JOIV : Int. J. Inform. Visualization, 6(4) - December 2022 743-748

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

journal homepage : www.joiv.org/index.php/joiv

Iris Image Watermarking Technique for Security and Manipulation Reveal

Rasha Thabit [a,*], Saad M. Shukr [b]

[a] Department of Computer Techniques Engineering, Dijlah University College, P. O. B. 6068, Al Jamaa, 10001, Baghdad, Iraq
[b] Department of Biology, Al-Rasheed University College, P. O. B. 6068, Al Jamaa, 10001, Baghdad, Iraq
Corresponding author: *rashathabit@yahoo.com

***Abstract*— Providing security while storing or sharing iris images has been considered an interesting research topic. Accordingly, various watermarking techniques have been used for iris image protection. Most of the available techniques have been presented to keep the secret data attached to their related images or hide a logo that can be used for copyright purposes. The previous security techniques can successfully meet their aims; however, they cannot reveal the manipulations in the iris region. This research aims to provide security and reveal manipulations in the iris region. Two algorithms have been implemented based on iris image watermarking technology in the proposed method. On the sender side, the proposed algorithm divides the image into the iris region (IR) and non-iris region (NIR), then generates the manipulation, reveals data from the IR, and thereafter embeds it in NIR. At the receiver side, the secret data is extracted from the NIR and compared with that generated from the IR to reveal manipulations if they exist. Experimental results obtained from evaluating the performance of the suggested technique demonstrated the efficiency in providing security and revealing manipulations in the IR. The proposed technique can be utilized in biometric-based security systems to check the input iris image before continuing to the individual's recognition procedure. Different watermarking techniques can be applied in future research to obtain the one with the best performance.**

***Keywords*—Manipulation reveals in iris images; verification and security; fake iris image.**

Manuscript received 17 Oct. 2022; revised 9 Dec. 2022; accepted 20 Dec. 2022. Date of publication 31 Dec. 2022.

I. INTRODUCTION

The rapid development of security systems and applications increased the demand for efficient and secure automatic human recognition methods [1]. Over the years, several biometric-based identification systems have been presented as alternatives to classical authentication systems that rely on passwords and cards. Different biometrics have been used in access control and security systems, such as the face, fingerprint, iris, palm, and voice [2], [3]. Many companies and institutions have adopted biometric-based identification systems because of their advantages, such as ease of use, fast processing, no fear of forgetting or losing data, reliability, and others [4]. The basic principle of these systems depends on capturing and extracting the features from the chosen biometric data and classifying the person according to the extracted data as an authorized or unauthorized person.

The biometric-based security systems can easily authenticate the captured biometric features; however, they are vulnerable to different challenges and attacks. There are different scenarios through which the security of the systems can be defeated, such as collecting and using the biometric data of the people without their knowledge, manipulating the saved datasets that are used for recognition, hacking the biometric data during the process of capturing or sharing them, and many other scenarios. One method that has been used to protect biometric data is associating additional information to the captured data, such as logos, texts, and digital signatures [5]. Adding information to digital biometrics must be unpretentious, which can be achieved by applying watermarking methods.

The biometric systems that can authenticate people through their iris images are widely used [1] because of the facility to capture and process data [6]–[8]. Some watermarking techniques have been presented to protect the iris images, which can be classified into two categories according to the strategy of securing the iris images. In the first category, the original iris image's template has been calculated and embedded in another cover image [9]–[11], while in the second category, the original iris image is used as a cover, and the secret data are embedded within the image [5], [12]. Fig.

1 illustrates the difference between these two categories. According to the study presented by Dong and Tan [13], the second category is preferable because it obtained better iris image recognition accuracy results.

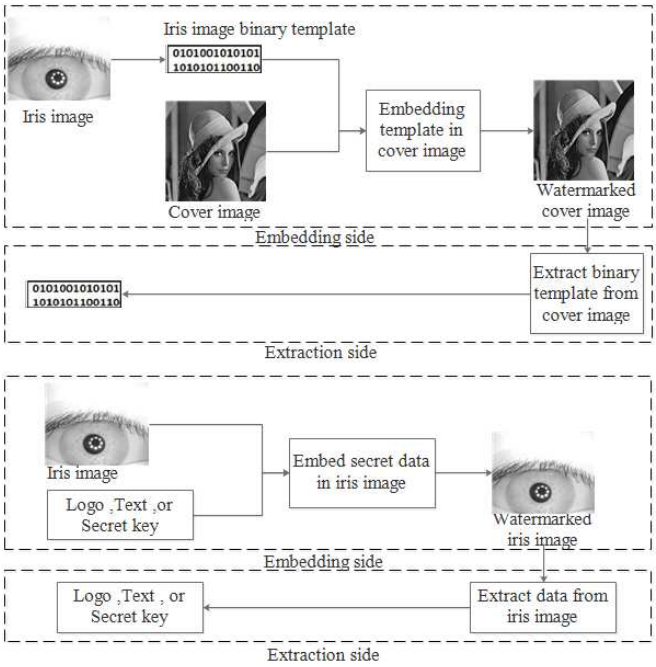

Fig. 1 Two categories of iris image watermarking

In Abdullah, Dlay, and Woo [5], a discrete cosine transform (DCT)-based technique has been presented to protect iris images. A bit from the watermark is embedded in a block of size (8×8) DCT coefficients. This technique obtained robustness against attacks but suffers from limited embedding capacity. In addition, artifacts or distortions are generated in IR. In [14], the effect of watermarking on the recognition performance of the iris image has been tested for various fragile watermarking methods [15]–[21]. The study proved that the watermarking reduces the efficiency of the iris recognition, and the performance is further degraded when the higher payload is hidden in IR. In Czajka, Kasprzak, and Wilkowski [12], another fragile watermarking technique has been presented in which a secret signature is embedded in the iris image. This technique can easily detect alterations in the image because the signature is destroyed when the iris image is altered. The fragile watermarking techniques are easy to implement, but the fragility of the embedded watermarks makes them suitable for only ideal data transmission channels, which are not available in practical applications. The noise generated while transmitting data through the channel has been considered an unintentional attack; therefore, the watermarking technique should have robustness against this kind of alteration.

Recently, the research interest has been directed toward using multiple biometric features to enhance the efficiency of the recognition process [22]–[24]. The types of security techniques that use multiple biometric features are called multi-biometric techniques. In Thabit [25], a multi-biometric technique based on Slantlet transform (SLT) has been presented in which text and fingerprint features are hidden in the cover iris image to provide security and privacy. In order to protect the iris region from distortions, the iris region has been selected using an integrative segmentation process and excluded from the embedding process. The scheme in Thabit [25] outperforms spatial and transform domain-based techniques [5], [12], [15]–[21]. However, it cannot reveal manipulations in the iris region.

The forensics and security systems requested image authentication and manipulation reveal schemes because they could distinguish the authentic image from the manipulated image. Recently, the research community directed many efforts to introduce image authentication schemes for different types of images, such as medical [26]–[28], face [29]–[31], and others.

The iris images can be stored or shared via open access networks or the internet or stored on the cloud for many purposes. The stored or shared images can face some security challenges, such as the lack of user control, unauthorized usage or manipulation of images, and reproduction attacks [6], [32]–[34]. Considering the image authentication requirement and the abovementioned security issues, it will be very useful to present a new technique that can reveal manipulations in the IR.

The scheme in Thabit [25] proved its efficiency compared to other schemes and provides robustness against unintentional attacks. Therefore, its algorithms have been adopted as part of the proposed technique. In order to reveal manipulations in the iris region, the proposed technique suggests that the generation of manipulation reveals information from IR and embeds them in the image blocks in NIR. The proposed technique's main contributions are the steps that have been added to the Thabit [25] algorithms to reveal manipulations in the iris region.

The coming section of the paper illustrates the details of the proposed algorithms in which the data are generated from text file, fingerprint features, and authentication information and embedded in NIR. The results and discussions are presented in section III followed by the conclusions of this work in section IV.

II. Materials and Method

The embedding algorithm of the proposed technique starts by applying the interactive segmentation algorithm from which a binary image is obtained and used for classifying the iris image blocks. The original image is divided into blocks, followed by a classification process. In Thabit [25], the blocks outside IR have been used to carry the binary sequence generated from secret text and fingerprint image features [35]. As mentioned before, the scheme in Thabit [25] provides privacy but cannot reveal manipulations in the IR.

Therefore, the proposed technique in this paper suggests extracting the authentication data from the blocks of the IR and embedding them in the NIR blocks. On the embedding side, the authentication information is converted to binary and concatenated with the binary sequence generated from the text and fingerprint image features. The blocks' final binary sequence is embedded using the SLT-based watermarking process. The hidden sequence is extracted from the iris image at the receiver side. The extracted bits are divided to recover the embedded text, features, and authentication data. Then the authentication data is calculated for the received IR. A comparison of calculated and extracted authentication data is conducted to check the authenticity of the iris image blocks.

The IR block is considered authentic when the compared authentication data are identical; the IR block is manipulated and localized by drawing a border of the block. The following subsections illustrate the steps of the proposed algorithms.

A. Embedding Algorithm

On the sender side, the proposed technique generates a binary sequence from the IR, input text, and fingerprint image and then embeds the sequence in the NIR. The steps are explained as follows:

Step 1: Read the input iris image, fingerprint image, and text file.

Step 2: Generate a binary image that is utilized for classifying image blocks using an interactive segmentation process as follows:

- Create an interactive ellipse shape and set its initial information (position, height, and width).
- Select the iris region and extract the vector of its information (this vector will be sent with watermarked iris image as side information which is required at the receiver side).
- Read the size of the input image.
- Generate binary mask images of zeros with the same iris image size.
- Convert the pixels of the binary image at the IR to ones as shown in Fig. 2.

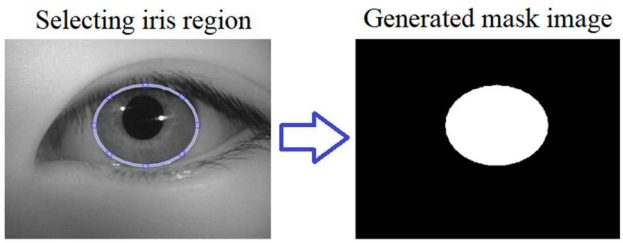

Fig. 2 Selecting iris region and generating binary mask image

Step 3: Divide the input image into non-overlapping blocks. Based on the previous experiments that have been conducted in Thabit [25], the block size (16×16) has been selected.

Step 4: Divide the mask image as done in step 3.

Step 5: Classify the iris image blocks as shown in Fig. 3. According to the average value of the mask image block at the same position, the blocks can be classified into two groups as follows:

$$if\ average \neq 0 \quad Group\ A: block \in IR$$
$$if\ average = 0 \quad Group\ B: block \notin IR$$

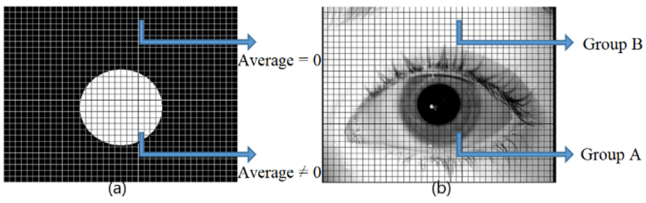

Fig. 3 Classification of iris image blocks

Step 6: Calculate the mean value for each 'Group A' block.

Step 7: Convert the mean values to binary and rearrange bits to obtain one binary sequence.

Step 8: Calculate the fingerprint image features (i.e., ridges and bifurcation) by applying the algorithm from [35] and save these features to the input text file.

Step 9: Convert the resultant text file to binary.

Step 10: Concatenate the binary sequences from steps 7 and step 9 to form the final binary sequence to be embedded in 'Group B' blocks.

Step 11: Calculate the total embedding capacity, which depends on the total number of blocks in 'Group B'. If the capacity is enough to carry the binary sequence generated from step 10 then continue; else stop the embedding procedure to inform the user that there is no enough space to embed the data.

Step 12: Apply pixel adjustment process to blocks in 'Group B' to avoid overflow/underflow problem as explained in Thabit [25]. **Step 13:** Transform the adjusted blocks using Slantlet transform (SLT) matrix then divide the coefficients into subbands (the reader can refer to Thabit [25] and Thabit and Khoo 36] to understand the details of SLT-based watermarking algorithm).

Step 14: Embed the binary sequence from step 10 in the SLT coefficients.

Step 15: Apply inverse SLT to obtain the new 'Group B' resulting from the watermarking process. Fig. 4 summarizes the steps from 6 to 15 as shown below.

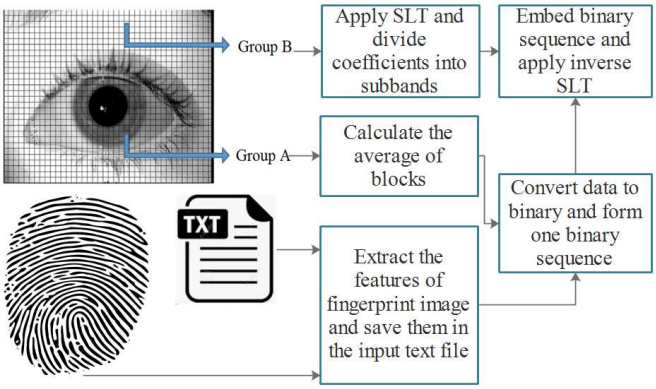

Fig. 4 Generating and embedding binary sequence

Step 16: Construct the watermarked iris image using the blocks from 'Group A' which has been kept without changes and the blocks from step 15 represent the watermarked version of 'Group B'.

Step 17: The watermarked iris image and the side information from step 2 are sent to the receiver side.

B. Extraction Algorithm

On the receiver side, the proposed technique extracts the binary sequence from the NIR and converts it to its original subsequences that are related to the text, fingerprint features, and manipulation reveal data. The steps are as follows:

Step 1: Read the watermarked iris image and the side information.

Step 2: Select IR and generate a binary mask image as follows:

- Select the IR based on the side information.
- Read the size of the input iris image.
- Generate binary mask image of zeros with the same iris image size.

- Convert the pixels of the binary image at IR to ones.

Step 3: Divide the mask as in the embedding procedure.
Step 4: Divide the watermarked iris image as in the embedding procedure.
Step 5: Classify the blocks from step 4 into two groups according to their corresponding blocks from step 3 as shown in Fig. 5.

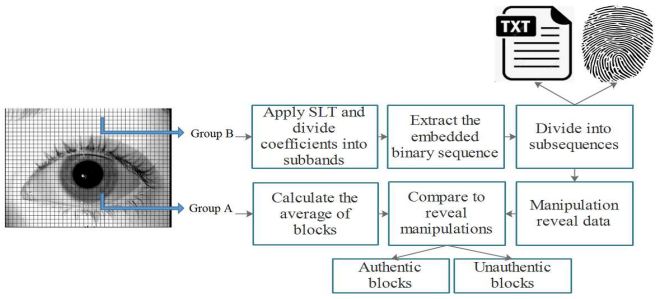

Fig. 5 Steps from the proposed extraction algorithm

Step 6: Apply SLT to 'Group B' and extract the embedded binary sequence using extraction rules from Thabit [25] and Thabit and Khoo [36].
Step 7: Divide the sequence into three parts (i.e., text file bits, fingerprint features bits, and authentication data bits).
Step 8: Convert the authentication data bits to decimal.
Step 9: Calculate the mean for each 'Group A' block.
Step 10: Compare the recovered values from step 8 and the calculated values from step 9 to classify the blocks into two types as shown in Fig. 5. The block is considered authentic if the compared values are identical, else the block is unauthentic.
Step 11: Localize the manipulated block in the iris region by drawing its boarder.
Step 12: Display the iris image after manipulation detection and localization.

III. Results and Discussion

To evaluate the performance of the proposed technique, test images have been collected from CASIA datasets [37] and IIT Delhi iris database [38]. Samples of the test images are shown in Figure 6. The experiments include visual quality test, embedding capacity tests, payload test, and manipulation reveal ability. The following subsections illustrate the experiments and their results. The characteristics of the proposed technique are compared with the state-of-the-art schemes to highlight its efficiency in comparison with previous methods.

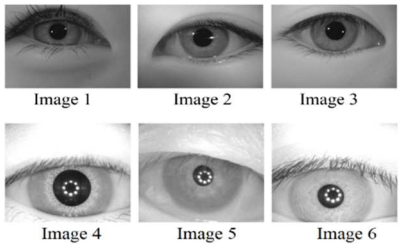

Fig. 6 Sample test images from [37] and [38].

A. Test of Capacity and Payload

The embedding capacity can be calculated based on the number of blocks in 'Group B'. The payload which refers to the total number of bits that are embedded in NIR depends on the number of blocks in 'Group A' in addition to the number of bits related to fingerprint image and the input text file. The same sample fingerprint image and text file used in Thabit [25] have been used in this experiment to illustrate the effect of blocks' number on the capacity and payload. The results of this experiment are shown in Table I which proved that the higher the number of blocks in 'Group B', the higher the capacity. On the other hand, the higher the number of blocks in 'Group A', the higher the payload.

TABLE I
CAPACITY AND PAYLOAD TEST

Image No.	No. of Group B blocks	No. of Group A blocks	Payload (bits)	Capacity (bits)
1	1061	139	12416	67904
2	1032	168	12672	66048
3	1017	183	12800	65088
4	220	120	12288	14080
5	219	121	12288	14016
6	217	123	12288	13888

B. Test of Visual Quality

The metrics used for visual quality evaluation are the Structural Similarity Index Measure (SSIM) and Peak-Signal-to-Noise Ratio (PSNR). The test images and their watermarked images are shown in Figure 7, which proves that no distortions are generated in the images, and the difference between the original and the watermarked images is imperceptible. The experimental results of this test are presented in Table II, which proved that the visual quality results for large-size images are better compared to those for the lower-size images which is related to the ratio of the original to the modified pixels.

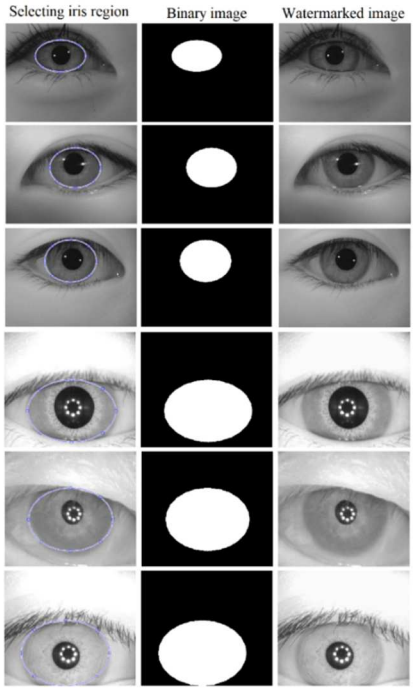

Fig. 7 Watermarked iris images.

TABLE II
VISUAL QUALITY TEST

Image No.	Image size	SSIM	PSNR (dB)	Payload (bits)
1	480×640	0.9966	52.5515	12416
2	480×640	0.9964	53.9248	12672
3	480×640	0.9962	51.8817	12800
4	280×320	0.9846	41.8522	12288
5	280×320	0.9818	45.1709	12288
6	280×320	0.9803	38.1349	12288

C. Test of Manipulation Reveal Ability

To test the manipulation reveal capability, copy_paste and iris_swap attacks have been imposed on the watermarked images using (PS Adobe Photoshop version 21.2.1). Samples of the results are shown in Fig. 8 and Fig. 9 which proved the efficiency of the proposed technique. The results show that the manipulations can be detected and localized without errors.

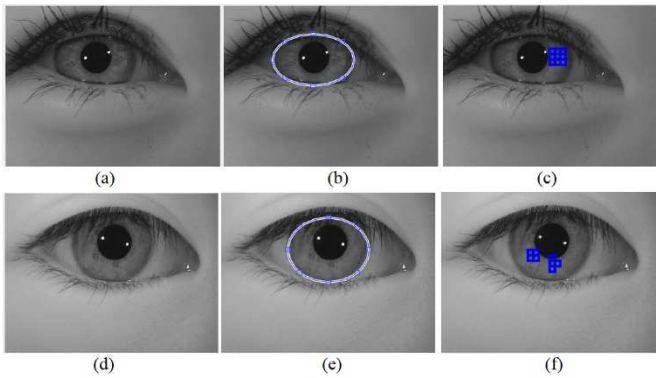

Fig. 8 Manipulation reveal results for copy_paste attack: (a) manipulated 'Image 1', (b) selecting iris region in 'Image 1', (c) manipulation reveal in 'Image 1'; (d) manipulated 'Image 3', (e) selecting iris region in 'Image 3', (f) manipulation reveal in 'Image 3'.

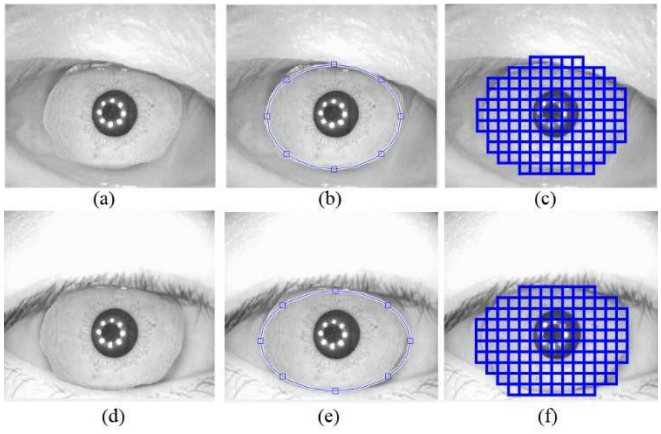

Fig. 9 Manipulation reveal results for iris_swap attack: (a) manipulated 'Image 5', (b) selecting iris region in 'Image 5', (c) manipulation reveal in 'Image 5'; (d) manipulated 'Image 4', (e) selecting iris region in 'Image 4', (f) manipulation reveal in 'Image 4'.

D. Comparison with Previous Techniques

The proposed technique can reveal manipulations in the iris region, which is useful in practical applications especially when the iris region is manipulated for malicious attacks such as stealing the identity or defeating the iris-based recognition systems. The proposed technique outperforms the techniques [5], [12], [15-21], [25], as illustrated in Table III.

TABLE III
COMPARISON WITH PREVIOUS TECHNIQUES

Ref.	Intactness of iris region	Multi-biometric	Manipulation reveal
[16]	D. in IR*	×	×
[20]	D. in IR	×	×
[15]	D. in IR	×	×
[21]	D. in IR	×	×
[18]	D. in IR	×	×
[17]	D. in IR	×	×
[19]	D. in IR	×	×
[5]	D. in IR	×	×
[12]	D. in IR	×	×
[25]	No D. in IR	✓	×
Proposed	No D. in IR	✓	✓

*D. in IR: Distortions in iris region

IV. CONCLUSION

The iris image watermarking techniques are useful in providing privacy and ensuring the attachment of secret data to their related iris images. The possibility of manipulating the iris region for malicious attacks brings the need for watermarking technique that can reveal manipulations. The proposed technique in this paper provides security and can reveal manipulations in IR. The proposed technique consists of two main algorithms that can be applied at the sender and the receiver sides. The embedding procedure starts by selecting IR using interactive segmentation and dividing and classifying the iris image's blocks into two groups. The manipulation reveals that data has been calculated from the IR blocks and concatenated with the data from fingerprint features and text file to generate one binary sequence. The resultant sequence is embedded in the NIR blocks using SLT-based watermark embedding process. The extraction procedure starts with selecting the IR followed by dividing the image into blocks and classifying them into two groups at the embedding side. The information embedded in the NIR blocks is extracted and divided into three parts (i.e., fingerprint features, text file, and manipulation reveal data). The average values of IR blocks are calculated and compared with the extracted data to reveal manipulations if exist. Experimental results proved the efficiency of the proposed technique and its superiority compared to previous techniques in this field. Future research can be conducted using different watermark embedding techniques.

ACKNOWLEDGMENT

The authors thank Dijlah University College and Al-Rasheed University College for supporting and encouraging this research.

REFERENCES

[1] G. Singh, R. K. Singh, R. Saha, and N. Agarwal, "IWT Based Iris Recognition for Image Authentication," Procedia Comput. Sci., vol. 171, pp. 1868–1876, 2020, doi: https://doi.org/10.1016/j.procs.2020.04.200.

[2] K. W. Bowyer, K. Hollingsworth, and P. J. Flynn, "Image understanding for iris biometrics: A survey," Comput. Vis. Image Underst., vol. 110, no. 2, pp. 281–307, May 2008, doi: 10.1016/j.cviu.2007.08.005.

[3] K. J. Anil, B. Ruud, and P. Sharath, Biometrics: Personal Identification in Networked Society. Springer Science & Business Media, 2006. [Online]. Available: https://www.springer.com/gp/book/9780387285399

[4] S. H. Moi et al., “An Improved Approach of Iris Biometric Authentication Performance and Security with Cryptography and Error Correction Codes,” JOIV Int. J. Informatics Vis., vol. 6, no. 2–2, pp. 531–339, Aug. 2022, doi: 10.30630/joiv.6.2-2.1091.

[5] M. A. M. Abdullah, S. S. Dlay, and W. L. Woo, “Securing Iris Images with a Robust Watermarking Algorithm based on Discrete Cosine Transform,” in Proceedings of the 10th International Conference on Computer Vision Theory and Applications, 2015, pp. 108–114. doi: 10.5220/0005305701080114.

[6] K. W. Bowyer, K. P. Hollingsworth, and P. J. Flynn, “A Survey of Iris Biometrics Research: 2008–2010,” in Handbook of Iris Recognition, London: Springer London, 2013, pp. 15–54. doi: 10.1007/978-1-4471-4402-1_2.

[7] P. De and D. Ghoshal, “Human Iris Recognition for Clean Electoral Process in India by Creating a Fraud Free Voter Registration List,” Procedia Comput. Sci., vol. 89, pp. 850–855, 2016, doi: https://doi.org/10.1016/j.procs.2016.06.071.

[8] Q. Hu, S. Yin, H. Ni, and Y. Huang, “An End to End Deep Neural Network for Iris Recognition,” Procedia Comput. Sci., vol. 174, pp. 505–517, 2020, doi: https://doi.org/10.1016/j.procs.2020.06.118.

[9] E. Mostafa, M. Mansour, and H. Saad, “Parallel-Bit Stream for Securing Iris Recognition,” IJCSI Int. J. Comput. Sci., vol. 9, no. 3–2, pp. 347–351, 2012, [Online]. Available: http://www.ijcsi.org/papers/IJCSI-9-3-2-347-351.pdf

[10] J. Lu, T. Qu, and H. R. Karimi, “Novel Iris Biometric Watermarking Based on Singular Value Decomposition and Discrete Cosine Transform,” Math. Probl. Eng., vol. 2014, pp. 1–6, 2014, doi: 10.1155/2014/926170.

[11] B.Alekya Hima bindu, “Watermarking of digital images with iris based biometric data using wavelet and SVD,” Int. J. Eng. Dev. Res., vol. 4, pp. 726–731, 2016.

[12] A. Czajka, W. Kasprzak, and A. Wilkowski, “Verification of iris image authenticity using fragile watermarking,” Bull. Polish Acad. Sci. Tech. Sci., vol. 64, no. 4, pp. 807–819, Dec. 2016, doi: 10.1515/bpasts-2016-0090.

[13] J. Dong and T. Tan, “Effects of watermarking on iris recognition performance,” in 2008 10th International Conference on Control, Automation, Robotics and Vision, Dec. 2008, pp. 1156–1161. doi: 10.1109/ICARCV.2008.4795684.

[14] A. Lock and A. Allen, “Effects of Reversible Watermarking on Iris Recognition Performance,” World Acad. Sci. Eng. Technol. Int. J. Mech. Mechatronics Eng., vol. 8, no. 4, 2014, [Online]. Available: https://publications.waset.org/abstracts/9663/effects-of-reversible-watermarking-on-iris-recognition-performance

[15] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, “Lossless generalized-LSB data embedding,” IEEE Trans. Image Process., vol. 14, no. 2, pp. 253–266, Feb. 2005, doi: 10.1109/TIP.2004.840686.

[16] Jun Tian, “Reversible data embedding using a difference expansion,” IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003, doi: 10.1109/TCSVT.2003.815962.

[17] V. Sachnev, Hyoung Joong Kim, Jeho Nam, S. Suresh, and Yun Qing Shi, “Reversible Watermarking Algorithm Using Sorting and Prediction,” IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989–999, Jul. 2009, doi: 10.1109/TCSVT.2009.2020257.

[18] S. Weng, Y. Zhao, J.-S. Pan, and R. Ni, “Reversible Watermarking Based on Invariability and Adjustment on Pixel Pairs,” IEEE Signal Process. Lett., vol. 15, pp. 721–724, 2008, doi: 10.1109/LSP.2008.2001984.

[19] Y.-C. Li, C.-M. Yeh, and C.-C. Chang, “Data hiding based on the similarity between neighboring pixels with reversibility,” Digit. Signal Process., vol. 20, no. 4, pp. 1116–1128, Jul. 2010, doi: 10.1016/j.dsp.2009.10.025.

[20] B. Yang, M. Schmucker, W. Funk, C. Busch, and S. Sun, “Integer DCT-based reversible watermarking for images using companding technique,” Jun. 2004, p. 405. doi: 10.1117/12.527216.

[21] S. Lee, C. D. Yoo, and T. Kalker, “Reversible Image Watermarking Based on Integer-to-Integer Wavelet Transform,” IEEE Trans. Inf. Forensics Secur., vol. 2, no. 3, pp. 321–330, Sep. 2007, doi: 10.1109/TIFS.2007.905146.

[22] P. Subramanian, K. N. Krishna, R. M. Sebastian, and N. U. Rahman, “Multi-Biometric Systems,” Int. J. Chem. Sci., vol. 14, no. S3, pp. 805–808, 2016, [Online]. Available: https://www.tsijournals.com/articles/multibiometric-systems.pdf

[23] Tuan Hoang, Dat Tran, and D. Sharma, “Remote multimodal biometric authentication using bit priority-based fragile watermarking,” in 2008 19th International Conference on Pattern Recognition, Dec. 2008, pp. 1–4. doi: 10.1109/ICPR.2008.4761869.

[24] M. Vatsa, R. Singh, and A. Noore, “Feature based RDWT watermarking for multimodal biometric system,” Image Vis. Comput., vol. 27, no. 3, pp. 293–304, Feb. 2009, doi: 10.1016/j.imavis.2007.05.003.

[25] R. Thabit, “Multi-Biometric Watermarking Scheme Based on Interactive Segmentation Process,” Period. Polytech. Electr. Eng. Comput. Sci., vol. 63, no. 4, pp. 263–273, Sep. 2019, doi: 10.3311/PPee.14219.

[26] R. Thabit and B. E. Khoo, “Medical image authentication using SLT and IWT schemes,” Multimed. Tools Appl., vol. 76, no. 1, pp. 309–332, 2017, doi: 10.1007/s11042-015-3055-x.

[27] R. Thabit, “Review of medical image authentication techniques and their recent trends,” Multimed. Tools Appl., vol. 80, no. 9, pp. 13439–13473, 2021, doi: 10.1007/s11042-020-10421-7.

[28] N. A. Memon and A. Alzahrani, “Prediction-based Reversible Watermarking of CT Scan Images for Content Authentication and Copyright Protection,” IEEE Access, p. 1, 2020, doi: 10.1109/ACCESS.2020.2989175.

[29] Y. Kortli, M. Jridi, A. Al Falou, and M. Atri, “Face Recognition Systems: A Survey,” Sensors, vol. 20, no. 2, p. 342, Jan. 2020, doi: 10.3390/s20020342.

[30] E. Fourati, W. Elloumi, and A. Chetouani, “Anti-spoofing in face recognition-based biometric authentication using Image Quality Assessment,” Multimed. Tools Appl., vol. 79, pp. 865–889, 2019.

[31] Z. Akhtar, D. Dasgupta, and B. Banerjee, “Face Authenticity: An Overview of Face Manipulation Generation, Detection and Recognition,” SSRN Electron. J., 2019.

[32] M. Aljanabi et al., “Cloud Computing Issues, Challenges, and Needs: A Survey,” JOIV Int. J. Informatics Vis., vol. 5, no. 3, pp. 298–305, Sep. 2021, doi: 10.30630/joiv.5.3.671.

[33] S. Li, X. Chen, Z. Wang, Z. Qian, and X. Zhang, “Data Hiding in Iris Image for Privacy Protection,” IETE Tech. Rev., vol. 35, no. sup1, pp. 34–41, Dec. 2018, doi: 10.1080/02564602.2018.1520153.

[34] Y. W. Lee and K. R. Park, “Recent Iris and Ocular Recognition Methods in High- and Low-Resolution Images: A Survey,” Mathematics, vol. 10, no. 12, p. 2063, Jun. 2022, doi: 10.3390/math10122063.

[35] A. Narayanan, “Fingerprint Minutiae Extraction.” MATLAB Central File Exchange, 2022. [Online]. Available: https://www.mathworks.com/matlabcentral/fileexchange/31926-fingerprint-minutiae-extraction

[36] R. Thabit and B. E. Khoo, “Robust reversible watermarking scheme using Slantlet transform matrix,” J. Syst. Softw., vol. 88, no. 1, 2014, doi: 10.1016/j.jss.2013.09.033.

[37] S.-S. I. Recognition, “CASIA iris image database,” 2020. https://hycasia.github.io/dataset/

[38] I. Delhi, “IIT Delhi Iris Database (Version 1.0),” 2010. https://www4.comp.polyu.edu.hk/~csajaykr/IITD/Database_Iris.htm.