Forensic Science International 288 (2018) 256–265

Contents lists available at ScienceDirect

Forensic Science International

journal homepage: www.elsevier.com/locate/forsciint

A robust and non-invertible fingerprint template for fingerprint matching system

Amit Kumar Trivedi*, Dalton Meitei Thounaojam, Shyamosree Pal

Department of Computer Science and Engineering, National Institute of Technology, Silchar, India

ARTICLE INFO

Article history:
Received 22 August 2017
Received in revised form 13 April 2018
Accepted 18 April 2018
Available online xxx

Keywords:
Fingerprint
Identification
Matching
Minutiae
Reconstruction
Template

ABSTRACT

Fingerprint Recognition System is widely deployed in variety of application domain, ranging from forensic to mobile phones. Its widespread deployment in various applications were person authentication are required, has caused concern that a leaked fingerprint template may be used to reconstruct the original fingerprint and the reconstructed fingerprint can be used to circumvent all the applications the person is enrolled. In this paper, a non-invertible fingerprint template that stores only the relative geometric information about the minutiae points is proposed. The spatial location of the minutiae points in original fingerprint and its orientations are not available in the proposed template which makes it impossible to estimate the orientation of fingerprint from the template. The proposed template is invariant to rotation, translation and distortion and immune to reconstruction algorithm. The proposed system is experimented using standard FVC2000 database and yields better results in terms of EER and FMR as compared with latest techniques.

1. Introduction

Now-a-days, Biometric (face image, fingerprint, iris, etc.) identification are widely used in government and private organizations either for identification and authentication of documents or for surveillance [1]. The extensive use of biometrics has raised increasing concern about the privacy and security biometrics security system itself [2]. The combination of very sophisticated hardware and software are used for biometric system. These system uses vendor specific software and database. Most of the algorithms used in biometric system for template generation and matching go along with the following steps [3]:

- capture biometric sample using sensors,
- transforming captured biometric sample into compact template and
- calculation of match score by matching the new (or live) template to stored templates.

Score generated by matching algorithm indicates similarity between live sample and target. The template representation is typically vendor specific. Template is a compact representation of feature used to store the identity of the subject. Many biometric system manufacturers have claimed that it is impractical to reconstruct the image from the templates (for example [4,5]). Considering this claim, biometric templates may be considered as non-identifiable data, much like a password hash [6]. Such type of biometric template can be stored in unprotected database. This assumed non-identifiability has been used to ignore the concerns expressed by biometric system users that their biometric data may stolen from their storage on identification cards etc. But researchers have shown that biometric templates are not non-identifiable as it is suppose to be. Adler [3] has shown that a coarse image of the source image can be reconstructed from biometric templates using a “hill climbing” strategy guided by match score value. To prevent the “hill climbing” strategy for biometric image reconstruction, the authors of the BioAPI specification [7] suggested that match score values can be quantized. So the small changes to the biometric image will be not reflected in quantized match score [8] and prevents such a “hill-climbing” attack [9]. Acceptance and invariability of fingerprint biometric increased the interest to use it as authentication and identification in security system.

1.1. Fingerprint feature

Fingerprint is ridge and valley like structure present on tip of the finger. Fig. 1 shows ridge and interleaving valleys that makes fingerprint and it contains fingerprint feature. These features can be categorized into three levels [10] as shown in Fig. 2.

* Corresponding author.
E-mail addresses: rivedi19@gmail.com (A.K. Trivedi), dalton.meitei@gmail.com (D.M. Thounaojam), shyamosree.pal@gmail.com (S. Pal).

https://doi.org/10.1016/j.forsciint.2018.04.045
0379-0738/© 2018 Elsevier B.V. All rights reserved.

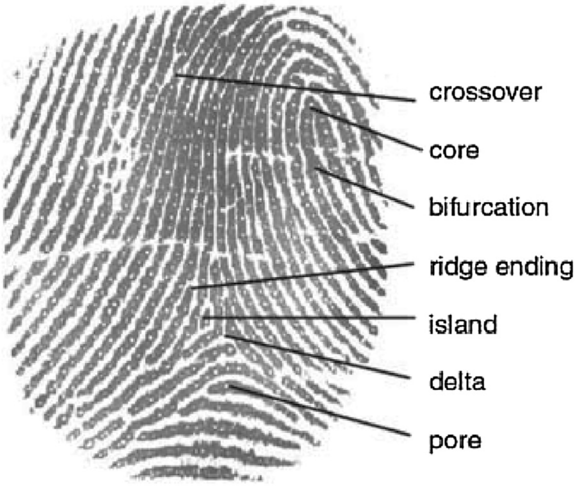

Fig. 1. The fingerprint image shows the features, which are used by most of fingerprint authentication/verification system. Ridge endings are the points where ridge terminate and at bifurcations ridge divides into two ridges. There are many different types of minutiae like pore, core, delta, etc.
Image taken from http://cnx.org/content/m12574/1.3/ [11], with permission of OpenStax CNX.

i. The level 1 feature mainly refers to ridge orientation. Depending on ridge orientation, Sir Edward Henry classifies the fingerprint into five classes: arch, tented arch, left loop, right loop and whorl. The singular points and pattern types are the main features derived from the level 1 feature.
ii. The level 2 features mainly contain features of ridge skeleton. The ridge bifurcation and terminations are the main features derived from the level 2 features.
iii. The level 3 features include information about position and shape of sweat pores, ridge contours and incipient ridges. A very high resolution sensor is required to capture these informations. These features are rarely used in biometrics system.

1.2. Fingerprint representation schemes

Most of the fingerprint recognition systems uses one of the four fingerprint representation schemes: gray-scale image, skeleton image, phase image and minutiae as shown in Fig. 3. Out of these four representation schemes, the minutiae is most distinct, compact and compatible with features used by human fingerprint experts and has become the most widely adopted fingerprint representation scheme for automated fingerprint matching system. Other representation schemes show strong performance but more prone to attack. The gray-scale representation scheme or gray scale image contains maximum informations and features of fingerprint at all levels and it makes the gray scale image most venerable to attack. In comparison to gray-scale image, skeleton image and phase image lose all the level 3 features. In comparison to skeleton image and phase image, the minutiae template lose all the level 3 and some of the level 2 features.

Among different types of fingerprint representation schemes, minutiae representation is the most widely used. It is very compact and contains enough information to identify a person, but contains very few information to reconstruct the original fingerprint [12]. The minutiae template contain least amount of information and is

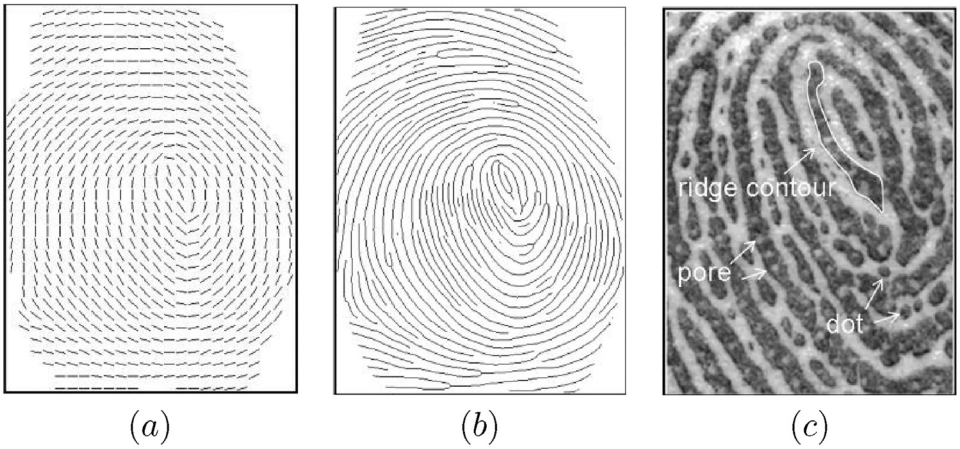

Fig. 2. Feature at three levels in fingerprint: (a) Level 1 features, (b) Level 2 features and (c) Level 3 features.

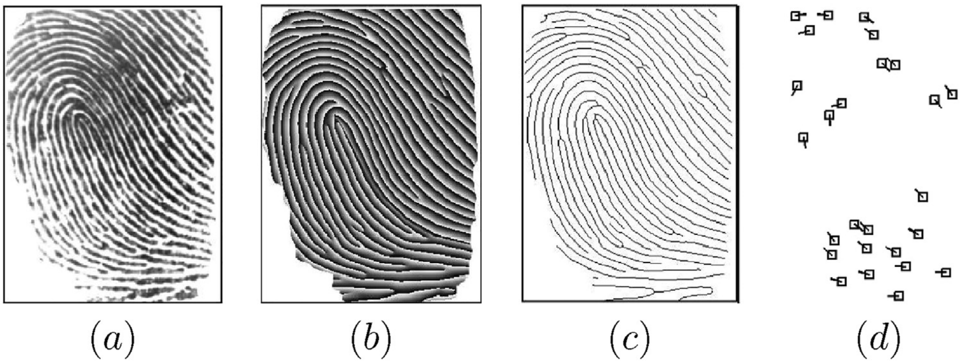

Fig. 3. Fingerprint representation schemes: (a) gray image, (b) phase image, (c) skeleton image and (d) minutiae.