International Journal of Computer Networks and Communications Security

VOL. 8, NO. 6, June 2020, 46–51
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

Tampering Reveal Technique for Iris Images

Rasha Thabit[1], Jaffer Ali[2] and Doaa Subhi[3]

[1, 2, 3] Computer Techniques Engineering Department, Al-Rasheed University College, P. O. B. 6068, Al Jamaa, 10001, Baghdad, Iraq

[1]rashathabit@yahoo.com, [2]jaafar.aa94@yahoo.com, [3]doaasubhi992@gmail.com

ABSTRACT

Nowadays, many biometric based security systems depend on the iris images for authentication because of their features and ease of use. However, storing and sharing these sensitive images through open access networks will expose them to tampering. In order to ensure the safety of the iris images, this paper presents a new tampering reveal technique based on watermarking in the transform domain. In the proposed technique, the iris region is selected and isolated using interactive segmentation process (ISA). The authentication bits have been generated from the iris region (IR) and embedded in the Slantlet transform coefficients of the remaining part of the iris image which has been named as non-iris region (NIR). The use of ISA ensures the intactness of IR because it has been excluded from the embedding process. Several experiments have been conducted to test the visual quality, capacity, payload, and the tampering reveal performance. The experiments proved the ability of the proposed technique to reveal and localize any tampering in IR, in addition, the difference between the original iris image and the watermarked iris image is imperceptible.

Keywords: *Iris image security, Iris image safety, Iris image authentication, Tampering reveal, Iris watermarking.*

1 INTRODUCTION

The use of biometric based security systems is increasing day after another and the applications that make use of biometric data are not bounded [1]–[3]. Different biometric information can be generated, stored, and shared such as face image [4], fingerprint image [5], [6], voice [7], and iris image [8]–[12]. One of the widely used biometric data types is the iris image. Storing or sharing these important and sensitive images through open access or unsecured networks will expose them to the danger of tampering and manipulation, therefore, data security techniques should be used to ensure the safety of the iris images [9], [12]–[14].

The iris image contains two regions as shown in Figure 1, the important region for the iris recognition process is the part that contains the iris region (IR) while the remaining part of the image is not used for the recognition process therefore it will be called non-iris region (NIR). Any tampering in the IR will change the features of the iris region and thus wrong diagnosis process could be happened. The IR should be protected against tampering and manipulation, therefore, iris image authentication technique is required.

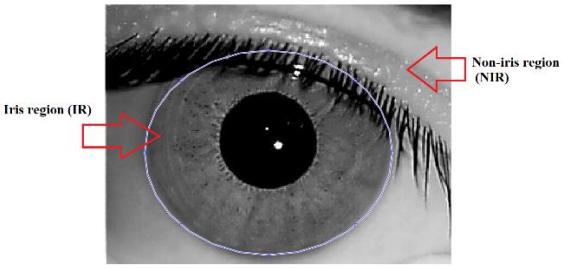

Fig. 1. Illustration of the iris image regions (i.e., IR and NIR)

Over the years, different image watermarking techniques have been used for image authentication purposes. The previous researches proved that the image watermarking techniques that are based on the transform domain are better candidates than the spatial domain based watermarking techniques [13]. In the transform domain based techniques, different transforms have been applied such as discrete cosine transform (DCT) [11], discrete

wavelet transform (DWT) [15], Slantlet transform (SLT) [16], and others. The DWT based techniques perform better than the DCT based techniques; on the other hand, the SLT based techniques perform better than the DWT based techniques [17]–[19]. According to the above mentioned information, this research suggests the use of SLT based watermarking for tampering reveal in the iris images.

The rest of the paper contains the details of the proposed technique followed by the experiments and their results. The final section contains the conclusions of this work.

2 PROPOSED TECHNIQUE

The IR is very important for the diagnosis process, therefore, the watermarking technique should ensure the safety of this region. The interactive segmentation algorithm (ISA) from our previous research [20] has been used in the proposed tampering reveal technique. The flow chart of ISA is shown in Figure 2, the algorithm starts by reading the iris image and selecting the IR region then a mask image is generated to be used in the embedding algorithm.

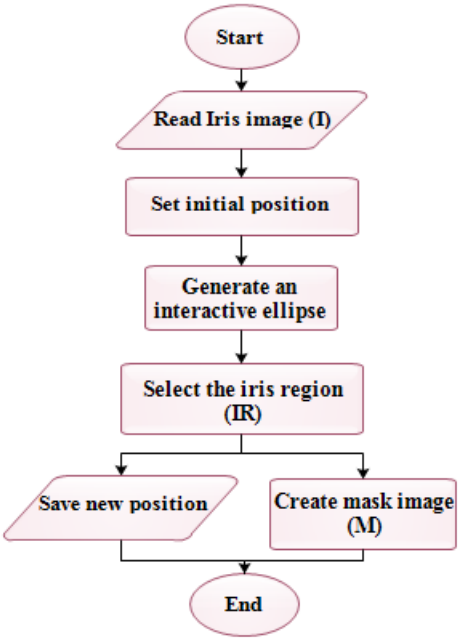

Fig. 2. Flow chart of ISA

The proposed tampering reveal technique consists of two main algorithms, one is at the embedding side and the other one is at the extraction side. A general block diagram for the proposed technique is shown in Figure 3 and the details of the algorithms are illustrated in the following subsections.

2.1 Embedding side

The proposed algorithm at the embedding side starts by applying the ISA to isolate the regions of the iris image then the authentication information is calculated from the IR blocks and converted to binary sequence. The binary sequence is embedded in the NIR by applying content based embedding technique in the SLT domain by adopting the techniques that have been presented in our previous works in [21], [22]. Figure 4 presents the flow chart for the main algorithm at the embedding side which starts by the input iris image and ends by the output watermarked iris image.

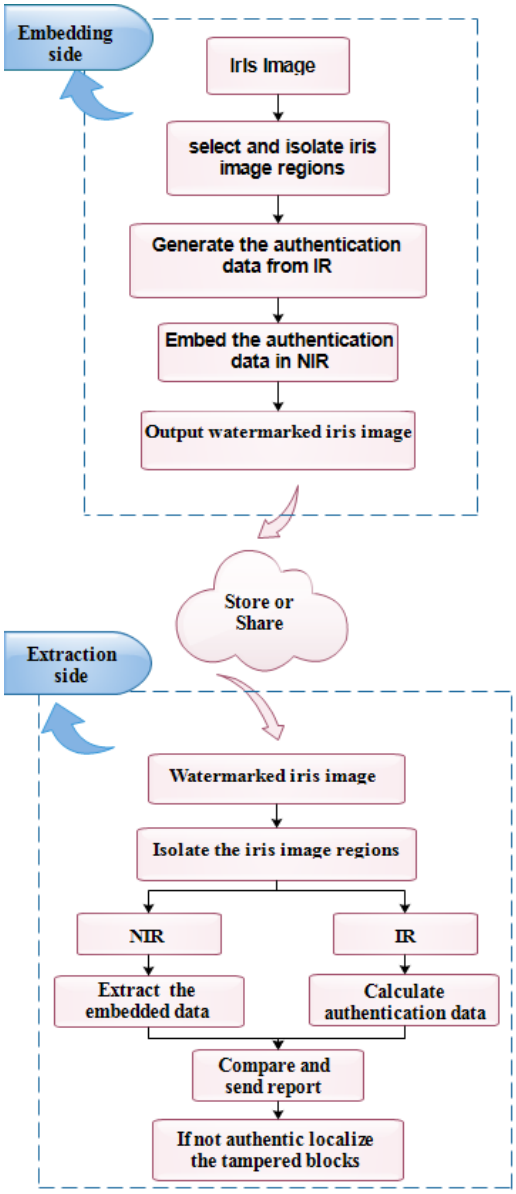

Fig. 3. General block diagram for the proposed technique.

2.2 Extraction side

The proposed algorithm at the extraction side starts by reading the watermarked iris image and dividing it into two regions. The original authentication information is extracted from the NRI using the data extraction method that has been adopted in [21], [22]. The new authentication information is calculated from IR. Then a comparison is performed between the extracted data and the calculated data; if both are equal then there is no tampering and the iris image is authentic else the iris image is not authentic and the localizing process is applied to locate the blocks that have been tampered. Figure 5 presents the flow chart for the main algorithm at the receiver side.

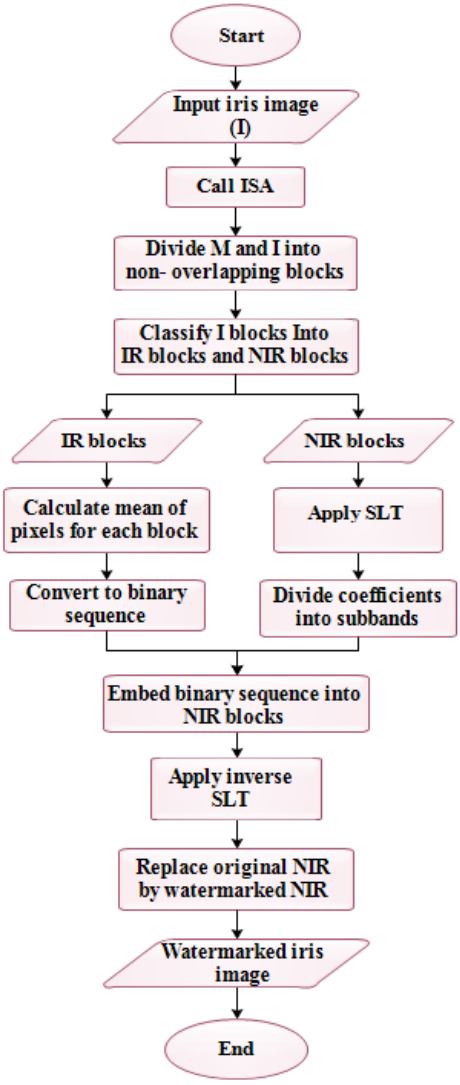

Fig. 4. Flow chart for the main algorithm at the embedding side

3 EXPERIMENTS AND RESULTS

To test the performance of the proposed tampering reveal technique, different iris images have been used from [23], [24]. The experiments have been conducted to test the visual quality of the watermarked iris images, the capacity and payload, and the tampering reveal capability. The following subsections contains the results of these experiments.

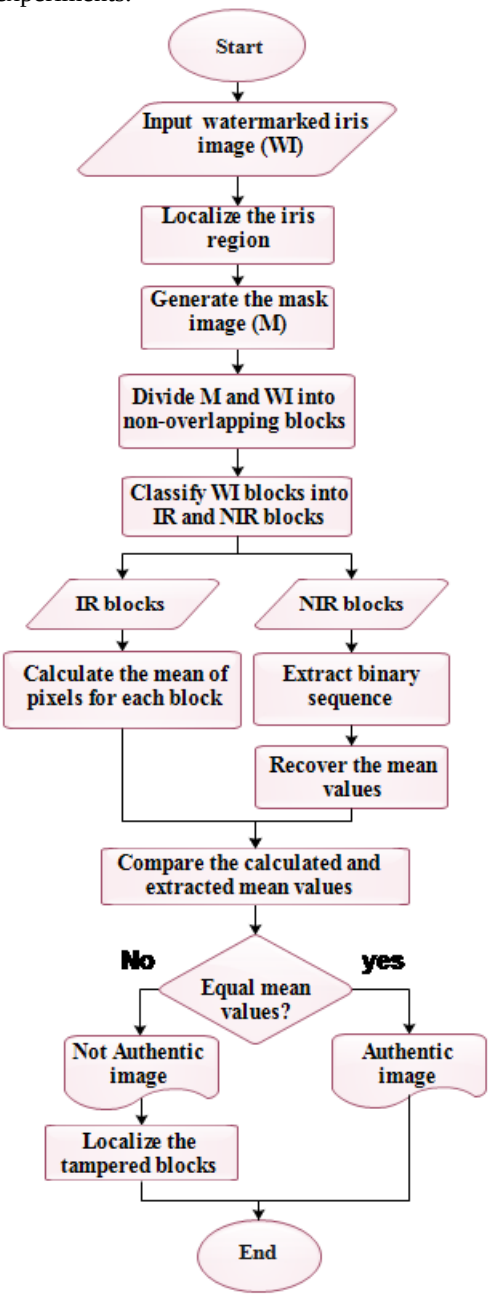

Fig. 5. Flow chart for the main algorithm at the extraction side

3.1 Testing visual quality

To check the visual quality of the watermarked iris images, two experiments have been conducted for different iris images. The first experiment is for subjective evaluation in which the watermarked image is viewed and compared with the original iris image to see if there is any perceptible difference between the two images. The second experiment is for objective evaluation in which the peak signal-to-noise ratio (PSNR) has been calculated. Samples of the results are shown in Figure 6 and Table 1 which proved that the watermarked images obtained good visual quality and the difference between I and WI is not perceptible.

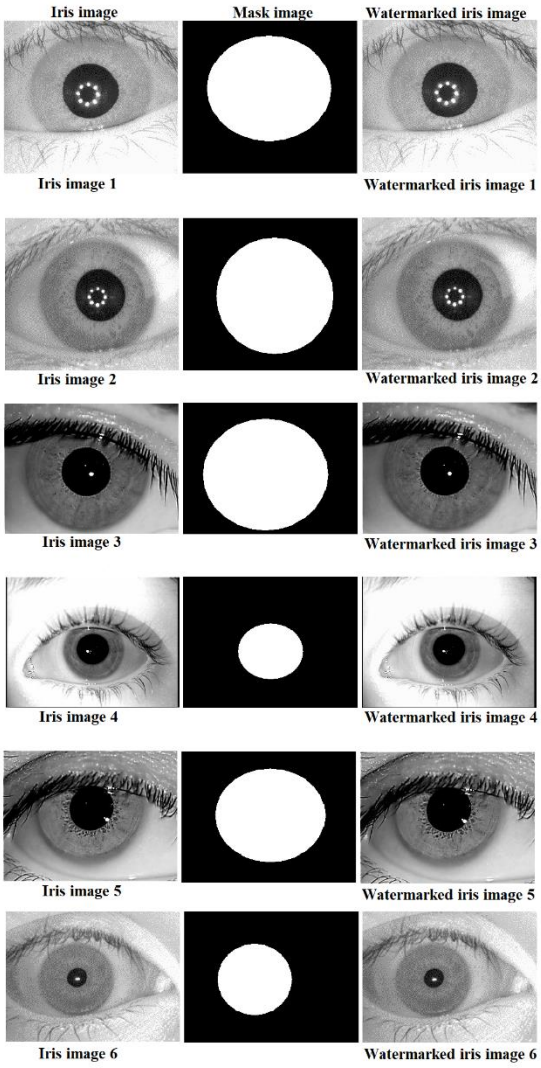

Fig. 6. Samples of the watermarked iris images

Table 1: Visual quality results for different iris images Center

Iris image	Size	PSNR (dB)
Iris image 1	320×280	40.8836
Iris image 2	1536×747	42.8123
Iris image 3	320×240	47.329
Iris image 4	640×480	46.6729
Iris image 5	320×240	41.9759
Iris image 6	354×266	46.7369

3.2 Testing capacity and payload

The embedding capacity refers to the total number of authentication bits that can be embedded in the NIR while the payload refers to the total number of authentication bits that have been generated from the IR. The results proved that the larger the IR, the higher the payload and vice versa. On the other hand, the smaller the IR, the larger the capacity. Table 2 illustrates the results of this experiment for the same test images that have been shown in Figure 6.

Table 2: Capacity and payload results for different iris images

Iris image	Capacity (bits)	Payload (bits)
Iris image 1	11392	1792
Iris image 2	11136	1856
Iris image 3	8192	1920
Iris image 4	65408	1984
Iris image 5	10944	1472
Iris image 6	17216	960

3.3 Testing tampering reveal capability

To test the performance of the proposed technique in revealing the tampering in the IR, two different tampering processes have been imposed on some test images. The first tampering process is copy and paste where some pixels from IR are copied and pasted in another place inside IR. The second tampering process is erasing in IR where some pixels of the iris region are erased. The results of this test are shown in Figure 7 and Figure 8 which proved the ability of the proposed technique in revealing any tampering and localizing the tampered blocks in the IR.

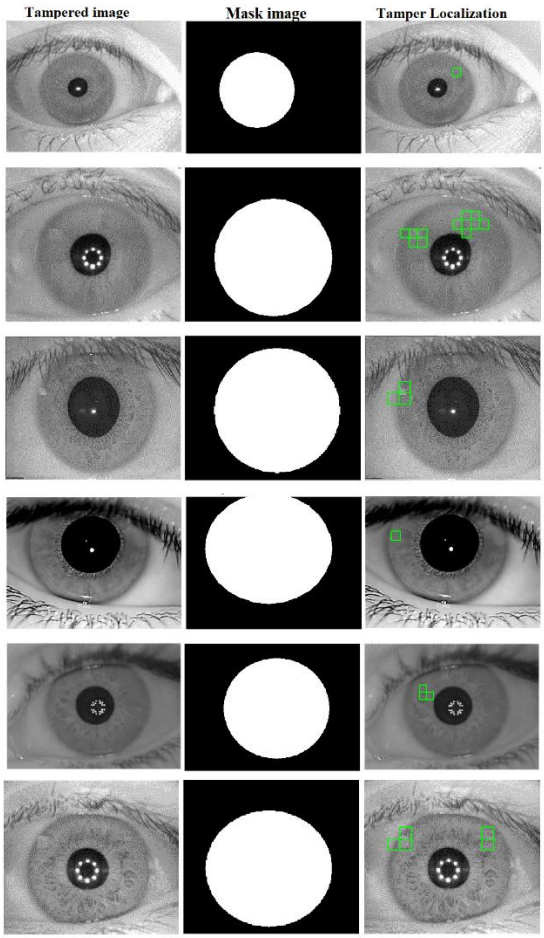

Fig. 7. Tampering reveal for copy and paste in IR

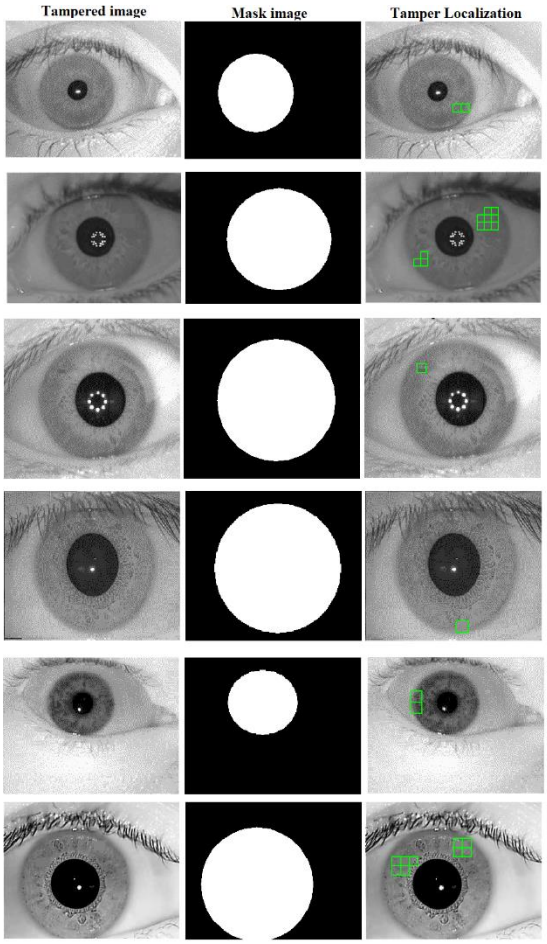

Fig. 8. Tampering reveal for erasing in IR

4 CONCLUSIONS

In this paper, a new iris image security technique has been introduced for revealing tampering in the iris region which is based on watermarking in the transform domain. The proposed technique used ISA in order to protect the iris region from distortions. The authentication data has been generated from IR and embedded in NIR using content based embedding method in the SLT domain which is based on modifying the coefficients in each NIR block. Different experiments have been conducted for different iris images and the results proved the efficiency of the proposed technique in terms of visual quality, capacity, and the ability to detect tampering and localizing the tampered blocks in IR.

5 REFERENCES

[1] J. Wayman, A. Jain, D. Maltoni, and D. Maio, "An Introduction to Biometric Authentication Systems," Biometric Syst., pp. 1–20, 2005, doi: 10.1007/1-84628-064-8_1.

[2] J. N. Pato and L. I. Millett, Biometric Recognition : Challenges and Opportunities. Washington: The national academies press, 2010.

[3] J. N. Pato and L. I. Millett, Biometric Recognition : Challenges and Opportunities. Washington: The national academies press, 2010.

[4] D. N. Parmar and B. B. Mehta, "Face Recognition Methods & Applications," Int.J.Computer Technol. Appl., vol. 4, no. 1, pp. 84–86, 2014, [Online]. Available: http://arxiv.org/abs/1403.0485.

[5] A. Chakraborty, S. Pathan, M. Kabir, and K. Thakur, "Fingerprint Authentication Security: An Improved 2-Step Authentication Method

with Flexibility," Int. J. Sci. Eng. Res., vol. 10, no. February, pp. 438–442, 2019.
[6] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "Security and accuracy of fingerprint-based biometrics: A review," Symmetry (Basel)., vol. 11, no. 2, 2019, doi: 10.3390/sym11020141.
[7] H. N. M. Shah, M. Z. A. Rashid, M. F. Abdollah, M. N. Kamarudin, C. K. Lin, and Z. Kamis, "Biometric Voice Recognition in Security System," Indian J. Sci. Technol., vol. 7, no. 2, pp. 104–112, 2014.
[8] K. W. Bowyer, K. P. Hollingsworth, and P. J. Flynn, Handbook of Iris Recognition. 2013.
[9] 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, 2008, doi: 10.1016/j.cviu.2007.08.005.
[10] M. T. Gaata and R. A. Jaafar, "Iris Image Authentication based on Adaptive Watermarking System," Int. J. Comput. Trends Technol., vol. 34, no. 2, pp. 63–67, 2016, doi: 10.14445/22312803/ijctt-v34p111.
[11] 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, 2014, doi: 10.1155/2014/926170.
[12] P. E. Mostafa, M. Mansour, and E. H. Saad, "Parallel-Bit Stream for Securing Iris Recognition," Int. J. Comput. Sci. Issues, vol. 9, no. 3, pp. 347–351, 2012.
[13] J. Dong and T. Tan, "Effects of watermarking on iris recognition performance," 2008 10th Int. Conf. Control. Autom. Robot. Vision, ICARCV 2008, pp. 1156–1161, 2008, doi: 10.1109/ICARCV.2008.4795684.
[14] M. A. M. Abdullah, S. S. Dlay, and W. L. Woo, "Securing iris images with a robust watermarking algorithm based on discrete cosine transform," VISAPP 2015 - 10th Int. Conf. Comput. Vis. Theory Appl. VISIGRAPP, Proc., vol. 3, no. July, pp. 108–114, 2015, doi: 10.5220/0005305701080114.
[15] A. H. Bindu and V. Saraswati, "Watermarking of digital images with iris based biometric data using wavelet and SVD," Int. J. Eng. Dev. Res., vol. 4, no. 1, pp. 726–731, 2016.
[16] 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.
[17] R. T. Mohammed and B. E. Khoo, "Image watermarking using slantlet transform," ISIEA 2012 - 2012 IEEE Symp. Ind. Electron. Appl., pp. 281–286, 2012,
[18] doi: 10.1109/ISIEA.2012.6496644.
[19] R. Thabit and B. E. Khoo, "Capacity improved robust lossless image watermarking," IET Image Process., vol. 8, no. 11, 2014, doi: 10.1049/iet-ipr.2013.0862.
[20] M. M. Lafta and I. M. Alwan, "Watermarking in Image Using Slantlet Transform," vol. 52, no. 2, pp. 225–230, 2011.
[21] R. Thabit, "Multi-biometric watermarking scheme based on interactive segmentation process," Period. Polytech. Electr. Eng. Comput. Sci., vol. 63, no. 4, 2019, doi: 10.3311/PPee.14219.
[22] 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.
[23] R. Thabit and B. E. Khoo, "A new robust reversible watermarking method in the transform domain," Lect. Notes Electr. Eng., vol. 291 LNEE, 2014, doi: 10.1007/978-981-4585-42-2_19.
[24] Research Center for Biometrics and Security, "CASIA iris image database." http://www.cbsr.ia.ac.cn/Databases.htm (accessed Jan. 01, 2019).
[25] Indian Institute of Technology Delhi, "IIT Delhi Iris Database version 1.0." http://web.iitd.ac.in/~biometrics/Database_Iris.htm (accessed Jan. 01, 2019).