Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P) Vol.5 No.2, 2016, pp.1-4
© The Research Publication, www.trp.org.in
DOI: https://doi.org/10.51983/ajcst-2016.5.2.1772

Multimodal Biometric Technology Using Fuzzy Logic Decision and Fuzzy Inference System

S. Senthil Kumar
Assistant Professor, Department of Commerce with Computer Applications,
Dr.SNS Rajalakshmi College of Arts and Science (Autonomous), Coimbatore, Tamil Nadu, India
E-mail: ssksnsmca@gmail.com

(Received 2 June 2016; Revised 19 June 2016; Accepted 10 July 2016; Available online 17 July 2016)

Abstract - **In this research paper I discuss about the challenges to implement secure personal identification protocols with biometric technology are increasing and the need for accurate human identification is higher than ever. Single modality biometric systems have to contend with a variety of problems such as noisy data, intra class variations, non-universality, spoof attacks, and distinctiveness. Some of these limitations can be addressed by deploying multimodal biometric systems that integrate multiple biometric modalities in a single scan to alleviate the challenges of a unimodal system. Performance in biometric verification is often affected by external conditions and variabilities. These are often related to mismatched conditions between enrolment and verification sessions, e.g. handsets/microphones for recording speech, cameras for capturing facial images and fingerprint readers. In addition, the user's speech may vary according to ambient noise conditions, the speaker's health (e.g. contracting a cold) or speaking styles. The user's facial images may vary due to changes in backgrounds, illumination, head positions and expressions. While none of the biometrics alone can guarantee absolute reliability, they can reinforce one another when used jointly to maximize verification performance. This motivates multi-biometric (multimodal) authentication.**

Keywords: **Multimodal, biometric, fuzzy inference system, fuzzy logic**

I. INTRODUCTION TO MULTIMODAL BIOMETRIC TECHNOLOGY

Multimodal biometrics are systems that are capable of using more than one physiological or behavioural characteristic for enrolment, verification, and identification. Human identification based on multi-modal biometrics is becoming an emerging trend, and one of the most important reasons to combine different modalities is to improve recognition accuracy. There are additional reasons to combine two or more biometrics such as the fact that different biometric modalities might be more appropriate for unique deployment scenarios or when security is of vital importance to protect sensitive data.

II. WORKING OF MULTI-MODAL BIOMETRIC SYSTEM

Multimodal biometric systems take input from single or multiple biometric devices for measurement of two or more different biometric characteristics. For example, a multi-modal system combining fingerprint and finger vein characteristics for biometric recognition would be considered a "multi-modal" system regardless of whether fingerprint and finger vein images were captured by different or the same biometric devices. It is not a requirement that the various measures be mathematically combined in any way because biometric traits remains independent from each other, which results in higher accuracy when identifying a person.

III. NEED FOR MULTI-MODAL BIOMETRIC SYSTEMS FOR HUMAN IDENTIFICATION

Every biometric system identifies a person by who the person is rather than what the person carries, unlike most traditional authorization systems such as personal identification numbers (PINs), passwords, or ID cards. Unlike these solutions that rely on "what you have," biometric credentials cannot be lost, forgotten, guessed, or easily cloned. Despite these advantages, the technology has some limitations too:

a. **Environment:** The environment in which biometric data is captured may have an effect on the ability of the system to identify an individual. For example, the accuracy of facial recognition is affected by illumination, pose, and facial expression.
b. **Noise in sensed data:** A fingerprint with a scar and voice altered by a cold are examples of noisy inputs. Noisy data could also result from defective or improperly maintained sensors
c. **Intra-class variations:** Fingerprint data acquired from an individual during authentication may be very different from data used to generate the template during enrolment due to a misplacement of the finger on a capture device, thereby affecting the matching process.
d. **Non-universality:** Some people cannot physically provide a standalone biometric credential due to illness or disabilities.
e. **Spoof attacks:** An impostor may attempt to spoof the biometric trait of a legitimately enrolled user in order to circumvent the system.

In each of these scenarios, a unimodal biometric system captures and matches only one biometric trait resulting in an absence of sustainable ways to solve these problems. Some of the limitations imposed by unimodal biometric systems can be overcome by using multiple biometric modalities. Such systems, known as multi-modal biometric systems, are expected to be more reliable due to the presence of multiple, independent biometric traits.

IV.IMPLEMENTATION OF A MULTI-MODAL BIOMETRIC IDENTIFICATION MANAGEMENT SYSTEM

a. Implementing a multi-modal biometric identification management system offers these additional benefits:
b. The accuracy of identifying a person increases significantly when multimodal biometrics are used. It's highly unexpected that, multiple forms of biometrics will be affected by the aforementioned conditions in which it has been captured.
c. The same concept applies to noisy data and intra-class variations that can be rectified with through the use of multiple biometric data credentials for authentication.
d. Multimodal biometric systems address the problem of non-universality, since capturing multiple biometric traits can ensure sufficient population coverage.
e. Multimodal biometric systems provide anti-spoofing measures by making it difficult for an intruder to simultaneously spoof the multiple biometric traits of a legitimate user.

V.ADVANTAGES OF A MULTI-MODAL BIOMETRIC SYSTEM

The advantages of multi-modal biometric system include:

a. **Accuracy:** Multi-modal biometric uses multiple modalities to identify a person which ensures higher accuracy.

b. **Security:** Multi-modal biometric systems increase the level of security by eliminating any chance of spoofing. It is unlikely that a person would be able to spoof multiple types of biometric traits at once.

c. **Liveness Detection:** Multi-modal biometric systems ask end users to submit multiple biometric traits randomly which ensures strong liveness detection to protect from spoofing or hackers.

d. **Universality:** A multimodal biometric system is universal in nature, even if a person is unable to provide a form of biometric due to disability or illness, the system can take other form of biometric for authentication.

e. **Cost-effective:** Multimodal biometric systems are cost effective by providing higher levels of security to lessen the risk of breaches or criminal attacks.

VI.METHODOLOGY FOR MULTIMODAL BIOMETRIC USING FUSION BY FUZZY LOGIC DECISION

The verification performance based on a biometric is affected by external conditions. For example, face identification performance may degrade when the lighting is too bright or too dark, or when the input facial image for verification is posed at an angle or carries an expression that differs from the enrolment images (see Figures 1a to 1d). Similarly, fingerprint verification performance may degrade if the input fingerprint image is off-centered, faded due to dry fingers or pressing too lightly, or smudged due to sweat or pressing too hard (see also Figures 1e to 1h). Speaker verification performance may also degrade if the input utterances are drowned out by ambient noise, if the speaker's voice characteristics have changed since enrolment (e.g. due to a sore throat or cold) or if the speaking styles between the enrolment and verification utterances are different. It may be difficult to precisely quantify these external conditions and their effects on verification performance. Hence we attempt to incorporate these conditions by the use of a fuzzy logic framework [1, 2] for multi-biometric fusion. Fuzzy logic enables us to process imprecise information in a way that resembles human thinking, e.g. big versus small, high versus low, etc., and allows intermediate values to be defined between true and false by partial set memberships. As an initial step, we consider fuzzy variables and fuzzy sets in a fuzzy inference system for face and fingerprint images. Application to speech will be pursued as a next step.

A.Fuzzy Inference System

The fuzzy inference system adjusts the weighting for each biometric as affected by the external conditions described above. There are 2 *output* fuzzy variables, w_{face} and w_{finger}, which correspond to the weightings for face and fingerprint verification respectively. Their values range from 0 to 1, with higher values implying higher confidence. The fuzzy sets of both output variables are triangular membership functions (see Figure 2) that define three levels of output weighting (high/medium/low) for each biometric. Defuzzification uses a standard centroid-of-area technique.

The Figure 1: Face identification may be adversely affected by different lighting conditions between enrolment and verification, e.g. (a) medium brightness indoors; (b) dark environment indoors; (c) medium brightness outdoors; (d) bright environment with angled pose, outdoors. Fingerprint identification may also be adversely affected by mismatches in conditions under which the fingerprint image is captured, e.g. (e) a normal image; (f) faded image due to dryness or low pressure; (g) smudged image due to sweat or high pressure; (h) off-centered image due to improperly placed finger.

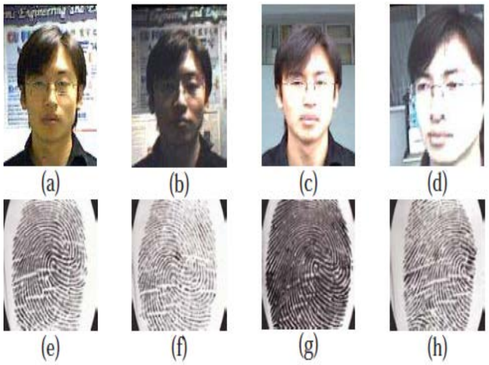


Fig.1 Face Identification Performance

There are 6 *input* fuzzy variables – two for the face biometric and four for the fingerprint. Each input variable has a fuzzy set that defines the *favored external condition* for each variable. As seen in Figure 3, the fuzzy sets are either linear or Gaussian combination membership functions *f(x)*. The latter combines two Gaussian functions to determine the shape of the left-most and right-most curves and involve such parameters as the means (*m*) and variances (σ*)* of the data, as well as the boundary points *c1* and *c2* which may be set at set using *m-0.5σ*□and *m+0.5σ*□respectively (see Equation 1). The *unfavored external condition* for each input fuzzy variable is can be represented by the fuzzy set *1-f(x).* We list the six input fuzzy variables as follows (see Figures 3a to 3f):

(i)FaceFindingConf is the face finding confidence obtained from FaceIt and has five discrete levels at (0, 2.5, 5, 7.5, 10).

Higher input levels represent higher confidence in face detection. A triangular membership function is applied seek high confidence in face finding.

(ii) Illuminance measures the average intensity of the face image. High/low input values are caused by bright/dark environments. The Gaussian combination membership function in Figure 3b defines medium brightness as a favoured condition for face images captured indoors by a web camera.

(iii) CorePosX is the x-coordinate of the fingerprint image core obtained from the fingerprint verification software. The membership function in Figure 3c defines a centrally placed fingerprint image which is favored. High/low values for CorePosX implies an off-centered image.

(iv) CorePosY is the y-coordinate of the fingerprint image. Other properties are similar to (iii).

(v) Darkness measures the proportion of dark pixels with intensities ≤30. Larger values imply darker images due to smudging. Small values are favored as normal images.

(vi) Low-clarity measures the proportion of light pixels with intensities between 110 and 160. Larger values imply faded images and therefore low values are favored by the membership function for clarity. Non-uniform pressure in the fingerprint image may result in high values for *Darkness* and *Low-clarity*.

$$f(x) = \begin{cases} e^{\frac{-(x-c_1)^2}{2\sigma^2}} & \text{, if } x < c_1 \\ 1 & \text{, if } c_1 \le x \le c_2 \\ e^{\frac{-(x-c_2)^2}{2\sigma^2}} & \text{, if } x > c_2 \end{cases}$$

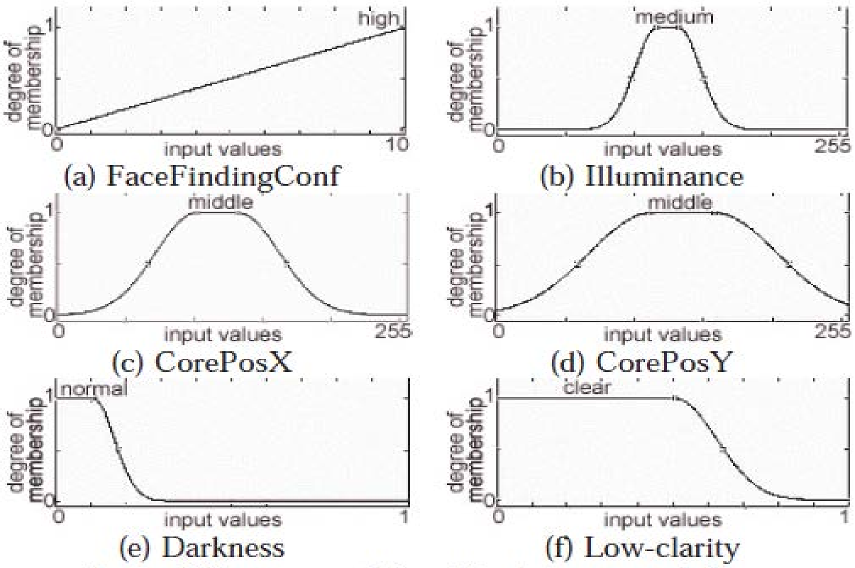
Figure 2: Fuzzy sets for the output fuzzy variables, W_{face} and $W_{fingerprint}$, corresponding to the weightings of the face and fingerprint biometrics.

B.Fuzzy Rules

The conditions that comprise the fuzzy logic are formulated by two groups of fuzzy IF-THEN rules (20 in all). One group controls the output variable *wface* (i.e. weighting for the face biometric) according to values of the input variables *FaceFindingConf* and *Illuminance*. The other group controls the output variable *wfinger* (i.e. weighting of fingerprint verification) according to the values of the input variables *CorePosX, CorePosY, Darkness* and *Low-clarity*. Main properties in the fuzzy rules are:

1. if all external conditions (input variables) are favorable, the output variable is set to high;
2. if one of the conditions are unfavorable, the output variable is set to medium;
3. multiple unfavorable conditions will map the output to low.

An example fuzzy rule for face identification is:
IF (FaceFindingConf is high) and (Illuminance is medium)THEN (wface is high).



(a) FaceFindingConf (b) Illuminance

(c) CorePosX (d) CorePosY

(e) Darkness (f) Low-clarity

Figure 3: Fuzzy sets defined for the input variables.

VII.CONCLUSION

Multimodal biometrics are actually a fusion of unimodal biometrics designed to overcome the problems a single modality may cause such as noisy data, interclass similarities, intra class variation, non-universality, and spoofing. To date, many multi-modal biometric systems have been designed for individual authentication but not all are suitable for every environment. There is no one-size-fits-all solution, ultimately the selection of appropriate modalities, the choice of acceptable fusion levels, and redundancy in extracted features are some of the vital features to ensure the success of a multi-modal biometric system for human identification.

REFERENCES

[1] M.X. He, S.J. Horng, P.Z. Fan, R.S. Run, R.J. Chen, J.L. Lai, M.K. Khan and K.O. Sentosa, “Performance Evaluation of Score Level Fusion in Multimodal Biometric Systems”, Journal of Pattern Recognition, Vol. 43, No. 5, 2010, pp. 1789-1800.

[2] A. Ross, and A.K. Jain, “Fusion Techniques in Multibiometric Systems”, from Face Biometrics for Personal Identification. In. R.I. Hammound, B.R. Abidi and M.A. Abidi (eds.), Publisher Springer Berlin Heidelberg, 2007, pp. 185-212.

[3] A. Jaina, K. Nandakumara, A. Ross, and A. Jain, “Score Normalization in Multimodal Biometric Systems”, Journal of Pattern Recognition, Vol. 38, 2005, pp. 2270.

[4] Z. Pan, G. Healey, M. Prasad, and B. Tromberg, “Face Recognition in Hyperspectral Images”, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 25, No. 12, 2003, pp. 1552–1560.