A Multimodal Approach to Increase the Security of Biometric System

Mamta Ahlawat¹, Arun Kumar Yadav², Dr. Chander Kant³

¹² Research Scholar, Department of Computer Science and Applications, K.U., Kurukshetra, INDIA
³ Asst. Professor, Department of computer Science and Application, K.U., Kurukshetra, INDIA

Abstract: Multimodal biometric system is the combination of more than one biometric trait to authenticate a person. Unimodal biometric systems use only one biometric trait (voice, gait, signature, iris, retina, face, ear, hand geometry, fingerprint, etc.) to recognize person. Unimodal biometric system have some limitations over authentication like noise in sensed data, intra-class variation, inter-class variations, distinctiveness, spoof attacks etc. Therefore unimodal biometric system is less secure and less reliable and this is the reason that unimodal biometric systems are become less acceptable where high security required. Some of the limitations imposed by unimodal biometric system can be overcome by incorporating multiple traits of individuals rather than one trait. Here in this paper, we have proposed a multimodal approach with integrating the soft biometrics (height) with iris and ear to enhance the security of personal recognition system. In our approach we have proposed a combined architecture of three different traits to raise the system security. We have also proposed an algorithm to authenticate person.

Keywords: Ear recognition, Height measurements, Iris recognition, Multimodal biometrics.

1. INTRODUCTION

Multimodal biometric system is a technique in which more than one traits of a person combined to acquire high security and reliable recognition. The combination has the advantage of the proficiency of each individual biometric trait and thus provides strong performance, reliability, robustness and security.

A biometric system authenticate persons based on their physiological and behavioural characteristics like hand-geometry, ear, fingerprint, iris, face, palmprint, retina, voice, signature, gait and keystroke [1]. Soft biometrics (color, eye color, weight, height, age, etc.) of a person also use for recognition. Soft biometrics is the primary way to recognize a person. But the information acquire from soft biometrics is unreliable, indistinctive and also unsecure so it is not adequate to recognize a person. And soft biometric does not provide unique identity. Therefore there is need a biometric system based on physiological and behavioural characteristics of a person. By using only single biometric trait, authentication of a person is not secure and reliable. Thus multimodal combine more than one trait either soft biometric, physiological or behavioural to provide better security. If soft biometrics combined with physiological characteristics of individual then it will provide a better secure and reliable authentication. Multimodal biometric system provides higher security, reliability, acceptability and low circumvention. Below figure presents multimodal biometric system with two different traits and fusion the match score to compute result either accept or reject.

In figure 1, FE: Feature Extraction and MM: Matching Module. This paper discusses an approach with integrating the information acquired by the soft biometrics (height) with iris and ear to enhance the security of biometric system.

2. RELATED WORK

The first system was proposed for the identification of criminals based on Morphological description,
Anthropometric measurements and Peculiar marks [2]. This system was tracking criminals but due to the features like weight, height, age and eye color are not satisfied and dynamic. Therefore this system had an unacceptably high error rate. Then the biometric system was proposed with human’s physiological and behavioural characteristics like fingerprint, face, retina, iris, hand geometry, voice, gait and signature [3]. This biometric system provides recognition to individual. But due to using only one trait this system has some drawbacks like noisy data, intra-class variations, non-universality, spoof attacks and unacceptable error rates. Multimodal biometric system was proposed to overcome unimodal biometric system limitations. Multimodal biometric systems combine more than one biometric trait and provide secure and reliable authentication [4]. Muhammad Imran Razzaq et al. [5] combined the face and finger veins characteristics to increase the robustness and reliable of the authentication system. Face and speech combine in order to improve the problem of one biometric authentication are proposed by Mohamed Soltane et al. [6]. A multimodal biometric system used lip movement and gestures proposed by Piotr Dalka et al. [7]. Face and ear combine for easy to capture information, proposed by A.A. Darwish et al. [8].

Kawulok et al. presented a combination of face and eyes to increase security of biometric system [9]. Linlin Shen et al. proposed integrating face and palmprint to efficient match between stored template in the database and acquired template [10]. Fusion of soft biometric and hard biometric can be use to provides better authentication result [11]. C.K.Verma proposed a combination of soft biometric with fingerprint and face to improve the performance of biometric system [12]. In our paper, we proposed a combination of soft biometric (height) with physiological traits (iris and ear) to enhance security of biometric system as discussed in section 3.

3. PROPOSED FRAMEWORK
This paper proposed an architecture and related algorithm with the combination of height, iris and ear and applies normalization, fusion method on that proposed combination. This combination provides better security as compare to other existing multimodal biometric systems. Next 3 subsections give a brief introduction separately of each biometric trait that are using in this paper.

3.1 Iris Biometric traits
Iris patterns are unique and are obtained through video based image acquisition system and stored in the database. Each iris structure have complex pattern. This can be a combination of specific characteristics like corona, crypts, filaments, freckles, pits, furrows, striations and rings [13]. Iris recognition uses camera technology with infrared illumination to acquire the image exact and clear [14].

3.2 Ear Biometric trait
Ear is a universal physiological characteristic of a person. Ear biometric trait is uses for recognize an individual. Ear has data rich anatomically features and also unaffected trait by ageing. Ear is present on the both side of the head and extraction is easier [15]. The ear feature for identification are using in forensic for almost more than 10 years [8, 16]. Ear biometric trait is using to improve accuracy and security of a biometric system.

3.3 Height Soft biometric trait
Height is a Soft biometric trait that is using to recognize a person but not uniquely. For using soft biometrics, a mechanism is there to automatically extract features of soft biometric from the individual [17].

3.4 Why Iris, Ear and Height Multimodal
For an efficient understanding and security we use the combination of iris, ear and height. There are some aspects discussed below.

a) Security: The first and foremost reason is that iris and ear are more secure biometric trait means less possibility of spoof attacks.

b) Uniqueness: Iris and ear of a person are unique.

c) Reliable: A distinctive iris pattern is not susceptible to theft, loss or compromise.

d) Performance: Iris and ear both are unique for each person therefore provides accurate result and increase performance.

\[
\text{Accuracy} \% = \left(100 - \frac{\text{FAR} + \text{FRR}}{2}\right)
\]

The accuracy of the system increases when FAR and FRR decreases.

e) Permanency: Both ear and iris biometric traits are permanent. So there is no need to change database continuously of a person.

3.5 Architecture of Proposed Scheme
It is present that iris and ear biometric traits combine with soft biometric provide better accuracy and security than other existing combination biometric systems. Proposed scheme (as shows figure 2) works by first measure height, comparing and matching it with existing database. If the result is not match then it will directly reject the person without capturing other biometric traits otherwise computes the match score. After that, capture iris and ear, extracts their feature set, compare it with existing database, compute match score respectively. Min-Max Normalization and then Simple Product rule Fusion method apply on all three computed match score and generate a combine Match score. If this match score is greater than and equal to specify threshold value then the query person is authenticate otherwise rejected.

<table>
<thead>
<tr>
<th>Height</th>
<th>Iris</th>
<th>Ear</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scale</td>
<td>Suitable Sensor</td>
<td>Suitable Sensor</td>
</tr>
</tbody>
</table>
The proposed scheme has some drawbacks,

a) Need extra storage database to store all three acquired biometric data.

b) Response time of the system is not satisfied if the query is genuine.

c) Always put-off shoes whenever need to recognition for height measurement.

3.6 Mathematical Terms

There are two mathematical terms that are using during algorithm,

**a) Min-Max Normalization:** Normalization methods are used to convert various (location and scale parameters) matching score of different matchers into a common domain. Min-Max Normalization is the simple and best suited for the case where the bounds (maximum and minimum values) of the matcher are known. It has original distribution of score except for a scaling factor and transforms all the scores into a common range \([0, 1]\).

The normalized score is given by

\[
S_{\text{kn}} = \frac{S_k - \min}{\max - \min}
\]

where \(S_{\text{kn}}\) is normalized score and \(S_k\) is the match score set.

**b) Simple Product Rule Fusion method**

It combines the match scores by multiplying all of the individual match scores. If \(S_i\) is the match score from \(i^{th}\) modality, \(S\) represents the resulting fused score.

\[
S = S_1 * S_2 * S_3 * \ldots * S_n
\]

This product gives the fused score then the result will compute based on that fused score.
3.7 Comparison with other Existing Multimodal technique

Propose scheme give better performance than other existing technologies.

As discussed earlier it provides higher accuracy due to presence of iris.

Iris and ear both are unique biometric traits therefore free from spoof attack and provide better security than other existing multimodal biometric system.

Due to accurate and permanent biometric traits it gives better result than other multimodal biometric technologies.

3.8 Proposed Figures

There are some figures that present proposed scheme.

Figure 3, 4 and 5 shows density plot between genuine and imposter for Iris, ear and eye height respectively.

4. CONCLUSION AND FUTURE PROSPECTUS

Multimodal biometric systems overcome numerous problems observed in unimodal biometric systems. To find a good combination of multiple biometric modalities, we have proposed a new multimodal (Iris, ear and height) and proved its efficiency over existing multimodal techniques. This combination provides high security of biometric system. The related work has shown the multimodal system under the different trait combination scheme and their objectives. The combination of iris, ear and height give an accurate result as compare to existing multimodal system. There are some drawbacks of proposed scheme as discussed in section 3.5. One of them is, need a high storage database. In future prospect, a mechanism can be
developing to overcome this limitation so that response time minimum and satisfy genuine person.

REFERENCES:


