A Novel System for Protecting Fingerprint Privacy by Combining Two Different Fingerprints into a New Identity

Ayesha Irfan¹, S.Nirmala Sugirtha Rajini²

¹Research Scholar, Department of Computer Applications, Dr. M.G.R. Educational and Research Institute University, Chennai
²Professor, Department of Computer Applications, Dr. M.G.R. Educational and Research Institute University, Chennai
Email: ayeshairfansa@gmail.com

Abstract- Fingerprint identity is a novel system that protects fingerprint privacy by combining them into two different fingerprints into a unique identity. With this a new virtual identity is created for the two different fingerprints which can be matched using Beta Skeleton Technique, compared with Beta Skeleton technique, one work has the advantage of creating a better new virtual identity when two different Fingerprints are randomly chosen we also use water marking method to combine two different fingerprints, then combine, by overlapping both fingerprint as one finger image. (i) Can be used to form virtual identities from two different fingers. (ii) Can be used to obscure the information present in an individual image prior to storing in a database. (iii) It can also be used to produce a cancelable fingerprint template, such as the template can be reset if the mixed fingerprint is been compromised.

I. INTRODUCTION

Fingerprints are the most widely used biometric feature for person identification and verification in the field of biometric identification. Fingerprints possess two main types of features that are used for automatic fingerprint identification and verification: (i) Ridge and furrow structure that forms a special pattern in the central region of the fingerprint and (ii) Minutiae details associated with the local ridge and furrow structure. In a traditional biometric recognition system, the biometric template is usually stored on a central server during enrollment. The candidate biometric template captured by the biometric device is sent to the server where the processing and matching steps are performed. This paper presents an approach to speed up the matching process by classifying the fingerprint pattern into different groups at the time of enrollment, and improves fingerprint matching while matching the input template with stored template. To solve the problem, we take several aspects into consideration like classification of fingerprint, singular points. The algorithm result indicates that this approach manages to speed up the matching effectively[2], and therefore prove to be suitable for large database like forensic divisions. The main scope of the project is to combined minutiae template from the original minutiae templates. With the help of an existing fingerprint reconstruction approach, we are able to convert the combined minutiae template into a real-look alike combined finger print [9].

II. RELATED WORKS

The Proposed Fingerprint Privacy protection System

Fig. 1 shows our proposed fingerprint privacy protection system. In the enrollment phase, the system captures two fingerprints from two different fingers, say finger prints respectively. We extract the minutiae positions from one fingerprint and the orientation from other fingerprint using some existing techniques [9] then, by using our proposed coding strategies, a combined minutiae template is generated based on the minutiae positions, the orientation and the reference points detected from both fingerprints. Finally, the combined minutiae template is stored in a database[6]. In the authentication phase, two query finger prints are required from the same two fingers, say fingerprints and from fingers and. As what we have done in the enrollment, we extract the minutiae positions from fingerprint and the orientation from fingerprint. Reference points are detected from both query fingerprints. This extracted information will be matched against the corresponding template stored in the database by using a two-stage fingerprint matching. The authentication will be successful if the matching score is over a predefined threshold [9].

III. METHODOLOGY

Following are some of methods and technique which is been used to improve the security level. Such as the following:

a) Water Marking Method
b) Beta Skeleton Technique

1) Water Marking Method:

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information does not need to contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copy right and or banknote authentication. Like traditional watermarks, digital watermarks are only perceptible under certain conditions. If a digital watermark distorts the carrier signal in a way that it becomes perceivable, it is of no use. Traditional Watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time. Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal. Since a digital copy of data is the same as the original, digital watermarking is a passive protection tool. It just marks data, but does not degrade it nor controls access to the data. One application of digital watermarking is source tracking. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies.

My work: We have used this water marking method to combine two different fingerprint into one image. By which it is very difficult for the hackers to identify the exact minutiae position of two fingerprints by which security level increases.

2) Beta Skeleton Technique:

In computational geometry and geometric graph theory, a \( \beta \)-skeleton or beta skeleton is an undirected graph defined from a set of points in the Euclidean plane. Two points \( p \) and \( q \) are connected by an edge whenever all the angles \( prq \) are sharper than a threshold determined from the numerical parameter \( \beta \).

Let \( \beta \) be a positive real number, and calculate an angle \( \theta \) using the formulas

\[
\theta = \begin{cases} 
\sin^{-1} \frac{1}{\beta}, & \text{if } \beta \geq 1 \\
\pi - \sin^{-1} \beta, & \text{if } \beta \leq 1 
\end{cases}
\]

For any two points \( p \) and \( q \) in the plane, let \( R_{pq} \) be the set of points for which angle \( prq \) is greater than \( \theta \). Then \( R_{pq} \) takes the form of a union of two open disks with diameter \( d(p,q) \beta \) for \( \beta \geq 1 \) and \( \theta \leq \pi/2 \), and it takes the form of the intersection of two open disks with diameter \( d(p,q) \beta \) for \( \beta \leq 1 \) and \( \theta \geq \pi/2 \). When \( \beta = 1 \) the two formulas give the same value \( \theta = \pi/2 \), and \( R_{pq} \) takes the form of a single open disk with \( pq \) as its diameter.

My Work: We have used this Beta Skeleton Technique to match the databases during enrollment and authentication time. At the time of enrollment the client stores two fingerprint by combining into one image. At the same time of authentication same two fingers are placed and combined, later the combined image is encrypted. Then the server checks by uploading the saved combined fingerprint image and match. At that time Beta Skeleton Technique is used to match two combined fingerprint one stored in server database and the other from the client database, then the matching result appears.

IV. DISCUSSION OF RESULT

Server Part (using Water marking method)
Matching Report

V. COMPARISON OF RESULT WITH OTHER METHOD

Fingerprint comparison is usually based on minutiae matching. The minutiae considered in automatic identification systems are normally ridge bifurcations and terminations. In this paper, we present a set of algorithms for the extraction of fingerprint minutiae from Skeletonized binary images. The goal of the present work is the extraction of the real minutiae of a fingerprint image from the 200 contained in typical Skeletonized and binarized images. Besides classical methodologies for minutiae filtering, a new approach is proposed for bridge cleaning based on ridge positions instead of classical methods based on directional maps. Finally, two novel criteria and related algorithms are introduced for validating the endpoints and bifurcations. The use of the fingerprint minutiae extraction algorithms has also been considered in a fingerprint identification system in terms of timing and false reject or acceptance rates. The presented minutiae extraction algorithm performs correctly in dirty areas and on the background as well, making computationally expensive segmentation algorithms unnecessary. The results are confirmed by visual inspections of validated minutiae of reference fingerprint image database. Their experimental results show that the EER of matching two mixed fingerprints is about 15% when two different fingerprints are randomly chosen for creating a mixed fingerprint. If the two different fingerprints are carefully chosen according to a compatibility measure, the EER can be reduced to about 4%.

VI. CONCLUSION AND FUTURE WORK

In this paper, we introduce a novel system for fingerprint privacy protection by combining two fingerprints into a new identity. In the enrollment, the system captures two fingerprints from two different fingers. A combined minutiae template containing only a partial minutiae feature of each of the two fingerprints will be generated and stored in a database. To make the combined minutiae template look real as an original minutiae template, three different coding strategies are introduced during the combined minutiae template generation process. In the authentication process, two query fingerprints from the same two fingers are required. A two-stage fingerprint matching process is proposed for matching the two query fingerprints against the enrolled template. Our combined minutiae template has a similar topology to an original minutiae template. Therefore, we are able to combine two different fingerprints into a new virtual identity by reconstructing a real-look alike combined fingerprint from the combined minutiae template. Since in fingerprint matching we use combined minutiae template to combine two fingerprint and create an single template, here we are creating multiple combination of the fingerprint of an single finger and get the same procedure for other finger and create an multiple template so that we can able to provide accurate information of the person and we use this information for the data transferring in data centric network so that the privacy of the information can’t be traced because we encrypt the data with the possible template of the fingerprint, thus the data will be secured and thus proper authentication of finger will be obtained which reduces the fraud activities.

REFERENCES