Simplified Native Language Passwords for Intrusion Prevention

Sreelatha Malempati
R.V.R. & J.C. College of Engineering,
Chowdavaram, Guntur, A.P

Shashi Mogalla
Andhra University College of Engineering,
Visakhapatnam, A.P.

ABSTRACT
Authentication is necessary in multi-user systems. User name and password are used to authenticate a user. Textual passwords are most common type used for authentication. Authentication schemes that use textual passwords are vulnerable to attacks password stealing, dictionary attack and shoulder surfing. Graphical passwords provide an alternative to graphical passwords but, simple schemes are vulnerable to shoulder surfing and hidden cameras. Native language passwords can be used for authentication and the user can remember it better than any other language. A shape based textual authentication is discussed in this paper and simplification of the native language passwords is proposed. Session passwords are generated for each login, making the authentication scheme more resistant to shoulder surfing and hidden camera attacks.

Keywords
Shape based authentication, Textual Password, Native language password, Intrusion prevention.

1. INTRODUCTION
Intrusion prevention is the first step of security. The main goal of the intruder is to gain access to a system as a legitimate user. User name and password are used for authenticating users in a system.. Textual passwords are the conventional type used for authentication. Generally users select simple and short passwords[1] to remember easily. But using these simple and short passwords make the task of intruder easy [2, 3]. Long and complex passwords are hard to remember. Two major difficulties in authentication are password length and guessable passwords. Most of the users select English for their textual passwords which makes password guessing, eaves dropping, dictionary attacks and shoulder surfing easy. To overcome these vulnerabilities graphical password schemes have been introduced.

The graphical password schemes use images or shapes for authenticating the user. Users remember the images or shapes better than textual password [4]. But for graphical schemes, shoulder surfing and hidden cameras are the main problems. As an alternative to textual passwords, biometrics, such as finger prints, irisscan or facial recognition have been introduced but not yet widely adopted. The major drawback of this approach is that such systems can be expensive and the identification process can be slow. This approach requires a special sensor for the biometric. In this paper, a new shape based textual authentication scheme for native language passwords is discussed. Users can remember their native language passwords better than any other language. User selects a character from his native language and submits the shape of that character in a grid during password creation. Later based on this information, the user is authenticated. Native language consists of many characters having different shapes. It may be difficult to follow the shape for difficult characters. User can have his own style for the characters and he can use that style as shape of the character for authentication.

This paper is organized as follows: Related work is discussed in section 2, in section 3 the new shape based textual authentication scheme is introduced, security analysis is done in section 4, conclusion and future work are proposed in section 5.

2. RELATED WORK
Since textual password schemes are vulnerable to many attacks, graphical password schemes are designed as alternative schemes to text-based schemes. Many authentication schemes are designed using images based on the concept that humans remember pictures better than text.

Blonder [5] designed a graphical password scheme in which a password is created by having the user click on several locations on an image. During authentication, the user must click on the approximate areas of the locations. Dhamija and perrig [6] proposed a graphical authentication scheme in which the user selects a certain number of images from a set of random pictures. Later user has to identify the pre-selected images for authentication. Passface [7] is a technique where the user sees a grid of nine faces and selects one face previously chosen by the user. Since there are four user selected images it is done for four times. The drawback of the both of these techniques is vulnerability to shoulder-surfing. Davis et al [8] proposed an alternative scheme story that used images instead of faces. It was difficult to remember images than faces but user choices were less predictable. Jansen [9],[10] proposed a graphical password scheme for mobile devices. During password creation, a user selects a theme consisting of photos in thumbnail size and set a sequence of pictures as a password. During authentication, user must recognize the images in the correct order. Each thumb nail image is assigned a numerical value, thus the sequence of the chosen images will create a numerical password. As the no. of images is limited to 30, the password space of this scheme is not large. Weinshall and Kirkpatrick [11] proposed several authentication schemes such as picture recognition, object recognition and pseudo word recognition and conducted user studies on these. The results declared that pictures are most effective than the other two proposed schemes. Goldberg [12] designed a technique known as "passdoodle". This is a graphical password authentication scheme using handwritten design or text usually drawn with a stylus onto a touch sensitive screen. Jermyn et al [13] proposed a technique called "Draw A Secret" (DAS) where a user draws the password on a 2D grid. The coordinates of this drawing on the grid are stored in order. During authentication user must redraw the picture. The user is authenticated if the drawing touches the grid in the same order.

All these graphical authentication schemes are vulnerable to shoulder surfing.

To overcome the shoulder-surfing problem, many techniques were proposed. Zhao and Li [14] proposed a shoulder-surfing resistant scheme "S3PAS". The main idea of the scheme is as follows. In the login stage, they must find their original text passwords in the login image and click inside the invisible triangle region. The system integrates both graphical and textual password scheme and has high level security. Man, et al, [15] proposed another shoulder-surfing resistant technique. In this scheme, a user chooses many images as the pass-objects. The pass-objects have variants and each of them is assigned to a unique code. In the authentication stage, the user must type the unique codes of the pass-objects variants in the scenes provided by the system. Although the scheme shows perfect results in resisting hidden camera, it requires the user to remember code with the pass-object variants. Luca, et al. [16] proposed a stroke based shape password for ATMs. They argued that using shapes will allow more complex and more secure authentication with a lower cognition load. More graphical password schemes have been summarized in a recent survey paper [17].

H.Tao and C. Adams [18] proposed Pass-Go named after an ancient board game Go. This scheme allows users to draw their password using grid intersection points instead of grid cells in DAS. H.Gao et al [19] proposed another modification to DAS. In this scheme, approximately correct drawing can be accepted by dividing "trend quadrants" and adopting Levenshtein distance string matching. ColorLogin [20] uses background color to decrease login time and resist shoulder-surfing. Zheng et al [21] designed a hybrid password scheme based on shape and text. The basic concept is mapping shape to text with strokes of the shape and a grid with text. They suggested it for general shapes and characters. It is difficult to remember general shapes and characters selected at random. This paper focuses on native language passwords because user can remember native language passwords better than any other language. Sreelatha Malempati and Shashi Mogalla [22] proposed authentication scheme based on native language passwords. They used Telugu language for their authentication scheme. Even it is possible to simplify the native language alphabet to make the authentication scheme easy and simple to use. This paper proposes a simplified form for native language for authentication.

3. THE AUTHENTICATION SCHEME

The new shape based textual authentication scheme consists of three steps:

- password creation
- password entry
- password verification

3.1 Password creation

User selects a character from his native language character set. Each character may contain one or more strokes. A stroke is an ordered list of cells. A password is represented by a sequence of strokes. The length of a stroke is the number of cells it contains. The length of the password is the sum of the lengths of its strokes. An interface consisting of a grid of size 5x 5 will be displayed on the screen. User has to select an ordered list of grid cells to represent the shape of the character selected for password. Consider the character "ga" in figure 1.

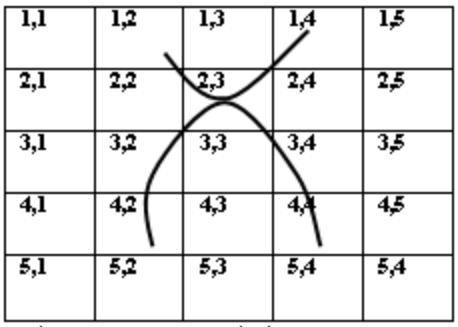


Figure 1: password character "ga"

This character consists of two strokes, each consisting of a set of ordered grid cells. The first stroke of the character starts from the grid cell (4,2) and ends with (4,4). The second stroke starts with (1, 2) and ends with (1, 4). Totally the shape of the character can be represented by the grid cells { (4,2), (3,2),(2,3),(3,4),(4,4),(1,2),(2,3),(1,4) } .User has to select the grid cells in this order at the time of password creation.

3.2 Password entry

At the time of login, user has to enter his login ID and password. An interface consisting of grid of size 5x5 will be displayed. The grid contains a symbol in each cell. Based on the symbol in the grid cells and shape of the character selected by him, user has to enter his password. For the interface in figure 2, suppose the user enters the password: {01110110}.

1	1	0	0	1
0	1	1	0	0
1	1	0	1	0
1	0	1	0	1
0	1	0	1	1

Login ID: _____
Password: _____

Figure 2: Login interface

3.3 Password verification

After password entry, the authentication scheme will verify the password. It will compare the symbols of the interface in the positions of the grid cells selected by the user at the time of password creation with the symbols of the password entered by the user at the time of login. If the password entered is not correct, the system will generate another login interface grid with different symbols.

At each login step, the symbols vary, but the shape of the character and the order of the grid cells that represent the shape

of the character do not vary and the password entered by the user varies. So, the text-based brute force attack will not work.

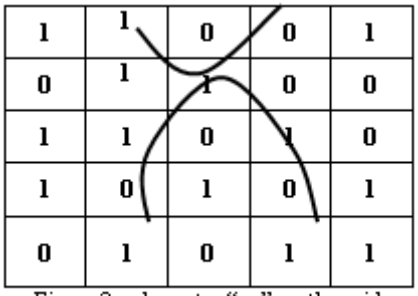


Figure 3: character "ga" on the grid

For the above interface, the password will be verified in this manner: The shape of the character is represented by the cells: (4,2),(3,2),(2,3),(3,4),(4,4),(1,2),(2,3),(1,4)}. For this interface, by considering the symbols of the cells in the above order, actual password is 01110110 and the password entered by the user is 01110110. In this example, user is authenticated.

4. SIMPLIFYING NATIVE LANGUAGE CHARACTERS

In this paper, Telugu language is selected as the native language of the user. Telugu is one of the official languages of India. There are 18 vowels and 36 consonants in the language. A syllabic unit could be a vowel, a consonant or their combination. In a combination, the vowel part is indicated using a diacritic sign known as maatra. The shape of a maatra is often completely different from the corresponding vowel. The shape of the consonant also changes when it combines with a vowel or with another consonant. Each character is represented by one or more strokes with some strokes extending above or below the main part of the character. There may be overlapping of these strokes in many of the characters. The shape of the characters "ya" and "ma" are shown in figure 4,figure 5 and figure 6,figure 7 respectively.

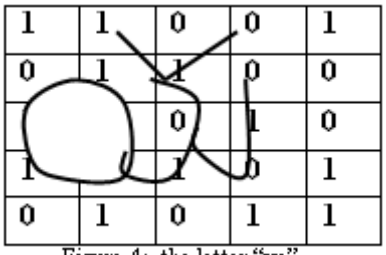


Figure 4: the letter "ya"

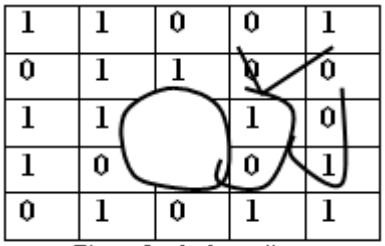


Figure 5: the letter "ya

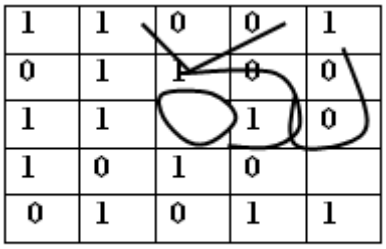


Figure 6: the letter "ma"

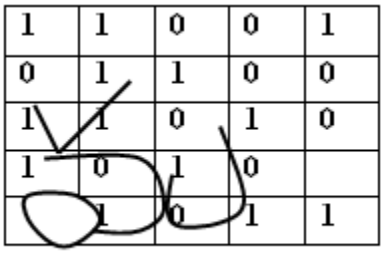


Figure 7: the letter "ma"

It may be difficult to remember the shape of the character, number of strokes and grid cells in the stroke. User can have his own style for writing the native language characters. Instead of using the shape of the character directly, he can use his style of representation as shape of the character which makes the authentication scheme easy and simple to use.

Some of the characters of the TELUGU language and the simplified form of those characters which can be used for authentication are shown in table1.

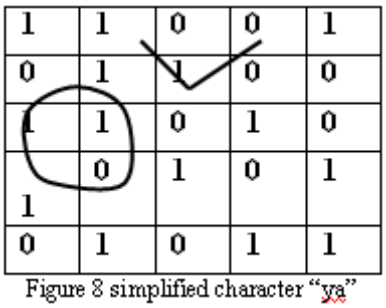


Figure 8 simplified character "ya"

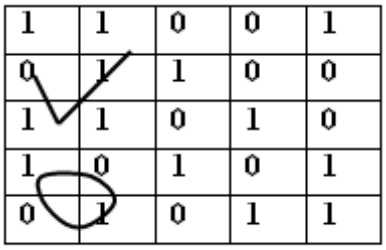


Figure 9: simplified character "ma"

The simplified character "ya" can be represented by the cells { (2,1), (3,1), (4,1), (4,2), (3,2), (2,2),(2,1), (1,2),(2,3), (1,4) }and the character "ma" can be represented by the cells {(3,1), (4,1), (4,2), (3,2), (3,1), (2,1), (3,1), (2,2)}.

The word "ee la" contains two characters "ee" and "la". Figure 10 shows the shape of the character "ee" with the sequence { (2,2), (2,3), (2,4), (3,4), (3,3), (3,3), (4,4) } and figure 11 shows the shape of the character "la" with the sequence { (3,3), (3,3), (4,3), (4,4), (3,4) }.

By the simplified characters, the word "eela" can be represented by the sequence { (2,3), (2,4), (3,3), (4,3), (4,4), (3,4) } as shown in figure 12 or by the sequence {(2,1), (2,2), (2,4), (3,4), (3,5), (2,5)} as shown in figure 13.

Figure 10 : shape of the word "ee"

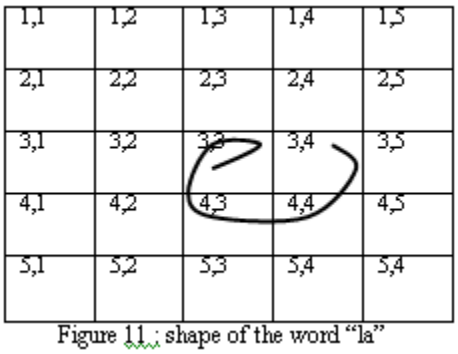


Figure 11 : shape of the word "la"

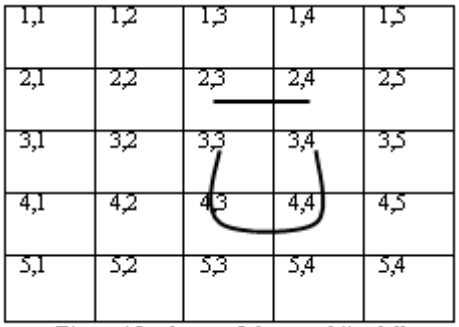


Figure 12: shape of the word "ee la"

Figure 13 : another shape of the word "ee la"

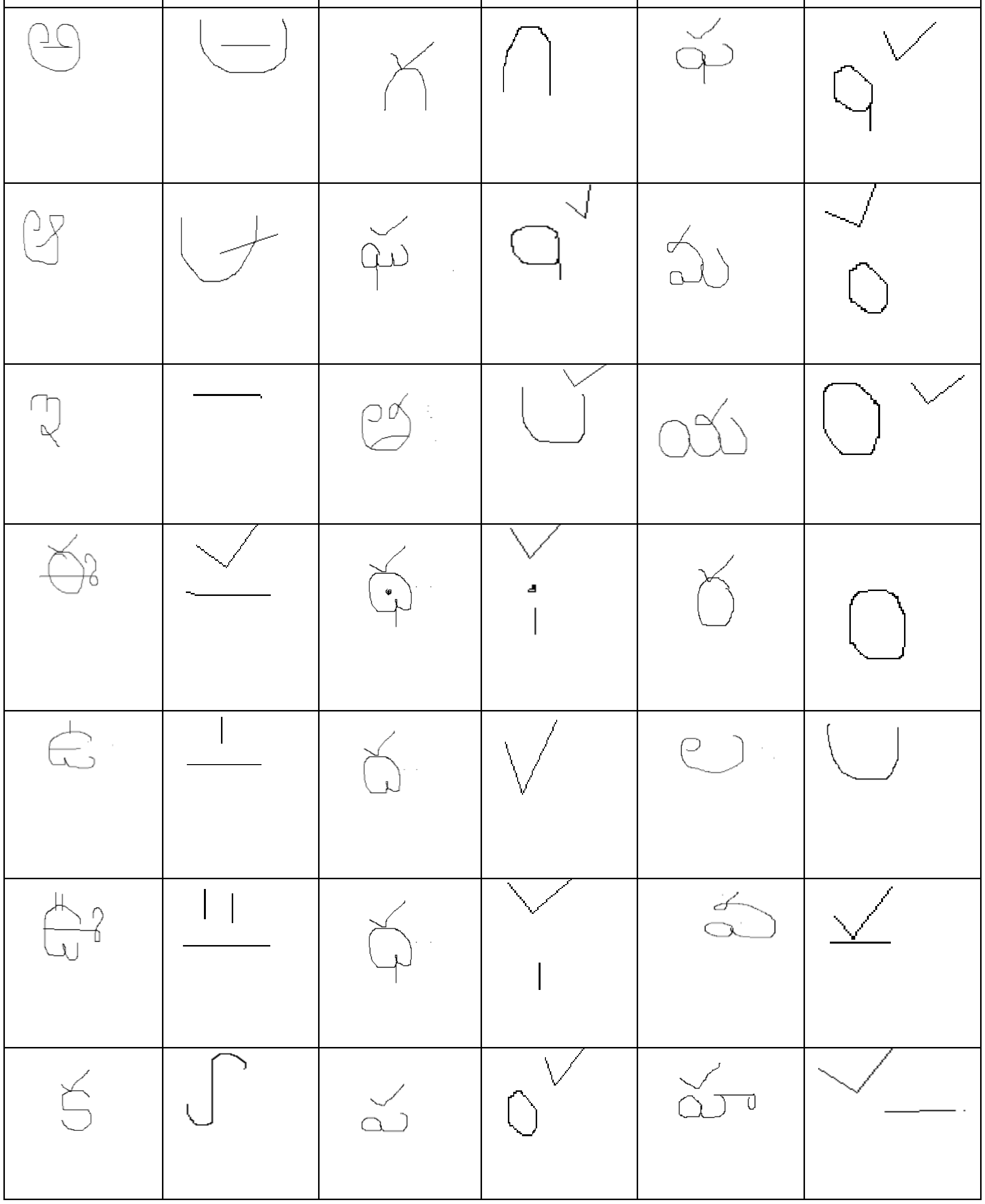
5. CONCLUSION

A new authentication scheme based on native language passwords is proposed. In this paper, Telugu language is selected as the native language of the user. Telugu is one of the official languages of India. Based on the shape of the characters of the native language and the grid symbols generated in each interface, passwords are entered by the user and the system verifies the password and authenticates the user. The proposed scheme is resistant to eves dropping, brute force attack, shoulder surfing and hidden camera.

The intruder should have the knowledge of native language of the user at first step to detect the password. The process of creating the password and entering the password are time taking and vulnerable activities because of complexity of characters. To reduce these problems, a simplified scheme is proposed. The simplified scheme presents the native language alphabet set in a simple form which makes authentication process simple and easy to use. Usability and memorability of this scheme should be studied . Applications of native language passwords for other aspects of the security should be studied.

Table 1: Simplified characters of the Telugu language

Telugu letter	Modified letter	Telugu letter	Modified letter	Telugu letter	Modified letter



6. REFERENCES

[1] A. Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," *Communications of the ACM*, vol. 42, pp. 41-46, 1999.

[2] A. S. Patrick, A. C. Long and S. Flinn, “HCI and Security Systems”. Presented at CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA, 2003.

[3] Gilbert Notoatmodjo, “Exploring the ‘Weakest Link’: A Study of Personal Password Security”. Thesis of Master Degree, the University of Auckland, New Zealand, 2007.

[4] R. N. Shepard, "Recognition memory for words, sentences, and pictures," *Journal of Verbal Learning and Verbal Behavior*, vol. 6, pp. 156-163, 1967.

[5] 5. G. E. Blonder, “Graphical Passwords,” in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed.United States, 1996.

[6] R. Dhamija and A Perrig, "Deja Vu: A User Study using Images For Authentication", 9th USENIX Security Symposium, 2000.

[7] RealUser. “www.realuser.com” last accessed in June 2005.

[8] Davis, D., F. Monrose, and M.K. Reiter. “On User Choice in Graphical Password Schemes” 13th USENIX Security Symposium, 2004.

[9] W. Jansen, "Authenticating Mobile Device User through Image Selection," in *Data Security*, 2004.

[10] W. Jansen, "Authenticating Users on Handheld Devices “in *Proceedings of Canadian Information Technology Security Symposium*, 2003.

[11] D. Weinshall and S. Kirkpatrick, “Passwords You’ll Never Forget, but Can’t Recall,” in Proceedings of Conference on Hman Factors in Computing Systems (CHI), Vienna, Austria: ACM, 2004.

[12] J. Goldberg, J. Hagman, V. Sazawal, "Doodling Our Way To Better Authentication", CHI '02 extended abstracts on Human Factors in Computer Systems, 2002.

[13] Jermyn, I., Mayer A., Monrose, F., Reiter,M., and Rubin., “The design and analysis of graphical passwords” in Proceedings of USENIX Security Symposium, August 1999.

[14] H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme," in *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW 07)*, vol. 2. Canada, 2007, pp. 467-472.

[15] S.Man, D. Hong, and M.Mathews, "A shoulder surfing resistant graphical password scheme," in *Proceedings of International conference on security and management. LasVergas*, NV, 2003.

[16] A. D. Luca, R. Weiss, and H. Hussmann, "PassShape: stroke based shape passwords," in *Proceedings of the conference of the computer-human interaction special interest group (CHISIG) of Australia on Computer-human interaction: design: activities, artifacts and environments*. 28-30 November 2007, Adelaide, Australia, pp. 239-240.

[17] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," *21st Annual Computer Security Applications Conference (ASCSAC 2005)*. Tucson, 2005.

[18] H. Tao and C. adams, “Pass-Go: A proposal to improve the usability of graphical passwords” International Journal of Network Security, vol. 7, no. 2, pp. 273-292, 2008.

[19] H. Gao, X. Guo, X. Chen, L. Wang, and X. Liu, “YAGP: Yet another graphical password strategy”. in 24th Annual Computer Security Applications Conference, ACSAC08, California, 2008, 121-129.

[20] H. Gao, X. Liu, R. Dai, S. Wang, and X. Chang. Analysis and evaluation of the colorlogin graphical password scheme. In Fifth International Conference on Image and Graphics, 2009, 722-727.

[21] Z. Zheng, X. Liu, L. Yin, Z. Liu “A Hybrid password authentication scheme based on shape and text” Journal of Computers, vol.5, no.5 May 2010.

[22] Sreelatha Malempati and Shashi Mogalla , “ Intrusion Prevention by Native Language Password Authentication Scheme “ in Fourth International Conference on network security & Applications, CNSA 2011, India (Accepted)