VISUAL EVOKED POTENTIALS IN BIOMETRIC AUTHENTICATION

Kamil Malinka
Doctoral Degree Programme (5), FIT BUT
E-mail: malinka@fit.vutbr.cz

Supervised by: Petr Hanáček
E-mail: hanacek@fit.vutbr.cz

ABSTRACT

This article deals with behavioural patterns and their impact on computer security namely biometric authentication. We propose an analysis of challenge-response approach usability together with an appropriate candidate for such an approach - visual evoked potentials (VEP). Their recognition capabilities are presented. We design and implement methods covering all phases necessary for processing VEP as a biometric characteristic and perform them on a test database. The efficiency of our approach is presented in an appropriate way.

1 ÚVOD

The main area of our interest is the biometric authentication. Like other security measures, biometric authentication is also exposed to various types of attack. From the definition, biometric authentication faces a few basic areas of the problems: treshold (biometrics by definition are forced to accept some inaccuracies.), counterfeit detection (the detection of counterfeits and effective prevention of their misuse is one of the classic problems of the current biometric authentication) and low flexibility (It is not possible to change your biometric characteristic or even to increase the number of your characteristics (a human has usually at most 10 fingers), thus corruption of systems with low levels of security could help an attacker to gain access to systems with a higher level of security.). Problems such as securing of communication, quality of sensors, query process speed or statistical properties are out of focus of this paper.

In the next part, we propose our own solution to some of the mentioned problems. We want to take advantage of the properties of unconditional reflexes.

2 A PROPOSAL OF MECHANISM OF CHALLENGE-RESPONSE BIOMETRIC AUTHENTICATION BASED ON UNCONDITIONAL REFLEXES

A challeng-response biometric authentication has special requirements and it is unclear which characteristic is suitable. The problem is that people are able to some degree learn how to control their behaviour and then attack systems based on behaviour. Signature dynamics can serve as an example. It is possible to learn signature dynamics of other people as well as the style of writing on a keyboard. A different situation arises if we attempt to use the unconditional reflexes.

The use of unconditional reflexes opens the possibility to think about a biometric system based on the challenge-response approach. The system will generate stimulation, which will serve as a challenge, and the user will react in relation. We could gain high robustness while using a biometric based on some appropriate unconditional reflex. The first huge benefit of this method is the impossibility of reaction control. This makes it harder to misuse this biometric, particularly for two reasons: unawareness of the challenge and problematic theft of reactions on this stimulus.

For proving our concept we propose, from our point of view, a suitable reflex - visual evoked potentials (VEP). It is a bioelectrical response of the brain to excitation of the optical receptor by a defined stimulus. At present these reflexes are used in medicine (ophthalmology) where they serve to reveal diseases such a multiple sclerosis. Detailed description of VEP can be found in our previous work [3]. As signal recording from the brain is rather complicated, biometrics based on brain signals has not been studied extensively though it is one of the most fraud-resistant biometrics.

We realize an experiment that simulates all the steps required by processing the VEP as a biometric characteristic - sample acquisition, sample preprocessing and feature extraction, the decision-making phase and finally the evaluation of the effectivness of our methods.

3 EVALUATION OF FLASH VEP USABILITY AS BEHAVIOURAL CHARACTERISTICS FOR BIOMETRIC AUTHENTICATION

In this section, we present the results of our experiment dealing with the usability of the flash VEP for user authentication. The primary goal of the experiment is to verify the properties of flash VEP and secondary to create the methodology for measuring and further processing of VEP as a biometric. As a feature we want to take advantage of the averaged representative waveform of the response. Thus, during the preprocessing of data, this average is done.

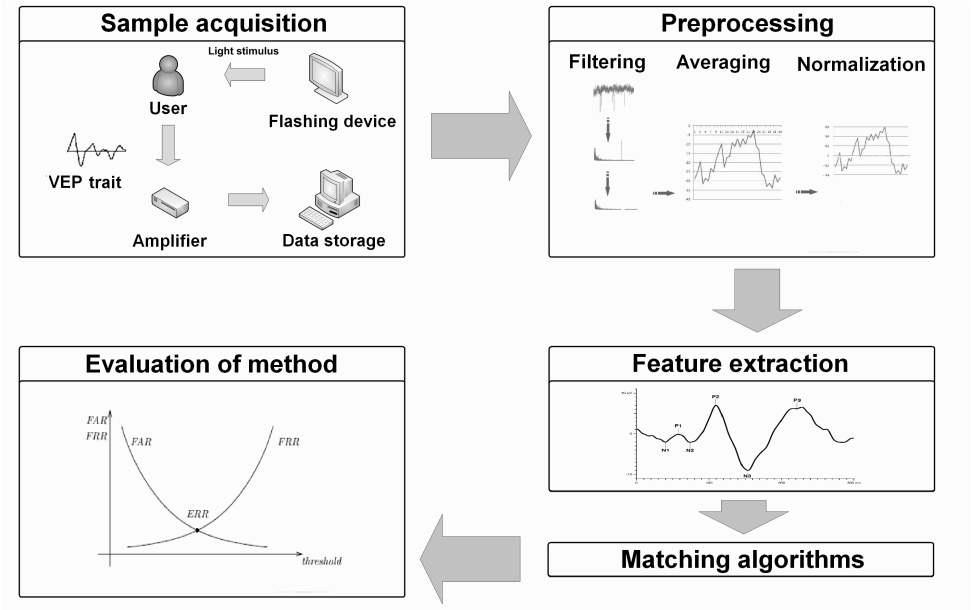
To prove that VEP evoked by flash stimulus is suitable for the biometric authentication, it is necessary to proceed as for the other biometrics. There are consecutive steps as visualized in Figure 1.

Firstly, it is necessary to acquire enough data. This was done by using fully equipped the EEG measuring device Alien. Sixty-five subjects were repeteadly examined based on recommended clinical protocol and responses to the flash stimulus were acquired. The next step is a preprocessing of EEG signals. We have reduced the baseline noise by the application of a high-pass filter on the EEG signals. Further we have averaged single responses to eliminate the noise. The last step is the normalization of the signal by removing the DC component, the result is a requested biometric characteristic prepared for the matching algorithm. After the creation of the sample database, we proceed to designing the convenient matching method.

Our feature is a curve represented by discrete values, which can be considered as a vector. Thus, we take advantage of methods used also for voice recognition, power analysis of smartcards, etc.

3.1 RESULTS

We perform the first type of evaluation - technology evaluation. It is an offline evaluation of one or more algorithms for the same biometric modality using specially-collected samples. These



Obrázek 1: Individual phases of processing VEP as a biometric.

results were acquired in accordance with standard ISO/IEC 19795 [2].

We are interesting in both methods used in biometric authentication - verification and identification. For the reporting of performance results, we use recommended metrics such as a false-positive identification error rate or a corresponding false-negative identification-error rate together with detection error trade-off (DET) curves corresponding to a test database for verification.

For analysis of an impostor transaction, we used an offline generation of these transactions. We performed a full cross-comparison, in which each sample feature is compared with every non-self template. This approach generates many more impostor attempts than could be achieved in other ways. As a template, we use two other measurements of a subject during identification and one measurement during verification.

Frequency (Hz)	Euclidean distance	Normalized cross-correlation	Horizontal histogram
1	11%	15%	0%
2	35%	35%	7%
3	48%	43%	14%
4	51%	45%	21%
5	59%	60%	40%
6	63%	62%	0%
7	65%	62%	37%
8	40%	41%	34%

Tabulka 1: Comparison of different methods efficiency. Test crew contains 65 persons.

Firstly, we want to prove that it is possible to identify a certain sample of VEP in a bigger set (identification). We have applied three basic algorithms (Euclidean distance, normalized cross-

correlation and a method using horizontal histogram.) on a test dataset containing 65 samples to determine the most appropriate matching algorithm. Results of this comparison are in Table 1.

We have counted distances of every sample to the rest and sorted them. As a success, we consider the appearance of one of the rest samples from the same person in the first position of the sorted list - the sample with the lowest distance. This approach represents the case when a candidate list of length 1 is used. From three selected candidates only two methods - Euclidean distance and normalized cross-correlation appear as suitable methods for the identification. Due to slightly better numbers, we choose the Euclidean distance as the most appropriate for further analyses. After choosing a suitable matching algorithm, we have conducted more analysis.

Frequency	**Candidate list length**				
(Hz)	1	2	3	4	5
1	11%	16%	19%	22%	24%
2	35%	46%	52%	57%	61%
3	48%	56%	63%	68%	72%
4	51%	57%	66%	75%	77%
5	59%	68%	79%	80%	83%
6	63%	75%	80%	84%	88%
7	65%	75%	80%	85%	87%
8	40%	58%	66%	70%	72%

Tabulka 2: Successfulness of identification with Euclidean distance used as matching algorithm. Test crew contains 65 persons.

We modify the selected algorithm (Euclidean distance) to use an expanded candidate list and apply it to the full test dataset containing 65 samples. Results of this expansion are in Table 2.

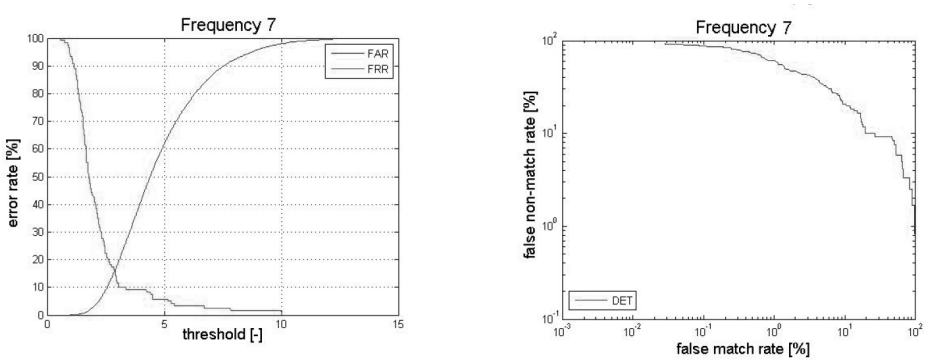
We can see that expansion of the candidate list by a few more candidates considerably improved recognition capabilities. Here we definitely prove that VEP is fully suitable for the biometric recognition, despite the fact that numbers are not as persuasive as expected.

The next step in our experiment is the analysis of the suitability of our characteristic for user verification, where we use Euklidean distance (due to best results in identification) for sample matching. We use a part of our data set to create templates - data from one measurement of each person was used as a template. The rest of the data set was used as a live sample. This was performed in all possible permutations to obtain as much data as possible. See resulting FRR - FAR diagrams and detection error trade-off curves (DET) obtained by using Euklidean distance for frequency 7 Hz on Figure 2.

The best results were obtained via stimulus with the frequencies 6 and 7 Hz, despite the lower range of values describing the characteristic curve provided by these frequencies and smaller amount of flash cycles in comparison with lower frequencies.

4 CONCLUSION

This work is devoted to the use of behavioural patterns in identification and authentication. The main contribution here is the idea of using unconditional reflexes for biometric authentication. This approach could take benefits of properties that provide unconditional reflexes. A suitable



Obrázek 2: Verification: FAR - FRR diagrams and detection error trade-off (DET) curves for frequency 7 Hz and various treshold. Used algorithm: Euclidean distance.

application could solve the problem of a narrow range of biometrics in a way of implementing a challenge-response system, which should be difficult to counterfeit. As a suitable candidate, we propose visual evoked potentials [1].

Suitability of VEP was verified by a set of experiments with very promising results. Due to the extent of testing a database consisting of VEP samples from 65 volunteers, we were able to design and implement methods covering the whole process of treating VEP as a biometric. We specify devices needed for apropriate sample acquisition. We design methods for the samples preprocessing and feature extraction, where we use information about methods for signal processing. We propose suitable matching algorithms such as Euklidean distance together with results of their implementation on our dataset. We were able to get a successfulness of around 88% for user identification using a candidate list of the length 5 and ERR around 15% for user verification.

We proved that our approach can be compared to other approaches of biometric authentication based on some behavioural characteristic.

ACKNOWLEDGEMENTS

This work was partially supported by the BUT FIT grant FIT-10-S-1 and the research plan MSM0021630528.

REFERENCE

[1] Malinka K.: Usability of Visual Evoked Potentials as Behavioral Characteristics for Biometric Authentication, In:The Fourth International Conference on Internet Monitoring and Protection, Venice, Italy, IEEE CS, 2009, ISBN: 978-0-7695-3612-5

[2] ISO: Information technology - biometric performance and reporting - part 1: Principles and framework, iso/iec 19795-1:2006(e).

[3] J. Vernon Odom, Michael Bach, Colin Barber, Mitchell Brigell, Michael F. Marmor, Alma Patrizia Tormene, Graham E. Holder, and Vaegan. Visual evoked potentials standard. Documenta Ophthalmologica, 115-123:1694, 2004.