An Efficient Multimodal Biometric Authentication based on IRIS and Electroencephalogram (EEG)

B. Sabarigiri a and D. Suganyadevi b
a, b Department of Computer Sciences, Sree Saraswathi Thiyagaraja College, Pollachi, Coimbatore-642107, India
sabarigiri.may03@gmail.com

Abstract—In current years, IRIS recognition is flattering a very dynamic topic in both research and sensible applications. In this part, fake IRIS is a possible hazard for IRIS based biometric systems. In this paper direct attacks using fake IRIS Images and its performance measures is presented. To improve the performance of the IRIS based biometric system the Electroencephalogram (EEG) is embedded. The fusion of these two modalities is achieved at the Matching Score Level and Decision Level. A widely presented IRIS recognition system is used for our experiments. Experimental results demonstrate that the highest identification performance is obtained in the Multi-modality system using IRIS and EEG. Furthermore, it is established that EEG is an interesting complementary modality to improve the anti-spoofing ability of conservative biometrics based systems. The aim of this work is to explore the possibilities to construct a biometric authentication system based on IRIS and EEG. The survey and discovery of the most ample Artifacts removal, feature extraction and classification techniques and how these can be used for authentication principle is included. The most applicable and combined AWICA-Wavelet Transform-RLS-LS-SVM Methods proposed for our problem, this paper erect and present a prototype system proficient of authenticating users based on the individuality of their brain-waves. Furthermore, we put into practice a novel authentication process, which leads the authentication system to be more secure and also, the proposed method is appraise the usability of the system and describe possible usage scenarios and advise a number of convenient suggestions for future improvements of the system.

Index Terms—AWICA-Wavelet Transform-RLS-LS-SVM, Direct Attacks, Electroencephalogram (EEG), Fake IRIS, Multi-modality Biometrics

I. INTRODUCTION

Implementing biometrics-based technologies has improved in current years and plateful to keep the nation and multi-national enterprises by keeping people and assets, more safe and to limit physical right of entry. Biometrics is having the skill to take a bodily trait as images and Signals, compute it, and then use it as evidence of —who you are? How ever, the offered biometric methods are huddles with the subsequent traditions. (1) Age of the person, Varying lighting conditions, facial expressions, poses and orientations can complicate the face recognition task, masking it one of the most difficult problems in face biometrics. (2) The voice of people can be easily duplicated (i.e. a tape recording) and the voice of people may change if they

© Elsevier, 2014
have pneumonia or bronchitis, illness, fatigue, pitch, surgery involving tampering with the vocal cord, or any combinations of them. Age can also cause changes in the voice. If the surrounding area is noisier this kind of identification can be spoof. (3) In the DNA molecular structures of only a few people have been identified at present. DNA design generated using the Polymerase Chain Reaction (PCR) process. The Preparation kit costs around (Open PCR) $500. It will take enormous effort and time to identify the type of DNA. The downsides are that DNA samples are contaminated easily, and they are hard to control and store. (4) The finger prints of people who work in chemical industries are sometimes diminished. When using finger prints the following materials used for spoofing. They are Silicone, Moldable plastic, Plaster, Dental molding material, Gelatin, Play-doh, Target-brand gummy bears, Silly Putty, Elmer’s Reusable Adhesive Tac ‘N Stik, Rose Art Modeling Clay, Crayola Model Magic Soft, Spongy Modeling Materials. The finger prints can be leave everywhere which can be replicated and used to achieve right of entry to any security information. (5) Direct attacks and Spoofing are major problem in IRIS Biometrics. (6) Certain biometrics is vulnerable to noisy or bad data, such as dirty fingerprints and noisy voice records and identical twins are not easy to be distinguished by face recognition systems. But no one can gain access to the brain signals because it is safely protected inside the skull. This Paper provides the valuable input to IRIS direct attacks and Spoofing. Liveness Detection Procedures are possible countermeasures against directs. Here EEG is Novel Modality used for liveness Detection as well as supplementary Biometric Modality to improve the performance of the IRIS Authentication system. This paper is organized as follows. The various IRIS Spoofing, EEG Biometrics and its discussions are reviewed in Section 2; Section 3 gives the existing methods and its drawbacks. Section 4 describes the proposed methods and its advantages. Finally, in the section 5 and 6, provides experimental results and conclusions respectively.

II. LITERATURE SURVEY

IRIS liveness detection is an important and challenging issue which determines the trustworthiness of biometric system security against spoofing at the time of sensor input [1], [5], [8], [17]. The sensor is attacked using artificial biometric samples. The attack is carried out in the analog area. Outside the digital limits of the system, so digital security mechanisms cannot be used [6]. Wavelength reflection coefficient Passive and Pupil Dynamics Active Method for fake IRIS Detection [9], [10], [13], [19], The Micro lithographic IRIS Spoofing Attack Approach, or MISAA [20], Electrical signals produced by brain activity were first recorded from the cortical surface in animals by richard caton in 1875 and in 1929, Hans Berger Recorded brain activity from the closed human skull. In 1957, Gray Walter Makes recordings with large numbers of electrodes, Visualizes brain activity with the toposcope and Shows that brain rhythms change according to the mental task demanded [21]. EEG as potential biometric for personal Identification has studied by Marios S.Poulos since 1998, and colleagues were EEG biometrics when in 1999. they presented an automatic person identification system that was based on EEG signals acquired from four subjects in a resting state with closed eyes, Closed Eye position and the restring state of the brain waves acquisition protocol has used for biometric authentication [25]. Later, the development of a mobile biometric authentication system based on EEG Recordings in combination with already proven technologies such as facial detection and near field Communication (NFC) presented [22]. EEG is potentially more secure and privacy compliant than traditional biometric identifiers [23]. Convert Warning (CW) is a feature that allows an authorized person, when coerced, to secretly send out a warning message along with his/her personal identification [24]. EEG-Based Authentication using Face Stimuli proposed in [26],[27] EEG based solution to improve security Check [28], The biometric multimodal interface can recognize a user’s emotion and concentration status by analyzing ECG (Electrocardiogram) and Electroencephalogram (EEG) Patterns [30],[31]. The Dual Multi modality based on Fingerprint and EEG is proposed in [32].

III. EXISTING METHODS AND ITS DRAWBACKS

First, Single modal systems execute person recognition based on single modality. Single biometrics systems have a variety of troubles such as noisy data, individuality, non-universality, High Spoof Rate, High fault rate, Liveness Detection and Direct attacks [6]-[7]. The existing biometrics communities are hurdles with confidentiality and unfairness, cancellable biometrics, risk to holder of Secured items. The reasons for the attacks are transform their individual uniqueness, violence, to create criminal actions, frauds; a person can use any one of the above described spoofing techniques to change the identity of a genuine person. Second,
without a clear strategy for enabling research efforts bio metrics build upon one another, but it will fall behind the market. In order to rectify this problem a new approach is suggested [29]. To overcome the above said inconvenience in the Single Modal biometric systems and develop the performance of biometric security is to be solved by using Multi-Modal Biometrics. These boundaries can be solved by deploying multimodal biometric systems. IRIS and EEG are the first of its kind in the international scenario and which provides outstanding Identification performance and effective anti-spoofing property.

**IV. PROPOSED METHODS AND ITS ADVANTAGES**

The Proposed integrated Multi modal biometric systems utilize two individual modalities, like IRIS and EEG. An EEG signal of each personality differs in such a way that they are not same even if they do the same work or task. The brain wave of each personality is unique; DNA and living expressions will certainly have a force on human brain structure. It can be said that even if the DNA of two persons are the same but their living experiences will vary. EEG always depends on the living experiences on each personality. So, Authenticating users based on their EEG is more accurate than other biometric technologies.

**A. IRIS Based Biometric Authentication**

IRIS recognition has gained popularity due to factors such as its superficial high accuracy, quick, robust, fast to compare, it’s non-contact acquisition method, and the availability of low cost sensors due to improvements in technology. The IRIS is plainly visible, colored ring that surrounds the pupil and it has a muscular structure. IRIS controls the amount of light entering the eye. Due to epigenetic nature of IRIS patterns each and every individual has a unique. IRIS is an externally visible internal organ which in turn remains plays a vital role through the human's entire life cycle. The IRIS formation starts at third month of born, and the structures creating its pattern are largely complete by the eighth month of born, and this formation wouldn’t be changed though out the human being life. The two eyes of an individual hold IRIS patterns which are completely independent from one another are advantages of IRIS. But, there are many false techniques evolved to cheat every IRIS biometric sensor, Fig.1 and Fig.4 shows that the IRIS spoofing [18] methods includes Printed IRIS Images and photographic surfaces, re-played video, fake glass/plastic eye and IRIS texture printed on contact lenses[2]-[4],[11],[12],[14],[15],[29]. A widely presented IRIS recognition system is used for our experiments developed by Libor Masek [16]. It consists of the following steps: Segmentation, Normalization, Encoding and Matching.

**IRIS Data Collection**

Thirty two healthy volunteers (20 males and 12 females) IRIS images were collected. At the time of Extraction took some efforts to control image quality on eye pictures, and as well as appropriate settings such as lighting and distance to camera were adjusted. DM365IPNC Camera used to extract IRIS Patterns in the Effective Manner. The image size is 320×240 pixels and 24 bit depth stored in the .bmp file format. For our authentication system only 32 Subjects were taken into account. From each person 5 samples were collected, only 3 samples stored in the data base, all the 5 samples used for testing. First 30 subjects considered as correct persons, Remaining (31st, 32nd) 2 subjects as false persons in the authentication system. Then the Real images were used for authentication, the total authentication Rate of the system is 100% (Threshold Value is 0.26) for e.g. Fig 14. After that the fake images produced using FALSE IRIS DATABASE GENERATION METHOD for e.g. Fig.2, Fig.3. **METHOD 1:** (1) Initially, the images are processed to progress its quality. (2) Then these images are printed in a regular paper using a usual printer. (3) The printed images are exhibited to the IRIS sensors to carry out a fake authentication. Using fake images the Total Authentication Rate of the
system is 76.67% (Threshold Value 0.42) for E.g. Fig 15.

METHOD 2: The only thing that was still missing was a printed picture of an IRIS with an appropriate degree of quality. Hence we presented to the Authentication digital image of a human eye that had been sprayed onto mat inkjet paper with a resolution of 2400 x 1200 dpi and into which we had previously cut a miniature hole [34].

<table>
<thead>
<tr>
<th>(a) Sample Contact Lenses Images</th>
<th>(b) CL's Under Infrared Illumination</th>
<th>(c) Hand Painted Contact Lens</th>
</tr>
</thead>
<tbody>
<tr>
<td>Naked</td>
<td>Color Enhancer</td>
<td>Naked</td>
</tr>
<tr>
<td>Under Visible Light</td>
<td>Color Changer</td>
<td>Under Visible Light</td>
</tr>
</tbody>
</table>

This was enough to overcome Authentication resistance: We were granted access to the system under the assumed identity of 'Master False Eye'. It was also possible to enrol with the aid of the 'artificial' eye. From that point onwards anyone in possession of the eye pattern was able to log on to the system. Moreover, the person whose eye had been used to create the pattern was also able to acquire authentication in relation to the picture-generated reference data set with his own live IRIS.

B. EEG Based Biometric Authentication

The human brain is the hub of the human nervous system and it monitors and regulates the body’s actions and reactions. It continuously receives sensory information, and rapidly analyses these data and then responds to the actions and functions. EEG has many advantages, (1) An Effective liveness Detection method [29], (2) EEG as an effective external force detection method to enhance the anti-spoofing capability of the existed biometric system to meet higher security requirement applications [35], (3) EEG is hard to mimic, (4) EEG can be used as an excellent complementary modality to the existed biometric systems which are not easy to be forged. (5) No one can gain access to the brain waves, because it is safely protected inside the skull. (6) Our brain activities are changeable. So this is first changeable biometrics system. (7) Brain wave signals, which is natural candidate for liveness detection it gives Anti Spoofing system design in existing unimodal IRIS biometrics. (8) EEG signals are particularly strong when a person is exposed to visual stimuli, and the visual cortex area of the brain on the backside of the head is the best place to measure brain-waves, related to the visual sense [33]. The idea of such a system is that instead of using e.g. normal textual passwords, the system stores a user's personal recording of brain-waves when exposed to self image, and compares this recording to new brain-wave recordings using the self image when the user authenticates prospectively. In this way the system acts as an involuntary challenge-response system. IRIS is a protected
internal organ and has cells that are directly connected to the brain. The integration of IRIS and EEG recognition biometric systems is to become the leading technology in identity verification. EEG is the spatially weighted summation of all these action potentials measured at the surface of the skull. The technique to extract the human brain information provides a new research paradigm as EEG-Based Biometry.

EEG Signal Acquisition

The EEG Measurements is obtained based on the Emotiv EPOC Research EEG neuroheadset in Fig 5: a 14 channel bio potential sensors with gold-plated connectors offer optimal positioning for accurate spatial resolution (plus CMS/DRL references, P3/P4 Reference Locations). 14 EEG channel names based on the International 10-20 locations are in Fig 6: AF3, F7, F3, FC5, T7, P7, O1, O2, P8, T8, FC6, F4, F8, and AF4. The sampling rate of the emotive EEG headset is 128 Hz on the output (To ensure the precise output values, the Emotiv headset has the internal sampling rate of 2048Hz frequency) with 1.95 μv least significant bit (LSB) voltage resolution, Therefore it is possible to detect VEPs (Which can be beneficial to deduce latencies of electrical impulse exchange representing uniqueness of neural-wiring of subjects brains), since average amplitude for VEP waves falls between 5 to 10 microvolt’s.

Fig 5: EEG Epoc Headset

Fig 6: 14-Default Electrode Position of EEG Epoc Neuroheadset

Fig 7: Subject Wearing Headset

Fig 8: Displaying self Image using webcam and EEG Signals Acquisition through EEG Epoc Headset

The proposed method has also been tested by 32 healthy subjects (Students and Working employees) (20 males and 12 females) has been collected in order to evaluate the performance of our system. An informed consent along with a health related questions were raised and questionnaire was signed and filled by all subjects before the data collection. The subjects are asked to sit in a comfortable chair, to relax and be quiet. The background is set as white board and foreground is blue window screen. There are two laptops with good configuration were fixed in front of the subject showed in Fig 7 and Fig 8. The first Laptop used for displaying Subject’s own face using Webcam with high resolution camera. EEG Epoc headset is used to extract the Brain Signals, and its High performance wireless automatically transfers the Signals to USB Dongle in the Second laptop. no custom drivers specially required for USB Dongle in this Extraction Process. To establish a good connection between the scalp and EEG electrodes, the saline liquid solution was put on every electrode before each experiment. However it was necessary to redo the experimental procedures, after checking if the EEG data is valid or not for the further analysis.

Artifacts Avoidance

Managing artifacts is to avoid their occasion by issuing suitable directives to users. Instructing individuals to steer clear of generating artifacts during data collection has the benefit that it desires less computational demand among the artifacts handling methods, since it is assumed that no relic is present in the signal. But it has a number of drawbacks.

First there is no leeway to stop our heart during the EEG signal extraction. Even in the case of EOG and EMG activities, it is not easy to organize eye and other progress activities during the data recording in our body. Second the amount of ocular and force activity during the online operation does not exist, and power
line interference is also manifest. Third collecting possible amount of data mining will be less due to artifacts presents in the EEG signal, particularly in cases where a consumer has a neurological disability. There are countless techniques were discussed by several Bio signal Researchers. The most of the proposed methods had a limited success rate. Some methods took more time to carry out the required computation work and others were very multifarious for practical applications. It is not easy to control eye and other progress activities during the data recording. Second the amount of ocular and influence activity during the online operation does not exist. Third collecting adequate amount of data lacking artifacts may be difficult, particularly in cases where a consumer has a neurological disability. Each recording is a single two minutes EEG event. There are totally 32 Subjects X 5 Samples=160 Sessions in the data set. The EMG, a high frequency component, is due to the random contraction of muscles, while the sudden transients are due to impulsive movement of the body. This well known problem that appears in the recorded EEG as intrusion causes cruel problems in EEG illumination and assessment. To remove the EOG, EMG from the EEG, we required to order the artifacts and brain waves without changing important in turn of EEG activity. The occasion of electrical artifacts generated by eye movements, open and closing of eyes, blink infectivity produce a signal known as Electrooculogram (EOG).

Cancelation of Artifacts
The proposed algorithm combines the valuable ICA knack of sorting out artifacts from brain waves, mutually among the online interference (50Hz) termination achieved by adaptive filtering. Wavelet based Denoising used to extract the low frequency component in order to eliminate the High frequency component the EMG signal. Fig 17 Shows that the performance of AWICA Method Compared with FastICA Method. The main steps of hybrid Pre-processing AWICA approach are the following.

Step1: the Extracted EEG data were processed by Adaptive Filtering to remove Power Line Interference, broken wire contacts and Electrode Impedance (50Hz and above).
Step2: To apply Wavelet Transform algorithm to 14 channels of the multichannel recordings separately. Finally, set of signals with different frequencies were obtained.
Step3: The base line was removed using wavelet decomposition and the signal was denoised by wavelets.
Step 4: To identify and select the highly correlated artifact components and produce the new data set.
Step 5: To transfer the constructed data set to Independent Component Analysis (ICA) Block.
Step 6: To make the signal to be uncorrelated and apply the whitening in order reduces the dimensionality and to light the computational charge.
Step 7: To estimate the independent components and remove ones related to the artifacts.
Step 8: According to the sources ICA would split and cleaned the signals. The correlated EOG, ECG and EMG signals should be classified which will be eliminated using FASTICA.
Step 9: Finally, to perform the wavelet reconstruction by (7) using the non-selected details and cleaned details after ICA step; finally, we obtain the multichannel recordings in which the artifacts are removed.

Channel Selection
EEG signals are predominantly strong while a person is bare to visual stimuli, and the visual cortex area of the brain on the reverse side of the head is the best place to measure brain-waves.

<table>
<thead>
<tr>
<th>Electrode Positions</th>
<th>No. of Channels</th>
<th>Channel Positions on Scalp</th>
</tr>
</thead>
<tbody>
<tr>
<td>O1</td>
<td>1</td>
<td>Occipital Lobe</td>
</tr>
<tr>
<td>O1, O2</td>
<td>2</td>
<td>Occipital Lobe</td>
</tr>
<tr>
<td>P7, P8, O1, O2</td>
<td>4</td>
<td>Parietal and Occipital Lobe</td>
</tr>
<tr>
<td>AF3, F7, F3, FC5, T7, P7, O1, O2, P8, T8, FC6, F4, F8, AF4</td>
<td>14</td>
<td>Default Channel With All 14 Positions</td>
</tr>
</tbody>
</table>

![Single Channel Selection Plotted with Biosignalplot](image1)

![Two Channel Selection-O1, O2 Electrodes](image2)
Here, the system arranged to utilize the subjects and their own face as Visual stimuli. The Extracted EEG signals clustered according to where the surface electrodes placed on the Scalp in Fig.13, 14, 15 and 16. Mostly in our system has taken the Occipital and Parietal Channel Positions for Authentication. Normalized value of Signals used for Authentication. The channel selection is in Table 1.

Feature Extraction
After Removal of artifacts signals are converted into vectors of extracted distinctive features that can be used for Human Identification System using EEG. In time domain analysis Parametric Models are very useful for extracting the feature from the EEG signal. Auto regressive based estimation methods will reduces the spectral loss problems and gives better frequency resolution. When compared to FFT, AR model will require only shorter duration of data records. The significant drawback existing on this method is difficulties in establishing the model property for different EEG signals (Non-Stationary Signals). Frequency domain approaches: The plan of signal analysis by this method is to extract appropriate information from a signal by transforming it to the frequency domain. The admired way of frequency analysis is (1) Power spectral
analysis via Fourier Transformation, which is extensively used for the standard quantitative analysis of the spectral decomposition of EEG Signals. This is suitable only for the signals for stationary nature and linear random processes. It also lags in instantaneous time and frequency dimension. The following analyses are the time-dependent spectrum of non-stationary signals. (i) STFT (ii) Wigner-Ville Distribution (iii) Time-Varying Parametric Model. The STFT assumes the stationary of the signal within a temporal window to match the time-frequency resolution chosen for spectral approximation. The problem in this method is lies on fixed time- frequency resolution chosen for the spectral estimation. WVD is excellent for time-frequency concentration and edge characteristic, but for multi-component signal, it can introduce cross-disturbance term, which may cause misinterpret for signal’s time-frequency features. An influential method was projected in late 1980’s to perform time-scale analysis of signals: The Wavelet Transform. It is a mathematical microscope is used to analyze different scales of neural rhythms is shown to be a powerful tool for investigating small-scale oscillations of the brain signals. The wavelet decomposition of the EEG records, transients features are precisely capture and localized in both time and frequency context. Last of all, The Wavelet Transform is an efficient feature extraction from non-stationary signals such as EEGs.

Data Reduction
It is reducing the amount of data generated after wavelet transform by without losing the Original in sequence of the signal features. All the data Reduction methods will lose some amount of useful data features on data reduction process. So here we required a new method to reduce the feature set but not leaving any features extracted from the EEG Signals. So, here we applied weighted mean to reduce the value but which is not leaving any feature vectors.

Classification
There are so many methods are available to classify the features from the EEG signal. The classification can be performed by using Support Vector machine (SVM), Neural Networks (NN), Linear Discriminant Analysis (LDA), Genetic Algorithm (GA), Naive Bayes classifier, and so on. SVM have very good solid foundation in statistical learning theory. Guarantees to find the optimal decision function for a set of training data, given a set of parameters determining the operation of SVM. SVM performs better classification on emotional features derived from the EEG signal than LDA and conventional NN. According to the survey many researchers closely concentrated on SVM classification for EEG Signals because of its performance. But the Classification Performance is depends on Features which is supplied to the classifier. So, Improving the Feature Extraction and Feature Reduction Method will give the accurate classification Results for EEG Signals. The System will give only two results Authenticated/ Not Authenticated.  So, The Least Square Support Vector Machine (LS-SVM) had been used. The combination of AWICA-Wavelet-RFS-LS-SVM helps to produce excellent results in EEG Based authentication.

IRIS and EEG Fusion: Multimodal biometric system can be consolidated at various levels, here, in this system matching score level and decision level strategies were applied. AND Rule and Weighted SUM used for fusing the IRIS and EEG. The sum-rule based fusion scores were calculated with equal weights assigned to each modality.

C. Proposed Multimodal Biometric Authentication using IRIS and EEG
Step 1: Extract the values from the IRIS and EEG, and Store them in respective Databases
Step 2: Read the IRIS data from Subject 1
Step 3: Match the IRIS data with the corresponding Template stored in the database.
Step 4: If Match occurs
  Display “IRIS Recognized Looking for EEG Match”
Else
  Display “Try Again”
Break
Step 5: Read EEG Signal from Subject 1
Step 6: Match the EEG data with the template stored in database
Step 7: If Match
  Display “EEG Recognized & “Welcome the Person”
Else
  Display “Access Denied & Try Again”
Break
V. RESULTS AND FINDINGS

Fig 14: Authentication Rate for Real IRIS Images

Fig 15: Authentication Rate for Fake IRIS Images

Fig 16: Pre-Processing AWICA and its comparison with other (JADE, ICA, SOBI and Infomax) algorithms (SNR vs. MSE)
VI. CONCLUSION

The performance of AWICA results showed in Fig 16, 17. From Table: 2 despite the fact that using 4 channels (P7, P8, O1, and O2) 97% accuracy achieved. While increasing the no. of channels up to 14 the Time taken for the process is 16.98 Seconds.

REFERENCES

25. Daria La Rocca, Patrizio Campisi, Gaetano Scarano, "EEG Biometrics for Individual Recognition in Resting State with Closed Eyes", International Conference of the biometrics Special Interest Group (BIOSIG), 2012.
34. http://www.pcmag.com/article2/0,2817,1158008,00.asp