Cloud Computing and Data Science
http://ojs.wiserpub.com/index.php/CCDS/

UNIVERSAL WISER PUBLISHER

Research Article

A Survey on Embedding Iris Biometric Watermarking for User Authentication

Taskeen Taj[*], **Manash Sarkar**

Department of Computer Science and Engineering, Atria Institute of Technology, Bangalore, India
E-mail: taskeentaj91@gmail.com

Received: 16 May 2023; **Revised:** 11 July 2023; **Accepted:** 11 July 2023

Abstract: This paper proposes an innovative approach called "Embedding Iris Biometric Watermarking" for user authentication. By utilizing the unique characteristics of the iris, a secure watermark is generated and embedded into the biometric data. This technique enhances the security and robustness of authentication systems, offering advantages such as high security, resistance to attacks, and non-intrusiveness. The proposed method has potential applications in access control, secure transactions, and digital rights management, providing a reliable solution for ensuring the integrity and confidentiality of digital systems and services.

***Keywords*:** biometric, authentication, accuracy, security, watermarking

1. Introduction

The process of watermarking involves overlaying a logo or line of text over a document or image file. By adding a watermark, unauthorized reuse or modification of data can be prevented and copyright can be protected. This implies that people won't steal your product, but they will still preview it before buying it. Digital watermarking is a technology that prevents information use from being impacted while embedding identification information into carrier data in ways that are difficult to detect. This often safeguards databases, text files, and copyrighted information from multimedia systems. Biometric authentication is a method to verify, that a person is who they say they are. Biometric authentication verifies by checking distinctive biological or behavioral characteristics. Both watermarking and biometric authentication are required to increase the digital security of user data. With iris biometrics as the iris is located at a remote area of an eye it is impossible to be copied and every individual has a unique iris pattern, even the iris of the same person are ideal identifiers because they are different. Thus iris biometric is considered the most reliable of all existing biometric authentication technology. There are many techniques for iris recognition. In order to conceptually conceal the user's unique identification, an image of a palm print is used as a watermark and make it resistant to attacks, Kumar et al. [1] used zero bit watermarking technique. It has been established that watermark extraction is erroneous. Processing high-quality data, like palm prints, takes longer.

The iris biometric is used to recognize people by their iris patterns, which are taken from photographs of their eyes. The three main components of the human eye are depicted in Figure 1: the sclera, which is white, the iris, which

DOI: https://doi.org/10.37256/ccds.4220233051

is colourful, and the pupil, which is located in the middle of the eye. The pupil in the eye is encircled by the iris. Since the pupil's size varies depending on the intensity of the light falling on it, the radius of the iris's inner border is likewise not constant. Every human being in the world has a distinctive iris pattern. From an image of the eye, this pattern can be retrieved and decoded. This code can be compared to codes found from images of 14 other eyes or from the same eye. The comparison's outcomes can show how different the compared codes are from one another. In this manner, it is possible to determine if the compared eye patterns are from the same or distinct eyes.

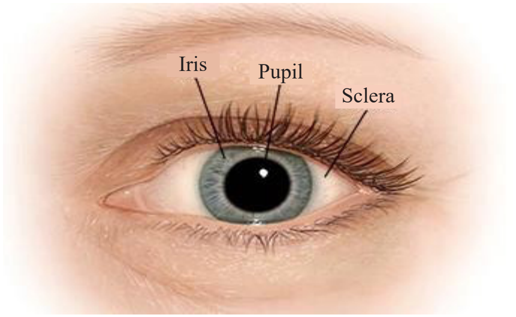

Figure 1. Front view of eye (Courtesy: Google)

2. Stages in iris identification system

As shown in Figure 2, Iris identification involves six steps: image capture, pupil segmentation, iris segmentation, normalization, feature extraction, and template matching. Due to its high rate of recognition, iris identification is recognized as the most trustworthy biometric model.

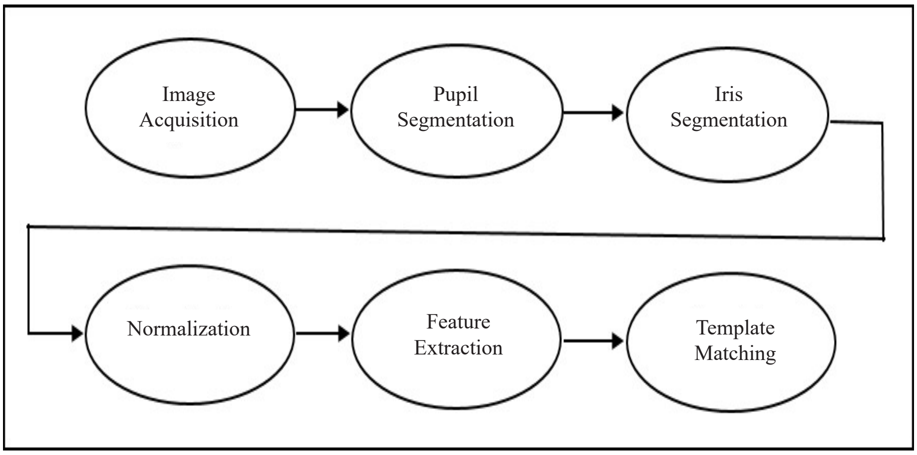

Figure 2. Stages in iris identification system

Image Acquisition: Image acquisition refers to capturing an iris image of high quality. It is required to obtain images with high resolution with sharpness. Images can be acquired using a near-infrared camera or LED. The distance between the lens and the imaging region is fixed, and by changing the form of the lens, the focal length required to achieve adequate focus is obtained.

Pupil Segmentation: By performing a 1D signal search and treating the eyelid as a parabola, the upper and lower eyelids of the human eye are discernible. Then, by using morphological techniques, the pupil of the eye is found. Finally, using superpixel segmentation, the human eye's iris is discovered.

Iris Segmentation: The texture of the iris becomes distorted because the iris image also includes the other eye elements. Through the use of iris segmentation, these elements can be taken out. Iris inner and outer boundaries, which correlate to the iris/pupil and iris/sclera boundaries, are localized during this phase. These two circles need not always be in perfect alignment.

Normalization: The iris region is transformed to have fixed dimensions during normalization to facilitate comparisons. The stretching of the iris, which is brought on by pupil dilatation due to variable levels of illumination, is the primary cause of the dimensional inconsistencies between representations of the eyes. Despite differences in pupil size between subjects, it makes sure that the irises of various people are all mapped into the same image domain.

Feature Extraction: Images of the iris are typically gray-scaled versions of colour images. This approach extracts features from the Iris Effective Region (IER) that are numerical characterizations of the underlying biometrics once the IER has been detected. The properties of the iris are encoded in 0 and 1 codes.

Template Matching: The encoded iris template is compared to the images of the eye recorded in the database during template matching, and a score that matches is obtained using either the Euclidean distance approach or the Hamming distance approach. Based on the matching score, the outcome is determined.

In section 3, we introduce the related works of different techniques used for biometric privacy. In section 4, we discuss the impact of embedding watermarks on recognition accuracy in iris biometric authentication. Section 5 concludes the paper.

3. Literature survey

3.1 *Face recognition techniques*

Deng et al. [2] presented the ArcFace or Additive Angular Margin loss function, which significantly improves the discriminative ability of feature embeddings trained using Deep Convolution Neural Network (DCNN) for facial recognition. The most extensive studies were used to demonstrate the consistent better performance of the new development. For soft biometric privacy enhancement of face representation, a model based on a neural network, (PFRNet) Privacy-improving Face Representation learning Network was introduced by Bortolato et al. [3] to achieve new developments of numerous face datasets. However, does not incorporate extra forfeiture into the PFRNet performance indicator that would facilitate discrimination using the latent descriptions more accurately. The amount of soft biometric privacy would rise in terms of identification. The 11 commercial face biometric systems' speed and accuracy were evaluated as part of the biometric system evaluation process proposed by Cook et al. [4] and are influenced by demographic parameters. Al-Jarba et al. [5] have suggested a trustworthy and reliable hybrid watermarking method for user authentication in mobile ecosystems that safeguards multimedia data from illegal access and prevents the use of identities or images by anyone other than the rightful owner. Kant et al. [6] have utilized iris and facial biometric features. Instead of keeping the original templates in the database, a watermark image created by embedding a processed iris image is kept there. The dataset lists and the number of facial images matching to each attribute are shown in Table 1. Table 2 lists the datasets in the train-test partitions along with the sample size and subject count.

3.2 *Privacy protection techniques*

In order to tackle gender privacy, Mirjalili et al. [7] adopted the FlowSan technique, which combines different perturbations for the facial image inputs to obfuscate the gender information. The FlowSan method performs better than previous ensemble-based strategies. It excludes soft biometric characteristics. With the help of generative adversarial networks and semi-adversarial network modules, Mirjalili et al. [8] created PrivacyNet, a deep neural network model for adding many attributes of privacy to face images. According to experimental methods carried out by Balakrishnan et al. [9], it is possible to measure algorithmic computer vision bias. The results of the approach could be very different from those of conventional observational investigations. Apart from the ones that are of immediate interest, a wide range of qualities and attribute combinations should be taken into account when studying algorithmic bias. These methods don't take into consideration or remove hidden confounders. Based on the assessment of mutual information, Dahr et al. [10] measured predictability. This method requires training a second network to measure predictability rather than relying on linear separability. The specifications for a Quality Assurance (QA) tool for estimating the correctness of a facial image used for facial recognition were derived by Ortega et al. [11] but are not trustworthy for making forecasts.

Table 1. Overview of datasets

Datasets	Gender		Race		Age groups		
	Male	Female	African-descent	Caucasian	Young	Midle-aged	Old
CelebA	84,434	118,165	11,119	142,225	79,848	91,373	16,337
MORPH	47,057	8,551	42,897	10,736	25,009	26,614	3,985
MUCT	1,844	1,910	1,030	1,480	1,326	1,807	620
RaFD	1,008	600	0	1,608	1,276	332	0
UTK-face	12,582	11,522	4,558	10,222	12,980	6,068	5,056

Table 2. Summary of datasets

Datasets	Train		Test		Excluded
	#Subj#	Samples	#Subj#	Samples	Experiments
CelebA	8,604	150,530	167	2,795	-
MORPH	11,176	45,512	1,968	8,038	-
MUCT	-	-	185	2,508	-
RaFD	-	-	67	1,608	Race
UTK-face	-	-	NA	14,182	Matching

3.3 *Bias mitigation and fairness techniques*

When domains do not share classes, Liang et al. [12] presented two stages disentangle learning approach to identify the difficulty of authentication. To train different domain differences, however, no defined learning techniques are used. Using a huge attribute classifier, Terhörst et al. [13] age and gender estimate model was suggested. It included a novel consistent metric evaluating the dependence in the algorithm's projection. However, it resulted in a face recognition system with poor quality and few patterns. A new approach to unsupervised face quality evaluation built on a face recognition model that was trained using dropout was developed by Terhörst et al. [14]. By assessing the embedding fluctuations created by random subnetworks of the face recognition model, the representation robustness of a sample and, as a result, the quality of the sample, are evaluated. However, it only serves as an identification method and has privacy issues. Terhörst et al. [15] proposed PE-MIU, a training-free, privacy-preserving face recognition technique based on minimum information units. But takes a long time to compare. Generic facial recognition methods, as described by Yin et al. [16], experience classifier bias as a result of uneven training data. Unbalanced issues with Under Represented (UR) classes are explored in a unique feature transfer recognition training. Not suited for feature transfers for applications like UR natural species recognition. Analysis of the data saved in face templates by Terhörst et al. [17] for efficient bias mitigation and privacy preservation.

3.4 *Recognition system improvement and attacks*

Terhörst et al. [18] improved facial privacy templates using the incremental variable elimination approach. A novel fair score normalization strategy was put forth by Terhörst et al. [19] to reduce bias from recognition systems. Not only facial biometrics but also improves the performance of recognition as a whole In order to maintain biometric performance, features of the original face recognition systems must be preserved using privacy-enhancing face recognition techniques, according to Osorio-Roig et al. [20]. With the very minimum of requirements, a black box method and a small set of arbitrary facial images for which an attack was suggested and could be implemented offline are both easily accessible. Excludes any privacy protection. Capable of possible assaults. Hybrid Adaptive Fusion (HAF) (Type-A & Type-B) algorithm was devised and evaluated against other algorithms by Prabhu et al. [21]. Great speed and high-edge precision have been shown to surpass current methods. However, it struggles to perform effectively when compared to more sophisticated algorithms, such as deep learning algorithms.

3.5 *Iris recognition techniques*

Thabit et al. [22] presented a novel watermarking-based tampering reveal technique in the transform domain. To choose and isolate the iris region, the Interactive Segmentation technique (ISA) is used. The Slantlet transform coefficients are encoded with authentication bits from the Iris Region (IR) to cover the remaining area of the iris image, known as the Non-Iris Region (NIR). According to Najafia et al. [23], a safe watermarking technique is created using a combination of Sharp Frequency Localized Contour Let Transform (SFLCT) and Singular Value Decomposition (SVD). Because of the beneficial characteristics of these two transforms, the suggested watermarking technique is improved in order to meet the requirements of watermarking. Because of the colored image layers and the change of applying the SVD on sub-bands, the proposed technique cannot be used on colored images while still maintaining the system's security and optimization. Two fish, the Triple Data Encryption System method and the Least Significant Bits of picture steganography were employed by Abikoye et al. [24] to encrypt and decrypt the iris template before it was saved in a database. Ashraf et al. [25] suggested a recognition system based on the iris and foot that takes into account the iris and foot modalities. Each biometric item's weight meter is determined for hammering archways using haar transformation classifier algorithms, and it is then gradually modified. Barni et al. [26] raised a severe privacy concern over the prospective application of cutting-edge iris recognition technologies on pictures uploaded on social media and websites. Based on the findings obtained, the recommended method can be used as an effective privacy-preserving tool for posting high-resolution facial pictures on social media and websites. Sagar et al. [27] developed an iris recognition system using Zernike Moments (ZM), Vector Reductions (VR), Gabor Filters (GF), and the fusing of performance metrics at the matching level. The Region of Interest (ROI) for the iris is identified via segmentation. To extract features from the ROI of the iris, GF and ZM are used. The number of feature vectors for a single person is aggregated into a single vector using the VR averaging technique in order to conserve memory and expedite matching. The performance parameters produced from GF and ZM are merged at the matching level to improve the biometric system's performance. Terhörst et al. [28] analyze the data that is recorded in biometric face embeddings in further detail. By examining the predictability of 73 different soft biometric parameters from popular face embedding over a range of difficulty levels. The Exclusive OR (XOR) function was employed by Wickramaarachchi et al. [29] to guarantee the system's anonymity. The suggested strategy retains neutral outcomes and continues to be efficient in terms of privacy. However, it fails when used with distorted and poor-quality iris images. Distorted iris images are caused by both internal and external events, including hereditary abnormalities and accidents. Image Future (IF), Normalized Cross-Correlation (NCC), and Peak Signal-to-Noise Ratio (PSNR) parameters were evaluated using the gain factor tuning criteria by Hassan et al. [30].

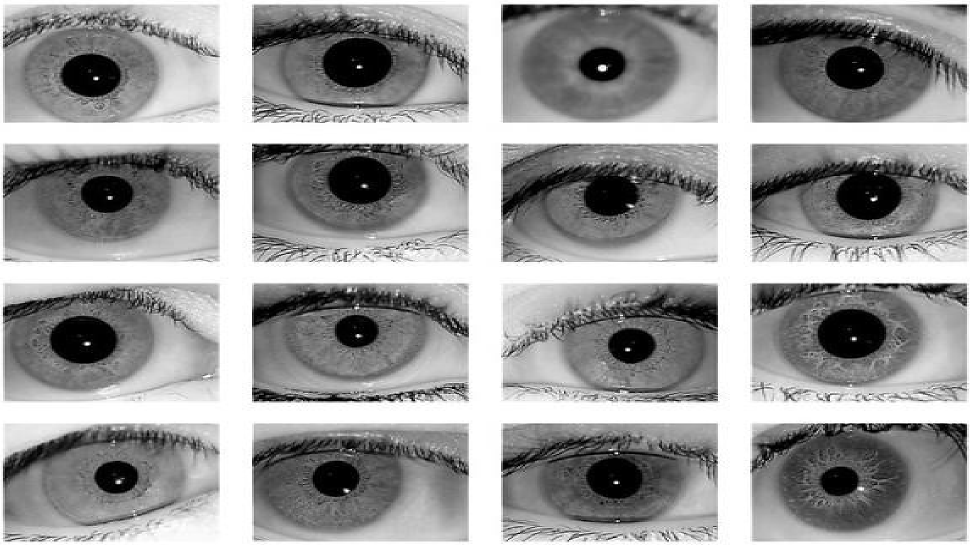

Figure 3. 16 Sample images from Indian Institute of Technology Delhi (IITD) iris dataset

Table 3. Features derived from the Gabor wavelet and the discrete wavelet transform

Technique	No. of features	Training %	Testing %	RR%
GW	48	20	80	57.2321
		40	60	74.5536
		60	40	86.1607
		80	20	91.3393
DWT	40	20	80	67.0536
		40	60	83.5714
		60	40	90.8036
		80	20	95.8929

4. Discussion

In order to determine the impact of embedding watermarks on recognition accuracy in iris biometric authentication, the IITD V1.0 dataset [31] is used in this study to understand the trade-offs between watermarking strength and recognition accuracy and assist in the selection and optimization of watermarking techniques that strike the right balance between security and performance. The IITD V1.0 dataset contains iris images from 224 classes. Bitmap (*.bmp) is the format utilized by all of the images. 48 female and 176 male subjects, ranging in age from 14 to 55, make up the dataset. All of the images in the database were captured indoors using the Near-Infrared (NIR) wavelength, and they total 1,120 images with a resolution of 320 × 240 pixels, resulting in 224 classes and five sample iris images in each. From the IITD Iris dataset, Figure 3 displays 16 samples of images. With all other images balanced, a single test image for each iris is analyzed. Table 3 shows the relationship between various training/testing ratios and recognition rates. The Recognition Rate (RR) for different ratios of training/testing for IITD databases was determined using the Gabor Wavelet (GW) and Discrete Wavelet Transform (DWT) techniques. The performance assessment on IITD with iris samples is shown in

Figure 4. Recognition accuracy can be quantitatively assessed using evaluation metrics such as the False Acceptance Rate (FAR) and False Rejection Rate (FRR).

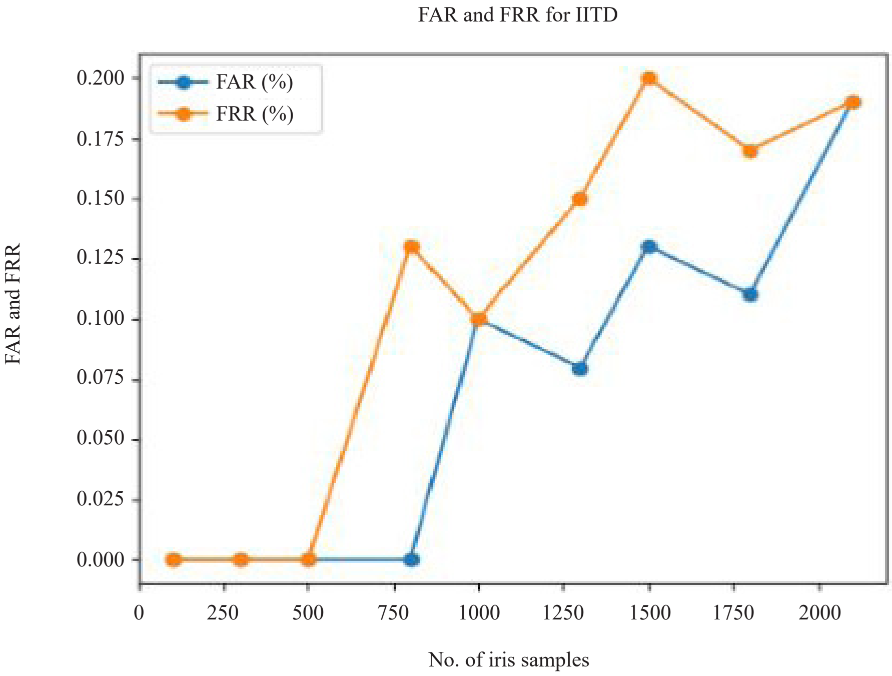

Figure 4. Varying threshold plot of FAR and FRR iris images of IITD dataset

5. Conclusion

In conclusion, this survey has provided a comprehensive overview of embedding iris biometric watermarking techniques for user authentication. The reviewed techniques in the spatial and transform domains offer various trade-offs between embedding capacity, robustness, and recognition accuracy. Comparative evaluations between watermarked and watermark-free systems are essential to understanding the impact of embedding watermarks on recognition accuracy. Advancements in addressing challenges and ethical considerations will further enhance the security and integrity of iris biometric authentication systems. Overall, embedding iris biometric watermarking holds promise for improving user authentication, and continued research is needed to advance its effectiveness in real-world applications.

Conflict of interest

The authors declare no conflict of interest.

References

[1] Kumar A, Dwivedi A, Dutta MK. A zero watermarking approach for biometric image security. In *2020 International Conference on Contemporary Computing and Applications Lucknow*. India: IEEE; 2020. p. 53-58.

[2] Deng J, Guo J, Xue N, Zafeiriou S. Arcface: Additive angular margin loss for deep face recognition. In *2019 Conference on Computer Vision and Pattern Recognition*. Long Beach, California: IEEE; 2019. p. 4690-4699.

[3] Bortolato B, Ivanovska M, Rot P, Križaj J, Terhörst P, Damer N, et al. Learning privacy-enhancing face representations through feature disentanglement. In *2020 15th IEEE International Conference on Automatic Face*

and Gesture Recognition. Buenos Aires, Argentina: IEEE; 2020. p. 495-502.

[4] Cook CM, Howard JJ, Sirotin YB, Tipton JL, Vemury AR. Demographic effects in facial recognition and their dependence on image acquisition: An evaluation of eleven commercial systems. *IEEE Transactions on Biometrics, Behavior, and Identity Science*. 2019; 1(1): 32-41.

[5] Al-Jarba F, Al-Khathami M. A Watermarking technique for user authentication based on a combination of face image and device identity in a mobile ecosystem. *International Journal of Computer Science & Network Security*. 2021; 21(9): 303-316.

[6] Kant C, Chaudhary S. A watermarking based approach for protection of templates in multimodal biometric system. *Procedia Computer Science.* 2020; 167: 932-941.

[7] Mirjalili V, Raschka S, Ross A. Flowsan: Privacy-enhancing semi-adversarial networks to confound arbitrary face-based gender classifiers. *IEEE Access*. 2019; 7: 99735-99745.

[8] Mirjalili V, Raschka S, Ross A. PrivacyNet: Semi-adversarial networks for multi-attribute face privacy. *IEEE Transactions on Image Processing*. 2020; 29: 9400-9412.

[9] Balakrishnan G, Xiong Y, Xia W, Perona P. Towards causal benchmarking of bias in face analysis algorithms. In *Deep Learning-Based Face Analytics*. 2021. p. 327-359.

[10] Dhar P, Bansal A, Castillo CD, Gleason J, Phillips PJ, Chellappa R. How are attributes expressed in face DCNNs? In *2020 15th IEEE International Conference on Automatic Face and Gesture Recognition*. Buenos Aires, Argentina: IEEE; 2020. p. 85-92.

[11] Hernandez-Ortega J, Galbally J, Fierrez J, Haraksim R, Beslay L. Faceqnet: Quality assessment for face recognition based on deep learning. In *2019 International Conference on Biometrics*. Crete, Greece: IEEE; 2019. p. 1-8.

[12] Liang J, Cao Y, Zhang C, Chang S, Bai K, Xu Z. Additive adversarial learning for unbiased authentication. In *2019 Conference on Computer Vision and Pattern Recognition*. Long Beach, California: IEEE; 2019. p. 11428-11437.

[13] Terhörst P, Huber M, Kolf JN, Damer N, Kirchbuchner F, Kuijper A. Multi-algorithmic fusion for reliable age and gender estimation from face images. In *2019 22th International Conference on Information Fusion*. Ottawa, ON, Canada: IEEE; 2019. p. 1-8.

[14] Terhorst P, Kolf JN, Damer N, Kirchbuchner F, Kuijper A. SER-FIQ: Unsupervised estimation of face image quality based on stochastic embedding robustness. In *2020 Conference on Computer Vision and Pattern Recognition*. Long Beach: IEEE; 2020. p. 5651-5660.

[15] Terhörst P, Riehl K, Damer N, Rot P, Bortolato B, Kirchbuchner F, et al. PE-MIU: A training-free privacy-enhancing face recognition approach based on minimum information units. *IEEE Access*. 2020; 8: 93635-93647.

[16] Yin X, Yu X, Sohn K, Liu X, Chandraker M. Feature transfer learning for face recognition with under-represented data. In *2019 Conference on Computer Vision and Pattern Recognition*. Long Beach: IEEE; 2019. p. 5704-5713.

[17] Terhörst P, Fährmann D, Damer N, Kirchbuchner F, Kuijper A. Beyond identity: What information is stored in Biometric face templates? In *2020 IEEE International Joint Conference on Biometrics*. Houston, TX, USA: IEEE; 2020. p. 1-10.

[18] Terhörst P, Damer N, Kirchbuchner F, Kuijper A. Suppressing gender and age in face templates using incremental variable elimination. In *2019 International Conference on Biometrics*. Crete, Greece: IEEE; 2019. p. 1-8.

[19] Terhörst P, Kolf JN, Damer N, Kirchbuchner F, Kuijper A. Post-comparison mitigation of demographic bias in face recognition using fair score normalization. *Pattern Recognition Letters*. 2020; 140: 332-338.

[20] Osorio-Roig D, Rathgeb C, Drozdowski P, Terhörst P, Štruc V, Busch C. An attack on facial soft-biometric privacy enhancement. *IEEE Transactions on Biometrics, Behavior, and Identity Science*. 2022; 4(2): 263-275.

[21] Prabu S, Lakshmanan M, Mohammed VN. A multimodal authentication for biometric recognition system using intelligent hybrid fusion techniques. *Journal of Medical Systems*. 2019; 43: 1-9.

[22] Thabit R, Ali J, Subhi D. Tampering reveal technique for iris images. *International Journal of Computer Networks and Communications Security*. 2020; 8(6): 46-51.

[23] Najafi E, Loukhaoukha K. Hybrid secure and robust image watermarking scheme based on SVD and sharp frequency localized contourlet transform. *Journal of Information Security and Applications*. 2019; 44: 144-156.

[24] Abikoye OC, Ojo UA, Awotunde JB, Ogundokun RO. A safe and secured iris template using steganography and cryptography. *Multimedia Tools and Applications*. 2020; 79: 23483-23506.

[25] Ashraf S, Saleem S, Ahmed T, Aslam Z, Shuaeeb M. Iris and foot based sustainable biometric identification approach. In *2020 Telecommunications and Computer Networks*. International Conference on Software. Split, Croatia: IEEE; 2020. p. 1-6.

[26] Barni M, Labati RD, Genovese A, Piuri V, Scotti F. Iris deidentification with high visual realism for privacy

protection on websites and social networks. *IEEE Access*. 2021; 9: 131995-132010.

[27] Ganapath Sagar V, Raja KB, Venugopal KR, Suresh Babu K, Madiwala CT. Iris recognition system based on ZM, GF, VR and matching level fusion. *International Journal of Computational Intelligence Research*. 2017; 13(5): 1307-1331.

[28] Terhörst P, Fährmann D, Damer N, Kirchbuchner F, Kuijper A. On soft-biometric information stored in biometric face embeddings. *IEEE Transactions on Biometrics, Behavior, and Identity Science*. 2021; 3(4): 519-534.

[29] Wickramaarachchi WU, Alhaj YA, Gunesekera A. Effective privacy-preserving iris recognition. In *2019 IEEE 4th International Conference on Image, Vision and Computing*. Xiamen, China: IEEE; 2019. p. 421-426.

[30] Hassan OM, Abdulazeez AM, Mohammed AI, Salih SO, Alih SH, Ahmed FY, et al. An efficient robust color watermarking algorithm based on DWT, DCT, BFO and implementation. In *2021 IEEE 11th International Conference on System Engineering and Technology*. Shah Alam, Malaysia: IEEE; 2021. p. 90-95.

[31] *IIT Delhi Iris Database (Version 1.0)*. Available from: https://www4.comp.polyu.edu.hk/~csajaykr/IITD/Database_Iris.htm [Accessed 5th November 2018].