International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Secure Graphical Passwords with Pass BYOP: Bring Your Own Picture

Rebeiro Caroline Leontia Carlton Christopher[1], Huda Noor Dean[2]

[1]PG Student, Department of Computer Science & Engineering, College of Engineering & Management, Punnapra, Kerala, India
[2]Assistant Professor, Department of Computer Science & Engineering, College of Engineering & Management, Punnapra, Kerala, India

Abstract: ***Secure access to information such as financial data, Personal media files are provided by authenticating to an identity. Dominant authentication methods are text passwords and personal identification numbers(PINS).However, most of the passwords are difficult to remember and thus individual users use non-secure methods such as reusing passwords and noting down their the passwords. Thus, in order to solve this problem, researchers have developed graphical passwords scheme that depend on the portions of the image as input. However, graphical password have problems such as it can be easily guessed as well as prone to shoulder surfing attack. Therefore, we have proposed a graphical password system based on a point-click, PassBYOP: Bring Your Own Picture, that prevents resistance to observation attack by combining users password to an image. SIFT (scale invariant feature transform) based on optical features are extracted from selections of the image (token) and then utilized as an eligible password. PassBYOP offers high reliability, security and usability as compared to the existing graphical password systems. The reliability in terms with image feature based passwords assures feasibility and also provides appropriate thresholds which contain a password items with minimum features. The usability factor measure error rate and time taken to complete the task. The security factor provides insight to resistance to various attacks such as malware. Hence, PassBYOP offers security by also maintaining the usability of this current graphical password method.***

Keywords: Authentication, Graphical Passwords, SIFT (scale invariant feature transform), Image.

1. Introduction

Among a majority of computer systems, passwords are the most prominently used authentication method. Generally, users often choose passwords which are easy to memorize and thus make them vulnerable to attack through the searching of the candidate password. The most dominant authentication method [1] is text password and personal identification number (PINs) which are used in various mobile devices, web and public terminals. Such passwords are difficult to remember and hard enough to guess [2]. There arises problem when user with 25 online accounts has to memorize six different passwords [3]. To deal with problem of memorization, users tend to note down password or might forget these passwords [4]. Thus, to solve such problems, researchers have introduced a scheme graphical password [5], [6]. It depends on the input which are portions selected from an image. There are problems such as intelligent guessing [7], [8] and shoulder surfing attack [9]. The users are vulnerable to various attacks based on the selection of images as input, the attacker might watch over from shoulders or set cameras to record password and users most probably choose hotspots in an image [10], [11]. Most of the image information is stored on authentication server and attackers tend to information by the identity of the user [12]. To address these problems, a new graphical password scheme called PassBYOP-Bring Your Own Picture prevents to attack by combination of user's password. PassBYOP is a multifactor authentication system. PassBYOP is different from many prior approaches. First, it is flexible, thus a complex image can be used as an PassBYOP token. Second, it has two factors for authentication password as well as token (input image) which are both tightly coupled. Finally, the image used as token has high entropy as compared to a single factor authentication scheme [13]. This paper focuses on a graphical authentication mechanism PassBYOP for providing secured authentication.

2. Related Work

In this section, existing graphical passwords are discussed. Graphical passwords have been introduced to problems associated with a text password schemes, it is known that pictures are easy to remember as compared to a text which can be referred to as "Picture Superiority Effect" [14]. A literature survey of various papers shows different graphical schemes can be categorized into four groups as follows as a shown in Fig 1:

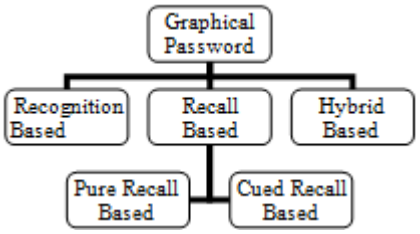

Figure 1: Taxonomy of graphical Authentication Technique

2.1 Recognition Based Technique

In this technique, users tend to choose a symbol or a symbol or icons from a set of images. During the authentication, users need to recognize the correct image or symbol chosen during the time of registration from a collection of images. Researchers have shown that users tend to remember even after 45 days [15]. Dhamija and Perrig [16] proposed a graphical authentication scheme which depends on the Hash Visualisation Technique [17]. The drawback of this system is server has to store seeds based on each image the user has selected into a plain text and also selecting a number of images can be time consuming and tedious process for the user. Akula and Devisetty's [18] Algorithm has similarities that of Dhamija and Perrig. The only difference is that, this method uses hash function SHA-I, to produce an output of 20

byte. The authors have a future enhancement to this method by using a persistent storage that can be deployed into web or cell phones. Weinshall and Kirkpatrick [19] sketched many schemes, as object recognition, picture recognition and pseudo word recognition. In the picture recognition scheme, a user has to identify a large number of images stored in a database. Sobardo and Birget [20] proposed an authentication scheme that deals the problems associated shoulder surfing attack. The drawback of this method the login process is really slow.

2.2 Pure Recall Based Technique

In this technique, users have to remember and recollect the password without any external help such as hints or reminder. The process is quite easy, but users find it difficult to remember the passwords. Jermyn [21] proposed a technique "Draw-A-Secret"(DAS) in which users draw their password into a 2D grid. During the authentication, the users have to redraw the passwords and also the drawing has to touch the same grid in the same consecutive sequence. Varehorst [22] proposed a scheme called "Passdoodle" in which user draw a freehand drawing a password. The doodle should have a minimum of two pen stroke.

2.3 Cued Recall Based Technique

In this technique, users are allowed to use reminders or hint, to reproduce the password. Blonder proposed a scheme the users has to select the password in an sequence based on the pre-selected area. However, it has some disadvantage-defined areas can be easily recognized and also the predefined areas are quite small. Weidenbeck [23] proposed a scheme called Passpoints which is an extension of blonder's idea. Thus, users can click any point of an image, it prevents the shortcomings of predefined area. Chiasson [24] proposed a scheme called "Cued Click Points"(CCP) in which users select an image based on the current selection, the next image will be displayed. Thus, if an user select an incorrect point, the next image will be incorrect one. Chiasson proposed a scheme called "Persuasive Cued Click Point" which users have to select points from an viewport and rearrange the viewport using an "shuffle" button. Thus, PCCP avoids hotspot issues.

2.4 Hybrid Based Technique

In this Technique, there is combination of two or more scheme. Jiminy [15] proposed a scheme in which users have to select an image then choose a template, then click on a location inside an image and choose position of the chosen template and store the password. During the login, users have to select the right template, place them in correct location and enter the corresponding characters. Gao [25] proposed a scheme called "Passhands" which is a combination of both recognition based and palm based biometric scheme. During the login, users have to choose palm images placed in a 3x3 grid where one image is password and other decoy images.

A more detailed study on the various graphical passwords has been done [26].

3. Proposed Scheme

The aim is to develop a graphical password authentication system based on the image features extracted through an SIFT image processing. Features are detected by a filtering approach to recognize stable points in a scale space. Image key points are formed based on the geometric deformation that represents blurred image gradients which depends on multiple scales and orientation plane

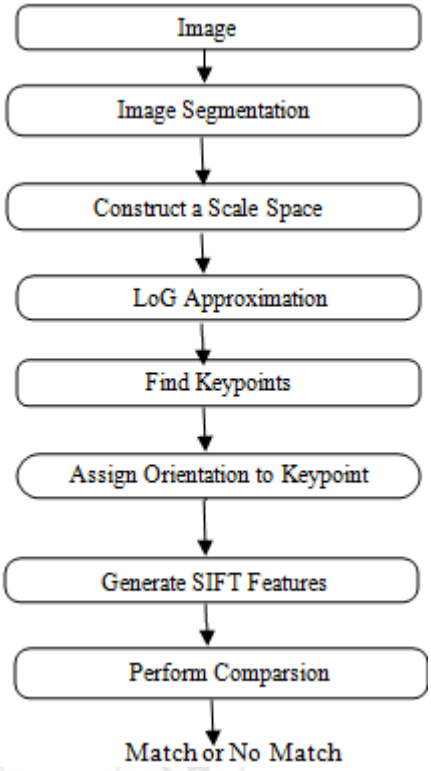

Figure 2: Block Diagram of Proposed System showing Flowchart of methodology that will be followed.

The PassBYOP implementation basically based on the SIFT image feature. Thus, it can be implemented by an SIFT algorithm. These are distinctive invariant feature which can perform reliable matching from different views. Features are unchanged to scale and rotation of an image and provides a robust matching to various viewpoints. The features are highly distinctive which means a single feature can match with appropriate feature from among a large database of features which are obtained from many images. The recognition follows by matching individual feature that is stored in the database using a nearest neighbour algorithm. The application of image matching forms a foundation to many areas such as computer vision i.e. solving 3D for multiple images, motion tracking and object recognition. Thus, large number of features can be extracted from multiple images using efficient algorithms. The algorithm goes through various forms of computation to generate image features.

3.1 Constructing a Scale Space

SIFT constructs a scale space, by taking the original image and generating consecutive set of blurred images. Then, resize the original image to half size of the original image and keep repeating the steps. Images having same size form

an octave. Thus, SIFT generally requires 4 Octaves and 5 blur levels for the algorithm as shown in Fig 3. Thus, to generate better key points, the original image is doubled and blurred. Blurring is defines as the convolution of the operator and image. Table 1 indicates the amount of blurring in terms of σ's.

$$L(x,y,\sigma) = G(x,y,\sigma) * I(x,y,\sigma) \quad \text{.....Eq(1)}$$

Table 1: Amount of blur based on octaves and scales

Octave	Scale				
	0.707107	1.000000	1.4142	2.000	2.8284
	1.414214	2.000000	2.8284	4.000	5.6568
	2.828427	4.000000	5.6568	8.000	11.313
	5.656854	8.000000	11.313	16.00	22.627

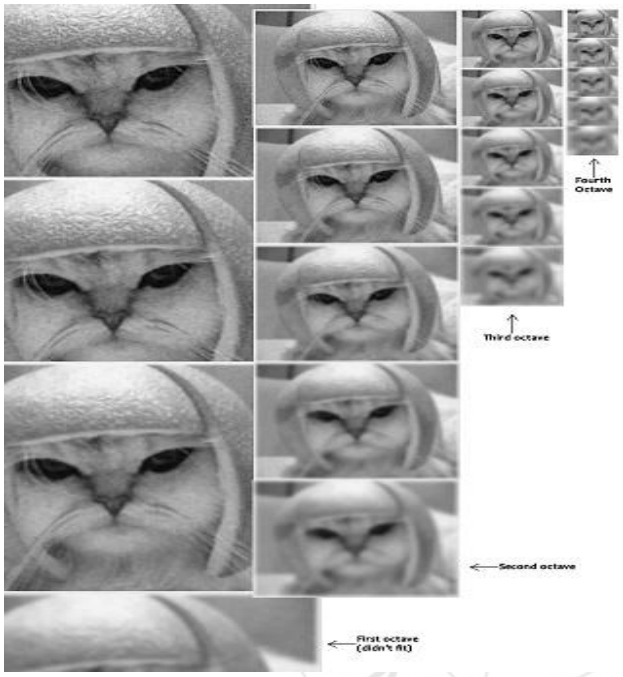

Figure 3: Scale space for 4 octaves and 5 blur levels

3.2 Laplacian of Gaussian (LoG) Approximation

The Two consecutive images in an octave are selected and one image is subtracted from the other image. Then the next pair of image is selected and the process is repeated. This is applicable for all octaves. Thus, the resulting images are Laplacian of Gaussian as shown in Fig 4.

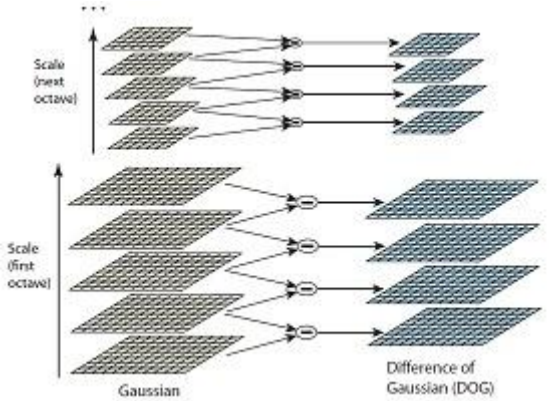

Figure 4: Laplacian of Gaussian (LoG)

3.3 Finding Keypoint

This is a two part process:

3.3.1 Locate maxima/minima of difference of gaussian images

To find the location of maxima and minima, iteration is performed on each pixel and check with all its neighbours check is performed on the current image, and the images below and above the current image. 'X' marks the current pixel. The green circle indicates the neighbour i.e. 26 checks. Thus, X becomes the keypoint if greatest or least of 26 neighbours as shown in Fig 5.

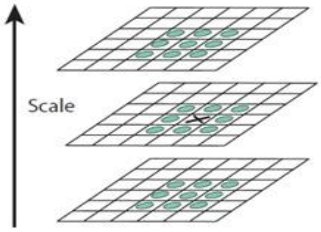

Figure 5: Maxima and Minima of Difference of Gaussian Images

3.3.2 Find Subpixel Maxima/Minima

The available pixel data are used to generate subpixel value. This is achieved by Taylor expansion as shown in Eq(2) of the image of an keypoint.

$$D(x) = D + \partial D^{T} / \partial x(x) + \tfrac{1}{2} x^{T} \frac{\partial^{2} D}{\partial x^{2}} x \quad \text{.....Eq(2)}$$

3.4 Assigning Orientation To Keypoint

The orientation of a keypoint is achieved by using histogram and a region around it. If there is only one peak it is assigned as a keypoint. Otherwise, in multiple peaks above 80% mark are converted into a new keypoint as shown in Fig 5.

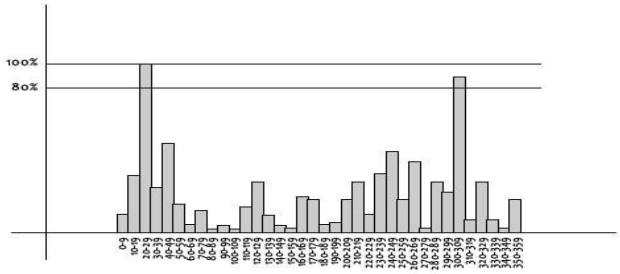

Figure 5: Assigning Orientation to Keypoint

3.5 Generating a SIFT Feature

Thus, to generate a SIFT feature, 16x16 window "in-between" pixels of a keypoint is split into a sixteen 4x4 window, histogram of 8 bins are generated. Thus, each bin has 0-44 degrees, 45-89 degree, etc... Thus, gradient orientations of 4x4 are put into bins. Thus, it is achieved for all 4x4 blocks. Finally 128 values are normalised.

3.6 Comparsion through Match Descriptors in a Feature Space

Shared Descriptor of a keypoint will be close enough to 128-dimension space. Thus, variance metric can be computed by the average distance which is between a shared descriptor and an individual patch in a descriptor of an image. The distance obtained is a Euclidean distance which can be computed in 128-dimensional space using Eq(3).

$$Dist(d1, d2) = \left\| d1i - d2i \right\| \quad \text{.....Eq(3)}$$

Where d1 and d2 represents 128 dimension descriptors used in SIFT.

$$\text{var}(d) = \sum_{i=1}^{m} Dist(d, f1) \Big/ m \quad \text{.....Eq(4)}$$

Where d represents the 128 dimension shared descriptors and 'f' represents the set of 'm' descriptors from 'm' patches.

Thus, in an original SIFT descriptor comparison approach. Each descriptor of every image is compared to another Euclidean distance. Thus, the variance of the shared descriptor is used to find the best match stored in the dictionary to decide whether the keypoint of the image finds a match or not. Thus, most successful technique to finding best match, using Euclidean distance of the closed shared descriptor is less than variance (threshold) of the descriptor as shown in Fig 6.

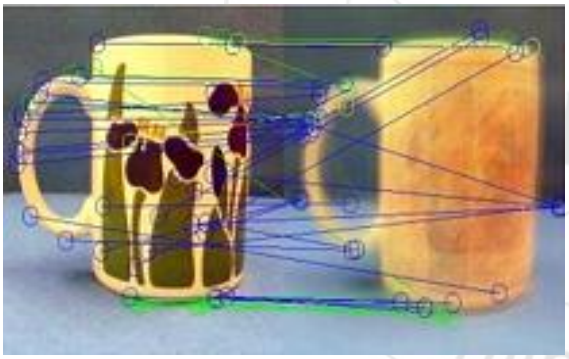

Figure 6: Matching based on variance threshold technique between a mug dictionary and a mug that has never seen earlier

4. Experimental Setup

The Proposed System uses MatlabR2011a as a framework to execute the new graphical password authentication system. The user interface for the system is provided GUI Matlab. WindowsXP requires a disk space of 1GB for Matlab and installation it requires 3-4GB. It requires RAM space of 1024MB. Matlab provides an image processing toolbox which consists of standardised algorithms and apps required for processing, virtualisation and analysis. Thus many operations related to image processing can be performed using this toolbox, such as image registration, geometric transformation, noise or blur reduction, image enhancement etc.

5. Implementation

The Implementation Module consists of:
1) User Registration
2) User Login

5.1 Registration Phase

During Registration Phase the user has to enter a valid username. The username is validated by checking if it exists in the database. If present, the user is advised to use a valid username otherwise user can continue with same username as shown in Fig 7.Once the username has been validated, the user is suggested to select any image from the database and also to choose points which has chosen to be set as password. The points selected are shown to the user in 4 segmented blocks as shown in Fig 8. The image portion goes through SIFT algorithm which extracts features of the portions and stores them in database.

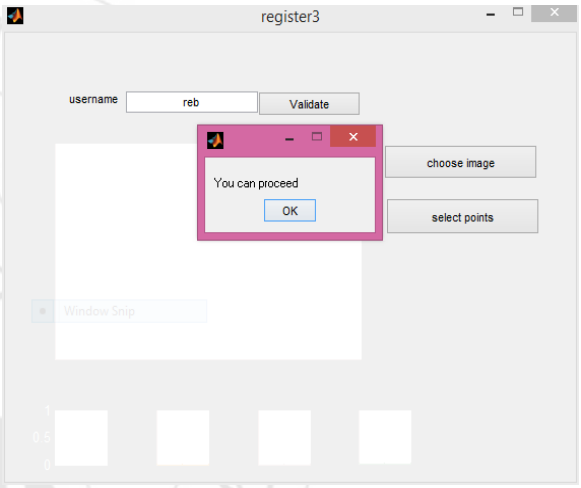

Figure 7: User Register Validation

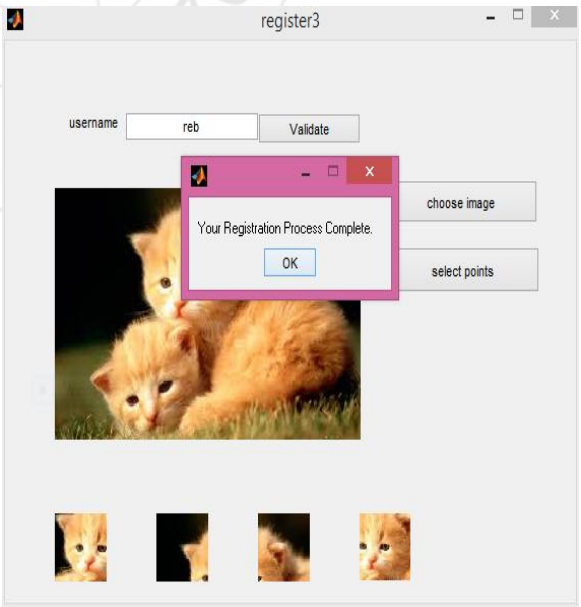

Figure 8: User Registration

5.2 Login Phase

During the Login Phase, the user has to choose the same image portions selected during registration phase, if the image portion matches with images in the database, then the user is authenticated. Match is based on the Euclidean distance of the closest neighbour. Thus, user is successfully logged in. In case of failing to select the same portions then the user is not authenticated.

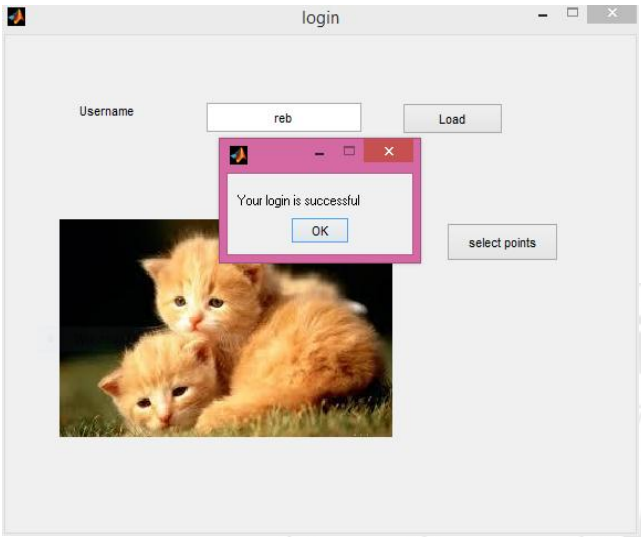

Figure 9: User Login

6. Result Analysis

The best candidate match for every keypoint is obtained by identifying the nearest neighbours. Thus, the nearest neighbour has minimum Euclidean distance. An Effective measure to identify a correct match is by comparing the distance with the second closed neighbour. Thus, for false matches within a similar distance there would be more false matches. Based on the correct match obtained a user is authenticated. The following graph Fig 10 shows the probability of the match is correct, if the ratio of distance of the match of closest neighbour is close to second closest neighbour.

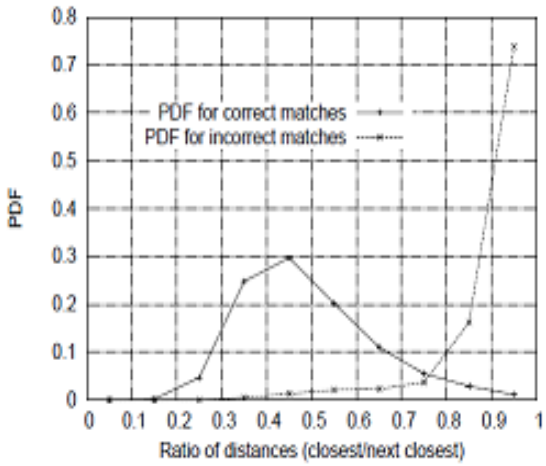

Figure 10: The probability of the match is correct based on the ratio of distance of the closest neighbour to the second closest neighbour.

7. Conclusion

We have proposed a Secure Graphical Passwords with PassBYOP: Bring Your Own Picture, a new graphical password authentication to solve the existing problems. The system provides security to attack such as brute force attack, dictionary attack. SIFT algorithm is competent to recognize the two objects which is similar, even if one image is concealed in other, irrespective of translation, scaling or rotation. Thus, SIFT demonstrates various features for authentication in this graphical password system. Also, it removes the pattern formation and hotspot problem.

References

[1] J. Bonneau, C. Herley, P. C. van Oorschot and F. Stajano, ”The Quest to replace passwords: A Framework for comparative evaluation of web authentication schemes, ”, in Proceedings IEEE Symp. Security Privacy, pp 553-567, 2012.
[2] H. kim and J. Hub, ”Pin Selection policies: Are they really effective?”, Comput. Security, vol 31, no. 4, pp 484-496, 2012.
[3] D. Florencio and C. Herley, ”A Large-scale study of web password habits”, in Proc 16th Int. Conf. World Wide Web, pp 657-667, 2007.
[4] A. Adams and M. Sasse, ”Users are not the enemy”, Commun. ACM, vol. 42, pp 40-46, 1999.
[5] R. Biddle, S. Chiasson and P. van Oorschot, ”Graphical Passwords: Learning from first twelve years, ”ACM Comput. Survey, vol 44, no 4, pp 19, 2012.
[6] G. E Blonder, ”Graphical Passwords”, U. S Patent 5 559961, 1996.
[7] S. Chiasson, R. Biddle and P. van Oorschot, ”A Second look at the usability of click-based graphical passwords, ”in Proc. 3rd Symp: Usable privacy security, pp 1-12, 2007
[8] Z. Zhao and G. J. Ahin, ”On the security of picture gesture authentication”, in Proc. 22nd USENIX Security Symp, pp 383-398, 2013.
[9] S. Weidenbeck, J. Waters, L. Sobardoand J. Birget, ”Design and evaluation of shoulder surfing attack resistant graphical password scheme, ”In Proceedings working Conf. Adv. Visual Interfaces, pp 177-184, 2006.
[10] S. Chiasson, E. Stobert, A. Forget, R. Biddle and P. C. van Oorschot, ”Persuasive Cued Click Points: Design, Implementation and evaluation of knowledge based authentication mechanism, ”IEEE Trans. Dependable Secure Comput, vol 9, no 2, pp 222-235, Mar 2012.
[11] J. Thorpe and P. van Oorschot, ”Human-seeded attacks and exploiting hotspots in graphical passwords”, In Proc. USENIX Security Symp, pp 8, 2007.
[12] F. Tari, A. Ozok and S. Holden, ”A Comparsion of Perceived and real shulder surfing risks between alphanumeric and graphical passwords”, In Proc 2nd Symp. Usable Privacy Security, pp 56-66, 2006.
[13] G. Lowe, ”Distinctive Image Features from Scale-invariant Keypoints”, Int. J. Comput Vision, vol-60, no 2, pp 91-110, 2004.

[14] S. Chiasson, A. Forget, R. Biddle and P. C. van Oorschot, "Influencing users towads better passwords: Persuasive Cued Click Points", In Human Computer Interaction (HCI), the british Computer society, Sept. 2008.
[15] K. Renaud and E. Smith. Jiminy, "Helping User to remember their passwords", Technicla report, School of Computing, Univ of South Africa, 2001.
[16] R. Dhamija and A. perrig, "Deja Vu: A User Study Using Images for Authentication", In Proceedings of the 9th USENIX Security Symposium, 2000.
[17] A. Perrig and D. Song, "Hash Visualisation: A New Technique to improve Real world Security", In Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-commerce, 1999.
[18] S. Akula and V. Devisetty, "Image Based Registeration and Authentication System", In Proceeding of Midwest Instruction and Computing Symposium, 2004.
[19] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, But Can't Recall, "In Proceedings of Conference on Human Factors in Computing Systems(CHI), pp 1399-1402, 2004.
[20] L. Sobardo and J. C. Birget, "Graphical Passwords", The Rutgers Scholar, An Electronic Bulletein for Undergraduate Research, vol 4, 2002.
[21] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter and A. D. Rubin, "The Design and Analysis of Graphical Passwords, "In Proceedings of the 8th USENIX Security Symposium, 1999.
[22] Varenhorst, "Passdoodles: A Lightweight authentication method", MIT Research Institute, July 2004.
[23] S. Weidenbeck, J. Waters, J. Birget, A. Brodskiy and N. Memom, "Passpoints: Design and Longitudinal evaluation of a graphical password system", International Journal Human-Computer Studies, 63(1-2): 102-127, 2005.
[24] S. Chiasson, P. C. van Oorschot and R. Biddle, "Graphical Password Authentication using Cued Click Points ", In European Symposium on Research in Computer Security(ESORICS), LNCS 4734, pp 359-374, Sep 2007.
[25] H. C Gao, X. Y. Liu, S. D Wang, R. Y Dai, "A New Graphical password scheme against spyware using captcha", In Proceeding of the symposium on usable privacy and security, July, 15-17, 2009.
[26] Rebeiro Caroline Leontia Carlton Christopher, Huda Noordean, "A Survey on Graphical Password Authentication Systems and their Security Issues", In International Journal Of Innovative Research in Science, Engineering and Technology, vol 6, Issue 6, June 2017