Classification and Improvement of Fingerprint Verification Using Support Vector Machine

Shaveta1, Amit Walia2
Students of masters of technology Computer Science, Department of Computer Science Engineering, Lovely Professional University, Punjab, India.

Abstract—Fingerprints are widely used in daily life for more than 100 years due to its feasibility, distinctiveness, permanence, accuracy, reliability, and acceptability. Fingerprint is a pattern of ridges, furrows and minutiae, which are extracted using inked impression on a paper or sensors. Fingerprints have been used as
The most popular biometric authentication and verification measure because of their high acceptability, immutability and uniqueness. The paper presents a fingerprint matching scheme that uses both minutiae localizations and estimated weights as features, transforming the matching problem to a classification problem and using SVM to solve it. The experiment switch both international and domestic fingerprint verification competition data show substantial improvements in accuracy and performance of fingerprint verification.

Keywords—SVM, PHT, verification, minutiae, RNN, FAR

I. INTRODUCTION

A fingerprint is the feature pattern of one finger. It is believed that each fingerprint is unique. Each person has his own fingerprints with the permanent uniqueness. So fingerprints have been used for identification and forensic investigation for a long time [3]. A fingerprint is composed of many ridges and furrows. These ridges and furrows present good similarities in each small local window, like parallelism and average width. Intensive research on fingerprint recognition shows that fingerprints are not distinguished by their ridges and furrows, but by Minutia, which are some abnormal points on the ridges. Among the variety of minutia types reported in literatures, two are mostly significant and in heavy usage: one is called termination, which is the immediate ending of a ridge; the other is called bifurcation, which is the point on the ridge from which two branches derive. The fingerprint recognition problem can be grouped into two sub-domains: one is fingerprint verification and the other is fingerprint identification. Fingerprint verification is to verify the authenticity of one person by his fingerprint. The user provides his fingerprint together with his identity information like his ID number. The fingerprint verification system retrieves the fingerprint template according to the ID number and matches the template with the real-time acquired fingerprint from the user. Fingerprint identification is to specify one person’s identity by his fingerprint(s). Without knowledge of the person’s identity, the fingerprint identification system tries to match his fingerprint(s) with those in the whole fingerprint database.

![Fig. 1 Verification vs. Identification](image)

The uniqueness of a fingerprint can be determined by the global pattern of ridges and valleys, and by the local pattern of bifurcations and endings which are called minutiae. Among all the biometric techniques fingerprint identification is today the most widely used biometric identification form. It has been used in numerous applications. The problem is to develop algorithms which are robust to noise in the fingerprints and able to deliver accuracy in real time. Fingerprint matching algorithms vary greatly in terms of false positive and false negative errors [4]. They may also vary with respect to features such as image rotation invariance and independence from a reference point given as the center or the core of the fingerprint pattern.

In automatic fingerprint verification system, the characteristic features obtained from the test fingerprint are matched against those from a template fingerprint. As the fingerprint of a person is unique and immutable, the automatic
fingerprint verification system can be widely used in both anti-criminal and civilian applications where precision is important. Therefore, accuracy and performance improvements are the key points in automatic fingerprint verification system current research.

II. MOTIVATION

A lot of work is being done today to decide which information in fingerprints should be used to keep the uniqueness. In addition to this work, the current work in this field concentrates on reducing the computation time for feature extraction and matching. The proposed approach is motivated by the following observations:

1. The minutiae information in fingerprint images may not be discriminative because of the different sensors and skin conditions. Most of the sensors, particularly capacitive sensors, capture only a small area of the finger tip, which means some minutiae information outside the area is missing. Furthermore, in practice a significant percentage of fingerprint images are of poor quality due to variations in skin conditions like postnatal marks or occupational marks, and impression conditions. This may lead a large number of errors in minutiae positions and orientations, which may cause problems in next matching stage.

2. After getting the total number t of matching minutiae, a judgment must be made: do these two images match? The normal method is to compare t with a certain λ. If ‘t ≥ λ’ then the two images match. If t is not greater than or equal to the threshold, than the images do not match. That means the value of λ is critical in the decision making process. In order to reduce the influence of the decision making process [14]. In order to reduce the influence of λ, a machine learning technique can be used to determine the threshold for different databases. In addition, SVM is a powerful classification method that can properly label matching results.

III. PROPOSED APPROACH

The work focuses on the minutiae-based matching scheme. The paper presents a fingerprint matching approach that uses not only the minutiae localizations, but also a weight feature, which is the distance between a minutia and its nearest neighbour minutia. Considering that the matching process can be regarded as a two-class classification problem (two fingerprint images are either matched or not), using the extracted minutiae positions, orientations and weights as features, we define a vector standing for the similarity of two fingerprints, and choose SVM as the classifier.

A. Existing System

In base paper polar harmonic transform (PHT) which was used to generate rotation invariant features. The computation of the PHT kernels is significantly simpler compared with that of ZMs and PZMs and hence can be performed at a much higher speed [9]. With PHTs, there is also no numerical instability issue, as with ZMs and PZMs which often limits their practical usefulness. A large part of the computation of the PHT kernel can be recomputed and stored. In the end, for each pixel, as little as three multiplications, one addition operation, and one cosine and/or sine evaluation are needed to obtain the final kernel value. In this paper, three different transforms will be introduced, namely, Polar Complex Exponential Transform (PCET), Polar Cosine Transform (PCT), and Polar Sine Transform (PST). We have grouped them under the name Polar Harmonic Transform as the kernels of these transforms are harmonic in nature, that is, they are basic waves.

B. Proposed Method

In this paper, we propose new fingerprint classification algorithms based on two machine learning approaches: support vector machines (SVM), and recursive neural networks (RNN). SVM is a relatively new technique for pattern classification and regression that is well-founded in statistical learning theory [15]. One of the main attractions of using SVM is that they are capable of learning in sparse, high-dimensional spaces with very few training examples. They have been successfully applied to various classification problems [4]. This architecture can exploit structural information in the data, which, as explained above, may help discriminating between certain classes. This vector is regarded as an additional set of features subsequently used as inputs for the SVM classifier. An important issue in fingerprint classification is the problem of ambiguous examples: some fingerprints are assigned to two classes simultaneously, i.e. they have double labels (these images are also called “cross-referenced”). In order to address this issue, we designed an error correcting code [5] scheme of SVM classifiers based on a new type of decoding distance. This method presents two main advantages. First, it allows a more accurate use of ambiguous examples because each SVM is in charge of generating only one code bit, whose value discriminates between two disjoint sets of classes. Then, if a fingerprint has labels all belonging to the same set for a particular code bit, we can keep this example in the training set without introducing any labelling noise. The second advantage of our system is its capability to deal with rejection problems. This is due to the concept of margin inherent to the SVM, which is incorporated in the decoding distance.

IV. SVM

Support Vector Machines are learning systems that use hypothesis space of linear functions in a high dimensional feature space, trained with a learning algorithm from optimization theory that implements a learning bias derived from statistical learning theory. Inherently, SVMs are binary classifiers. They are used to build a decision boundary by
mapping data from the original input space to a high dimensional feature space, where the data can be separated using a linear hyper plane. For the pattern recognition case, SVMs have been successfully applied to isolated handwritten digit recognition, text categorization [7], speaker identification [4], face detection in images [8], Bio-informatics [9], etc. This paper presents some experiments on fingerprint database using support vector machine, to handle multi classification, One versus all technique is used for fingerprint classification.

A. SVM Algorithm
Our algorithm maintains a candidate Support Vector set. It initializes the set with the closest pair of points from opposite classes like the Direct SVM algorithm. As soon as the algorithm finds a violating point in the dataset it greedily adds it to the candidate set. It may so happen that addition of the violating point as a Support Vector may be prevented by other candidate Support Vectors already present in the set. We simply prune away all such points from the candidate set. To ensure that the kernel conditions are satisfied we make repeated passes through the dataset until no violators can be found. We use the quadratic penalty formulation to ensure linear separability of the data points in the kernel space.

B. Flowchart of Algorithm
An iterative algorithm can be designed which scans through the dataset looking for violators.

V. RESULTS AND DISCUSSION
In this section, the proposed method is simulated. Some simulations are performed in NS-2. The simulation results are compared with the existing system as in [9].
Fig. 3 Total matched & unmatched image.

Fig. 4 Total tested image

Fig. 5 FAR & FRR
Fig. 3-5 shows the simulation results of the existing PHT algorithm in MATLAB.

Fig. 6 Total matched & unmatched image.

Fig. 7 Total tested image

Fig. 8 FAR & FRR

Fig. 6-8 shows the simulation results of the proposed algorithm implemented in MATLAB. The results show that the proposed approach is better as it provides Better FAR (False Acceptance Rate) and FRR (False Rejection Rate). They have been reduced to zero.
VI. CONCLUSION

The intent of the paper is to throw light that using support vector machine (SVM) fingerprint match has been improved w.r.t. the polar harmonic transform (PHT). SVM has improved false rejection ratio (FRR) as well as false acceptance ratio (FAR). Initially the execution time was low as there was no image training was there but with results with SVM goes with image training leads to more execution time but better results.

Acknowledgment

The paper has been written with the kind assistance, guidance and active support of my department who have helped me in this work. I would like to thank all the individuals whose encouragement and support has made the completion of this work possible.

References