A Novel Graphical Interface for User Authentication on Mobile Phones and Handheld Devices

Mohammad Sarosh Umar
Department of Computer Engineering,
Aligarh Muslim University, Aligarh,
India
saroshumar@zhcet.ac.in

Mohammad Qasim Rafiq
Department of Computer Engineering,
Aligarh Muslim University, Aligarh,
India
mohdqasim@zhcet.ac.in

***Abstract* — Mobile phones are rapidly becoming an important tool to carry out financial transactions besides the normal communication. They are increasingly being used to make payments, access bank accounts and facilitate other commercial transactions. In view of their increased importance there is a compelling need to establish ways to authenticate people on the mobile phones. For the last several decades the popular method of authentication on computers has been text based. Both the username and password are alphanumeric. The textual password scheme though convenient to use suffers from various drawbacks. Alphanumeric passwords are most of the times easy to guess, vulnerable to brute force attacks, prone to shoulder-surfing, and are easily forgotten. With financial transactions at stake, the need of the hour is to have a secure, robust, and usable scheme for authentication. Graphical passwords are one of such schemes that offer a plethora of options and combinations. In this paper we are proposing a scheme which is simple, secure and robust. The proposed graphical password scheme will provide a large password space and at the same time will facilitate memorability. It is suitable to implement on all touch sensitive mobile phones as well as PDAs and Tablet PCs.**

Keywords- User authentication, graphical password, mobile phone security, usability, security

I. INTRODUCTION

Mobile phones have made their presence felt in different walks of human life. Today's technically advanced mobile phones are capable of not only receiving and making phone calls, but can very conveniently store data, take pictures and connect to the internet. They have also become a powerful tool to conduct commercial and financial transactions. They are increasingly being used to make payments, such as at retail shops, public transport, paid parking areas and also to access the bank accounts via internet. In view of this the security and safety of mobile phones have become paramount to prevent unauthorized persons from conducting any unwarranted transactions through the phones. Conventional method of authentication remains mainly text based as it has been around for several decades and also because of ease of implementation. However, text based passwords suffer from various drawbacks such as they are easy to crack through dictionary attacks, brute force, shoulder surfing, social engineering etc.

The "small dictionary" attack is so successful that in Klein's case study [2], about 25% of 14,000 passwords were cracked by a dictionary with only 3 million entries. Following the same method used by Van Oorschot and Thorpe [12], such a dictionary can be exhausted by a 3.2 GHz Pentium™4 machine in only 0.22 second. Graphical passwords, which require a user to remember and repeat visual information, have been proposed to offer better resistance to dictionary attack. Psychological studies support the hypothesis that humans have a better capability to recognize and to recall visual images than alphanumeric strings [3], [4] and [5]. If users are able to remember more complex graphical passwords (i.e., from a larger password space), an attacker has to build a bigger dictionary, thus spend more time or deploy more computational power to achieve the same success as for textual passwords.

In this paper, we will demonstrate a graphical grid-based password scheme which will aim at providing a huge password space along with ease of use. We will also analyze its strength by examining the success of brute force technique. In this scheme we will try to make it easy for the user to remember and more complex for the attacker. In Section II we describe the recent work done in the area of graphical password schemes. Sections III to VI describe the proposed scheme in detail. Security analysis of the proposed scheme is illustrated in the Section VII. This is followed by a case study described in the Section VIII.

II. RELATED WORK

Many papers have been published in recent years with a vision to have a graphical technique for user authentication. Primarily there are two methods, having recall and recognition-based approach respectively. Traditionally both the methods have been realized through the textual password space, which makes it easy to implement and at the same time easy to crack.

The study shows that there are 90% recognition rates for few seconds for 2560 pictures [24]. Clearly the human mind is best suited to respond to a visual image. A number of Recall-Based approaches have been proposed and some of the significant ones based on their security and usability features are presented in this section [23].

Passdoodle is a graphical password comprised of handwritten designs or text, usually drawn with a stylus onto a touch sensitive screen [23]. In their 1999 paper, Jermyn et al. [10] prove that doodles are harder to crack due to a theoretically much larger number of possible doodle passwords than text passwords: while there are only 2.08 x 10^{11} 8 letter passwords, there are 10^{400} different 100-point doodles in a 100 x 100 grid. Figure 1 shows a sample of Passdoodle password.

Figure 1: An Example of a Passdoodle

The issue of recognition prevents widespread use of the Passdoodle. The length and identifiable features of the doodle set the limits of the system. Only a finite amount of computer differentiable doodles can be made. To maintain security the system cannot simply authenticate a user as the user whose recorded doodle is most similar, a minimum threshold of likeliness and similarity must be set. This prevents the use of blatant guessing to authenticate as a random user. However speed and accuracy remain top priorities for the system. A complicated recognition design requiring a hundred training samples and a minute of computation to authenticate negates the purpose of the original pervasive design. Often, the authentication schemes based on the doodles uses a combination of doodle velocity and distribution mapping to recognize and authenticate a doodle [21]. Goldberg and his colleagues [21] developed a Passdoodle algorithm, which was a graphical password comprised of handwritten designs or text, usually drawn with a stylus onto a touch sensitive screen. Their study concluded that users were able to remember complete doodle images as accurately as alphanumeric passwords. They found that people could remember complete doodle images as accurately as alphanumeric passwords, but they were less likely to recall the order in which they drew a doodle than the resulting image. In the other research [22], users were fascinated by the doodles drawn by other users, and frequently entered other users' login details merely to see a different set of doodles from their own.

Another recall-based password approach is VisKey [6], which is designed for PDAs. In this scheme, users have to tap spot in sequence to make a password. As PDAs have a smaller screen, it is difficult to point exact location of spot. Theoretically, it provides a large password space but not enough to face a brute force attack if number of spots is less than seven [7].

A scheme like *Passfaces* in which user chooses the different relevant pictures that describes a story [8] is an image recognition-based password scheme. Recent study of graphical password [9], says that people are more comfortable with graphical password which is easier to remember. In Recall-based password, user has to remember the password.

Figure 2: VisKey SFR

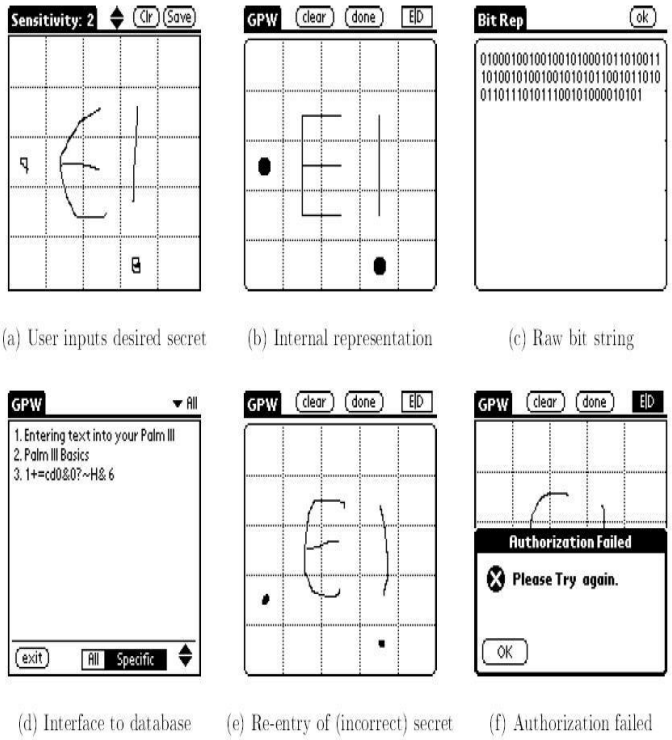

Figure 3: DAS scheme.

Jermyn et al. [10], proposed a technique, called "Draw- a-secret (DAS)", which allows the user to draw their unique password (Figure 3). In the DAS scheme, stylus strokes of the user-defined drawing are recorded and the users have to draw the same to authenticate themselves. DAS scheme also allows for the dots as well as shown in one of the examples in Figure 4.

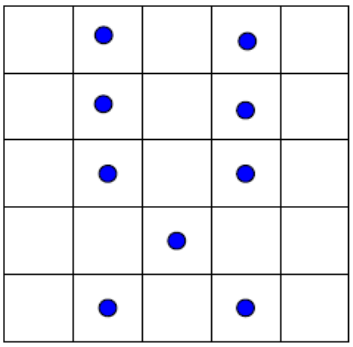

Figure 4: Example of a password in DAS has only dots.

But research shows that people optimally recall only 6 to 8 points in pattern [11], and also successful number of recalls decreases drastically after 3 or 4 dots [12]. Our main motivation will be to increase password space. The user can choose the geometrical shape of their choice for the device like PDA having graphical user interface that will also optimize that password storage space. In our scheme, we will allow users to draw some geometrical shape with some fixed end points and by putting dots at different location but it will give some filed triangle in such a way that chances of remembering those positions will be better.

M. Sarosh Umar and M.Q. Rafiq [1] proposed a technique for mobile devices and PDAs that uses a grid on which the users can authenticate using a password composed of lines and dots.

III. DRAWING GEOMETRY

Drawing geometry is a graphical password scheme in which the user draws some geometrical object on the screen. Through this scheme we are targeting devices like mobile phones, notebook computers and hand-held devices such as Personal Digital Assistants (PDAs) which have graphical user interface. Since these devices are graphical input enabled we can draw some interesting geometries using stylus.

In this scheme there will be *mxn* grids and each grid is further divide into four parts by diagonal lines as shown in Figure 5. We have considered 4x5 grid keeping in mind the typical screen size of the PDAs these days and its width height ratio. Depending on the screen size it can be changed with justifiable number of rows and columns.

On taking the size (4x5) we have total of 5x4 = 20 blocks and each block has four triangles so total number of possible triangles is: (20 blocks) x (4 triangle/block) = 80 triangles. Similarly each block has 4 small diagonal lines so total lines in that way (20 blocks) x (4 lines/block) = 80 lines. Also we do have some lines which are a result of joining adjacent points horizontally and vertically. That will give 4x6=24 (horizontal) and 5x5=25 vertical lines which makes a total of 24+25 = 49 (horizontal and vertical) lines.

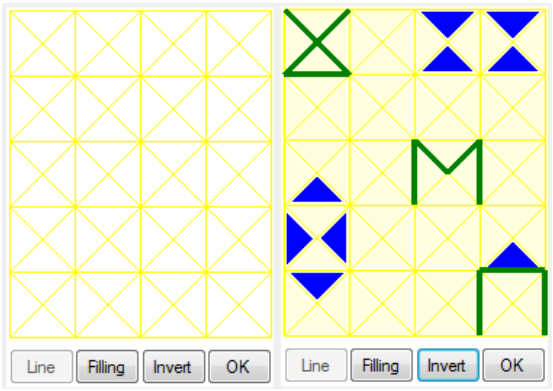

Figure 5: Grid provided to user and some simple geometrical shape drawn by user.

In that way we will have total of

$$p\ (5,4) \Rightarrow 80 + 80 + 49 = 209 \quad (1)$$

These 209 objects can be used to choose password by drawing some of these objects in an easy and efficient manner. A password is considered to be the selection of certain lines and triangles. When a triangle is selected it is filled with some color and when a line is selected the color of that line changes (gets highlighted). Any combination of the selection of lines and triangles will form a password as shown in Figure 6. In this way, highlighted lines and filled triangle will provide us larger password space. Filling triangle and highlighting work can be done by using stylus of PDAs either by putting dot in triangle or by dragging the stylus crossing that line. As research shows that if the number of dots increases to difficult to remember those it is also increases. In this scheme we fill the triangle highlighted lines makes geometric shape which is to be recalled not the dots. More over we give another option which converts all highlighted lines to un-highlighted and vice-versa and the same for filling triangle by single click a button "Invert" a button which at least double the password space within practical limit of password length. A line which is not inclined at an angle of 45° or 0° or 90° i.e. the line which is not parallel to diagonal, horizontal as well as vertical lines. (Let's call them *non-parallel* lines) These non-parallel lines can also be drawn by joining two points after enabling those drawing by clicking the button given labeled line "Line" which enables user to draw non-parallel lines. As we can see that crossing the same lines again cancels the effect of highlighting, Figure 7, in general we can say that crossing even number of times the same line will cancel the highlighting effect. The users don't need to recall the strokes but the resulting geometry. By using inversion operation as shown in Figure 8 the user can deselect all currently highlighted lines and triangles and select all the unselected lines and triangles.

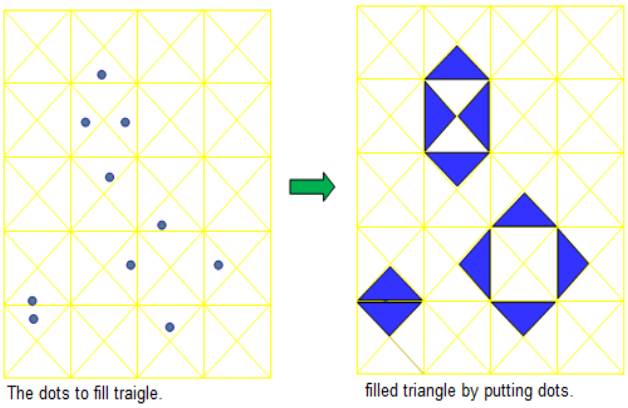

Figure 6: Drawing solid triangle

Note that the inversion does not take place for non-parallel lines. Figure 9 shows a password made by using parallel and non-parallel lines. To draw that we have button stylus able to draw those lines by dragging stylus from one point to another. The start point and end point of such line will be decided by actually where stylus touches the screen and where it leaves it. As illustrated in Figure 9 if stylus touches the screen at any location say coordinate (*x,y)* where two vertical line *va* and *vb* (nearest vertical lines from point P at a distance half cell width) such that *va* _ *x* < *vb* and *ha*_ *y* < *hb* the nearest point of region P will be considered. Same strategy will be adopted for end point where stylus release screen. If lines drawn by user are parallel but procedure adopted by user to draw is as of nonparallel, in that case the scheme will automatically detect that and even if parallel lines are drawn by non-parallel method of drawing it will be considered as parallel lines.

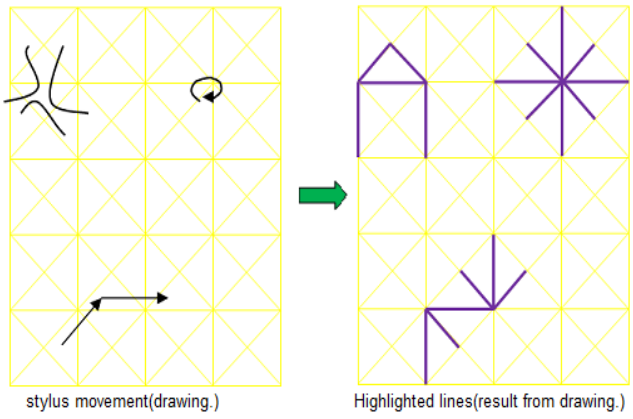

Figure 7: Drawing lines

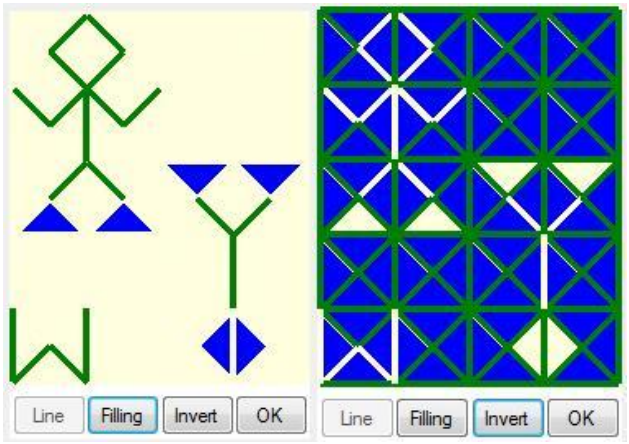

Figure 8: Inversion of drawn geometry

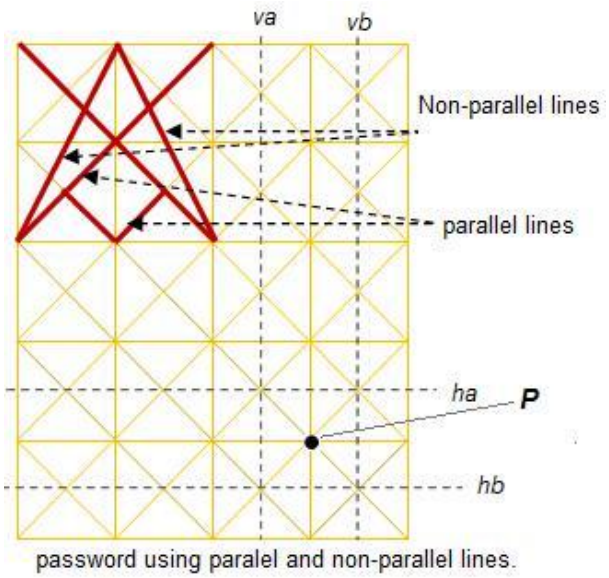

Figure 9: Example of non-parallel lines

The grid shown on screen is for the user's convenience. Password drawn on invisible grids is shown in Figure 8 also illustrates the inversion.

IV. TEXT SIMULATION

Interestingly, the above proposed technique can also be used to write any textual password in graphical manner [1]. In the example shown the word "IMAGINE" is written vertically to accommodate more letters on the screen, still letter E is missing (purposely) as shown in Figure 10. If the password contains more words then multiple screens (say frames) can be used to accommodate them.

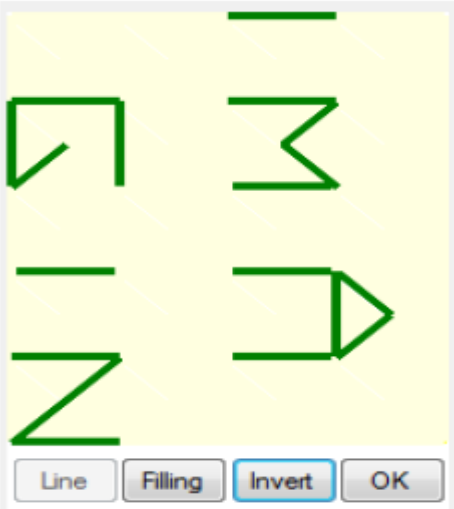

Figure 10: Example of textual password

This can allow users to use textual passwords in graphical way. The letter(s) can be drawn in any direction and any letter can be entered at any position on the screen as per the user's convenience. Thus this method of entering text based passwords has the convenience of the alphanumeric passwords and enjoys the security and robustness of graphical passwords.

V. EXTENSION FOR POSITION INDEPENDENCE AND MULTISTAGE

As of now we have considered that the shapes as well as its location constitute the password, together. If the user has written letter 'A' but fails to recall the position of the 'A' even then the password will be incorrect. This scheme can be extended to accommodate such cases. The location of the figure can be ignored if the shape is correct (as illustrated in Figure 11). The same shape pattern at two different location circled should be treated as same. Obviously doing so the password space decreases but by increasing number of grid this can be compensated. As we have seen that text can be drawn but size of the PDAs limits the grid size. We can have multiple stages for drawing shapes i.e. one shape in first frame followed by next frame and so on.

The user can select the *more* button provided (not shown any where) to go into next fresh blank frame on which more letters or shape can be drawn. As we could not write full word IMAGINE but by doing so (multistage) we can write first few letters say IMA in first frame and rest GINE in second frame. Multistage increases the time required to enter the password but also it gives us huge password space like my password word GRAPH is simulated in geometry the way it can be entered or chosen by user increased like GR and APH or GRA and PH etc for two stage, though stages will be less normally but by not fixing the number of stage we get advantage of high password space.

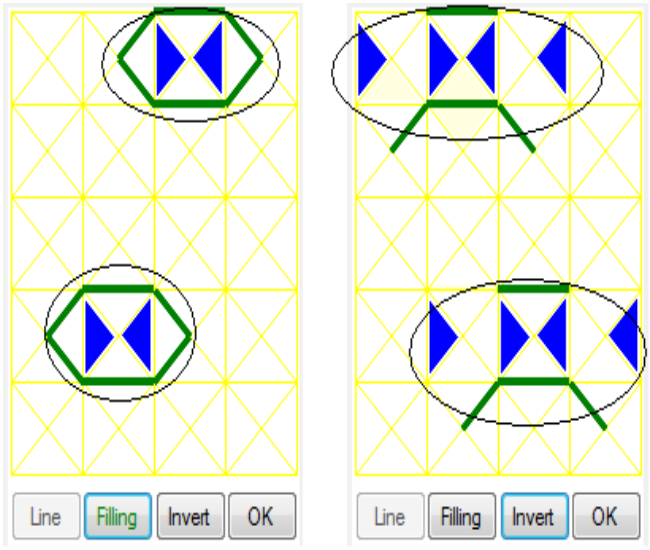

Figure 11: Example of position independence

VI. STORAGE OF PASSWORD

Since there is no need to store any image therefore only password need to be stored as we have seen in case of grid size (4x5) there are 209 possible objects if non-parallel lines are not considered, if we numbered every object from number 0, 1, 2,… , 208 then 209 bits are sufficient to store such password. An extra bit should be kept for inversion whether the password is inverted or not to avoid more calculation while entering the password. For including non-parallel lines, each non-parallel line can be stored by storing the coordinates of two points (start point and end point). The first fix number of bits will represent how many such lines are there and then the coordinates of end points of each line (10 bits for each). So if number of non-parallel lines is *np* then total password length by taking 10 bits for representing each non-parallel line is given in Figure 12.

Required number of bits to store password;

$$= 209 + 1 + 10 + np * 10;$$
$$= 220 + np * 10.$$

So this scheme does not take much space to store the password as many other graphical schemes take [10].

VII. SECURITY ANALYSIS

As we have seen in eqn.(1) that we have 209 objects each can be either highlighted or unselected, individually. Considering only the 209 objects and excluding the non-parallel lines then we have a total of $2^{209} = 8.2275X10^{62}$ possibilities which is huge in terms of password space.

So it is very robust from security point of view even after excluding non-parallel lines. If we consider non-parallel lines also the additional 220 lines will be added which will be also either highlighted or unselected so in that case total password possible $2^{(209+220)} = 2^{429} = 1.386X10^{129}$. It is clear that the password space will increase exponentially with increase in rows or columns as shown in table above. It will be possible for device with a bigger screen (like ATM) to have many more columns and rows.

Due to this larger password space it is very difficult to carry out brute force attack on this password. With this scheme even if user decides to have the graphical representation of the text, he will not be susceptible to dictionary attacks. We have computed above password space in simple case with only 4x5 grids and single stage password entry. Since we have not made any special assumption for text simulation in this scheme, the password space remains same even if we use it as textual password scheme.

VIII. CASE STUDY

A case study was conducted and twenty five users were chosen randomly comprising undergraduate and graduate students of engineering discipline. A short questionnaire was developed and the users were requested to try this scheme and share their experience with us. Interestingly, the users rated it 8.5 on a scale of 10.0 on ease of use which demonstrates the acceptable usability of the scheme. 80% of the users (20) found it easier to remember passwords in the form of graphical figures. Twenty one users out of twenty five could reproduce their passwords after an interval of one week. A rigorous study may be conducted to further explore the proposed scheme.

IX. CONCLUSION AND FUTURE WORK

In this paper, we have proposed a graphical password scheme in which the user can draw simple geometrical shapes consisting of lines and solid triangles. The user need not remember the way in which the password is drawn but only the final geometrical shape.

This scheme gives large password space and is competent in resisting brute force attack. Moreover, the way of storing the password requires less memory space as compared to the space required by other existing graphical authentication schemes.

This scheme is less susceptible to shoulder surfing as the screen of the hand held device is visible to the user only. However, when employed on PCs and ATM machines it is susceptible to shoulder surfing. To make it more robust and handle the problem of shoulder surfing, the geometrical shape will have to be drawn by assigning an order to the various components i.e. triangles and lines. This consideration will limit the scheme's vulnerability to shoulder surfing and will further expand the password space. Moreover, a background image on the grid may be chosen by the user to aid the process of inputting the geometry of the password. This would further enhance the memorability of the graphical password.

REFERENCES

[1] M. Sarosh Umar and M. Q. Rafiq, "A Graphical Interface for User Authentication on Mobile Phones", in Proceedings of The Fourth International Conference on Advances in Computer-Human Interactions (ACHI 2011), IARIA, ISBN: 978-1-61208-117-5, pp. 69-74, 2011.

[2] D. Klein, "Foiling the Cracker", A Survey of, and Improvements to, Password Security in The *2nd USENIX Security Workshop*, pp. 5-14, 1990.

[3] A. Paivio, T. B. Rogers, and P. C. Smythe, "Why are pictures easier to recall than words?", Psychonomic Science, 11: 137-138, 1968.

[4] G. H. Bower, M. B. Karlin, and A. Dueck, "Comprehension and memory for pictures". Memory and Cognition, 3, 216-220, 1975.

[5] L. Standing, "Learning 10,000 Pictures". Quarterly Journal of Experimental Psychology, 25: 207-222, 1973.

[6] SFR-IT-Engineering, http://www.sfr-software.de/cms/EN/pocketpc/viskey/, Accessed on January 2011.

[7] M. D. Hafiz, A. H. Abdullah, N. Ithnin, and H. K. Mammi, "Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique", in Proceedings of the Second Asia International Conference on Modelling & Simulation, IEEE Computer Society, pp. 396-403, 2008.

[8] D. Davis, F. Monrose, and M. Reiter, "On User Choice in Graphical Password Schemes", in Proceedings of *13th USENIX Security Symposium*, pp. 151–164, 2004.

[9] J. Thorpe and P. C. van Oorschot, "Graphical Dictionaries and the Memorable Space of Graphical Passwords", in Proceedings of *13th USENIX Security Symposium*, pp. 135–150, 2004.

[10] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The Design and Analysis of Graphical Passwords", in Proceedings of *8th USENIX Security Symposium*, pp. 1-14, 1999.

[11] R. S. French, "Identification of Dot Patterns From Memory as a Function of Complexity", *Journal of Experimental Psychology*, 47: 22–26, 1954.

[12] S. I. Ichikawa, "Measurement of Visual Memory Span by Means of the Recall of Dot-in-Matrix Patterns", *Behavior Research Methods and Instrumentation*, 14(3):309–313, 1982.

[13] X. Suo, Y. Zhu, and G. S. Owen, "Graphical Passwords: A Survey", in Proceedings of the 21st Annual Computer

Security Applications Conference (ACSAC 2005), IEEE Computer Society, pp. 463-472, 2005.

[14] K. Chalkias, A. Alexiadis, and G. Stephanides, "A Multi-Grid Graphical Password Scheme", in 6th International Conference on Artificial Intelligence and Digital Communications (AIDC 2006), Greece, pp. 80-90, 2006.

[15] J. Thorpe and P. C. van Oorschot, "Towards Secure Design Choices for Implementing Graphical Passwords", in Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC'04), IEEE Computer Society.

[16] J. Thorpe, P.C. van Oorschot, and A. Somayaji, "Pass-thoughts: Authenticating With Our Minds", Proceedings of Workshop on New security paradigms, Lake Arrowhead, California, pp. 45 – 56, 2005

[17] P. L. Lin, L. T. Weng, and P. W. Huang, "Graphical Passwords Using Images with Random Tracks of Geometric Shapes", in Proceedings of 2008 Congress on Image and Signal Processing, IEEE Computer Society, pp. 27-31, 2008.

[18] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical Password Authentication Using Cued Click Points", ESORICS 2007, 12th European Symposium on Research in Computer Security, Dresden, Germany, September, pp. 24-26, 2007.

[19] M. W. Calkins, "Short studies in memory and association" from the Wellesley College Laboratory. Psychological Review, 5:451-462, 1898.

[20] M. A. Borges, M. A. Stepnowsky, and L. H. Holt, "Recall and Recognition of Words and Pictures by Adults and Children". Bulletin of the Psychonomic Society, 9:113-114, 1977.

[21] C. Varenhorst, "Passdoodles: a Lightweight Authentication Method", Massachusetts Institute of Technology, Research Science Institute, July 27,2004.

[22] K. Renaud, "On User Involvement in Production of Images Used in Visual Authentication"; Elsevier, Journal of Visual Languages and Computing, pp. 1-15, 2009.

[23] A. H. Lashkari, R. Saleh, F. Towhidi and S. Farmand, "A complete comparison on Pure and Cued Recall-Based Graphical User Authentication Algorithm", IEEE - ICCEE '09: Proceedings of the Second International Conference on Computer and Electrical Engineering - December 2009, Volume 01, pp. 527-532, 2009.

[24] L Standing, J. Conezio, and R. N. Haber, "Perception and Memory for Pictures: Single-trial Learning of 2500 Visual Stimuli". Psychonomic Science, 19(2): 73-74, 1970.

Total cells	No. of Rows(i)	No. of Columns(j)	Parallel lines and triangles. ($p(i,j)$)	No. of Non-Parallel lines. ($n(i,j)$)	Total lines and triangles.	Password space (without non-parallel lines)	Password space (including non-parallel lines)
9	3	3	96	44	140	7.922×10^{28}	1.393×10^{42}
12	4	3	127	80	207	1.701×10^{38}	2.057×10^{62}
16	4	4	168	140	308	3.741×10^{50}	5.215×10^{92}
20	5	4	209	220	429	8.227×10^{62}	1.386×10^{129}
24	6	4	250	320	570	1.809×10^{75}	3.864×10^{171}
25	5	5	260	340	600	1.852×10^{78}	4.149×10^{180}
30	6	5	311	490	801	4.712×10^{93}	1.333×10^{241}
36	6	6	372	700	1072	9.619×10^{111}	5.060×10^{322}
49	7	7	504	1288	1792	5.237×10^{151}	2.791×10^{539}

Figure 12: Variation of password space with increase in the number of grids