SECURE FINGERPRINT USING MOSAICING

Keerthi Priya Pulukuri[1], G Deepak Rao[1], Swathi Kandala[1], Rupali Nilaj Deshmukh[2]

[1](Student, Computer Department, Fr. C. Rodrigues Institute of Technology, Vashi / University of Mumbai, India)
[2](Assistant Professor, Computer Department, Fr. C. Rodrigues Institute of Technology, Vashi / University of Mumbai, India)

ABSTRACT: *Among all biometric traits, fingerprints have one of the highest levels of reliability and have been extensively used by forensic experts in criminal investigations. A fingerprint refers to the flow of ridge patterns in the tip of the finger. The ridge flow exhibits anomalies in local regions of the fingertip, and it is the position and orientation of these anomalies that are used to represent and match fingerprints. Fingerprints are believed to be unique across individuals, and across fingers of the same individual. There are various stages involved in fingerprinting. This paper discusses the various means of Fingerprint analysis and its methods of storage, along with a comparison between several different methods used for each different stage and finally propose a five stage fingerprinting system involving - Fingerprint Acquisition, Fingerprint Representation using Mosaicing, Storage using classification, Fingerprint Matching using Singularity Point Detection and Watermarking of Fingerprints using Discrete Wavelet Transform for security.*

In proposed system Fingerprint Mosaicing included in Fingerprint Representation to obtain an efficient query image which is used for matching because it requires less storage space. The Singularity point matching algorithm not only matches the core and delta points but also considers the orientation and thus provides an efficient matching technique and takes less time to retrieve data. Watermarking provides security to the stored query image.

Keywords- *Biometrics, Minutiae, Mosaicing, Watermark.*

I. INTRODUCTION

It is universally known, that an individual’s fingerprints represent unique and reliable identity as well as the most prominent biometric traits of them all. The ridge flow in fingerprint shows different variations at various locations, thus providing a means to match and distinguish between fingerprints.

In this rapid growth of scientific technology, fingerprints are one of the most reliable biometrics traits of human-beings. The occurrence of a different fingerprint in each individual person has lead to the use of fingerprints as a legitimate proof of evidence all around the world.

As the development in this field has increased, the use of fingerprints as crime evidence as well as use of it in the forensic division has come in place. There is increasing applications of fingerprint analysis in commercial as well as non-commercial sectors, such as Entry authorization in various offices, securing personal files and its authentication, etc.

Fingerprints obey three fundamental principles. These principles are:

- A fingerprint is an individual characteristic.
- A fingerprint will remain unchanged during an individual’s lifetime.
- Fingerprints have general characteristic ridge patterns that permit them to be systematically classified.

II. STAGES IN ANALYSIS

2.1. ACQUISITION

When a finger is placed on one side of a glass platen (prism), ridges of the finger are in contact with the platen, while the valleys of the finger are not in contact with the platen. The rest of the imaging system essentially consists of an assembly of an LED light source and a CCD placed on the other side of the glass platen. The laser light source illuminates the glass at a certain angle and the camera is placed such that it can capture the laser light reflected from the glass. The light incidenting on the platen at the glass surface touched by the ridges is randomly scattered while the light incidenting at the glass surface corresponding to valleys suffers total internal reflection.

2.2. REPRESENTATION

2.2.1. FINGERPRINT MOSAICING

The global configuration defined by the ridge structure is used to determine the class of the fingerprint, while the distribution of minutiae points is used to match and establish the similarity between two fingerprints. A query print is matched against a large database of prints, using pattern of ridges in the query image to narrow their search in the database.

[6] Fingerprint verification is done two distinct phases:

- The enrollment phase, during which multiple impressions of a fingerprint are acquired and stored in the database as templates, and
- The authentication phase, where the query image of a user is matched against the stored templates pertaining to that user.

This loss of information affects the matching performance of the verification system **-** the relatively small overlap between the template and query impressions results in fewer corresponding points and therefore, results in higher false rejects and higher false accepts.

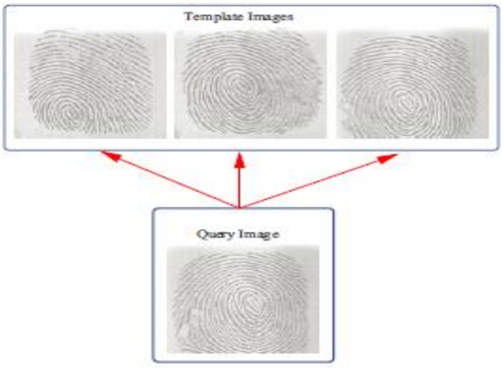


Fig. 1 Fingerprint verification

To deal with this problem, a fingerprint mosaicing scheme that constructs a composite fingerprint template using evidence accumulated from multiple impressions has been developed. A composite template reduces storage, decreases matching time and alleviates the quandary of selecting the "optimal" fingerprint template from a given set of impressions. In the following algorithm, two impressions(templates) of a finger are initially aligned using the corresponding minutiae points. This alignment is used by a modified version of the well-known iterative closest point algorithm (ICP) to compute a transformation matrix that defines the spatial relationship between the two impressions.

Advantages of using Fingerprint Mosaicing**:** Since two three templates of the same fingerprint are superimposed over one another to get a query image, the chances of matching it with a person's fingerprint becomes easier and efficient.

1.1.1.ITERATIVE CLOSEST POINT ALGORITHM

[8] The ICP is known to be one of the best suited algorithms for this process due to its simple and cost effective implementation. The algorithm of ICP is follows:

1. Align Templates
2. Generate spatial co-ordinates, intensity and orientation:
   p(xi,yi,zi, θi) ; q(xi,yi,zi, θi)
3. Compute initial transformation
4. Finger-Print preprocessing
5. Finger-Print image scaling
6. Image segmentation
7. Define Range images (R_p , Rq)
8. Map Range images (R_p , Rq)

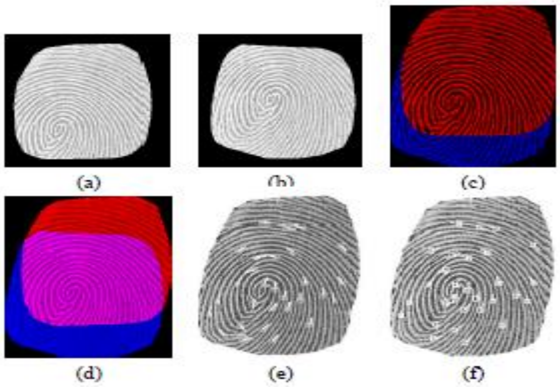
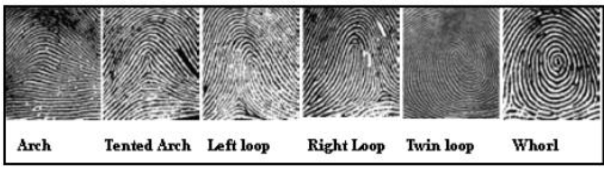


Fig. 2 Composite template construction: (a) (b) First and Second image after segmentation (c) (d) Initial and Final alignment (e) Minutiae extraction (f) Composite minutiae sets.



1.2. STORAGE

Storage of fingerprints is done usually using indexes and hash keys. However, storing the fingerprints by classifying them into various classes makes the entire storage and retrieval process much more efficient. A simple k-means clustering algorithm can be used to store the various samples of fingerprints.

1.2.1.STORAGE CLASSIFICATION

[3] Fingerprints are classified into five categories: whorl, right loop, left loop, arch, and tented arch as shown in Fig. 3.These are always made up of the following patterns: line unit, line-fragment, ending, bifurcation, eye and hook as shown in Fig. 4.

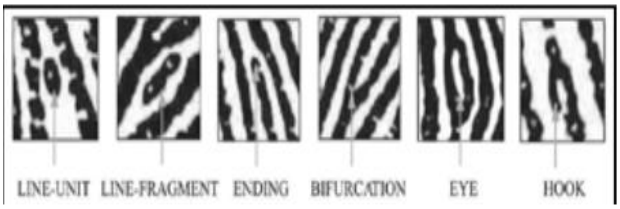


Fig. 3 Six features of Fingerprint.

PARAMETER	**CORRELATION BASED**	**MINUTIAE BASED**
DISTORTIONS	Has non linear distortions	More accurate, less distortions
EFFECT OF VARIATON IN SKIN CONDITION AND FINGER PRESSURE	Cause difference in brightness, contrast, ridge thickness across different fingerprints	No difference on fingerprints
COMPUTATION COST	Technique-computational expensive	More economical

COMPUTATIONAL COMPLEXITY	Very difficult to compute	Easily computed
PERFORMANCE	Comparatively low	Better performance
IMAGE QUALITY	Not robust with respect to image quality	Robust with respect to image quality
USAGE	Not very widely used	Most authentic and widely used technique for matching

Advantages of Storing the Fingerprints by Classification: When the fingerprint in the database has to be matched with a fresh fingerprint sample or retrieved from the database, instead of searching the entire database, this algorithm reduces time taken and complexity involved by searching only those classes which share the features of the fingerprint sample. k-means clustering algorithm can be used for the same.

Fig. 4 Classes of Fingerprints.

1.2.2. MATCHING AND RECOGNITION

The matching process of fingerprints consists of comparison between the input and the template image. Matchers critically relying on extraction of ridges or their connectivity information show drastic degradation in performance with deterioration in the quality of the input fingerprints. We, therefore, believe that point pattern matching (minutiae matching) approach facilitates the design of a robust, simple, and fast verification algorithm while maintaining a small template size.

There are basically two matching techniques:

- Correlation based
- Minutiae based

Comparison of Correlation based and Minutiae based Matching Algorithms

1.2.2.1. SINGULARITY POINT DETECTION ALGORITHM

The detection of the singular points (cores and deltas) is an important and difficult task in automatic fingerprint classification and identification which is a minutiae based technique. Fingerprint images often contain noise, which makes the classification task even more difficult. Core points are the points where the innermost ridge loops are at their steepest. Delta points are the points from which three patterns deviate.[3]

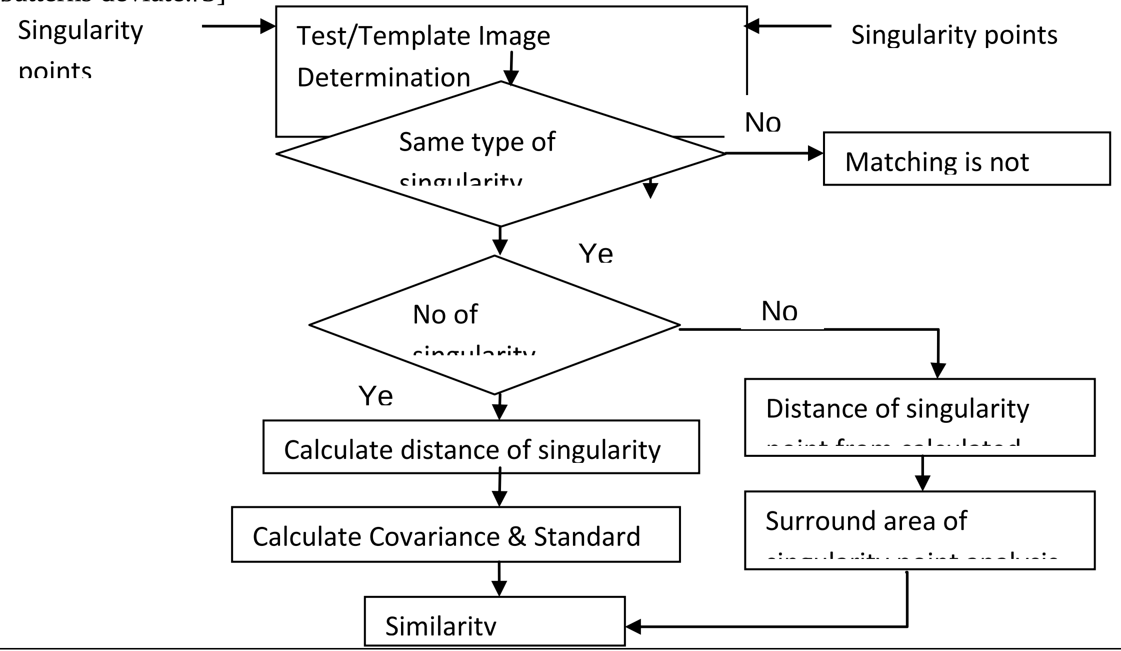

Singularity points
Test/Template Image Determination
Singularity points
Same type of singularity
No
Matching is not
Ye
No of singularity
No
Ye
Distance of singularity point from calculated
Calculate distance of singularity
Surround area of singularity point analysis
Calculate Covariance & Standard
Similarity

Fig.5 Flowchart of Singularity Point Detection Algorithm

1.3. SECURITY

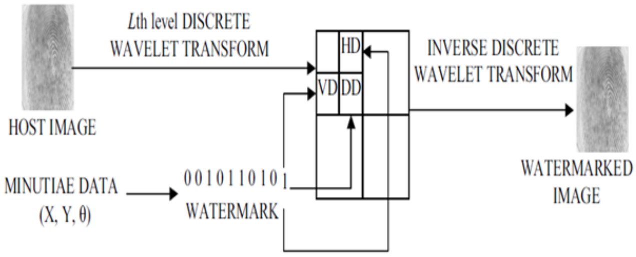
Fingerprints are susceptible to accidental and intentional attacks, when transmitted over network. Thus, a protective scheme is needed which will preserve fidelity and prevent alterations. Watermarking of digital media has gained considerable attention in the last years as a means of copyright protection and content verification. Watermarking of fingerprint images aims to embed watermark information to the fingerprint image without decreasing the fingerprint identification-verification performance.

Watermarking is a technique that can be used to increase the security of the biometric data. Watermarking describes methods to embed information transparently into a carrier signal. Besides preservation of the carrier signal quality, watermarking generally has the additional requirement of robustness against manipulations intended to remove the embedded information from the marked carrier object. Watermarking is of two kinds: spatial-domain techniques (spatial watermarks) and frequency-domain techniques (spectral watermarks). However, spatial watermark can be easily destroyed if the watermarked image is low-pass filtered or JPEG compressed. Frequency domain watermarking can be achieved using Discrete Fourier Transform, Discrete Wavelet transform or Discrete Cosine Transform. Out of these Wavelet Transform is the best. The watermark is then embedded in the transformed coefficients of the image such that the watermark is less invisible and more robust to some image processing operations. Finally, the coefficients are inverse-transformed to form the watermarked image.

Advantage of securing fingerprint samples by Watermarking (using Discrete Wavelet Transform) : It is flexible and does not truncate values while passing through a filter.

1.3.1.ALGORITHM[7]

- Convert the minutiae values.
- Compute the L^{th}-level discrete wavelet transform of the host image where L is limited by the size of the image and the length of the watermark.
- Select the exact locations of the coefficients to be watermarked and sort the detail coefficients in descending order.
- Every watermark bit is embedded in each detail (i.e. horizontal, vertical and diagonal) by quantizing the coefficients.
- Calculate the L^{th} inverse discrete wavelet transform to obtain the watermarked image.



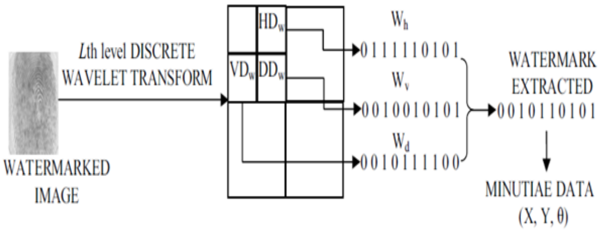
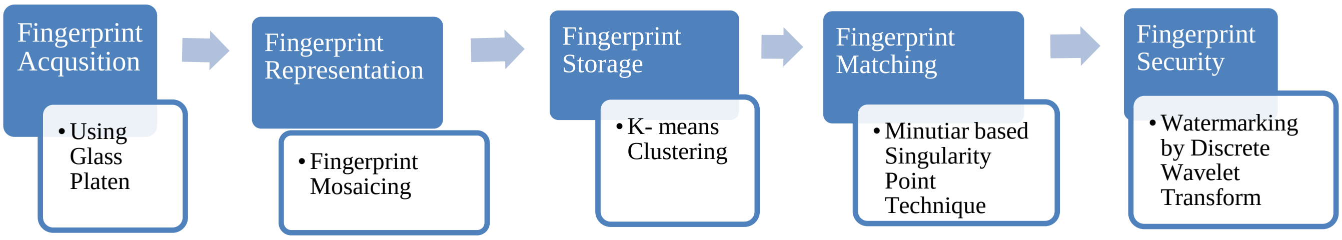


Fig. 6 Embedding process to hide the minutia data.

Fig. 7 Watermark extraction process.

2. PROPOSED SYSTEM

After studying and comparing various techniques used in the different stages of Fingerprinting system, the following system is proposed. Fingerprint Mosaicing scheme constructs a composite fingerprint template using evidence accumulated from multiple impressions. A composite template reduces storage, decreases matching time and alleviates the quandary of selecting the "optimal" fingerprint template from a given set of impressions. K – Means Clustering is an efficient way to classify the Fingerprint based on the feature or classes and accordingly store it in Database. This helps for fast retrieval of Fingerprint as this reduces the space and search complexity. Minutiae based Singularity Point matches the Fingerprint on core and delta points. It also considers the relative distance between core and delta points. **T**hus, improving the robustness of the system in presence of changes introduced by displacement and rotation on the image. This is an efficient technique for matching and recognition of Fingerprint. Watermarking is to add a watermark signal to the query image stored in database to be watermarked such that the watermark signal is unobtrusive and secure in the signal mixture but can partly or fully be recovered from the signal mixture later on.


Fingerprint Acqusition
- Using Glass Platen

Fingerprint Representation
- Fingerprint Mosaicing

Fingerprint Storage
- K- means Clustering

Fingerprint Matching
- Minutiar based Singularity Point Technique

Fingerprint Security
- Watermarking by Discrete Wavelet Transform

Fig. 8 Proposed System Fingerprint stages with techniques.

III. CONCLUSION

After studying the entire fingerprinting process and keeping in mind the pros and cons of different algorithms as well as the techniques available, for Representation of Fingerprints, Fingerprint Mosaicing is certainly an efficient method in acquisition of fingerprints. Mosaicing helps to store the optimized fingerprint query image which is used for fingerprint matching. This reduces space complexity for storage. For storage using classification by k - means technique, while for fingerprint matching and recognition, minutiae based technique-singularity point detection is most suitable. Singularity point detection technique is used for matching using core and delta points as it can efficiently match with varied aligned alignment fingerprint sample. This reduces time complexity for retrieval of fingerprint. For securing fingerprints, watermarking can be used. This five stage fingerprinting system can be used as password authenticators in banks or used in forensics.

REFERENCES

[1] Monowar Hussain Bhuyan, Sarat Saharia, Dhruba Kr Bhattacharyya, An Effective Method for Fingerprint Classification, *International Arab Journal of e-Technology, Vol. 1, No. 3, January 2010*

[2] Jitendra P. Chaudhari, Pradeep M. Patil, Y.P.Kosta Charotar, Singularity Points Detection in Fingerprint Images,*International Journal of Computer Applications (0975 – 8887) Volume 45– No.5, May 2012*

[3] Uma Maheswari, E. Chandra, A Review Study on Fingerprint Classification Algorithm used for Fingerprint Identification and Recognition, *IJCST Vol. 3, Issue 1, Jan. - March 2012*

[4] Raffaele Cappelli, Matteo Ferrara, Davide Maltoni, Minutiae-Based Fingerprint Matching, *IEEE Transactions On Pattern Analysis And Machine Intelligence, Vol. 21, No. 5, May 1999*

[5] Abhishek Rawat, *A Hierarchical Fingerprint Matching,* Indian Institute of Technology Kanpur July 2009

[6] Arun Abraham Ross, *Information Fusion in Fingerprint Authentication,* Michigan State University 2003

[7] Khalil Zebbiche, Lahouari Ghouti, Fouad Khelifi, Ahmed Bouridane, Protecting Fingerprint Data using Watermarking,*First NASA/ESA Conference on Adaptive Hardware and Systems (AHS'06)*

[8] Anil Jain, Arun Ross, Fingerprint Mosaicing, *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), Orlando, Florida, May 13 - 17, 2002.*