International Journal of Electronics, Communication & Soft Computing Science and Engineering
ISSN: 2277-9477, Volume 3, Issue 7

Increase in Performance for Fingerprint Matching System on GPU – A Review

Ms. Shital T. Tupe Prof. Amol D. Potgantwar

Abstract: - **Fingerprints are the biometric features usually used for identification. These can be characterized through some particular elements which are called as minutiae. The identification of a given fingerprint requires the matching of its minutiae against the minutiae of other fingerprints. Biometric is an authentication and verification technique that relies on measurable physical characteristics. The biometrics is suitable for network access and it is a technology that meets the needs for network security. To prevent identity theft, biometric data is usually encrypted when it's gathered. Working of Biometric i.e. is on the back end in following manner which convert the biometric input. Software application identifies specific points of data as match points. An algorithm matches points in the database that translates that information into a numeric value. Finally the value in database is compared with the biometric input entered by the end user then authentication is either approved or denied. The minutia cylinder-code (MCC) is the best performing algorithm in terms of accuracy. A rigorous empirical inference fingerprint databases shows the efficiency by taking advantage of the GPUs.**

Keywords- **MCC, GPU, Fingerprints, Biometric, Large Database.**

I. INTRODUCTION

Security in the system is most required aspect in today's era. For providing security to the systems various ways are being adopted, one of these is Biometric Identification. Physical or psychological trait is used for identification and for authentication in Biometric technology. Biometrics always refers to metrics relating to human characteristics and traits. In Computer science both biometrics authentication and realistic authentication is used as a form of identification and access control. Identifying individuals in groups is also done. There are various types of Biometric authentication by considering the Unique Features of Human Body.

Fingerprints are the most widely used biometric features in identification tasks thanks to the usability and reliability of systems based on them. Many applications use fingerprints for example in forensic identifications, ID cards, access control, etc. Even fingerprints are also one of the most studied biometric features. Proposals addressing their acquisition, processing, classification and matching can be found over the last years [1].

There are two different kinds of issues in this field: verification and identification. Verification systems try to determine if two fingerprints were produced by the same finger with the highest possible reliability. On the other hand, identification systems try to find which fingerprint in a database matches the input fingerprint. Since the identification complexity is much higher than verification, an identification system accepts an accuracy loss for achieving a faster matching process.

Graphics Processing Units (GPUs) have proven to be a very useful tool in the acceleration of computationally intensive algorithms. Massive parallelism is introduced in the calculations reducing run times of magnitude. Molecular modeling [3] is the application as compared with different fields.

II. LITERATURE REVIEW

Most fingerprint matching algorithms are based on minutiae (i.e., ridge ending and bifurcations). In the last decade, these weaknesses were addressed by introducing local minutiae matching techniques. Attributes of local minutiae structures are characterized that are invariant with respect to global transformations (e.g., translation, rotation, etc.). Matching fingerprints based only on local minutiae [2].

In 1996 [4], Nalini Ratha and her fellows proposed a Real Time Matching System for large Fingerprint Database. They elraged their Fingerprint Database for the purpose of good quality images storage and retrival but evaluation of image quality at the input stage to accept or reject an input is being considered. In 2000 [5], Anil K. Jain introduced filter-based algorithm uses a bank of Gabor filters. The fingerprint matching is based on the Euclidean distance between the two corresponding Finger Codes and hence is extremely fast. We achieved a verification accuracy which is only marginally inferior to the best results of minutiae-based algorithms published in the open literature.

In 2001 [6], Salil Prabhakar & Anil K. Jain proposed Filter Bank Based Algorithm for classifier combination at decision level which stresses the importance of classifier selection during combination. The proposed scheme was optimal (in the Neyman–Pearson sense) when sufficient data are available to obtain reasonable estimates of the join densities of classifier outputs. Experiments conducted on a large fingerprint database (2700 fingerprints) confirm the effectiveness. Matching performance increases by 3%. A combination of multiple impressions or multiple fingers improves the verification performance.

In 2009 [8], HaiyunXu, Raymond N. J. Veldhuis, Asker M. Bazen, Tom A. M. Kevenaar, Ton A. H. M. Akkermans, and BerkGokberk [sept 09] introduces a new approach of authentication i.e. spectral minutiae. These characteristics enable the combination of fingerprint recognition systems with template protection schemes. During Implementation on they faced some problems.

In December 2010 [2], Raffaele Cappelli, Matteo Ferrara, and Davide Maltoni proposed introduced the Minutia Cylinder-Code (MCC): a novel minutiae-only representation and matching technique for fingerprint recognition. MCC depends on a robust discretization of the neighborhood of every minutia into a 3D cell-based structure named cylinder. Simple but efficient techniques for the estimation and consolidation of cylinder similarities are provided to search the global similarity among two fingerprints. In order to compare MCC with three well-known approaches, a systematic experimentation has been carried out, involving a total of 24 matching approaches (six algorithms and four global-scoring techniques) over 20 minutiae data sets extracted from FVC2006 databases, resulting in more than nine million matching attempts. Their Experimental results demonstrated that MCC is more accurate than well known minutiae-only local matching techniques. MCC is also very speedy and appropriate to be simply coded in hardware due to the bit-wise characteristics of the matching technique. This allows it's porting on inexpensive secure platforms such as a smart-card or a system-on-a-chip. They mainly focused on the problem of robustly and efficiently matching two fingerprints, that the peculiarities of MCC also allow the development of new effective techniques for fingerprint indexing and template protection: These two issues were the main targets of future research efforts.

In January 2014 [1], Pablo David Gutierrez, Miguel Lastra, Francisco Herrera, and José Manuel Benítez proposed presented an efficient GPU based fingerprint method using the MCC algorithm. Their proposal was implies an effective design of the parallel algorithm with the inclusion of smart techniques to overlap memory transfers with computation as well as packaging sets of independent identifications. While implementing the concept they obtained speed-up ratios up to 100.8× with respect to a single-thread CPU implementation. They also showed that our system has no scaling issues when the fingerprint database size increases and that the speed-up ratios are highly independent of the fingerprint type and the mean number of minutiae per fingerprint.

III. Identification And Matching Of Fingerprint

There are various algorithms for fingerprint authentication as, Minutiae Direction Map- MDM, Minutiae extraction algorithm, Feature extraction algorithm, Fingerprint binarization algorithm, Fingerprint pattern recognition and matching algorithms. But all these algorithms cannot provide the efficient output of the identification in small time. Minutia cylinder-code (MCC) takes about 45 milliseconds to perform a single comparison between two fingerprints matching. It would take 45 seconds to identify a fingerprint in a database of 1000 individuals. Extrapolating this result it would take 45 minutes to identify a fingerprint in a database of 60000 individuals. Thus implementation of MCC is fruitful for Biometric Authentication in GPU for parallel computing which can reduce the execution time up to high extend [1], [3].

A. Minutiae Matching

A minutia is a change on the ridges of the fingerprint,
usually ridge endings and bifurcations. A minutia is defined by its position, angle and type although other representations like a spectral representation have also been proposed [12]. Minutiae-based algorithms are the most used mainly due to their reliability and the amount of data involved. There are two types of minutiae based matching algorithms: global and local, but most of the algorithms use a combination of both models. Local algorithms define a neighbourhood and try to match minutiae from two fingerprints with similar neighbours,
while global algorithms use the information of all the minutiae at once. Algorithms that focus on local matching processes can be divided into two categories depending on how they define the neighbourhood of the minutiae:

1) Nearest neighbour: The neighbourhood of a given minutia is defined by the *K* closest minutiae.
2) Fixed radius: The neighbourhood of a given minutia is defined by the minutiae inside an imaginary circle of radius R cantered at the minutia.

B. Graphics Processing Unit

Recently, graphics processing units (GPUs) have emerged as a parallel computing resource offering hundreds or thousands of processing cores and providing large-scale parallelism on computing platforms. The characteristics of GPUs and GPU programming are exposed. It provides a background about these devices and their programming model. Explains the high and low level structures used by GPUs to introduce parallelism.

C. Data Structures

Data structures are one of the key issues when designing GPU based programs because data organization has a big impact on the resulting performance. Coalesced memory accesses is one of the factors which reduces memory access times by allowing several memory operations issued by different cores or GPU threads to be combined into one access. The use of coalesced memory accesses does also have an impact on the design of the computational structure of the GPU program but suitable data structures are the basis to achieve this goal. As stated the MCC algorithm requires the storage of data related to every minutia (position (x, y), orientation θ and validity v) and the cylinder cells associated to each minutia (each cell stores one floating point value). For each fingerprint, minutiae data is stored as float 4 elements. Float4 data types are native in GPU programs and represent floating point 4-tuples that offer the optimum memory alignment. This representation allows retrieving all the information of a minutia with a single memory access. It also reduces the amount of memory transfer operations between the host and the GPU and increases the throughput achieved. Cell data is also packed in 4-tuples and stored in a lineal array. A fingerprint database is therefore constructed using two lineal arrays. The first one contains the minutiae data of each fingerprint and the second one the values of the cells associated to each minutia, in the same order as they are stored in the first array.

D. Computation

The computational model offered by CUDA requires the distribution of the input fingerprint data structures computation and the subsequent matching process into a set of threads. These threads have to be grouped into blocks that share a Fig. 3. Computation mapping $Ns = 8$. Small common memory area and that are run on the same GPU multiprocessor. The mapping chosen for each computation step will be detailed in the following sections.

1) Cylinder Generation: The fingerprint to be compared to the fingerprint database has to be represented in terms of cylinders representing minutiae and cylinder cells. The number of cells per cylinder ($Ns \times Ns \times Nd$) is one of the MCC algorithm parameters. For this work the two configurations proposed in [5] have been chosen: $(Ns = 8, Nd = 6)$ and $(Ns = 16, Nd = 6)$. For the first configuration, the total number of cells per cylinder is below the maximum number of threads per block (which is limited by the device to 1024 since the Fermi GPU generation) and allows the computation of one cylinder per thread block. All the computations associated to a cell are assigned to one thread. The main advantage of mapping the computations related to one cylinder to the same thread block is that the process of determining the validity of a cylinder, which is a reduction process, will be run on the same multiprocessor and can be fully implemented using the block shared memory. The reduction process computes the count of the valid cells of the cylinder. When the number of cells per cylinder is increased by setting $Ns = 16$, keeping the *cell computation*-thread mapping requires the process to be split over several blocks. In our system, cell layers were assigned to thread blocks. As each cylinder has Nd layers, the same number of thread blocks is created. Dividing this process into several blocks requires and additional reduction step to compute the validity of a cylinder in terms of the partial validity values computed for each layer.

2) Fingerprint Matching: The fingerprint matching process requires comparing an input fingerprint to a set of fingerprints stored in a database. This process can be split into a set of one to one matching processes. Each of these comparisons or matching processes has been adapted to the parallel GPU architecture.

CONCLUSION

Biometric is an authentication and verification technique that relies on measurable physical characteristics. It focuses on measuring and analyzing biological data. The biometrics technology meets the needs for network security. The minutia cylinder-code (MCC) is the best performing algorithm in terms of accuracy. A rigorous empirical inference fingerprint databases shows the efficiency by taking advantage of the GPUs. System is able to perform identification in a reasonable amount of time for large databases, processing up to 55700 fingerprints per second with a single GPU, maintaining the accuracy of the CPU implementation and making the MCC algorithm usable in real-world situations. With MCC, it is possible to have strong authentication and still keep the logistics manageable.

REFERENCES

[1] Ion TUTANESCU, Constantine ANTON, University of Pitesti, ROMANIA, *Elliptic Curve Cryptosysytem Approches*, IEEE, 2012.

[2] Pablo David Gutiérrez, Miguel Lastra, Francisco Herrera, and José Manuel Benítez*, A High Performance Fingerprint Matching System for Large Databases Based on GPU*, IEEE, 2014.
[3] Raffaele Cappelli, Matteo Ferrara, and Davide Maltoni, *Minutia Cylinder-Code: A New Representation and Matching Technique for Fingerprint Recognition,* IEEE, 2010.
[4] Nalini Ratha, *Real Time Matching System for large Fingerprint Database*, IEEE, 1996.
[5] Anil K. Jain, *Filterbank-Based Fingerprint Matching*, IEEE, 2000.
[6] Salil Prabhakar, Anil K. Jain, *Decision-level fusion in fingerprint verification*, Elsevier, 2001.
[7] Heeseung Choi, Kyoungtaek Choi, and Jaihie Kim, *Mosaicing Touchless and Mirror-Reflected Fingerprint Images,* IEEE, 2010.
[8] Haiyun Xu, Raymond N. J. Veldhuis, Asker M. Bazen, Tom A. M. Kevenaar, Ton A. H. M. Akkermans, and Berk Gokberk, *Fingerprint Verification Using Spectral Minutiae Representations*, IEEE, 2009.
[9] H. Choi, K. Choi, and J. Kim, "Mosaicing touchless and mirror-reflected fingerprint images," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 52–61, Mar. 2010.
[10] F. Turroni, D. Maltoni, R. Cappelli, and D. Maio, "Improving fingerprint orientation extraction," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 1002–1013, Sep. 2011.
[11] K. C. Leung and C. H. Leung, "Improvement of fingerprint retrieval by a statistical classifier," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 59–69, Mar. 2011.
[12] R. Cappelli, M. Ferrara, and D. Maltoni, "Minutia cylinder-code: A new representation and matching technique for fingerprint recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 32, no. 12, pp. 2128–2141, Dec. 2010.
[13] M. Friedrichs, P. Eastman, V. Vaidyanathan, M. Houston, S. Legrand, A. Beberg, *et al.*, "Accelerating molecular dynamic simulation on graphics processing units," *J. Comput. Chem.*, vol. 30, no. 6, pp. 864–872, 2009.
[14] M. Schatz, C. Trapnell, A. Delcher, and A. Varshney, "High-throughput sequence alignment using graphics processing units," *BMC Bioinformat.*, vol. 8, p. 474, Dec. 2007.
[15] M. Lastra, J. M. Mantas, C. Ureña, M. J. Castro, and J. A. García-Rodríguez, "Simulation of shallow-water systems using graphics processing units," *Math. Comput. Simul.*, vol. 80, no. 3, pp. 598–618, Nov. 2009.
[16] C. Watson and C. Wilson, "Nist special database 4," National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep., 1992.
[17] C. Watson, "Nist special database 14," National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep., 1993.
[18] R. Cappelli, D. Maio, and D. Maltoni, "Synthetic fingerprint-database generation," in *Proc. 16th Int. Conf. Pattern Recognit.*, vol. 3. 2002, pp. 744–747.
[19] H. Xu, R. Veldhuis, A. Bazen, T. Kevenaar, T. Akkermans, and B. Gokberk, "Fingerprint verification using spectral minutiae representations," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 3, pp. 397–409, Sep. 2009.
[20] F. P. Preparata and M. I. Shamos, *Computational Geometry: An Introduction*. New York, NY, USA: Springer-Verlag, 1985.
[21] (2013, Jun. 28). NVIDIA Corporation, Santa Clara, CA, USA [Online]. Available: http://www.nvidia.com/