SECURE DUEL AUTHENTICATION USING IRIS AND OTHER BIOMETRICS

Nida Afreen¹, Mohammed Junaid Tariq², Preeti Kumari ³, Siddaramappa .V ⁴

¹²Department of Computer Science &Engineering, CEC, India
³Department of Computer Science &Engineering, CEC, India

ABSTRACT:

Providing security to the confidential data is critical job nowadays. To provide enhanced security—23⁵y, dual biometric authentication can be used. In this, two different biometric data is implemented where primary authentication method is Iris recognition and secondary authentication method is chosen randomly using random option generator. Secondary authentication methods such as Fingerprint Recognition, Face Detection, Voice Recognition, Palm detection. By this it is ensured that the rendered services are accessed only by a legitimate user and no one else. It would be really hard to guess which of the secondary authentication could be requested to bypass the system even if they somehow manage to bypass Iris Recognition. With the help of this type of authentication theft of highly confidential data will not be possible.

Keywords: Biometrics, Dual-Authentication, Security

[1] INTRODUCTION

“Biometrics” is a Greek term inspired from the words “bio” - life and “metrics”-to measure physical characteristics of human body. In any commercial and secured system makes use of an unique user name and its corresponding password for validation of a person which can be hacked by criminals and can rupture the doors of security. Intrusion is intolerable in high secured zones like defence systems, bank transactions on online trading/ and government officials.
Biometrics specifies the usage of a measurable physical characteristics and behavioural trait against identity theft. Behavioural approach uses recognition of signature, voice etc. while physiological approach include fingerprint, iris, retina, DNA, palm print etc. For each individual the features of contours and contour let are unique and be persistent during his/her entire life.

The authentication system using biometric features are categorized as single mode and dual mode. i.e., single modality and dual modality based authentication system. In singular mode authentication biometric system the features from one mode of input is used for recognition or identification. There are certain disadvantages with the single mode authentication systems like failing. For e.g. the lack of biometric template. For such scenarios dual modality are used.

Over the life of a person iris is persistent and remains unaltered. Each human has two distinct iris pattern i.e., it is impossible to enroll with the left eye and authenticate using right. Pupil is like a black disk of circular shape located at the center of the eyeball. During light the pupil expands and in dark it contracts. Hence light is a factor which determines the pupil size. Even though the visible portion of iris changes as a function of pupil dilation, this does not inversely affect the authentication. Iris has a flowery pattern which is persistent to each one and is like a annular ring like structure between pupil boundary and sclera.

Fingerprints are the one of the widely used technique for secure transactions. Through our naked eyes the global features of each fingerprint is visible and the minutia points or local features is unique for each fingerprint. For identifying the individual, using of fingerprint biometric is the best technique. Fingerprint has many ridges and valleys on the finger surface.

Face Recognition consists of face identification and face verification. Face identification is matching area in one-to-one way and face verification is matching area in a one-to-many way. Face identification is using cross-checking with a several of images in the database to recognize an image. Face verification is analysing and checking two images from their similarity.

Biometric voice recognition and identification technology focuses on training the system to recognize an individual’s unique voice characteristics (i.e., their voice print). The technology lends itself well to a variety of uses and applications, including security access control for cell phones (to eliminate cell phone fraud), ATM manufacturers (to eliminate pin # fraud) and automobile manufacturers (to dramatically reduce theft and carjacking).

Palm identification has emerged as one of the most popular and promising biometric modalities for personal identity verification due to its ease of acquisition, non-invasive procedure, high user acceptance and reliability.
[2] SYSTEM BLOCK DIAGRAM

The figure shows the system block diagram where a primary authentication i.e., iris recognition is interfaced to the processor, and as secondary authentication fingerprint recognition, face recognition, voice recognition and palm recognition are interfaced to the processor. And fused result is displayed on the LCD screen.

![System Block Diagram](image)

Iris detection is taken as Primary Authentication here, once an individual bypasses this authentication the processor randomly chooses any one of the option from secondary fingerprint detection, face detection, voice detection and palm detection. When both authentication have been successful, this completes the authentication and the user gets the required access.

[3] IMPLEMENTATION

3.1 Iris Recognition

Primarily acquiring Image is either a manual or automated procedure. Image enhancement is done to compensate the factors due to light in iris image. Average filtering and median filtering is used to remove the noise from image and improve textural features in Image Pre-Processing step. Exact circular iris is located using edge detection, pupil detection or any other suitable methods during localization phase. The iris of different or same person varies in size because of the differences in illumination and other features such as elastic deformation in textures that influence the results of iris matching. The features of iris are extracted using various feature extraction techniques. After extracting the unique iris features are stored as template in database. These features are called as Iris code for template creation. Finally bit by bit comparison is done to match the iris images.

![Iris Recognition Process](image)
The above process shows how the iris is matched with the existing documented iris template. This is used as the primary authentication method, once this process has been completed the system randomly selects the secondary authentication method among the specified biometric like fingerprint detection, face detection, voice detection and palm detection.

**3.2 Algorithm**

The each biometric is specified with a number where the total number of biometrics is used as an input to random option generator, here a number is randomly selected using an algorithm the specified number with biometric as its label is asked for secondary login/authentication method.

**3.3 Fingerprint**

The biometric modality which mainly uses are the combination of contours and contourlets of curves and valleys on the front surface of the finger. A minutia extraction method for comparison is used in this. The below figure shows how the fingerprint recognition takes place.

![Fingerprint Recognition Process](image)

Fig 3.1 (a) Fingerprint Recognition Process
3.4 Face Recognition

Face Recognition consists of face identification and face verification. Face identification is matching area in one-to-one way and face verification is matching area in a one-to-many way. Face identification is using cross-checking with a several of images in the database to recognize an image. Face verification is analyzing and checking two images from their similarity.

3.5 Voice Recognition

Biometric voice recognition and identification technology focuses on training the system to recognize an individual’s unique voice characteristics (i.e., their voice print). The technology lends itself well to a variety of uses and applications, including security access control for cell phones (to eliminate cell phone fraud), ATM manufacturers (to eliminate pin # fraud) and automobile manufacturers (to dramatically reduce theft and carjacking). In this paper, we present an implementation of a security system based on voice identification as the access control key. Verificationalgorithm is developed using MATLAB (SIMULINK) function blocks which is capable of authenticating a person’s identity by his or her voice pattern. A voicematch will produce logic ‘1’ while a mismatch, logic ‘0’.
SECURE DUEL AUTHENTICATION USING IRIS AND OTHER BIOMETRICS

3.5 Voice Recognition Process

3.6 Palm Recognition

There are various ways to capture palm print image. Researchers utilize CCD-based scanners, digital scanners, video camera and tripod to collect palm print images. The below figure shows a CCD-based scanner developed by Hong Kong Polytechnic University. A CCD-based scanner captures high resolution images and aligns palms accurately because it has pegs for guiding the placement of hand. The palm print recognition system includes pre-processing followed by ROI extraction. After ROI extraction, features are extracted using the feature extraction algorithms. The palm print is then accepted or rejected on the basis of matching the extracted features.

[4] RESULT

The result indicates that this paper provide high security than the other duel biometric authentication system. Because other authentication system use only two biometric authentication, Here in this paper we use primary authentication as Iris and secondary authentication such as fingerprint detection, face detection, voice detection and palm detection, So it would be really hard to guess which of the secondary authentication could be requested to bypass the system even if they somehow manage to bypass Iris Recognition. With the help of this type of authentication theft of highly confidential data will not be possible.
[5] CONCLUSION

The assessment of the vulnerabilities to direct attacks of An Iris-based Verification system has been offered. Here we have proposed a system which is an efficient accurate and precise duel biometric authentication system by combining the features of iris and other various biometrics. It has already been evaluated that iris is most secure way of biometric authenticity to enhance our security we have made it much more difficult to bypass the security system in an un-ethical way since we have proposed a system that uses random biometric authenticity as secondary authentication that is randomly asked by the system which is hard to predict by a human which secondary authentication could be asked by the system.

REFERENCES


