4.1 Introduction to Choice Based Graphical Authentication

Security has been an issue from the origin of social networking sites and users have related safety issues with usability. Secured systems must be usable to maintain proposed security so we need to have a proper password authentication that must be usable and secure. Text passwords are widely used but suffer with respect to both security and usability problems. The existing framework of text based passwords is benefited by combining graphical password with text password at login in social networking sites, might proves useful. The framework includes better password strength (space), better protection from key logging attacks, protection from phishing and man in the middle attacks. It consists of a regular text login followed by a graphical component. For logging in the social networking site, the user will choose one image from a grid of images, called TwoStep concept which is similar in concept to Passface (Brostoff and Sasse, 2003).

A password is said to be trustworthy and efficient if it fulfills the following two requirements:-

Usability: Passwords should be simple. It should be easy to remember and must take less time to process the authentication.

Security: Passwords should be secure. It must not be easily guessed. Also the user must change their passwords regularly.
A combination password that is text based and graphical authentication at login in social networking sites is proposed as a potential solution to the problem. Pictures are usually easier to be remembered or accepted than text. Also, since the number of possible pictures is sufficiently large than that of text based schemes so this technique provides better resistance to dictionary attacks, shoulder surfing, brute force.

4.1.1 Analysis of Choice Based Graphical Authentication

Our novel framework combines textual and choice based graphical password system that enhances the security, keep the resources optimized and smoothen the working in social networking sites. Main goal of our designed framework is that it works as a combination based graphical authentication scheme that allows users to make combination of text, image and number as their password to successfully overcome existing forms of ethical social hacking. With the new developments, the accent on building very secure system is paramount since services are not on client’s computer and the server would need to know who is an authorized user. So, the proposed framework will authenticate user while logging in social networking site. Along with the textual password, the chosen image will be encrypted and stored on the server.

The foremost usable features of graphical authentication are listed below:

1. Improved memorability: The chosen images are very easy to remember and recall.
2. Simple, cost efficient and tension free login experience: Our proposed framework achieves the desired security without the support of any extra hardware. It does not need costly software installations or dedicated hardware to run. The login interface is very sensitive and spontaneous.
3. Cognitive scalability: Our proposed framework is language independent. The defined set of images or pictures are ideal for use by everyone.
4. Software as a Service (SaaS): This framework can easily be included into current secure online validation for authentication in various financial applications like ATM, ecommerce and mobile commerce.
5. Configurable: The framework is designed to increase the security and can be customized based on user requirements. The attributes like number of images, length of the password etc can be altered.

We believe that authentications between the user and the server are made secure through SSL that avoids simple attacks based on network sniffing. The Brute force attack, Dictionary attack are the listed countermeasures against possible attacks on our framework of graphical authentication in social networking sites.

1. Brute force attack: The attacker must presume the password images from the grid to break the password. He tries to randomly guess the one time access code which strengthens the security of choice based graphical authentication at users profile login in social networking sites.

2. Dictionary attack: In choice based graphical authentication, each user authenticates him with a set of six random images and the textual password. Users are free to use dictionary words as password. Although this may appear as a threat since an attacker can build a dictionary of most common six-letter words with maximum permutation of 21,767 English words.

3. Social engineering attack: At every login, images are randomly placed in the grid with a different set of numbers associated with them. The positions of images as well as the related numbers within the grid changes, in regular interval of usage which makes the password unique per session. Thus social engineering techniques are difficult.

4.1.2 Framework Design

System includes a SQL server for storing user information and graphical password, GUI is provided with the help of windows forms, which provide an interface for interaction to users with the system for creating graphical password by choosing images.
4.1.3 Registration Process

1. User has to fill the form for doing registration in the webpage of SNS.

Figure 4.1: Flow Chart of Proposed Choice Based Graphical Password.
2. User clicks the signup button if not an existing member of this social networking site.

![Login Page Screenshot](image)

Figure 4.2: Screen Shot of Login Page Showing Choice Based Graphical Password Authentication.

After clicking the signup option, user is required to fill the credentials in the form.

1. User has to enter his first name that must not be more than 20 char long. It must be character only.
2. Gender, to be filled as option button.
3. User also has to enter date of birth by using calendar or by typing in dd-mm-yyyy format.
4. User must fill valid email-id to get confirmation message. If user gives wrong password then it will not register him. If user leave any field empty than alert message is shown to user.
5. User is required to fill state, country in the signup form.
Figure 4.3: Screenshot of the Registration Form for a New Member.

By clicking on signup button it will send six character verification code on given email-id submitted at registration time.
It includes combination of character and number.
If user enter correct e-mail id than popup window is generated which shows message "Verification code send to your mail".
If user enter wrong e-mail id then code will not be send. If user not gets verification code it will not complete registration process.

It is very important step as it identify that user creating account is not fake user.

It is mandatory that password must contain four characters and two numbers.
User has to enter password that is combination of an image, text and number. The sequences of characters and numbers images are depending on user but strictly follow this sequence during login. All images placed randomly. It means every time place of each image is different. It creates record in the database table. From this page user can go on start page.

![Login Screen](image-url)

Figure 4.4: Login Screen for Verification of User Name, Password and Image

4.1.4 Findings

We have conducted a survey questionnaire with 300 participants to evaluate the feasibility of our proposed framework. Results of the test are satisfactory which confirms that our proposed system of profile login in social networking site is secure as discussed in Chapter 6.

The survey was conducted by using a questionnaire to determine the impact of attacks against choice based graphical passwords that depends on choosing from specific image. In total, this study managed to recruit a total number of 300 participants with age group range from 12 years to more than 50 years.
We believe that when choice based graphical password is combined with text passwords, may help to bridge the gap between security and usability. This framework also has a very good performance in terms of speed, accuracy and ease of use.

Majority of the participants were female, where only 88 of the participants were male, 165 of the participants were undergraduate students and rest include professionals or home makers. They have been asked if they would like to have graphical user authentication along with text password during login in SNS, the response is 56% user agrees to it, 29% are strongly agreed to the idea, 4% are neutral of this implementation, 10.33% were disagree.

Table 4.1: Preference of Respondents towards Graphical Authentication

<table>
<thead>
<tr>
<th>Option</th>
<th>User input</th>
<th>Percent (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly Agree</td>
<td>87</td>
<td>29</td>
</tr>
<tr>
<td>Agree</td>
<td>168</td>
<td>56</td>
</tr>
<tr>
<td>Disagree</td>
<td>31</td>
<td>10.33</td>
</tr>
<tr>
<td>Strongly Disagree</td>
<td>2</td>
<td>0.67</td>
</tr>
<tr>
<td>Disagree</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Neutral</td>
<td>12</td>
<td>4</td>
</tr>
<tr>
<td>Total</td>
<td>300</td>
<td>100</td>
</tr>
</tbody>
</table>

4.2 Introduction to Biometrics

These days password leakage is becoming a major problem for the users of social networking sites. If a person knows the password of any other person, he will try to login through his account and collect certain private or secret data thus violating the terms and conditions of the sites. Tampering with user’s confidential data may results
as a major problem for the victim users. To overcome this problem biometric technology can be implemented with the social networking sites for user login rather than passwords. Biometrics provides user with more secure and trustworthy platform for communication. It offers certain schemes for the authentication of unique users to login into his account. Thus, there is no alternative of revealing others personal and private information.

In terms of security, biometrics is a computerized method of identifying an individual based on physiological or behavioral characteristics.

Some of the biometric identification schemes are:

Face: The study of facial characteristics for the authentication of an individual.

Fingerprint: With the use of ridges and valleys on the surface tips of humans, exclusive fingerprints of every finger and thumb of an individual is analyzed.

Hand geometry: The study of width and length of the hand & the fingers.

Retina: Analysis of veins at the back of the eye.

Iris: Analysis of the colored ring at the edge of the eye.

Signature: The analysis of the handwriting style used by an individual to signs his name.

Voice: Identification of the person who is speaking by characteristics of his tone, pitch and frequency.
4.2.1 Analysis of Biometric Techniques

Certain factors of biometric technology are accountable when implemented for authentication of users in social networking sites. Some of them are:

1. Recognition through biometric techniques provides accurate and secured access to information through fingerprints, retinal and iris scans.
2. Biometric identification can be done rapidly with minimum training.
3. Individual’s identity can be confirmed without producing the documents that may either be lost or stolen.
4. Minimizes the fraud rate.
5. No need to remember passwords that may be shared or observed.

4.2.2 Implementation of Biometrics

SSN in US and AADHAR in India

Unique Identification System is defined where every citizen of a country uses a unique 12 - 16 digit alphanumeric number to provide security. Using this scheme individuals do not need to submit multiple documents every time, in order to avail a new service. It contain the details of user like the name, sex, date of birth, address, marital status, photo, identification mark, finger prints and face biometrics. For the process of authentication the UID is stored in a primary and secondary database that is connected to the server. This scheme undergoes two defined processes:

1. Recording Process: The UIDAI builds a centralized database consisting of UID and other information about the person. The card assigns a unique 16 digit number that is randomly generated for every citizen by the main computer.

2. Authentication Process: The identified citizen has to fill the data along with identification proof to check if the user is genuine or not. The processed information is sent to the centralized server. The server receives the input and compares it with the already stored records in the database. The person is designated to be a genuine citizen if a relevant match from the database is found.

Figure 4.6: AADHAR or SSN Card for Biometric Inputs
4.2.3 Flow Chart of Biometric Authentication

Figure 4.7, represents the different conditions about the flow of verification in biometric authentication at login session.

![Flowchart for Unique Identification Management System](image)

Figure 4.7: Flowchart for Unique Identification Management System
In a social networking site the user need to enter the identification number (SSN or AADHAR) and a registered email id along with other necessary details while making an account. This information serves the purpose of verification and is not displayed in the user profile pages. The credentials should match with the information provided by the user while creating account in social networking sites. In case of any discrepancy no account should be allotted to the user.

Figure 4.8: Dataflow of UIDM
4.2.4 Methodology

In our existing framework of social networking website, 300 users were analyzed for the security concerns related to their authentication. Initially an online survey of 1205 user’s questionnaire was created to confine the awareness of trust, privacy concern, information sharing and usage of the site. Analyzed through the research survey, indicated that users express concerns about privacy of their personal information, but are less attentive about safeguarding it. We found that users want to implement biometric technique in social networking sites and they find the technique is easy to learn. It provides a more secure, proper and reliable communicating platform in social networking sites as compared to earlier hence, satisfies the working capabilities of the technology.

Figure 4.9, presents a column chart showing user responses towards implementation of biometric technique in SNS out of 1205 respondents, where 726 respondents are comfortable with and 312 respondents are not aware of biometric technique whereas 113 and 49 are either not able to decide or are not satisfied with the issue.

Figure 4.9: Bar Chart Showing User Satisfaction Level towards Biometric
4.3 Introduction to Digital Watermarking

Digital Watermarking is a relatively new field in social networking sites. Digital information can be embedded in pictures, photos and videos that the users of social networking sites wish to share within his community. The watermarking information can be texts, logos, handwritten signatures or numbers.

In order to deal with the problem of reliability of data and mistreat of photographs, security techniques are used to verify the information integrity and the authenticity of data.

The two main tools designed for Multimedia authentication are digital signature or watermarking.

Digital signature is an encrypted form of the actual data. It is always required to prove integrity and originality to the data which is compared with original data that is stored in a separate file.

Watermarking techniques refers multimedia data as a tool for communication channel. The embed watermark contains either a specific producer ID or some content-related codes that are usually used for authentication. Therefore, there is a need for implementing robust watermarks for social networking sites.

4.3.1 Analysis of Digital Watermarking

Digital watermarking embeds identifying information in an image. The information will be in the form of text, number or any predefined image that is visible to the user along with the actual image and that cannot be simply removed. Watermarks provides authentication in terms of a secondary image which is superimposed on the primary image, and protects the original image. This overlay may be visible or invisible. It has a device control code that prevents unlawful usage. An application of watermarking is copyright control which prevents illegal copying of the image.
Application areas of watermarking:-

1. Copyright protection - to prevent the misuse by unwanted users from copying or claiming the ownership of the digital media.
2. Authentication - to prevent from altering and tampering detection and monitoring
3. Owner identification – to restrict from copying.
4. Broadcast monitoring - to track the broadcast of over a communication channel.
5. Medical Applications - used in X-ray film for individual patient’s reference by marking with a unique ID.
6. Fingerprinting - to track information about distributed copies of the media.
7. Image authentication - to check the authenticity of the image.

The 5 distinct prerequisites of a watermark are:-

1. Imperceptibility: The watermarked work must not affect the view of original image that is it must be embedded within the image and should not be noticeable.
2. Robustness: The watermarked work may undergo several processing inflicts and it should be able to process.
4. Efficiency: The designed algorithm must be efficient that is insertion can be done quickly.
5. Capacity: It is the scope of watermark that an image can hold.
The general form of all designed and implemented algorithms involves the watermark and the original image. The basic constraint in all watermarking techniques is the Embedding Procedure that provides the watermarking in the image.

![Watermarking algorithm general form](image)

Figure 4.10: Watermarking algorithm general form (Lin and Delp, 1999)

4.3.2 Implementation of Digital Watermarking

In our designed framework we have implemented visible watermarking. It is a visible transparent text that is overlaid on the primary image like photos that doesn't totally obscure the primary image. Visible watermarking is adding an image as a watermark to another image. It is important to overlay the watermark so that it will be difficult to remove.

Visible Watermarking Algorithm

The steps for watermark insertion are discussed below:

1. Define an image manipulation class.
2. Create an instance of database.
3. Upload the image.
4. Place it into your folder.
5. Create a function to resize the image files of jpg, gif or png format.
6. Copy the image.
7. Design a function for cropping the image files.
8. Design a function for converting .gif or .png to .jpg format upon uploading.
9. Create a function for applying a .png watermark file to a file into .jpg.

Figure 4.11: Image with Watermarked Text Feature in Social Networking Sites