IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-10 E-ISSN: 2347-2693

Resisting Cyber-attacks in Digital Banking using Visual Cryptography

B.V.Prasanthi[1*], Sridevi Bonthu[2]

[1*]Department of Computer Science and Engineering, Vishnu Institute of Technology, Bhimavaram, India
[2] Department of Computer Science and Engineering, Vishnu Institute of Technology, Bhimavaram, India

[*]*Corresponding Author: prasanthibeera@gmail.com, Tel.: +91-9705017503*

Available online at: www.ijcseonline.org

Received: 15/Sep/2017, Revised: 28/Sep/2017, Accepted: 19/Oct/2017, Published: 30/Oct/2017

***Abstract*—** With increasing demand of security, user authentication occupies prior in information security and plays a prominent role in protecting user's privacy, which has become a critical issue nowadays. In this digital world the usage of online transactions became very common and at the same time various attacks are performed behind this. The most common method used for authentication in online banking is by providing text password, which is the combination of letters, sequence of characters and special symbols. Authentication system, based on text passwords is widely used but they can easily compromise with attacks. Users normally select simple passwords because they can easily memorize at the time of login. So providing more security than existing assists in protecting resources against unauthorized access. Image-based-authentication is a good alternative to traditional password system. Apart from many conventional cryptographic methods, visual cryptographic techniques have also been used for providing security to data. In this proposed work, Visual cryptographic scheme is used that encrypts a secret image by breaking into image shares. Along with text based password login, image based authentication using visual cryptography is included. This authentication system is useful for various sectors like industries, online banking and shopping.

***Keywords*—** Information Security, Virtual cryptography, authentication, online banking, encryption

I. INTRODUCTION

Internet has become a very important in almost in every one's life. Internet banking has gained wide acceptance internationally and appears to be quick catching up in digital india.Online banking allows the customers to use all the banking services from a pc which has internet, then the customers can perform financial transactions on secure sites operated under banks. The transactions such as banks statements, fund transfers-bill payments, withdrawal etc., The top most widespread internet banking security threats and risks are Zbot,Zeus Gameover (P2P), SpyEye, IceIX, Citadel, Carberp, Bugat, Torpig, CryptoLocker, key loggers and viruses. These risks and threats have the capability to manipulate typical banking customers and illegal access of user's sensitive information. There are many cyber forensics tools[1][2]to solve this cyber attacks.

If we see the importance of digital Banking, It saves time that spent in banks. It also provides convenient ways for international banking and well-organized cash management for internet optimization. It provides banking services throughout the year 24/7 days from any place have internet access. Taking advantage of integrated banking services, banks may compete in new markets can get new customers and grow their market share. It provides more security and privacy to customers, by using state-of-the-art encryption and security technologies.

Knowledge based techniques are classified as recall and recognition based methods needed before performing any online transaction. In recall based technique, user has to recall the secret password which is created before. While in recognition based, user requires to identify or recognise the secret password. There are different types of passwords and some of them are as follows.

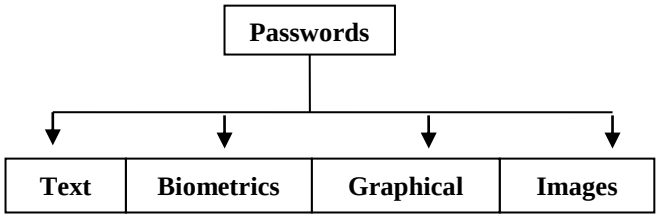

Figure 1. Different types of passwords used for authentication

A. Textual Passwords:

Present Online Banking System is using text based passwords, which is a combination of character, number and

special characters. It is very easy and has maximum chances to hack the accounts.

B. Biometric Passwords:

The biometric traits or samples such as fingerprint, DNA[3], iris, knuckleprint ,palm vein[4] etc., which are given as input or password to login into respective accounts and perform online banking transactions which provides higher security. Present the Biometric passwords are used in few countries as japan, Isreal, Afganistan, South Africa, India etc., in many applications for authentication.

C. Graphical Passwords:

2D & 3D passwords are commonly considered. A virtual 3D password provides means to the user or programmer to combine all permutations and combinations of existing authentication schemes into a 3-D virtual environment.3-D virtual environment is a form of computer-based simulated environment where user can interact with different entities .3d password scheme is very flexible and gives users to create infinite number of passwords possible and it is relatively easy to remember and difficult to hack.

D. Image passwords:

Images are given as passwords for authentication
In the proposed work, both the combination of text and image as passwords is used. Forgetting of any one(either image or password) denys the transaction.

By providing internet banking to customers, most of the banks have revised their business strategies, plans and policies to gain high benefits, which improve performance and decrease operational costs. Consequently, these improved strategies, plans and policies allows internet banking customers to gain access to their bank accounts and make transactions around the clock and around the world and even security concerns are more important for this implementation.
Today, most applications are only as secure as their underlying system. Since the design and technology has improved rigoursly, their detection is a difficult problem. As a result, it is nearly impossible to be sure whether a computer that is connected to the internet can be considered trustworthy and secure or not. Phishing scams became a major problem for e-banking and e-commerce users.

The question is how to handle applications that require a high level of security? The existing system allows user to choose passwords which can be easily hacked and the chosen passwords can be easily guessed and shared to others. No proper security measures were provided in various fields like business, government organizations and academic organizations are investing a lot of efforts, money, time and computer memory system is not providing proper security. The issues raised in existing system are resolved in proposed system.

II. VISUAL CRYPTOGRAPHY

Visual cryptography technique was introduced by Naor and Shamir in 1994 as an alternative for conventional cryptography. It is a form of online identity theft that aims to steal sensitive information such as online banking passwords and credit card information from users. One definition of Visual cryptography is given as "it is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes the job of the person to decrypt via sight reading". Hacker 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. This paper explains the design and why image can be used as password for online transaction and also explains steps taken to process the image and generate shares of images.Noar & Shamir demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n − 1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear.
Using a similar idea, transparencies can be used to implement a one-time pad encryption, where one transparency is a shared random pad, and another transparency acts as the cipher text.
There are few methods to implement the Visual cryptography[5]are K out of K Visual Cryptographic Scheme[6]. K out of N Visual Cryptographic Scheme, General Access structure VCS in which all the shares has equal priority, Recursive threshold VCS [7] in which a secret of s bits is distributed among n shares .Halftone VCS uses half toning techniques to create shares[8][9][10]. It maintains good contrast and security and finally VCS for grey image etc.,even we can provide security to shares by conventional cryptographic method [11].

III. PROPOSED METHOD

The technique implemented in this paper is K out of K visual cryptographic scheme. And K value is taken as 2. In (2, 2) Visual Cryptography Scheme[12], the original image is broken into 2 image shares. Guessing the share, generated while registration is very difficult for an attacker.

A. System Architecture

There are two modules. Registration module & Login Module

1) Registration Module:

In this module, user has to fill personal details, then upload the image based on his or her interest. Half part of the image has been encrypted and stored in Database and remaining half image is given to user .The user has to save this image for future reference and has to use it during login.

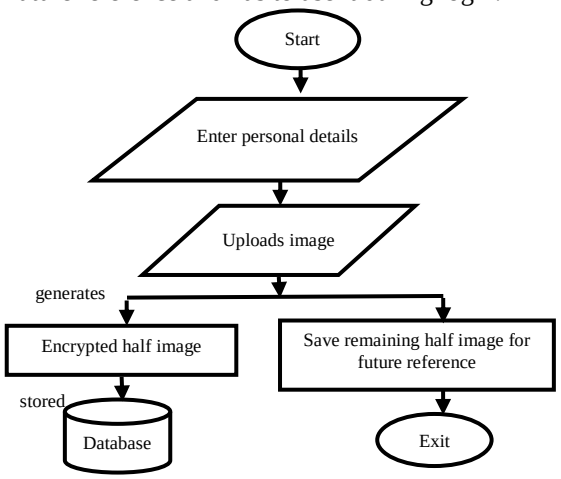

Figure 2. Registration Module

2) Login Module:

In this module user fills his /her credentials and uploads the images given at registration time. The uploaded image is verified with database. If match occurs it gives access rights to perform online banking transactions. If match does not occurs, it asks to relogin or denys the transactions.

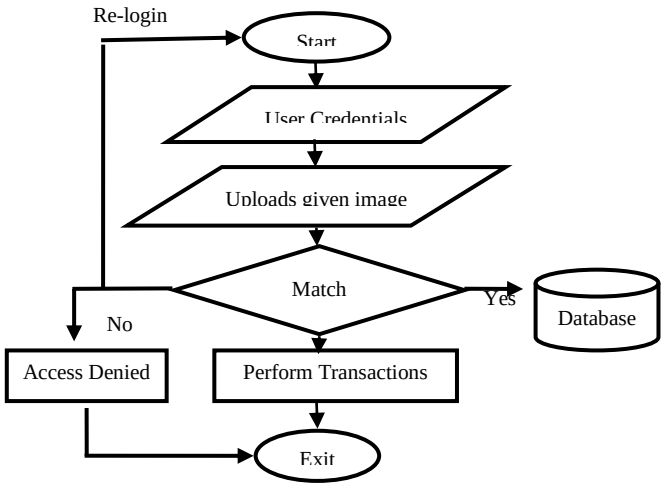

Figure 3. Login Module

This proposed system is more secure because of image based authentication along with text based password than the existing system. Only the legal user knew what image they have uploaded during registration which makes more secure. Password in the proposed system is a combination of characters, numbers, special characters and user selected image. This system perceives more user friendly technique that helps to increase the password quality tremendously along with text based approach.

B. Technical Architecture

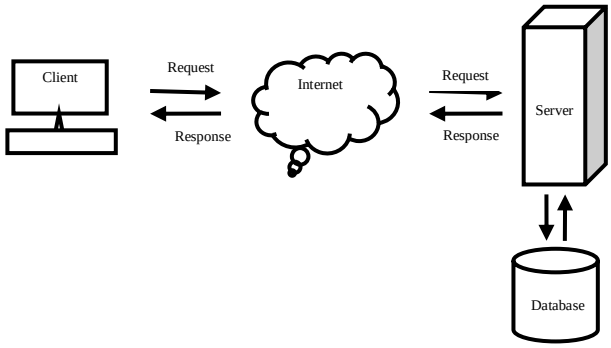

Figure 4. Technical Architecture

Initially Clients sends requests to server during the time of registration and login by filling required fields. The server responds to the requests that are given by client. The required data is saved in database for future reference via server.

C. Algorithm used in this proposed method

```
Algorithm encrypt_Image
//to resize the image to fixed size and divide it into two
halves vertically.
//this algorithm generates chunks number of sub images.
{
    count:=0, rows:=1, cols:=2, chunks:=rows*cols;
    chunk_width=imagewidth/cols,
chunkheight=imageheight/rows;

    for i:= 1 to rows do
        for j:=1 to cols do
            get a portion of the image with dimensions
chunk_width and chunk_height ;
            imgs[count] := extracted image;
            count := count + 1;
}
```

D. Implementation of above stated algorithm

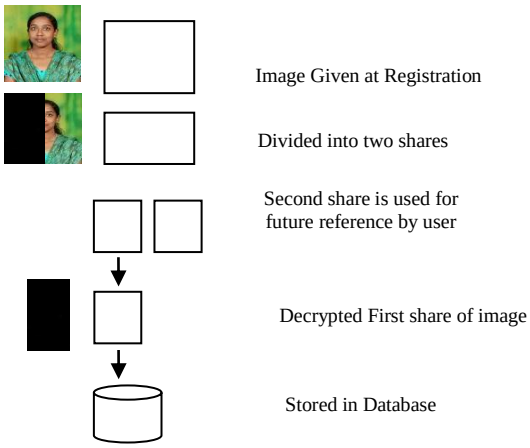

Figure 5. Splitting and Encryption of Original Image

E. Histograms

The histograms for obtained results Share1, Share2 and Original image are shown below. Either left or right half of image is decrypted, that is chosen randomly.

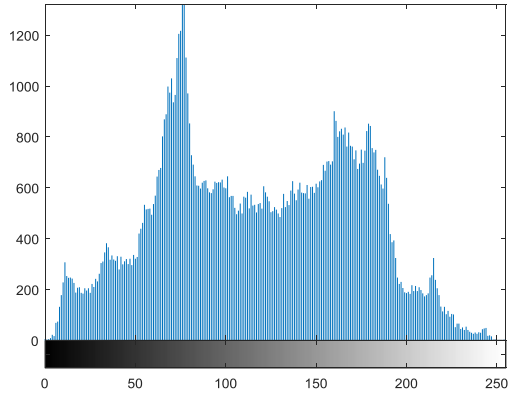

Fig. 6. Histogram for Original Image at registration

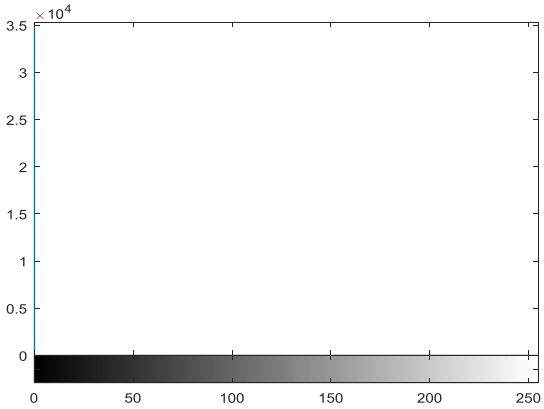

Fig. 7. Histogram for Decrypted image Share 1

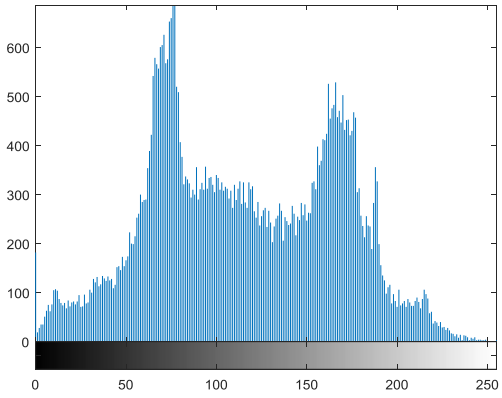

Fig. 7. Histogram for Remaining Image Share2

IV. CONCLUSION

This system provides a better security system for all users. Images are very easy to recall in comparison to string of characters which provides user friendly environment. The purpose of this system is to present the authentication process which is simple enough and cost effective. This work has been successfully developed using the standard software development strategies. It would help the Web Service users fulfil their requirements.It is also used providing security for large datasets[13]. It has many features, which are very secure and helps in protecting user's privacy and identification through image based authentication using visual cryptography. The developed system was successful in depicting the anti phishing based on visual cryptography

REFERENCES

[1] B.V.Prasanthi ,"*Cyber Forensics Tools : A Review*" International Journal of Engineering Trends and Technology (IJETT),vol 41 no 5,pp.266-271,2016.

[2] Prasanthi, B. V., Prathyusha Kanakam, and S. Mahaboob Hussain. "*Cyber Forensic Science to Diagnose Digital Crimes-A study*."International Journal of Scientific Research in Network Security and communication (IJSRNSC), vol 50 no 2,pp.107-113,2017.

[3] Prasanthi, B. V., et al. "*Security Enhancement of ATM System with Fingerprint and DNA Data.*" International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, no. 12, pp. 477–479, Dec. 2014.

[4] Prasanthi, B. V., et al. "*Palm Vein Biometric Technology: An Approach to Upgrade Security in ATM Transactions.*" International Journal of Computer Applications ,vol 112 no 9,2015.

[5] P. S. Revenkar, Anisa Anjum and W. Z. Gandhare. *"Survey of Visual Cryptographic Schemes*". International Journal of Security and Its Applications Vol. 4, No. 2, April, 2010.

[6] Feng Liu, Chuankun Wu, Xijun Lin. "*Step Construction of Visual Cryptography Schemes*". IEEE transactions on information forensics and security, vol. 5, no. 1, march 2010.

[7] A. Parakh and S.kak .”*A Recursive Threshold Visual Cryptography Scheme ”*. Department of Computer Science, Oklahoma State University Stillwater, OK 74078.

[8] N. Askari, H.M. Heys, and C.R. Moloney. ”*An extended visual cryptography scheme without pixel expansion for halftone images”*. 26th annual ieee canadian conference on electrical and computer engineering year 2013.

[9] Zhi Zhou, Gonzalo R. Arce and Giovanni Di Crescenzo. ”*Halftone Visual Cryptography”*. IEEE transactions on image processing, vol. 15, no. 8, august 2006.

[10] D. Jena and S. Jena . ”*A Novel Visual Cryptography Scheme*”. 978-07695-3516-6/08 2008IEE DOI 10.1109/ICACC.2009.109

[11] Kulvinder Kaur and Vineeta Khemchandani. ”*Securing Visual Cryptographic Shares using Public Key Encryption*”.3rd IEEE International Advance Computing Conference (IACC),pp.1108-1113,2013.

[12] Bhuyan, Sangeeta.” *Image Security using Visual Cryptography*”. Diss. 2015.

[13] Bonthu, Sridevi, B. V. Prasanthi, and K. Himabindu. "*Automation Of Pre-Processing Of Students Data*",vol 8 no 3,pp.241-245,2016.

Authors Profile

Mrs. B.V.Prasanthi pursed Bachelor of Technolgy in Computer Science & Engineering from Kakatiya University, Kothagudem in 2009 and Master of Technology in Computer Science & Engineering from JNTUH affiliated college,Hyderabad in year 2014. She is currently working as Assistant Professor in Department of Computer Science, in Vishnu Institute of Technology since 2014. Her main research work focuses on Information Forensics, Network Security and Biometrics. She has 3 years of teaching experience.

Sridevi Bonthu received her B.Tech. in Computer Science and Engineering from Acharya Nagarjuna University, India and her MTech in Computer Science from JNTUK, Kakinada, India. She is currently a faculty in Computer Science and Engineering department at Vishnu Institute of Technology, Bhimavaram, Andhra Pradesh, India. Her primary research interests include web application development, Big Data, data and web analytics.

