Appendix III

FingerTec® Technology White Paper

MAY 2005 • VERSION 1

Compiled by Y.C. Khong

SCOPE

FingerTec® technology is an advanced fingerprint-matching algorithm that ensures accuracy and security when used as an authentication method. FingerTec® technology is the foundation for all authentication solutions from FingerTec® and operates seamlessly with many third-party security applications, smart cards and biometric readers on the market. This article describes the principles and advantages of FingerTec® technology.

INTRODUCTION

Using biometrics to verify identity means using a physical characteristic such as face, voice or fingerprints to authenticate an individual's claimed identity. Fingerprint matching is by far the most successful biometric technology because of its ease of use, non-intrusiveness and reliability. Fingerprints consist of ridges and valleys formed in complex patterns that are unique for every person and thereby provide an optimal verification method.

This article discusses two main algorithm families commonly used to recognize fingerprints: minutia based and pattern based matching. These two methods evaluate fingerprint images in different ways; minutia matching compares specific details within the fingerprint ridges while pattern matching compares the overall characteristics of the fingerprints. As will be shown in this article, both methods have advantages and disadvantages. FingerTec® continued research and development work has led to a more reliable and efficient fingerprint technology, the FingerTec® solution.

FingerTec® technology is designed for those integrated solution company, computer manufacturer, PDA manufacturer and other professional time and attendance, door access security, network security manufacturer that required ultimate fingerprint algorithm. FingerTec® is a reliable technology where it has been well-research and developed for more than 15 years, near 10 millions of users has been using it.

FingerTec® has tested and compared with almost all international fingerprint algorithm, and now it is compatible with most of the fingerprint sensor, with 360° rotation, high identification speed, and suitable for any public or defence application with a low expectation on fingerprint image (> = 200dpi). A typical example is a national or sub-national ID card, where the template on the ID card will be matched against live fingerprint images from a broad variety of sensors. The FingerTec® requires small amount of memory, where whole matching algorithm required just 350KB, allowing low-cost DSP or CPU-based hardware product is possible equipped with Biometric technology.

FINGERPRINT MATCHING METHODS

Minutia Matching:

Every fingerprint consists of a number of ridges and valleys. Ridges are the upper skin layer segments of the finger and valleys are the lower segments. The ridges form so-called minutia points; ridge endings-where a ridge ends-and ridge bifurcations-where a ridge splits.

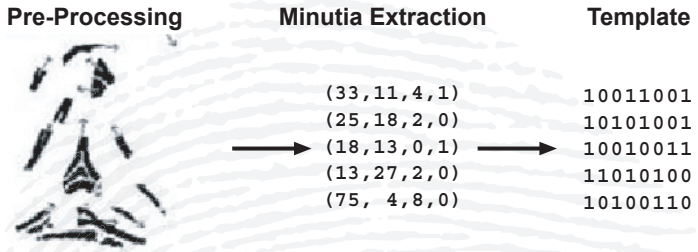

Figure 1: Enrolment of minutia points.

At registration-enrollment-the minutia points are located (figure 1) and the relative positions to each other and their directions are recorded. This data forms the template, the information later used to authenticate a person. At the matching stage (figure 2), the incoming fingerprint image is pre-processed and the minutia points are extracted. The minutia points are compared with the registered template, trying to locate as many similar points as possible within a certain boundary. The result of the matching is usually the number of matching minutiae. A threshold is then applied, determining how large this number needs to be for the fingerprint and the template to match.

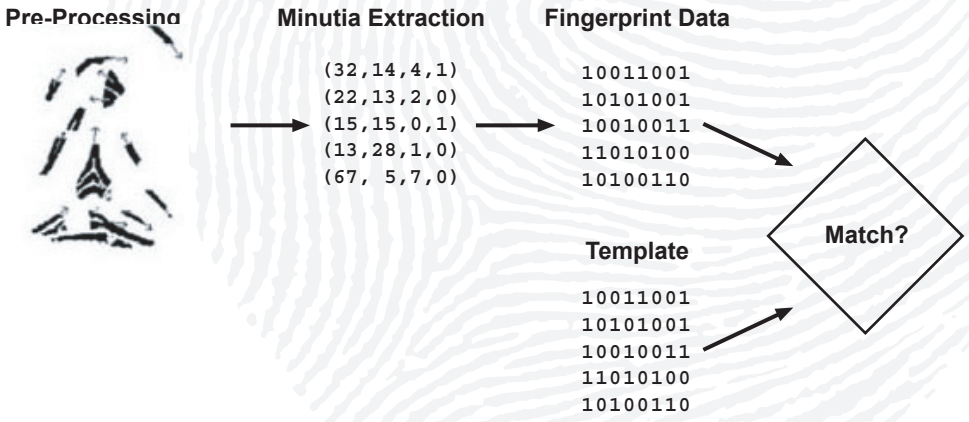

Figure 2: Verification using minutia points.

Pros:

- Used in AFIS applications
- Well-known and well-researched method
- Algorithm is well suited for 1-many matching

Cons:

- Cannot be used with all fingerprint sensor technologies, since it puts high demands on sensor resolution and sensor size. Gives poor results with fingerprint sensors less specified than AFIS grade.
- People with no or few minutia points (special skin conditions) cannot enroll or use the system. The number of minutia points can be a limiting factor for security of the algorithm.
- Can be confused by false minutia points (areas of obfuscation that appear due to low-quality enrollment, imaging, or fingerprint ridge detail).