International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 10 | Oct -2016 www.irjet.net p-ISSN: 2395-0072

Efficient Database Search Facilitating Eye Movement Biometric Identification in Banking System

Harish Yadav[1], Kumkum Yadav[2]

[1]Envestnet|Yodlee, Karnataka, India
[2]Deloitte Consulting US India Pvt. Ltd., Karnataka, India

Abstract - *- The evolution of authentication system has shed light on the utility of biometrics as the basis of identification. Due to reliability and security biometric authentication is eliminating the conventional authentication methods. Nevertheless, there are loopholes and gaps in different available biometrics like fingerprint, voice, and face but eye movement provides a promising technique as it is based on brain activity and extraocular muscle properties which cannot be imitated [2]. So eye movement can be used as a universal mode of authentication in the banking system. But in order to implement it practically for a huge population, the complete authentication process should occur at a fast pace. The data retrieval from a biometric database would play a key role in expediting the process. In this paper we are proposing a way to use eye movement as a feasible way of authentication for a large population which when combined with the efficient search algorithm can dramatically increase the acceptance of this system for authentication.*

Key Words: Eye Movement, Fixation, Saccade, Binning.

1. INTRODUCTION

Widespread implementation of Biometric authentication will soon eliminate the conventional authentication methods since the conventional methods like static passwords are excessively vulnerable. But as the technology advances, it is easier to reproduce biometric traits and bypass the authentication process by exploiting the loopholes in most of the biometric authentication [1]. Eye movement provides a unique way of biometric authentication as they are highly counterfeit resistant because brain activity and extraocular muscle properties of an individual are distinctive factors that form the basis of eye movement authentication. Consequently, it is not possible to accurately replicate the eye movements outside of a living human [2]. There are other important aspects which make eye movement as the unparalleled biometric authentication system -

1.1 Hard to spoof

Eye movement reflexes by their very nature are beyond conscious control, so could not be spoofed even if the attacker were to use sophisticated materials, equipment, or even surgery. [3]

1.2 Practical and Easy to implement in the real world

Eye movement signals are more practical than any other biosignal due to simpler signal capture methods. Small camera or electrodes in a glass shaped device can be utilized to capture signal by simply wearing as spectacles [4].

As we have already proposed the benefits of using eye movement biometrics over other, we would now like to focus on the practical implementation of eye movement biometric in the banking system. A little investigation has been conducted for real world implementation of eye movement as a biometric identification method. In order to implement it in banking system, we would require to maintain a humongous biometric database which would store a template of eye movement data for each individual. Search and retrieval of the template would play a crucial role for the feasibility of such system.

2. BACKGROUND

The eye movement can be measured in terms of fixations and saccades. When the eye is held in a relatively stable position which in turn allows heightened visual activity on a particular subject the fixations gets generated. When eye rotates between any two fixation points quickly with the speed as high as 700 degrees/s such that no visual acuity is maintained during rotation then saccades occur [7].

3. INTERFACES AND TECHNIQUES FOR CAPTURING EYE MOVEMENT

The acceptability of any authentication method depends on the ease of use. Appropriate interfaces for capturing eye movement input play a major role for widespread acceptability of eye movement as method of authentication. Below are some of the interface variations that can be deployed –

1.1 Targeting variant

In this variant user has to gaze at the highlighted circle. The circles would be in a grid of 3 X 3 matrix. A small "plus" icon would be present at the center of the circle that can help the user to center his/her gaze. Only one circle would be highlighted and rest of the circle would be shaded. To follow the user's gaze a small red dot is used. The circle will start to fade green as soon as the red dot enters the highlighted circle and the white border of the circle will thicken slightly. The button flashes white, and fades, having been activated after 0.5 seconds. Next, some other random circle will get highlighted, and the process continues until all the circles are highlighted once (see Figure 1) [5].

Fig -1: Targeting variant interface [5]

1.2 Reading Variant

In this variant, the user is required to read a selection of text. The selected text should be difficult which would require the reader to read carefully [5]. For example, the displayed text can be selected from Lewis Carroll's "The Hunting of the Snark" due to its difficult and nonsensical text [8].

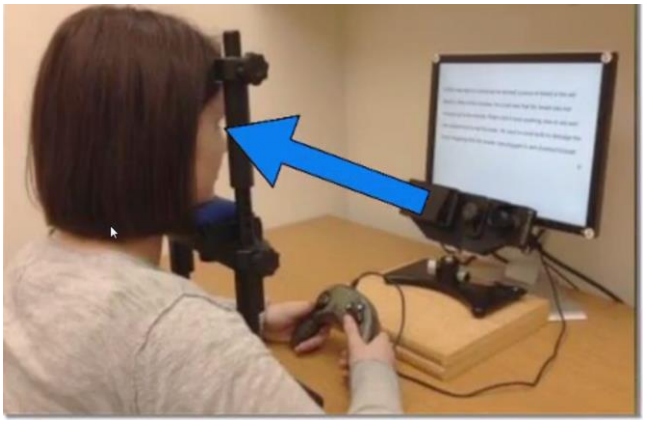

Fig -2: Eye positioning [7]

Capture of eye movement for storage in database [6] –

1) Positioning of the eye tracking equipment which consists infrared light source and video camera so that the eye is clearly visible when the subject looks at the display monitor (see Figure 2).
2) The software is calibrated to appropriately record the movements of the eye (see Figure 3).
3) The passage is displayed to be read (see Figure 5).
4) Storing the eye movement data in the form of duration of fixation of words and saccades in the passage (see Figure 6).

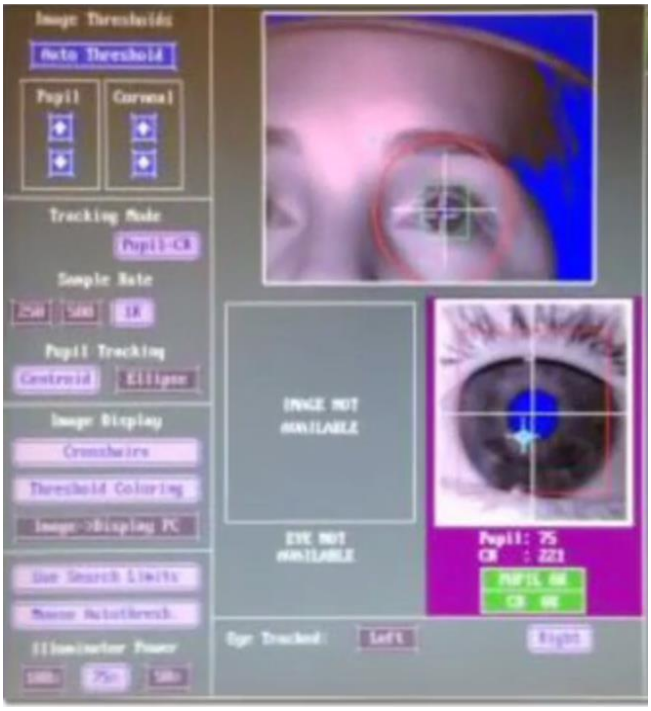

Fig -3: Software calibration [7]

4. EFFECTIVE SEARCH ALGORITHM – BINNING AND PRUNING [9]

Binning and pruning approach executes the exhaustive search after a coarse level classification is done. Using k-means clustering algorithm the database is clustered or partitioned into several bins. A certain partition of the database is assigned to the query template and all the templates within the partition are considered as the potential match for final identification. The search will greatly depend on the shortlisted bins which qualify to be searched for an actual match. The C closest bins are searched to avoid the failure to select the bin in which actual match lies. The value of C is highly influenced by the penetration rate of the system and hence it is application dependent.

The search space can be reduced by partitioning the database into several bins. Once the binning is completed, partitioning is performed on the biometric database in such a

way that each bin has templates which are similar and correspond to some statistical or natural class. The vector representation of a biometric template Xi can be represented as [x1,x2,x3,……..,xk]. The critical task in binning is to classify from a database constituting a vector space S. In this classification the N vector templates of database are segregated into M distinct classes {Y1,Y2,……,Ym}, such that -

$$\sum_{i=1}^{m} y_i = S \text{ and } y_i \cap y_j = \phi, \forall\, i \neq j$$

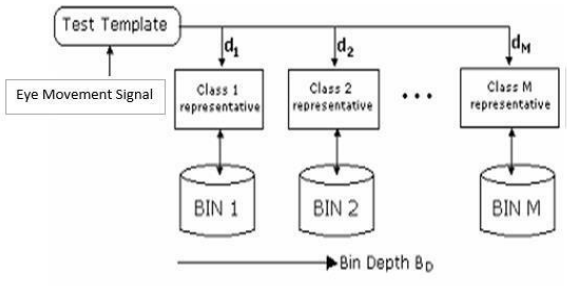

Fig -4: Testing of test template with the class representative. [9]

Time complexity of binning search –

The time consumed in a traditional search which involves a 1: N comparisons for a particular identification depends on the distance of test template and the N templates in the database. Therefore, the time spent in this type of search can be defined as - O(N). On the contrary, the binning method eliminates the futile comparisons resulting from the bins which do not qualify as the C closest bins i.e. (M-C) bins are rejected at the beginning of search itself. So, the bins where the probable match for test template lies can be found as C closest bins to proceed for the search. The C closest bins can be found by calculating the distance of the test template from the centers of all the bins. The utmost number of comparisons required for extracting C closest bins are C x M and this can be attained by a single scan. The time complexity of finding out C closest bins and completing the whole identification task can be deduced as-

O(C x M) – Time complexity of finding C closest bins O(C x M) + C x O(AM) – Time complexity of complete identification process.

Where AM = N/M (Average bin density).

Since N is the total number of vector templates which are classified into M bins among them C bins qualify for search so we can have the relation as C < M << N, also it is known that AM < N. Hence it can be inferred that the time complexity of the final task through binning approach is way lesser than the conventional time complexity, below inequality states the mathematical relation: -

$$O(C \times M) + C \times O(AM) < O(N) \qquad (1)$$

It can be noted that in relation (1) the distribution among the bins is considered as uniform. Nevertheless, if the distribution is skewed within the bins then also the time complexity of binning approach remains lesser than the conventional approach. In skewed distribution, the term C x O(AM) can be replaced by Psys x N where Psys is the penetration factor or in other words it is the fraction to

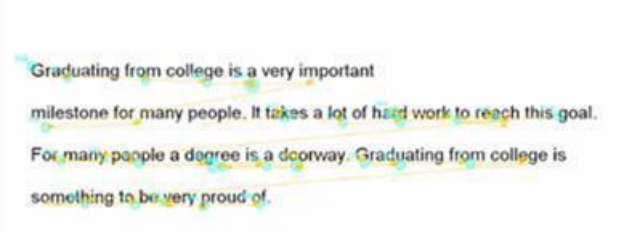

Fig -5: Fixation (colored dots) and saccades (line joining two dots) while reading the passage [7].

which the search space has been reduced through binning. Thus Psys x N < N which still yields the final time complexity lesser than O(N).

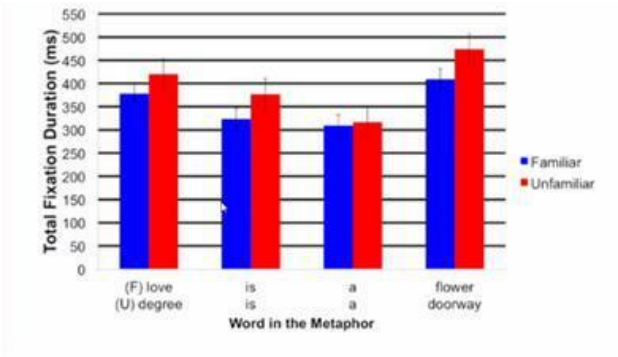

Fig -6: Fixation duration versus familiarity graph [7]

5. USE OF EYE DATABASE IN BANKING SYSTEM HARNESSING BINNING AND PRUNING ALGORITHM

The implementation can be performed for authentication purpose in banks or any public devices such as automatic teller machine (ATM). The authentication method should be easy to use for everyone. Our proposed method presents a platform for all the individuals with varying education level. Also, people suffering from the disease like dyslexia can choose the proposed targeting variant of interface for authentication. For this approach to work, banks are required to collect the samples of eye movement data of all the customers and save them in the database. Once the database is ready then binning can be performed by partitioning the database. To perform authentication at the ATMs the

customer needs to set the head in front of the eye tracking equipment site and the system captures eye movement data when the customer performs the targeting/reading activity. Then Fixation and saccade information is extracted from the captured data which gets processed to generate the template in the form of a vector for matching. After the eye movement data is captured the customer is also asked to enter the CIN (Customer Identification Number). Both the eye movement data template and CIN number are used for comparisons from the existing CIN number and sample eye movement data in bank's database through the intranet. The verification server performs the comparisons of information extracted from the input signal at ATM with the retrieved template from the database at the bank. If input signal matches successfully then the access is provided to the user otherwise access is denied (See Figure 7).

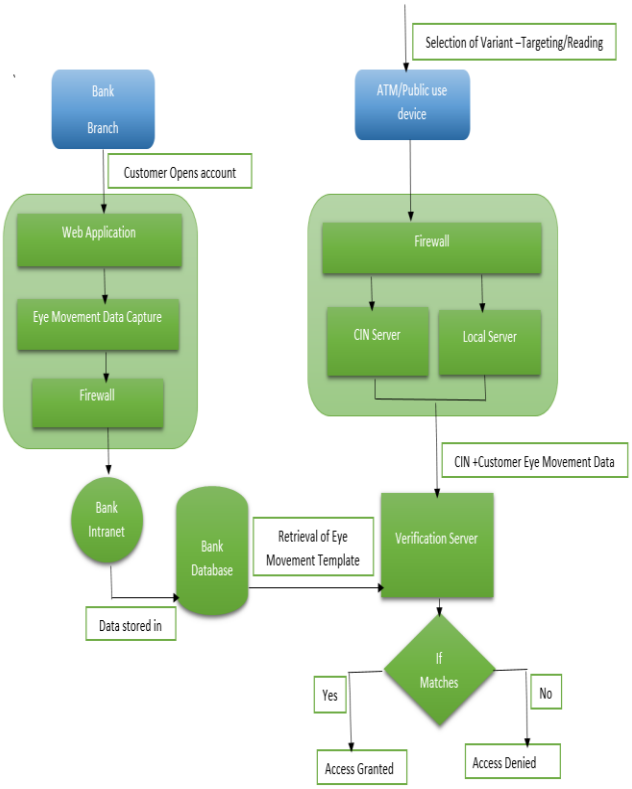

Fig -6: Eye Movement Authentication System in banking

5. CONCLUSIONS

As per our knowledge research for eye movement as a biometric is in incipient stage and there is still a wide scope that needs to be explored. In this paper, we have proposed a way to use eye movement equipped with effective search algorithm for authentication purpose. Many types of research are going on in this field and in future we will extend and focus on below aspects –

1) For more dependable search we can use multiple biometric measures to broadly identify the potential matches and the final authentication can be performed by eye movement biometrics.
2) To apply eye movement biometrics for personal use which will provide users an ease to use personal devices like mobiles, laptops at their home for authentication.
3) We will also extend our research so that other security systems can utilize this approach as well.
4) We will work on making the system robust for efficient fault tolerance.

REFERENCES

[1] C. Roberts, "Biometric attack vectors and defences," Computers & Security. vol. 26, pp. 14-25,2007.

[2] Corey Holland, Oleg V. Komogortsev "Biometric Identification via Eye Movement Scan paths in Reading" presented at the IEEE International Joint Conference on IEEE Biometrics Compendium. pp 1-8, 2011

[3] Inderscience Publishers. "Eyeball Reflexes: Security and Biometrics That Cannot Be Spoofed." ScienceDaily. ScienceDaily, 4 September 2008.

[4] Nastaran Maus Esfahani "A Brief Review of Human Identification Using Eye Movement" JPPR Vol 11, No 1 (2016); doi:10.13176/11.705

[5] Michael Brooks1, Cecilia R. Aragon, and Oleg V. Komogortsev "Perceptions of Interfaces for Eye Movement Biometrics" presented at the IEEE International Conference on Biometrics. pp 1-8, 2013

[6] Gary E. Raney, Spencer J. Campbell, Joanna C. Bovee , Department of Psychology, University of Illinois at Chicago , "Using Eye Movements to Evaluate the Cognitive Processes Involved in Text Comprehension" . J. Vis. Exp. (83), e50780, doi:10.3791/50780 (2014).

[7] R.1. Leigh and D. S. Zee, The Neurology oj Eye Movements, 4 ed.:Oxford University Press, USA, 2006.

[8] C. Holland and O. V Komogortsev, "Biometric identification via eye movement scanpaths in reading" in Proc. IJCB 2011, 2011.

[9] Amit Mhatre, Srinivas Palla, Sharat Chikkerur and Venu Govindaraju "Efficient Search and Retrieval in Biometric Databases" presented at Proceedings of SPIE – The International Society for Optical Engineering in March 2005.

[10] Michael Brooks, University of Washington, "Eye – tracking could outshine password if made user – friendly" published on July 16, 2013.