Enhanced Password Processing Scheme Using Visual Cryptography And Steganography

Amar Walke
IT-SAKEC
Mumbai,India
amar.walke@sakec.ac.in

Jignesh Bhanushali
IT-SAKEC
Mumbai,India
jcb.3594@gmail.com

Akshay Rajgor
IT-SAKEC
Mumbai,India
akki.rajgor898@gmail.com

Jeenit Jain
IT-SAKEC
Mumbai,India
jeenit06.dec@gmail.com

***Abstract*--**With the rise in internet users, the need for security has increased as well. The first step in securing digital information is through the use of passwords. These text bases passwords are then converted to hash values. However, they are susceptible to attacks like man in the middle attacks and other hacks. Information leaks proves fatal in such scenarios.

To combat these issues, we have proposed a new system that has lower computational requirements and utilizes visual cryptography and text steganography. We have also proposed using visual cryptography with utilizes meaningful shares to hide the intent of the images.User's secret information is used to form an image which is divided and shared over multiples parties.This results in no single party having complete information.The benefit of this is that a hack at any one user won't compromise user's information.

With the number of online users now in billions,this system has a huge scope and will prove important for information security when privacy and security are of paramount importance.

*****

I. INTRODUCTION

User authentication in general systems has proceeded basically through verification of the ID and password. In order to send and verify password, the system uses a hash-based password scheme that transforms original password to hash value by famed function. The advantages are that it can be adapted in system without difficulty, and computational velocity of process is fast because a type of hash-based scheme is fundamentally based on text utilizing popular hash function such as MD5, SHA256. But it is vulnerable to attacks such as brute force attack or dictionary-based attack plainly by password cracking tool or hash-cracking online sites.

Another major reason is using of easy passwords. The factors contributed in password security are password reuse, frequency of changing password, length, entropy level, and uniqueness with regard to password.

Consequentially those behaviors become weak point and affect whole system. Many researchers have improved hashbased password scheme into the combination of password and some salts in hash function.However the salts prefixed to password cannot obstruct pre-computed birthday attack to forge an unknown password. In view different from text-based scheme, we suggest enhanced password scheme based on an image created by VC. The image implicitly involves password and ID. In order to verify password, proposed scheme checks ID through MSER. The goal of our proposal is to prevent cyber-attack and support privacy of personal information.

A. Scope of the Project

The main motive of the proposed system prescribed in this paper is to handle applications that require a high level of security, such as E-Commerce applications, core banking and internet banking. This can be done by using combination of two applications: Text Steganography and Visual Cryptography for safe online shopping and consumer satisfaction.

The project will help to mitigate one of the biggest threats i.e. theft or exploitation of data, data breaches/leaks as consumer safety is of paramount importance, which will help to make payment systems more secure thus making people shed their apprehensions about online payment's safety and give rise to digital users making this system a great success as there are around 462 million internet users which is almost half of our population.

II. EXISTING SYSTEM

Many graphical password schemes with different degrees of resistance to shoulder surfing have been proposed, Seeing that most users are more familiar with textual passwords than pure graphical passwords, we have proposed a text-based shoulder surfing resistant graphical password scheme. The user has to mix his textual password on the login screen to get the session password. However, the login process of scheme is complex and tedious. And then, several text based shoulder surfing resistant graphical password schemes have been proposed. Unfortunately, none of existing text-based shoulder surfing resistant graphical password schemes is both secure and efficient enough.One still has to trust the merchant and its employees not to use card information for there ownpurposes.Breach in any one side can adversely effect security.

III. PROPOSED SYSTEM

First, user inputs the ID and password on device. The device starts to create an original image consisted of black letters implying ID and white background. The user may save the image in the device. The device constructs first shared image adapting VC. The pattern to make up the first shared image is determined by pseudorandom generator with SEED which has password and ID as salts. After completing building the first shared image, the user sends ID of text type and the image instead of password to the server via security channel and destroys the image. If the server saves the data about user information, the initial registration process is finished. The server does not know the password at all because it is impossible for server to retrieve the password of the user from just one shared image.

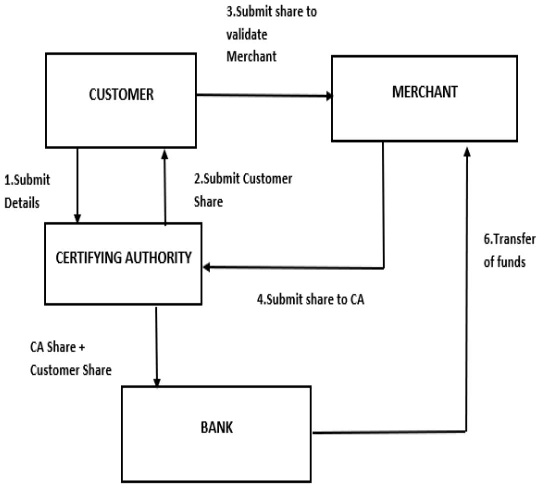

Figure1.Proposed System

A customer is the one who does the shopping, Customer visits the e-commerce website, selects the products they want and proceeds to do the payment. The customer then enters their details that are sent to the certifying authority.
Certifying Authority is the 3rd party intermediary between the Customer and Merchant.CA approves the transaction by accepting the request from the customer by accepting their details.
Customer is the dealer from whom the customer buys goods. Merchant is receiver of the funds from the customer and the end party in the process.

A .Advantages

The old system posed a threat to user’s credentials stored with the merchant as they could be misused and heavily relied on customer’s trust on merchant.
The various advantages involve adopting VC instead of text-based hash, lower computational cost, preventing cyber-attack using vulnerable points of hash functions ,supporting privacy of users, this scheme is able to prevent cyber-attack such as dictionary-attack and birthday-attack from the attackers aiming at cracking hash values.

IV.DESIGN & IMPLEMENTATION

This system is implemented using text steganography and visual cryptography.

A.Text Steganography

Steganography is a data hiding technique used for hiding secret messages. The messages could be hidden under image, audio, video, text.The algorithm used for text steganography is:
Encoding:
1.Represent every character of pin in ASCII code.
2.Convert ASCII to 8 bit binary.
3.Concatenate the 8 bit binary.
4.Divide the binary into 4 bit packets.
5.Choose suitable letters corresponding to the decimal equivalent of the 4 bit binary packet which will be used to form cover message.

Decoding:
1.First letter in each word of cover message is take and represented by corresponding number.
2.Convert the number to 4 bit binary.
3.Concatenate the 4 bit binary.
4.Divide the binary into 8 bit packets.
5.Obtain ASCII codes from 8 bit binary.
6.Pin is recovered from ASCII codes.

B. Visual Cryptography

Visual Cryptography is an encryption technique used to generate shares of images. (2,2) Visual Cryptography works same as visual cryptography scheme in which 2 meaning full shares are generated.

Issues with meaningless shares:

- Shares are meaningless.
- Meaningless shares arouse suspicion.
- Draws attention of hackers and eavesdroppers.

Advantages of Meaningful shares:

- A considerable part of the storage space can be saved due to pixel extraction and half toning.
- Meaning full shares results in them being inconspicuous.
- The true intent of the shares can be hidden.

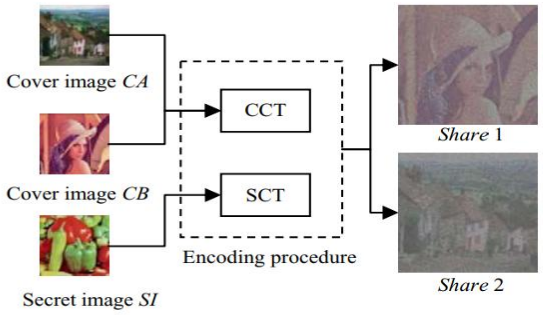

Figure 2:Visual Cryptography

To generate the shares, two N×N cover images, named CA and CB, are used to encode the N×N secret image SI and make two 2N×2N shares.The shares are called Share 1 and Share 2. Share 1 will be a meaningful share that appears just like CA. Share 2 will be also a meaningful share that looks just like CB. Finally, during the decoding procedure, the secret image can be easily reconstructed by stacking Share 1 and Share 2 together.

V. FURTHER IMPROVEMENT

Project can be further enhanced by including features like digital watermarking and introducing security features to prevent steganalysis.

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as an audio, video or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to, contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyrightinfringements.

The goal of steganalysis is to identify suspected packages, determine whether or not they have a payload encoded into them, and, if possible, recover that payload.

Unlike cryptanalysis, where it is obvious that intercepted data contains a message (though that message is encrypted),steganalysis generally starts with a pile of suspect data files, but little information about which of the files, if any, contain a payload. The steganalyst is usually something of a forensic statistician,and must start by reducing this set of data files (which is often quite large; in many cases, it may be the entire set of files on a computer) to the subset most likely to have been altered.

VI. CONCLUSION

Phishing is a criminal mechanism that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. 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.

Many people use the same or short length of passwords inmultiple systems and are neglectful password management.Consequentially cyber-accidents are occurred often. Wesuggested a distinctive method different from conventionalpassword scheme. It is based on encoded images by VC with aSEED number and MSER and more strong protection from cyber-attacks.We evaluated security aspect on attacks, computationalcost and privacy. Our proposal is light weight and more securein the aspect that hashed values of important information are notstored in the system.

VI. REFERENCES

[1] Gaw, Shirley, and Edward W. Felten, "Password management strategiesfor online accounts," Proceedings of the second symposium on Usableprivacy and security. ACM, 2006.

[2] Nguyen, Thi Thu Trang, and Quang Uy Nguyen, "An analysis ofPersuasive Text Passwords, "Information and Computer Science (NICS),2015 2nd National Foundation for Science and Technology DevelopmentConference on. IEEE, 2015.

[3] Tam, Leona, Myron Glassman, and Mark Vandenwauver, "Thepsychology of password management: a tradeoff between security andconvenience, "Behaviour& Information Technology 29.3 (2010): 233-244.

[4] Wang, Luren, Yue Li, and Kun Sun, "Amnesia: A Bilateral GenerativePassword Manager," 2016 IEEE 36th International Conference onDistributed Computing Systems

[5] Gauravaram, Praveen, "Security Analysis of salt|| password Hashes,"Advanced Computer Science Applications and Technologies (ACSAT),2012 International Conference on. IEEE, 2012.

[6] Dana Yang, InshilDoh, KijoonChae, "Mutual Authentication based onVisual Cryptography and MSER for Secure IoT Service," Source of theDocument 2016 6th International Workshop on Computer Science andEngineering, WCSE 2016, 2016, Pages 214-219

[7] M. Naor and A. Shamir, "Visual Cryptography," Advances in CryptologyEURMSERYPT94 LNCS, Vol. 950, pp. 1-12, 1995.

[8] Mori, Shunji, Ching Y. Suen, and Kazuhiko Yamamoto, "Historicalreview of MSER research and development," Proceedings of the IEEE 80.7(1992): 1029-1058.

[9] Patel, Chirag, Atul Patel, and Dharmendra Patel, "Optical characterrecognition by open source MSER tool tesseract: A case study,"International Journal of Computer Applications 55.10 (2012).

[10] Holley, Rose, "How good can it get? Analysing and improving MSER accuracy in large scale historic newspaper digitisation programs," D-LibMagazine 15.3/4 (2009).

[11] Marsaglia, George, "Xorshiftrngs," Journal of Statistical Software 8.14(2003): 1-6.

[12] Pallavi Das, Satish Chandra Kushwaha, MadhuparnaChakraborthy,"Multiple embedding secret key image steganography using LSB substitution and Arnold Transform", *2nd International Conference on Electronics and Communication Systems (ICECS)* pp845 – 849, 2015.

[13] K.S. Seethalakshmi , Usha B A , Sangeetha K N, "Security enhancement in image steganography using neural networks and visual cryptography", *International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS),* 2016 DOI: 10.1109/CSITSS.2016.7779393

[14] Dana Yang, InshilDoh, Kijoon Cha, "Enhanced Password Processing Scheme Based on Visual Cryptography and MSER", *IEEE ICOIN 2017*, 978-1-5090-5124-3/17