Semi-Fragile Watermarking in Biometric Systems: Template Self-Embedding

Reinhard Huber[1], Herbert Stögner[1], and **Andreas Uhl**[1,2]

[1]School of Communication Engineering for IT, Carinthia Tech Institute, Austria
[2]Department of Computer Sciences, University of Salzburg, Austria
Contact author e-mail: uhl@cosy.sbg.ac.at

Motivation

There has been a lot of work done during the last years proposing watermarking (WM) techniques to enhance biometric systems security in some way. Here, the aim of WM is to ensure the integrity and authenticity of the sample data acquisition and transmission process. During data acquisition, the sensor (i.e. camera) embeds a watermark into the acquired sample image before transmitting it to the feature extraction module. The feature extraction module only proceeds with its tasks if the WM can be extracted correctly (which means that (a) the data has not been tampered with and (b) the origin of the data is the correct sensor).

We focus on semi-fragile WM which has to offer a certain amount of robustness. We propose to embed biometric template data instead of general purpose watermark information which can then be used as redundant template material in the matching process in addition to facilitiating the integrity check. This approach is sensible since

- template data are of course image dependent data and therefore are able to prevent WM copy attacks or similar;
- in case of tampering the aim in biometrics is not to reconstruct the sample data but to be able to generate template data – this can be directly facilitated with the embedded template data.

Semi-Fragile Watermarking by Template Self Embedding

1. From the acquired sample data, a template is extracted.
2. The template is embedded into the sample data employing a semi-fragile embedding technique (this template is referred to as "template watermark" subsequently).
3. The data is sent to the feature extraction and matching module.
4. At the feature extraction module, the template watermark template is extracted, and is compared to the template extracted from the sample (denoted simply as "template" in the following). In this way, the integrity of the transmitted sample data is ensured when there is sufficient correspondence between the two templates. In case of a biometric system operating in verification mode the template watermark can also be compared to the template in the database corresponding to the claimed identity (denoted "database template" in the following).
5. Finally, in case the integrity of the data has been proven, the watermark template and the template are used in the matching process in a fused manner, granting access if the similarity to the database template(s) is high enough.

Questions

- What is the impact of the embedded template watermark on the recognition performance using the template for matching only ?
- Can a combination of template watermark and template result in more robustness in an actual matching process ?
- Does integrity verification indeed work in a robust manner ?

Experimental Settings

- **Datasets:** CASIAv3 Interval (320×280 pixels, 500 images used), MMU (320×240 pixels, 450 images used), and UBIRIS (200×150 pixels, 318 images used).
- **Iris Recognition:** A 1-D version of the Daugman iris recognition algorithm as implemented by Libor Masek in Matlab (the phase of Gabor responses is encoded into a binary iris code).
- **Watermarking:** The fragile spatial domain embedding scheme by Yeung and Mintzer is used, iris codes are embedded redundantly to result in a certain amount of robustness (we can embed 9, 8, and 3 templates into images from the CASIAv3, MMU, and UBIRIS databases, respectively) when using majority decoding in WM detection.

Experimental Results

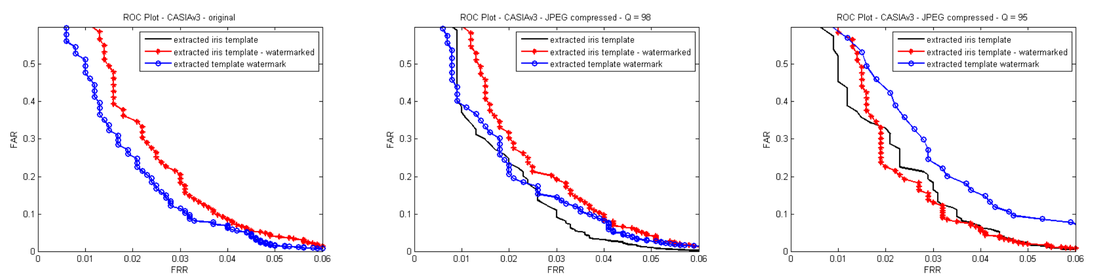

Fig. 1 EER results of CASIA V3: Uncompressed, JPEG98%, and JPEG95% .

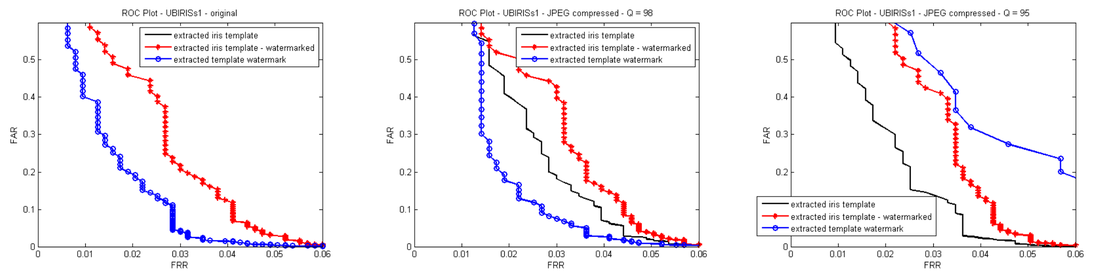

Fig. 2 EER results of UBIRIS: Uncompressed, JPEG98%, and JPEG95%.

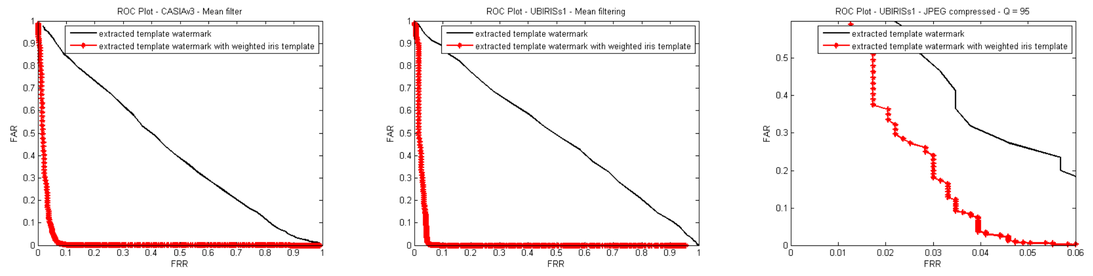

Fig. 3 EER results of fused templates: CASIA V3 (mean filter), UBIRIS (mean filter), and UBIRIS (JPEG95%).

Observations and Conclusions

⟶ for less severe distortions, the watermark template exhibits higher robustness while for severe distortions, the template extracted from the sample is more robust for matching (see Figs. 1 & 2).

⟶ the fused template (template plus template WM) offers improved robustness in case of more severe distortions (see Fig. 3).

⟶ there is impact of the embedded WM on recognition performance, but this is more then compensated by the higher robustness of the fused template scheme (see Figs. 1 & 2).