A framework for Authentication using Fingerprint and Electroencephalogram as Biometrics Modalities

Tegpreet Kaur Neela¹ and Dr. Karanjeet Singh Kahlon²

Department of Computer Science and Engineering
Guru Nanak Dev University- Amritsar, Punjab (India)

Abstract— In today’s scenario security is becoming a crucial concern due to increased number of frauds, theft and hooligans. This paper proposes a multimodal biometrics system by combining two unimodal modalities that is fingerprint and EEG. Fingerprint unimodal Systems can be spoofed using artificial fingers and fingerprints made from readily available materials (e.g. gelatine, silicon) or even cadaver fingers (finger of dead person). Proposed system eliminates the disadvantages of the fingerprint recognition system as only living persons have EEG and it varies from person to person. So, combining fingerprint and EEG modalities make system more secure, robust and hard to spoof.

Keywords— Biometrics, Unimodal, Multimodal, Fingerprint, EEG.

I. INTRODUCTION
Traditionally, the identification of an individual or the verification of an individual’s claimed identity involved the use of a password, personal identification number (PIN) or cryptographic key. [1] There are a number of problems associated with these security measures. Now a day’s biometric authentication is done.

Biometric is any measurable, physical or physiological feature or behaviour trait that can be used to identify an individual or to verify the claimed identity of an individual.[2] Physiological biometrics include fingerprints, hand geometry[3], the face, the iris, the retina, the venous networks of the hand and even body odour. Behavioural biometrics includes voice, keystroke dynamics and gait [4].

A number of other modalities are current being investigated as potential biometric identifiers. For example, research has indicated that an individual’s baseline brainwave pattern from electroencephalogram (EEG) recordings is distinctive enough to be used as a means of biometric recognition. Few more are ECG[23], Footprint Recognition and geometric shape and physiological structure of the tongue.

Take an example if as person break/cut the finger of other person in that case the systems will lose the security and also artificial finger and fingerprints made from readily available materials (e.g. gelatine, silicon) easily spoof the fingerprint system. Meanwhile, EEG is hard to reproduce under coercion. It is ideal for liveness detection and difficult to spoof. [5]

III. LITERATURE SURVEY
The earlier work in the fingerprint recognition was done by Moayer [24],[25]. He considered fingerprint as a 1-D character string and another method considering fingerprint as 2-D tree and verifying two fingerprints by grammar matching. These methods worked for a rough classification but failed on low quality images and thus, were not suitable for an identification system.

Minutiae based technique was introduced by Bebis et al. [28] Jain et. Al [26]. used ridge patterns in fingerprint matching. Wang [27] proposed a new feature called polyline to extend ridge information.

Among the various current fingerprint matching algorithms such as minutiae based matching, correlation filters based matching, transform feature based matching, graph based matching ,genetic algorithms based and hybrid feature based matching and other global and local methods, minutiae based fingerprint matching is dominant.

Marios S. Poulos[29] recorded background EEG i.e. EEG recorded while people were resting and used it to identify these people.

EEG Field was also studied extensively by Ramaswamy Palaniappan.[30] In his method, a simple picture is shown to user and then this EEG is used to identify person. Method was tested on a huge dataset and its accuracy is more than 90%. Despite of such good performance, method is far from real-world application because it requires a lot of channels.

IV. AUTHENTICATION BASED ON FINGERPRINT
Fingerprints have been in use for biometric recognition since long because of their high acceptability, immutability and individuality.[6] Fingerprints are rich in details also called minutiae. Sir Francis Galton noticed that position of those minutiae doesn’t change over the time.

There are two types of minutiae, ridge endings and ridge bifurcations that constitute a Fingerprint pattern. Ridges are generally used for minutiae extraction.
There are number of fingerprint matching algorithms such as minutiae based matching[7], correlation filters based matching[8], transform feature based matching, graph based matching, genetic algorithms based and hybrid feature based matching[9].

A fingerprint recognition system consists of two stages: enrollment and authentication. In the enrollment stage, the fingerprint image is captured by the device and after pre-processing; its features are extracted and stored in the database as a template. In the authentication stage, the initial same stages are applied and the feature extracted is matched with the template to have personal authentication.

A. Data Acquisition

Fingerprint images were collected using optical fingerprint sensor. The optical sensors are most popular and are fairly inexpensive. Optical fingerprint imaging involves capturing a digital image of the print using visible light.

B. Fingerprint pre-processing

Once fingerprint is acquired next stage is to preprocess the fingerprint by using the spatial and frequency domain filters to remove the noise content in the image. After filtering binarization of image is done using a Thresholding value.[10]

C. Minutiae Extraction

Next stage is to extract minutiae for that thinning has to be done using thinning algorithm. It is a morphological operation[11] that successively erodes away the foreground pixels until they are one pixel wide. Then mark the minutia using Rutovitz’s crossing number [12]. Crossing number definition is given in below equation

\[ C_n(P) = \frac{1}{2} \sum_{i=1}^{8} |P_i - P_{i+1}| \]

If \( C_n(P) = 1 \) it’s a ridge end and if \( C_n(P) = 3 \) it’s a ridge bifurcation point. If \( C_n(P) = 0 \) it is a isolated point and if \( C_n(P) > 3 \) then there is no need to consider it as it is crossing point. [30]

D. Post Processing

Extraction algorithm produces a large number of spurious minutiae such as break, spur, bridge, merge, triangle, ladder, lake, island, and wrinkle.[13] In order to remove false minutia calculate Euclidean distance \( D \). Procedures in removing false minutia are:

- **Process 1**: if the distance between a termination and a bifurcation is smaller than \( D \), we remove this minutiae
- **Process 2**: if the distance between two bifurcations is smaller than \( D \), we remove this minutia
- **Process 3**: if the distance between two terminations is smaller than \( D \), we remove this minutia

After post processing specify the region of interest and estimate orientation.

E. Matching

Minutia based matching is done, which involves comparing extracted minutiae data from the fingerprint to the dataset stored in the database.

V. AUTENTICATION BASED ON EEG

Research shows that EEG signals of a person are different from one individual to another, even when they perform the same thought or task.

An adult brain contains about 100 billion neurons that each generates and leads electrical charges. The sum of all these very small electrical charges contributes to the generation of an electric field with fluctuating electrical potentials around our scalp. The fluctuating potentials are typically in the \( \mu V \) range and it is these fluctuations that can be measured [14]. The potentials are measured between two or more points called electrodes or sensors, which is placed on the scalp at different locations. The measurements have been named Electroencephalography (EEG), which is why the term brain waves is used when referring EEG signals.
The brain wave is categorized in five bands delta (3 Hz and less), theta (3.5 - 7.5 Hz), alpha (8 - 13 Hz), beta (14 - 30 Hz), gamma (greater than 30 Hz).[15]

VEP based authentication is done.[16],[18] Visual evoked potentials (VEPs) are brain activity responses to visual stimuli, which may comprise different components, such as color, texture, motion, objects, readability, etc. for achieving individual identification using VEPs produced upon the presentation of images from the Snodgrass and Vanderwart picture set.[17]

In EEG based authentication there are two stages. In enrollment EEG data filtering is done, then features are extracted and stored in database. During authentication extracted dataset is matched with the data set stored in database.

Fig. 3 General architecture of EEG-based Authentication

A. Data Acquisition

EEG data of 20 individual is recorded non-invasively from the scalp. EEG signals were acquired by 32 electrodes measured at a sampling rate of 256 samples per second. For building our authentication system we considered only 7 occipital channels from the 32 available in the dataset.

B. Pre-processing

As EEG data is recorded non-invasively so it is affected by noise from the surroundings. Bandpass filtering [19] is done to remove noise below 1Hz and above 50-Hz. Filtering produced noise-free VEP signals that are filtered again with a 30-50 Hz pass-band to get EEG γ-band frequency.

C. Feature Extraction and Matching

EEGLAB is used for filtering and extraction purpose.[20] After pre-processing stage, we have EEG γ-band frequency shown in fig.4. In this paper values of EEG are extracted using following procedure.

VI. AUTHENTICATION BASED ON FINGERPRINT AND EEG AS BIOMETRICS

Multimodal biometric systems[21],[22] use a number of biometric modalities from the same individual in the recognition process which increases performance and accuracy, reliability, flexibility, inclusiveness and security. Proposed multimodal biometrics system has two stages that are enrollment and authentication. Firstly during the enrollment stage store the data of fingerprint and EEG in the corresponding fingerprint and EEG database.
Fig5. represents the authentication stage here firstly fingerprint data is matched with the template stored in fingerprint database if it matches then EEG data is matched with template stored in EEG database and authenticate the person.

A. Proposed Algorithm for authenticating person using Fingerprint and EEG

Step1. Extract the values from the fingerprint and EEG, and store them in respective databases.

Step2. Read fingerprint of Person1 and Fingerprint database.

Step3. Match the fingerprint data with the template stored in database.

Step4. If match occur
   Display “Fingerprint recognized”
   “Looking for eeg match”
Else
   Display “try again”
   Break;

Step5. Read EEG of person 1 and EEG database.

Step6. Match the EEG data with the template stored in database using size 5 window.

Step7. If match
   Display “EEG recognized”
   “Welcome person”
Else
   Display “access denied”
   “try again”
   Break;

VII. CONCLUSION

Person may leave fingerprint in every place touch with hands, so everyone who needs to attack the system can collect & replicate it. Brain, in contrary, is safely hidden inside a skull.

Research work also shown that EEG based Authentication is also possible as each person have unique brain wave pattern.

REFERENCES