International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:8, No:4, 2014

Effects of Reversible Watermarking on Iris Recognition Performance

Andrew Lock, Alastair Allen

Abstract—Fragile watermarking has been proposed as a means of adding additional security or functionality to biometric systems, particularly for authentication and tamper detection. In this paper we describe an experimental study on the effect of watermarking iris images with a particular class of fragile algorithm, reversible algorithms, and the ability to correctly perform iris recognition. We investigate two scenarios, matching watermarked images to unmodified images, and matching watermarked images to watermarked images. We show that different watermarking schemes give very different results for a given capacity, highlighting the importance of investigation. At high embedding rates most algorithms cause significant reduction in recognition performance. However, in many cases, for low embedding rates, recognition accuracy is improved by the watermarking process.

Keywords—Biometrics, iris recognition, reversible watermarking.

I. Introduction

BIOMETRICS are proving an increasingly popular alternative to traditional authentication mediums as they resolve many issues associated with token or password-based systems. However, many works identify threats to biometric systems such as spoofing, mimicry and man in the middle attacks [1], [2]. Watermarking has been suggested as one possible means to reduce the security vulnerabilities of biometrics, and in some cases to enhance their functionality [3].

All watermarking methods alter the host image to some extent, though the perceptibility of this modification varies with the watermarking scheme and the capacity – the quantity of data embedded. The acceptability of the distortion depends on the particular application. The effect of watermarking methods on biometrics, in particular iris detection, has been investigated for robust techniques [4], [5]. However, the effect of fragile algorithms has not been studied.

In this paper, we investigate the effect fragile watermarking algorithms, specifically reversible or lossless algorithms, have on iris recognition accuracy. We aim to address whether particular watermarking techniques are more suited to this application than others, and the impact that capacity has on iris recognition performance.

Section II provides an overview of watermarking in the context of biometric systems. Section III describes experiments in which we test the impact of seven watermarking algorithms on iris recognition accuracy over a range of embedding capacities. Section IV discusses the results and Section V concludes the paper.

A. Lock and A. Allen are with the Department of Engineering, University of Aberdeen, Aberdeen, UK (phone: +44 1224 272501, e-mail: r04al9@abdn.ac.uk).

II. Watermarking and Biometrics

A. Watermarking

Watermarking is a technique of hiding data within a host image by modifying the image such that the data can be extracted later. By definition, watermarking modifies the cover work, introducing distortion. The level to which this distortion is permissible depends on the particular application, but is often required to be imperceptible [6]. If modifications of the watermarked image prevent recovery of the embedded data, the watermark is termed fragile, otherwise it is robust.

In some fields, for example in the medical or military domain, even slight distortions of the original image are not permissible. Consequently many watermarking algorithms have been proposed that allow recovery of the original image during the extraction process. These are termed reversible or lossless algorithms. While these have the additional capabilities of allowing recovery of the original image, they retain all other characteristics of normal watermarking schemes. In this paper, we focus on this area of fragile reversible watermarking algorithms. Reversibility is not essential for most biometric applications; however its presence does not affect the conclusions that may be drawn from studying the effect of fragile watermarking on iris recognition.

B. Watermarking in Biometric Systems

In [3] multiple scenarios are suggested where watermarking can improve the security of biometrics. The first is purely steganographic, in which biometric data is embedded within an arbitrary host image, with the aim of concealing the embedded data from a potential attacker. This technique is suggested by Jain and Uludag in [7], in which facial data is hidden in an artificial fingerprint image. Hassanien describes a watermarking method using the discrete wavelet transform in [8] to embed iris images into a host image. Dong and Tan explore the effect of embedding iris templates into host images using robust watermarking in [5], and the extent to which attacks on the host image reduce the ability to extract and match the embedded iris template. Although the majority of algorithms proposed for biometric steganography are robust, it is suggested in [3] that robust watermarking should not be used for steganographic purposes, as the robustness typically implies an increase in perceptibility, the key feature in this scenario [6].

Watermarking can also be used to authenticate the sample and sensor by embedding a fragile watermark containing an identifier unique to the camera and a cryptographic hash of

the original, creating a 'secure camera'. On verification, if the watermark cannot be extracted and verified, then the image has been tampered with and cannot be authenticated. Blythe and Fridrich use this approach in [9] to create a secure digital camera for securing iris images, while Yeung and Pankanti use a fragile watermark to secure fingerprint data in [10]. It is important that the watermark is fragile so that any attack results in failure to authenticate [3]. This contrasts with liveness detection schemes, whereby detection of a watermark indicates the data has been previously acquired and is being presented again. In this case, the watermark must be highly robust against attempts to remove it.

An alternative scenario, multi-modal biometric verification, in which biometric data is embedded into a biometric image and recovered during verification to improve recognition performance, has been the subject of many works. Bartlow et al. [11] propose a framework that embeds voice feature descriptors in iris images, using robust watermarking to provide added authentication, data integrity and non-repudiation of origin. Hoang et al. [12] propose using fragile watermarking to embed biometric data in facial images, while Jain et al. [13] and Noore et al. [14] propose using robust watermarking to embed facial data in a fingerprint image. Vatsa et al. demonstrate the improved recognition accuracy of multi-modal biometrics using robust watermarking in [15].

A variation of this approach is two-factor authentication, in which a token must be presented along with biometric data for verification. The token is used to partially authenticate the user, and is subsequently embedded into the biometric sample, which can be transferred to a central database for verification, providing data integrity as well as two-factor authentication. Huber et al. suggest such a method in [16] in which a semi-fragile watermark is embedded into iris images. In [17], Jain and Uludag propose embedding face data in fingerprint images stored on a smart card, while Satonaka proposes to embed a traditional password token in face data in [18]. Whilst robust watermarks are often suggested for two factor and multi-modal authentication, it is suggested in [3] that fragile techniques should be preferred, to provide security against tampering along with improved capacity.

As described, many application scenarios call for fragile watermarks. While the impact of robust schemes on iris recognition was described in [4], the impact of fragile watermarking on recognition accuracy is hardly discussed.

C. Iris Detection

The majority of iris recognition algorithms follow the well-known work of Daugman [19], including the OSIRIS (Open Source for IRIS) [20] implementation used for this study.

After image acquisition, the pupil is located, and from here the iris is localized using a circular Hough transform followed by an active contour approach [21], to identify the two approximately concentric circles of the pupil and iris. The identified iris is unwrapped and normalized using polar coordinates to a rectangular texture of 512×64 pixels. A mask of the same size is generated that identifies regions which should be excluded from the feature detection, e.g. eyelids. Finally, the iris code is generated by applying 2D Gabor filters to the masked image at selected points and coding the output coefficients to produce a binary sequence. Matching of iris codes is performed by finding the minimum Hamming distance between two codes at multiple shifted positions.

III. Experimental method

Experiments were performed using the ICE-Right database [22] released by the National Institute of Standards and Technology (NIST) in 2005. It contains 1425 monochrome 8-bit images, from 124 subjects' right eyes. In order to focus the watermarking effect on the iris itself, all images were cropped to 320×320 pixels, centred on the iris.

Seven watermarking algorithms were implemented for the study and are briefly described below. They were selected to investigate a variety of different watermarking techniques, including state-of-the art approaches.

Celik et al. [23] proposed a generalized form of least significant bit embedding. An image is quantized and the difference in images is compressed and embedded with the payload in the quantized image. The capacity is highly image dependent as it depends on the compressibility of features. The method is herein denoted as 'LSB'.

Tian [24] proposed a spatial domain algorithm (herein denoted as 'DIFF') that expands the difference between adjacent pixels to create space for embedding. As well as the data embedded, a location map indicating which locations were selected must be embedded as overhead.

Sachnev et al. [25] used sorting and prediction to extend this approach (herein denoted as 'SP') by expanding prediction-error differences rather than raw pixel differences. This allowed a greater capacity with reduced distortion.

Weng et al. [26] use an alternative transform for difference expansion. They extend the method to reduce the magnitude of pixel modification by using pairwise difference adjustment and creating a highly compressible location map (herein denoted as 'PDA').

Li et al. [27] proposed shifting the histogram of adjacent pixel differences, such that each pixel was shifted by at most one intensity value (herein denoted as 'APD'). The capacity is highly image dependent and comparatively small compared to the other algorithms presented.

Yang et al. [28] propose applying an integer version of the 8×8 discrete cosine transform and using bit-shifting in the transform domain to provide capacity for the watermark (herein denoted as 'DCT'). Due to the relatively large number of blocks that cause overflow during watermarking, the capacity of the scheme was relatively small for the iris images compared to natural images.

Lee et al. [29] propose a similar approach to that of Yang et al. by using bit-shifting on the coefficients of the integer $5/3$ discrete wavelet transform. The resulting scheme (herein denoted as 'DWT') has a high capacity with a relatively low distortion rate.

TABLE I
MEAN PSNR AND SSIM OF WATERMARKED. AREA OVER THE DET CURVE (AOC), p-VALUE AND EQUAL ERROR RATE (EER) FOR ORIG-WMK AND WMK-WMK MATCHING.STATISTICALLY SIGNIFICANT DIFFERENCES ARE EMBOLDENED

Watermark & bpp		PSNR (dB)	SSIM	Orig-Wmk			Wmk-Wmk		
				AOC	p-value	EER (%)	AOC	p-value	EER (%)
Originals				0.988		4.93	0.988		4.93
APD	0.25	41.6	0.95	0.988	0.183	5.08	0.988	0.683	5.17
	0.50	36.1	0.90	0.987	0.152	5.10	0.987	0.226	5.21
DCT	0.25	39.0	0.96	0.988	0.259	4.93	0.988	0.327	4.78
	0.50	35.5	0.92	0.988	0.161	5.13	0.988	0.514	4.90
DIFF	0.25	40.6	0.97	0.987	0.842	4.78	0.989	0.494	4.50
	0.50	33.6	0.88	0.990	0.544	4.91	**0.991**	**0.007**	**4.40**
	0.75	31.3	0.84	0.988	0.425	5.09	0.989	0.825	5.26
	1.00	25.9	0.64	**0.985**	**0.000**	**5.91**	**0.982**	**0.000**	**6.58**
DWT	0.25	41.3	0.97	0.988	0.918	5.07	0.989	0.905	4.96
	0.50	36.5	0.93	0.989	0.694	4.98	0.989	0.465	4.90
	0.75	31.3	0.84	0.989	0.264	4.82	0.990	0.086	4.43
	1.00	27.7	0.73	**0.987**	**0.034**	**5.16**	0.988	0.755	4.80
LSB	0.25	49.5	0.99	**0.989**	**0.048**	**4.83**	**0.991**	**0.014**	**4.44**
	0.50	46.5	0.98	**0.990**	**0.039**	**4.68**	**0.991**	**0.016**	**4.59**
	0.75	35.7	0.85	0.989	0.240	4.85	0.990	0.164	4.87
PDA	0.25	41.4	0.97	**0.990**	**0.000**	**4.55**	**0.993**	**0.000**	**4.06**
	0.50	34.9	0.91	0.989	0.187	4.80	0.990	0.116	4.87
	0.75	31.2	0.83	0.989	0.397	5.03	0.990	0.111	4.92
	1.00	26.1	0.65	**0.987**	**0.027**	**5.34**	**0.985**	**0.008**	**5.86**
SP	0.25	43.1	0.98	0.989	0.056	4.79	**0.991**	**0.001**	**4.58**
	0.50	37.8	0.94	0.989	0.498	4.90	0.990	0.114	4.96
	0.75	33.6	0.88	**0.987**	**0.041**	**5.02**	0.986	0.111	4.96
	1.00	28.4	0.72	**0.987**	**0.048**	**5.02**	**0.985**	**0.012**	**5.40**

Watermarking was performed using the seven algorithms discussed with a randomly generated payload at four embedding capacities: 0.25, 0.50, 0.75 and 1.00 bits per pixel (bpp). Where the required capacity could not be achieved with an algorithm natively, as was the case for APD at all levels, and DIFF, PDA and SP at and above 0.50 bpp, the image was recursively watermarked until the total required payload capacity was reached. Due to the nature of the algorithms, not all schemes could watermark all the images at all capacities, even using recursion. Where the number of images that could be watermarked by an algorithm at a given capacity was less than half the total number of images, the algorithm/capacity pair was excluded from the group comparison. Consequently LSB at 1.00 bpp, and both APD and DCT at 0.75 and 1.00 bpp were excluded. A total of 608 images were successfully watermarked at all of the selected capacities by all algorithms to create 23 sets of 608 watermarked images, plus the original images set.

All of the image sets were processed with OSIRIS to generate the iris codes. Two matching scenarios were investigated: matching of original images to watermarked images (Orig-Wmk), and matching of watermarked images to watermarked images (Wmk-Wmk). The former scenario describes the situation where an unwatermarked template is compared to a sensor image which has been watermarked to create a 'secure camera'. The later represents the case where the stored template was also generated from a watermarked sensor image.

For Wmk-Wmk matching, each watermarked code in a set was matched with every other watermarked code in the set, for a total of 181,302 inter-class and 3,226 intra-class comparisons within each set. For Orig-Wmk matching, all original images were matched to all other watermarked images, for a total of 362,604 inter-class comparisons and 6,452 intra-class comparisons. Given the computational cost of performing over 500,000 comparisons in total for each set, it was not possible to investigate more than one iris recognition algorithm. Hmmerle-Uhl et al. [4] found that the specific recognition algorithm used made no difference in results for robust watermarking, suggesting the use of a single algorithm should not affect the conclusions that may be drawn. However, extension to further iris algorithms is a clearly desirable area of further work.

IV. EXPERIMENTAL RESULTS

The mean quality of the watermarked images compared to the originals is shown in Table I. The PSNR ranges from 25.9 to 49.5 dB, while the SSIM [30] ranges from 0.64 to 0.99. This level of degradation is approximately comparable to the PSNR of 30 dB and 45 dB used by Hmmerle-Uhl et al. [4] when investigating robust watermarking, although in that case two embedding capacities were used, approximately 0.001 bpp and 0.010 bpp. The considerable additional payload capacity achieved thanks to the use of fragile watermarking could facilitate additional applications.

Fig. 1 shows the detection error trade-off (DET) curves for Wmk-Wmk matching. They show the trade-off between the false accept rate (FAR) and false reject rate (FRR) along with the equal error rate (EER) for each matching case. The match rate for the original images, where no watermarking has been applied, is shown for reference in each plot. The optimal DET curve would be positioned to the bottom left of each

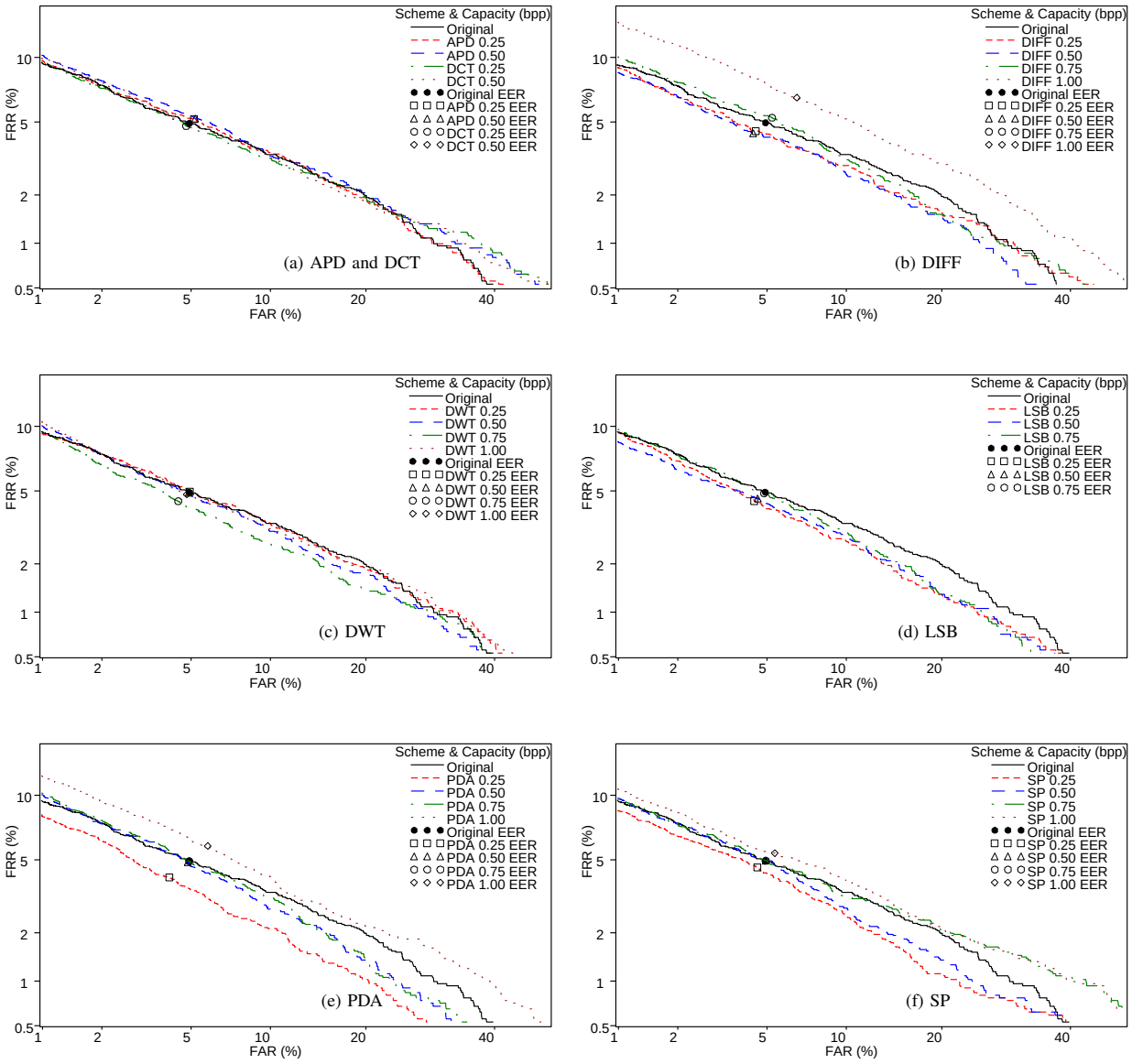

Fig. 1 DET plots of iris matching for Wmk-Wmk matching

plot. In general, it can be seen that for lower embedding rates the DET curve for each algorithm closely follows that of the reference curve, in some cases outperforming it. At the highest embedding level, 1.00 bpp, the curve deviates significantly for SP, PDA and particularly DIFF. These large deviations are associated with an observable increase in EER. Space considerations prevent displaying DET curves for Orig-Wmk matching, however the watermarked curves broadly follow those of Wmk-Wmk matching.

Table I summarizes the DET curves for each matching scenario by providing the area over the DET curve (AOC) and the EER. The larger the AOC, the better the performance, with the optimal area being 1.0. Also shown is the p-value found when testing for significant difference in AOC between each watermarked DET curve and the reference curve, using the method of DeLong et al. [31].

The precise behaviour of the DET curves is different for each watermarking algorithm, varying with embedded capacity and matching scenario. APD shows no significant difference to the original curve in terms of AOC, however the EER is larger in all cases. As may be expected, the EER for 0.50 bpp is greater than for 0.25 bpp. Also, Wmk-Wmk matching produces

higher EERs than Orig-Wmk matching.

DCT also shows no significant difference in terms of AOC, however the EER is not larger than the originals in all cases. While the EER for 0.50 bpp is greater than for 0.25 bpp in both matching scenarios, Wmk-Wmk matching actually outperforms both Orig-Wmk and the original EER. Watermarking in this case results in an improvement in the segmentation stage of the iris recognition algorithm compared to the original images, giving a slight improvement in EER. This may be due to increased high frequency content in the watermarked image allowing easier delineation of boundaries.

This effect is also observed for DIFF watermarking at lower embedding levels, with the improvement in segmentation resulting in an AOC that is significantly improved compared to the original ($p < 0.05$) at 0.50 bpp for Wmk-Wmk matching. However at the highest embedding level, the AOC is significantly worse than the original curve and the EER significantly larger. This is due to the effect of watermarking on the template generation stage of the recognition algorithm. Although watermarking can improve the segmentation, the effect of watermarking is always found to be negative on the template generation stage, with the negative effects larger for Wmk-Wmk matching. Consequently the overall DET curve at a given capacity is the interaction between the improvement in segmentation and deterioration of template generation.

This trade-off between segmentation and template generation is responsible for the trends seen in the remaining algorithms. For DWT, the improvement relative to the original images peaks at 0.75 bpp for both scenarios. However, at 1.00 bpp, the adverse effect on template generation results in a significantly poorer curve for Orig-Wmk matching.

The comparatively high image quality of LSB results in significant improvements over the original images for both scenarios at 0.25 and 0.50 bpp. The watermarking distortion allows improved segmentation but is insufficient to cause disruption to the template generation process. Improvements in EER can also be seen across all embedding capacities.

PDA shows a significant improvement in AOC at 0.25 bpp, and a significant decrease in performance of AOC at 1.00 bpp. This is again typical of the segmentation improvement and template generation detriment trade-off described previously.

SP shows slightly better performance in Wmk-Wmk matching than in Orig-Wmk matching. The AOC is significantly improved for Wmk-Wmk at 0.25 bpp but not for Orig-Wmk, while at 0.75 bpp the performance is significantly worse for Orig-Wmk but not for Wmk-Wmk. In both cases 1.00 bpp causes a significant reduction in performance.

The experiments presented demonstrate some unexpected consequences of fragile watermarking when applied to iris recognition. Firstly, the impact of watermarking is not always negative, but rather was found to improve recognition performance in several cases. This is due to an improvement in the segmentation stage of the recognition algorithm. The level of this effect varied between watermarkers.

In contrast to this improvement, the template generation stage of the recognition algorithm was always adversely affected by watermarking. The interplay of these two factors leads to the second observation, that increasing the capacity does not always result in a reduction in recognition performance. The capacity of the optimum performing DET curve varies with the particular watermarking scheme.

Finally, Orig-Wmk matching does not always outperform Wmk-Wmk matching. Again related to the the described trade-off, Wmk-Wmk matching tends to outperform Orig-Wmk at lower capacities where the improvement due to segmentation is large. It is typically outperformed by Orig-Wmk at high capacities where the detriment due to template generation dominates.

The levels of embedding, and hence degradation, used in this study are significantly higher than would be expected for many scenarios. For example, iris template data typically requires only 2048 bits; in this case equivalent to 0.02bpp of data. However, the additional capacity allows embedding of multiple biometrics, along with further security data such as image hashes etc., creating the possibility of more powerful security applications.

While reversible algorithms were used in the study, they were treated simply as fragile watermarking algorithms. Although reconstructing the original image prior to iris matching would give unaffected results, it is the effect of watermarking, without the security risks and computational overhead of original image extraction, that is of interest. Also removing the watermark would leave the image unprotected, and hence would offer little advantage over purely cryptographic methods. The real value of watermarking lies in the direct replacement of an original image with its watermarked version.

V. Conclusion

This study showed that fragile watermarking significantly affects iris recognition performance in many cases. The extent to which iris recognition is affected, and whether the effect is positive or negative, depends highly on the watermarking scheme, the level of embedding, and the matching scenario, i.e. whether watermarked images are matched to watermarked or original images.

No significant decrease in AOC was found for any algorithm at rates of 0.50 bpp or less, with many algorithms showing a significant improvement. This suggests that for the watermarking algorithms studied, rates of embedding less than 0.50 bpp would be acceptable.

While this study shows promising results for the reversible watermarking algorithms studied, it is by no means conclusive in determining the best algorithm for the scenario, with many different approaches proving successful at low rates. However at the highest embedding rate, the error expansion techniques of DIFF, PDA and SP show the largest errors, suggesting they are not suited to applications with large capacity requirements. A more extensive study with a wider variety of capacities, alternative iris recognition algorithms and additional iris databases may clarify this effect.

REFERENCES

[1] Biometric Working Group, "Biometric security concerns," Biometric Working Group, UK Government, Tech. Rep., 2003.
[2] C. Roberts, "Biometric attack vectors and defences," *Computers & Security*, vol. 26, no. 1, pp. 14 – 25, 2007.
[3] J. Hämmerle-Uhl, K. Raab, and A. Uhl, "Watermarking as a means to enhance biometric systems: a critical survey," in *Proceedings of the 13th international conference on Information hiding*, ser. IH'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 238–254.
[4] ——, "Experimental study on the impact of robust watermarking on iris recognition accuracy," in *Proceedings of the 2010 ACM Symposium on Applied Computing*. ACM, 2010, pp. 1479–1484.
[5] J. Dong and T. Tan, "Effects of watermarking on iris recognition performance," in *Proc. 10th Int. Conf. Control, Automation, Robotics and Vision ICARCV 2008*, 2008, pp. 1156–1161.
[6] J.-B. Feng, I.-C. Lin, C.-S. Tsai, and Y.-P. Chu, "Reversible watermarking: Current status and key issues," *I. J. Network Security*, vol. 2, no. 3, pp. 161–170, 2006.
[7] A. K. Jain, U. Uludag, and R.-L. Hsu, "Hiding a face in a fingerprint image," in *Proc. 16th Int Pattern Recognition Conf*, vol. 3, 2002, pp. 756–759.
[8] A. Hassanien, "Hiding iris data for authentication of digital images using wavelet theory," *Pattern Recognition and Image Analysis*, vol. 16, pp. 637–643, 2006, 10.1134/S1054661806040092.
[9] P. Blythe and J. Fridrich, "Secure digital camera," in *in Proceedings of Digital Forensic Research Workshop (DFRWS*, 2004, pp. 17–19.
[10] M. M. Yeung and S. Pankanti, "Verification watermarks on fingerprint recognition and retrieval," in *Proc. SPIE EI*, 1999, pp. 66–78.
[11] N. Bartlow, N. Kalka, B. Cukic, and A. Ross, "Protecting iris images through asymmetric digital watermarking," in *Proc. IEEE Workshop Automatic Identification Advanced Technologies*, 2007, pp. 192–197.
[12] T. Hoang, D. Tran, and D. Sharma, "Remote multimodal biometric authentication using bit priority-based fragile watermarking," in *Proc. 19th Int. Conf. Pattern Recognition ICPR 2008*, 2008, pp. 1–4.
[13] A. Jain and U. Uludag, "Hiding fingerprint minutiae in images," in *Proceedings of Third Workshop on Automatic Identification Advanced Technologies (AutoID), 2002*, 2002, pp. 97–102.
[14] A. Noore, R. Singh, M. Vatsa, and M. M. Houck, "Enhancing security of fingerprints through contextual biometric watermarking," *Forensic Sci Int*, vol. 169, no. 2, pp. 188–194, Jul. 2007.
[15] M. Vatsa, R. Singh, and A. Noore, "Feature based rdwt watermarking for multimodal biometric system," *Image Vision Comput.*, vol. 27, pp. 293–304, February 2009.
[16] R. Huber, H. Stögner, and A. Uhl, "Two-factor biometric recognition with integrated tamper-protection watermarking," in *Proceedings of the 12th IFIP TC 6/TC 11 international conference on Communications and multimedia security*, ser. CMS'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 72–84.
[17] A. K. Jain and U. Uludag, "Hiding biometric data," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 11, pp. 1494–1498, 2003.
[18] T. Satonaka, "Biometric watermark authentication with multiple verification rule," in *Proc. 12th IEEE Workshop Neural Networks for Signal Processing*, 2002, pp. 597–606.
[19] J. Daugman, "High confidence visual recognition of persons by a test of statistical independence," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15, no. 11, pp. 1148–1161, 1993.
[20] E. Krichen, A. Mellakh, S. Salicetti, and B. Dorizzi, "Osiris (open source for iris) reference system," BioSecure Project, Tech. Rep., 2008. [Online]. Available: http:/www.biosecure.info
[21] C. Xu and J. Prince, "Snakes, shapes, and gradient vector flow," *IEEE Transactions on Image Processing*, vol. 7, no. 3, pp. 359–369, 1998.
[22] P. Phillips, K. Bowyer, P. Flynn, X. Liu, and W. Scruggs, "The iris challenge evaluation 2005," in *Biometrics: Theory, Applications and Systems, 2008. BTAS 2008. 2nd IEEE International Conference on*. IEEE, 2008, pp. 1–8.
[23] M. Celik, G. Sharma, A. Tekalp, and E. Saber, "Lossless generalized-lsb data embedding," *IEEE Transactions on Image Processing*, vol. 14, no. 2, pp. 253–266, 2005.
[24] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits and Systems For Video Technology*, vol. 13, no. 8, pp. 890–896, 2003.
[25] V. Sachnev, H. Kim, J. Nam, S. Suresh, and Y. Shi, "Reversible watermarking algorithm using sorting and prediction," *IEEE Transactions on Circuits and Systems For Video Technology*, vol. 19, no. 7, pp. 989–999, 2009.
[26] S. Weng, Y. Zhao, J. Pan, and R. Ni, "Reversible watermarking based on invariability and adjustment on pixel pairs," *Signal Processing Letters, IEEE*, vol. 15, pp. 721–724, 2008.
[27] Y. Li, C. Yeh, and C. Chang, "Data hiding based on the similarity between neighboring pixels with reversibility," *Digital Signal Processing*, vol. 20, no. 4, pp. 1116–1128, 2010.
[28] B. Yang, M. Schmucker, W. Funk, C. Busch, and S. Sun, "Integer dct-based reversible watermarking for images using companding technique," in *Proceedings of SPIE*, vol. 5306. Citeseer, 2004, pp. 5306–41.
[29] S. Lee, C. Yoo, and T. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform," *Information Forensics and Security, IEEE Transactions on*, vol. 2, no. 3, pp. 321–330, 2007.
[30] Z. Wang, A. Bovik, H. Sheikh, and E. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, 2004.
[31] E. DeLong, D. DeLong, and D. Clarke-Pearson, "Comparing the areas under two or more correlated receiver operating characteristic curves: a nonparametric approach." *Biometrics*, vol. 44, no. 3, pp. 837–845, 1988.