AUTHENTICATION FRAMEWORKS FOR ENHANCING SECURITY IN BIOMETRIC SYSTEMS

Prof. S. BALAJI
Professor, Department of ECE, CMR Institute of Technology, India

Dr. Habibullah Khan
Professor, Department of ECE, KL University, India

Dr. M. Janga Reddy
Professor, Department of CSE, CMR Institute of Technology, India

Dr. M. Gurunadha Babu
Professor, Department of ECE, CMR Institute of Technology, India

ABSTRACT

Due to demonetization by Indian government recently, there is need for security enhancement in biometric systems present all over the country. Biometrics refers to the automatic identification of individuals based on their physiological and/or behavioral uniqueness. Although the difficulty of automatic fingerprint matching has been extensively studied, is nevertheless, not a fully solved problem. In this paper, an in order combination approach is adopted to address some of the limitations of existing fingerprint matching systems. A fusion fingerprint system that utilizes both minutiae points and ridge feature maps to signify and match fingerprint images has been developed. The fusion matcher is shown to perform extensively better than a conventional minutiae-based matcher. The ridge feature maps extracted by this method have also been used to line up and register fingerprint image pairs via a correspondence process thereby obviating the need to rely on finer points for image registration [3]. Even identical individuals having similar DNA are believed to have different fingerprints [10]. To address the problem of fractional prints obtained from small sized sensors, a fingerprint mosaicking scheme has been developed. The proposed method constructs a composite fingerprint pattern from partial fingerprint impersonation by using iterative control point algorithm that determines the makeover parameters relating the two impressions. To lessen the effect of non-linear distortions in fingerprint images on the matching process, an average warp replica has been proposed. The model is developed by comparing a fingerprint impression with several other impressions of the same finger and observing the common ridge points that occur in them. A index of twist has been suggested in this framework to aid in the selection of an
finest fingerprint impression from the set of impressions [12]. Single biometric systems perform person detection based on a single source of biometric information and are affected by troubles like noisy sensor data, non-universality and lack of uniqueness of the chosen biometric characteristic and vulnerability to circumvention. Some of these problems can be alleviated by using multimodal biometric systems that merge evidence from multiple biometric sources. Methods to combine fingerprint in sequence with the other biometric traits of a subject (viz., iris, face and signature) are presented. To improve user convenience, a learning method has been used to compute user-specific parameter in a multi biometric system, in sequence combination systems, as presented in this paper, are likely to be more dependable and strong than systems that rely on a single source of information. The general task of aliveness detection is to detect whether a biometric probe (e.g. a fingerprint) belongs to a living subject that is present at the point of biometric detain. Using aliveness detection methods, a reliable recognition of deceased fingers or photographed faces can be established.

Key words: BIOMETRICS, Enhancement, Matching, SIKP Operator, Multimodal Biometrics, Aliveness, Detection, FAR, FRR

http://www.iaeme.com/IJMET/issues.asp?JType=IJMET&VType=8&IType=7

1. FINGERPRINT ENHANCEMENT AND MATCHING ANALYSIS

Biometric Systems make use of fingerprints, hand geometry, iris, retina, face etc. to personally identify a person [1, 2]. A common biometric system can be cast in the framework of a sample recognition system [4], summarizes the typical stages in this common system. A biometric system has two main measures: registration (enrollment) of biometric data and verification (authentication) of biometric data, which are represented as dotted lines and solid lines in Figure 1.1, respectively. The first stage of listing is to obtain the original biometric signal (typically, an image) by means of a sensor. The next stage is to remove invariant features from this unique signal to make a robust depiction for biometric data that can exclusively determine an individual.

The extracted features are store as a outline of a template. In the case of fingerprint recognition, a template contain fingerprint minutiae points. A minutiae point is a abnormal point in a fingerprint image, for example, where a ridge moreover begins or divide into two ridges [2]. A characteristic fingerprint may have tens of such points, and those points form a template exclusively determine the attribute of a specific fingerprint. Existing fingerprint recognition systems are very precise; in particular, they can give a false rejection rate of 0.01% at a false acceptance rate of 0.1% [6].
1.1. Iterative Fingerprint Enhancement
The flow-chart of the proposed approach, is composed of five main steps: i) filter-bank convolution, ii) combined image computation, iii) homogeneity image computation, iv) selection of the candidates and v) enhancement of the candidates. The input of the proposed approach is a gray-scale noisy fingerprint where the ridge flow has been segmented from the background [3]. The output consists in a binary image. Each step of the computation is explained in the following sections.

1.2. Convolution with a Gabor filter-bank
A Gabor filter is defined by a sinusoidal plane wave tapered by a Gaussian. The even symmetric two-dimensional Gabor filter has the following form:

\[
g(x, y; \theta, f) = \exp \left( -\frac{1}{2} \left[ \frac{x^2}{\sigma_x^2} + \frac{y^2}{\sigma_y^2} \cos^2(2\pi f \cdot x) \right] \right) \cos(2\pi f \cdot x \cdot \theta)
\]

Where, \( \theta \) is the orientation of the filter and \([x_0, y_0] \) are the coordinates of \([x, y]\) after a clockwise rotation of the Cartesian axes by an angle of \((90^\circ - \theta)\). Such filter depends on four parameters \((\theta, f, \sigma_x, \sigma_y)\) even if often it is used
with $\sigma_x = \sigma_y$. A Gabor filter-bank is defined as a set $G = \{g_{i,j}(x, y) | i = 1..n_\theta, j = 1..n_f\}$ of Gabor filters, where $n_\theta$ is the number of discrete orientations $\{\theta_i | i = 1..n_\theta\}$ and $n_f$ the number of discrete frequencies $\{\theta_j | j = 1..n_f\}$. Let $I$ a $h \times w$ fingerprint image, the output of the convolution between $I$ and the filter-bank $G$ is a set $V_\theta$ of $n_\theta \cdot n_f$ images where $V_{i,j} = [v_{i,j}(x,y)]$, $x = 1..w$, $y = 1..h$ denotes the response image to a filter $g_{i,j}$ with orientation $\theta_i$ and frequency $\theta_j$. Typically $n_\theta$ is set to 8 or 16 and $n_f$ in the range $[1,4]$ . To save computation time in low-cost and computation-limited fingerprint systems, the filter bank can be pre-computed.

1.3. Fingerprint Matching Analysis

A fingerprint is made up of a sequence of ridges and furrows on the surface of the finger. The individuality of a fingerprint can be indomitable by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are local ridge distinctiveness that occur at either a ridge bifurcation or a ridge ending. Fingerprint matching methods can be separated into two categories: minutiae-based and correlation based. Minutiae-based methods first find minutiae points and then map their relative position on the finger as shown in Figure 1.3.

![Figure 1.3. Matching minutiae points in two fingers](image)

Matching minutiae points in two fingerprints. Nevertheless, there are few difficulties when using this technique. It is difficult to extract the minutiae points precisely when the fingerprint is of low quality. Also this technique does not take into relation the global pattern of ridges and furrows. The correlation-based technique is able to conquer some of the difficulties of the minutiae-based approach. However, it has some of its own disadvantages. Correlation based techniques require the accurate location of a registration point and are affected by image translation and rotation. Fingerprint matching based on minutiae have dilemma in matching unregistered minutiae patterns. Local ridge structures cannot be totally characterized by minutiae. A typical fingerprint-based authentication system needs a very low False Reject Rate (FAR) for a given False Accept Rate (FAR).

2. FINGERPRINT CHECK USING SIKP OPERATOR

Fingerprint based authentication systems have gained enormous recognition due to the high level of individuality endorsed to fingerprints and the ease of use of solid fingerprint sensors that can be easily set in into a range of devices require user authentication. Fingerprints are being widely used for person identification in a quantity of commercial, civil, and forensic applications. Most of the current fingerprint verification systems utilize features that are based on minutiae points and ridge patterns. Despite the fact that minutiae based fingerprint verification systems have shown quite high accuracies, further improvement in their presentation are needed for adequate performance, particularly in applications connecting very large scale databases[4]. In an effort to extend the existing equipment for fingerprint verification, we propose a new illustration and matching scheme for fingerprint using Scale Invariant Key Points[10]. We take out uniqueness of Scale Invariant Key Points in scale space and carry out matching based on the texture in order around the feature points using SIKP operator.
systematic approach of applying Scale Invariant Key Points to fingerprint images is anticipated. We have used a public domain fingerprint database. We have shown that the SIKP operator can be used for fingerprint feature taking out and matching. We have performed fingerprint matching in two steps: i) point-wise match and ii) trim false matches with arithmetical constraints [11]. The fusion with a minutiae based matcher shows important performance development on two public domain databases. We believe the presentation development due to fusion is possible because the sources of information used in minutiae and SIKP based matchers are considerably different. SIKP shows a good likelihood of extending minutiae based or minutiae related fingerprint representation. It is possible to further improve the performance of SIKP if proper preprocessing is perform on the input image that can reduce the noise in the images. The distinctive preprocessing in minutiae based technique involve connecting broken ridges and extract skeleton of the ridge pattern, which remove all the texture information that is used in the SIKP operator[7].

3. IMPROVING SECURITY THROUGH MULTI-BIOMETRIC SYSTEMS

Multi biometric systems deal with the issue of non-universality i.e., incomplete population coverage. For example, if a person’s poor quality of fingerprints prevents him from enrolling in the system; then the use of other biometric traits such as iris, face, voice etc. will help the system acquire meaningful biometric data and enroll the user [5].

It is extremely difficult to spoof multiple biometric traits of a legitimate user. If each subsystem determines the probability of the particular trait being a spoof, it is possible to find out the probability of the user being an imposter by using an appropriate fusion technology [11]. Moreover, a challenge response mechanism can be included that asks user to present the random subset of traits (in a particular order) at the point of acquisition. This would ensure that the system is interacting with a live user.

Multibiometric systems effectively address the problem arising because of noisy data. When the information acquired from one biometric trait is corrupted by noise, it is possible to use information acquired from the other biometric trait. Some systems also take into considerations the quality of acquired input biometric signals during the fusion process [8]. Estimating the quality of acquired biometric data is in itself a challenging problem. However, if done appropriately, multibiometric systems gain significant benefits.

A multibiometric system acts as a fault tolerant system by continuing to operate even when information from certain biometric sources becomes unreliable because of sensor or software malfunctions or intentional user manipulation. Fault tolerance is usually desirable in authentication systems involving large number of subjects (for example, in border control applications).

Consolidation of evidences from multiple sources can offer substantial improvement in the accuracy of biometric systems [9]. Use of proper sources of information and the right fusion methodology determines the improvement in matching accuracy. The availability of multiple sources also increases the feature space thereby increasing the number of individuals that can be discriminated reliably. Therefore, the capacity (i.e., the number of users that can be enrolled) of an identification system can be increased.

4. LIVENESS DETECTION SYSTEMS

Liveness discovery (once in a while called imperativeness location) in a biometric framework implies the capacity for the framework to recognize, amid enlistment and ID/check, regardless of whether the biometric test displayed is alive or not. Besides, if the framework is intended to secure against assaults with fake fingerprints, it should likewise watch that the displayed
biometric test has a place with the live individual who was initially selected in the framework and an extraordinary live person. Many individuals trust that biometric frameworks can identify liveness in biometric tests [12]. A few makers of biometric framework additionally guarantee that they have liveness discovery in their framework. It has however been demonstrated that unique finger impression frameworks can be tricked with counterfeit fingerprints, that static facial pictures can be utilized to trick confront acknowledgment frameworks, and that static iris pictures can be utilized to trick iris acknowledgment frameworks. After a general depiction of the idea liveness location in biometric frameworks, this part will concentrate on liveness identification in unique mark frameworks, which strategies unique mark scanners can use to distinguish liveness, and how these unique finger impression scanners can be tricked.

Liveness recognition can be performed either at the procurement arrange, or at the handling stage. For instance, an optical unique finger impression scanner would make a picture of an eraser, yet not extricate any elements; the liveness discovery happens at the preparing stage. A capacitive unique mark sensor then again, would not make a picture of the eraser; the liveness recognition happens at the procurement arrange.

5. RESULTS AND SUMMARY

Biometric experts have invested a significant amount of effort in study fingerprints in the framework of forensics, computer vision, image processing, pattern recognition, and biometrics. This apparently simple pattern of ridges and valleys on the tip of a finger has, as a result, established considerable consideration [10]. In spite of this consideration, the difficulty of automatic fingerprint matching continues to retreat abundance of challenge. In this paper we have approach the challenge in fingerprint matching from an information fusion perception. We first developed a hybrid matcher that collective the minutiae and texture information present in a fingerprint. In the planned technique, the texture information was represented using ridge feature maps which could also be utilized to line up and register pairs of fingerprint images. The hybrid system existing here was shown to improve the matching presentation of a fingerprint system. One of the compensation of using a hybrid approach is the complementary nature of the information being combined. This aids in diminishing the false accept rate (i.e., the false match rate) as follows: by investigative the underlying ridge information via ridge feature maps after align the images using minutiae points, the reliability of the matcher is improved.

- We then describe a mosaicking scheme that integrated the information present in two impersonation of a finger. In this technique, fingerprint images were viewed as range images, and the iterative control point (ICP) algorithm was used to record them. The technique presented here utilized minutiae points to determine an initial position between image pairs. The mosaicking process resulted in a composite template which was more sophisticated than the individual images. Mosaicking is an essential component of a fingerprint system since it sophisticatedly consolidates the information available in several incomplete prints.

- We have shown that the SIKP operator can be used for fingerprint feature extraction and matching. We have performed fingerprint matching in two steps: i) point-wise match and ii) trimming false matches with arithmetical constraints. The combination with a minutiae based matcher shows significant performance enhancement on two public domain databases. We believe the performance enhancement due to fusion is possible because the sources of information used in minutiae and SIKP based are different. SIKP shows matchers are significantly good minutiae related possibility of extending minutiae based fingerprint representations.

To account for non-linear distortion in fingerprints, an "normal" warp model was proposed. In this approach ' a fingerprint impression (baseline) was compared with several other impersonation of the same finger in order to decide the "relative" non-linear deformation
present in it. The normal deformation model was developed using thin-plate splines (TPS) and ridge curves were used to ascertain correspondences between image pairs. The estimated average deformation was utilized to pre-distort the minutiae points in the template image prior to matching it with the minutiae points in the query image. The use of an regular deformation model resulted in a better alignment among the template and query minutiae points. An index of twist was also defined for choosing the deformation replica with the least variability from a set of template impressions corresponding to a finger. To conclude, the fingerprint facts of a user was united with the face, iris and signature traits to design a multi biometric system. A multi biometric system not only improves matching presentation as was demonstrated in this paper, but it also addresses the problem of non-universality and spoofing that are prevalent in single modal systems.

6. CONCLUSION AND FUTURE SCOPE:

Major efforts are currently being undertaken to join together biometrics into the framework of society (e.g., National ID card, US-VISIT program, etc.). It is, therefore, essential that researchers and practitioners methodically study the engineering aspects of biometric systems that would ensure their successful mechanism in real-world applications. The social and legal implications of biometric systems will also have to be one by one studied and understood, before deploying these systems on a great scale. We bring to a close this paper by suggesting possible ways in which due to demonetization there is always threat from hackers and attacks can happen to biometric systems and government should take necessary steps in researching on biometric systems and help the public in safety of their money transactions and create robust fingerprint (biometric) systems.

REFERENCES


