Implementation of 2-Way Graphical Password Verification by Using Hash Algorithm and Morphological Method

Khushboo Shrivastava[1], Harish Sahu[2]
[1]*Student, Department of Computer Science & Engineering, CIET, Raipur*
[2]*Assistant Professor, Department of Computer Science & Engineering, CIET, Raipur*

ABSTRACT –Identification play a fundamental component in most computer preservation contexts. There are various kind of user authentication methods, alphanumerical and identification are most commonly used user authentication the human brain is preferable in recollecting a figure then textual characters. The graphical password as superior authentication system user click on image to authenticate itself graphical password method have been proposed as feasible alternatives to text based scheme ,motivated partially by the fact that humans can remember images better than text .many investigation have been carried out in several places to recognize a useful graphical password authentication system using this potential. This paper aims at the constructing the simple graphical password verification method using image fusion algorithm. The proposed work includes three phases: 1. Sing in, 2. Sing up and 3. Verification.

Keywords: Preservation, recollecting, feasible, investigation.

I. INTRODUCTION

The importance of preservation is increasing day by day in a complicated society also as generation changes, preservation techniques are also changing. password are often used to secure computers and information. There are three main Areas where human computer interaction is important: verification ,security operations and developing secure system .here We focus on the preservation problem, many people in this current society who demand password often use a single password in many places.

In this case, however, if you lose your password, you can lose a lot of information graphical passwords, seek to have password that are both memorable and Secure graphical password use picture instead of text .graphical password are based on the fact that images are easier to remember than characters instead of numbers and letters ,patterns or pictures are used as passwords, which are easy to remember then text based passwords.

An important aim for the security system is to select passwords. Users frequently generate memorable passwords that are easy for attackers to guess but a strong system allocated password is very hard for users to remember. So researchers gone for an alternative method that is a graphical images are used as passwords graphical password generally used by the pictures representation as a password. The human brain is superior in reconnecting a pictures then textual characters.

The main interest for graphical password is that people are better at remembering images then alphanumeric. for example we can recognize the people we know from thousands of faces. This fact was used to implement an authentication system. This is the basis for the graphical passwords. a survey of numerous graphical password schemes have been developed which classifies the password systems as recognition-based systems, pure recall based systems and cued recall based systems.

In recognition based system :- user would choose images, icons from collection of pictures. in preservation process, the user need to recognize their registration choice among a set of candidates the research shows that 90% of users can remember their password after one or two month.

A. Graphical Password Authentication Methods

1. Token based authentication method.
2. Biometric based authentication method
3. Knowledge based authentication method

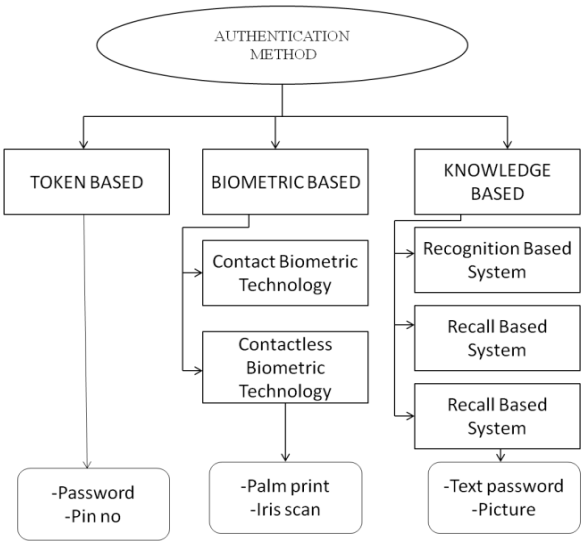


Figure1: Types of Authentication

1)Token based authentication: Token based techniques, like key cards, bank cards and smart cards are mostly used. Token based authentication systems also use knowledge based techniques to upgrade security, for example: ATM cards are generally used together with a PIN number.

2) Biometric based authentication: Biometric based authentication techniques, such as a fingerprints, iris scan, or facial recognition, are not yet broadly accepted. the main drawback of this scheme is that such systems can be costly, and the identification system can be slow and often unreliable. However, this type of technique provide the uppermost level of security.

3) Knowledge Based Authentication: knowledge based authentication method are the further most broadly used authentication techniques and include both text-based and picture-based password the picture based techniques can be further divided into two system:-recognition based authentication system and recall based the graphical authentication system knowledge based authentication method shared secret key which is used in banks, financial institutions, internet service provider and email services provider like Gmail, Yahoo mail etc.

3.1) *Recognition based technique:* Dhamija and Perring advised a graphical authentication technique established on the Hash visualization scheme in their method the user is asked to select a certain number of pictures from a set of random images generated by a program later the user will be required to identify the preselected images in order to be authenticated. A weakness of this system is that the server needs to store the seeds of the portfolio images of each user in plain tab text.

3.2) *Recall based techniques:* In the recall based techniques user need to recall or remember the particular images or drawing which he or she has already generated in the phase of registration. There are lot of techniques provided for recall based scheme. Here we have selected a scheme proposed by Jemyn called Draw-A- Secret (DAS) for our analysis. in this scheme user need to design a picture or signature on a 2D grid. The coordinate occupied by the picture drawn by user are stored in the order of drawing. In the authentication process user need to redraw the same picture. If the picture touches the same grid, then the user is authenticate

II METHODOLOGY

This procedure is the description in the research to accomplish the objective by describing the development of the project .suitable flow of design can make the system more systematic and effective and performing theoretical analysis of the method applied to a field of studies

In pure recall- based:- graphical password scheme, users need to reproduced their password without being given any hint or cues, jeremyn et al. described a graphical password schemes draw a secret (DAS) where the user has to draw a something shape or a picture on a grid. Users need to draw approximately the same shape in order to authenticate themselves, the graphical password scheme based on Pure recall are quick and convenient to use but they have the same disadvantage as alphanumeric password.

Cued recall-based graphical password scheme:- in cued recall, the user have to recall a password, but the system offers a framework of hint context and cues, that help the user reproduce their password or help them make the reproduction more accurate.

A framework describes a process system on for implementing the project figure shows the framework of graphical password authentication by using past point method.

In registration phase- user will enter their name, email, contact number after that user is required to select password either by image by color or by map after that

object detection in 2nd way authentication user will legally registered after they had fill all of the requirements needed in the registration phase. In user phase- firstly user is required to enter their username that has been registered before. Then user will login his password either by color, by image or by map then come to the 2nd way authentication process here user will detect the object which was done in the registration phase, during registration phase lastly user is authenticated and they can log into the system.

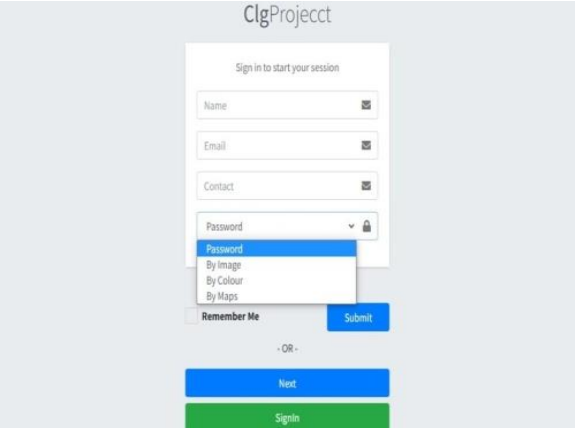


Fig: User Selecting Their Password

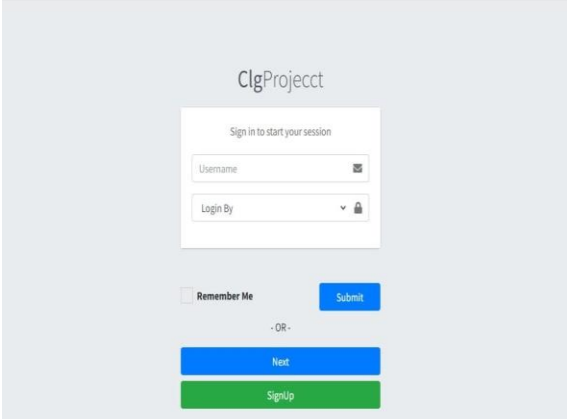


Fig: User Login their Password

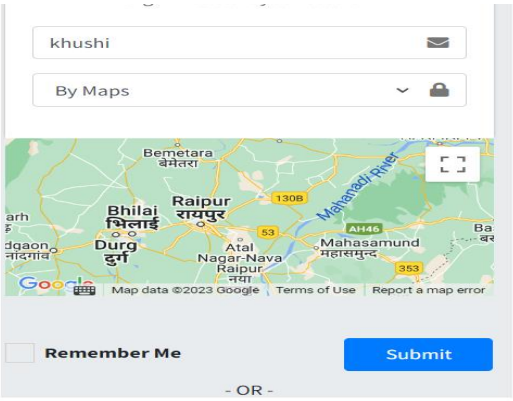


Fig: User Login Their Password By Using Map

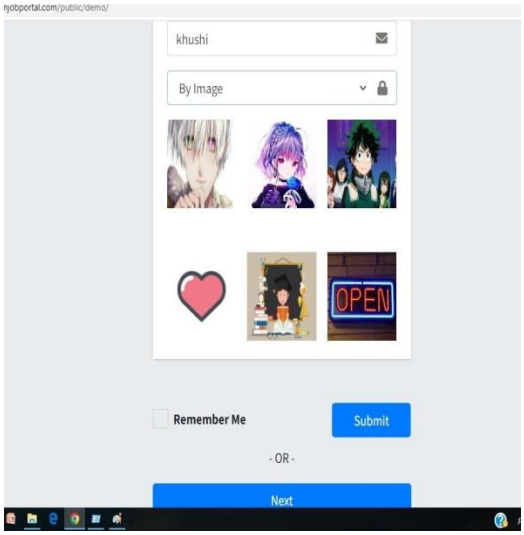


Fig: User Login Their Password By Using Image

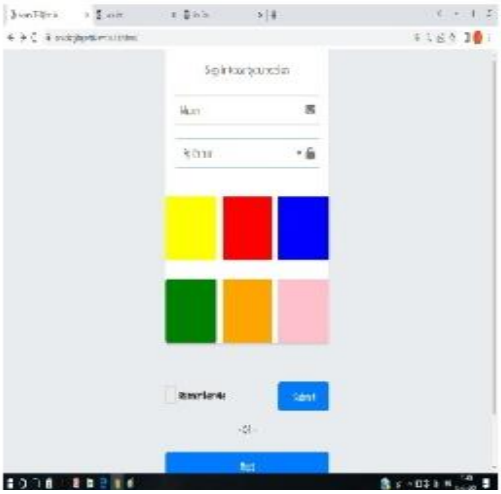


Fig: User Login Their Password By Using Color

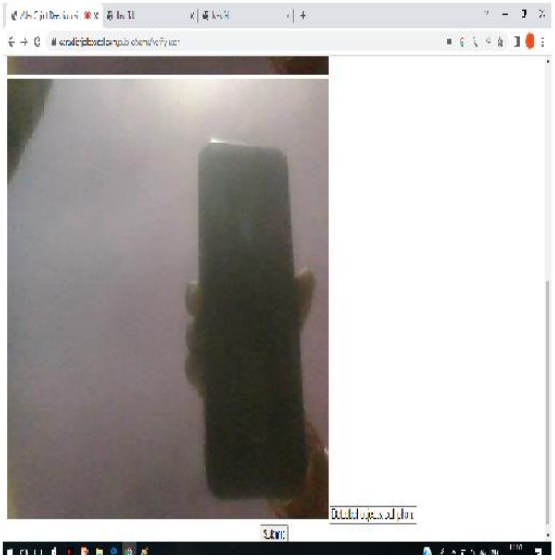


Fig: User Login Their Password by Using Object Detection

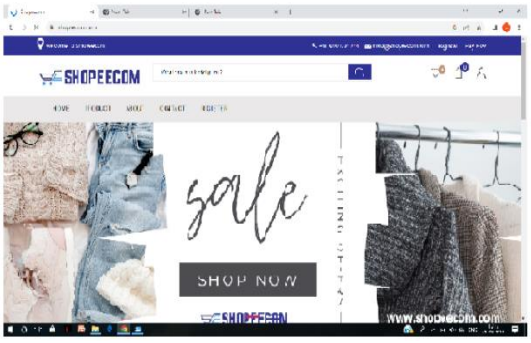
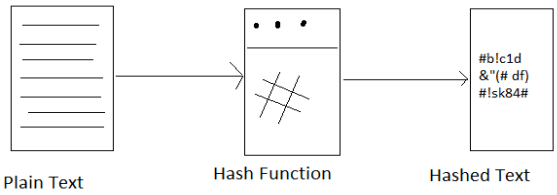


Fig: User Login Their Page Successfully

Hashing : Hashing is a technique that is used to uniquely identify a specific object from a group of similar objects. Hashing store and retrieve a data in 0(1) time. Hashing also known as a mapping technique, large value mapped into small value by using the concept of mapping. Hashing is a technique to integrity the data. Search key, insertion key, deletion key, Hash Table, Hash Function.



Cryptographic Hash objective: A Cryptographic hash objective is a type of hash function which is considered approximately impossible to create again the input data from its hash value alone. The input data is often called the message and the hash value is often called the message digest or simply the digest.
The ideal cryptographic hash objective has four main properties:
1) Easy to compute the hash value for any given massage.
2) Infeasible to modify a massage without changing the hash.
3) Infeasible to generate a message from its hash.
4) Infeasible to find two different message with the same hash.

Hashing Function: Hash Function are irreversible, one-way function which protect the data, at the cost of not being able to recover the original message. Hashing is a way to transform a given string into a fixed length string .A good hashing algorithm will produce unique output for each input given. The only way to crack a hash is by trying every input possible, until you get the exact same hash. A hash can be used for hashing data (message/password/signature/certificate/fingerprint)

Morphological Operation:
Morphological is a broad set of image processing operations that process binary images based on structuring element or kernel which decides the nature of operation. In morphological operation, each pixel in the image is adjusted based on the value of other pixels in its neighborhood.
Morphological image processing (or morphology) describes a range of image processing techniques that deal with the shape (or morphological) of features in an image…Morphological operation is typically applied to remove imperfections introduced during segmentation, and so typically operate on bi- level image. These operations are performed using the concepts of reflection and translation.

Types of morphological operations:
1. Dilation: just opposite of erosion here, a pixel element is 255 if at least one pixel under the kernel is 255.
2. Erosion: A pixel in the original image (either 255 or 0) will be considered 255 only if all the pixels under the kernel is 255, otherwise it is eroded(made to zero).
3. Opening: Erosion followed by dilation, many times used in noise removal.
4. Closing: Reverse of opening(Dilation followed by erosion), filling patches in the foreground object mask.
5. Gradient: Dilated image – Eroded image, to find outlines of objects.
6. Top Hat: Difference between input image and its opening, Highlights minor details in image(only)
7. Black Hat: Closing- input image, To find bright objects on dark background

Structuring element: It is a small set to probe the image under study. For each structuring element, we should define the origin. The shape and size must be adapted to geometric properties for the objects. We check for three conditions while applying the SE: Fit, Hit and Miss.

Dilation and Erosion
Dilation enlarges foreground and shrinks background.
Erosion shrinks foreground and enlarges background.

Dilation: it is the set of all points in the image where the structuring element "touches or hits" the foreground. Consider each pixel in the input image. If the structuring element matches completely with the pixel value or even of at least one match is found. Write a "1" at the origin of the structuring element. Dilation is denoted by A(+)B.

Application of dilation: Repair breaks (bridging the gaps), Repair intrusions and enlarge the object.

Erosion: It is the set of all points in the image where the structuring element" fits into". Consider each foreground pixel in the input image. If the structuring element matches completely with the pixel value, write a "I" at the origin of the structuring element. Erosion is denoted by A(-)B.

Application of erosion: Strip away extrusions, shrink the objects, split apart joined objects.

III COMPARATIVE ANALYSIS

The identification is performed mainly to test the preservation insurance measures. Hence through deep studies of the previous work loopholes have been determined and the proposed approach has reached to present our 3-layers preservation architecture. Table 1 shows our list of images with user choosing speed for proper CAPTCHA images. The proposed strategy implements a comprehensive encode technique of AES cryptography beside Hashing, which gives a more efficient edge to the verification process. Table 1 shows how all techniques are evaluated for protection, integration and complexity, as marked between low level valued 0, moderate as 1, standard as 2 and our high level as 3.

Technique	Notation	Attack Prevention	Delay	Integration Complexity
Secure Scheme For CAPTCHA-Based Cloud Authentication.	2010	Dictionary attack & Phishing attack	Delay	1
Password- Based Identity Authentication System	2014	Dictionary Attack	Moderate	2
Authentication By Encrypted Negative Password	2016	Rainbow Table & Lookup-Table Attack	Moderate	1
Improved Security Captcha Hash Encry pted	2021	Dictionary-Attack DOS	Low	3
Graphical Password Verification Method	2022	Password Attack & Dictionary attack	Very Low	3

Table 1: Time Consumption And Complexity Table vs Security

Table 2 summaries the contributions, comparison of the advantages and disadvantages of the techniques, including our work.

Based on Table 3, Vaithyasubramanian (2016) research is only using audio-based CAPTCHA, which is beneficial to users who are visually affected, but may be not very convenient to all. As an overview,

Contribution	Technique	Advantage	Disadvantage
Audio Captcha Words	2016	optical Impair Users	Audio-Noise Vocabulary
Chinese CNN	2016	Recognition precision	Low Security
Vertical Projection	2017	Recognition perfection	Low Reliability
Zhang's CATCHA via intelligent communication with RIA	2019	Two line of defense	Time-delay &complexity
CAPTCHA based encrypted hash	2021	Security & Practical usability	Improve Hash Function Efficiency
Graphical Password Verification Method	2022	Strong, Security & Practical Usability	Improve Hash Function performance and morphological method

Table 2: Systems overall comparisons based on contribution, advantages and disadvantages

Table 3 below summarizes the observation of promising techniques on basis of the essential verification layers' availability and practically various characteristics. We involve proper labeling for CAPTCHA images to be clear enough for the user to choose figures from the grid benefitting from all other schemes.

Technique	Notation	Usability	Encryption	Hashing	CAPTCHA
A non-OCR approach	Kaur 2016	No	Yes	Yes	No
Modification Based CAPTCHA	Althumaly & E1-Alfy,2017	No	Yes	Yes	No
Improved-Security Captcha Hash Encrypted	Nafisah Kheshaifaty 2021	Yes	Yes	Yes	Yes
Graphical Password Verification Method	Proposed	Yes	Yes	Yes	No

Table 3: Authentication layer's Availability and Practicality evaluation

IV RELATED WORK

Since it has been verified that images are easier to recall than text phase, some people have been recommended graphical password as an alternate Diriket al classify the graphical password into three systems such as pure recall based system, recognition based systems and cued recall based systems people who use recall based password.

Haichang et al. selected pass image one by one with the same continuance in drawing the curve beginning from the given image (red rectangle) and finished the image marked with a green rectangle

System have to recognize their password to access to system further more one of the most unforgettable studies of the recall Based techniques was offered by Jermyn et al.

Hai Tao. authentication using grid intersection point instead of grid cells. In addition, this scheme gave users a opportunity to select longer password and use color both resulting in Greater identification complexity then in DAS

The system of Govindarajul et. al. used Doodles as recall based systems requires expensive item of equipment such as Touchpad and digitizing tablet and are connected to a computer and user also need time to remember how to use the system recognition based graphical password system lie in a multiplicity of image used and user either chooses benefits provided by the system or provided their own images WhileThorpe.et.al selected location "×" Marker near his or her previously selected location, they used Google maps and large password space.

V SECURITY ANALYSIS

As the terminal variation every time, the session password changes. This methodology is resistant to shoulder surfing. Due to dynamic identification, dictionary attack is not applicable. Hidden camera attacks are not applicable to PDAs because it is difficult to capture the interface in the PDAs.

Brute Force Attack:-These methodologies are particularly resistant to brute force due to use of the session identification. The use of these will take out the authentic brute force attack out of the capabilities.

Dictionary attack:-These are attacks directed towards textual identification. Here in this attack, hacker uses the set of dictionary words and authenticate by trying one word after one. The dictionary attacks fails towards our authentication systems because session identification are used for every login.

Guessing:-Guessing can't be a threat to the pair based because it is hard to guess secret pass and it is 36*4.The hybrid textual method is dependent on user selection of the colors and the rating. If the general order is followed for the colors by the user, then there is a capability of breaking the system.

Complexity: Pair-Based Authentication scheme is to be carried over the secret pass. For a secret pass of length 8, the complexity is 368. In the case of the Hybrid Textual verification method the complexity depends on colors, image, map, object and ratings

VI RESULTS

All the specification in this research paper shows that implementing the technique Graphical Password verification method for folder preservation provides a safe mechanism to the folder. It does not allow the unauthorized user to access the folder and also it protect from the malwares, viruses for corrupting the files current in the folder. Normally we can implement this technique in case of defense, banking sector, drive cryptography, captcha, security section, and online password.

VII CONCLUSION

For large system main problem is private authentication graphical password authentication system using fusion algorithm. Graphical password verification technique is one of major authentication method actively researched around world and getting big attentions from several business organizations these days. Graphical passwords are not easily stolen than text-based passwords and are easy for users to remember.

Hence we successfully concluded and it is easy to recall and it is tough to predict. Graphical password methods offer a way of creating more human-friendly passwords. Pictures are stress-free to recall than text strings. The new scheme provides solves the several problems of existing system. It can also be useful for user in security point of view.

REFERENCE

[1] D. R. Pilar, A. Jaeger, C. F. A. Gomes, and L. M. Stein, "Passwords usage and human memory limitations: a survey across age and educational background,"PLoS,One,vol.7,no. 12,2012 Authorized
[2]Openwall,Wordlists,Collection,"http://www.openwall.com/wordlists/," accessed 2 January 2019.
[3]H.Yuan,Y.Han,andJ.Hu,"Password memorability and security : empirical results," Int. Comput. Sci. Softw. Eng. Conf. Vol. 4, pp. 25– 31, 2008.
[4]John,the,Ripper,Password,Cracker,"http://www.openwall.com/john/," accessed 2 January 2019.
[5] G. C. Yang, "PassPositions: A secure and user-friendly graphical password scheme," in Proc. 4th International Conference on Computer Applications and Information Processing Technology,Bali, 2017.
[6] Sharayu S.Ganorkar1 ,Prof. H. V. Vyawahare 2 "ReviewPaperOn Graphical Password Authentication Techniques " Volume 5, Issue 03, March -2018
[7] A. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security," IEEE Trans. Information Forensics and Security (TIFS), vol. 1, no. 2, pp. 125-143, June 2006.
[8] Authentication Using Graphical Passwords: Basic ResultsSusan Wiedenbeck Jim Waters ,College of IST,Drexel,University,Philadelphia,PA,19104USA
surfingresistant graphical password scheme," in Proceedings of the working conference on Advanced visual interfaces, pp. 177–184, ACM,2006.
[9] A. F. Syukri, E. Okamoto, and M. Mambo, "A user identification system using signature written with mouse," in Australasian Conference on Information Security and Privacy, pp. 403–414, Springer, 1998.
[10] A Survey on Recognition-Based Graphical User Authentication Algorithms FarnazTowhidi Centre for Advanced-Software-Engineering-University
Technology Malaysia Kuala Lumpur, Malaysia
[11] S. Agrawal, A. Z. Ansari, and M. S. Umar, "Multimedia graphical grid based text password authentication: For advanced users," in Wireless and Optical Communications Networks (WOCN), 2016 Thirteenth International Conference on, pp. 1–5, IEEE, 2016.
[12] Security Analysis of Graphical Passwords over the Alphanumeric Password by G.Agarwal ,1Deptt.of Computer Science, IIET, Bareilly, India 2,3 Dept. of Information Technology, IIET, Bareilly, India 27-11-201
[13] Real User Corporation, Passfaces TM http://www.realuser.com, Accessed on January 2007.
[14]. R. Dhamija, and A. Perrig, "Déjà vu: A User study Using Images for Authentication", in 9th Unisex Security Symposium, 2000.
[15].Scheier, Bruce, "Cryptanalysis of MD5 and SHA: Time for a New Standard", Computerworld, retrieved 15 October 2014.
[16] A. Almulhem,"A graphical password authentication system," in internet security (World CIS), 2011 World Congress on, pp. 223-225,IEEE,2011.
[17] X. Suo, Y. Zhu, and G. S. Owen, "Graphical password; A survey,"in computer security application conference,21st annual,pp,10-pp,IEEE,2005.
[18] O.Ayannuga,Olanrewaju and F. Olusegun, "Graphic-text Authentication of a window-based application," International journal of computer application,vol.21,no.6,pp.36-42,2011.
[19].M.G. Tuscano and A. Tulasyan,"Graphical Password Authentication using pass faces," International journal of engineering research and application,vol.5.no.3,pp.60-64,2015.
[20] H. yuan, Y. Han, and j. Hu, "password memorability and security empirical results," Int. Comput Sci. Softw. Eng. Conf. Vol. 4,pp.25-3,2008.
[21] D.R. Pilar,A. Jaeger,C.F.A.Gomes, and L.M.Stein,"Passwords usage and Human memory limitations: a survey across age and educational background," PLoS One, vol 7,no. 12,2012.