ISSN:0975-9646

Multi-factor Authentication in Banking Sector

Tushar Bhivgade , Mithilesh Bhusari , Ajay Kuthe , Bhavna Jiddewar ,Prof. Pooja Dubey

Department of Computer Science & Engineering,
Rajiv Gandhi College of Engineering & Research, Nagpur,India.

Abstract-In the world of Internet, security is the major concern to avoid fekes and forgeries. Internet does not use secure links, thus it is necessary to provide security measures against the most common attacks on web-applications. Since now a days all the transactions are done via Internet so it's an urgent need to protect the data from malicious attacks. The purpose of this project is to develop a secure multi-factor authentication that would provide high security in their own web-applications. The risks of using static passwords to authenticate users show more and more security risks with the development of hacking.

In this paper, we introduce a DCT based steganographic method for data hiding. The embedding approach is designed to satisfy three goals; maximizing the amount of hidden message, minimizing difference between the cover image and stego-image, and maximizing the robustness of embedding. This paper gives a solution to implement Multi-factor authentication.

Keywords-Multi-factor Authentication,Single-Factor Authentication, Discrete Cosine Transform (DCT), Steganography.

1. INTRODUCTION

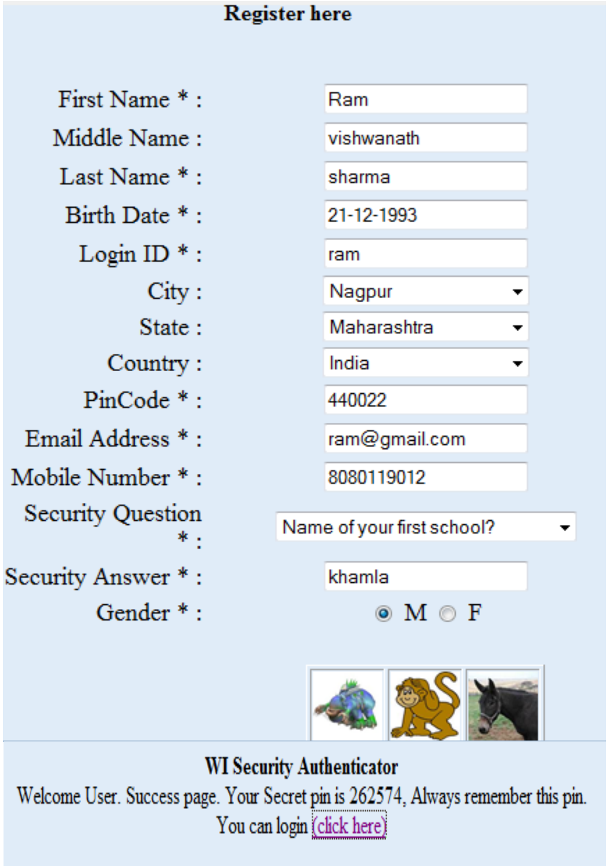
Security and usability in web application's aretwo important factors that are designed to prevent from malicious attack. As the communication increases day by day the value for security over network also increases. Presently, most users need to use user name and password to log on for authentication. Passwords used in systems, such as email system, online banking, are most static. But static passwords don't provide security. One advantage is that static passwords are easy to remember. But There are many disadvantages of static passwords that includes how easy they Are to decipher. Also they are vulnerable to social engineering, i.e., people asking for passwords or guessing them correctly. Nowadays it is not a hard job to obtain passwords by using hacking tools. There-fore, a more secure multi-factor authentication mechanism is needed.

1.1 Multi-factor Authentication

Multifactor Authentication is the latest secure authentication technique. Since Single-factor authentication (SFA) have been used widely. It is not secure enough for online financial transactions. Single factor authentication has been around for a while now. Yet it's not enough for having any meaningful security. The solution is to have multi-factor authentication which includes following authentication factors:

- Username
- Question Answer Verification
- Image Authentication
- Password

The security levels are increased by using multiple authenticating factors. Multi-factor authentication adds more Security because the user must provide more than one "secret" Entity i.e. the security question. The Image response confirmation of a previously saved image allocated to each user during registration into the authentication server gives user satisfaction that he is on correct site. This prevents us from Phishing attack. Random number created by system is made by using current date and time of registration. This increases more security as date and time is unique each time user registers. Main Objective of MFA is to provide security to online transactions



Register here

First Name * :	Ram
Middle Name :	vishwanath
Last Name * :	sharma
Birth Date * :	21-12-1993
Login ID * :	ram
City :	Nagpur
State :	Maharashtra
Country :	India
PinCode * :	440022
Email Address * :	ram@gmail.com
Mobile Number * :	8080119012
Security Question * :	Name of your first school?
Security Answer * :	khamla
Gender * :	● M ○ F

WI Security Authenticator

Welcome User. Success page. Your Secret pin is 262574, Always remember this pin. You can login (click here)

Fig. 1: Registration Process

1.1.1 Registration Process :

For Authentication user have to go through different steps. When user registers to Bank site, he first enters his User Name then he has to select the Question and Answer it uniquely. After following these steps set of Images are shown to user and he has to select the one. This Image response confirmation is given to user at the time of log in, This selected image is saved in the authentication server, server then shows this selected image during log in time that you have selected this image during registration. This gives user satisfaction that he is on correct site. This prevents user from Phishing attack. After that system will generate the password which is of six digit using Walsh algorithm[1]. Password generation is based on current date, time, minute, second. At what time and at which date user is registering to bank site using that date and time password is generated which is unique at each minute and at each second.

Increasing security levels increases efforts to be spent in order to hack the system.

1.1.2. What is Steganography ?

There is another important issue of steganography, Steganography[4] is the science of *covered writing*. Its purpose is to hide information in a cover medium so that it is "hard" for everyone to detect the existence of the embedded information. By embedding a secret message into image, a stego-image is obtained. It is important that the stego-image does not contain any easily detectable information.

The embedding is typically parametrised by a key; without knowledge of this key it is difficult for a hacker to detect or remove the embedded material. Once the cover object has material embedded in it, it is called a *stego object*. Some papers introduced the utilization of various embedding techniques in DCT domain [4, 5].

2. Literature Review

In literature review we focuses on insecurity in web applications and try to find evidence of principles, methods, and tools that can clarify the need for security, and usability. Our focus is primarily on web-based authentication systems. The focus of this review is those authentication methods that regular people use on a daily basis. Initially, our user domain is populated with home users, businessman's, and so forth. The rest of this paper is organized as follows. The first section deals with describing and understanding the users of online authentication, their perceptions towards security, discussing notions of risk, and privacy in this context. Section 2 goes along a different path, as we introduce the most common authentication method used on the internet today: passwords; to get more security we introduce new technique called Multi-factor Authentication. Section 3 deals with those usability factors important when designing usable security. In section 4 we introduce current methods for developing usable security software. Some algorithms are used and their implementation is carried out. We conclude the review by outlining recommendations for further research and development.

3. Problem Defenition

Before MFA Single-factor authentication (SFA) have widely used. It is not secure enough for online financial transactions. Single-factor authentication is not secure now-a-days. It uses only user name and password to authenticate the user. Passwords used in Single-factor authentication are static in nature. Most people can agree on the fact that the longer the password, the better the protection of the service it grants access to. Three reasons are obvious:

- The time it takes to input the password naturally grows as the length grows,
- There is a more possibility for typing errors, and
- Very few people are capable of memorising passwords of such lengths.

3.1 Weak Single-factor Authentication

- There is one main advantage and many disadvantages to weak single-factor authentication, which many are more familiar with as the single static passwords still employed by most companies. One advantage is that static passwords are easy to remember. However, when different systems have different passwords, they can be difficult to remember and may have to be written down, raising their vulnerability.
- The many disadvantages of single static passwords include how easy they are to decipher.
- Most often, they are short and based on subjects close to the user—birthdays, nick names, children's names and so on.

Multi-factor authentication seeks to decrease the problem of static password. It includes more authentication levels to log on,namely Username, Password, Question Answer verification, and Image Authentication.

4. Proposed System

Data hiding techniques have been widely used to hide secret message for long time. Ensuring data security is a big challenge for us. Businessmen, professionals, and home users all have some important data that they want to secure from others. In this proposed system we are generating password by using Walsh algorithm and encrypting it in image using DCT algorithm. This system combines the effect of these two methods to enhance the security of the data. The proposed system encrypts the data and then embeds the encrypted data in an cover file. This system improves the security of the data by embedding the encrypted data and not the plain data in image. The block diagram of proposed system is as shown in fig 2

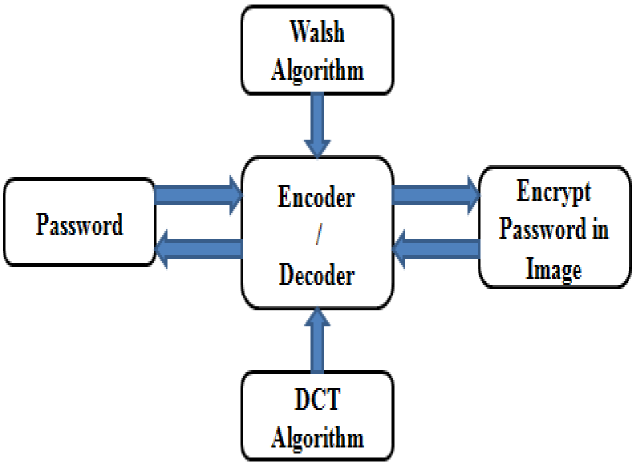


Fig. 2: Block diagram of proposed system

Above figure depicts the encoding and decoding of password in image. Encoding of password is done when

User registers to bank site, enters his/her details and password generated by system is encrypted in image

On the other hand, As soon as user enters password to Log in, System apply the inverse DCT in order to get the encrypted key from Lena image and if calculated answer match the encrypted key user is permissible to access account otherwise he has to enter correct password.

We have introduced a new randomization method for generating the randomized key.

4.1 Proposed Work

During registration, System itself generates password by using Walsh Algorithm[1] ,and during log in time when user enters password, it will not directly save in database instead, it will save in the Lena image. password is embedded in image by using DCT Algorithm[2].

4.1.1 Walsh Transform:

Walsh transform[1] makes the image compression algorithm orthogonal transform stage more fast and easy. This method increases the Walsh-based image compression algorithm speed by 30% for compression and by 60% for decompression. The JPEG algorithm is a "de-facto" standard for image compression. It is the lossy compression algorithm based on DCT (Discrete Cosine Transform). The natural ordered Hadamard matrix is defined by the formula , and the sequency ordered Hadamard matrix is formed by rearranging the rows so that the number of sign-changes in a row is in increasing order.

The Hadamard matrices of dimension 2^k for $k \in N$ are given by the recursive formula

The lowest order of Hadamard matrix is 2

$$H(2^1) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

$$H(2^2) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix},$$

$$H(2^k) = \begin{bmatrix} H(2^{k-1}) & H(2^{k-1}) \\ H(2^{k-1}) & -H(2^{k-1}) \end{bmatrix} = H(2) \otimes H(2^{k-1}),$$

and in general for $2 \leq k \in N$, where $\otimes$ denotes the Kronecker product.

The Walsh matrix (and Walsh functions) are used in computing the Walsh transform and have applications in the efficient implementation of certain signal processing operations.

4.1.2 Discrete Cosine Transform:

A discrete cosine transform[2] expresses a finite sequence of data points in terms of sum of cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering, from lossy compression of audio (e.g. MP3) and images (e.g. JPEG) (where small high-frequency components can be discarded).

DCT is a general transform for digital image processing and signal processing with advantages such as high compression ratio, small bit error rate, good calculation complexity. DCT allows an image to be broken up into different frequency bands namely the high, middle and low frequency bands thus making it easier to choose the band. In DCT based techniques, DCT coefficients are obtained for the given carrier image. The secret data is embedded in the carrier image for DCT coefficients lower than the threshold value. To avoid visual distortion, embedding of secret information is avoided for DCT coefficient value 0. Insertion and extraction of secret image is an important part for any steganographic technique.

4.1.3 Modules of our Project are:

Password Generation :

Walsh Algorithm is use to generate the password.It uses the 2*2,4*4 matrix to arrange the elements. The lowest order of Hadmard matrix is 2*2. Formula is :

$$H(2^1) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

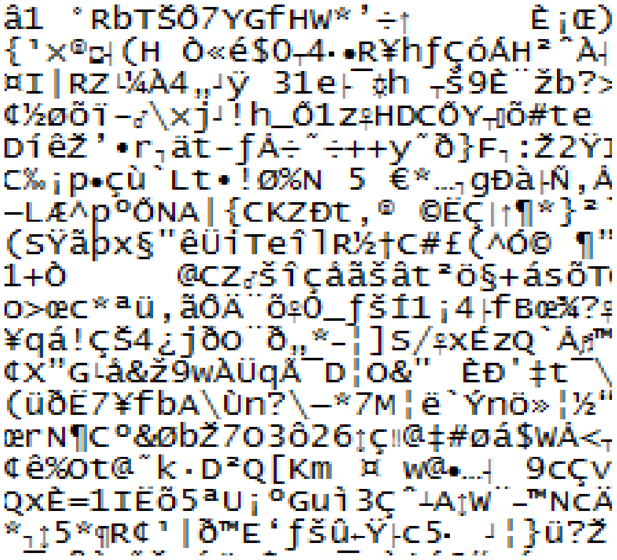
$$H(2^2) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix},$$

Password Encryption :

The stego-image quality and message capacity are the two most important criteria in evaluating a steganographic method. Thus, we focus on these two criteria. During registration, System itself generates password by using Walsh Algorithm as stated above, and during log in time when user enters password, it will not directly save in database instead, it will save in the Lena image. Password is encrypted in image by using DCT algorithm[3].

DCT has advantages such as high compression ratio, small bit error rate, good calculation complexity. It allows an image to be broken up into different frequency bands namely the high, middle and low frequency bands thus making it easier to choose the band. Multiple factors are present in MFA. The first factor is usually in the form of PIN or password that the user types, for instance, into a web-based Internet application. The second factor is usually in the form of mobile phone that is known to be able to receive OTP as SMS directed to a particular mobile phone number.

The same process is followed in communication between sender and receiver. The proposed scheme consists of two processes, the hiding process and the extraction process. Suppose a sender wants to share some information with a receiver. The sender uses the hiding process to hide the information in a cover image and then delivers the stego image to the receiver. When the receiver receives the stego image, the extraction process is used to decode the stego image and to extract the information.If the user successfully retypes this OTP into the web application.Password is stored in Lena image anywhere belonging to any pixel value. The encrypted message is stored in the background of image .If we open this image in notepad it shows byte code which human can't read.If we try to see this password even also it is invisible like this :



```
âl  °RbTŠÔ7YGfHW*'÷↑        È¡Œ)
{'x®¤┤(H Ò«é$0┬4·•R¥hƒÇóÁH²ˆÀ┤
¤I|RZ└¼À4„┘ÿ 31e├¯¢h ┬š9È¨žb?>
¢½øõï-♂\xj┘!h_Õ1z♀HDCÕY╤Õ#te
DíêŽ'•r┐ät-ƒÅ÷˜÷++y˜ð}F┐:Ž2Ÿ]
C‰¡p•çù`Lt•!Ø%N 5 €*…┐gÐà├Ñ,Å
—LÆ^p°ÕNA|{CKZÐt,® ©ËÇ|↑¶*}²`
(SŸãþx§"êÜiTeîlR½†C#£(^Ó© ¶"
1+Ò        @CZ♂ŠîçåãšâT²ö§+ásõT
O>œc*ªü,ãÕÄ¨õ♀Õ_ƒšÏ1¡4├fBœ¾?♀
¥qá!çŠ4¿jðo¨ð„*-¦]S/♀xÉzQ`Å♫™
¢X"G└å&ž9wÀÜqÅ¯D¦O&" ÈÐ'‡t¯\
(üðË7¥fbA\Ùn?\—*7M¦ë`Ýnö»¦½"
œrN¶C°&øbŽ7O3ô26↕ç‖@‡#øá$WÅ<┬
¢ê%Ot@˜k·D²Q[Km ¤ w@•…┤ 9cÇv
QxÈ=1IËõ5ªU¡°Guì3Ç˜┴A↕W¨—™NCÄ
*┐↕5*¶R¢'|ð™E'ƒšÛ┼Ÿ├c5· ┘¦}ü?Ž
```

Figure 3 shows secret message encrypted in Lena image

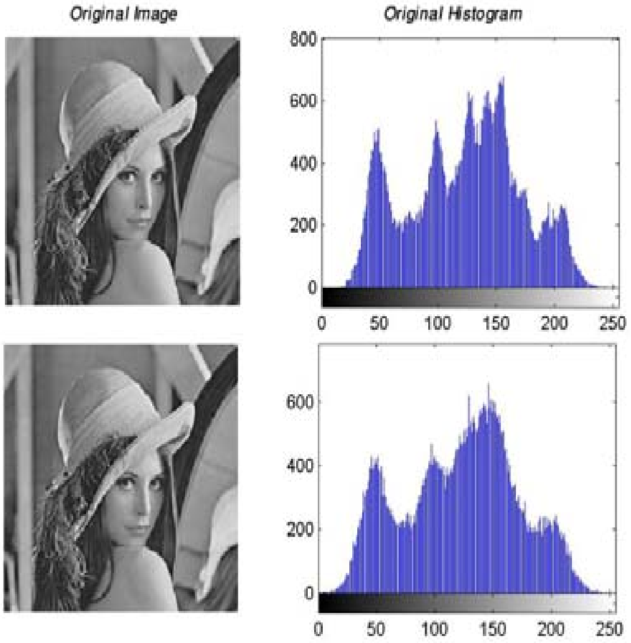


Figure 4 shows the original image and encrypted image with its histogram

Password Decryption:

After Registration, when user Logs In, password entered by him is verified by using Inverse DCT. User enters password to Log in, System apply the inverse DCT in order to get the encrypted key from Lena image and if calculated answer match the encrypted key user is permissible to access account otherwise he has to enter correct password

.

5. System Architecture

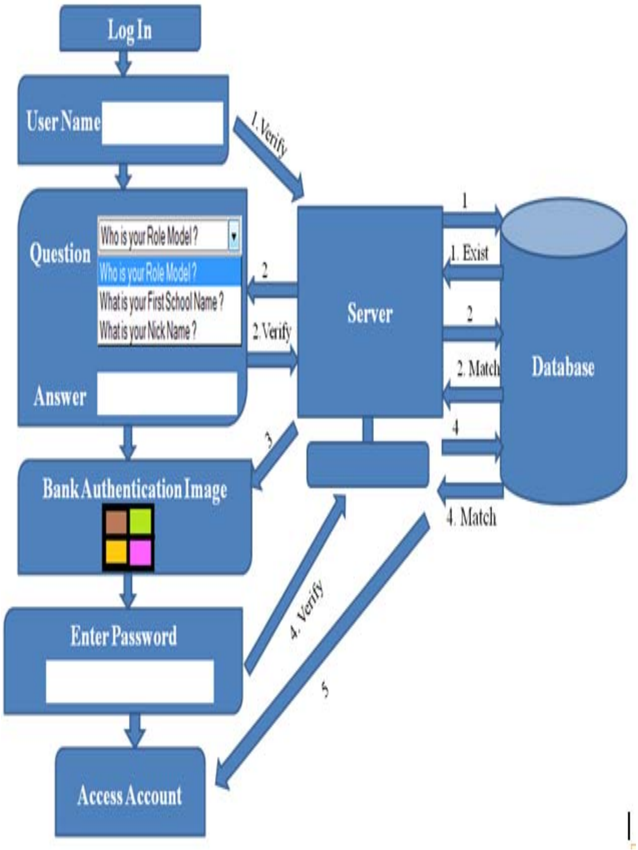


Fig 4: Authentication Process

5. Conclusion

In this paper, we proposed the process of multi-factor authentication of user identity can be achieved through the dynamic password provided by system during registration. The reliability of verification is improved and all user information verified will be stored in the system for later use. The goal of data hiding is to make the secret messages hidden in the cover-images. We proposed a simple and efficient information-hiding scheme based on the quantization based embedding technique for images. We compared the image quality and hiding capacity of the proposed method. The observations on the visual quality of the stego-images and encrypted images in the proposed method were also given. The proposed scheme can not only conceal large amount of secret information in the cover images but can also repair the stego image to generate the repaired image, which only has a small distortion compared with the original cover image.

Acknowledgment

We are sincerely expresses our gratitude to Department of Computer Science for providing necessary help and assistance. Our thanks to Prof. Pooja Dubey who guided us to develop such an innovative idea and who have contributed towards development of the template.

REFERENCES

[1] A.Pratt,"Hadamard Transform Image Coding," Proceedings of the IEEE, vol. 57, No. 1, Jan., 1969.

[2] Sican Gmbh “Method and circuit for forward/inverse discrete cosine transform (DCT/IDCT)” Dec1,1995

[3] K. WONG and K. TANAKA , “StegErmelc: A Novel DCT-Based Steganographic Method Using Three Strategies”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 2008 E91-A(10):2897-2908.

[4] K.B. Raja, C.R. Chowdary, K.R. Venugopal, L.M. Patnaik,“A Secure Image Steganography Technique”,ICISIP 2005 Third International Conference on Intelligent Sensing and Information Processing 2005,Sp.p. 170- 176.

[5] K. Wong, X. Qi,Tanaka,“A DCT-based Mod4 method Steganographic ”, Signal Processing 87 2007, p.p.1251–1263.

[6] P. Dourish, R. E. Grinter, J. D. de la Flor, and M. Joseph. Security in the wild: User strategies for managing security as an everyday, practical problem.8:391–401, 2004.

[7] Hsu,C.-T.,Wu,J.-L,(1998)"Multiresolution Watermarking for Digital images", in IEEE Transactions on Circuits and Systems - II: Analog and Digital Signal Processing, vol. 45,no. 8, pp. 1097-1101.