Real-Time Fingerprint Analysis & Authentication for Embedded Appliances

Frank Callaly, Catalin Cucu, Alex Cucos, Mark Leyden and Peter Corcoran, *Member, IEEE*

***Abstract* — A complete fingerprint analysis system is described. The design and architecture of a loadable device driver for a USB fingerprint sensor is described. Image processing filters to enhance the raw image data and to extract key points from fingerprint images are also described. Finally a novel pattern matching techique which allows fast authentication is described. The results of initial reliability testing and some example applications of fingerprint authentication in CE appliances are given.**

***Keywords* — Biometrics, Multimedia, Digital Media Encoding, Home Networks.**

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. Either of these approaches can yield a high level of granularity for the comparison step but with the trade-off of requiring an expensive sensing subsystem or sufficient computing power and memory to perform complex post-processing. Typical applications will also require secure access to a large database for comparing acquired and processed biometric signatures. In the CE sector a number of PDA appliances featuring built-in fingerprint authentication have appeared in recent years. Such devices have, however, been targeted at business users and are marketed as providing a means to secure sensitive business data in the case of theft or loss of the PDA appliance. Again they require strict authentication and can occasionally cause problems by preventing users from accessing their stored data.

Our interests lie in applying authentication techniques to CE devices and services and in the use of biometrics to manage digital content and as a means for actuating the recording or duplication process for digital content [3]. These CE applications have different requirements: the strict level of authentication which is necessary for specialized business applications is simply not necessary; faster response times and greater certainty of correct user authentication are desirable. Using such modified criteria could allow biometric authentication to be built directly into the recording switch on a digital media recorder.

In order to investigate further the concepts of flexible authentication for CE applications we have implemented our own fingerprint analysis and verification system which is described in this paper. A useful summary of biometric techniques for fingerprint analysis and matching can be found in [4].

There are 6 key components to our system:

(i) a touch sensitive USB fingerprint sensor
(ii) an interrupt driven Linux device driver
(iii) image enhancement algorithms
(iv) a keypoint extraction software module
(v) a pattern matching module
(vi) a database for storing data from enrolled users

In addition we have built support applications which allow user enrollment, user authentication and batch mode testing of the sensor input.

II. USB Fingerprint Sensor

TFor our initial system development the DKF200 software development kit from Fujitsu Inc was used with the MBF200 fingerprint sensor to implement the fingerprint scanning subsystem. The MBF200 features a built-in USB interface which makes it an ideal peripheral for appliances with USB host or OTG connetivity.

The DKF200 kit also includes supporting software libraries, however these did not provide access to raw image data of acquired fingerprints so we developed our own device driver to enable such access. Thus the image processing algorithms described in this paper may be applied to any generic fingerprint image and are not specific to this sensor hardware.

III. Device Driver Architecture

WThis is illustrated in ***Fig 1*** below. The driver makes use of the touch sensitivity of the MBF200 to generate interrupts, allowing background processing of acquired fingerprints. It can be ported to embedded appliances which supports the standard Linux USB subsystem.

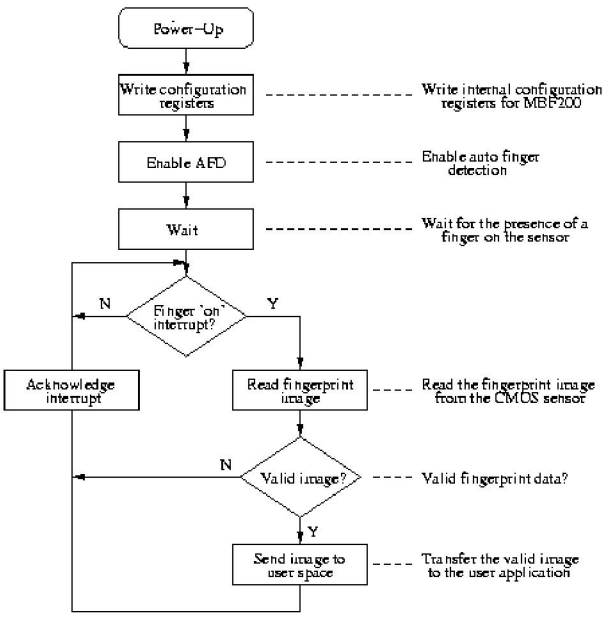

Fig 1: *Device Driver Architecture*

This work is supported under the CFTD Program (CFTD/2004/206) of Enterprise Ireland under the National Development Plan.

Peter Corcoran is with the Dept. Electronic Engineering, National University of Ireland, Galway (e-mail: peter.corcoran@nuigalway.ie).

IV. Image Enhancement Algorithms

The main steps in our enhancement algorithm are illustrated in ***Fig 2***. The algorithm has been optimized to run on embedded systems. It can can also run in a network distributed mode when image processing is performed on a central server to reduce the computational burden on a less powerful embedded CPU. Examples of raw and corrected images are illustrated in ***Fig 3***. The algorithm is an modified version of the method described in [5]

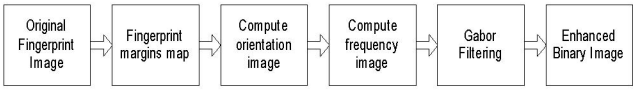

Fig 2: *Fingerprint Enhacement Algorithm*

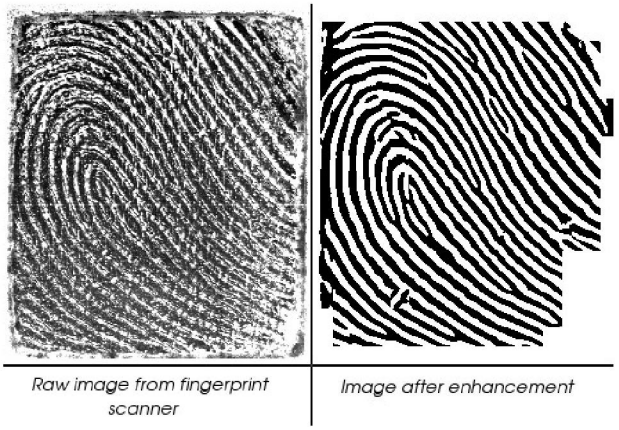

Fig 3: Original & Enhanced Fingerprint Images

V. Minutiae Extraction Algorithm

TAn overview of this algorithm is given in ***Fig*** 4 below. Again the algorithm has been optimized for embedded appliances, or may be run in a network distributed mode.

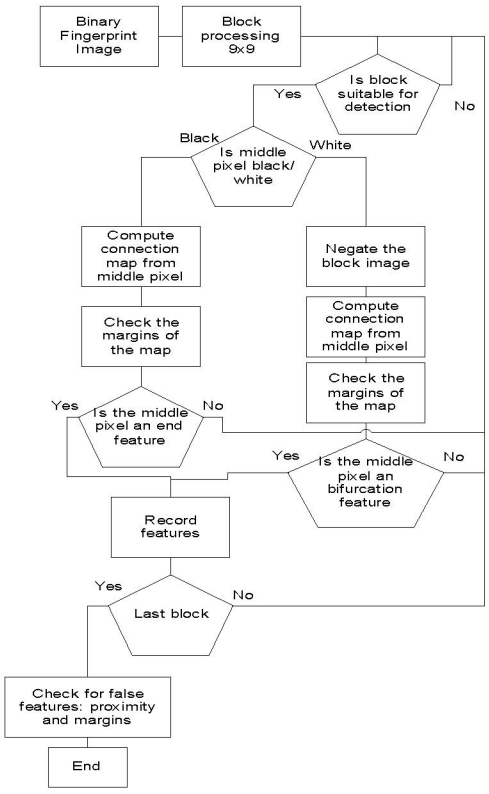

Fig 4: *Minutiae extraction algorithm*

VI. Fingerprint Pattern Matching

The patten matching algorithm, illustrated in ***Fig 5*** below, employs a novel approach which enables orientation matching to be combined with the determination of an overall measure of pattern similarity. This aspect of our system is particularly advantageous for embedded appliances as it eliminates the need for a separate alignment step for the two patterns being compared.I

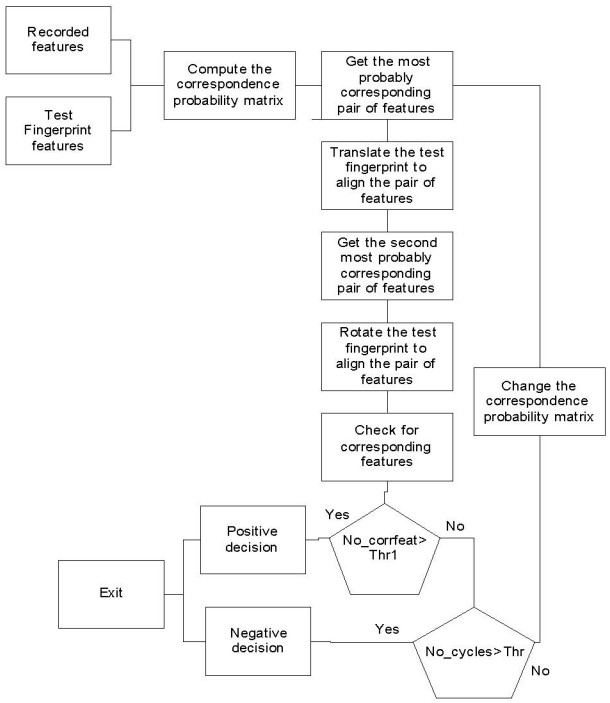

Fig 5: *Fingerprint matching algorithm*

VII. Example CE Applications

The system serves as a component in multimedia encoding and content rebroadcasting system such as those described in [3].

Performance has been improved from several tens of seconds to achieve complete processing time of 3-5 seconds on an 800 Mhz CPU. We expect to be able to further improve this to achieve processing times of less than 1 second once the individual algorithms are further optimized.

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 Transactions on Consumer Electronics, Vol. 51, No. 2, pp. 545-551 , May 2005

[4] D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, Handbook of Fingerprint Recognition; Springer, 2003

[5] L. Hong, Y. Wan and A. Jain, "Fingerprint Image Enhancement: Algorithm and Performance Evaluation", IEEE PAMI, Vol 20. No. 8, 1998.