© 2014 IJIRT | Volume 1 Issue 6 | ISSN : 2349-6002

Palm Print Identification System Using Haralick Features

Kuldeep Yadav,Atul Kumar,Kunal Taneja

Student, Department of ECE, Dronacharya College of Engineering, Gurgaon, India

Abstract: **To confirm or determine the identification of an individual, different types of systems are used depending upon the area in which it is used. The purpose of each system is to ensure that the service is provided to the only the legitimate user. Examples of such applications include secure access to buildings, computer systems, laptops, cellular phones and ATMs. Knowledge-based and token-based person recognition rely on surrogate representations of identity such as passwords or ID cards, which can be easily forgotten/lost, guessed/stolen, or shared. Moreover, they cannot provide vital identity management functions like nonrepudiation and detecting multiple enrollments by the same person under different identities. For example, individuals can easily deny (repudiate) using a service by claiming that their password had been stolen or guessed. Individuals can also conceal their true identity by presenting forged or duplicate identification documents. In addition, traditional mechanisms like passwords and tokens do not provide strong evidence for post-event person recognition, such as suspect identification at a crime scene. Therefore, it is becoming increasingly apparent that knowledge-based and token-based mechanisms alone are not sufficient for reliable identity management. Since the biometric identifiers are inherent to an individual, it is more difficult to manipulate, share, or forget these traits. Hence, biometric traits constitute a strong and reasonably permanent link between a person and his identity. Identity theft or identity fraud occurs when a person usurps the identity of another individual or claims a false identity in order to access resources or services to which he is not entitled.**

I. INTRODUCTION

The ability to identify individuals uniquely and to associate personal attributes with individuals has been crucial to the fabrics of the human society. Humans typically use body characteristics such as face, voice and gait along with other contextual information like location and clothing to recognize each other. The set of attributes associated with a person constitutes their personal *identity*. However, an explosion in population growth accompanied by increased mobility in modern society has necessitated the development of sophisticated identity management systems that can efficiently record, maintain and obliterate personal identities of individuals. Identity management plays a critical role in a number of applications. Examples of such applications include regulating international border crossings, restricting physical access to important facilities like nuclear plants or airports, controlling logical access to shared resources and information, performing remote financial transactions, or distributing social welfare benefits.

A wide variety of such application requires reliable personal recognition schemes (which we call (**Biometric System**) to either confirm or determine the identity of an individual requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user and no one else. Examples of such applications include secure access to

buildings,computer systems, laptops, cellular phones, and ATMs. In the absence of robust personal recognition schemes, these systems are vulnerable to the wiles of an impostor.

Biometric System:

A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. Normally, personal characteristics such as fingerprints or palm prints geometry are obtained through a sensor and fed into the pattern recognition engine to return a result of success or failure. Fig 1 shows the architecture of a typical biometric system. In general, biometric systems consist of the following four stages:

1) Data acquisition

2) Signal/Image preprocessing

3) Feature extraction

4) Feature matching

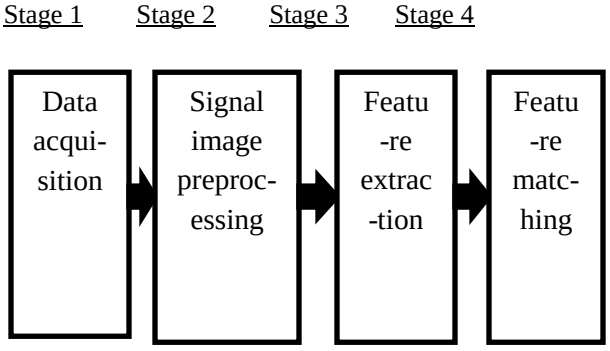

Figure1: Flow diagram of biometric system

1) ***Data acquisition*** – Biometric data (signal/image) is obtained from an input device. The quality of signals is very important since they form the raw input for subsequent processing.

2) ***Signal/Image preprocessing*** – Enhancement of the signal/image is performed in this stage, including segmentation, noise reduction, and rotation and translation normalization.

3) ***Feature extraction*** – The features defined possess the stable and unique properties of
low intra-class difference and high inter-class difference. These features are used to
create a master template which is stored in the system database.

4) ***Feature matching*** – A matching score is obtained by matching the identification
template against the master templates. If the score is less than a given threshold, the
user is authenticated.

Characteristics for Biometric:

Any human physiological and/or behavioral characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

- 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. However, in a practical biometric system (i.e., a system that employs biometrics for personal recognition), there are a number of other issues that should be considered.
- Performance: Refers to the achievable recognition accuracy and speed, the Resources required to achieve the desired recognition accuracy and speed,

Verification mode:

The system validates a person's identity by comparing the captured biometric data with her own biometric template(s)[4] stored in the system database. In such a system, an individual who desires to be recognized claims an identity, usually via a personal identification number (PIN), a user name, or a smart card, and the system conducts a one-to-one comparison to determine whether the claim is true or not (e.g., "Does this biometric data belong to Bob?"). Identity verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity.

Identification mode:

The system recognizes an individual by searching the templates of all the users in the
database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual's identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an identity (e.g., "Whose biometric data is this?"). Identification is a critical component in negative recognition applications where the system establishes whether the person is who she (implicitly or explicitly) denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities.

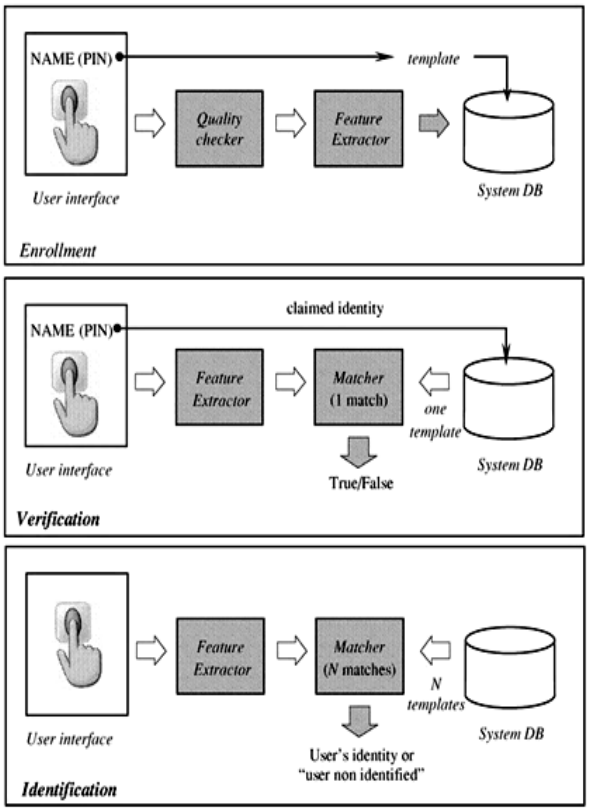

Figure 2: Schematic Diagram of verification & identification modes

Haralick Features :

Haralick introduced 14 statistical features[3][8] which are basically texture features which can be extracted from a matrix.

The texture features are:

- Angular Second Moment
- Contrast
- Inverse Difference moment
- Entropy
- Correlation
- Variance
- Sum Average
- Sum Entropy
- Difference Entropy
- Inertia
- Cluster Shade
- Cluster Prominence

The important are :

Contrast: The relative difference between light and dark areas of an image. Contrast is how dark to how light something is. Contrast makes the lighter colors more lighter, andthe darker colors darker.

$$CONTRAST = \sum_{n=0}^{G-1} n^2 \{ \sum_{i=1}^{G} \sum_{j=1}^{G} P(i,j) \}, \quad |i-j| = n$$

Where P is GLCM matrix ad G is Grey-Scale value

Entropy: It can be described as a measure of the amount of disorder in a system. In the case of an image, entropy is to consider the spread of states which a system can adopt.

A low entropy system occupies a small number of such states, while a high entropy system occupies a large number of states. For example, in an 8-bit pixel there are 256 such states. If all such states are equally occupied, as they are in the case of an image which has been perfectly histogram equalized, the spread of states is a maximum, as is the entropy of the image. On the other hand, if the image has been thresholded, so that only two states are occupied, the entropy is low. If all of the pixels have the same value, the entropy of the image is zero.

$$ENTROPY = -\sum_{i=0}^{G-1} \sum_{j=0}^{G-1} P(i,j) \times log(P(i,j))$$

Where P is GLCM matrix ad G is Grey-Scale value.

Variance : The variance is a measure of how far a set of numbers is spread out. It is one of several descriptors of a probability distribution, describing how far the numbers lie from the mean (expected value).

$$VARIANCE = \sum_{i=0}^{G-1} \sum_{j=0}^{G-1} (i-\mu)^2 P(i,j)$$

Where P is GLCM matrix ad G is Grey-Scale value, mu is mean value.

Correlation : Measure that determines the degree to which two pixel values are associated.

$$CORRELATION = \sum_{i=0}^{G-1}\sum_{j=0}^{G-1} \frac{\{i \times j\} \times P(i,j) - \{\mu_x \times \mu_y\}}{\sigma_x \times \sigma_y}$$

Where P is GLCM matrix ad G is Grey-Scale value, mu-x, mu-y are mean values & sigmax, sigma-y are standard deviations along X and Y axis.

$$\mu_x = \sum_{i=0}^{G-1} i \sum_{j=0}^{G-1} P(i,j)$$

$$\mu_y = \sum_{}^{G-1}\sum_{}^{G-1} jP(i,j)$$

$$\sigma_x^2 = \sum_{i=0}^{G-1}(i-\mu_x)^2 \sum_{j=0}^{G-1} P(i,j)$$

$$\sigma_y^2 = \sum_{j=0}^{G-1}(j-\mu_y)^2 \sum_{i=0}^{G-1} P(i,j)$$

Performance:

The performance of a biometric system is measured by following metrics:

Genuine Acceptance Rate (GAR) : It tells what percentage of genuine user will be authorized during authentication. If GAR[11][5][4] is 98% that means out of 100, 98 genuine user will be accepted and 2 will be rejected falsely. We define GAR in terms of FRR[5] i.e. False Rejection Rate.

GAR=1-FRR

FRR= Genuine attempts that generate comparison score below threshold ÷ Total genuine attempts.

False Acceptance Rate(FAR) : It tells what percentage of fake/imposter user will be authorized during authentication. If FAR[11][5][4] is 5% that means out of 100, 5 imposter will be accepted falsely.

FAR = Imposter attempts that generate comparison score above threshold ÷ Total imposter attempts.

For a biometric to be useful, it must have high GAR and low FAR.

If we plot the distribution of Scores of imposter and genuine (Fig. 4) users we get a curve that is distributed about the mean of the match score. Theoretically these 2 curve should not cross each other because theoretically no imposter should be accepted as genuine and no genuine should be rejected as an imposter. But practically they intersect and hence cause GAR and FAR.

Reasons for not 100% GAR are : No proper scanning, cuts or burns on the palm, change of palm features over a long period of time.

Reasons for having FAR are : Not good algorithms that can determine if a little difference is there or not in the palm images of genuine and imposter.

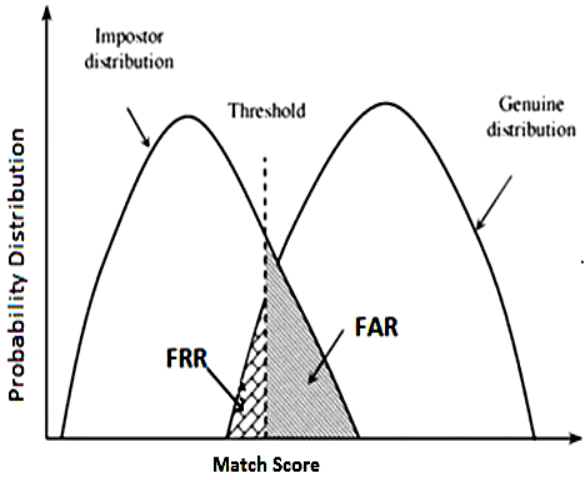

Figure 3: Distribution graph showing FAR &FRR

Matching of Images:

For matching of two images we used formula. Given the two images X & Y and A & B are feature vector are calculated from Haralick formulas. Matching Score[10] is Calculated as follows:

Matching Score = 1 - Norm(X-Y)/ (Norm (X) + Norm (Y))

Where Norm is the Euclidean Norm which is the square root of the summation of square of the values i.e. If Vector P is [x y z] then Euclidean Norm [10] is :

Norm (P) = $\sqrt{x2+y2+z2}$

References:

1. Albregtsen, Fritz. "Statistical texture measures computed from gray level coocurrence matrices." *Image Processing Laboratory, Department of Informatics, University of Oslo* (1995).

2. Eleyan, Alaa, and Hasan Demirel. "Co-occurrence based statistical approach for face recognition." *Computer and Information Sciences, 2009. ISCIS 2009. 24th International Symposium on*. IEEE, 2009.

3. Haralick, Robert M., Karthikeyan Shanmugam, and Its' Hak Dinstein. "Textural features for image classification." *Systems, Man and Cybernetics, IEEE Transactions on* 6 (1973): 610-621.
4. Jain, Anil K., Arun Ross, and Salil Prabhakar. "An introduction to biometric recognition." *Circuits and Systems for Video Technology, IEEE Transactions on* 14.1 (2004): 4-20.
5. Biometrics Metrics Report v3.0, U.S. Military Academy(USMA) – west point.
6. Kekre, H. B., et al. "Image Retrieval using Texture Features extracted from GLCM, LBG and KPE." *International Journal of Computer Theory and Engineering* 2.5 (2010): 1793-8201.
7. du Buf, JM Hans, M. Kardan, and Michael Spann. "Texture feature performance for image segmentation." *Pattern recognition* 23.3 (1990): 291-309.
8. Haralick, Robert M., Karthikeyan Shanmugam, and Its' Hak Dinstein. "Textural features for image classification." *Systems, Man and Cybernetics, IEEE Transactions on* 6 (1973): 610-621.
9. He, Dong-Chen, Li Wang, and Jean Guibert. "Texture feature extraction."*Pattern recognition letters* 6.4 (1987): 269-273.
10. Wang, Song, and Jiankun Hu. "Alignment-free cancelable fingerprint template design: A densely infinite-to-one mapping (DITOM) approach." *Pattern Recognition* 45.12 (2012): 4129-4137