Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 3, Issue 7, July-2016

Fingerprint Image Quality Parameters: A Review

Muskan Sahi [#1], Kapil Arora[#2]

[12] Department of Electronics and Communication

[12]RPIIT, Bastara

Haryana, India

Abstract— Biometrics system has now become the most popular method for the person identification. The quality of the biometric image captured should be robust enough to minimize/eliminate duplicate and fake identities. The Integrated Automated Fingerprint Identification System (IAFIS) Appendix F Standard and PIV Specification Standards are acclaimed standards for validating the quality of biometric images. To assure the good quality of biometric image it is important that the fingerprint scanner shall be capable of producing images that exhibit good geometric fidelity, sharpness, detail rendition, gray-level uniformity, and gray-scale dynamic range, with low noise characteristics. In this paper the biometrics type, fingerprint scanner image quality specification according to the ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) standards is given. These specifications provide criteria for ensuring the image quality of fingerprint scanners that input fingerprint images to, or generate fingerprint images from within, an Automated Fingerprint Identification System (AFIS).

Keywords— **Fingerprint Scanner, Image Quality, Biometrics**

I. INTRODUCTION

Biometrics refers to the use of distinctive anatomical (e.g., fingerprints, face, iris) and behavioral (e.g., speech, signature) characteristics, called biometric identifiers or traits for automatically recognizing individuals. Biometrics is an essential component of effective person identification solutions because biometric identifiers cannot be shared or misplaced, and they intrinsically represent the individual's bodily identity. A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database.

FINGERPRINTS

A fingerprint is an impression left by the friction ridges of a human finger. Human fingerprints are detailed, nearly unique, difficult to alter, and durable over the life of an individual, making them suitable as long-term markers of human identity.

Figure 1: Fingerprint

Depending on the application context, a biometric system may operate either in verification mode or identification mode:

- A verification system authenticates a person's identity by comparing the captured biometric characteristic with her previously captured (enrolled) biometric reference template pre-stored in the system. It conducts one-to-one comparison to confirm whether the claim of identity by the individual is true. A verification system either rejects or accepts the submitted claim of identity.
- An identification system recognizes an individual by searching the entire enrollment template database for a match. It conducts one-to-many comparisons to establish if the individual is present in the database and if so, returns the identifier of the enrollment reference that matched. In an identification system, the system establishes a subject's identity (or determines that the subject is not enrolled in the system database) without the subject having to claim an identity.

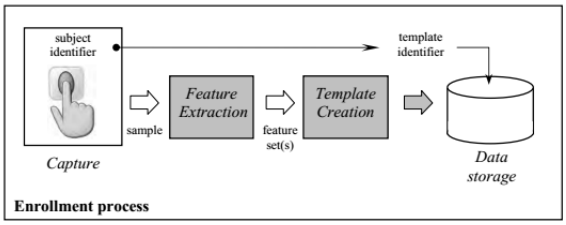

Figure 2: Enrollment Process

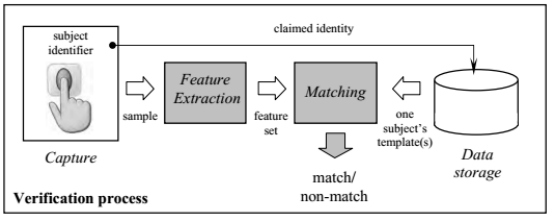

Figure 3: Verification Process

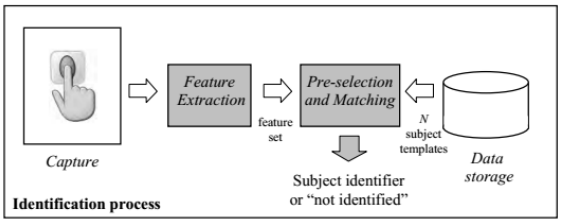

Figure 4: Identification Process

User enrollment is a process that is responsible for registering individuals in the biometric system storage. During the enrollment process, the biometric characteristic of a subject is first captured by a biometric scanner to produce a sample. A quality check is often performed to ensure that the acquired sample can be reliably processed by successive stages. A feature extraction module is then used to produce a feature set. The template creation module uses the feature set to produce an enrollment template. Some systems collect multiple samples of a user and then either select the best image (or feature set) or fuse multiple images (or feature sets) to create a composite template. The enrollment process then takes the enrollment template and stores it in the system storage together with the demographic information about the user (such as an identifier, name, gender, height, etc.)

QUALITY PARAMETERS

Unique Identification Authority of India (UIDAI) has selected biometrics as the primary method to check duplicate identity record. In order to ensure that an individual can establish their identity uniquely in an easy and cost effective manner, it is essential that the captured biometrics information is:

- Robust enough to minimize/eliminate duplicate and fake identities.
- Can be verified and authenticated.

Quality of biometrics information depends on the quality of device and biometrics images obtained. Quality parameters of a fingerprint image gives the ability of a fingerprint scanner to acquire images that maximize the accuracy of automated recognition algorithms. Different elements contribute to the fingerprint image quality: Scanner (Poor image quality), finger (cuts on the fingertip), and user-dependent factors (incorrect finger placement).

There are mainly six parameters that are defined in the ISO/IEC 19794-4:2011 which describes the overall quality of the images of the fingerprint scanners.

- Geometric Accuracy
- Linearity
- Gray-level uniformity
- Signal-to-noise ratio
- Spatial frequency response
- Gray Scale Linearity Output
- Fingerprint Image Quality

II. LITERATURE REVIEW

According to R. Cappelli. *et al.,* the operational quality of fingerprint scanners is the ability of acquiring images that maximize the accuracy of automated fingerprint recognition. Experiments have been carried out by the authors which showed the most critical quality parameters.

Sravya. V. *et al.,* presents the detailed information about fingerprint biometrics and specially focused on methods that overcome the disadvantages of fingerprint biometric system. It explains the privacy and security issues of the biometric systems.

A. Alessandroni. Et al., analyzes two recently released image quality specifications for single-finger scanners i.e PIV (Personal Identification Verification) & PassDEÜV and proposes three new CNIPA-A/B/C specifications targeted to different types of applications.

ISO/IEC 19794-4:2011 consists of a variety of mandatory and optional items, including scanning parameters, compressed or uncompressed images and vendor-specific information.

III. CONCLUSION

The fingerprint capture device shall provide fingerprint image quality which is high enough to support the intended applications; a primary application is to support subject authentication via one-to-one fingerprint comparison. The fingerprint capture device is expected to generate good quality finger images for a very high percentage of the user population, across the full range of environmental variations seen in the intended applications.

References:

[1]Raffaele Cappelli, Matteo Ferrara, and Davide Maltoni " On the Operational Quality of Fingerprint Scanners " IEEE Transactions on Information Forensics and Security" Volume:3 , Issue: 2 pp 192 – 202.2008

[2]Sravya. V, Radha Krishna Murthy, Ravindra Babu Kallam, Srujana B "A Survey on Fingerprint Biometric System "International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 4, April 2012.

[3]A. Alessandroni, R. Cappelli, M. Ferrara, D. Maltoni. "Definition of Fingerprint Scanner Image Quality Specifications by Operational Quality "

[4] .Handbook of Fingerprint Recognition Second Edition by Davide Maltoni, Dario Maio, Anil K. Jain Salil Prabhakar

[5] A Survey on Fingerprint Biometric System Sravya. V, Radha Krishna Murthy,Ravindra Babu Kallam, Srujana B Aizza College of Engineering & Technology, Mancherial India

[6] ISO/IEC 19794-4:2011

[7] Personal Identity Verification; information available at: http://csrc.nist.gov/piv-program

[8] FBI certified product list. 2007. [Online]. Available: http://www.fbi.gov/hq/cjisd/iafis/cert.htm.