Iris Recognition from Websites and Social Media: State of the Art and Privacy Concerns

Ruggero Donida Labati, Vincenzo Piuri, Fabio Scotti

Department of Computer Science, Università degli Studi di Milano, Italy

Abstract. Traditional iris recognition systems rely on dedicated sensors, typically using near-infrared illumination, which demand a high degree of user cooperation. Recent studies have demonstrated the feasibility of performing iris recognition on samples captured from uncooperative users in uncontrolled environments, including ocular images cropped from high-resolution facial portraits posted on websites and social media. These advancements are largely driven by novel artificial intelligence techniques and the availability of datasets containing ocular samples collected under non-ideal conditions. Nevertheless, the improved accuracy and robustness of iris recognition methods introduce new challenges related to privacy protection. This chapter examines recent advancements in iris recognition using samples obtained from websites and social media, focusing on algorithms, public datasets, privacy concerns, and potential mitigation strategies.

1 Introduction

The number of deployed biometric systems is continuously growing all over the world in security-oriented and everyday applications. Among other biometric traits, the iris is widely used in high security applications thanks to its high distinctive and lifespan stability. Furthermore, current iris recognition technologies are particularly suitable for identification applications characterized by biometric databases populated by high numbers of individuals, as a result of the simplicity and high speed of the identity comparison algorithms.

Despite the positive characteristics of the biometric trait, traditional iris acquisition procedures come with several limitations. In fact, most of the current iris recognition technologies are based on dedicated acquisition devices. Specifically, they employ near-infrared illumination, require the users to remain still with their eyes open, and use a camera-to-eye distance of approximately 30 cm [1]. The acquisition process is therefore characterized by low usability and can cause false to acquire errors. Furthermore, near-infrared illuminators could be considered as harmful for the health, thus limiting the acceptability of the biometric technologies [2].

A growing number of studies aim to relax the acquisition constraints of current iris recognition systems by utilizing ocular images captured in uncontrolled

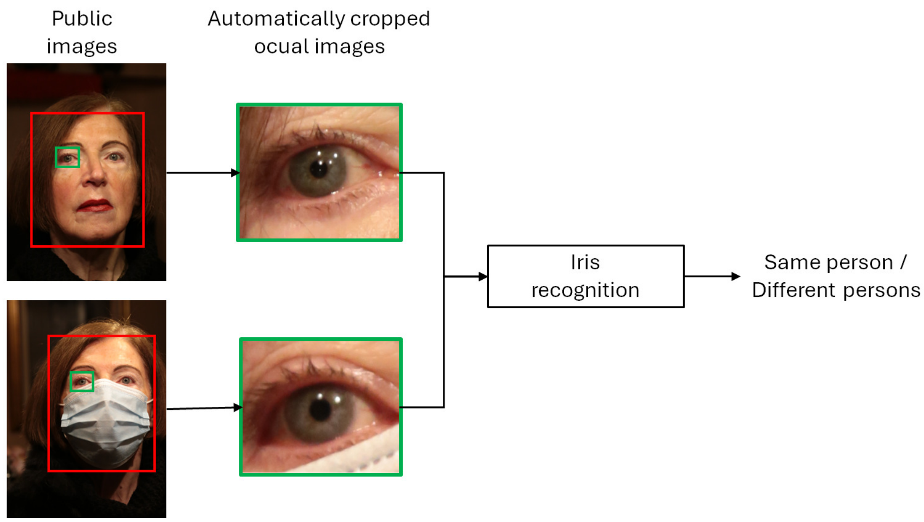


Fig. 1: Computational steps for automatic iris recognition from facial portraits collected from websites and social media.

conditions from uncooperative users. Such images can be obtained using consumer cameras [3] or smartphones [4]. In this context, recent advancements have enabled researchers to explore iris samples acquired from websites and social media for biometric recognition [5].

High-resolution portraits posted on websites and social media often provide a sufficient iris diameter for iris recognition. Furthermore, state-of-the-art face detectors can accurately estimate iris coordinates in facial portraits, enabling the automatic cropping of ocular samples suitable for iris recognition techniques. Figure 2 illustrates the computational steps for automatic iris recognition from facial portraits collected from websites and social media.

Ocular images collected in such conditions often exhibit significant non-idealities. They are captured using various cameras with different focal lengths and from varying distances. Additionally, illumination conditions are frequently suboptimal, and users often display uncooperative behavior.

To effectively process iris samples acquired in uncontrolled and uncooperative conditions, several studies have proposed specialized methods for each stage of the biometric recognition process. These stages include quality assessment, iris segmentation, feature extraction, and matching.

In this context, recent research has largely focused on artificial intelligence [6], which have improved accuracy and robustness against image non-idealities compared to traditional algorithmic techniques. Since training artificial intelligence models requires a large number of samples captured under diverse conditions, research has released dedicated datasets of non-ideal ocular images [5].

The high accuracy achieved by recent iris recognition methods raises potential privacy concerns [7], particularly the possibility of performing biometric recognition without an individual's consent by using images published online [8]. Among the biometric traits visible in portrait images, iris patterns are among the most sensitive for several reasons. First, the iris remains stable throughout a person's lifetime, allowing for individual recognition even when images are taken years apart. Second, while facial recognition methods often struggle to match images captured years apart, iris recognition techniques can still reliably identify individuals over long time intervals. Third, iris recognition can frequently be performed even in cases where face recognition is not possible, such as in the presence of significant occlusions caused by masks or makeup. Therefore, specific strategies for data anonymization [9] are needed to protect privacy for images released in websites and social media.

This chapter focuses on iris recognition from samples collected on websites and social media. Section 2 outlines the main steps of the biometric recognition pipeline, with emphasis on recent advancements based on artificial intelligence. Section 3 provides a brief overview of publicly available datasets. Section 4 discusses privacy concerns and possible countermeasures. Section 5 highlights open research challenges. Finally, Section 6 concludes the chapter.

2 Iris Recognition Technologies

Biometric recognition systems perform two main functions: enrollment and recognition. During enrollment, the system generates an abstract and distinctive representation of biometric data (called template) from an acquired biometric sample and stores it in the system. The recognition phase involves comparing two or more templates. Specifically, the system can perform identity verification, where it compares a fresh template with the one associated with the identity claimed by the user, or identification, where it searches for the identity corresponding to the fresh biometric template within the database.

The iris recognition process can be divided into four main steps: (*i*) quality assessment, (*ii*) segmentation, (*iii*) feature extraction, and (*iv*) matching. Figure 2 presents a schema of the iris recognition process.

The quality assessment step determines whether an acquired ocular image contains sufficient detail to be effectively used in subsequent recognition steps. This step is not implemented in all currently deployed biometric systems. However, it is particularly relevant for iris recognition technologies designed for unconstrained and uncooperative application contexts, where samples may exhibit strong non-idealities, potentially reducing the overall recognition accuracy.

The segmentation step aims to isolate the iris region from the background while also removing occlusions and specular reflections.

The feature extraction step generates a template from the iris texture. During the matching step, the computed template is then compared with one or more templates stored in the biometric database. A matching method typically returns a numerical value representing the similarity or distance between the considered templates. In recent biometric systems based on deep learning, the

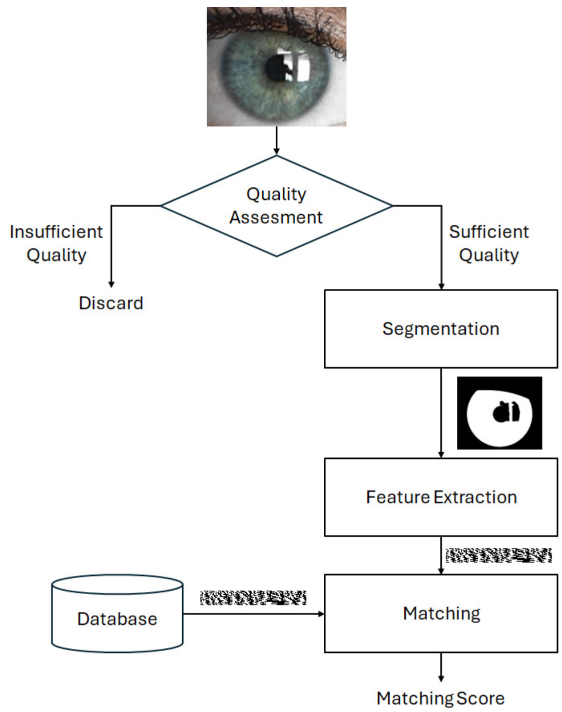


Fig. 2: Schema of the identity verification process.

feature extraction and matching steps can be performed simultaneously by a single deep neural network.

This section presents recent advancements in all steps of the iris recognition process, primarily focusing on artificial intelligence approaches. Specifically, we first discuss quality assessment methods, followed by an analysis of iris segmentation techniques. Finally, we present feature extraction and matching techniques.

2.1 Quality Assessment

Several studies have proposed different approaches for assessing iris image quality, focusing on individual quality parameters, global quality assessment based on hand-crafted features, and deep learning techniques [10].

Approaches that focus on individual quality parameters separately estimate quality scores that describe various non-idealities. In particular, the IREX II Iris Quality Calibration and Evaluation (IQCE) competition, organized by the National Institute of Standards and Technology (NIST) and detailed in [11], assessed the impact of various nonidealities in iris images in near-infrared illumination on system performance. The influencing factors were ranked by relevance, including: usable iris area, iris-pupil contrast, pupil shape, iris-sclera contrast, gaze angle, sharpness, dilation, interlacing, gray-scale spread, iris shape,

Table 1: Factors resulting in non-ideal iris images collected from websites and social media.

Source of nonideality	**Effects**
Acquisition sensor	Low signal-to-noise ratio (SNR) Frame interlacing Poor focus Motion blur
Low cooperation from the user	Strong occlusion Gaze deviation
Uncontrolled distance from the camera	Strong differences in iris radii Differences in illumination conditions
Illumination conditions	Low illumination High illumination and pixel saturation Non-constant illumination Pupil dilation Specular reflections Shadows
Photo editing	Blur Modified colors Artifacts introduced to reduce the red-eye effect
Image compression	Blur Artifacts Modified color tones

iris size, motion blur, and signal-to-noise ratio. The study highlighted that factors associated with illumination, such as iris-pupil contrast, iris-sclera contrast, and gray-scale spread, significantly affect the performance of iris segmentation methods.

Other studies apply fusion strategies to derive a single numerical score from the estimated values [12]. Studies on global quality assessment based on handcrafted features often utilize Feedforward Neural Networks or Support Vector Machines [13]. Deep learning techniques, the most recent advancement in this field, are frequently based on Convolutional Neural Networks (CNNs) [14].

While most studies on iris quality assessment focus on images acquired using iris scanners, some research has explored the quality assessment of iris images captured under uncontrolled conditions and visible light illumination [15]. However, most of these studies consider ocular images collected in simulated non-cooperative conditions or using smartphones.

Iris samples collected from websites and social media frequently exhibit additional non-idealities with respect to other ocular images. Table 1 summarizes the main non-idealities, extending the taxonomy reported in [16] to include the most common issues affecting ocular images captured in more controlled conditions. In particular, uncooperative and uncontrolled acquisition conditions can introduce blur, motion blur, occlusions, and specular reflections. Additionally, post-processing and compression can result in artifacts, color distortions, and secondary blur. As a result, existing quality assessment algorithms, which are typically designed for samples acquired in controlled conditions, may perform poorly when applied to ocular images collected from websites and social media.

To the best of our knowledge, there is only one method specifically designed to assess the quality of iris samples extracted from images collected from websites and social media [17]. This method utilizes different deep neural networks to evaluate the iris image quality, categorizing images in two possible classes: sufficient quality and insufficient quality. Furthermore, this method can be used in three configurations: (*i*) applied directly to ocular images; (*ii*) leveraging information obtained from the iris localization step of the recognition process; (*iii*) leveraging information from both the iris localization and segmentation steps. Additionally, the method is based on deep neural networks with limited computational complexity, ensuring its suitability for deployment on edge devices. The classifiers were validated using a dataset of more than three thousand ocular images labeled by a human expert. Experimental results demonstrated that discarding samples classified as insufficient quality reduced the Equal Error Rate (EER) [18] of a state-of-the-art biometric matcher [19] from 18.5% to 11.8% on the considered dataset.

2.2 Segmentation

Iris segmentation involves computing a binary mask that identifies the iris region within an ocular image [20]. This process includes detecting both the inner and outer iris boundaries and estimating the regions of the iris occluded by eyelids, eyelashes, hair, eyeglasses, and reflections.

Most iris boundary segmentation methods have been developed for images captured using dedicated iris scanners and approximate the contours using predefined geometric shapes, such as circles or ellipses. A widely adopted method, introduced in [21], employs an integro-differential operator to locate circular contours by maximizing the intensity gradient in the radial direction. The same method adapts its integral path to an arcuate shape to detect eyelid boundaries. Several variants of this technique have been proposed in the literature, including those designed to detect elliptical shapes, as in [22]. Another popular approach that models the iris boundaries as circular shapes is based on the Hough transform [23].

Some methods describe the iris boundaries using more flexible models. These include active contours [24], approximations using a limited number of Fourier coefficients [25], and RANSAC-based algorithms [16]. Several of these techniques have been specifically developed for ocular images captured under natural light and in unconstrained and uncooperative acquisition conditions [26].

Recent advances in deep learning have enabled the development of more accurate and robust segmentation techniques that extract the iris texture directly from ocular images without imposing constraints on the boundary shape. Commonly used models include encoder-decoder architectures [27], U-Net-based networks [28], and Mask-RCNN [29]. To the best of our knowledge, while some of these methods have been designed for images captured in natural lighting and under uncooperative conditions [30], none have been specifically trained on images sourced from websites or social media platforms.

Although iris segmentation methods based on deep learning can achieve high accuracy even on images acquired from online sources [5], they may struggle to segment effectively reflection regions common in such contexts. The method proposed in [31] presents a modified U-Net architecture specifically designed to segment reflection areas in ocular images obtained from websites and social media. Results demonstrate that incorporating reflection segmentation significantly enhances the performance of state-of-the-art iris segmentation techniques.

2.3 Feature Extraction and Matching

Algorithmic approaches are typically designed for samples acquired using iris scanners but are frequently applied to ocular images captured under natural light conditions. One of the most widely used techniques is based on a template called IrisCode [21]. During feature extraction, this approach first computes a representation of the iris texture that is robust to scale variations and pupil dilation, known as the Rubber Sheet Model. Subsequently, a Gabor Wavelet is applied, and the real and imaginary responses to the filters are quantized into a binary representation based on zero-crossings. The matching step calculates the matching score as the Hamming distance between the non-occluded regions of two IrisCodes. To increase the robustness to possible eye rotations, one of the IrisCodes is shifted multiple times, and the final result corresponds to the lowest Hamming distance obtained.

Similar to IrisCode, most feature extraction approaches in the literature, algorithmic as well as based on artificial intelligence, derive distinctive iris texture information from representations based on the Rubber Sheet Model.

Other algorithmic approaches rely on different types of features, such as the Scale-Invariant Feature Transform (SIFT) [32] and Quadratic Spline Wavelet (QSV) [33].

There are three main types of feature extraction and matching strategies based on artificial intelligence techniques: (*i*) methods based on handcrafted features, (*ii*) methods based on softmax classifiers, and (*iii*)) methods based on similarity networks.

Methods based on handcrafted features use well-established regressors and classifiers, such as Feedforward Neural Networks and Support Vector Machines. For example, the matcher proposed in [34] is based on Support Vector Machines, while the feature extractor presented in [35] uses features optimized through a machine learning technique.

Methods based on softmax classifiers are particularly suitable for identification tasks. These methods employ multi-class classifiers, where each class corresponds to a distinct identity. Various deep neural network architectures, such as ResNet [36] and EfficientNet [37], can be utilized in these approaches.

Methods based on similarity networks often involve heterogeneous deep neural network models and can be divided into two categories based on their training approach: pairwise loss and triplet loss. In pairwise loss methods, a deep neural network takes two input samples and directly computes a similarity score [38].

The network is trained to minimize the dissimilarity for genuine pairs and maximize it for impostor pairs. Triplet loss, which is generally more robust to unbalanced datasets, involves a trio of images: an anchor image, a positive image (same identity as the anchor), and a negative image (different identity) [39]. The network is trained to reduce the similarity distance between the anchor and the positive image, while increasing it between the anchor and the negative image. Most methods use CNN-based models [40], although there are also studies exploring Differentiable Neural Architecture Search [41].

Some studies in the literature have also investigated deep neural networks that do not rely on the Rubber Sheet Model and do not require a preliminary iris segmentation step [42].

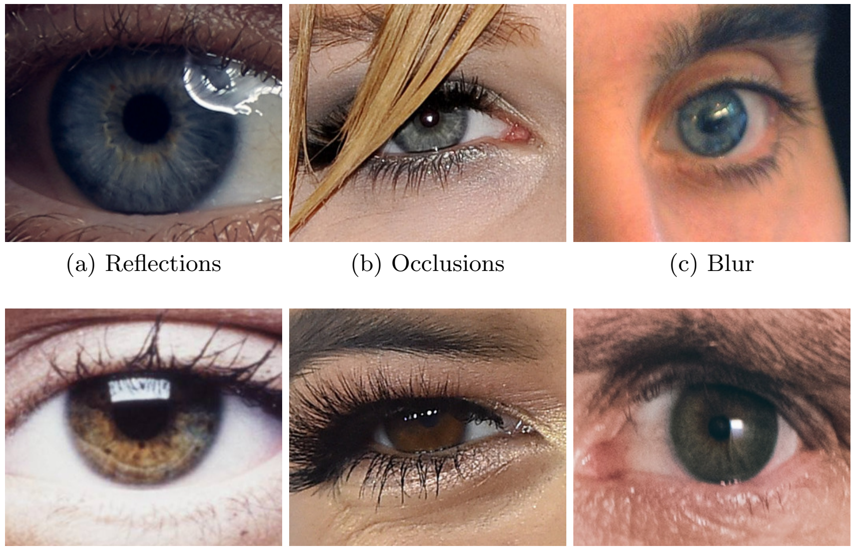
To the best of our knowledge, there are currently no feature extraction and matching methods specifically designed for iris samples acquired from websites and social media. However, state-of-the-art techniques developed for ocular images captured in uncontrolled and uncooperative conditions have shown promising results on such samples [5].

3 Datasets

To design and evaluate the performance of iris recognition methods, it is essential to use large datasets that exhibit the non-idealities characteristic of the target application context. In particular, recent deep learning approaches require datasets with significantly more samples than those needed by traditional algorithmic methods. These datasets should ideally encompass the full range of possible non-idealities to enable the development of robust biometric recognition systems.

To the best of our knowledge, the only public dataset of ocular images collected from websites and social media is I-SOCIAL-DB [5]. It includes ocular images captured from uncooperative subjects under varying lighting conditions and in uncontrolled environments. The dataset comprises $3,286$ ocular images, extracted from $1,643$ high-resolution facial portraits belonging to 400 individuals. Each ocular image is accompanied by a segmentation mask, manually annotated by a human expert, which can serve as ground truth for developing segmentation methods or as reference data for designing feature extraction and matching techniques.

Figure 2 presents examples of ocular images from I-SOCIAL-DB. Although the samples exhibit notable non-idealities, such as reflections, occlusions, and blur, the image resolution and visibility of distinctive iris features are sufficient to enable biometric recognition in a large number of cases. For example, the evaluation reported in [5] shows that state-of-the-art methods developed for iris scanner images can still achieve promising identity verification accuracy, with an EER of 18.97%. Although an EER of 18.97% might appear relatively high for security-critical applications, this figure reflects an overall average across all samples in the dataset. In practice, certain individuals with more distinct iris details, especially in cases where visible features are clearer, can be recognized



(a) Reflections (b) Occlusions (c) Blur

(d) Reflections (e) Occlusions (f) Blur

Table 2: Examples of ocular images from I-SOCIAL-DB. Although the samples exhibit notable non-idealities, such as reflections, occlusions, and blur, the image resolution and visibility of distinctive iris features are sufficient to enable biometric recognition in a large number of cases.

with higher accuracy. Conversely, subjects exhibiting faint iris patterns or heavy occlusions drive the EER upward. Consequently, while 18.97% EER is not yet suitable for robust security usage, recent improvements in image quality assessment, segmentation, and feature extraction techniques are steadily reducing these error levels. As demonstrated in our experiments on I-SOCIAL-DB [17], removing low-quality samples or leveraging more detailed iris regions can significantly enhance the accuracy. Over time, such advancements may enable iris recognition from web-sourced images to achieve error rates closer to those of dedicated IR-based systems, ultimately becoming more viable for real-world security applications.

Since the sample size of I-SOCIAL-DB may be insufficient for training the latest and most computationally intensive deep neural networks, additional datasets containing ocular images captured under natural lighting and varying conditions can be leveraged to design and evaluate methods tailored for images sourced from websites and social media.

To facilitate a concise comparative analysis of existing public datasets that include ocular images acquired in visible light and under relaxed acquisition constraints, Table 3 summarizes the primary characteristics of several widely used datasets. Specifically, it includes MobBio [43], VISOB [43], MICHE [4], UBIRIS v2 [3], and I-SOCIAL-DB. The table reports key attributes such as the

Table 3: Comparison between public datasets of ocular images acquired in visible light conditions and with relaxed acquisition constraints.

Dataset	Samples	Individuals	Acquisition	Distance	User	Masks
MobBio [44]	800 single eye images	100	Asus Eee Pad Transformer TE300T Tablet	Constant, close to the camera	Cooperative users	Yes
VISOB [43]	158,136 single eye images	550	3 smartphones (anterior camera)	Constant, close to the camera	The user captures a selfie image	No
MICHE [4]	3,732 single eye images	92	3 smartphones (anterior and posterior cameras)	Inconstant, close to the camera	Cooperative users	Partially
UBIRIS v2 [3]	11,102 single eye images	261	Canon Eos 5D	Inconstant, from 3 m to 10 m	The user walks looking at the camera	Partially
I-SOCIAL-DB [5]	3,286 single eye images	400	Websites and social media	Heterogeneous, unknown	Uncooperative users	Yes

total number of samples, number of subjects, acquisition devices, availability of segmentation masks, and a brief overview of the acquisition conditions.

As shown in Table 3, MobBio and VISOB reflect relatively controlled acquisition environments, where subjects are positioned close to the camera and lighting conditions are consistent. MICHE includes images captured using mobile devices, offering more variability in device quality and usage. In contrast, datasets such as UBIRIS v2 and I-SOCIAL-DB reflect greater diversity in capture conditions, including on-the-move acquisitions. Notably, only MobBio and I-SOCIAL-DB provide binary segmentation masks manually annotated by human experts for each ocular image, which represent a valuable resource for realizing accurate and robust segmentation algorithms.

Overall, Table 3 underscores that while each dataset presents specific strengths and application scenarios, the scarcity of large-scale, fully annotated image collections captured in unconstrained environments remains a key bottleneck for advancing the field.

4 Privacy Issues and Mitigation Strategies

Among the various biometric traits visible in images shared on websites and social media, the iris stands out as one of the most sensitive for several compelling reasons:

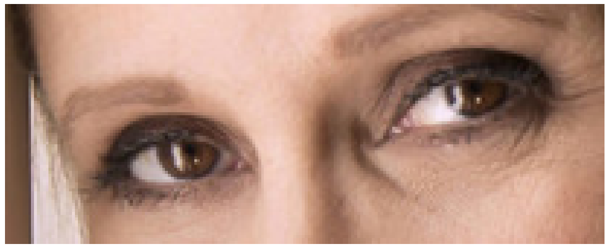
1. The iris pattern remains stable over an individual's lifetime, enabling accurate recognition even when images are captured years apart [20]. Unlike facial recognition, which often struggles with images taken over long time intervals, iris-based recognition maintains a high level of reliability.

2. The likelihood of two individuals having iris patterns similar enough to be mistakenly identified as the same person is extremely low, allowing for high-confidence identification even within very large image databases [45].
3. Iris recognition remains effective in scenarios where face and periocular recognition systems fail, such as in the presence of heavy makeup, occlusions, extreme head poses, or exaggerated facial expressions [46].
4. There is growing public concern over the unauthorized use of biometric traits. In particular, traits typically acquired in a cooperative setting, such as the iris or fingerprint, are often considered particularly sensitive due to their widespread use in critical applications, including government identification systems.

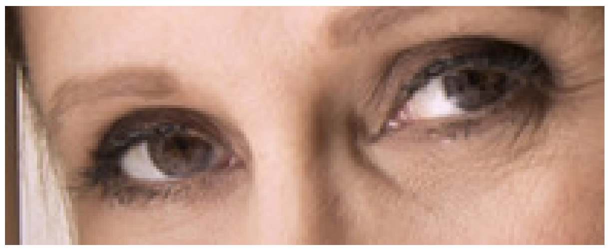
The works presented in [5,8] have demonstrated the feasibility of iris recognition from face portrait images uploaded on websites and social media. For example, [8] showed that a widely used iris recognition approach, originally designed for samples acquired using iris scanners [21], can successfully identify individuals with high certainty in more than 25% of the samples from I-SOCIAL-DB. Methods specifically designed for non-ideal samples achieved even higher accuracy [5].

Protecting the distinctive characteristics of the iris in images uploaded online remains an ongoing research challenge requiring specific data anonymization strategies [47]. To the best of our knowledge, only four studies have addressed the topic of iris protection. The work in [48] focuses on detecting the eye and scrambling the region using rectangular patterns. The study in [49] applies a cryptographic method designed for JPEG 2000 images, which encrypts rectified iris images obtained through a Rubber Sheet Model [21]. The approach in [50] generates visually realistic ocular regions for inclusion in face portraits to inpaint closed eyes. However, this technique is limited to low-resolution images, which are unsuitable for iris recognition. It does not generate detailed iris textures and entirely replaces the eye and eyelash regions to modify the original facial expression. The work in [8] analyzed privacy risks associated with images collected from websites and social media, proposing a privacy protection method that substitutes the original iris textures in portrait images with synthetic textures that are both high-resolution and visually plausible. Specifically, this iris de-identification method can operate in various configurations by using different algorithms to generate synthetic iris textures. It involves extracting the iris region from a high-resolution face image, generating a synthetic iris texture, and inserting the synthetic iris into the original image. The synthetic texture is generated using a Generative Adversarial Network and preserves the original eye color to achieve realistic results.

Figure 4 shows an example of results obtained by the iris anonymization presented in [8]. This example shows that the anonymized image presents the original face characteristics, while synthetically created iris textures present visual realism.



(a) Detail from the original face image



(b) Detail from the anonymized face image

Table 4: Examples of results obtained by the method for protecting the iris anonymization presented in [8]. The anonymized face image presents the original face characteristics, while synthetically created iris textures present visual realism.

5 Open Problems

Iris recognition from ocular images collected from websites and social media is still in its infancy. Although studies in the literature have shown promising results, numerous open challenges should be addressed by researchers. These challenges can broadly be categorized into three main areas: (*i*) improving the accuracy of iris recognition technologies for samples acquired in non-ideal conditions, (*ii*) creating novel datasets, and (*iii*) developing privacy protection techniques to safeguard individuals from unauthorized biometric recognition.

Regarding the first category, new methods must be developed to enhance the accuracy and robustness of each stage in the biometric recognition pipeline.

- *Quality Assessment*: It is essential to analyze the impact of each non-ideality found in ocular images from websites and social media, as many of these are not typically present in other acquisition settings. Automatic detection methods for identifying each type of non-ideality would be particularly useful for distinguishing between images suitable for biometric processing and those of insufficient quality. Additionally, insights gained from analyzing individual non-idealities could be leveraged to design advanced image enhancement algorithms, ultimately improving recognition performance by increasing the visibility of the distinctive iris texture.

– *Iris Segmentation*: While recent methods based on deep neural networks have achieved impressive performance on iris images acquired under controlled conditions, specific studies targeting ocular images collected from websites and social media are still needed. These efforts should focus on improving segmentation robustness under challenging lighting conditions, including environments with multiple and unknown light sources.
– *Feature Extraction and Matching*: A major challenge in iris recognition from online images is the limited visibility of the iris pattern, especially in dark eyes captured under visible light. Although deep learning approaches have enhanced the robustness of traditional feature extraction and matching techniques, further research is needed to achieve reliability and accuracy on par with more mature biometric technologies. In this context, novel image enhancement strategies could also contribute significantly.

Considering the second category of challenges, the main open challenge is the lack of sufficient data for developing robust and accurate processing methods based on the latest, computationally intensive deep learning strategies. In this context, future research should prioritize the creation of novel datasets, along with the development of new benchmark protocols that capture the full spectrum of real-world operating conditions.

For the third category of challenges, researchers should seek to deepen the understanding of the privacy implications associated with the release of high-resolution facial images on websites and social media. For example, the impact of recent biometric technologies based on deep neural networks has not yet been thoroughly evaluated in this context. Additionally, future research should focus on developing privacy-preserving approaches applicable both to biometric samples and to biometric templates. Sample protection methods should aim to safeguard or anonymize iris textures in portrait images, making it more difficult to perform unauthorized biometric recognition. In contrast, template protection techniques for data collected from websites and social media should enhance the privacy and security of biometric systems by being robust to the significant non-idealities affecting the iris samples.

6 Conclusion

The iris is a widely-used biometric trait in highecurity applications due to its high distinctiveness and lifelong stability. Recent studies have demonstrated the feasibility of performing iris recognition using high-resolution facial images collected from websites and social media.

This chapter presented a literature review on iris recognition from samples collected in such contexts, focusing both on technological advancements and on the analysis of privacy implications and potential countermeasures.

While deep learning strategies have shown promising performance in this domain, several technological challenges remain. These include improving the accuracy and robustness of biometric recognition systems when processing iris samples acquired under non-ideal, unconstrained conditions. Furthermore, researchers should create novel datasets composed of many images representing diverse non-idealities. Additionally, a more comprehensive analysis of privacy risks, along with the development of novel privacy-preserving strategies, is essential to ensure the safe and ethical use of biometric technologies in online environments.

7 Acknowledgments

This work was supported in part by the EC under projects EdgeAI (101097300) and GLACIATION (101070141), and by project SERICS (PE00000014) under the MUR NRRP funded by the EU - NGEU. Project EdgeAI is supported by the Chips Joint Undertaking and its members including top-up funding by Austria, Belgium, France, Greece, Italy, Latvia, Netherlands, and Norway under grant agreement No. 101097300. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union, the Chips Joint Undertaking, or the Italian MUR. Neither the European Union, nor the granting authority, nor Italian MUR can be held responsible for them.

References

1. D. Ackerman, "Optics of iris imaging systems," in *Handbook of Iris Recognition*, K. W. Bowyer and M. J. Burge, Eds. London: Springer London, 2016, pp. 63–88.
2. H. Proença, "Unconstrained iris recognition in visible wavelengths," in *Handbook of Iris Recognition*, K. W. Bowyer and M. J. Burge, Eds. London: Springer London, 2016, pp. 321–358.
3. H. Proenca, S. Filipe, R. Santos, J. Oliveira, and L. A. Alexandre, "The UBIRIS.v2: A database of visible wavelength iris images captured on-the-move and at-a-distance," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 32, no. 8, pp. 1529–1535, 2010.
4. M. De Marsico, M. Nappi, D. Riccio, and H. Wechsler, "Mobile iris challenge evaluation (miche)-i, biometric iris dataset and protocols," *Pattern Recognition Letters*, vol. 57, pp. 17–23, 2015, mobile Iris CHallenge Evaluation part I (MICHE I).
5. R. Donida Labati, A. Genovese, V. Piuri, F. Scotti, and S. Vishwakarma, "I-SOCIAL-DB: A labeled database of images collected from websites and social media for iris recognition," *Image and Vision Computing*, vol. 105, p. 104058, 2021.
6. K. Nguyen, H. Proença, and F. Alonso-Fernandez, "Deep learning for iris recognition: A survey," *ACM Comput. Surv.*, vol. 56, no. 9, Apr. 2024.
7. V. Ciriani, S. De Capitani di Vimercati, S. Foresti, and P. Samarati, "Theory of privacy and anonymity," in *Algorithms and Theory of Computation Handbook (2nd edition)*, M. Atallah and M. Blanton, Eds. CRC Press, 2009.
8. M. Barni, R. Donida Labati, A. Genovese, V. Piuri, and F. Scotti, "Iris deidentification with high visual realism for privacy protection on websites and social networks," *IEEE Access*, vol. 9, pp. 131 995–132 010, 2021.

9. B. Moriarty, C.-F. Chen, S. Hu, S. Moran, M. Pistoia, V. Piuri, and P. Samarati, "Utility-preserving biometric information anonymization," in *Proc. of the 27th European Symposium on Research in Computer Security (ESORICS 2022)*, Copenhagen, Denmark, September 2022.
10. N. A. Schmid, "Iris image quality," in *Encyclopedia of Biometrics*, S. Z. Li and A. Jain, Eds. Boston, MA: Springer US, 2009, pp. 801–805.
11. E. Tabassi, P. Grother, and W. Salamon, "Iris quality calibration and evaluation (IQCE): Performance of iris image quality assessement and algorithms," National Institute of Standards and Technology (NIST), Tech. Rep., 2011.
12. H. Proença, "Quality assessment of degraded iris images acquired in the visible wavelength," *IEEE Trans. on Information Forensics and Security*, vol. 6, no. 1, pp. 82–95, 2010.
13. M. Eskandari and O. Sharifi, "Optimum scheme selection for face–iris biometric," *IET Biometrics*, vol. 6, pp. 334–341, 2017.
14. E. Jalilian, H. Hofbauer, and A. Uhl, "Iris image compression using deep convolutional neural networks," *Sensors*, vol. 22, no. 7, p. 2698, 2022.
15. M. Jenadeleh, M. Pedersen, and D. Saupe, "Realtime quality assessment of iris biometrics under visible light," in *Proc. of the 2018 IEEE/CVF Conf. on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 2018, pp. 556–55 609.
16. R. Donida Labati, E. Muñoz, V. Piuri, A. Ross, and F. Scotti, "Non-ideal iris segmentation using polar spline ransac and illumination compensation," *Computer Vision and Image Understanding*, vol. 188, p. 102787, 2019.
17. N. Fakhraei, R. Donida Labati, V. Piuri, and F. Scotti, "Deep learning-based iris quality assessment for images sourced from websites and social media," in *Proc. of the IEEE Int. Conf. on Computational Intelligence and Virtual Environments for Measurement Systems and Applications*, 2025.
18. A. K. Jain, P. Flynn, and A. A. Ross, *Handbook of Biometrics*, 1st ed. Springer Publishing Company, Incorporated, 2010.
19. C. Rathgeb, A. Uhl, P. Wild, and H. Hofbauer, "Design decisions for an iris recognition sdk," in *Handbook of Iris Recognition*, second edition ed., ser. Advances in Computer Vision and Pattern Recognition, K. Bowyer and M. J. Burge, Eds. Springer, 2016.
20. R. Donida Labati, A. Genovese, V. Piuri, and F. Scotti, *Iris Segmentation: State of the Art and Innovative Methods.* Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 151–182.
21. J. Daugman, "How iris recognition works," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, pp. 21–30, 2002.
22. M. Shamsi and A. Kenari, "Iris boundary detection using an ellipse integro differential method," in *Proc. 2nd Int. Conf. Comput. and Knowledge Eng.*, October 2012, pp. 1–5.
23. R. P. Wildes, "Iris recognition: An emerging biometric technology," *Proc. IEEE*, vol. 85, pp. 1348–1363, 1997.
24. S. Shah and A. Ross, "Iris segmentation using geodesic active contours," *IEEE Trans. Inf. Forensics Security*, vol. 4, pp. 824–836, December 2009.
25. J. Daugman, "New methods in iris recognition," *IEEE Trans. Syst., Man, Cybern., B, Cybern.*, vol. 37, pp. 1167–1175, October 2007.
26. R. Donida Labati and F. Scotti, "Noisy iris segmentation with boundary regularization and reflections removal," *Image Vision Computing*, vol. 28, pp. 270–277, February 2010.

27. D. Kerrigan, M. Trokielewicz, A. Czajka, and K. W. Bowyer, "Iris recognition with image segmentation employing retrained off-the-shelf deep neural networks," in *Proc. of the 2019 Int. Conf. on Biometrics (ICB)*, 2019, pp. 1–7.
28. C. Wang, J. Muhammad, Y. Wang, Z. He, and Z. Sun, "Towards complete and accurate iris segmentation using deep multi-task attention network for non-cooperative iris recognition," *IEEE Trans. on Information Forensics and Security*, vol. 15, pp. 2944–2959, 2020.
29. A. Kuehlkamp, A. Boyd, A. Czajka, K. Bowyer, P. Flynn, D. Chute, and E. Benjamin, "Interpretable deep learning-based forensic iris segmentation and recognition," in *Proc. of the 2022 IEEE/CVF Winter Conf. on Applications of Computer Vision Workshops (WACVW)*, 2022, pp. 359–368.
30. T. Schlett, C. Rathgeb, and C. Busch, "Multi-spectral iris segmentation in visible wavelengths," in *Proc. of the 2018 Int. Conf. on Biometrics (ICB)*, 2018, pp. 190–194.
31. R. Donida Labati, V. Piuri, F. Rundo, and F. Scotti, "Iris reflection segmentation from ocular images acquired in uncontrolled and uncooperative conditions," in *Proc. of the 2023 IEEE Int. Conf. on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA)*, 2023, pp. 1–6.
32. T.-D. Yang and C.-P. Fan, "Effective scale-invariant feature transform based iris matching technology for identity identification," in *Proc. of the 2018 IEEE Int. Conf. on Consumer Electronics-Taiwan (ICCE-TW)*, 2018, pp. 1–5.
33. L. Ma, T. Tan, Y. Wang, and D. Zhang, "Efficient iris recognition by characterizing key local variations," *IEEE Trans. on Image Processing*, vol. 13, no. 6, pp. 739–750, 2004.
34. K. Roy and P. Bhattacharya, "Iris recognition with support vector machines," in *Advances in Biometrics*, D. Zhang and A. K. Jain, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 486–492.
35. A. Czajka, D. Moreira, K. Bowyer, and P. Flynn, "Domain-specific human-inspired binarized statistical image features for iris recognition," in *Proc. of the 2019 IEEE Winter Conf.ce on Applications of Computer Vision (WACV)*, 2019, pp. 959–967.
36. K. Nguyen, C. Fookes, A. Ross, and S. Sridharan, "Iris recognition with off-the-shelf cnn features: A deep learning perspective," *IEEE Access*, vol. 6, 2018.
37. C.-S. Hsiao and C.-P. Fan, "Efficientnet based iris biometric recognition methods with pupil positioning by u-net," in *Proc. of the 3rd Int. Conf. on Computer Communication and the Internet (ICCCI)*, 2021, pp. 1–5.
38. N. Liu, M. Zhang, H. Li, Z. Sun, and T. Tan, "Deepiris: Learning pairwise filter bank for heterogeneous iris verification," *Pattern Recognition Letters*, vol. 82, pp. 154–161, 2016, an insight on eye biometrics.
39. F. Schroff, D. Kalenichenko, and J. Philbin, "Facenet: A unified embedding for face recognition and clustering," in *2015 IEEE Conf. on Computer Vision and Pattern Recognition (CVPR)*, 2015, pp. 815–823.
40. K. Nguyen, C. Fookes, S. Sridharan, and A. Ross, "Complex-valued iris recognition network," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 45, no. 1, pp. 182–196, 2023.
41. K. Nguyen, C. Fookes, and S. Sridharan, "Constrained design of deep iris networks," *IEEE Trans. on Image Processing*, vol. 29, pp. 7166–7175, 2020.
42. Y. Chen, Z. Zeng, and F. Hu, "End to end robust recognition method for iris using a dense deep convolutional neural network," in *Biometric Recognition*, Z. Sun, R. He, J. Feng, S. Shan, and Z. Guo, Eds. Cham: Springer International Publishing, 2019, pp. 364–375.

43. A. Rattani, R. Derakhshani, S. K. Saripalle, and V. Gottemukkula, “Icip 2016 competition on mobile ocular biometric recognition,” in *Proc. of the 2016 IEEE Int. Conf. on Image Processing (ICIP)*, 2016, pp. 320–324.
44. A. F. Sequeira, J. C. Monteiro, A. Rebelo, and H. P. Oliveira, “Mobbio: A multimodal database captured with a portable handheld device,” in *Proc. of the 2014 Int. Conf. on Computer Vision Theory and Applications (VISAPP)*, vol. 3, 2014, pp. 133–139.
45. J. Daugman, “Information theory and the IrisCode,” *IEEE Trans. on Information Forensics and Security*, vol. 11, no. 2, pp. 400–409, February 2016.
46. A. Dantcheva, C. Chen, and A. Ross, “Can facial cosmetics affect the matching accuracy of face recognition systems?” in *Proc. of the 2012 IEEE Fifth Int. Conf. on Biometrics: Theory, Applications and Systems (BTAS)*, 2012, pp. 391–398.
47. C. Chen, B. Moriarty, S. Hu, S. Moran, M. Pistoia, V. Piuri, and P. Samarati, “Model-agnostic utility-preserving biometric information anonymization,” *International Journal of Information Security (IJIS)*, vol. 23, pp. 2809–2826, 2024.
48. D. Lee and K. N. Plataniotis, “A novel eye region based privacy protection scheme,” in *Proc. of the IEEE Int. Conf. on Acoustics, Speech, and Signal Processing (ICASSP)*, 2012.
49. M. Rieger, J. Hammerle-Uhl, and A. Uhl, “Efficient iris sample data protection using selective JPEG2000 encryption of normalised texture,” in *Proc. of the Int. Workshop of Biometrics and Forensics (IWBF)*, 2018.
50. B. Dolhansky and C. C. Ferrer, “Eye in-painting with exemplar generative adversarial networks,” in *Proc. of the IEEE/CVF conf. on Computer Vision and Pattern Recognition (CVPR)*, June 2018, pp. 7902–7911.