Information Sciences 301 (2015) 195–214

Contents lists available at ScienceDirect

Information Sciences

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

Fast fingerprint identification using GPUs

Miguel Lastra [a,*], Jesús Carabaño [b,c], Pablo D. Gutiérrez [c], José M. Benítez [c], F. Herrera [c]

[a] Depto. Lenguajes y Sistemas Informáticos, E.T.S. Ingeniería Informática y Telecomunicación, CITIC-UGR, Universidad de Granada, Spain
[b] Department of Information Technologies, Åbo Akademi University, Finland
[c] Depto de Ciencias de la Computación e Inteligencia Artificial, E.T.S. Ingeniería Informática y Telecomunicación, CITIC-UGR, Universidad de Granada, Spain

ARTICLE INFO

Article history:
Received 13 November 2013
Received in revised form 24 November 2014
Accepted 31 December 2014
Available online 9 January 2015

Keywords:
Fingerprint matching
Identification
GPU
CUDA

ABSTRACT

Fingerprints are widely used in a variety of biometric identification systems. The fingerprint matching process is a processing step whose computational requirements limit the size of the fingerprint database that can be dealt with.

Fingerprint matching algorithms based on minutiae are one of the most relevant families of biometric identification techniques. The scalability of these models is determined not only by the number of fingerprints but also the number of minutiae per fingerprint. Therefore, processing millions of fingerprints per second requires being able to process hundreds of millions of minutiae per second.

In this paper we present a new design of the minutiae based fingerprint matching algorithm presented by Jiang et al. specifically created for GPU based massively parallel architectures. The parallel design allows speed-up ratios of up to 15 with one GPU compared to multi-threaded CPU implementations, and up to 54 using several GPUs in parallel and fingerprint processing rates of between 300,000 and 1,500,000 fingerprints per second.

1. Introduction

The fingerprint matching process is the keystone of many biometric identification environments [24]. Different aspects of the fingerprint identification systems such as acquisition [2], classification [32] and matching [5] have been widely studied, but designing systems able to produce reliable real-time results when handling large databases with several million fingerprints is still an open problem.

There is a wide range of biometric features related to fingerprints, such as minutiae and orientation fields [23], and other hand areas that are used in identification systems: finger veins [35], finger knuckles [20], palmprint [7] and many more. Many identification techniques focus on extracted features but others use image based operations [17]. This is of course an immense area of research and only a few samples of recent research work in this field are provided.

Minutiae based fingerprint matching algorithms represent each fingerprint as a set of elements called minutiae which are extracted from the fingerprint ridges. These minutiae are recorded at singular points such as ridge endings, bifurcations and sharp direction changes. Each minutia is represented by its 2D position, direction and its type. The fingerprint matching process for this kind of algorithm consists of deciding whether the minutiae set of the input fingerprint matches the minutiae set of any of the template fingerprints stored in a database. The main challenge in this process is being able to handle the

[*] Corresponding author. Tel.: +34 958246144.
E-mail addresses: mlastral@ugr.es (M. Lastra), jcaraban@abo.fi (J. Carabaño), pdgp@decsai.ugr.es (P.D. Gutiérrez), J.M.Benitez@decsai.ugr.es (J.M. Benítez), herrera@decsai.ugr.es (F. Herrera).

http://dx.doi.org/10.1016/j.ins.2014.12.052
0020-0255/© 2015 Elsevier Inc. All rights reserved.

deformations, rotations and translations which occur as a result of different conditions, or the different capturing devices used when fingerprints are captured while providing very reliable results. Minutiae based algorithms are one of the most widely used techniques in biometric identification systems because of the quality of the results and also because their associated acquisition process is less intrusive than those associated with other biometric features.

This work focuses on creating a highly efficient fingerprint matching technique able to tackle millions of fingerprints in a reasonable time (ideally in tenths of a second). The goal is to overcome the limits, in terms of efficiency and cost, imposed by existing CPU based solutions [29].

The minutia based fingerprint matching technique presented by Jiang et al. [19] is composed of a local structure matching phase, which accounts for rotations and translations, and a global matching phase to reduce the number of false positive results and to increase the accuracy of the algorithm.

The use of parallel architectures has enabled us to process large amounts of data in a reasonable time. Graphics Processing Units (GPUs) provide massive parallelism and are universally used as almost every computer has one. These devices have been applied to several problems with intense floating point calculations such as bioinformatics [31], shallow-water simulation [21] and also fingerprint identification [3,16]. Some approaches have explored the idea of using FPGAs (Field Programmable Gate Arrays) for fingerprint matching tasks [30,18] but without state-of-the-art matching techniques and hardware or focusing on low cost proposals that could be used in embedded systems for small-scale scenarios more suited to verification systems [11,12].

In this work, we propose a massively parallel redesign of the algorithm created by Jiang et al. suited to GPU based architectures. The process for creating the new fingerprint matching system requires dealing with different non trivial tasks such as correctly identifying the sources of parallelism, creating an efficient workload mapping between computational tasks and parallel computing elements to fully utilize the computational power offered by GPUs, avoiding any GPU idling periods by using asynchronous memory transfers and overlapping the processing of different tasks (and memory transfers) and avoiding bottlenecks such as those produced by memory allocations.

The speed-up factor of the many-core approach with respect to traditional multi-core systems is obtained while maintaining the same accuracy of the original algorithm. The rates of over 300,000 fingerprint matching operations per second obtained by our proposal with one GPU and up to 1,500,000 matching operations per second using four GPUs, matching the performance of a cluster with 12 dual processor nodes with 12 physical cores per node, allows the presented system to be used as part of a hybrid model to achieve the right balance of accuracy and efficiency by combining it with other, slower but more accurate techniques such as the MCC fingerprint matching algorithm [5]. These ideas will be discussed in Section 6.6.

The paper is structured as follows: Section 2 describes fingerprints as biometric characteristics and their importance in the identification systems domain, Section 3 describes the original fingerprint matching algorithm on which this work is based, Section 4 presents an introduction to GPU based general purpose programming and its application to the fingerprint identification process, in Section 5 a detailed description of the GPU based algorithm redesign is provided and Section 6 shows the results of the different experiments that have been carried out, together with a comparison with parallel CPU implementations and finally, a hybrid fingerprint matching model is discussed with a view to obtaining a balance between performance and accuracy. The conclusions are presented in Section 7.

2. Fingerprint based biometrics

Biometric systems are designed to perform the recognition of people. The need to verify that a person corresponds to the individual it is claiming to be (verification) or to determine which person is trying to access a certain piece of information, restricted area or device is an issue that has been tackled for over a century. The idea of identifying criminals by the fingerprints collected from crime scenes started in the 19th century although evidences exist that some cultures used fingerprints many centuries B.C. As an example a Chinese clay seal dated 300 B.C was found with a finger imprint and it is believed that in the Chinese culture they were to some degree aware of the uniqueness of fingerprints 5000 years ago [22,24].

In the modern era fingerprints started being studied scientifically in the 17th century [4,15] and its uniqueness was established in the 18th century [25]. The identification of criminals in the forensics field using fingerprints was the main use of this biometric feature and this includes the use of fingerprints as part of criminal record databases.

Some of the reasons fingerprints are the most used biometric trait:

- They are assumed to be unique.
- They were introduced as identification method many centuries ago.
- They are inalterable unless they get scarred or affected by a burn.
- Fingerprints can be acquired using non intrusive methods.
- They could be captured and compared without the need of electronic devices. Ink impressions and manual comparison were the techniques used in the pre-electronic era.
- A vast amount of research has been done to create efficient systems for capturing and comparing fingerprints automatically.