NATIONAL CONFERENCE ON EMERGING TRENDS IN INTELLIGENT COMPUTING AND COMMUNICATION
APRIL 13-14, 2012

A Review on Biometric Recognition Systems

Prashant Kumar Gautam
B.Tech (IT) student,
Dronacharya College of Engg.
GreaterNoida, India
prashantgautam2626@yahoo.com

Akhilesh Dwivedi
Assistant Professor
Department of IT,
Dronacharya College of Engg.
Greater Noida , India
dwivedian5@gmail.com

Abstract
Biometric is a modern day technique to establish an authenticated access to a legitimate person in a service. Examples of such applications include secure access to buildings, computer systems, laptops, Cellular phones and ATMs.But this system somewhere fails to address the error of proper authenticated access because of a single biometric is inadequate due to few problems like noisy observed sample, dependency on contextual information etc, therefore focus should be on multimodal biometric system.
Keywords- biometric, authenticated access, multimodal biometric system

1. INTRODUCTION

It works by recognizing the features of person based on the physical or behavioral
characteristics. By using biometric system we can establish an identity based on 'who she is?' and not on 'what she possesses?'.[5]
Although the use of human characteristics has been done over a long period of time.
But Alphonse Bertillon, chief of the criminal identification division of the police department in Paris, started using the fingerprints of criminals to identify them, soon this trend was followed by other parts of the world as well to identify criminals.
Any biological characteristic can be used in biometric if it fulfils the following rules:

- Universality: each person should have the characteristic.
- Distinctiveness: any two persons should be sufficiently different in terms of the
characteristic.
- Permanence: the characteristic should be sufficiently invariant (with respect to the
matching criterion) over a period of time.
- Collectability: the characteristic can be measured quantitatively.

2. BIOMETRIC SYSTEMS

Depending upon context the biometric system can operate in two modes either in identification mode or in verification mode.
Identification mode: In this mode the system compares the users identity with the 'n' number of templates stored in the database, if the match is found the result says 'users identity' otherwise it says 'user non identified'. It is basically a one to many comparisons and the aim of this comparison is to prevent a one person using multiple identities.
Verification mode: In this mode the system compares an individual's claim usually via PIN, name or smart card. If the users identified system shows 'true' else 'false'. It is a one to one comparison and the aim of this is to prevent many users use one identity.[1]

The verification method to recognize is: given an input vector $\boldsymbol{X_Q}$ (extracted from the biometricdata) and a claimed identity $\boldsymbol{I}$, determine if $(\boldsymbol{I}, \boldsymbol{X_Q})$ belongs to class W_1 or W_2 , where W_1 indicates that the claim is true (a genuine user) and W_2 indicates that the claim is false (an impostor). Typically,$\boldsymbol{X_Q}$is matched against $\boldsymbol{X_I}$, the biometric template
Corresponding to user, to determine its category. Thus

$$(\boldsymbol{I},\boldsymbol{X_Q}) \in \begin{cases} W1, IF\ S(XQ, XI) \geq t \\ W2, Otherwise \end{cases}$$

Where$\boldsymbol{S}$ is the function that measures the similarity between feature vectors $\boldsymbol{X_Q}$ and $\boldsymbol{X_I}$, and is a predefined threshold. The value$\boldsymbol{S\ (\ X_Q\ ,\ X_I)}$ is termed as a similarity or matching score between the biometric measurements of the user and the claimed identity. Therefore, every claimed identity is classified into W_1 or W_2 based on the variables $\boldsymbol{X_Q}$, $\boldsymbol{X_I}$,$\boldsymbol{I}$ and the function $\boldsymbol{S}$. Note that biometric measurements (e.g., fingerprints) of the same

ISBN: 9788175157262

individual taken at different times are almost never identical.
This is the reason for introducing the threshold.

The identification problem, on the other hand, may be stated as follows. Given an input feature vector X_Q, determine theidentityI_k ,$k \in \{1,2,3 \ldots, N, N+1\}$Here I_1, $I_2 \ldots$ I_N arethe identities enrolled in the system and I_{N+1}indicates the rejectcase where no suitable identity can be determined for the user. Hence

$$XQ \in \begin{cases} Ik, \max S(XQ, XIk) \geq t, k = 1,2, \ldots\ldots, n \\ In+1, \quad otherwise \end{cases}$$

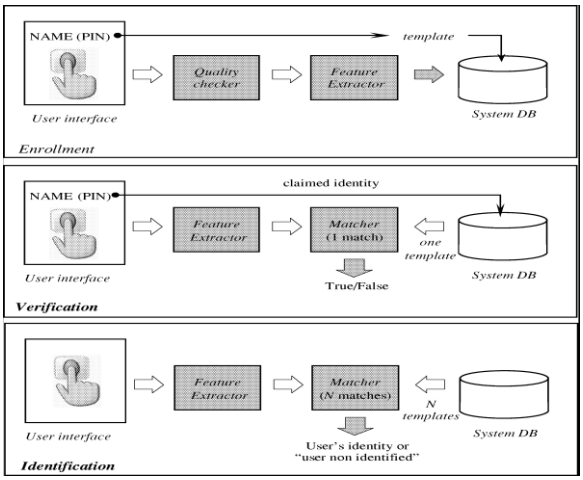
Where$X_{Ik}$is the biometric template corresponding to identityI_k, and $t$is a predefined threshold.

A biometric system has four major modules which are:

1) Sensor module: this captures the biometric data from an individual like fingerprints ridges etc.
2) Extractor module: this extracts the discriminatory features from the sensored data like the position and orientation of minutiae points (local ridge and valley singularities) in a fingerprint image are extracted in the feature extraction module of a fingerprint-based biometric system.
3) Matcher module: in this the extracted data is compared with the already stored templates in the database. Example For example, in the matching module of a fingerprint-based biometric system, the number of matching minutiae between the input and the template fingerprint images is determined and a matchingscore is reported. The matcher module also encapsulates a decision making module, in which a user's claimed identity is confirmed (verification) or a user's identity is established (identification) based on the matching score.
4) Database module: this module is the brain of the system. All the templates are stored here which are already enrolled in the system. Depending on the application the templates can be stored in the central database or in a smart card issued to the individual.

There are some errors related to the biometric system. No two samples of a same characteristic can be same due to different reasons like imperfect imaging conditions, changes in the users physiological or behavioral characteristics, ambient conditions, improper interaction of user with sensor. Therefore the response of the matching score$S(X_Q, X_1)$ will be low. If the value of the matching score is greater than or equal to the threshold value$t$. Pairs of samples generating value greater than t are called 'mate' pairs and those which doesn't are called 'non-mate'. The distribution of scores generated from pairs of samples from the same person is called the genuine distribution and from different persons is called the impostordistribution.

ISBN: 9788175157262



3. ERRORS

There are two types of errors that biometric verification system makes:

I. Mistaking biometric data from to persons to be from one (this is called 'false match').

II. Mistaking biometric data from one person to be from two different persons (this is called 'false non-matching').

These two types of errors are often called as 'false accept' and 'false reject' respectively.

There is tradeoff in FNMR (false non match rate) and FMR (false match rate). These are related to threshold value ***t.*** As the value of ***t*** decreases FMR increases and with ***t*** increases FNMR increases. The system performance at all the operating points (thresholds) can be depicted in the form of a receiver operating characteristic (ROC) curve. A ROC curve is a plot of FMR against (1-FNMR) or FNMR for various threshold values ***t.***

Mathematically the errors can be formulated as follows:

If the stored biometric template of the user ***I*** is represented by X_1 and the acquired input for recognition is represented by X_Q, then the null and alternate hypotheses are:

h_0 input X_Q does not come from the same person as the template X_1;

h_1 input X_Q comes from the same person as the template X_1.

The associated decisions are as follows:

D_0 person is not who she claims to be;

D_1 person is who she claims to be.

Hypothesis testing formulation inherently contains two types of errors.

Type I: false match (D_0 is decided when is h_0 true);

Type II: false non-match (D_1 is decided when is h_1 true).

FMR is the probability of type-I error (also called significance level in hypothesis testing) and FNMR is the probability of type-II error as

$$FMR = P(D_1 \mid h_0)$$
$$FNMR = P(D_0 \mid h_1)$$

There are two more error rates one is FTC (fail to capture), this error only occurswhen there is automatic capture system is implemented. Other one is FTE (fail to enroll). This is the percentage of times when user is not enabling to enroll itself. The accuracy of system in identification mode can be acquired by using the system accuracy in verification mode as follows:

Let us denote the identification false non-match and false match rates with $FNMR_N$and FMR_N, respectively, where N represents the number of identities in the system database (for simplicity, we assume that only a single identification attempt is made per subject, a single biometric template is used for each enrolled user, and the impostor scores between different users are uncorrelated).

ISBN: 9788175157262

Then,$FNMR_N$ =~ FNMRand FMR_N = 1-(1-FMR) N=~ N. FMR (the approximations hold well only when N. FMR < 0.1). [2] and [3]

If the templates of the identification system database are already indexed then only a portion of the database is searched for identification system. The formula is follows:

• $FNMR_N$ = RER + (1 – RER). FNMR, where RER (retrieval error rate) is the probability that the database template corresponding to the searched finger is wrongly discarded by the retrieval mechanism. The above expressionism obtained using the following argument: in case the template is not correctly retrieved (this happens with probability RER), the system always generates a false-non-match, whereas in case the retrieval returns the right template [this happens with probability (1-RER)], false non-matchrate of the system is FNMR. [4]

• FMR_N = 1-(1-FMR)$^{N.P}$, where P (also called thepenetration rate) is the average percentage of database searched during the identification of an input fingerprint.

The accuracy requirements of the system depend on the application type. For example in the case of criminal identification the major role is played by FNMR and not by FMR. In the case of high secure access control application major role is played by FMR.

Although in many civilian applications both FMR and FNMR are required such as: In the case of ATM system if the FMR will be low than there will be a loss of several rupees and if FNMR will be high than customer will not be able to gain access to his money .

There are two types of biometric systems:

- Uni-modal: In this type of modal there is single biometric is used to verify or identify a person. Examples fingerprints, iris, face.
- Multimodal: in this type of modal multiple biometric features are used at once to have more authenticated access to user. Examples fingerprint, iris, face together.

4. Different biometric features:

• Face: Face recognition is a nonintrusive method, and facial images are probably the most common biometric characteristic used by humans to make a personal recognition. The applications of facial recognition range from a static, controlled “mug-shot” verification to a dynamic, uncontrolled face identification in a cluttered background (e.g., airport). The most popular approaches to face recognition are based on either: 1) the location and shape of facial attributes such as the eyes, eyebrows, nose, lips and chin, and their spatial relationships, or 2) the overall (global) analysis of the face image that represents a face as a weighted combination of a number of canonical faces.

• Fingerprint: Humans have used fingerprints as identification resource since a long period of time. In fact they have proven to be very accurate in matching. The accuracy of the current available fingerprint scanners systems is adequate. There is one problem that fingerprint scanners require large amount of computational resources, especially in identification mode.

• Retinal scan: The retinal vasculature is rich in structure and is supposed to be a characteristic of each individual and each eye. It is claimed to be the most secure biometric since it is not easy to change or replicate the retinal vasculature. The image acquisition requires a person to peep into an eye-piece and focus on a specific spot in the visual field so that a predetermined part of the retinal vasculature could be imaged. The image acquisition involves cooperation of the subject, entails contact with the eyepiece, and requires a conscious effort on the part of the user.

• Iris: The iris is the annular region of the eye bounded by the pupil and the sclera (white of the eye)

ISBN: 9788175157262

on either side. The visual texture of the iris is formed during fetal development and stabilizes during the first two years of life. The complex iris texture carries very distinctive information useful for personal recognition. The accuracy and speed of currently deployed iris-based recognition systems is promising and point to the feasibility of large-scale identification systems based on iris information. Each iris is distinctive and, like fingerprints, even the irises of identical twins are different.

5. Levels of fusion:

There is need of using multimodal biometric system as to ensure a continuous authenticated access to a user in case any one or two features fail to verify.

There are two levels of fusion:

- **Pre-classification: In** this level of fusion the information from the user is gathered prior to apply any matching algorithm [6]. It is further classified into two categories one is sensor level and other one is feature level. Since the sensor level and feature level data set contains information about input biometric data than the output therefore these provides better verification results. however fusions at these levels are hard to achieve due to:
- Data overload.
- The chances noise interruption is more at sensor level. [6]
- The feature sets of the various modalities may be incompatible.
- Most commercial biometric systems do not allow access to feature sets.

- **Post classification level**: In this level the information is gathered post to application of matching algorithm. [6]. It can further be divided into four categories classifier selection level, decision level, rank level and matching score level. [6]. Classifier selection level can choose the best classifier result. In rank level fusion biometric results are stored in accordance to their confidence levels. Fusion at decision level is rigid due to limited information, the decision is taken generally by logical AND, OR majority voting rule. Fusion at the match score level is usually preferred because it is easy to access and combine the scores presented different modalities.

VI. Biometric systems have different applications in today's time vise:

1. **Commercial**: applications such as computer network login, electronic data security, e-commerce, Internet access, ATM, credit card, physical access control, cellular phone, PDA, medical records management, and distance learning.
2. **Government** applications such as national ID card, correctional facility, driver's license, social security, welfare disbursement, border control, and passport control.
3. **Forensic** applications such as corpse identification, criminal investigation, terrorist identification, parenthood determination, and missing children.

REFERENCES

[1]J. L. Wayman, "Fundamentals of biometric authentication technologies,"Int. J. Image Graphics, vol. 1, no. 1, pp. 93–113, 2001.

[2] Best Practices in Testing and Reporting Performance of Biometric Devices, Version 2.01. U. K. Biometric Work Group (UKBWG). [Online]. Available:http://www.cesg.gov.uk/technology/biometrics/

[3] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain"FVC2002: Fingerprint verification competition," in Proc. Int. Conf.Pattern Recognition (ICPR), Quebec City, QC, Canada, Aug. 2002, pp. 744–747.

[4] R. Cappelli, D. Maio, and D. Maltoni, "Indexing fingerprint databasesfor efficient 1:N matching," in Proc. 6th Int. Conf. Control AutomationRobotics and Vision, 2000.

ISBN: 9788175157262

[5] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometricrecognition:Securityand privacy concerns," IEEE Security Privacy Mag., vol. 1, no. 2, pp. 33–42, 2003.

[6] Anil jain ,KarthikNandkumar , and Arun Ross, " Score normalization in multimodal biometric systems "Pattern Recognition 38 (2005) 2270 2285

[7] R. Brunelli and D. Falavigna, "Person identification using multiplecues," IEEE Trans. Pattern Anal. Machine Intell., vol. 12, pp. 955–966, Oct. 1995.

[8] E. S. Bigun, J. Bigun, B. Duc, and S. Fischer, "Expert conciliation formultimodal person authentication systems using bayesian statistics," in Proc. Int. Conf. Audio and Video-Based Biometric Person Authentication(AVBPA), Crans-Montana, Switzerland, Mar. 1997, pp. 291–300.

[9] R. W. Frischholz and U. Dieckmann, "Bioid: A multimodal biometricidentification system," IEEE Comput., vol. 33, pp. 64–68, 2000.

[10] T. K. Ho, J. J. Hull, and S. N. Srihari, "Decision combination in multipleclassifier systems," IEEE Trans. Pattern Anal. Machine Intell., vol. 16 pp. 66–75, Jan. 1994.

[11] J. Kittler, M. Hatef, R. P. W. Duin, and J. Matas, "On combining classifiers,"IEEE Trans. Pattern Anal. Machine Intell., vol. 20, pp. 226–239,Mar. 1998.

[12] S. Prabhakar and A. K. Jain, "Decision-level fusion in fingerprint verification,"Pattern Recognition., vol. 35, no. 4, pp. 861–874, 2002

ISBN: 9788175157262