Gaze Pattern Lock for Elders and Disabled

Conference Paper · June 2012

DOI: 10.1007/978-3-642-31196-3_59

2 authors:

Tomasz Kocejko
Gdansk University of Technology
43 PUBLICATIONS **387** CITATIONS

SEE PROFILE

Jerzy Wtorek
Gdansk University of Technology
128 PUBLICATIONS **558** CITATIONS

SEE PROFILE

Gaze pattern lock for elders and disabled

Kocejko Tomasz, Wtorek Jerzy

Gdansk University of Technology, Biomedical Engineering Department,

Gdansk, Poland,

Abstract. The experiences with the eye tracker have highlighted new issues for further investigation and developing solution. On our ongoing research we are trying to combine two different biometric user authentication methods relying on gaze pattern recognition while face features matching. This article presents methodology of using the mobile eye tracking system for user authentication. The project is mostly aimed in to the elderly and disabled computer users and includes supporting authentication procedure that gives access to the classified data with gaze pattern lock. The experiment is to use the eye movement tracking system to collect the data while the eyes of the person who is being identified follow the point on the computer screen. Whole experiment relays on the Yarbus's experiment who showed that the viewers' eye movements differ according to the viewer's task. This article also presents a results of gaze pattern matching as the authentication procedure

1 Introduction

THERE are different methods of human identification which can be used for user authentication. Nowadays, all personal devices, including mobile phones, has got an user authentication protocols. Almost all computer systems involve an identity authentication process before user can access requested services such as: online transactions, entrance to a secured vault or logging into a computer system. One of the approaches is usage of a Personal Identification Number - PIN or a password which is a secrete-knowledge based technique. This technique offers a standard level of protection and provides cheap and quick authentication. However, according to the N.L. Clarke's and S.M. Furnell's work [1] the level of user authentication implemented on the devices should be extended beyond the Personal Identification Number, because password is never completely protected by the owner. Another approach is application of a biometric techniques, that means the users are identified by who they are, not by something they have to remember or carry with them. Biometric systems are gaining more interest due to the advantages of such systems over traditional authentication, to ensure that the rendered services are accessed only by legitimate users. Authoritatively authentication issues are nowadays very important. Every security administrator should consider selecting appropriate authentication protocols and authentication methods of users who may have access to sensitive data. The most popular biometric human identification and user authentication systems are those based on iris recognition [2][3], finger print matching [4] and hand veins recognition [5][6]. There are novel systems where authors try to use human's skill model for identification [7]. Although those methods give great results, required hardware is very expensive. Also non of mentioned methods was designed considering the disabled people, including this with serious movement disabilities.

In his work, P. Kasprowski proves that it is possible to identify the human on base of on his eye movements [8]. There are also works which showed how scan paths differs according to the users knowledge about the image [9].

Our research is the tryout of combining biometric methods of user authentication based on face recognition and gaze pattern matching. In the project the model based of face recognition was implemented. According to P. Mohanty, the goal of the modeling is to approximate the distances computed by a face recognition algorithm between two faces by distances between points, representing these faces, in an affine space. Given this space, templates from an independent image set (break-in) are matched only once with the enrolled template of the targeted subject and match scores are recorded. These scores are then used to embed the targeted subject in the approximating affine (nonorthogonal) space. Given the coordinates of the targeted subject in the affine space, the original template of the targeted subject is reconstructed using the inverse of the affine transformation [10]

However, methods presented in this paper refers to gaze pattern matching authentication method. Two different approaches are presented: feature-based approach, where user visual attention is investigated according to the feature of interest and approach relaying on gaze pattern matching (gaze pattern lock). Moreover article also shows the way of using mobile eye tracking system [11][12] as an input device in the authentication procedure. The whole project is dedicated to elderly and disabled users having problems with memorizing or entering the alpha-numeric passwords and contains first part of human authentication method based on face feature matching and gaze pattern recognition.

This paper is organized as follows. Authentication procedure and algorithms are presented in section II, section III shows experimental results. Discussion and conclusions are presented in section IV.

2 Method

Gaze pattern lock user authentication method relays on the constant tracking of user gaze and areas of interest. This level of interaction is possible due to eye tracking glasses recording fixation within region of interest [11]. Presented model of interface requires user to wear dedicated goggles for all the time of interaction. Information about pupil position and selected area of analysis are correlated. Authentication procedure relays on extracting fixations from particular image included in detected area. Computer verifies user according to his visual attention and information about what features were set as important for this significant user. This article presents two different methods of gaze pattern recognition, classification and gaze based authentication.

2.1 Feature-based approach

When viewers observe the environment, they do not perceive all its components as being equally interesting. Some objects automatically and effortlessly "pop out" from their surroundings, and naturally draw viewers visual attention. In every input image some particular features and locations will automatically and in-consciously attract viewers attention towards them [13]. The image properties can be described by following features: low-level ones, such as intensity, color, and texture, or high-level features that are related to certain anatomical structures like in medical images. In general, features can be divided into three categories: interval (the distance between features is known), ordinal (the order between features is known), and nominal (the distance and order between features are unknown).

According to this theory, if the viewer has not have any knowledge about particular image and he is watching it for the first time, it is highly probable that he will pay attention to some certain features and omit the others. However, if the viewer knows that the image contains feature that might draws his attention, he will try to find them avoiding other locations containing interest features. This fact was used in proposed authentication procedure. User is being authenticated by (partially) conscious attracting his visual attention on one (or more) previously established features. They can be extracted from the visual attention map or can be marked manually During the authentication procedure software is displaying 4 images to be watched be the user. Each image is presented for less than 5 seconds. Authentication depends of the knowledge about certain features and relies on comparison of visual attention distribution.

The course of action is presented in a following steps:

1. Image selection

2. Important features selection
3. Image observation
4. Visual data acquisition with mobile eye tracker
5. User verification by attention map comparison method

The prove of concept requires validation of the procedure according to the visual attention of the naive viewers.

The experiment was divided into different phases and involved 10 subjects. First phase relayed on checking how the people perceive different images. The set of pictures were presented to all subjects. Second phase relied on establishing subject's visual attention according to provided information about significant features (numbers or number-like looking signs). After introduction to the procedure the set of images was presented once again to the same group of people. For each phase and subject the visual attention map was created according to the recorded fixations.

To compare visual attention distribution from both phases, for every picture, a set of heat maps were computed. A heat map is a graphical representation of data where the values taken by a variable in a two-dimensional map are represented as colors. It is a useful tool for determination on what areas the viewer observes at and what areas he ignores. In this case the heat map was used for analyzing the viewers attention while watching the picture. The heat maps from first (unaware viewers) and second phase (viewers were informed about the important feature) were compared to establish potential difference in viewers visual attention.

If user marked important features manually software simply counted the number of fixations within selected region. The Authentication threshold was setup to 70 percent matches. Of course the threshold of correct fixation could be changed. If important features were represented by attention map generated during "features establishing" phase, similar map was calculated for the data gathered during authentication phase. To authenticate the user, both maps were compared. The comparison relayed on multiplication and subtraction of binary representation of both visual attention distributions. Authentication result corresponded to the numbers of black pixels left after subtraction procedure. Authentication was considered as passed when the result was less the 20% of all black pixels in multiplied image.

2.2 Gaze Pattern Matching

Mobile devices equipped with touch sensitive displays offer the authentication protocol based on touch pattern recognition (pattern lock). To authenticate himself, user touches the screen creating a unique pattern (e.g., up, down, etc.). Device compares created pattern to the one previously setup as a password. However, this solutions has got common disadvantage, the password (pattern) can be spotted by the third person. Also Pattern lock protection will not be the first choice of a person with movement disabilities.

With the assistance of eye-tracking technology, it is possible to map the exact scan paths of the subject's gaze, and consequently document the sequence of fixations. Scan path is the set of lines traced by the eye traveled across the image. Fixations, that are represented in the form of circles, jointed with lines creating the scan paths.

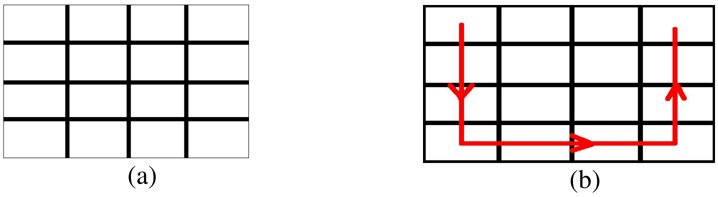
It is possible to use eye movements (certain order of fixation) to copy a pattern. The human's eye is able to move smoothly and continuously only when following the moving object. Otherwise, it skips from one point to another. This fast movements of an eye are called sacades. Because of the sacads it is impossible to copy sophisticated rounded shape patterns using eye movements. However, user can easily draw lines. In the proposed method predesigned pattern stands for the password. While authenticating, user is looking at the on-screen grid on which mapping the desired pattern. The acceptation relays on comparison of the similarity of the mapped pattern to the exemplary one. The procedure includes following steps:

1. Pattern setup
2. Pattern mapping by watching the grid
3. Visual data acquisition with mobile eye tracker
4. User verification

In our experiment the 16 fields on-screen board was used for making the pattern marking easier (typical pattern lock application contains 9 fields). Subject was asked to fixate his gaze on a desired locations on the presented grid. Unique gaze pattern was created be joining all registered fixations together. As a matter of fact drawing the pattern was rather choosing the fields in a certain order.

As the authentication relies on comparison of previously setup password with the input one, user had to define exemplary patterns: either by drawing them or, in a gaze mode, by looking on a grid in a specific order.

Two different methods of gaze pattern lock authentication were tested. First one relayed on verifying if recorded gaze pattern covers desired locations from 16 field board in particular order. Pictures below illustrates the procedure:


(a)

(b)

Figure 1: Procedure of gaze pattern setup. a) exemplary grid b) exemplary pattern to match be gaze

If the red line represents pattern drawn by the user, to pass the authentication procedure, the scan path and recorded fixations had to indicate to all the fields covered by the pattern as it is shown on pictures below:

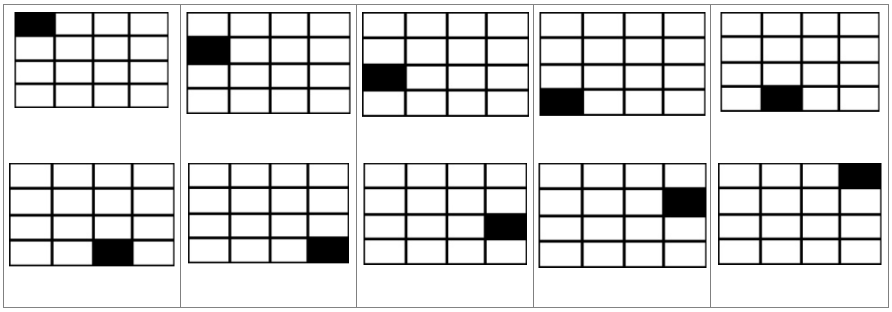


Figure 2: Sequences of gaze fixations located in particular gird fields in time

Figure 2 presents the order of user fixations occurrence during authentication procedure according to the desired pattern (fig. 1b.) to the desired pattern

Consequently, to pass the authentication procedure software had to detect fixation in each selected location in order. Time setup was an additional factor.

The second approach relied on presenting registered visual flow and exemplary pattern as time dependent 2D signal of positions in x/y axis. Then, the result of comparison of two signals corresponds to the level of similarity between recorded gaze patterns.

The comparison of the two digital signals (series of data) was made by calculating the deviation between corresponding samples. However, before the comparison, the number of samples had to be equalized by re-sampling shorter signal. To increase the number of samples their particular values were duplicated. As an estimation method of a degree to which two series (signal representations) are correlated, the cross correlation method was used.

$$r = \frac{\sum_i [\,(x(i) - mx) * (y(i-d) - my)\,]}{\sqrt{\sum_i (x(i) - mx)^2}\,\sqrt{\sum_i (y(i-d) - my)^2}}$$

The cross correlation r at delay d is defined as

Where mx and my are mean values of the corresponding series. If the above is computed for all delays d=0,1,2,...N-1 then it results in a cross correlation series of twice the length as the original series.

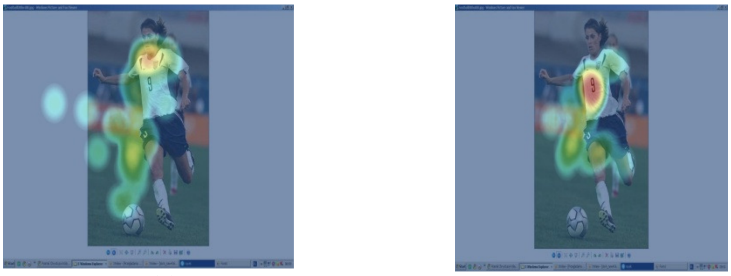
$$r(d) = \frac{\sum_i [\,(x(i) - mx) * (y(i-d) - my)\,]}{\sqrt{\sum_i (x(i) - mx)^2}\,\sqrt{\sum_i (y(i-d) - my)^2}}$$

Because the recorded data can have different length, both signals have to be normalized.

3 Results

3.1 Feature-based approach

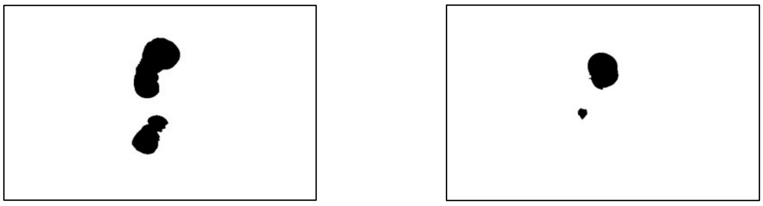
The experiment involved 10 different subjects of different age (from 25 to 80 years old) and gender. Before the introduction to the authentication procedure all subjects were asked to view the same set of images. It allowed to establish a way of perceiving the pictures by particular subject and attracting features. Then, users were asked to view the same pictures paying attention on the chosen feature.



(a)

(b)

Figure 3: Picture of football player with attention map marked (heatmap): a) attention map recorded for a naive 80 years old female viewer, b) attention map recorded for viewer informed to pay attention at numbers



(a)

(b)

Figure 4: Binary representation of heat maps a) naïve viewer, b) viewer attracted by the feature

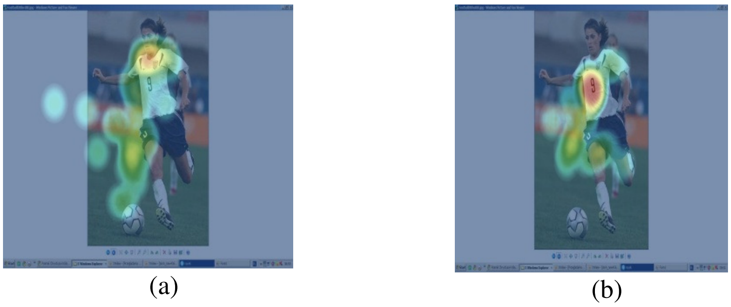


Figure 5: Picture of football player with attention map marked (heatmap): a) attention map recorded for a naive 80 years old female viewer, b) attention map recorded for viewer informed to pay attention at numbers

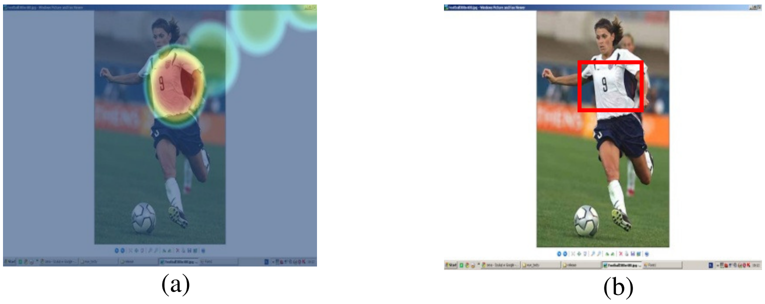


Figure 6:result of choosing the feature of interest a) by gaze, b) selecting by mouse

For every recorded visual attention map (represented as a heat map) its binary representation was generated.

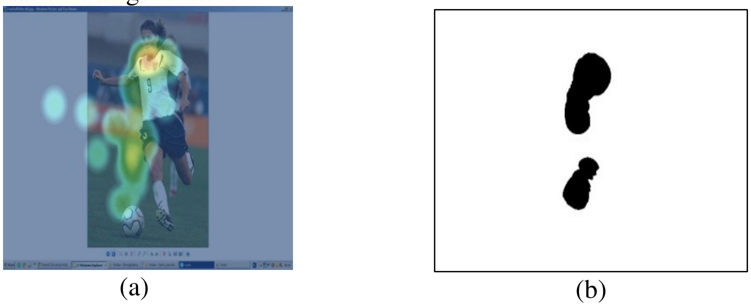
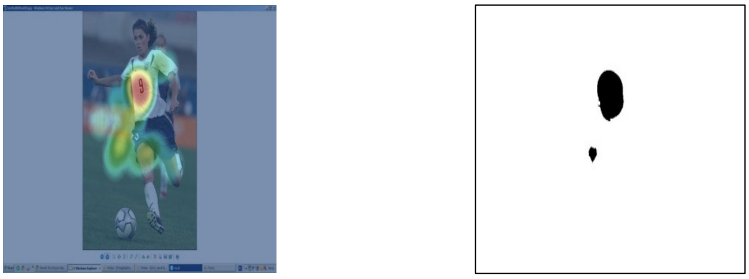


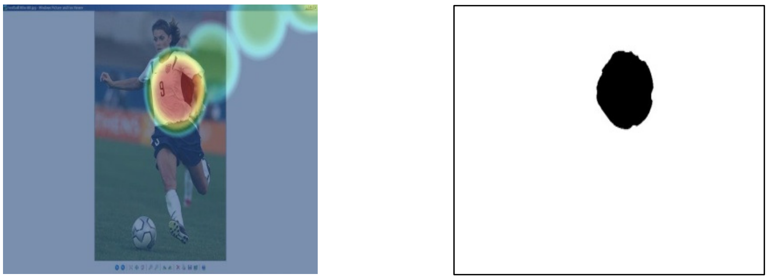
Figure 7:a) attention map recorded for a naive 80 years old female viewer, b) binary representation of recorded attention map



(a) (b)

Figure 8:a) attention map recorded for viewer informed to pay attention at numbers b) binary representation of recorded attention map

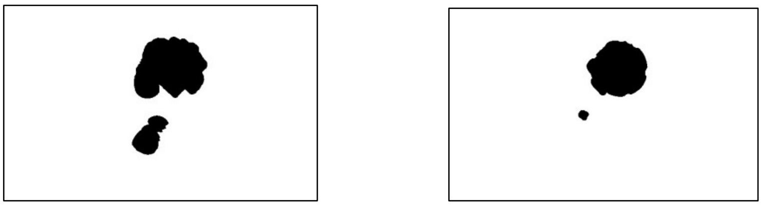
According to the way of establishing the feature of the interest different approaches of user verification were used.



(a) (b)

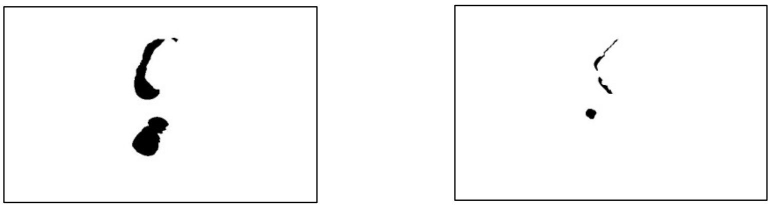
Figure 9:a) result of choosing the feature of interest by gaze, b) binary representation of recorded attention map

If user marked important features manually software simply counted how many fixations were within the selected region. If important features were established according to the visual attention, then verification procedure relayed on multiplying and subtracting binary representations of recorded heat maps.



(a) (b)

Figure 10: Results of binary representation of attention maps multiplication. a) unaware user b) for user knowing the feature of interest



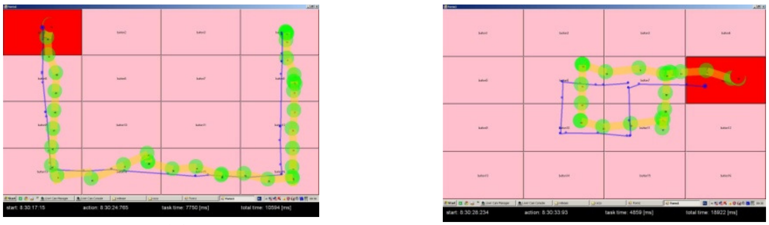
(a) (b)

Figure 11: Result of binary representation of attention maps subtraction a) unaware user b) aware user(informed about important feature)

The number of black pixels in resulting image (fig11b) was equal to 8% off all black pixels in the binary representation of exemplary heat map (fig9b). It means that user passed the authentication with 92%match. The number of black pixels in image presented on fig11a was equal to 96% of all black pixels of the exemplary binary representation of attention map. User did not pass the authentication procedure. Naive user obtained a 4% match.

3.2 Gaze pattern matching

Subject were asked to match desired pattern using gaze.



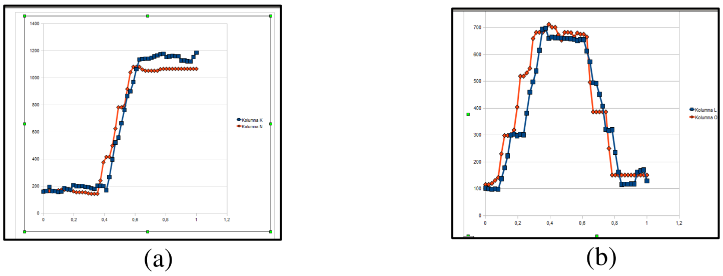
start: 8:30:17:15 action: 8:30:24:765 task time: 7750 [ms] total time: 10594 [ms]

start: 8:30:28:234 action: 8:30:33:93 task time: 4859 [ms] total time: 18922 [ms]

(a) (b)

Figure 12: Graphic representation of pattern matching. Blue line indicates to the pattern draw with computer mouse, yellow line with green dots represents the scan path recorded during pattern matching by gaze while authentication a) simple pattern b) complex pattern

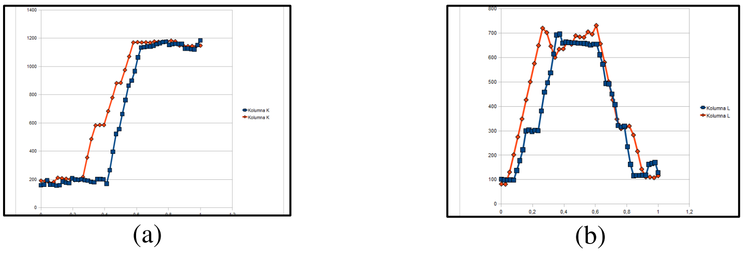
Recorded signal was also presented as a 2D signal and compared to the cursor root recorded as a pattern to be matched.



(a) (b)

Figure 13: Visual flow (blue line) and pattern design with computer mouse (red line) represented as a 2D signals. a) x coordinates representation, b) y coordinates representation

Signal representation of visual flow was also be used for comparison of the data recorded during authentication phase with this established as a desired pattern using gaze.

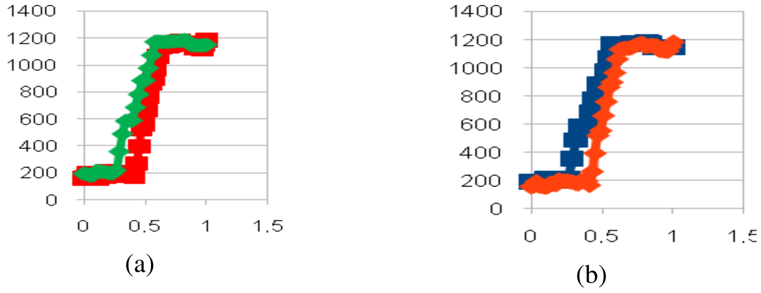


(a) (b)

Figure 14: Visual flow recorded during authentication phase (blue line) and pattern design with gaze (red line) represented as a 2D signals. a) x coordinates representation, b) y coordinates representation

Graphs presented on fig.13 and fig.14 proves that it is possible to use presented method for gaze patter matching. The results presented on fig. 14 shows that visual flows recorded during authentication phase and during pattern designing phase are corresponding to each other.

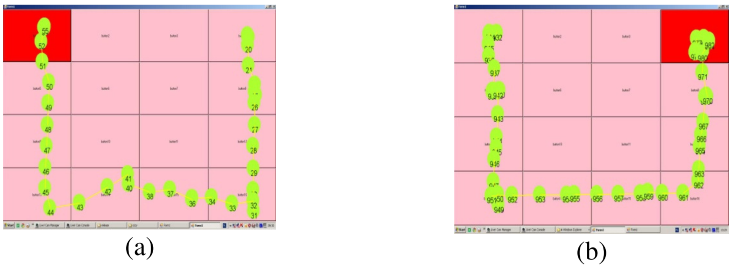
In order to compare two signals they were normalized according to time and the number of samples.



(a) (b)

Figure 15: Two 2D signals normalized on time scale: a) different number of samples b) with equalized number of samples

For signals presented on fig. 15 the cross correlation were computed. The result was 0,977 which means that signals are well correlated and that user matched the established pattern correctly.

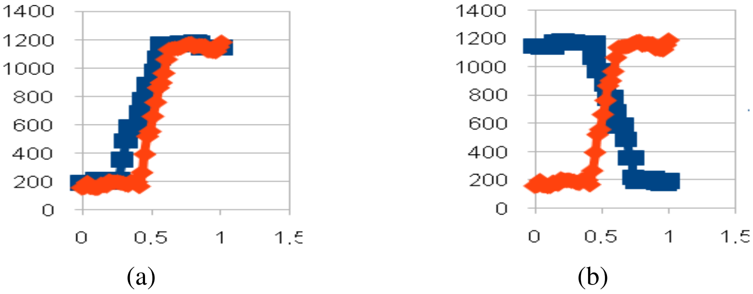


(a) (b)

Figure 16: Visual representation of recorded fixations a) for exemplary patter, b) for pattern recorded during authentication procedure

Patterns presented on fig. 16 have the same shape, however first one (fig 16a) was recorded in different order then one presented on fig. 16b.

Figure 17 shows the 2D signal representation for recorded fixations:



(a) (b)

Figure 17: 2D signal representation of exemplary pattern (red) and pattern recorded during authentication. a) Correlated signals b) Not correlated signals

The cross correlation computed for presented signals presented was equal 0,469.The result (representing the level of signals similarity) was to low to pass the authentication procedure.

4 Discussion and Conclusions

Presented solutions are a part of research under the human authentication method based on face feature tracking and gaze pattern recognition. Whole procedure involves user face recognition and fixation registration while watching the set of images. Ongoing research are focused on designing complementary interception methods enabling complex communication with computer unit limited number of interface. That is why, in presented research, goggles designed for hands free communication [11][12] were used.

In the experiment, the image exposure time was setup for 5 seconds, however in further experiments the time will be gradually decreased. The assumption is that whole procedure (face and gaze pattern recognition) took 4-5seconds.

The method of user authentication by gaze is mostly directed to elderly and disabled people. The main assumption was that it is easier to remember particular features and locate them in a set of images then to remember complicated password. The eye tracker used in the experiment was design to enable communication between computer and disabled person. In this experiment showed that it is possible to use designed eye tracking goggles in different application. Presented methods can increase the level of data protection. Gaze based authentication can be set as complementary part of to traditionally methods.

Proposed method depends on using mobile eye tracker to record and compare visual attention maps. User has to pay attention to desired, previously established features on set of 4 different images. The used eye tracking device was setup to extract fixations from 1 of 25 fields.. It means that if user has to locate only one desired feature from 25 locations in 4 different images, the probability of accidental authentication is 1/390625. The accidental authentication using 4 digit PIN is 1/10000. Time of watching every image was established to 5 seconds, which means that user have to spend 20 seconds on authenticating himself. However, the time of watching the single picture can be decreased. All users that were involved in the experiment passed the authentication procedure.

The great advantage of gaze based authentication approach is that it is impossible to copy or steal the “password” by looking directly at user's eye as without the dedicated hardware it is extremely difficult to determine at what region of picture one is looking at and it is hardly possible to guess the desired feature. Both techniques, feature-based and pattern matching one, gives promising results. The disadvantage of these methods is that they need external hardware. However, we assume that soon similar technique can be used on mobile devices equipped with build-in cameras or interacting with eye trackers built in traditional glasses (or sunglasses). Proposed technique can help elderly and disabled computer users. Memorizing one particular feature in the image is easier then memorizing complicated alphanumeric password and it gives similar level of security.

Acknowledgment

Acknowledgment (if any) should appear as a separate non-numbered section before the list of references. Use the singular heading even if you have many acknowledgments.

References

[1] Clarke N.L., Furnell S.M.: Authentication of users on mobile telephones – A survey of attitudes and practices, Computers & Security, October 2005, Vol.24, pp. 519-527

[2] Miyazawa K., Ito K., Aoki T., Kobayashi K., Katsumata A.: An Iris Recognition System Using Phase-Based Image Matching, IEEE International Conference on Image Processing, 2006, 8-11 Oct. 2006, pp. 325-328, Atlanta, GA

[3] Jen-Chun Lee, Ping S. Huang Chung-Shi Chiang, Tu, T.-M. Chien-Ping Chang: An Empirical Mode Decomposition Approach for Iris Recognition, IEEE International Conference on Image Processing, 2006, 8-11 Oct. 2006, pp. 289-292, Atlanta, GA

[4] Fons M., Fons F., Canto E., Lopez M.: Design of a Hardware Accelerator for Fingerprint Alignment, International Conference on Field Programmable Logic and Applications, 2007. 27-29 Aug. 2007 pp. 485 – 488, Amsterdam, Netherlands

[5] Wang L., Leedham C.G.: A thermal hand vein pattern verification system. Proceedings of International on Advances in Pattern Recognition, pp. 58-65, Springer, Bath, UK

[6] Kumar A., Prathyusha K.V.: Personal authentication using hand vein triangulation. Proceedings of the SPIE, Biometric technology for Human Identification V, pp. 69440E-69440-13

[7] Shangchang Ma, Tadanao Zanma, Muneaki Ishida: Human Identification Based on Human Skill Models, WRI Global Congress on Intelligent Systems, 2009. GCIS '09, 19-21 May 2009, pp. 273-277, Xiamen

[8] Kasprowski P, Ober J: With the flick of an eye, Biometric Technology Today Vol. 12, March 2004, pp. 7-8

[9] Dempere-Marco L., Hu X-P., Ellis S. M., Hansell D. M., Yang G-Z.: Analysis of Visual Search Patterns with EMD Metric in Normalized Anatomical Space, IEEE Transactions on Medical Imaging, pp. 1011-1021

[10] Mohanty P., Sarkar S., Kasturi R.: From Scores to Face Templates: A Model-BasedApproach, IEEE Transactions on Pattern Analysis and Machine Intelligence, 2007 , pp. 2065 - 2078

[11] Kocejko T., Bujnowski A., Wtorek J.: Eye Mouse For Disabled, IEEE Conference on human System Interactions, 2008, 25-27 May 2008, pp. 199 – 202, Krakow, Poland

[12] Kocejko T., Bujnowski A., Wtorek J.: Eye Mouse For Disabled, Advances in Soft Computing, Human-Computer Systems Interaction, pp. 109-122, Springer Berlin

[13] Itti L., Models of bottom-up and top-down visual attention, Dissertation (Ph.D.), California Institute of Technology 2000