A FRAMEWORK FOR IMAGE BASED AUTHENTICATION

C.Perra, Member, IEEE, D.D.Giusto, Member, IEEE

Department of Electrical and Electronic Engineering, University of Cagliari

ABSTRACT

This paper presents an innovative framework for user authentication based on images. Common user authentication based on passwords has the main drawback of the human difficulty in recalling them. Images are instead easier to remember than passwords. Moreover, modern compression and transmission techniques make image exchange between different devices (e.g. mobile phones, personal digital assistants, laptops, and workstations) in heterogeneous networks practically feasible. In the proposed approach, images are coded using the emerging JPEG2000 standard and taking advantage of many of its features (e.g. image scalability, embedded bitstream, image tiling, and interactivity protocol). The described image based authentication is more secure than the common approach based on password.

1. INTRODUCTION

An authentication system based on character strings as password is very vulnerable. An attacker can guess the user password when people use words that are easy to remember or he can use the well known dictionary attacks methods for discovering the password.

An authentication method based on images can improve the security of the user authentication compared to that of textual password.

An image based authentication system has two advantages: the user can remember images more easily than passwords [1]; the system will be less vulnerable to hacker attack techniques [2,3].

For this reason, the use of personal/personalized images can be a means of user authentication more effective than string based (password) authentication.

An authentication system can collect user images to be used by a challenge and response protocol for authenticating the user.

Functionalities such as scalability, progressive image transmission, client/server interactivity are undoubtedly necessary in order to make the image exchange and user authentication process feasible.

The emerging JPEG2000 standard for image coding published by the JPEG committee (ISO/IEC JTC 1/SC 29/WG 1) provides the required feature for the framework described in this paper.

Furthermore, at the 31st JPEG Meeting, a new call for technology [4] was issued with the goal of providing standard specifications for an authentication protocol in an image based authentication system based on the JPEG 2000 standard.

This paper proposes an innovative framework for image based authentication (IBA) which takes full advantage of JPEG 2000's functionalities and JPEG 2000's interactivity protocol [5].

The rest of the paper is organized as follows. A brief analysis of the related work is presented in Section 2. The IBA framework is described in Section 3. Finally, Section 4 concludes this paper.

2. RELATED WORK

There are some graphical/image based authentication approaches proposed in the literature.

In [6], a user is required to select some predetermined points on an image ("graphical password") in a particular order for being authenticated.

Two graphical password schemes were proposed in [7]. The first method was a simple enhancement of the input of textual passwords using graphical techniques. The second method required the user to draw a secret design on a display grid. These schemes achieved better security than conventional textual passwords.

The requirements of a recognition-based authentication system were examined in [8]. In this approach, the user authentication depends on his ability to recognize previously seen images.

An interface similar to a numeric keyboard is proposed in [9], but numbers are replaced with images. Results presented in [8,9] show that visual approaches to user authentication have advantages over password authentication.

The technique proposed in [10] relies on image password randomly generated by the system and the authentication process is based on image recognition.

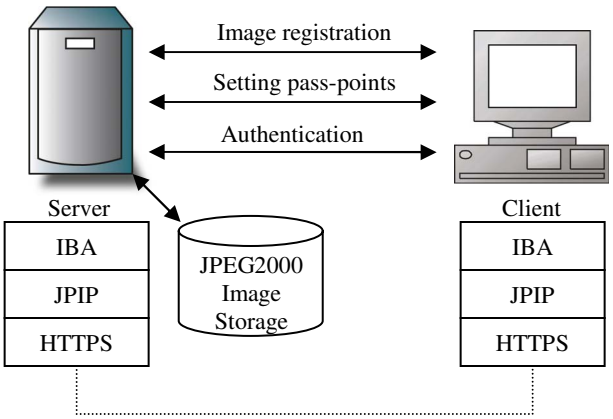

Fig. 1. – Proposed Image Based Authenticaton (IBA) framework.

Images provided by the user are used as "pass-images" in [2]. A set of images are shown to the user. He selects his personal pass-images or none of them if the pass-images are not present. Such process is iterated n times changing the set of images. If all verification stages are successful then the user is authenticated. This method has the same security level of a n-digit number password.

In [11], a set of small objects are randomly scattered in the display. The user has previously chosen a set of *pass-objects*. These objects are randomly placed inside a region of the display. The user must select an invisible triangle containing at least three pass-objects in order to be authenticated. The number of possible graphical password is a little higher than the number of possible alphanumeric password. Therefore, the probability of a successful attack is lower in the graphical password authentication.

Another image based authentication method was presented in [3]. The user can provide personal set of images or he can use predefined images. The authentication is obtained selecting a sequence of images as in [2]. Such sequence is then used to derive an associated password.

3. IMAGE BASED AUTHENTICATION

The proposed Image Based Authentication (IBA) framework provides a user authentication mechanism based on JPEG2000 compressed imagery and Client-Server interaction. Fig. 1 shows an overview of the proposed system. Images are compressed using the JPEG2000 standard in order to take advantage of its capabilities (e.g. image scalability, embedded bitstream, image tiling, and interactivity protocol). JPIP [5] defines an interactive protocol to achieve an efficient exchange of JPEG2000 images and related data. JPIP allows the delivery of portion of JPEG2000 images in arbitrary order. HTTPS is a possible transport for JPIP and provides security to the connection.

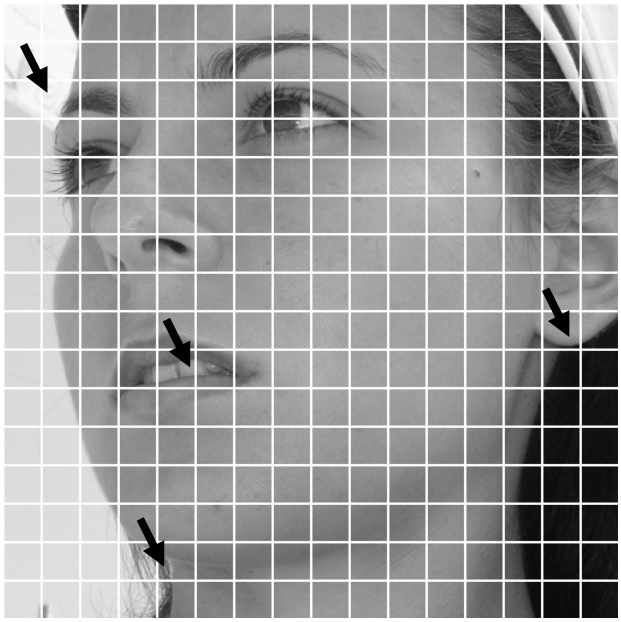

Fig. 2. An example of personal image. Horizontal and vertical lines are superimposed to the image for showing the image tiling and are not visible in true application. Arrows indicates the pass-points chosen by the user.

3.1. Image registration

Image registration is divided into two distinct phases. In the first phase, the user registers his personal information (Name, e-mail, etc.) and uploads his authentication image to the server. An e-mail is sent to the user for confirming the registration.

Let the image be of size $w \times h$ pixels. The image is coded by the server using JPEG2000 and subdivided into non-overlapping tiles of $m \times n$ pixels. The number of tiles is $t = (w/m)(h/n)$. Then the coded stream is reordered in a stream media type suitable for subsequent JPIP connection.

In the second phase, the user access for the first time to the authentication system and selects k points (pass-points) of the image. These points are stored in the server and used in the authentication process described in Section 3.2.

Fig. 2 shows a personal image registered to the server and partitioned into non-overlapping blocks (tiles). The image size is 512×512 pixels and tiles are 32×32 pixels. Hence, the image is a chessboard of 16×16 tiles. Tiling reduces memory requirements and can be used for

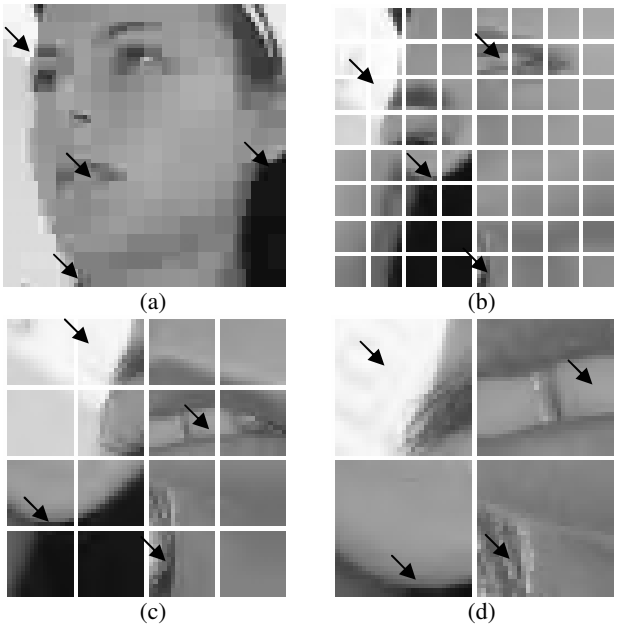

Fig. 3. Four input stages (p=4) authentication example. Display resolution is 64×64 pixels. (a) Image at low resolution (256 tiles at the lowest resolution), (b) Selected areas at higher resolution (64 tiles are enhanced), (c) Selected areas at higher resolution (32 tiles are enhanced), (d) Four tiles at full resolution. Horizontal and vertical lines are superimposed to the images (b), (c), and (d) for showing the image tiling and are not visible in true application. Arrows indicates the pass-points chosen by the user.

decoding specific part of the image instead of the whole image. In Fig. 2, four pass-points ($k = 4$) are chosen by the user.

3.2. User authentication

The user authentication session consist of p input stages. The client receives and displays a low-resolution version of the image (stage $s = 1$, e.g. Fig. 3 (a)).

The user chooses k points in the image. These points should correspond approximately to the pass-points. Selected points are sent to the server in a IBA request. The server responds to the client sending appropriate tile parts corresponding to the chosen areas at a resolution higher than at the previous stage (e.g. Fig. 3(b)).

The procedure continues iteratively ($s > 1$, e.g. Fig. 3(c)) until the highest resolution is reached ($s = p$, e.g. Fig. 3(d)).

When the maximum resolution is reached, the server evaluates the distance between selected points and pass-points. If such distance is lower than a threshold d then the user is authenticated.

At each stage ($s > 1$), the k areas, chosen at the previous stage, are randomly ordered in the display. Hence, there is not correlation between the selection order of the k points and the display order of corresponding areas in the following stage.

3.3 Considerations

The total number of selectable items for each input stage s, before the last, is the number of tiles t_s displayed. The user selects k points and the corresponding areas are transmitted at a higher resolution. Hence, at each stage, the total number of possible combination is

$$C_{t_s,k} = \binom{t_s}{k} = \frac{t_s!}{k!(t_s - k)!} . \quad (1)$$

For the last input stage, considering a maximum error of d pixel in the pass-point selection, the possible selection areas are

$$t_p = \frac{v_x v_y}{2d} , \quad (2)$$

where $v_x \times v_y$ pixels is the displayed image resolution and the number of possible combinations is $C_{t_p,k}$.

For the example in Fig. 3, setting $d = 8$, the total number of possible cases is

$$N = C_{256,4} \cdot C_{64,4} \cdot C_{16,4} \cdot C_{64,4} \approx 1.28E + 23 . \quad (3)$$

An alphanumeric password has c^l possible combinations, where c is the alphabet size and l is the password length. The standard visible characters (printable characters) are $c = 95$. A password of 12 characters should be used for obtaining the same order of magnitude of N. Moreover, it should be observed that passwords are usually not randomly chosen and only a small subset of the c^l possible combinations is used.

IBA requires more network resources than textual authentication. Nevertheless, image tiling and JPIP protocol allows an efficient transmission because only information relevant to enhance the required tiles are transmitted at each stage. This approach optimizes the transmission and allows image exchange between different devices (e.g. mobile phones, personal digital assistants, laptops, and workstations).

The pass-points selected by the user on his image should have a personal meaning in order to help a long term recall. Furthermore, the user needs a precise recall of

Image Based Authentication (IBA)			
Input Stages (p)	2	3	4
Tiles	$t_0 = 256$ $t_1 = 64$	$t_0 = 256$ $t_1 = 64$ $t_2 = 64$	$t_0 = 256$ $t_1 = 64$ $t_2 = 16$ $t_4 = 64$
Combinations (N)	1.11E+14	7.06E+19	1.28E+23
Password authentication			
Length (l)	7	10	12
Combinations (N)	6.98E+13	5.99E+19	5.40E+23

Tab. 1. Comparison between IBA, and password authentication. For increasing input stages, the password length (number of characters) is determined in order to obtain a number of possible combinations of the same order as the number of IBA possible combinations.

a password while, in IBA, the displayed image will help in recalling the pass-points.

Table 1 shows a comparison between IBA and password authentication. For example, if the IBA session is composed of two stages ($p = 2$), the number of possible input combinations (1E+14) is nearly equivalent to the possible combinations (6E+13) of a randomly generated password of seven characters.

The IBA system security is higher than password security:

- of course, password cracking techniques cannot be used with images;
- pass-points and images are not as easy to write down and share with other as it is for passwords;
- the IBA system requires more network resource; an exhaustive search by an attacker of the pass-points would require far more time than an exhaustive search of passwords, under the same number of possible combinations.

4. CONCLUSIONS

A framework for user authentication based on images (IBA) has been presented. For a user, it is easier to recognize images than remembering passwords. In the proposed method the user has to recognize pass-points on his personal images for being authenticated. The security level of the IBA system is higher than that of a common password authentication system. IBA takes full advantage of emerging image compression techniques (i.e. JPEG2000) in order to provide an efficient exchange of information between server and client.

5. REFERENCES

[1] A. Paivio, T. B. Rogers, and P. C. Smythe: "Why are pictures easier to recall than words?," *Psychonomic Science*, 11(4), pp. 137-138, 1968

[2] T. Taada, H. Koike, "Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images," *Proceedings on MobileHCI*, 2003

[3] W. Jansen, S. Gavrila, V. Korolev, R. Ayers, R. Swanstrom, "Picture Password: A Visual Login Technique for Mobile Devices," *National Institute of Standard and Technology,* NISTIR7030, July 2003

[4] T. Ebrahimi, "JPEG 2000 new activities and explorations," *ISO/IEC JTC 1/SC 29/WG1N3170*, December 2003

[5] Prandolini, S. Houchin, G. Colyer (JPIP Editors), "JPEG 2000 image coding system – Part 9: Interactivity tools, APIs and protocols – Final Committee Draft 2.0, *ISO/IEC JTC 1/SC 29/WG1N3174*," December 2003

[6] G. Blonder. Graphical passwords. *United States Patent 5559961*, 1996.

[7] I. Jermyn, A. Mayer, F. Monrose, M.K. Reiter, A. D. Rubin, "The Design and Analysis of Graphical Passwords," *Proceedings of the 8th USENIX Security Symposium*, August, Washington DC, 1999

[8] R. Dhamija, A. Perrig, "Deja Vu: A User Study Using Images for Authentication," *9th Usenix Security Symposium*, pp. 45–58, August 2000

[9] A.D.Angeli, M.Coutts, L.Coventry, G.I.Johnson, "VIP: a visual approach to user authentication," *Proceedings of the Working Conference on Advanced Visual Interface (AVI2002)*, pp. 316–323, May 2002

[10] A. Perrig, D. Song, "Hash Visualization: a New Technique to improve Real-World Security," *International Workshop on Cryptographic Techniques and Ecommerce (CrypTEC)*, 1999

[11] L. Sobrado, J-C Birgetm, "Graphical passwords," The Rutgers Scholar, *An Electronic Bulletin of Undergraduate Research*, Vol. 4, 2002