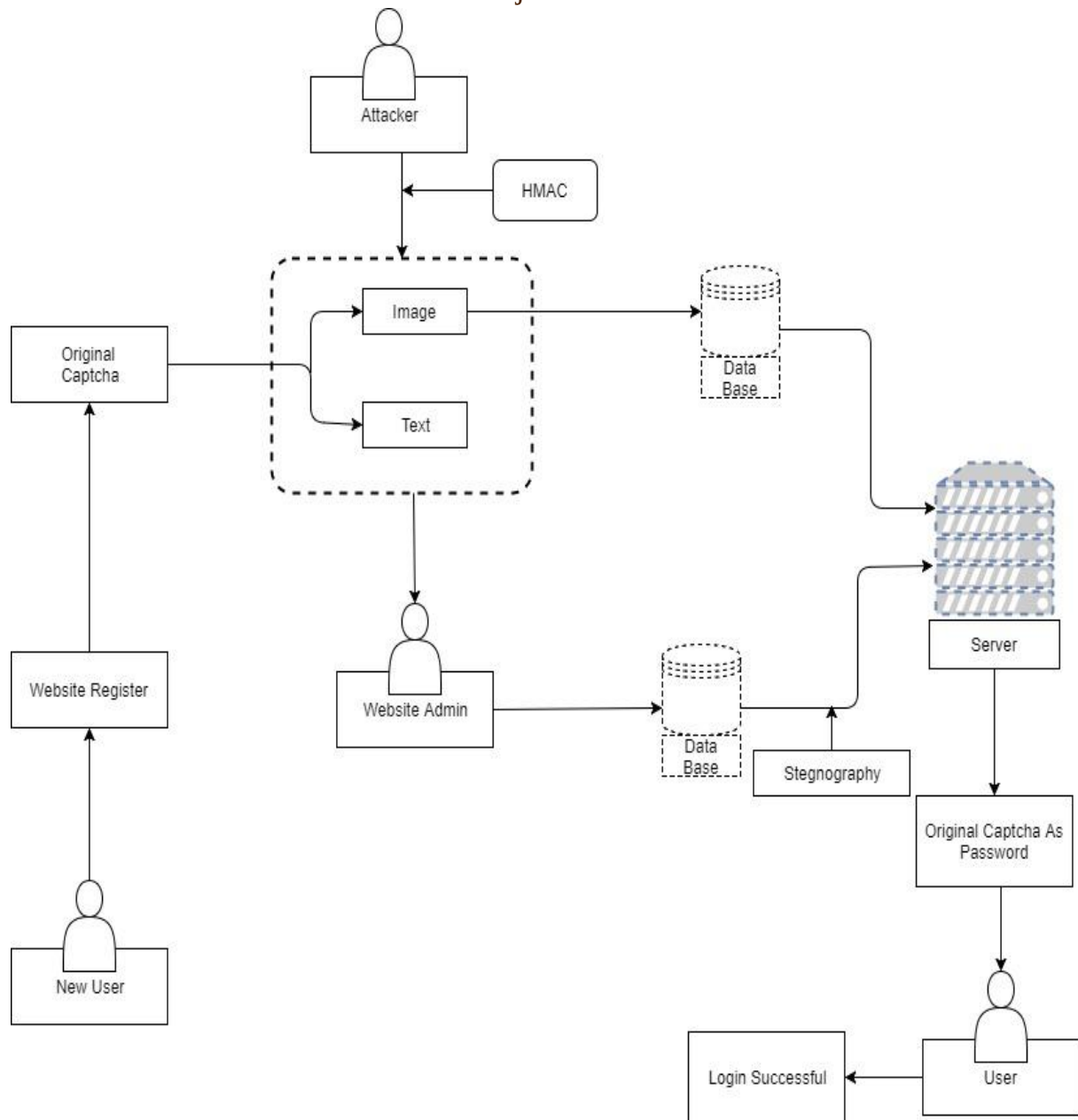


Fig. 1 Architecture diagram

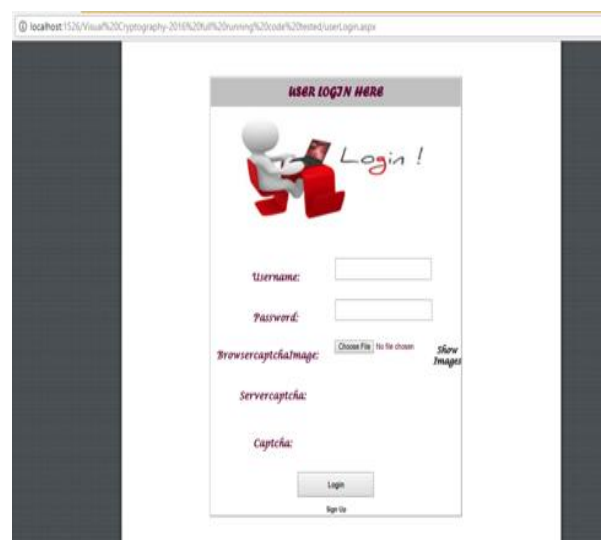
A. User and admin authentication

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



B. Captcha encryption

This module describes the signup form. captcha in encrypted form is made as image format to access the user login page for security purpose.





C. Captcha decryption

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



IV. EXPERIMENTAL EVALUATION

Microsoft Visual Studio is an integrated development environment from Microsoft. It is used to develop computer programs for Microsoft Windows, as well as web sites, web applications and web services. Visual Studio uses such as Windows API, Windows Forms, Windows Presentation Foundation. Visual Studio includes a code editor supporting IntelliSense (the code completion component). The integrated debugger works both as a source-level debugger and a machine-level debugger. Other built-in tools include a forms designer for building GUI

applications, web designer, class designer, and database schema designer. It accepts plug-ins that enhances the functionality at almost every level—including adding support for source-control systems.

ASP.NET XML web services	Windows Forms
Base Class Libraries	
Common Language Runtime	
Operating System	

CONCLUSION

In proposed system, 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 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, XiaoyaoXie, 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," Proceeding of 14th International Conference on Computational Science and Engineering, pp. 57-61, Dalian, Liaoning, 2011.
- [7] K. Bennet, "Linguistic Steganography: Survey, 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 improves the security of tongue as a biometric in banking system," Proceedings of 2011 2nd International Conference on Computer and Communication Technology (ICCCCT), pp. 412 – 415, 2011.