Two-Factor Biometric Recognition with Integrated Tamper-Protection Watermarking

Reinhard Huber, Herbert Stögner, Andreas Uhl

▶ **To cite this version:**

Reinhard Huber, Herbert Stögner, Andreas Uhl. Two-Factor Biometric Recognition with Integrated Tamper-Protection Watermarking. 12th Communications and Multimedia Security (CMS), Oct 2011, Ghent, Belgium. pp.72-84, 10.1007/978-3-642-24712-5_6 . hal-01596199

HAL Id: hal-01596199

https://inria.hal.science/hal-01596199v1

Submitted on 27 Sep 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Two-Factor Biometric Recognition with Integrated Tamper-protection Watermarking *

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

[1] School of CEIT, Carinthia University of Applied Sciences, Austria
[2] Department of Computer Sciences, University of Salzburg, Austria

Contact author e-mail: uhl@cosy.sbg.ac.at

Abstract. Two-factor authentication with biometrics and smart-cards enabled by semi-fragile watermarking is proposed. Several advantages of the scheme as compared to earlier approaches are discussed and experiments for an iris-based recognition system demonstrate that semi-fragile integrity verification can be provided by the system. This is achieved without impact on recognition performance, since the slight degradation in terms of ROC behavior which is observed on the watermarked sample data is more than compensated by the additionally available template that is transferred from the smart-card to the matching site via watermarking technology.

1 Introduction

Biometric recognition applications become more and more popular. Biometric authentication systems can resolve most of security issues of traditional token-based or knowledge-based authentication systems, since a biometric feature belongs only to one person and cannot be lost or forgotten. But eventually, biometric features can be stolen or adopted and there exist various other ways to circumvent the integrity of a biometric authentication system (see e.g. a corresponding collection of security issues compiled by the UK Government Biometrics Working Group[3]). Recent work systematically identifies security threats against biometric systems and possible countermeasures [15, 16] and e.g. discusses man-in-the-middle attacks and BioPhishing against a web-based biometric authentication system [21].

Among other suggestions to cope with security threats like applying liveness detection or classical cryptographic encryption and authentication techniques, watermarking has been suggested to solve security issues in biometric systems in various ways [5]. Dong et al. [2] try to give a systematic view of how to integrate watermarking into biometric systems in the case of iris recognition by distinguishing whether biometric template data are embedded into some host

* This work has been partially supported by the Austrian Science Fund, project no. L554-N15.

[3] http://www.cesg.gov.uk/policy_technologies/biometrics/media/biometricsecurityconcerns.pdf

data ("template embedding"), or biometric sample data is watermarked by embedding some data into them ("sample watermarking").

One of the application scenarios described in literature involving watermarks actually represents a two-factor authentication scheme [8]: biometric data is stored on a smart-card and the actual biometric data acquired at the sensor is used to verify if the user at the sensor is the legitimate owner of the smart-card. Watermarking is used to embed data of a second modality into the data which is stored on the card (in the reference given, facial data is embedded into fingerprint images and at the access control site, a fingerprint sensor is installed). Therefore, watermarking is employed as a simple means of transportation data of two different modalities in an integrated manner. Obviously, this application scenario represents as well a case of enabling the application of multibiometric techniques by using watermarking techniques, where biometric template data is embedded into biometric sample data (of different modalities) to enable multibiometric fusion. Traditionally, in these schemes two different sensors are used to acquire the data and again, watermarking is used as a transportation tool only.

For an overwhelming majority of watermarking-based techniques for these two scenarios (i.e. two-factor authentication with smart-cards and multibiometrics), **robust** watermarks have been suggested. However, the motivations for applying this specific type of watermarks are not made clear and discussed superficially only, if at all, in most papers. The usage of robust embedding schemes seems to indicate that both data need to be tightly coupled and that the entire transmitted data might be subject to various manipulations, since robust embedding is meant to make the embedded data robust against changes of the host data. Therefore it seems that an insecure channel between sensor and processing module is assumed in this context. In such an environment host data manipulations are to be expected, including even malicious tampering like cropping. In recent work [4] it has been shown that most robust watermarks cannot prevent even a massive tampering attack (i.e. exchanging the entire iris texture) in the context of an iris recognition system with embedded template data. This comes as no surprise since these watermarks are actually designed to be robust against this type of attacks. Obviously, robust watermarking is not the best suited watermarking technology for the purpose it is suggested for in this context.

While this specific attack discussed is targeted against the security of robust embedding (and can be resolved by using different types of watermarks as shown in this work), robust watermarking additionally introduces distortions into the sample data impacting on recognition performance [3]. Also for this problem, different types of watermarks may represent better solutions as also covered here.

In this paper, we introduce the application of semi-fragile watermarking in the context of a two-factor authentication scheme using iris recognition and smart-cards. Contrasting to most multibiometric approaches, we do not embed template data from a different modality, but the modality of sample data and template data do match. We demonstrate that in addition to enable tightly cou-

pled transport, semi-fragile watermarking can also provide sensitivity against tampering and almost negligible impact on recognition performance. An additional advantage of the proposed scheme is the improved recognition accuracy due to the use of two templates in the matching process and increased security due to the two factor approach in general.

Section 2 provides an overview of several techniques how to incorporate watermarking techniques into biometric systems. Emphasis is given to the discussion of several examples of two-factor authentication and multibiometric techniques, which are enabled by embedding template data into sample data using watermarking.

In Section 3, we explain and discuss the proposed scheme and present experimental results in Section 4. Section 5 concludes the paper.

2 Watermarking in Biometric Systems

A recent overview on the topic and an extensive literature review is given in [5]. One of the first ideas to somehow combine biometric technologies and watermarking is "biometric watermarking" [18]. The aim of watermarking in this approach is not to improve any biometric system, but to employ biometric templates as "message" to be embedded in classical robust watermarking applications like copyright protection in order to enable biometric recognition after the extraction of the watermark (WM).

A second application case for robust WMs is to prevent the use of sniffed sample data to fool the sensor in order to complement or replace liveness detection techniques. During data acquisition, the sensor (i.e. camera) embeds a WM into the acquired sample image before transmitting it to the feature extraction module. In case an intruder interferes the communication channel, sniffs the image data and presents the fake biometric trait (i.e. the image) to the sensor, it can detect the WM, will deduce non-liveness and will refuse to process the data further (see e.g. [1] embedding voice templates into iris sample data).

A steganographic approach is to transmit biometric data (i.e. template data) hidden into some arbitrary carrier / host data or biometric samples of different biometric modalities. The idea is to conceal the fact that biometric data transfer takes place, e.g. Jain et al. [6] propose to embed fingerprint minutiae data into an arbitrary host image while Khan et al. [9] suggest to embed fingerprint templates into audio signals.

Questions of sensor and sample authentication using watermarks have also been discussed. 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. For example, fragile watermarking has been suggested to serve that purpose either embedding image-independent [20] or image-dependent data as WM [19].

A significant amount of work has also been published in the area of using WMs to enable a multibiometric approach by embedding a biometric template

into a biometric sample of different biometric modalities. There are two variants: First, there are two different sensors acquiring two biometrics traits. Since for one modality template data is embedded, these data need to be generated at the sensor site which makes this approach somewhat unrealistic, at least for low power sensor devices. In addition to that, besides the increased recognition performance of multimodal systems in general there is no further specific gain in security (see for example: Jain et al. [7] embed face data into fingerprint images as well as do Chung et al. [11] and Noore et al. [12]; Park et al. [13] suggest to use robust embedding of iris templates into face image data, etc.).

The second variant is to store the template on a smart-card which has to be submitted by the holder at the access control site. The smart-card embeds the template into the host sample data. This in fact represents a two-factor authentication system which increases security by introducing an additional token-based scheme and also leads to higher recognition accuracy as compared to a single biometric modality.

With respect to general two-factor authentication schemes, [17] propose to embed additional classical authentication data with robust watermarking into sample data, where the embedded signature is used as an additional security token like a password. Jain and Uludag [8] propose to embed face template data in fingerprint images stored on a smart-card (called scenario 2 in the paper while scenario 1 is a steganographic one). Instead of embedding an additional security token also biometric template data from a second sensor can be embedded – in [14] an encrypted palmprint template is embedded into a fingerprint image, where the key is derived from palmprint classes. Since these additional data are not used in multibiometric fusion but serve as independent second token coming from a second sensor, this approach can be interpreted as being both, a multibiometric recognition scheme or a two factor authentication scheme.

The impact of watermarking on the recognition performance of biometric systems has been investigated most thoroughly in the context of iris recognition. While Dong et al. [2] do not report on performance degradations when investigating a single watermark embedding algorithm and one iris recognition technique only, Hämmerle et al. [3] find partially significant reductions in recognition accuracy (especially in case of high capacity) when assessing two iris recognition schemes and a couple of robust watermarking algorithms. Similar to the latter results, recognition impact has been observed as well for speech recognition [10] and fingerprint recognition [14].

3 Two-Factor Biometric Recognition: Semi-fragile Template Embedding

We focus on a two-factor authentication scheme based on biometrics and a token, i.e. a smart-card. When a user is enrolled into the system, sample data are acquired, corresponding template data is extracted and stored in two different ways: first, in the centralized biometric database required for the actual recognition process, and second, on the smart-card. In the authentication phase, the

smart-card is submitted by the user to the access control site and the sensor acquires "new" sample data. The following actions are performed (Fig. 1 illustrates the scenario):

1. From the acquired sample data, a template is extracted and compared to the template on the smart-card. Only if there is sufficient correspondence, the following stages are conducted subsequently. Note that this is done at the sensor site, so there is no necessity to contact the centralized database.
2. The smart-card embeds its template 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 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). Note that in the latter case, the correspondence is expected to be higher since the template generated during enrollment has been extracted as template watermark – coming from the smart card – and is also extracted from the database.
5. Finally, in case the integrity of the data has been proven, the template watermark and the template are used in the matching process, granting access if the similarity to the database template is high enough.

When comparing this approach to previous techniques proposed in literature, we notice the following differences / advantages: As opposed to techniques employing robust watermarking, the proposed scheme can ensure sample data integrity in addition to enabling tightly coupled transport. As opposed to techniques employing arbitrary (semi-)fragile watermarks for integrity protection (instead of the template watermark used here), there is no need to transmit / store the watermarks at the receiving site for integrity verification. Additionally, the recognition performance is better since two templates can be used in the matching process, one of which eventually identical to the database template.

When compared to integrity protection enabled by (robust) digital signatures, our approach offers the advantage of disclosing the location of eventual modification which enables the assessment of the modifications' significance. Also, the verification data is embedded and does not have to be taken care of separately. Besides, a signature-based scheme cannot provide the functionality of transporting the authentication data stored on the card, it is intrinsically restricted to integrity verification and cannot support the two-factor aspect of the scheme we have introduced here.

However, some issues need to be investigated with respect to the proposed scheme (which will be done in the experiments):

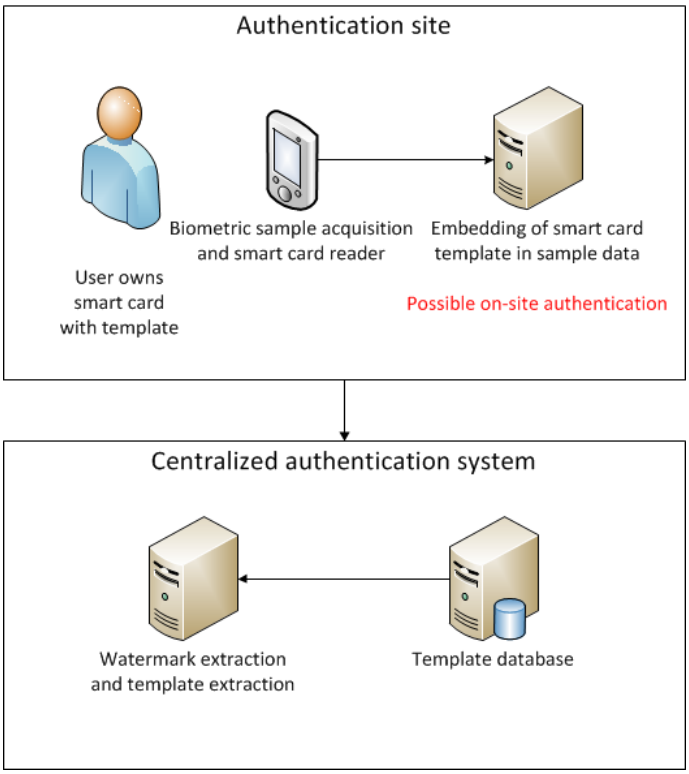


Fig. 1. Considered application scenario

- How can we construct an actual semi-fragile watermarking technique capable of embedding template data ?
- What is the impact of the embedded template watermark on the recognition performance using the template for matching only ?
- What is the amount of robustness we can support with a scheme like this (as opposed to a fragile scheme) ?
- Does integrity verification indeed work in a robust manner ?
- Can biometric matching take advantage of the two different templates available for matching ?

4 Experiments in the Case of Iris Recognition

4.1 Iris Recognition and Iris Databases

The employed iris recognition system is Libor Masek's Matlab implementation[4] of a 1-D version of the Daugman iris recognition algorithm. First, this algorithm

[4] `http://www.csse.uwa.edu.au/~pk/studentprojects/libor/sourcecode.html`

segments the eye image into the iris and the remainder of the image. Iris image texture is mapped to polar coordinates resulting in a rectangular patch which is denoted "polar image". For feature extraction, a row-wise convolution with a complex Log-Gabor filter is performed on the polar image pixels. The phase angle of the resulting complex value for each pixel is discretized into 2 bits. The 2 bit of phase information are used to generate a binary code. After extracting the features of the iris, considering translation, rotations, and disturbed regions in the iris (a noise mask is generated), the algorithm outputs the similarity score by giving the Hamming distance between two extracted templates. The sensible range of the Hamming distance reaches from zero (ideal matching of two iris images of the same person) to 0.5 (ideal mismatch between two iris images of different persons).

The following three datasets are used in the experiments:

CASIAv3 Interval database[5] consists of 2639 images with 320×280 pixels in 8 bit grayscale .jpeg format, out of which 500 images have been used in the experiments.

MMU database[6] consists of 450 images with 320×240 pixels in 24 bit grayscale .bmp format, all images have been used in the experiments.

UBIRIS database[7] consists of 1876 images with 200×150 pixels in 24 bit colour .jpeg format, out of which 318 images have been used in the experiments.

All intra-class and inter-class matches possible with the selected respective image sets have been conducted to generate the experimental results shown.

4.2 The Watermarking Scheme

As the baseline system, we employ the fragile watermarking scheme as developed by Yeung et. al and investigated in the context of fingerprint recognition [20]. For this algorithm, the watermark embedded is binary and padded to the size of the host image. Subsequently, the WM is embedded into each pixel according to some key information. As a consequence, the WM capacity is 89600, 76800, and 30000 bits for CASIAv3, MMU, and UBIRIS, respectively. Fig. 1 shows PSNR values averaged over all images embedding 10 randomly generated WM into each image. Obviously, the quality of the images remains very high after embedding, especially with enabled error diffusion which is therefore used in all subsequent experiments.

In Figure 2 we display tampering localization examples of the original fragile scheme. Fig. 2.b shows a doctored image corresponding to images as used in the attack in [4] – the attack is clearly revealed and the location is displayed in exact manner. As expected, when applying compression to the image with JPEG quality 75%, the WM indicates errors across the entire image (except for the pupil area which is not affected by compression due to its uniform grayscale) as shown in Fig. 2.f.

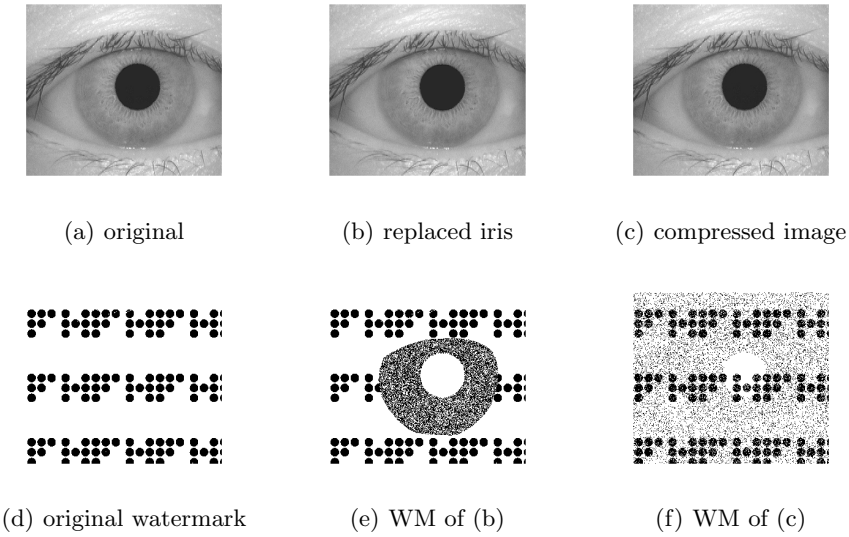
[5] `http://www.cbsr.ia.ac.cn/IrisDatabase.htm/`

[6] `http://pesona.mmu.edu.my/~ccteo/`

[7] `http://www.di.ubi.pt/~hugomcp/investigacao.htm`

	CASIAv3	MMU	UBIRIS
PSNR [dB]	48.07	43.22	47.69
PSNR with ED [dB]	49.57	44.57	49.16

Table 1. PSNR without and with error diffusion.



(a) original (b) replaced iris (c) compressed image

(d) original watermark (e) WM of (b) (f) WM of (c)

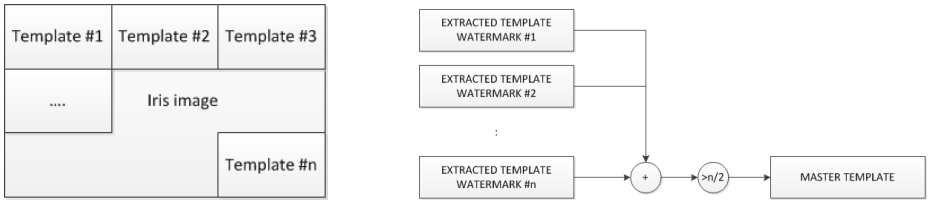
Fig. 2. Tamper localization of the original Yeung scheme.

Since this technique is a fragile WM scheme, no robustness against any image manipulations can be expected of course. Table 2 demonstrates this property by displaying averaged bit error rates (BER) computed between original and extracted WMs for a subset of 100 images with randomly generated WMs. As can be observed, there is a certain amount of robustness against noise and JPEG compression with quality 100. For the other attacks, the BER of 0.5 indicates that the extracted WMs are purely random and therefore entirely destroyed by the attack.

So far, randomly generated WM with size identical to the images have been embedded. The usually smaller size of biometric templates can be exploited to embed the template in redundant manner, i.e. we embed the template several times as shown in Fig. 3.a. After the extraction process, all template watermarks are used in a majority voting scheme which constructs a “master” template watermark as shown in Fig. 3.b. We expect to result in higher robustness leading to an overall semi-fragile WM scheme for the template WMs.

Attack	CASIAv3	MMU	UBIRIS
Mean filtering	0.50	0.50	0.50
Gaussian Noise $N = 0.0005$	$4.6 \cdot 10^{-5}$	$5.6 \cdot 10^{-5}$	$6.1 \cdot 10^{-5}$
Gaussian Noise $N = 0.001$	0.03	0.03	0.03
JPEG Q100	0.05	0.06	0.05
JPEG Q95	0.43	0.45	0.45
JPEG Q75	0.49	0.50	0.50

Table 2. BER for six different attacks.



(a) redundant embedding (b) majority voting

Fig. 3. The semi-fragile Yeung scheme.

In our implementation, the iris code consists of 9600 bits, therefore, we can embed 9, 8, and 3 templates into images from the CASIAv3, MMU, and UBIRIS databases, respectively.

4.3 Experimental Results

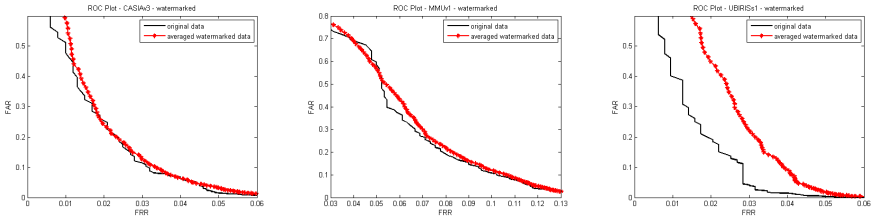
In Table 3 we show results for the robustness tests when applied to the database images with redundantly embedded template watermarks. When compared to Table 2, we clearly observe improved robustness against noise insertion and moderate JPEG compression. It can be clearly seen that with an increasing amount of redundancy, robustness is improved which is to be expected due to the more robust majority decoding (please recall, that for CASIAv3 redundancy is maximal among the three datasets).

In interesting question is the extent of influence an embedded watermark has on the recognition performance of the system. In Fig. 4 we compare ROC curves of the original data and ROC curves of sample data with embedded WMs - in the latter case, the average of ten embedded WMs is shown. While for the CASIAv3 and MMU there is hardly a noticeable impact, we notice significant result degradation in the case of the UBIRIS dataset.

A possible explanation for this effect is the already low quality of this dataset, in case of additional degradation results get worse quickly, while for the other datasets there is still room for slight quality reduction since the original quality is very high.

Attack	CASIAv3	MMU	UBIRIS
Mean filtering	0.50	0.50	0.50
Gaussian Noise $N = 0.0005$	0	0	0
Gaussian Noise $N = 0.001$	0	0	0.003
JPEG Q100	0	0	0.01
JPEG Q99	0	0.01	0.05
JPEG Q98	0.08	0.14	0.22
JPEG Q95	0.35	0.40	0.43

Table 3. BER for seven different attacks.



(a) CASIAv3 (b) MMU (c) UBIRIS

Fig. 4. ROC curves for the sample data with random embedded WMs and without.

The situation changes when it comes to additional distortions: As shown in Table 4, also in the case of the CASIAv3 we notice some impact on recognition performance with embedded WMs as compared to the original sample data without WMs embedded. Beside the EER, we show FRR (for $FAR = 10^{-3}$) and FAR (for $FRR = 5 \cdot 10^{-3}$). It is interesting to see that mean filtering and moderate JPEG compression can even improve the recognition results of the data without WM embedded – this effect is due to the denoising capabilities of mean filtering and compression. In any case, we notice a slight result degradation for the variant with embedded WMs.

Finally, we want to consider the question in how far matching between template WM and database template(s) is influenced by attacks, i.e. we investigate robustness of the embedded template WM. The corresponding information can be used to assess the integrity of the data, i.e. in case a sufficient high degree of correspondence between those templates is observed, the integrity of the sample data is proven. We consider the case that 5 different templates are stored in the database out of which a single database template is generated by majority coding like explained before in the case of the template WM (compare Figure 3.b). Table 5 shows the BER for the different attacks considered.

A typical decision threshold for the iris recognition system in use is at a BER ranging in $[0.3, 0.35]$. When taking this into account, we realize that integrity verification in our technique is indeed robust against moderate JPEG compression and noise. On the other hand, mean filtering and JPEG compression at quality

		ERR	FRR	FAR
CASIAv3				
no attack	original	0.045	0.091	0.650
	template watermark	0.048	0.081	0.742
mean filter	original	0.035	0.061	0.644
	template watermark	0.044	0.063	0.669
JPEG Q98	original	0.037	0.074	0.626
	template watermark	0.049	0.086	0.617
UBIRIS				
no attack	original	0.032	0.062	0.764
	template watermark	0.046	0.071	0.865
Gaussian Noise $N = 0.001$	original	0.038	0.068	0.871
	template watermark	0.049	0.073	0.868
JPEG Q95	original	0.036	0.066	0.838
	template watermark	0.045	0.070	0.975

Table 4. ROC behavior under different attacks.

Attack	CASIAv3	MMU	UBIRIS
No attack	0.21	0.23	0.19
Mean filtering	0.49	0.50	0.50
Gaussian Noise $N = 0.0005$	0.21	0.23	0.19
Gaussian Noise $N = 0.001$	0.21	0.23	0.19
JPEG Q100	0.21	0.23	0.19
JPEG Q99	0.21	0.24	0.22
JPEG Q98	0.25	0.30	0.32
JPEG Q95	0.41	0.45	0.45

Table 5. BER for seven different attacks.

95% destroys the template WM and indicates modification. The distribution of incorrect bits can be used to differentiate between malicious attacks (where an accumulation of incorrect bits can be observed in certain regions, compare Fig. 2.e) and significant global distortions like compression (compare Fig. 2.f).

5 Conclusion

In this paper we have introduced a two-factor authentication system using biometrics and a token-based scheme, e.g. a smart-card. Semi-fragile WM is used to embed the template data stored on the smart-card into the sample data acquired at the authentication site. We have discussed certain advantages of the approach as compared to earlier work and have shown experimentally in the case of an iris recognition system, that indeed semi-fragile integrity verification is achieved using the proposed approach. Care has to be taken in the actual

biometric matching process since contrasting to claims in literature recognition performance of the templates extracted from watermarked sample data suffers degradation to some minor extent. However, this can more than compensated by the additional template watermark which should be involved in matching as well.

References

[1] Nick Bartlow, Nathan Kalka, Bojan Cukic, and Arun Ross. Protecting iris images through asymmetric digital watermarking. In *IEEE Workshop on Automatic Identification Advanced Technologies*, volume 4432, pages 192–197, West Virginia University, Morgantown, WV, USA, June 2007.

[2] Jing Dong and Tieniu Tan. Effects of watermarking on iris recognition performance. In *Proceedings of the 10th International Conference on Control, Automation, Robotics and Vision (ICARCV 2008)*, pages 1156–1161, 2008.

[3] J. Hämmerle-Uhl, K. Raab, and A. Uhl. Experimental study on the impact of robust watermarking on iris recognition accuracy (best paper award, applications track). In *Proceedings of the 25th ACM Symposium on Applied Computing*, pages 1479–1484, 2010.

[4] J. Hämmerle-Uhl, K. Raab, and A. Uhl. Attack against robust watermarking-based multimodal biometric recognition systems. In C. Vielhauer et al., editor, *Proceedings of the 2011 BioID Workshop*, volume 6583 of *Springer LNCS*, pages 25–36, Brandenburg, Germany, 2011.

[5] J. Hämmerle-Uhl, K. Raab, and A. Uhl. Watermarking as a means to enhance biometric systems: A critical survey. In A. Ker, S. Craver, and T. Filler, editors, *Proceedings of the 2011 Information Hiding Conference (IH'11)*, Springer LNCS, Prague, Czech Republic, 2011. to appear.

[6] A. K. Jain and U. Uludag. Hiding fingerprint minutiae in images. In *Proceedings of AutoID 2002, 3rd Workshop on Automatic Identification Advanced Technologies*, pages 97–102, Tarrytown, New York, USA, March 2002.

[7] A. K. Jain, U. Uludag, and R. L. Hsu. Hiding a face in a fingerprint image. In *Proceedings of the International Conference on Pattern Recognition (ICPR'02)*, pages 756–759, Quebec City, Canada, August 2002.

[8] A.K. Jain and U. Uludag. Hiding biometric data. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 25(11):1494–1498, November 2003.

[9] M.K. Khan, L. Xie, and J.S. Zhang. Robust hiding of fingerprint-biometric data into audio signals. In *Advances in Biometrics*, volume 4642 of *LNCS*, pages 702–712, Seoul, Korea, August 2007.

[10] A. Lang and J. Dittmann. Digital watermarking of biometric speech references: impact to the eer system performance. In E. J. Delp and P. W. Wong, editors, *Security, Steganography, and Watermarking of Multimedia Contents IX*, number 6505 in Proceedings of SPIE, page 650513ff, 2007.

[11] D. Moon, T. Kim, S.-H. Jung, Y. Chung, K. Moon, D. Ahn, and S..K. Kim. Performance evaluation of watermarking techniques for secure multimodal biometric systems. In *Proceedings of CIS 2005 (Part II)*, volume 3802 of *LNAI*, pages 635 – 642, 2005.

[12] A. Noore, R. Singh, M. Vatsa, and M.M. Houck. Enhancing security of fingerprints through contextual biometric watermarking. *Forensic Science International*, 169:188–194, 2007.

[13] Kang Ryoung Park, Dae Sik Jeong, Byung Jun Kang, and Eui Chul Lee. A study on iris feature watermarking on face data. In *Proceedings of the 8th International Conference on Adaptive and Natural Computing Algorithms, ICANNGA '07*, volume 4432 of *Lecture Notes in Computer Science*, pages 415–423, Warsaw, Poland, April 2007. Springer Berlin, Heidelberg.

[14] M. I. Rajibul, M.S Shohel, and S. Andrews. Biometric template protection using watermarking with hidden password encryption. In *Proceedings of the International Symposium on Information Technology 2008 (ITSIM08)*, pages 296 – 303, 2008.

[15] N.K. Ratha, J.H. Connell, and R.M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3):614–634, April 2001.

[16] Chris Roberts. Biometric attack vectors and defenses. *Computers & Security*, 26:14–25, 2007.

[17] T. Satonaka. Biometric watermark authentication with multiple verification rule. In *Proceedings of the 12th IEEE Workshop on Neural Networks in Signal Processing*, pages 597–606, 2002.

[18] Claus Vielhauer and Ralf Steinmetz. Approaches to biometric watermarks for owner authentification. In *Proceedings of SPIE, Security and Watermarking of Multimedia Contents III*, volume 4314, San Jose, CA, USA, January 2001.

[19] D.-S. Wang, J.-P. Li, D.-K. Hu, and Y.-H. Yan. A novel biometric image integrity authentication using fragile watermarking and Arnold transform. In J.P. Li, I. Bloshanskii, L.M. Ni, S. S. Pandey, and S. X. Yang, editors, *Proceedings of the International Conference on Information Computing and Automatation*, pages 799–802, 2007.

[20] Minerva M. Yeung and Sharat Pankanti. Verification watermarks on fingerprint recognition and retrieval. *Journal of Electronal Imaging, Special Issue on Image Security and Digital Watermarking*, 9(4):468–476, October 2000.

[21] C. Zeitz, T. Scheidat, J. Dittmann, and Claus Vielhauer. Security issues of internet-based biometric authentication systems: risks of man-in-the-middle and BioPhishing on the example of BioWebAuth. In E.J. Delp, P.W. Wong, J. Dittmann, and N.D. Nemon, editors, *Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, volume 6819 of *Proceedings of SPIE*, pages 0R–1 – 0R12, 2008.