



Provided by the author(s) and University of Galway in accordance with publisher policies. Please cite the published version when available.

Title	Determining Unique Fingerprint Features for Biometric Encoding of Data
Author(s)	Cucu, Catalin; Cucos, Alex; Corcoran, Peter M.
Publication Date	2008-01-09
Publication Information	Cucu, C., Cucos, A., & Corcoran, P. (2008). Determining Unique Fingerprint Features for Biometric Encoding of Data. Paper presented at the Consumer Electronics, 2008. ICCE 2008. Digest of Technical Papers.
Publisher	IEEE
Link to publisher's version	http://www.ieeexplore.ieee.org/search/srchabstract.jsp?tp=&arnumber=4588002
Item record	http://hdl.handle.net/10379/1342

Downloaded 2024-04-19T08:03:41Z

Some rights reserved. For more information, please see the item record link above.



9.1-1

Determining Unique Fingerprint Features for Biometric Encoding of Data

Catalin Cucu, Alex Cucos and Peter Corcoran, *Member, IEEE*
National University of Ireland, Galway

Abstract- A novel approach to determining unique fingerprint features with high repeatability is described. The techniques described are particularly suitable for CE applications and devices employing inexpensive capacitive fingerprint sensors. The extraction of robust seeds for generating repeatable encryption keys is discussed and some preliminary approaches are described.

I. INTRODUCTION

Typical applications for biometric authentication require very accurate sensing technique with high repeatability [1] or a complex analysis technique [2] which can compensate for variations in the sensing process.

Our interests lie in applying authentication techniques to CE devices and services and in the use of biometrics to manage digital content [3]. These CE applications have very different requirements. The strict level of authentication used in specialized business applications is simply not required; faster response times and greater certainty of correct user authentication are desirable. Using these criteria would enable biometric authentication to be built directly into the recording switch on a digital media recorder.

II. FINGERPRINT MATCHING TECHNIQUES

In this paper we focus on a novel approach to extracting robust, rotation invariant features from a typical set of fingerprint minutiae. To place our work in context it is useful to quickly summarize some of the prior art in fingerprint analysis.

Quite a few different algorithms have evolved, particularly from the field of image registration to determine an optimal match between two 2D point patterns. Amongst the most recent approaches we mention the iterative closest point algorithm (ICP) described in [4]. For real-time applications [5] examines performance improvements to the basic algorithm. However such algorithms are unsuited to our purposes as they assume a correspondence between the point sets to be matched and are not optimized to indicate quickly when point sets are unlikely to allow a good match.

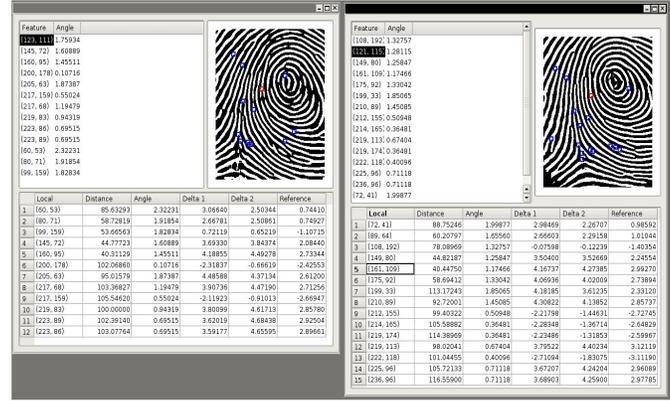


Fig 1: UI to our Fingerprint Analysis Tools

An alternative approach to fingerprint pattern matching is provided by analyzing the ridge-field fingerprint pattern. This provides useful global information which is relatively robust to the quality of image acquisition [6]. When combined with local, minutiae based features the use of this orientation field data provides accurate and robust matching [7]. However the algorithms proposed by these authors are too slow for consumer applications.

A number of authors have turned their attention to another approach based on the use of local triangular features formed from nearest-neighbor minutiae groupings [8-11]. One weakness in the use of such triangular descriptors, and indeed for all of the above techniques is that they are susceptible to erroneous acquisition data.

III. DETERMINATION OF UNIQUE AND ROBUST FEATURES

Bearing the above considerations in mind we have developed a novel approach to extracting repeatable fingerprint features from the unreliable minutiae feature sets which occur when low-resolution fingerprint sensors are employed for biometric authentication or encoding applications. Our approach draws inspiration partly from the local triangular features described by the authors of [11]. To overcome the problem of unreliable minutiae we only require that a repeatable feature consists of two corresponding minutiae, and each minutiae point may be analyzed in terms of the set of features it shares with its neighboring minutiae

points. This is illustrated in **Fig 2** below.

To properly determine a set of such repeatable two-point features we employ a multi-stage enrollment where the user must provide a set of, typically, 4-6 fingerprint scans. After each scan the set of determined features is classified into a set of angle and distance bins. Minutiae are matched across the set of scans – this is easily achieved by a comparison of the extracted feature sets. Then the most repeatable features from each minutiae are recorded across the set of enrollment scans.

Neighbor	Distance	Angle	Self Angle
A	A	284.1°	50.1°
B	B	209.7°	143.2°
C	C	296.9°	242.6°

Where a scan is of poor quality or yields a significantly higher or lower number of minutiae points it is rejected and the enrollee is requested to enter additional enrollment scans as necessary.

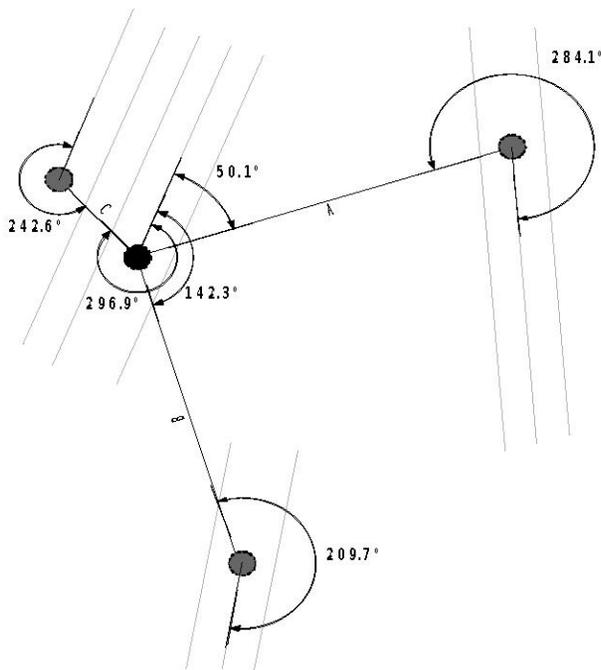


Fig 2: A minutiae and its three nearest neighbours.

At the end of the enrollment process the most reliable two-point features are determined. Minutiae points which have at least 2 high-reliability features associated with them are retained within the enrollment set. In this way we typically obtain 3-4 minutiae points and 6-10 high reliability two-point features. The resulting enrollment data set is not unduly large and facilitates fast authentication or the generation of repeatable encryption keys.

The corresponding matching process involves obtaining a single fingerprint scan. The associated set of minutiae are analyzed for two-point features. Typically we begin at the central minutiae points and work outwards. A set of features is extracted for each minutiae point and compared with the enrolled features.

For CE applications, such as media encoding [12] it is typically sufficient to match two features on a common minutiae, or to match three across different minutiae. When applications are more security conscious it may be required to match a larger number of features.

ACKNOWLEDGMENT

This research was funded under the *Technology Development Phase* of the Enterprise-Ireland Commercialization Fund.

REFERENCES

- [1] http://bio-tech-inc.com/Bio_Tech_Assessment.html
- [2] Yongdong Wu, Feng Bao, Robert H. Deng, Secure Human Communications Based On Biometrics Signals, 20th IFIP International Information Security Conference (SEC 2005), pp.205-221, Chiba, Japan, May 30 - June 1, 2005
- [3] Corcoran, P., and Cucos, A.; Techniques for securing multimedia content in consumer electronic appliances using biometric signatures, IEEE Trans Consumer Elec., Vol. 51, No. 2, pp. 545-551, May 2005
- [4] P.J. Besl and N. D. McKay. A method for registration of 3-d shapes. IEEE Trans. Pat. Anal. and Mach. Intel. 14(2), pp 239-256, Feb 1992.
- [5] S. Rusinkiewicz and M. Levoy, Efficient Variants of the ICP Algorithm, Proceedings of the 3rd International Conference on 3D Digital Imaging and Modeling, pp145-152, Quebec, Canada, May 2001.
- [6] A. N. Marana, and A. K. Jain, Ridge based fingerprint matching using Hough Transform, Proceedings of the XVIII Brazilian Symposium on Computer Graphics and Image Processing (SIBGRAPI '05), 2005.
- [7] J. Gu, J. Zhou, and C. Yang, Fingerprint Recognition by Combining Global Structure and Local Cues, IEEE Transactions on Image Processing, Vol 15, No 7, p. 1952-64, July 2006.
- [8] Z. M. Kovacs-Vajna, A fingerprint verification system based on triangular matching and dynamic time warping, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol 22, No. 11, p. 1266-1276, Nov 2000.
- [9] X. Jiang, and Y-W, Yau, Fingerprint minutiae matching based on the local and global structures, Proceedings of 15th International Conference on Pattern Recognition, p 1038-1041, 2000.
- [10] X. Chen, J. Tian, X. Yang, and Y. Zhang, An algorithm for distorted fingerprint matching based on local triangle feature set.
- [11] X. Zhao, Y. Wang, J. Qi, and X. Zheng, Non-Alignment Fingerprint Matching Based on Local and Global Information, Proceedings of the First IEEE International Conference on Innovative Computing, Information and Control (ICICIC), 2006.
- [12] P. Corcoran, C. Iancu, F. Callaly, M. Leyden and A. Cucos, "Biometric Access Control for Digital Media Streams in Home Networks", IEEE Trans. on Consumer Electronics., Vol. 53, No. 3, August 2007