2nd International Conference on Current Research Trends in Engineering and Technology
© 2018 IJSRSET | Volume 4 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Image Password Based Security System

Ravi Pandya[1], Jay Patel[2], Bhumi Patel[3]
[1-3]Computer, Sigma Polytechnic, Vadodara, Gujarat, India

ABSTRACT

In today's world, hacking is starting to become a major issue and this is the reason that user cannot easily trust the information on the internet. To solve the problem of authenticity, we are proposing an algorithm based on Visual Cryptography and watermarking and this algorithm is applicable for any Login authentication system. This Research proposes a technique of hiding username and password into QR-code after using VCS dividing it into 2 shares or sub images where one of the shares is stored in the database and the other is watermark with reCAPTCHA or User define image and kept by the customer. During all of his transaction the Customer has to present his watermark image. So it will extract share is stacked with database share to get the original QR-image. Once again Decoding is used to extract the secret username and password from the QR- image. Compare it with the original, if both are same user authenticity may be granted and if both are not same, one can decide that the share produced by user is fake and can be rejected.

Keywords: Secure Login, QR-Code, VCS (Visual Cryptography Scheme), Embedding.

I. INTRODUCTION

The Dramatic increase of computer usage has given rise to many security concerns. One major security concern is authentication, which is the process of validating who you are to whom you claimed to be. The password is a very common and widely authentication method still used up to now but because of the huge advance in the uses of computer in many applications as data transfer, sharing data, login to emails or internet, some drawbacks of normal password appear like stolen the password, forgetting the password, week password, etc so a big necessity to have a strong authentication way is needed to secure all our applications as possible, so researches come out with advanced password called multiple password techniques where they tried to improve the password techniques and avoid the weakness of normal password. (Sobrado and Birget, 2007), today, many networks, computer systems and Internet-based environments used this technique to authenticate their users. The vulnerabilities of this technique have been well known generally.

Dictionary attack is the commonly method used by hackers to break or crack the alphanumeric password, such attack is very efficient mechanism because its only need a little time to discover the users passwords. Another major drawback of this method is the difficulty of remembering the passwords. Recent studies (Dhamija et al, 2000) showed that humans are only capable to memorize a limited number of passwords, because\ of this syndrome, they often to write down, share and use the same passwords for different current account.

Graphical password techniques have been proposed as an alternative to conventional based techniques. It has

been designed to overcome the known weakness of conventional password. It also designed to make the passwords more memorable, easier for people to use and therefore more secure. Based on the two assumptions; first, humans can remember pictures better than alphanumeric characters and second, a picture worth a thousand passwords.

A collection of usability features will be implemented in the multiple password prototype to be more usable for the users where this usability set includes more secure, the ease of use, memorize, creation, learning and satisfaction. Finally we propose a new secure password authentications scheme.

II. RELETED WORKS

In [1] has presented a novel system for data and image encryption using AES algorithm for cryptography, image steganography and image stitching which can be used by banking, consultancies and detective agencies. As the image to be sent is broken down into parts and encrypted individually and sent over the network it becomes difficult of the intruder to get access of all the parts. Additionally since every part is camouflaged by a cover image, the encrypted image looks like just another regular image.

In [2] While creating an account the bank, signature of the applicant is taken by scanning his/her signature from the application. Now the scanned image is taken as input and is pre-processed. This pre-processed image to encrypt into two share by using two out of two scheme. One share is stored in the bank database, another share is printed and given to the applicant. Applicant had to provide his share during every transaction. During transaction applicants share is scanned and overlapped with the bank's share, if higher correlation coefficient is obtained, then authentication will be success.

In [3], a payment system for online shopping is proposed by combining text based steganography and visual cryptography that provides customers data privacy and prevents misuse of data at merchant's side. The method is concern 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 proposed method can be applied for E-Commerce with focus area on payment during online shopping as well as physical banking.

In [4] have proposed an effective technique to provide greater security in the field of Internet banking system by restricting the unauthorized user. To verify the same by giving note or image will be broke into two parts and one will have buyer another will have seller, after meeting they need check it if it matches then item and money will be exchanged otherwise not. Based on this concept we did this application. It's useful to customers, website holders and banks. Image will divided, first half send to customer and second half of image will be kept in bank server. In future enhancement this can be extended to signatures. Here image are taken as inputs since they are uniquely Identified, but according to the user and bank convenience any kind of images can also be used like signature image of the applicant.

In [5] there are many techniques and methodologies applied for watermarking of images. In this paper, method to perform secure authentication using captcha image is discussed. The user has to generate image of the unique id and send to the server. Then watermarking techniques are used to check the re-captcha image and checks for authenticity.

III. PROPOSED SYSTEM

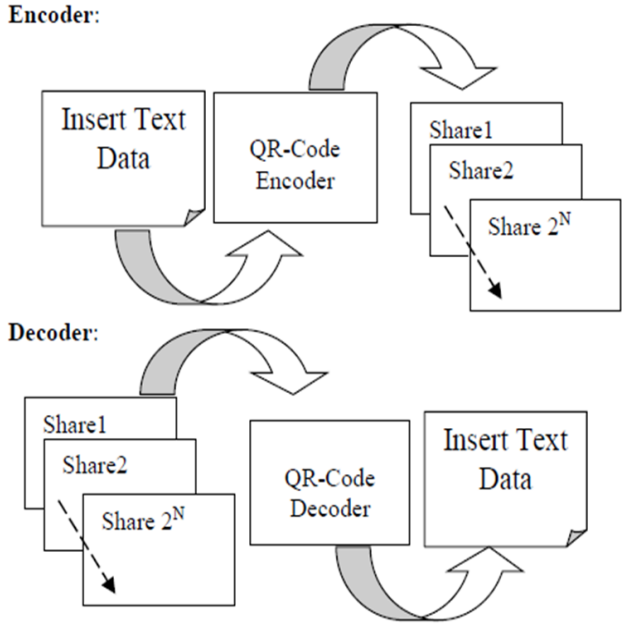

Figure 1: Proposed System Flow Diagram

As shown in the figure 1 Decode block diagram, First User will do the login process and if the login is successful the next step will be selection of Recaptcha after then Water marking will be done. VCS will be applied on the selected Image and both the shares will be add for authentication. After that QR code decoding technique will be applied and at the last Login Successfully done.

As shown in figure 1 Encode block diagram, User will register his/her personal information in order to use the system. First user will input the user name and password for main authentication purpose after that the system will perform the pre-defined method of high secured registration that is encoding of QR code. In that the username and password will be encoded so that no one else can hack or try to see the same.

After QR code encoding VCS technique will be applied to add some more security in the process which will make the 2 different shares of image. One will be stores in Data Base and the other will go to the watermarking. In watermarking technique the image will be checked and compare that the image user is selected is actually same as the one stored in database or not if it is not same then the user will not allow to use the system and if it matches then the request will be completed.

A. QR-Code

i. QR Encoding: In encoding process, first take text data as an input and evaluate QR code using ZXing library. After that generation of shares in user define patterns.

ii. QR Decoding: At the decoding new Combine XOR based VCS apply to convert share into QR-code. Usually, QR decoding is done with the help of camera equipped mobile phones and scanner. The decoding technique is just the inverse of the encoding technique.

B. Visual Cryptography

Visual cryptography is used to encrypt information like handwritten text, images, etc. The original information to be encrypted is called as secret. No mathematical computations are required to decrypt the secret. The generated ciphers are referred as shares. The part of secret in scrambled form is known as share. Fundamental idea behind visual cryptography is to share the secret among all participants. To share the secret, it is divided into number of shares. These shares are distributed among the participants. To retrieve the original secret, each participant provides his own share. Complete knowledge of all shares is unable to decrypt the secret.

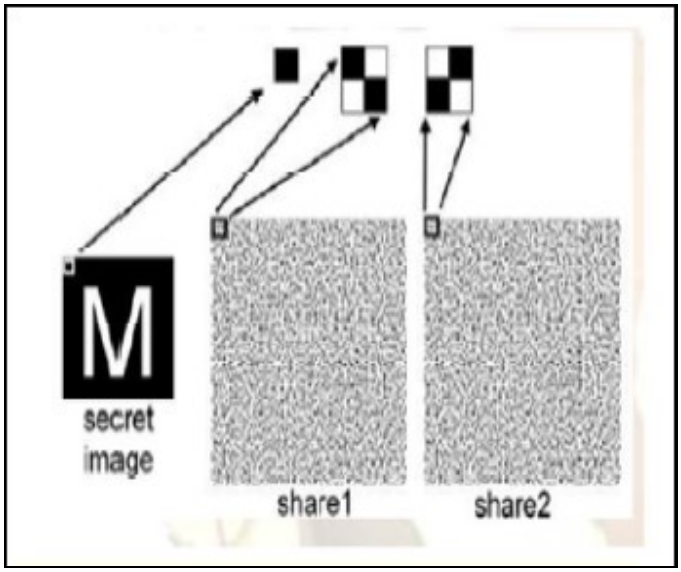

Figure 2: VCS Flow

Every pixel from the secret image is encoded into multiple sub pixels in each share image using a matrix to determine the colour of the pixels. In the (2, N) case a white pixel in the secret image is encoded using a matrix from the following set, where each row gives the sub pixel pattern for one of the components.

C. Image Steganography

Steganography is used for hiding a message within an image or audio file in such a way that someone cannot know the presence of contents in the hidden message. Steganography attempts to hide the existence of communication. The basic structure of Steganography contains three components: the "carrier", the message, and the key. The carrier can be a painting, a digital image or an mp3. It is the object that will 'carry' the hidden message. A key is used to decode/decipher/discover the hidden message.

TABLE I

ANALYSIS OF TRANSFORMATION

Compressive Sensing Method	Advantage	Disadvantage
DWT [1][2]	-Robust Image Compression For The Signals /Images Are Practically Sent Over Noisy Channel. -Wavelet Based Uses The Parallel Computing -Introduce Block Artifacts In The Reconstructed Image.	-Do Not Provide Directionality (Multi-scaling) And Anisotropy So Does Not Produce Good Result While Capturing Edges.
DCT[4][1]	-Low Processing Power	- It Has Blocks Artifacts Means Loss Of Some Information.
DCT[4][1]	-Fast Algorithms Can Be Used For Computation, And The Output For (Near) Constant Matrices Generally Consists Of A Large Number Of (Near) Zero Values.	-While The Input From Pre-processed 8 X 8 Blocks Are Integer-valued, The Output Values Are Typically Real-valued. Thus We Need A Quantization Step To Make Some Decisions About The Values In Each DCT Block And Produce Output That Is Interger-valued.

IV. RESULTS

Input:ravi@123

Figure 3: QR-Code

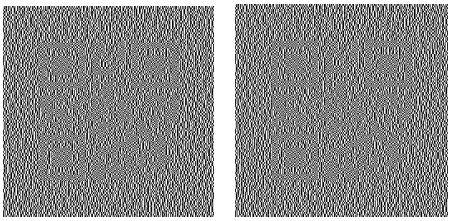

Figure 4: Visual Cryptography

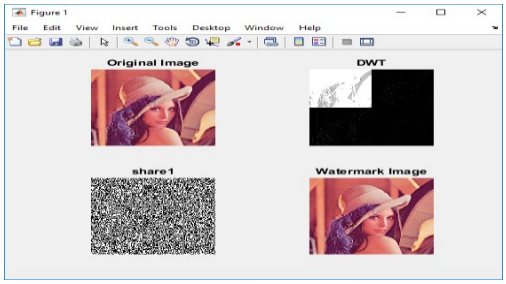

Figure 5: Watermarking

V. CONCLUSION

We have come to a conclusion that the proposed system have managing your accounts with security. In all the accounts on internet, security begins with the authentication process. We propose an algorithm to secure the user's information .Our system will provide efficient as well as Privacy. In final we had a factor like if user wants to protect his/her all the account then they have to buy premium membership for that also.

VI. REFERENCES

[1] Shubhangi Khaimar, Reena Kharat "Online Fraud Transaction prevention system using Extended Visual Cryptography and QR code"

[2] Nancy Victor "Enhancing the Data Capacity of QR Codes by Compressing the Data before Generation "International Journal of Computer Applications (0975 – 8887)Volume 60– No.2, December 2012

[3] Delphin Raj K. M and Nancy Victor "Secure QR Coding of Images Using the Techniques of Encoding and Encryption"International Journal of Applied Engineering Research ISSN 0973-4562 Volume 9, Number 12 (2014) pp. 2009-2017

[4] M. Sukumar Reddy, S. Murali Mohan "Visual Cryptography Scheme for Secret Image Retrieval"IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.6, June 2014