International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869, Volume-3, Issue-5, May 2015

A Novel Study on Fingerprint Biometrics based on Discretized Fingerprint Texture Descriptors

Er. Veena Rani, Er. Neeraj Kamboj

***Abstract*— accurate automatic personal identification is critical in a variety of applications in our electronically interconnected society. Biometrics, which refers to identification based on physical or behavioural characteristics, is being increasingly adopted to provide positive identification with a high degree of confidence. Among all the biometric techniques, fingerprint-based authentication systems have received the most attention.**

The main objective of this paper is to design a biometric fingerprint system based on texture descriptors. So, this paper reviews on fingerprint biometrics based on discredited texture descriptors. The texture descriptors, namely, the filter-based Finger Code, a binary pattern (BP), and their various combinations are considered. In this, these fingerprint texture descriptors are binarized using a biometric discretization method. Also a region of interest is to be finding out for proper matching of minutia. In this, template information is also secured in notepad for further processing.

***Index Terms*— Fingerprint technique, Biometrics, Texture descriptors, minutia matching etc.**

I. INTRODUCTION

Nowadays, there is an emerging interest in the application of biometric authentication and identification. Biometric identification is a growing and notorious field in which civil liberties groups express their concern over identity and privacy issues. Today, biometric laws and regulations are in process and biometric industry standard are being tested. This development has the great concern of security in the use of Internet application for consistent and automatic personal identification. Traditional automatic personal identification schemes such as knowledge based (password or personal identification number) and token based (passport, driver license, and ID card) identifications are prone to fraud because pins may be forgotten or guessed by an imposter and the tokens may be lost or stolen. Therefore, traditional knowledge-based and token-based approaches are unable to satisfy the security requirements of our electronically interconnected information society [17].

The selection of biometric feather depends on requirements of application. The most common biometric trait is fingerprint identification. Fingerprint recognition has been widely adopted for user identification due to its reliable performance, usability, and low cost compared with other biometric traits such as signature, iris, face, and gait recognition.

Er. Neeraj Kamboj,Research Scholar, Electronics & Communication Engg. Deptt. JCDM College of Engineering, Sirsa, India.

Er. Veena Rani, Assistant Professor, Electronics & Communication Engg Deptt.JCDM College of Engineering, Sirsa, India

Fingerprint pattern contain narrow ridge separated by narrow valleys and these ridges flow almost parallel to each other. The end point and bifurcation points of ridges are called minutiae. The minutiae are the most important features in fingerprint matching. The objective of Automatic Fingerprint Identification system is to extract these features. However, minutiae extracted especially from dirty images contain many pseudo-minutiae. For instance, fingerprint images may be worsened by various kinds of noise causing cracks, scratches and bridges in the ridges as well as ink blurs. These make many pseudo-minutiae on fingerprint images and cause matching errors. Effective image enhancement for fingerprint matching must therefore eliminate these pseudo-minutiae.

Figure 1: Fingerprint Image [17]

The paper is ordered as follows. In section II, it represents related work with proposed system in fingerprint biometrics. In Section III, It defines various steps included in fingerprint biometrics. Finally, conclusion is explained in Section VI.

II. RELATED WORK

Some Authors [1] proposed an effective algorithm for fingerprint image quality improvement is proposed. The algorithm consisted of two stages. The first stage was decomposing the input fingerprint image into four sub-bands by applying two-dimensional discrete wavelet transform. At the second stage, the compensated image was produced by adaptively obtaining the compensation coefficient for each sub-band based on the referred Gaussian template. The method concluded an improved clarity, quality and continuity of ridge structures therefore accuracy was also increased. Background and the blurred region of fingerprint images were also removed.

Some [2] proposed a biometrics-based authentication scheme for multi-server environment using elliptic curve cryptography. To the best of our knowledge, the proposed

scheme is the first truly three-factor authenticated scheme for multi-server environment. They also demonstrated the completeness of the proposed scheme using the Burrows Abadi–Needham logic.

Authors [3] presented the several improvements to an adaptive fingerprint enhancement method that was based on contextual filtering. In the global analysis and matched filtering blocks, different forms of order statistical filters were applied. These processing blocks yield an improved and new adaptive fingerprint image processing method.

Some [4] proposed a novel and effective two-stage enhancement scheme in both the spatial domain and the frequency domain by learning from the underlying images. They first enhanced the fingerprint image in the spatial domain with a spatial ridge-compensation filter by learning from the images. With the help of the first step, the second stage filter, i.e., a frequency band-pass filter that was separable in the radial- and angular-frequency domains was employed. An experimental result showed that our proposed algorithm was able to handle various input image contexts and achieves better results compared with some state-of-the-art algorithms over public databases, and to improve the performances of fingerprint-authentication systems

Some [5] proposed a high-resolution palm print recognition system based on minutiae. The proposed system followed the typical sequence of steps used in fingerprint recognition, but each step had been specifically designed and optimized to process large palm print images with a good trade-off between accuracy and speed. A sequence of robust feature extraction steps allowed to reliably detecting minutiae; moreover, the matching algorithm was very efficient and robust to skin distortion, being based on a local matching strategy and an efficient and compact representation of the minutiae. Experimental results showed that the proposed system compares very favourably with the state of the art.

Some authors [6] proposed that a novel fingerprint reconstruction algorithm is proposed to reconstruct the phase image, which is then converted into the grayscale image. The proposed reconstruction algorithm has been evaluated with respect to the success rates of type-I attack and type-II using a commercial fingerprint recognition system. The experimental results show that the reconstructed image is very consistent with the original fingerprint and that there is a high chance of deceiving a state-of-the-art commercial fingerprint recognition system.

Authors [7] presented High-resolution automated fingerprint recognition systems (AFRSs) offer higher security because they were able to made use of level-3 features, such as pores, that were not available in lower resolution images. After experiments on their collected fingerprint images and applying three requirements for the proportions of minutiae and pores that must be retained in a fingerprint image, they recommended a reference resolution of 800 dpi.

Some [8] introduced a novel fingerprint matching algorithm using both ridge features and the conventional minutiae feature to increase the recognition performance against nonlinear deformation in fingerprints. Experiments were conducted for the FVC2002 and FVC2004 databases to compare the proposed method with the conventional minutiae-based method. The proposed method achieved higher matching scores as the EER % reduced. Thus, they had concluded that the proposed ridge feature gave additional information for fingerprint matching with little increment in template size and used in conjunction with existing minutiae features to increase the accuracy and robustness of fingerprint recognition systems.

Some [9] presented an investigation of the problem of retrieving candidate lists for matching partial fingerprints by exploiting global topological features. They proposed an analytical approach for reconstructing the global topology representation from a partial fingerprint. Statistical experiments show that proposed model-based approach can effectively reduce the number of candidates for pair wised fingerprint matching, and thus significantly improve the system retrieval performance for partial fingerprint identification.

Authors [10] proposed the Minutia Cylinder-Code (MCC): a novel representation based on 3D data structures, built from minutiae distances and angles. The cylinders can be created starting from a subset of the mandatory features defined by standards like ISO/IEC 19794-2 (2005). Cylinder invariance, fixed-length, and bit-oriented coding, some simple but very effective metrics can be defined to compute local similarities and to consolidate them into a global score. MCC relied on a robust discretization of the neighbourhood of each minutia into a 3D cell-based structure named cylinder. Simple but effective techniques for the computation and consolidation of cylinder similarities were provided to determine the global similarity between two fingerprints.

III. Automatic Fingerprint Identification System

The various aspects of Automatic Fingerprint Identification System, like fingerprint representation, feature extraction from fingerprint image, fingerprint matching with stored template to prove identify and fingerprint classification for easy and fast search in the database, are explained below.

1. Need for Automatic Fingerprint Identification System (AFIS)

The tremendous success of fingerprint based in law enforcement application recognition technology in law enforcement application, decreasing cost of fingerprint sensing devices, increasing availability of inexpensive computing power, and growing identity fraud/theft have all ushered all ushered in an era of fingerprint-based person recognition application in commercial, and financial domains [11].

In 1893 the home Ministry office, UK accepted that no two individuals have the same fingerprints .Soon after this discovery many major law enforcement departments embraced the idea of booking the fingerprint of criminals, so that their records are readily available and later using leftover fingerprint smudges, they could determine the identity of criminals. These agencies sponsored a rigorous study of fingerprints recognition for nailing down the perpetrators.

Despite the ingenious method improvised to increase the efficiency of the manual approach to fingerprint indexing and search, the ever growing demand on manual fingerprint recognition quickly became overwhelming. The manual

methods of fingerprint indexing resulted in a highly skewed distribution of fingerprint into bins. Most fingerprints fell into a few bins and this did not improve search efficiency. Fingerprint training procedures were time intensive and slow. Furthermore, demand imposed by the painstaking attention needed to visually match the fingerprint of varied qualities, tedium of the monotonous nature of the work, and increasing workload due to a higher demand on fingerprint recognition services, all prompted the law enforcement agencies to initiate research into acquiring fingerprints through electronic media and automate fingerprint recognition based on the digital representation of fingerprints. These efforts led to development of **Automatic Fingerprint Identification System (AFIS)** over the past few decades. Law enforcement agencies were the first to adopt the fingerprint recognition technology, more recently; however, increasing identity fraud has created a growing need for biometric technology for person recognition in a number of non-forensic application .As fingerprint gets embedded into various systems (e.g. cellular phone, laptops), it becomes increasingly important to analyze the impact of biometric on the overall integrity of the system and its social acceptance as well as the related security and privacy issues.

2. Fingerprint Analysis, Representation and Feature Extraction

A fingerprint is the print of a fingertip epidermis, produced when a finger is pressed against a smooth surface. Individual epidermal ridges and furrows have different characteristics. This forms the foundation of fingerprint. In a fingerprint image, ridges are dark whereas valleys are bright, as show in Fig.1.2.

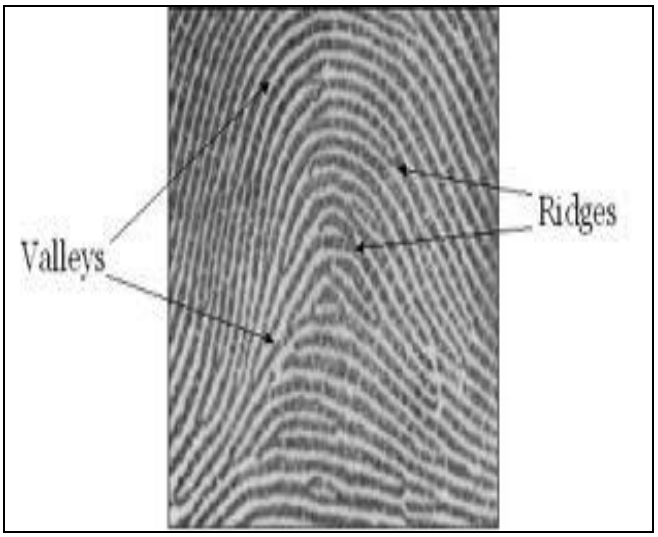

Figure 1.2: A Fingerprint image showing ridges and valley [11]

Ridge varies in width from 100µm, for very thin ridges, to 300µm for thick ridges. Generally the period of a ridge/valley cycle is about 500µm. Injuries such as burns, abrasions, or cut do not affect the underlying ridge structure, and the original pattern is duplicated in any new skin that grows.

Fingerprint when analyzed at the global level, the fingerprint pattern exhibits one or more regions where the ridge lines assume distinctive shapes (characterized by high curvature, frequent, termination etc).These regions (called singular regions) may be classified into three topologies: loop, whorl, delta (Fig.1.3).Right loop and left loop is also called delta.

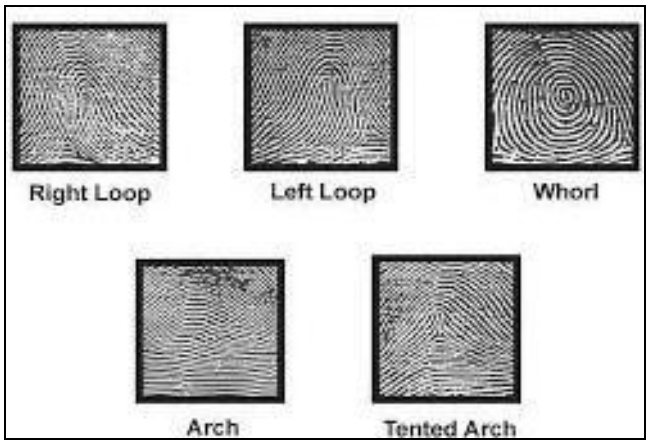

Figure 1.3: Fingerprint showing singular regions and five major classes [12]

Several fingerprint algorithms pre-align fingerprint images according to a centre point, called core. The core point is defined as the north most point of the innermost ridge line. Singular regions are commonly used for fingerprint classification. Show the core point and delta point in fig.1.4.

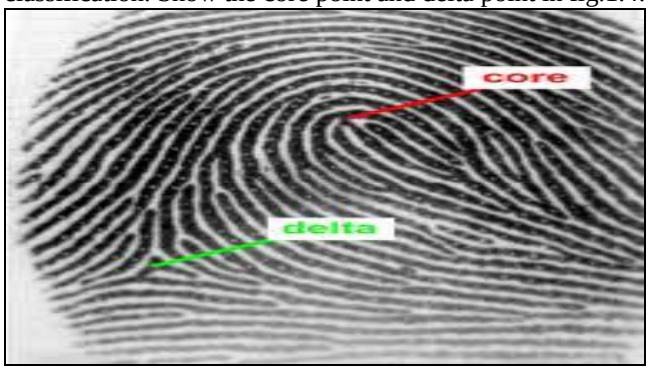

Figure 1.4: A Fingerprint image showing core and delta points [13]

The representation of fingerprint is important issue in the design of fingerprint recognition system. There is larger variability in different impressions so there is a need to determine salient features of the input fingerprint image that can discriminate between different identities as well as remain invariant for a given individual. Thus the problem of representation is to determine a feature space in which the fingerprint images belonging to the same finger form a compact cluster and those belonging to different finger occupy portion of the feature space, which means features should have low intra-class variation and high inter-class variation.

A good fingerprint representation should have the following two properties:

Saliency- A representation should contain distinctive information about the fingerprint.

Suitability- The representation can be easily extracted, stored in a compact fashion, and be useful for matching. A salient representation is not necessarily a suitable representation.

The fingerprint patterns are analyzed for different types of features

a) **Global features**: Fingerprint patterns have singular points called loop and delta. Singular point and coarse

ridge line map are very important for fingerprint classification and indexing, but their distinctiveness is not sufficient for accurate matching. Orientation image and frequency image also from a feature set that can be detected at the global level.

b) Local features: The local ridge characteristics are called minute point. The two most prominent minute points are ridge termination and ridge bifurcation. A ridge ending is defined as the ridge points where a ridge ends abruptly. A ridge bifurcation is defined as the ridge point where a ridge forks or diverges into branch ridge. Although a minutiae-based representation is characterized by a high saliency, a reliable automatic minutiae extraction can be problematic in low-quality fingerprints.

3. Fingerprint Matching

Fingerprint matching is a difficult problem because of the variability in different impressions of the same finger. The main reason for these variations is displacement, rotation, non-liner distortion, variable pressure, changing skin condition and noise. Therefore fingerprint from the same finger may sometimes look quite different whereas fingerprint from different fingers may appear quite similar. Although automatic minutiae-based fingerprint matching inspired by the manual procedure, it may not necessarily follow the same guidelines. A categorization of automatic fingerprint matching approaches is:

- **Correlation-based matching**: Two fingerprint images are superimposed and the correlation between corresponding pixels is computed for different alignments.
- **Minutiae-based matching**: Minutiae are extracted from the fingerprint and stored as sets of points in the two-dimensional plane. Minutiae matching are finding the maximum alignment between the stored template and the input minutiae set.
- **Ridge feature-based matching:** Minutiae extraction is difficult in very low-quality fingerprint images. Though the distinctiveness of feature like local orientation and frequency is low but these features are extracted more reliably than minutiae.

4. Fingerprint Classification and Indexing

Automatic identification based on fingerprint requires this input fingerprint to be matched with a large number of fingerprints stored in a database (e.g. the FBI database contains more than 200 million fingerprints). To reduce the search time and computational complexity, it is desirable to classify these fingerprints into different bins so that input fingerprint needs to be matched only with a subset of the fingerprint in the database. Fingerprint classification is a technique used to assign a fingerprint to one of several pre-specified types. Fingerprint classification can be viewed a coarse-level matching of the fingerprint. An input fingerprint is first matched to one of the pre-specified types and then it is compared to a subset of the database corresponding to that fingerprint type. For example, if the fingerprint database is binned into five classes and a fingerprint classifier output two classes with high accuracy, then identification system will only need to search two of the five bins, thus decreasing the search space.

Unfortunately, only a limited number of major fingerprint categories have been identified, the distribution of fingerprints into these categories is not uniform. There are fingerprints whose exclusive membership cannot be reliably stated.

5. Application of Fingerprint Recognition System

Fingerprint recognition is a rapidly evolving technology that has been widely used in forensic such as criminal recognition and prison security, and has a very strong potential to be adopted in a broad range of civilian applications (Table 1.1).

Table 1.1 Application of Fingerprint Recognition System [14]

Forensic	Government	Commercial
Corpse Identification, Criminal Investigation, Terrorist Identification, Parenthood Determination, Missing Children, etc.	National ID card Correction Facility, Driver's License, Social security, Welfare Disbursement, Border Control, Passport Control, etc.	Computer network Logon, Electronic Data Security, E-Commerce, Internet Access, ATM, Credit card, Physical Access Control, Cellular Phones, Personal digital assistant, medical records management, distance learning, etc.

Most of the fingerprint recognition applications are divided into three categories. Traditionally, forensic applications have used manual biometric, government application have used token based systems, and commercial application have used knowledge base system. Fingerprint recognition system now being increasingly used for all these sectors

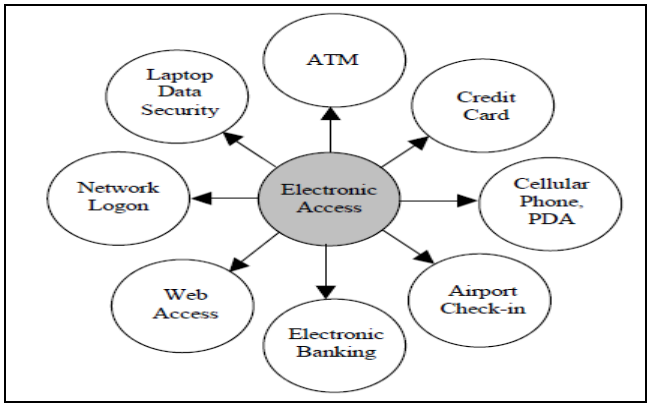

Figure 1.5: Various Electronic Access Applications in widespread use that require automatic recognition

IV. PROPOSED SYSTEM

In this paper, we proposed an effective biometric system construction for biometric template protection using a discretized fingerprint texture descriptors. It reviews on steps required for image fingerprint matching. The binarized will also be done using texture descriptors. The region of interest will also be studied. The process of validation of images is

also provided. At last, the template information will also be secured in a file that helps in minutia matching. So, overall it will be very effective for image fingerprinting biometrics system.

V. CONCLUSION

Motion Estimation forms a major computation bottleneck in video processing applications such as the detection of noise in image sequences, interpolation/ prediction of missing data in image sequences and de-interlacing of image sequences.In this, it proposes a compensated motion frame prediction and detection using block based and pixel based technique. The main objective is to reduce the computation time and improves the PSNR value of system. Sometimes, the pixel value is very low, so to detect these pixels, it may use the enhancement concept to improve the pixel value so that it may detect and reconstruct that frame easily.

REFFERENCES

[1] Jing-Wein Wang, Ngoc Tuyen Le, Chou-Chen Wang, and Jiann-Shu Lee, " Enhanced Ridge Structure for Improving FingerprintImage Quality Based on a Wavelet Domain", 2015 IEEE
[2] Debiao He, and Ding Wang, "Robust Biometrics-Based Authentication", 2014 IEEE Scheme for Multiserver Environment.
[3] Josef Strom Bart unek, Mikael Nilsson, Benny Sallberg, and Ingvar Claesson,, "Adaptive Fingerprint Image Enhancement With Emphasis on Preprocessing of Data", 2013 IEEE
[4] Jucheng Yang, Naixue Xiong, and Athanasios V. Vasilakos, "Two-Stage Enhancement Scheme for Low-Quality Fingerprint Images by Learning From the Images" 2013 IEEE
[5] Raffaele Cappelli, Matteo Ferrara, and Dario Maio, "A Fast and Accurate Palmprint Recognition System Based on Minutiae" 2012 IEEE
[6] Jianjiang Feng,Member, and Anil K. Jain, "Fingerprint Reconstruction: From Minutiae to Phase" 2011 IEEE
[7] David Zhang , Feng Liu, Qijun Zhao, Guangming Lu, and Nan Luo, "Selecting a Reference High Resolution for Fingerprint Recognition Using Minutiae and Pores" 2011 IEEE
[8] Heeseung Choi, Kyoungtaek Choi, and Jaihie Kim, "Fingerprint Matching Incorporating Ridge Features With Minutiae" 2011 IEEE
[9] Yi (Alice) Wang, Jiankun Hu, "Global Ridge Orientation Modeling for Partial Fingerprint Identification" 2011 IEEE
[10] Raffaele Cappelli, Matteo Ferrara, Davide Maltoni, "Minutia Cylinder-Code: A New Representation and Matching Technique for Fingerprint Recognition" 2010 IEEE
[11] Praveer Mansukhani, Sergey Tulyakov, and Venu Govindaraju, " A Framework for Efficient Fingerprint Identification Using a Minutiae Tree" 2010 IEEE
[12] Lavanya B N, K B Raja, Venugopal K R and L M Patnaik, "Minutiae Extraction in Fingerprint using Gabor Filter Enhancement" 2009 IEEE
[13] Fanglin Chen, Jie Zhou and Chunyu Yang, "Reconstructing Orientation Field From Fingerprint Minutiae to Improve Minutiae-Matching Accuracy" 2009 IEEE
[14] Weiguo Sheng, Gareth Howells, Michael Fairhurst, and Farzin Deravi, "A Memetic Fingerprint Matching Algorithm" 2007 IEEE
[15] Arun Ross, Jidnya Shah, and Anil K. Jain, "From Template to Image: Reconstructing Fingerprints from Minutiae Points" 2007 IEEE
[16] Xudong Jiang, Manhua Liu, and Alex C. Kot, "Fingerprint Retrieval for Identification" 2006 IEEE
[17] R. Gonzalez, R. Woods and S. Eddins "Digital Image Processing Using Matlab", 2004, Prentice Hall.