BASTA: Biometric Authentication System for Trusted Access

Internet and Multimedia Laboratory

Alessandro Casagrande – ID 2066716

07/02/2024

Introduction

In this report, a biometric authentication system is presented. The project proposes some critical components for the development of enhanced authentication for biometric systems using commutative watermarking and encryption. In particular, the biometric information used is the fingerprint.
The environment selected for this project is Matlab.

Image cleaning and enhancement

The first thing done. Processing the image is a crucial step for the authentication that allows to more easily extract relevant information from the fingerprint (i.e., minutiae).
Given a fingerprint image, to clean it and enhance fine details, the following steps have been performed, in order: some preprocessing (as indicated in [1]), a combination of a high-pass Laplacian filter – to highlight high-frequency components, e.g. fine details – and a Gaussian low-pass filter – to attenuate the noise – in the Fourier transform domain, a weighted summation of the edges extracted using Canny, to again emphasize the contours.
Using as an example `fingerprint3.jpg` as the input fingerprint image (taken from the dataset in [1]), the computation of the evaluation metrics provides these results for PSNR and SSIM:

$$PSNR = 51.0889 \qquad SSIM = 0.95127$$

suggesting that what has been done gives a good result.

TCP/IP Client-Server connection

Let the client be the device trying to authenticate, and the server the device that checks the user identity trying to connect. Information exchange between the client and the server has been set up using `tcpserver` and `tcpclient`. This connection will be used by both entities to implement the security part, as well as the actual exchange of biometric data, making the whole process a proper protocol.

Diffie-Hellman key exchange

To make encryption possible, a key is needed. A symmetric key has been chosen, that can be secretly exchanged between client and server using the Diffie-Hellman procedure, implementing what is outlined in [2]. To increase security, the key is 256 bit long, implemented in Matlab as a Variable Precision Integer, using [3].

Encryption and Watermarking

The path followed takes its cue from what is presented in [4], that is, a commutative encryption and watermark technique: the image is first sliced into 8 binary bit planes, then the first 7 most significant bit planes are encrypted, using a random shuffle algorithm based on the previous exchanged key, and the least significant bit plane is replaced with a binary watermark. In this way, it is possible to encrypt and apply a watermark to the image separately and simultaneously, allowing ownership to be verified without decrypting and, vice versa, decrypting without altering the watermark.

Transmission over TPC/IP

The resulting image is now ready to be securely transmitted to the server using the same TCP/IP connection as before. With the biometric image safely encrypted and watermarked, a possible intruder cannot understand what is being transmitted, and the security of the user's identity is guaranteed.

Decryption and identity check

On the server it is required to decrypt the image, using the same algorithm as before and the same symmetric key, in reverse. Now the image is ready to be processed by the server that needs to extract the relevant information about the fingerprint and check the correctness of the identity of whoever is trying to connect.

Future improvements

Since extracting minutiae, comparing them, and notifying the client of the authentication result have not been implemented, these features are part of future developments.
Moreover, in addition to the fingerprint, is it possible to also use facial recognition, iris recognition, voice recognition, etc. as biometric data.
Finally, to improve security, attacks carried out by an external party (brute force, man-in-the-middle, replay, etc.) can be simulated to detect and fix security vulnerabilities.

References

[1] Reyof-AlQurashi. *Image Processing Project — GitHub*. 2024. URL: https://github.com/Reyof-AlQurashi/Image_Processing_Project. [Online, last checked: 07.02.2025].

[2] Wikipedia contributors. *Diffie–Hellman key exchange — Wikipedia, The Free Encyclopedia*. 2025. URL: https://en.wikipedia.org/w/index.php?title=Diffie%E2%80%93Hellman_key_exchange&oldid=1271677942. [Online; last checked 07.02.2025].

[3] John D'Errico. *Variable Precision Integer Arithmetic — Matlab Central File Exchange*. 2025. URL: https://www.mathworks.com/matlabcentral/fileexchange/22725-variable-precision-integer-arithmetic?status=SUCCESS. [Online, last checked: 07.02.2025].

[4] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F.G.B. De Natale, and A. Neri. "A commutative digital image watermarking and encryption method in the tree structured Haar transform domain". In: *Signal Processing: Image Communication* 26.1 (2011), pp. 1–2, 5–6. DOI: https://dx.doi.org/10.1016/j.image.2010.11.001.