A Survey on Protecting Privacy Using Biometric of Fingerprint Combination

B. Janani M.Sc\textsuperscript{1}, Dr. N. Radha M.Sc, M.phil, Phd\textsuperscript{2}

\textsuperscript{1}Research Scholar, Department of Computer Application, PSGR Krishnammal College for Women, Coimbatore, India.
\textsuperscript{2}Assistant Professor, Department of Computer Application, PSGR Krishnammal College for Women, Coimbatore, India.

Abstract— With the extensive applications of fingerprint techniques in authentication systems, protecting the privacy of the fingerprint becomes an important issue. Traditional encryption is not sufficient for fingerprint privacy protection because decryption is required before the fingerprint matching, which exposes the fingerprint to the attacker. Therefore, in recent years, significant efforts have been put into developing specific protection techniques for fingerprint. In this paper, various methods for recognizing fingerprint have been surveyed. These methods have been compared against the proposed method of SIFT Based Ridge enhanced fingerprint recognition method. Thus each and every method in literature provides satisfiable result and lacks the result in analysis when compared with the proposed research.

I. INTRODUCTION

Recently, fingerprint recognition is one of the leading biometric technologies based on fingerprint distinctiveness, persistence and ease of attainment. Even though there are many real applications utilizing this technology, its problems are still not completely solved, particularly in poor quality fingerprint images and when low-cost acquisition devices with a small area are assumed.

These matching algorithms may be classified into three types such as minutiae-based, correlation-based and feature-based approaches. Still, based on analysis, the score of these algorithms is not high (particularly in case fingerprints are of the same finger but they are rotated or the intersection is moreover small). Consequently, it’s essential to design a model for standardized fingerprint template so as to improve matching score.

Exploring the possibility of generating a template in the direction of conventional fingerprint approach represents a joint identity through a mixing process. In particular, the digital identity has been created by mixing the fingerprints of two individuals to generate a single fingerprint in turn defines the joint identity. Figure 2 refers to the flow of ridge patterns of the fingerprint in the tip of the finger. Irregularities in local regions of the fingertip have been exhibited, referred as minutiae points. The distribution of these minutiae points, with the associated ridge structure, is considered to be different for each fingerprint.

Fig. 1 Fingerprint Recognition process

The basic process of fingerprint recognition process is shown in the above figure 1. In fingerprint recognition process, the significant step which involves on system accuracy is matching between template and query fingerprint. Various solutions are designed to enlarge this step’s accuracy.

Fig 2. A design of mixing fingerprints of two different individuals to generate a mixed fingerprint representing their joint identity

To provide better verification and authentication various methods of fingerprint recognition can be surveyed in the following literature.
II. FINGERPRINT AUTHENTICATION

A. BIO HASHING APPROACH

In [1] Teoh et al. presented a bio hashing approach by estimating the inner products among a pseudorandom number that is probably said to be key and user’s fingerprint features. These two factors of Bio Hashing has major functional advantages over singular biometrics or token usage, namely clear separation of the genuine and the imposter populations and zero EER(Equal error rate) level, thus moderate the suffering from increased amount of FRR while eliminate the FAR(False acceptance ratio). The method of generating a token of pseudo-random vectors happening only once for an individual, it can be assumed secure in the case that there is no mode to recover the fingerprint data by attaining on the token (one-way transformation). Accordingly, a sole compact code per person should be attained, which is highly advantageous in a secure environment and outperforms the standard verification scheme, assumed as a weak-security system for it needs to admit an external database of user data. Additionally, Bio Hashing technique also dealt with the invasion of privacy problem, such as biometric fabrication.

B. NON–INVERTIBLE TRANSFORM APPROACH

In [2] Ratha et al. presented an approach to produce cancellable fingerprint templates by applying noninvertible transforms on the minutiae. The noninvertible transform is conducted by a key; it normally leads to a reduction in matching accuracy. Fundamentally, a user can be given as numerous biometric identifiers as needed by producing a new transformation “key.” Original identifiers can be ignored and replaced when compromised. The performance of some algorithms such as surface folding transformations and Cartesian, polar of the minutiae positions has been compared. It is established through numerous experiments that we can attain revocability and stop cross-matching of biometric databases. It is also shown that the changes are noninvertible by indicating that it is computationally as hard to recover the original biometric identifier from a changed version as through random guessing.

C. FUZZY-FAULT APPROACH

In [3] Nandakumar et al. presented fuzzy fault on the minutiae in turns susceptible to the key-inversion attack. The fuzzy vault construct is a biometric cryptosystem that provides secure system for both the secret key and the biometric template through connecting them within a cryptographic structure. A fully automatic implementation of the fuzzy vault scheme is presented based on fingerprint minutiae. As the fuzzy vault holds only a transformed report of the template, aligning such a query fingerprint with the template is a challenging job. High curvature points derived from the fingerprint orientation field has been extracted and used them as supporting data to align the query minutiae and template. The supporting data itself do not disclose any information about the minutiae template, however contain enough information to align the template and query fingerprints perfectly. In addition, a minutiae matcher has been applied during decoding to justify nonlinear distortion and this show the ways to significant improvement in the genuine accept rate.

D. VISUAL CRYPTOGRAPHIC SCHEME

In [4] Othman presented visual cryptography for guarding the privacy of biometrics. The fingerprint image is partitioned by utilizing a visual cryptography scheme to create two noise-like images (referred as sheets) which is stored in two distinct databases. While authentication, the two sheets are stacked to create a temporary fingerprint image for matching. The benefit of this system is that in which the identity of the biometrics is never exposed to the attacker in a single database. Still, it needs two distinct databases to work jointly, which is not useful in same applications.

E. MULTI BIOMETRIC TEMPLATE

In [5] Yanikoglu et al. presented two distinct fingerprints into a single identity either in the image level or in the feature level. In this the idea of combining two different fingerprints into a new identity is first projected, where the novel identity is created by combining the minutiae positions extracted from the two different fingerprints. The positions of original minutiae of each fingerprint can be defended in the new identity. Yet, it is easy for the attacker to identify such a new identity since it holds more minutiae positions than that of an original fingerprint.

In [6] Arun Ross presented the method in which an input fingerprint image is mixed with another fingerprint that is from a different finger, so as to produce a new mixed image that produces difficult to understand the identity of the original fingerprint. Mixing fingerprints produces a new unit that looks like a reasonable fingerprint and, therefore, (a) it can be practiced by traditional fingerprint algorithms and (b) an intruder may not be able to decide if a given print is mixed or not. In order to mix two fingerprints, each fingerprint is partitioned into two components, viz., the spiral and continuous components. Subsequent to the pre-aligning the two components of each fingerprint, the continuous component of one fingerprint is united with the spiral component of the other fingerprint image so as to generate a mixed fingerprint.

In [7] Eren Camlikaya et al. presented a multimodal biometric verification system by mixing fingerprint and voice modalities. The framework combines the two modalities at the template level, using multiibiometric templates. The combination of fingerprint and voice data productively diminishes privacy concerns through hiding the minutiae points from the fingerprint, between the artificial points produced by the features which are attained from the spoken utterance of the speaker.
III. CONCLUSION

In the present work, various methods of fingerprint recognition have been surveyed. The methods based on Bio hashing approach, Non –invertible transform approach provides better accuracy however it is vulnerable to intrusion and linkage attacks when both the key and the transformed template are stolen. Then Fuzzy-fault approach provides better recognition since it vulnerable to the key-inversion attack. Next the scheme of visual cryptography is used for the purpose of authentication and confidentiality however it requires two separate databases to work together, which is not practical in same applications. Finally, Multibiometric template scheme has been used for providing robust integrity among fingerprint templates and difficult for the attacker to distinguish a mixed fingerprint from the original fingerprints. However the ridge enhancement is not addressed in these approaches when the user fingerprint is considered in a least frequency model. Thus the proposed scheme outperforms these model and authentication has been done through the ridge enhancement based on SIFT based approach.

REFERENCES


