DIGITAL IMAGE WATERMARKING TECHNIQUES AND BIOMETRICS DATA SECURITY: A REVIEW

Jelena Tašić,
Saša Adamović,

Faculty of Informatics and Computing,
Singidunum University,
Belgrade, Serbia

Abstract:

In this study, we review digital watermarking techniques used for protection of biometrical data in authentication services based on biometry. In addition to the development of protection biometrical templates, there has been a breakthrough in additional privacy protection within biometrical systems that perform authentication without preserving biometry in their databases. We begin with theoretical foundations of digital watermark and biometry and then review current research advances in this area, which combine the two technologies and thus create a new ground for exploration better known as biometrical watermarking.

Key words:

Biometric watermarking, Biometric identification systems, Data protection, Digital watermarking, Steganography

1. INTRODUCTION

Using biometric authentication has recently increased due to the easy access to the Internet and the risk of misuse. Biometric is beginning to replace traditional authentication methods because of the quality of biometric data. Many organizations are using biometric data to protect individuals from identity thefts.

Biometric samples may be compromised despite being stored in databases. Biometrics cannot ensure authenticity or guarantee rejection because it may be copied or counterfeited. If the biometric data are stolen or modified, they are forever lost. Hence, the security and integrity of biometrics data represent a challenge. In order to increase safety and improve system performance, various types of authentication should be combined.

Techniques based on steganography are suitable for transferring the critical biometric data from the user to the server thus reducing the possibility of illegal changes to biometric data. After enrolment, encryption is applied on a biometric sample, which is then decrypted during the authentication by using a secret key. Encryption provides security until the data are decrypted.

Correspondence:
Jelena Tašić

e-mail:
jecatasic89@gmail.com

DOI: 10.15308/Sinteza-2017-55-62

2. RELATED WORK

If a verification system guarantees that the biometric data at the moment of entry originates from a legitimate user, the biometric system will function properly [1]. Biometric watermarking helps increase safety of authentication systems. Watermarks provide security after the data have been decrypted. Biometric data embedded into the decoded data host may be recovered only by using the secret key [2].

In order to protect its integrity, information is hidden in the host data image by using a watermarking technique. There are various watermarking techniques for embedding data into the image. They may be divided into spatial domain techniques [3], [4] and frequency domain techniques [1], [5], [6], [7]. Although techniques in the spatial domain have the lowest complexity and large load capacity, they cannot withstand attacks such as image processing and low-pass filtering [8].

Biometric watermarking techniques increase security. Jain et al. [9] proposed using a secret key for embedding a bit sequence of eigenface coefficients into randomly selected pixels of fingerprint image by using a blind watermark technique. Jain and Uludag [10] applied steganography technique for hiding the minutiae data within the data bearer that are unrelated to the original fingerprint image. Information was hidden in three types of images: fingerprint, facial, and arbitrary image. Authors hid eigenface coefficients within the fingerprint image. The results have shown that 100% of the minutiae points were recovered thus proving that the watermarked fingerprint image does not degrade performance. Moon et al. [11] proposed several watermarking techniques to increase safety of biometric system by using a fingerprint and a face image. Superior verification accuracy was achieved by embedding fingerprint features into a face image, which is not the case when facial features were embedded into a fingerprint image.

A watermark and cryptography technique based on block- wise image for embedding a fingerprint template into a facial image that preserves the image quality, was introduced by Komninos and Dimitriou [12] while Park et al. [13] proposed using robust embedding of iris template into a face image. Vatsa et al. [14] combined discrete wavelet transform (DWT) and the least significant bit (LSB) methods for watermarking biometrics. Watermarking technique based on the DWT method is robust to frequency attacks but vulnerable to geometric attacks. In contrast, the watermarks based on LSB algorithms are robust to geometric attacks but they are more vulnerable to frequency attacks. Authors have shown that the combined algorithm works better than separate techniques. Acting together, DWT and LSB enhance encryption and decryption in the case of frequency and geometric attacks.

Embedded voice features into an iris image were used by Bartlow et al. [15]. Instead of randomly choosing points within the image, voice feature descriptors were hidden inside a segmented iris. Results have shown that introduction of voice feature descriptors does not significantly interfere with the quality of iris image or matching performance. For improving biometrics data integrity, authors have proposed usage Public Key Infrastructure (PKI), which provided non- repudiation of origin and data integrity through cryptography.

Low et al. [16] applied the discrete random transform (DRT) and principal component analysis (PCA) for decomposing a signature into binary bit strings. Three methods of embedding and extraction are compared to determine robustness and strength against JPEG compression: LSB, CDMA spread spectrum in the spatial domain, and CDMA spread spectrum in the DWT domain. Performance of these methods was tested by the human visual perception, peak signal to noise ratio (PSNR), and the distortion rate (normalized Hamming distance). Results indicated that the LSB method is highly fragile to JPEG compression despite having the simplest access to biometric watermarks. The CDMA spread spectrum in DWT domain is complicated while being much more resistant to JPEG compression.

Rajibul et al. [17] embedded encrypted palmprint template into a fingerprint image by using a key extracted from palmprint while Ma et al. [18] proposed a block pyramid scheme based on an adaptive watermarking quantization for embedding fingerprint minutiae into a face image. Watermark's numeric bits with higher priority and embedding strength are embedded into an upper level of the pyramid by using the first order statistics (the Quantization Index Modulation (QIM) method).

A scheme for the iris pattern protection by combining cryptography and watermarking techniques was presented by Fouad et al. [19]. An iris image was protected with a key and embedded into a cover image by using the LSB and DWT techniques. The embedding location is defined by a second key. Both keys (iris and embedded) are necessary in the process of iris extraction.

The Cox's algorithm for embedding watermark into a face image was applied by Isa and Aljareh [20]. In the identification process, a face image was used for the username while a watermark was used as a password for the authentication. A disadvantage of the scheme is that it

requires the original image during the watermarking detection process.

In order to obtain an eigenvector, Majumder et al. [21] applied a biometric watermark by using the DWT method and singular value decomposition (SVD) of the host image. Iris features were extracted by using the discrete cosine transform (DCT) technique and embedded into the eigenvector. A disadvantage of this approach is the inability to change the algorithm used for extracting iris features.

Paunwala and Patnaik [22] embedded fingerprint and iris features into a cover image that is divided into blocks. Each block is transformed into a two-dimensional DCT and classified into blocks with or without edges. Biometric features were embedded into low frequency coefficients of the 8 x 8 DCT block while removing the block with edges.

3. DISADVANTAGES OF BIOMETRICAL SYSTEMS

Development and application of biometric system revealed deficiencies that may be divided into two categories: The first category is related to poor privacy protection of biometric data. If cryptographic keys are compromised, biometric data will be lost in spite of the encrypted biometric pattern. The second category deals with the system security [23]. Biometric patterns are not always encrypted. For example, decrypted biometric data are used in the authentication process (checking the degree of matching between two biometric patterns) [24].

Determining the authenticity of the original biometric data is also an issue especially when sensors, feature extractors, and template generators are not integrated. Given that the traditional methods for data authentication (hash functions or message authentication) are very sensitive to every input bit of data, they cannot be applied [25]. Information carried by the biometric image is retained even if data undergo the content preserving operations (compression and quality improvement).

A compromise between robustness and security makes a system vulnerable to numerous threats. During a transfer of biometric data from the sensors to the decision-making module, there is a risk of various types of attacks such as spoofing, masquerade attack, eavesdropping, replay attack, recorded data insertion, remaking, tampering, Trojan horse insertion, data interception, substitution attack, or overriding yes/no responses [26]. A generic scheme of potential attacks on a biometric system is shown in Fig.1.

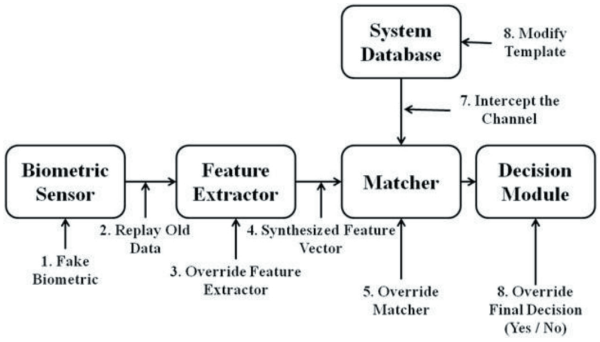

Fig. 1. Examples of possible attacks on a biometric identification system [27]

Digital watermarking offers the best solution. Watermarking is becoming a prominent security tool that has been successfully applied to many applications in order to protect the original multimedia data such as copyright protection and content authentication. Secret information is embedded into a host image by using a robust watermarking method so that the watermark content could be recovered even after experiencing a moderate distortion.

4. BIOMETRIC WATERMARKING

Biometric watermark is an invisible digital watermark embedded into a cover image that may be easily recovered by using software tools. The embedding location of biometric data is defined by a secret key thus preventing the possibility of biometric data misuse. The invisible watermark should be robust to various signal processing techniques and should be recoverable from the modified image. Furthermore, invisible watermarking technique should be applied within the legal framework, together with the location security and encryption.

Jain et al. [10] proposed the watermarking technique as an additional defense for biometric systems. Using the watermark may effectively improve the safety and reliability of biometric systems [25]. Listed are advantages of biometric watermarks:

- Invisibly hidden into host data, a watermark may be used as authentic token in forensics for safekeeping. In case of interception of biometric data, it may provide a mechanism for monitoring in order to identify the origin of the data.
- Watermarked information is connected to a host data and hence it does not require an additional storage or transfer of resources. Furthermore,

verification "on the spot" does not require privileges for accessing biometric or watermark databases.

- Watermarks do not affect other security tools. Hence, cryptographic operations or techniques for template protection may be applied on watermark data or watermarked host data.

Application of Visual Cryptography and Transformation Methods

Visual cryptography and DWT methods have been applied in order to hide an iris image [28] that was embedded into a cover image divided into four parts by using the DWT method and was then compressed. The three-least-significant-bit technique was applied for embedding the secret message.

Results have shown that application of these methods protects the iris and the secret message from the identity theft. Good results have been achieved by combining the DWT method and the Haar filter. Compared to the original iris image, the resulting image has a reduced number of pixels while preserving the image quality.

Good quality of iris and cover images with reduced required range may be achieved by decomposing the iris image into two levels by using the DWT method without final compression of the watermarked image. By using the three- least-significant-bit method in the embedding process, the size of the secret message increases while the quality of the iris image remains unchanged.

Application of the Robust Watermarking Algorithm Based on DCT

The middle band coefficient exchange (MBCE) method was presented by Zhao and Koch [29]. Later, Hsu and Wu [30] applied the DCT method for embedding the middle band coefficients. The algorithm encrypts one bit of the binary watermark object into an 8 x 8 sub block of the host image so that the difference between the two middle band coefficients is positive if the encrypted value is 1. Otherwise, the two middle band coefficients will change.

The image is divided into three frequency bands by using a watermarking technique in the DCT domain, as shown in Fig. 2, which made it easier to embed watermark information into a specific frequency range [31]. The 8 x 8 block is taken after the DCT has been applied to the image.

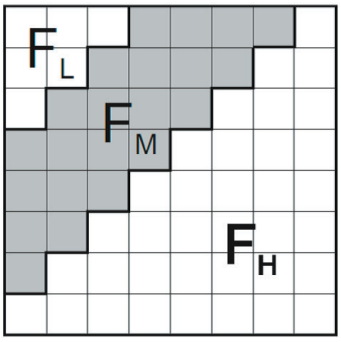

Fig. 2. Frequency regions in the 8 x 8 DCT block [34]

The low frequency range F_L bears the most important part of the visual image while the high frequency range F_H is vulnerable to noise attacks and to removal under lossy compression. The most preferred range for the embedding watermark information is a medium frequencies range F_M because it does not affect important parts of the visual image. The high frequency components F_H are not overly exposed to removal if they were target of attacks [32].

Two locations from DCT blocks ($DCT_{(U1;V1)}$ and $DCT_{(U2;V2)}$) are chosen for the middle frequency band F_M for comparison. After the watermarked text has been converted into a binary image, the pixel values are checked. If the relative size of each coefficient does not agree with a bit that has to be encrypted, the coefficients are replaced. If the value of the pixels in the binary text is 1, the DCT coefficient is replaced so that $DCT_{(U1;V1)} > DCT_{(U2;V2)}$. If the value is 0, the coefficient is replaced so that $DCT_{(U1;V1)} < DCT_{(U2;V2)}$. This scheme hides watermarked data so that it interprets 0 and 1 with relative values of two fixed locations ($DCT_{(U1;V1)}$ and $DCT_{(U2;V2)}$) in the middle frequency range F_M instead of inserting any data. This kind of coefficient replacement does not significantly affect watermarked image because the DCT middle range frequency coefficients have similar magnitudes [29], [33]. In the image extraction process, the 8 x 8 DCT image is taken again so that 1 will be decoded if $DCT_{(U1;V1)} > DCT_{(U2;V2)}$ and 0 will be decoded if $DCT_{(U1;V1)} < DCT_{(U2;V2)}$. In this manner, the watermark has been created.

If only one pair of coefficients is used for hiding the watermark data, an attacker may analyze several copies of the watermarked images in order to predict location of coefficients and destroy them. Abdullah et al. [34] solved this problem by choosing three pairs of middle range frequency coefficients thus increasing redundancy and robustness of the scheme to various attacks. Authors have proposed adding a constant k so that $DCT_{(U1;V1)} - DCT_{(U2;V2)} < k$

in order to increase robustness of the watermark algorithm. The strength of the watermark will increase by choosing the value of k. Increasing k will degrade the image but will reduce the error probability in the detection phase. Choosing $k = 15$ proved to be the best value for the perception versus robustness.

A good watermarking algorithm should be imperceptible to the user and should not significantly affect the matching performance of a biometric system. It should also reliably detect embedded information even if a watermarked image is degraded.

One bit of the watermark text will be hidden in each 8 x 8 block of the image. A one-dimensional string of zeros and ones is taken as the watermark object. An image of the watermarked text carries user's information (name, ID, and date of birth). The difference between the original and watermarked image, shown in Fig. 3, cannot be seen without applying image processing techniques. The average value of the peak signal to noise ratio (PSNR) between the original image and the watermarked image is 37.69 while the average value of the bit error rate (BER) is 0.257%. The average value of the PSNR for the extracted watermarked text is 84.25 while the BER is 0.0244%.

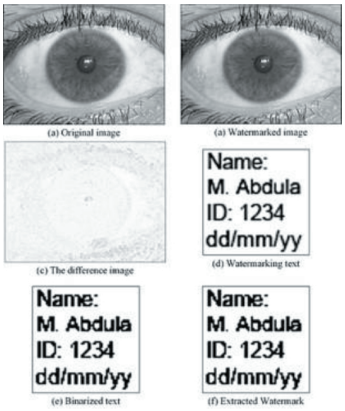

Fig. 3. Perceptibility of the watermarked image [34]

The original image is not required for the watermark extraction. Furthermore, the integrity of the biometric features may be verified from the extracted text. This watermarking method is highly beneficial for a biometric system. For instance, biometric features and user's information are mostly stored in an independent database. The watermark integrates biometric features with personal information into a file, which allows the simultaneous storage and extraction of data. This method is easily applicable to all biometric images and does not significantly affect quality of the iris image or performance of the biometric matching. Furthermore, it is robust to JPEG compression, filtering, and noise.

Watermarked Biometric Based on Singular Value Decomposition and DCT Methods

Lu et al. [35] proposed a scheme that in order to increase the security focuses more on iris identification rather than on the digital watermarking. DCT is applied on the iris pattern and the obtained value is then encrypted into the Bose– Chaudhuri–Hocquenghem (BCH) code for error control. The host image is divided into four equal blocks. The BCH code is embedded into the singular value of each coefficient of the host image by using the key that is obtained by using the DCT method. After the DCT coefficients of the host image are altered with the watermark, the inverse cosine transform (IDCT) is applied on the image as shown in Fig. 4. The watermark strength depends of the employed key. The results show that the proposed method may effectively extract the watermark.

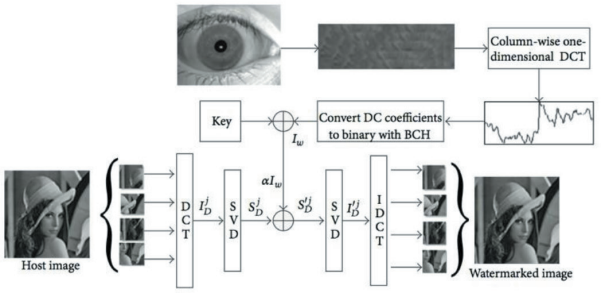

Fig. 4. Process of the watermark embedding into the host image [35]

Applications of the Watermark and Steganography for Multimodal Biometric Data Security

Whitelam et al. [36] proposed a multilayer structure by combining the watermarking and the steganography techniques in order to increase security of the multimodal biometric data. The amplitude modulation [37], which repeatedly embeds information into the spatial domain of the image, was used for the watermarking encryption and the steganographic image. The method is widely used in signal processing for telecommunications.

The eigenface coefficients were converted into a continuous sequence of bits and then embedded into a fingerprint image by using an encryption technique

specifically designed for biometric watermarks. By using steganographic techniques, obtained watermarked data (fingerprint and face) were hidden into an arbitrary host image that was not essential for biometrics or forensics. Examples are shown in Fig. 5.

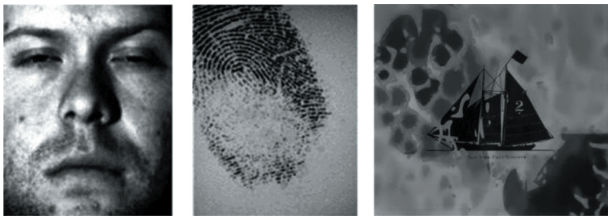

Fig. 5. Images used for watermarking and steganography: (a) face image, (b) fingerprint image, and (c) the host image [36]

Watermarked image of a fingerprint and a face was converted into a binary string. The maximum pixel intensity is then used to determine the number of bits required for steganography. The place of embedding is randomly determined from all three-color channels of the host image. This method provides additional security to the user in the case of compromised data by taking into account that there is no indication that the biometric data are present.

For example, in order to access a protected resource, Alice sends a request to Bob. Alice provides her authentication data (fingerprint and facial characteristics). The eigenface characteristics were embedded into the fingerprint image by using Bob's public key for getting a watermarking location. By using the same key, the watermarked fingerprint image may be embedded into a cover image. Additional security for the biometric data was provided through a public key infrastructure (PKI) by using RSA encryption as well as Alice's private and Bob's public keys. The data will then be stored into a central database or in a secured token. The difference between the original and watermarked image is shown in Fig. 6.

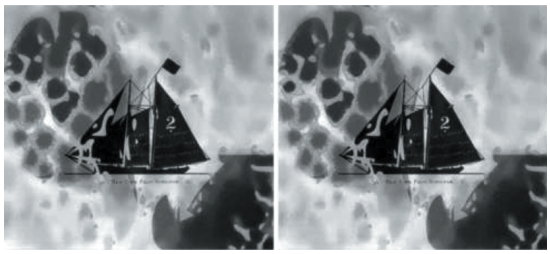

Fig. 6. The original (a) and the watermarked image with the fingerprint as a watermark (b)

In the decryption process, Bob decrypts the steganography image by using his private key and Alice's public key. The fingerprint image and eigenface characteristics may be extracted by using the Bob's private key for getting the watermarking location. The extracted fingerprint image and eigenface characteristics may be used for data authentication.

The security of the multimodal verification system may be increased by using the eigenface characteristics and the fingerprint. At the end of the process, the system will be secured with the multiple layer authentication (cryptography, watermark, steganography, and multimodal biometric verification). Cryptography provides a data integrity while the public key infrastructure provides a non-repudiation of origin. Unlike cryptography, the watermarking and steganography techniques enable the special layers for monitoring since the decoded image has the watermark that reveals the origin of the image.

Multimodal Two-Step Authentication Based on Wavelet Quantization Watermarking

Ma et al. [38] proposed a watermarking method based on a two-stage authentication in order to increase the safety and reliability of biometric systems shown in Fig. 7. The face features are embedded into the fingerprint image during the data collection process. The authenticity of the entered data is determined by checking the validity of the extracted watermark. The system executes the next authentication phase only if data are authentic. The watermarked face image then serves as additional information in order to facilitate biometric authentication.

The authenticity of data is verified by checking the validity of the extracted watermark. This increases the robustness of the system to malicious attacks such as tampering and forgery. As with conventional watermarks, template classification (of watermark) instead of searching the database may be applied for reliable verification. The presence of the watermark may be inferred by a detector that compares the extracted template with all watermarked samples in the database in order to find the sample with the highest matching. However, due to the presence of noise, it is unlikely that extracted watermark will be identical to the original. Furthermore, the face watermark is an extremely sampled image and poses a major challenge for identification. As a solution to the problem of recognizing the watermark, authors applied the sparse representation based classification (SRC) that produced good results when combined with a detector.

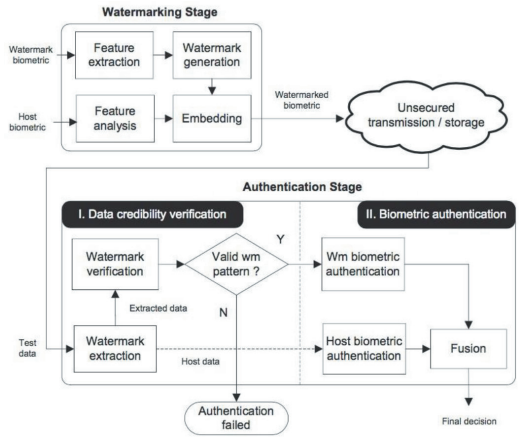

Fig. 7. Diagram of the watermark embedding based on a two-stage biometric authentication [38]

5. CONCLUSION

In this paper, we provided a detailed overview of the biometric watermarking techniques and the current state of the art in this field. We also presented several solutions that employ steganographic and cryptographic techniques in order to protect the biometric data.

Vulnerability of the biometric data is addresses by using a digital watermark, which serves as an authentication token. Hence, the authentication will fail if the watermark is damaged or absent. Increasing the watermark capacity for use in extensive identification of information reduces the robustness of the watermark. System security increases by combining various cryptographic and steganographic techniques.

Applying techniques for pattern protection of the embedded data guarantees security and prevents counterfeiting of the watermarked image. Employing a secret key for randomly selecting embedding position of the watermark or encrypting a watermark sequences before embedding, makes the watermarking data safe from unauthorized extraction. Even if able to identify the algorithm for extraction, an attacker is unable to obtain the watermark data because they are additionally protected with a secret key. Therefore, procedures used to maintain the secrecy of the key are very important as well as is replacing of compromised keys.

REFERENCES

[1] Y. Wang, J. F. Doherty, and R. E. Van Dyck, "A wavelet-based watermarking algorithm for ownership verification of digital images," *IEEE Trans. Image Process.*, vol. 11, no. 2, pp. 77–88, Feb. 2002.

[2] T. Hoang, D. Tran, and D. Sharma., "Bit priority-based biometric watermarking," in *Proc. IEEE 2nd Int. Conf. Commun. Electron.*, Hoi An, Vietnam, Jun. 2008, pp. 191–195.

[3] D. P. Mukherjee, S. Maitra, and S. T. Acton, "Spatial domain digital watermarking of multimedia objects for buyer authentication," *IEEE Trans. Multimedia,* vol. 6, no. 1, pp. 1–15, Feb. 2004.

[4] A. K. Singh, N. Sharma, M. Dave, and A. Mohan, "A novel technique for digital image watermarking in spatial domain," in *Proc. 2nd IEEE Int. Conf. Parallel Distributed and Grid Computing*, Solan, India, Dec. 2012, pp. 497–501.

[5] W. Wang, A. Men, and X. Chen, "Robust image watermarking scheme based on phase features in DFT domain and generalized radon transformations," in *Proc. 2nd Int. Congr. Image and Signal Process*, Tianjin, China, Oct. 2009, pp. 1–5.

[6] M. N. Sakib, S. B. Alam, A. B. M. R. Sazzad, C. Shahnaz, and S. A. Fattah, "A basic digital watermarking algorithm in discrete cosine transformation domain," in *Proc. 2nd Int. Conf. Intelligent Syst., Modelling and Simulation*, Phnom Penh, Cambodia, Jan. 2011, pp. 419– 421.

[7] K. Deb, M. S. Al-Seraj, M. M. Hoque, and M. I. H. Sarkar, "Combined DWT-DCT based digital image watermarking technique for copyright protection," in *Proc. 7th Int. Conf. Elect. Comput. Eng.*, Dhaka, Bangladesh, Dec. 2012, pp. 458–461.

[8] P. Dabas and K. Khanna, "A study on spatial and transform domain watermarking techniques," *Int. J. Comput. Appl.*, vol. 71, no. 14, pp. 38– 41, May 2013.

[9] A. K. Jain, U. Uludag, and R. L. Hsu, "Hiding a face in a fingerprint image," in *Proc. 16th Int. Conf. Pattern Recognition*, Quebec City, Canada, vol. 3, Aug. 2002, pp. 756–759.

[10] A. K. Jain and U. Uludag, "Hiding biometric data," *IEEE Trans. Pattern Anal Mach. Intell.*, vol. 25, no. 11, pp. 1494–1498, Nov. 2003.

[11] D. Moon, T. Kim, S. H. Jung, Y. Chung, K. Moon, D. Ahn, and S. K. Kim, "Performance evaluation of watermarking techniques for secure multimodal biometric systems," in *Lecture Notes in Computer Science: Computational Intelligence and Security,* Y. Hao et al., Eds. Springer, 2005, vol. 3802, pp. 635–642.

[12] N. Komninos and T. Dimitriou, "Protecting biometric templates with image watermarking techniques," in *Lecture Notes in Computer Science: Advances in Biometrics*, S.-W. Lee and S. Z. Li, Eds. Springer, 2007, vol. 4642, pp. 114–123.

[13] K. R. Park, D. S. Jeong, B. J. Kang, and E. C. Lee, "A study on iris feature watermarking on face data," in *Lecture Notes in Computer Science: Adaptive and Natural Computing Algorithms*, B. Beliczynski, A. Dzielinski, M. Iwanowski, and B. Ribeiro, Eds. Springer, 2007, vol. 4432, pp. 415–423.

[14] M. Vatsa, R. Singh, A. Noore, M. Houck, and K. Morris, "Robust biometric image watermarking for fingerprint and face template protection," *IEICE Electron. Express*, vol. 3, no. 2, pp. 23–28, Jan. 2006.

[15] N. Bartlow, N. Kalka, B. Cukic, and A. Ross, "Protecting iris images through asymmetric digital watermarking," in *Proc. 5th IEEE Workshop Automat. Identification Advanced Technol.*, Alghero, Italy, Jun. 2007, pp.192–197.

[16] C. Y. Low, A. B. J. Teoh, and C. Tee, "A preliminary study on biometric watermarking for offline handwritten signature," in *Proc. IEEE Int. Conf. Telecommun. and Malaysia Int. Conf. Commun.*, Penang, Malaysia, May 2007, pp. 691–696.

[17] M. I. Rajibul, M. S. Shohel, and S. Andrews, "Biometric template protection using watermarking with hidden password encryption," in P*roc. Int. Symp. Inform. Technol.*, Kuala Lumpur, Malaysia, Aug. 2008, pp. 296–303.

[18] B. Ma, C. Li, Y. Wang, Z. Zhang, and Y. Wang, "Block pyramid based adaptive quantization watermarking for multimodal biometric authentication," in *Proc. 20th Int. Conf. Pattern Recognition*, Istanbul, Turkey, Aug. 2010, pp. 1277–1280.

[19] M. Fouad, A. El Saddik, Z. Jiying, and E. Petriu, "Combining cryptography and watermarking to secure revocable iris templates," in *Proc. IEEE Int. Instrumentation and Measurement Technol. Conf., Hangzhou*, China, May 2011, pp. 1–4.

[20] M. R. M. Isa and S. Aljareh, "Biometric image protection based on discrete cosine transform watermarking technique," in *Proc. Int. Conf. Eng. Technol.*, Cairo, Egypt, Oct. 2012, pp. 1–5.

[21] S. Majumder, K. J. Devi, and S. K. Sarkar, "Singular value decomposition and wavelet-based iris biometric watermarking," *IET Biometrics*, vol. 2, no. 1, pp. 21–27, Mar. 2013.

[22] M. Paunwala, and S. Patnaik, "Biometric template protection with DCT- based watermarking," *Mach. Vision Appl.*, vol. 25, no. 1, pp. 263–275, Jan. 2014.

[23] M. Milosavljević and S. Adamović, *Kriptologija II*. Belgrade, Serbia: Singidunum Univ., 2014.

[24] M. Veinović and S. Adamović, *Kriptologija I*. Belgrade, Serbia: Singidunum Univ., 2013.

[25] B. Ma, Y. Wang, C. Li, Z. Zhang, and D. Huang, "Secure multimodal biometric authentication with wavelet quantization based fingerprint watermarking," *Multimedia Tools and Appl.*, vol. 72, no. 1, pp. 637–666, Sept. 2014.

[26] B. Popović, D. Ranđelović, and M. Bunđur, "Izazovi vezani za privatnost i bezbednost prilikom upotrebe biometrike," in *Naučno Stručno Savetovanje Ziteh*, Belgrade, Serbia, 2010. [Online]. Available: https://singipedia.singidunum.ac.rs.

[27] R. Thanki and K. Borisagar, "A novel robust digital watermarking technique using compressive sensing for biometric data protection," *Int. J. Electron. Commun. Comput. Eng.*, vol. 4, no. 4, pp. 1133–1139, July 2013.

[28] P. Bhirud and N. Prabhu, "Secured biometric authentication using visual cryptography and transforms," *Int. J. Comput. Appl.*, vol. 77, no. 8, pp. 23–28, Sept. 2013.

[29] J. Zhao and J. Koch, "Embedding robust labels into images for copyright protection," in *Proc. Int. Congr. on Intellectual Property Rights for Specialized Inform., Knowledge and New Technol.*, Vienna, Austria, Aug. 1995, pp. 242-251.

[30] C.-T. Hsu and J.-L. Wu, "Hidden signatures in images," in *Proc. 3rd IEEE Int. Conf. Image Process.*, vol. 3, Lausanne, Switzerland, Sept. 1996, pp. 223–226.

[31] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data. A state-of-the-art overview," *IEEE Signal Process. Mag.*, vol. 17, no. 5, pp. 20–46, Sept. 2000.

[32] J. R. Hernandez, M. Amado, and F. Perez-Gonzalez, "DCT-domain watermarking techniques for still images: detector performance analysis and a new structure," *IEEE Trans. Image Process.*, vol. 9, no. 1, pp. 55– 68, Jan. 2000.

[33] N. F. Johnson and S. Katzenbeisser, "A survey of steganographic techniques," in *Information Hiding Techniques for Steganography and Digital Watermarking*, S. Katzenbeisser and F. A. P. Petitcolas, Eds. London: Artech House, 2000, pp. 43–78.

[34] M. Abdullah, S. Dlay, and W. Woo, "Securing iris images with a robust watermarking algorithm based on discrete cosine transform," in *Proc. 10th Int. Conf. Comput. Vision Theory and Appl.*, vol. 3, Berlin, Germany, Mar. 2015, pp. 108–114.

[35] J. Lu, T. Qu, and H. R. Karimi, "Novel iris biometric watermarking based on singular value decomposition and discrete cosine transform," *Math. Problems Eng.*, vol. 2014, pp. 1–6, Feb. 2014.

[36] C. Whitelam, N. Osia, and T. Bourlai, "Securing multimodal biometric data through watermarking and steganography," in *IEEE Int. Conf. Technol. for Homeland Security*, Waltham, MA, USA, Nov. 2013, pp. 61–66.

[37] M. Kutter, F. Jordan, and F. Bossen, "Digital signature of color images using amplitude modulation," in *Proc. SPIE, Storage Retrieval for Image Video Databases V*, vol. 3022, pp. 518–526, Jan. 1997.

[38] B. Ma, C. Li, Y. Wang, Z. Zhang, and D. Huang, "Enhancing biometric security with wavelet quantization watermarking based two-stage multimodal authentication," in *Proc. 21st Int. Conf. Pattern Recognition*, Tsukuba, Japan, Nov. 2012, pp. 2416–2419.