Microprocessors and Microsystems 35 (2011) 510–521

Contents lists available at ScienceDirect

Microprocessors and Microsystems

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

An embedded multi-core biometric identification system

G. Danese, M. Giachero, F. Leporati *, N. Nazzicari

Dip. di Informatica e Sistemistica, University of Pavia, via Ferrata, 1, Italy

ARTICLE INFO

Article history:
Available online 17 March 2011

Keywords:
Multiple-processor systems
Algorithms implemented in hardware
Field programmable gate arrays
Real-time and embedded systems
Biometric authentication

ABSTRACT

Biometric identification systems exploit automated methods of recognition based on physiological or behavioural characteristics. Among these, fingerprints are very reliable as biometric identifiers. In order to build embedded systems performing real-time authentication, a fast computational unit for image processing is required. In this paper we propose a parallel architecture that efficiently implements the high computationally demanding core of a matching algorithm based on Band-Limited Phase Only spatial Correlation (BLPOC), performed by two concurrent computational units implemented onto a Stratix II Altera family FPGA. The device here described is competitive with similar hardware solutions described in literature and outperforms the elaboration capabilities of general-purpose processors.

1. Introduction

A quick and accurate system of personal identification can be of tremendous importance to restrict the access to places or resources to legitimate users, by now, and particularly after 9/11, such systems are part of our daily life. Traditional identification means, either token-based (access cards, keys, etc.) or knowledge-based (passwords, PINs, etc.), may be subject to theft or discovery. However, these are not the only identification technologies available. Biometric systems help to identify people by exploiting their physiological or behavioural differences. These systems do not rely on reproducible information, and therefore they are not liable to the risks characterizing passwords and keys.

Among the various biometric parameters that can be used to identify a person, fingerprints are undoubtedly the most used, as they are easy to acquire and have been studied since the 19th century, indeed, fingerprint recognition systems can now be found into many commodity goods (such as notebooks).

Despite their long history, Automated Fingerprint Identification Systems (AFIS) [1,2] still offer interesting challenges. More specifically, the time required to compare two fingerprints can become a problem if general-purpose computers are used, especially when the database to which we are comparing our sample is very large.

This is the main reason for the extensive work in the development of efficient dedicated architectures able to compare two fingerprints in a small fraction of the time needed by a general-purpose computer.

In this paper, we propose the FPGA architecture of a complete AFIS system. The Band-Limited Phase-Only Correlation [3,4] algorithm is used to compute the matching scores between a new (*input*) fingerprint and each image contained in a database. Several computational cores can be hosted on a single chip computer together with a general-purpose processor. External memories are managed through DMA and can be dynamically configured and a bottleneck/scalability projection is proposed.

After a brief description of the state of the art, the algorithm will be illustrated in detail. The hardware architecture is also discussed, followed by a description of the software implementation used as a term of comparison. Then, the performance (both in terms of speed and accuracy) will be described, and some conclusions drawn.

2. Fingerprints

Typical fingerprints are characterized by an alternation of *ridges* and *furrows* (dark and light areas in Fig. 1); fingerprints are different for each individual, and each finger of the same subject has its own unique pattern. They are already formed in a 7 months fetus and they are not affected by surface abrasions, burns and cuts, since their original pattern is reproduced as the skin regenerates.

The different arrangement and shape of dermal fibers create several ridges and a precise *papillary* layout, which is used as the subject's identifier. This papillary configuration does not change during the subject's life and, since different for each individual, it can be used for a systematic classification.

The efforts made to automatize the matching process based on digital representation of fingerprints led to the development of *Automatic Fingerprint Identification Systems* (AFIS) [1,2]. In order to establish the identity of an individual, his fingerprint must be compared with millions of fingerprint records contained in a database, which must be entirely searched for a match. To provide a reasonable response-time for each query, nowadays special

* Corresponding author. Tel.: +39 0382 985350; fax: +39 0382 985373.
E-mail address: francesco.leporati@unipv.it (F. Leporati).

0141-9331/$ - see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.micpro.2011.03.003

Fig. 1. A typical fingerprint.

hardware solutions implement matching and/or classification algorithms in a really efficient way.

A fingerprint can be thoroughly described by two kinds of different parameters, *global* and *local*. The former identify a general property of the ridges and furrows weft and is used for classification, while the latter are typically extracted from a restricted portion of a digital representation of the fingerprint and allow its unique identification. As for the first aspect, the pattern shows regions into which the ridges display a greater curvature together with frequent endings; within these regions there are singular points called *core* and *delta* (Fig. 2): the first represents the fingerprint's centre, while the second ones are the points where two ridges diverge. Since these points show a remarkable steadiness and invariance to rotation and scale variation, they are widely employed in the classification algorithms. Following the so-called "Galton–Henry classification scheme", fingerprints are divided into five different classes: *arch, right loop, left loop, tented arch, whorl* (Fig. 3). We refer the reader to [2], for details about the features

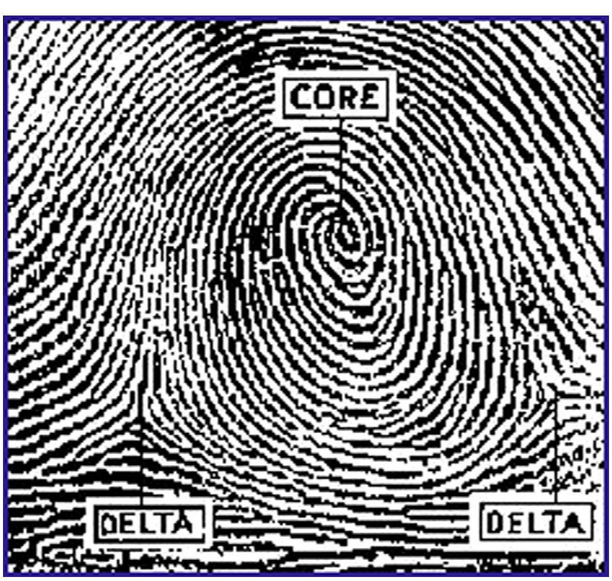

Fig. 2. Singular points.

of these classes. For what concerns local investigation, nearly 150 different fingerprint characteristics have been identified (*minutiae*), corresponding to irregularities in ridges; unfortunately, their identification is highly influenced by the surface conditions. Different types of *minutiae* can be taken into consideration, leading to different classifications: for example, while the ANSI institute proposes a four classes distinction (*ending, bifurcation, crossovers and undetermined*), the FBI considers only endings and bifurcations.

Although several approaches have been conceived to achieve automatic fingerprints classification, they can be grouped into the following categories:

- *Model based*: which ascribes the fingerprint to one of the 5 above-mentioned classes according to the position of the *core* and *delta* points;
- *Structure based*: which makes use of the *orientation field parameter* calculated from the acquired image of the fingerprint itself (even though affected by noise);
- *Frequency based*: which evaluates the spatial spectrum of the acquired image;
- *Syntactical*: which uses a formal grammar to describe and classify fingerprints.

Hybrid models, mixing two or more of these approaches, have also been developed. Some classification methods evaluate the ridge's global orientation and then try to identify singularities in the fingerprint to trace it back to one of the five categories. This approach reproduces the one usually employed by experts when performing a "manual classification" and consists of the following three steps:

- *Estimation of the local ridge orientation*: the normalized image is divided into blocks to which a proper orientation term (*orientation field*) is assigned, by evaluating the gradients of the grey tones in the block.
- *Search of singularities*: a point in the orientation field is classified as ordinary, core or delta, by evaluating the Poincaré index along a little closed curve around the point itself: the index is the sum of the orientations met by going along the curve counterclockwise.
- *Classification of the fingerprint*: a proper set of rules is established.

3. State of the art

Fingerprint matching allows to understand whether two fingerprints belong to the same finger and has been studied since the 19th century. Such a long history favoured the development of many different computational techniques.

The traditional approach, directly linked to human experts matching techniques, involves the comparison between two sets of *minutiae*, which are generally characterized by position, orientation and type.

Minutiae are not the only characteristic points in the image space: for example, the *singularities* are of great interest, but they are generally very few for each fingerprint and are more commonly used for classification (database partitioning) than for direct matching.

Another major family of matching algorithms is correlation-based: the idea is to compare the fingerprints in the (spatial) frequency domain. Different algorithms (see for example [3–6]) use different transformations and/or correlation functions, but they all exploit the many accurate results of efficient correlation computation (see [7,8]) available in literature.

Despite the very different nature of the various algorithms, it is generally possible to identify two distinct phases: