

Embedded Fingerprint Verification System

Mikroelektronik / Prof. Dr. Marcel Jacomet

In a world where everything is connected, the need of security is larger than anytime before, and the demand for a fast and secure an approach to prove an identity, is growing steadily. Biometric recognition is a way to solve the question of security. There are several biometric recognition possibilities that fulfill the above requirements. These are iris, fingerprint, face, and hand identification, to mention just some of them. Fingerprint scanning is guarded with less skepticism by people than iris scans.



Brönnimann Michael
1981

078 760 09 79

broenni@gmx.ch



Eicher Andreas
1980

031 371 64 13

andreas.eicher@gmx.ch

Objectives

The objective of this diploma thesis is to design a fast minutiae detection algorithm for low power embedded systems, with an acceptable quality for high security applications. As a reference, we used the Latent Fingerprint System (LFS) from the National Institute of Standards and Technologies (NIST), also used by the FBI agency. This tool is basically splitted into six tasks, which have well defined interfaces. This allows us to replace any single task by our own speed optimized version.

Reference System

In addition to the fast minutiae detection algorithm, we designed a test bench to measure the fingerprint recognition quality. The two values, false acceptance rate (FAR) and false rejection rate (FRR) should be as low as possible for a high quality fingerprint recognition system. To get the FRR rate, fingerprints of the same finger are necessary, to get the FAR rate, those of different fingers are required; Standard databases are available to do these quality measurements. The rejection rates of the optimized LFS algorithm should be in the same region as the original algorithm.

Speed Optimized Fingerprint Algorithm

A human fingerprint is composed of ridges and valleys. Every persons fingerprint is unique. Different fingerprints can be distinguished by its

features, which are called minutiae. The minutia types, its directions, and positions differentiate human beings from each other. In a first step, the minutiae detection algorithm computes a direction map of the fingerprint ridges and valleys. This is realized with a discrete Fourier transformation in the LFS algorithm, which needs a very high processing power. We managed to drastically reduce the necessary processing power and execution time by implementing a different approach. The second most time consuming part is the conversion of the 8-bit gray scale fingerprint image to a 1-bit black and white image. This is done by a direction dependent filter. As we did not find any alternative filter methods, we concentrated in speeding up the LFS algorithm. A speedup factor of 5 was achieved with a negligible loss of quality. In a third step we managed to compress the fingerprint memory size by a factor of 32, adapting the data structure to the processors architecture. With this new structure, the succeeding fingerprint image processing steps, like filling so called sweat holes and minutiae detection, could also be sped up considerably. The overall speedup manifests itself as an execution time reduction from the original 5.5 sec to 0.3 sec for the main fingerprint image processing steps. Due to lack of time, the final processing steps, removing false minutiae, ridge counting, and the matching algorithm, have to be implemented in a following project.



Original fingerprint image



Direction map of fingerprint ridges and valleys



Binarized fingerprint image



Fingerprint image with feature extraction (minutiae)