

A New Additive Watermarking Technique for Multimodal Biometric Identification

Asad Javed¹, Muhammad Fasihullah¹, Muhammad Akhtar Munir¹, Imran Usman²,
M. Farhan Shafique², Tariq Bashir¹, Mehmood Ashraf Khan²

¹Department of Electrical Engineering, COMSATS Institute of Information Technology, Park Road, Chak Shahzad, Islamabad, Pakistan.

²Center for Advance Studies in Telecommunications, COMSATS Institute of Information Technology, Park Road, Chak Shahzad, Islamabad, Pakistan.

ABSTRACT

This paper presents a new additive watermarking technique for multimodal biometric identification systems comprising four-tier security and repetitive coding based enhanced robustness. In the proposed technique, frontal face information is embedded as a watermark in fingerprint image; the fingerprint features information is then embedded in the iris image of the same individual. This provides availability of features of one modality in other modalities. Thus, providing an additional layer of security, whereby, the host images are used for verification and cross authentication of the individuals in order to secure biometric data. The hidden data are easily and accurately extracted from host images using predefined secret key available in the decoder. The proposed method is robust, viable in biometric systems, and is resistant to common signal processing attacks.

KEYWORDS: additive watermarking, multimodality, fingerprints, facial watermarking.

I. INTRODUCTION

Biometric identification systems have recently gained considerable attention from the research community, since these systems have been used in various commercial applications such as surveillance and access control against potential imposters [1]. Nowadays, multimodality is a new and rapidly developing subject of research in the field of biometrics. Multimodal biometric systems are a type of pattern recognition systems, which identifies an individual on the basis of physiological and/or behavioral characteristics, such as fingerprint, face, iris, retina, palm, speech, and vein [2]. In order to recognize individuals, multi-biometric systems use more than one biometric trait. These systems provide higher recognition rate as compared to uni-biometric systems [3] that rely on only one biometric trait.

The multi biometric modalities for verification, such as fingerprint, iris, and face, are one of the most widely used and effective modalities [4]. Literature reveals that they are more robust, reliable, and efficient as compared to token-based (e.g. key) or knowledge-based (e.g. Password) methods [4]. However, the biometric techniques provide unique data, but the critical problem regarding this kind of data is that they do not endow with security themselves [5]. Biometric data is vulnerable to a number of hostile attacks once it is on the storage system, thus originating the requirement of integrated and inter-modality security [6]. Thus security and integrity of stored information is the major problem in multimodal biometric data.

For securing a multimodal biometric system, three possible techniques (Encryption, Cryptography, and Digital watermarking) are used [7]. Encryption doesn't provide much needed mutually integrated security and is futile once the data is decrypted after being transmitted over some network. Cryptography uses methods of encryption to construct secure information. As encryption and cryptography are not fully capable of providing security throughout the entire life of the work [5], digital watermarking has emerged to fulfill this requirement. Digital watermarking can be used to embed data in host images as watermark, such as hiding company logo in the host image to protect rights of Intellectual Property (IP) [8]. Encryption can also be applied in conjunction with watermarking on biometric templates to increase the level of security.

In recent years, a lot of work has been done on hiding features or image of one biometric modality in another biometric modality of the same subject. As an example, hiding fingerprint image features in face image or any arbitrary image [9], or concealing personal data in fingerprint image [10], or embedding face information into fingerprint image [11, 12]. Nevertheless, one of the major challenges with these approaches is that the induced distortion with watermark embedding sometimes destroys the biometric features of the host image itself. For example, when the face features are embedded into fingerprint image, the features of fingerprint may get disturbed and wrong

*Corresponding Author: Asad Javed, Department of Electrical Engineering, COMSATS Institute of Information Technology, Park Road, Chak Shahzad, Islamabad, Pakistan.

minutiae points may arise. Another problem is that these approaches hide the information in the form of complete image and carry information in the form of features. So when image compression is performed the watermarked features are disturbed and robustness suffers.

In this paper, we implement a four-tier security and enhanced robustness using a new additive watermarking technique. Three biometric images, frontal face, fingerprint, and iris image, of the same individual are used. The proposed technique hides the personal information (watermark) into host images very effectively and efficiently. This allows the host images to be used for verification and the watermarks for cross authentication of the individuals. The watermarked images are easily transmitted over the communication channel without disturbing the hidden data. At the receiving side, the watermarks are accurately extracted using a pre-defined key available in the decoder. The generic framework of the proposed multimodal identification system is shown in Fig. 1.

The rest of the paper is organized as follows. Section 2 presents multimodal biometrics feature extraction techniques. Section 3 describes the proposed watermarking algorithm. The experimental results obtained using additive watermarking is discussed in section 4. Section 5 concludes this paper.

II. MATERIALS AND METHODS

Multimodal Biometrics

The multimodal biometrics algorithm deals with the extraction and recognition of fingerprint minutiae points and frontal face points.

For fingerprint minutiae extraction, the algorithm described in [13] has been used. In this algorithm, a filter of size 3×3 is applied over the thinned fingerprint image. If sum of the filter is 2, then the center pixel is a termination. Similarly, if sum is 4, then the center pixel is a bifurcation. Fingerprint recognition is performed using the algorithm described in [14].

For extraction and recognition of frontal face information, a well known Principal Component Analysis (PCA) based algorithm [15] is used. In this algorithm, the database is created in which all the frontal face images of the same size are present. These images are actually the Eigen faces of the original images.

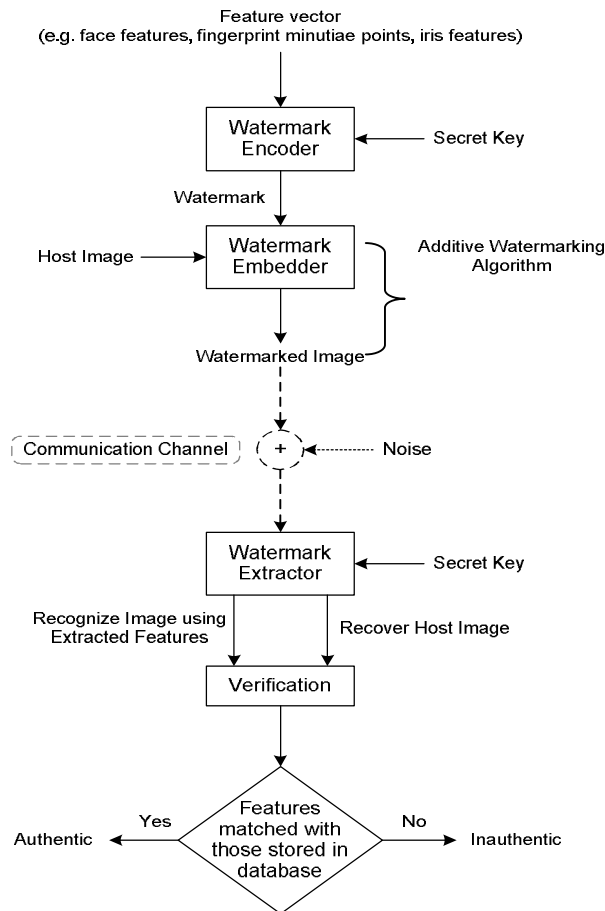


Fig. 1. Basic architecture of the proposed technique

Proposed Watermarking Technique

The watermarking section consists of two phases. In the first phase, the frontal face information is embedded as a watermark in the fingerprint image. Here, the fingerprint image acts as a host/cover image and face information is considered as the watermark. Similarly, in the second phase the fingerprint minutiae points are embedded in the iris image of the same individual. Again, the iris image is used as the cover image and the minutiae point’s acts as a watermark. This algorithm embeds the watermark in Region of Non-Interest (RONI) area, i.e., the portion of an image having meaningless information. Fig. 1 shows the basic architecture of the proposed multimodal watermarking system. Individual modules are elaborated in subsequent subsections.

Phase I (Embedding face features into fingerprint image)

Watermark Encoder

In this module the features vector (frontal face information vector) is converted into a binary image which act as a watermark W. A secret key is used to protect the binary watermark so that no malicious attacker can alter the features or use features for fraudulent purposes. The secret key adds extra layer of security over the binary image.

The size of watermark W depends upon the size of the feature vector. The gray levels present in a feature vector are converted into bits and then the total number of bits occupied by vector decides the size used to construct the watermark. The decimal converted value in first 16 bits of the watermark gives the information of the forthcoming bits stored in the watermark. For robustness, all bits of the vector are repeated in the watermark after every successive set of bits, which is identified by the first 16 bits. This repetitive coding based watermark is used to increase security and introduce robustness, so that if noise disturbs one cluster of bits then another cluster is used to reconstruct the watermark or meaningful information. The output of the watermark encoder block is shown in step 3 of the Watermark Embedder section.

Watermark Embedder

In the second module, we implement additive watermarking technique to accurately embed watermark image or frontal face information into the fingerprint image (which act as a cover image) of the same individual. The steps of this algorithm are given below:

Step 1: A threshold value T for the fingerprint image is calculated using Otsu’s method [16]. This method minimizes the weighted within-class variance using Eq. (1):

$$\sigma_q^2(t) = q_1(t)\sigma_1^2(t) + q_2(t)\sigma_2^2(t) \tag{1}$$

Where: q1, q2 – probabilities of two classes, σ_1, σ_2 - variances of two classes, t – gray scale values.

The class probabilities are estimated as:

$$q_1(t) = \sum_{i=1}^t P(i) \tag{2}$$

$$q_2(t) = \sum_{i=t+1}^I P(i) \tag{3}$$

Where: P – probability of pixels, I – range of grayscale values.

The class variances are estimated as:

$$\sigma_1^2(t) = \sum_{i=1}^t [i - \mu_1(t)]^2 \frac{P(i)}{q_1(t)} \tag{4}$$

$$\sigma_2^2(t) = \sum_{i=t+1}^I [i - \mu_2(t)]^2 \frac{P(i)}{q_2(t)} \tag{5}$$

Where: μ_1, μ_2 are the class means which are computed from the histogram of image using Eq. (6) and (7).

$$\mu_1(t) = \sum_{i=1}^t \frac{iP(i)}{q_1(t)} \tag{6}$$

$$\mu_2(t) = \sum_{i=t+1}^I \frac{iP(i)}{q_2(t)} \tag{7}$$

In order to find the threshold value T, we insert the full range of t values (0 – 255) in Eq. (1) and choose the appropriate gray scale value that minimizes $\sigma_q^2(t)$.

Step 2: The fingerprint image is then converted into binary image using thresholding. Thresholding is a process of image segmentation, which creates binary image using specific threshold value [17]. The result of applying thresholding is shown in Fig. 2. Let $f(x, y)$ be the fingerprint image of size $M \times N$, then binary image $b(x, y)$ can be obtained using Eq. (8).

$$b(x, y) = \begin{cases} 1 & \text{if } f(x, y) \geq T \\ 0 & \text{otherwise,} \end{cases} \quad (8)$$

Where: T – constant threshold value.

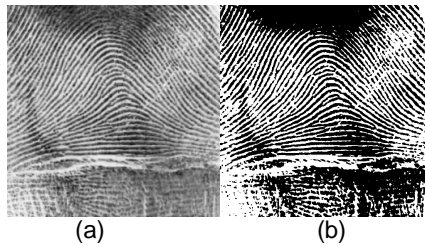


Fig. 2. Result of thresholding; (a) original fingerprint image, (b) Binary image using $T = 0.5608$

Step 3: The watermark in the form of an image is embedded into RONI area. The RONI areas (portion of an image having meaningless information) for fingerprint image are the white lines (i.e. valleys). For embedding of watermark bits, the mask k of size $m \times n$ is applied on the binary fingerprint image b using Eq. (9). Next, we calculate the sum S of the pixels which are occupied by the mask.

$$S = \sum_{s=-l}^l \sum_{t=-w}^w k(s, t) b(x + s, y + t) \quad (9)$$

Where:

$$l = \frac{(m-1)}{2}, \quad w = \frac{(n-1)}{2}$$

The range of x and y is $0 \leq x \leq M$ and $0 \leq y \leq N$ respectively. Fig. 3 illustrates the graphical representation of additive watermarking scheme in which we have a segment of fingerprint image and a mask of size 5×5 . We slide that mask (shown by dashed line) over the binary fingerprint image as shown in Fig. 3(a). Whenever value of S is equal to $m \times n$ or 25 (in case of 5×5 mask), it means that a location (x, y) in the grayscale fingerprint image $f(x, y)$, corresponding to the center of the mask, is the desired location for embedding of watermark bit.

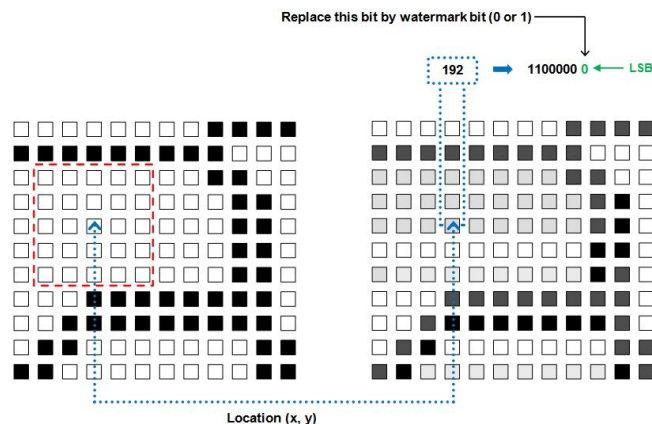


Fig. 3. Graphical representation of additive watermarking technique; a) Segment of binary fingerprint image with 5×5 mask, b) Same segment of grayscale fingerprint image

Now the pixel of grayscale fingerprint image $f(x, y)$ from location (x, y) is extracted and is converted into binary value. The watermark bit is then embedded into the Least Significant Bit (LSB) of the binary value as shown in Fig. 3(b). Next the binary value is converted into the decimal and stored on the same location (x, y) of the fingerprint image $f(x, y)$. We repeat step 3 until all the bits of the watermark are embedded in the fingerprint image. After completion of this procedure we get our required watermarked image as shown in Fig. 4 along with the watermark and original fingerprint image. The watermarked image can then be transferred over some communication channel. The proposed technique is a robust watermarking technique, which ensures that no malicious attacker can alter the features and extract the watermark.

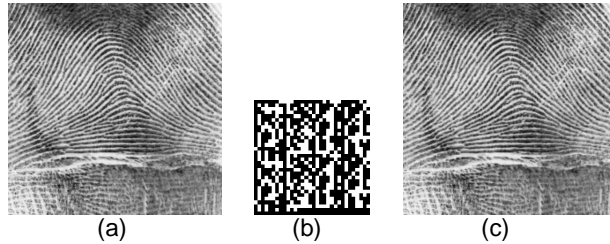


Fig. 4. Watermark embedding in fingerprint image; a) Original fingerprint image, b) Frontal face features in the form of image, c) Watermarked image

Watermark Extraction

At the decoding side, the watermarked fingerprint image is used to verify the individual. For cross authentication of the same individual, we use the watermark which is embedded in the image. So the watermark extractor module is used to extract the watermark using the same secret key in order to decode the watermark.

For extraction, first we convert this watermarked fingerprint image into binary image using step 1 and step 2 of the watermark embedded module as described previously. Then we apply a mask k of size $m \times n$ on binary image b and calculate the sum S of the pixels which are occupied by the mask using Eq. (9). Fig. 5 shows the graphical representation of extraction process performed on a small segment of image with mask of size 5×5 shown by dashed line.

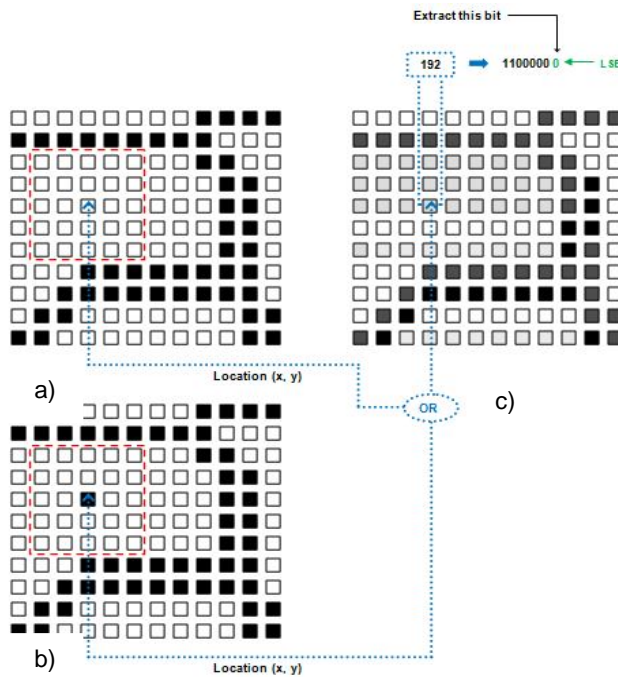


Fig. 5. Graphical representation of watermark extraction process with respect to two cases; a) Segment of binary watermarked fingerprint image w.r.t first case, b) Segment of binary watermarked fingerprint image w.r.t second case, c) Grayscale watermarked image

There are two cases in extraction process. In the first case, whenever center of the mask contains white pixel and value of S is equal to $m \times n$, it means that a location (x, y) in the grayscale fingerprint image $f(x, y)$, corresponding to the center of the mask, is the desired location for extraction of watermark bit as shown in Fig. 5(a). In second case, whenever center of the mask contains black pixel and value of S is equal to $(m \times n) - 1$, it means that a location (x, y) in the grayscale fingerprint image $f(x, y)$ is the desired location for extraction of watermark bit as shown in Fig. 5(b).

Now, after finding the desired location (x, y) , we pick the decimal/grayscale value from that location and convert it into the binary equivalent value. The LSB is then extracted from the binary value and stored in a matrix. The first 16 bits represent the number of forthcoming bits which comprises the watermark. The decimal converted value of these 16 bits also gives the information about the size of the watermark. When all bits are extracted and stored, the process of watermark extraction is completed. Now the decoder decodes the watermark using the predefined secret key. The image is reconstructed and recognized from the features present in watermark image. The host image is also recovered. Both images are used to authenticate a person by comparing the stored images or features in a database.

Phase II (Embedding fingerprint features into iris image)

Watermark Encoder

In this module the feature vector which contains fingerprint minutiae points information is converted into a binary image which acts as a watermark W . The process of making watermark is the same as described in phase I.

Watermark Embedder

In the second module, we implement another type of additive watermarking technique to accurately embed watermark image or minutiae points information into the RONI area of the iris image of the same individual. The RONI area for iris image is the black portion (i.e. pupil). For embedding of watermark bits, first we calculate the mask of the iris image using [18] as shown in Fig. 6. In this mask the black portion represents pupil and the white portion represents the iris.

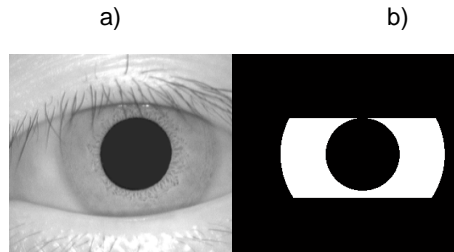


Fig. 6. Result of masking; a) Original iris image, b) Mask of iris image

Next, we start from the top left corner of an iris image and embed the watermark bits on those locations of grayscale iris image where the mask contains the black pixels. The pixel of iris image is extracted from that location and is converted into binary value. The watermark bit is then embedded into the LSB of the binary value. Rest of the embedding process is the same as described in phase I. The watermarked image in this phase is shown in Fig. 7.

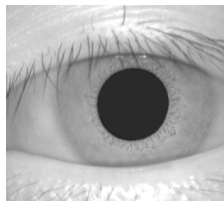


Fig. 7. Watermarked image containing fingerprint features information.

Watermark Extraction

At the decoding side, the watermarked iris image is used for verification and cross authentication of the individuals. So, first we extract the watermark information from the iris image and then the same predefined secret key is used to decode the watermark.

For extraction of the watermark, first we calculate the mask of iris image using algorithm described in [18]. Next, we extract the watermark bits from those locations of the watermarked iris image where the similar locations of the mask contain black pixels. We start from the top left corner and extract 16 LSBs from the first 16 grayscale pixels of the watermarked iris image. These 16 bits represent the number of forthcoming bits which would be extracted as the watermark. When all bits are extracted and stored, the process of watermark extraction is completed. The rest of the process is same as described in phase I.

III. RESULTS AND DISCUSSION

In this section, some experimental results are demonstrated to illustrate the robustness and imperceptibly performances of our proposed additive watermarking technique. The results shows that the watermarked image is perceptually equal to the original image, and also the extracted features are same as compared to watermarked

features. We also evaluate the result on the basis of Peak Signal-to-Noise Ratio (PSNR) value. The PSNR value is used to estimate the quality of watermarked images. When the PSNR value is greater than 45db [19], it is considered as perceptually acceptable to the human eye.

Table 1 shows different fingerprint images along with PSNR value. According to this table, the value of PSNR is extremely greater than 45db. Table 2 illustrates different iris images along with PSNR values. This table also has PSNR values much greater than 45db. In both the tables, the original images and the watermarked images are perceptually equal due to our proposed watermarking technique. These results depict that the watermarked images are imperceptible and human visual system cannot discriminate between the original image and the watermarked image.

Table 1. Comparison of watermarked fingerprint images with original fingerprint images using PSNR value.













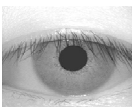

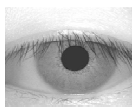

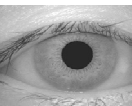

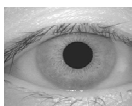

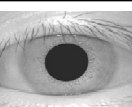

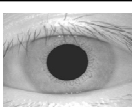

Sr. No.	Original Image	Watermark	Watermarked Image	Extracted Watermark	PSNR
1					82.2730
2					75.5315
3					76.1476

Table II: Comparison of watermarked iris images with original iris images using PSNR value.

Sr. No.	Original Image	Watermark	Watermarked Image	Extracted Watermark	PSNR
1					71.4839
2					63.3386
3					68.7218

IV. CONCLUSION

This paper proposes a new additive watermarking algorithm to present four-tier security, whereby, the frontal-face features are embedded as a watermark in fingerprint image; the fingerprint features information is then embedded in the iris image of the same individual. For robustness, the repetitive coding based technique is used in which we embed the whole watermark on different locations in the host image. This watermark image is embedded into the Region of Non-Interest (RONI) portion of the host image to increase imperceptibility. Experimental results demonstrate that the proposed algorithm produces enhanced and acceptable results and is more robust to signal processing attacks. In future we intend to incorporate machine learning approaches for intelligent attack resistant multimodal biometric watermarking systems.

REFERENCES

- [1] Xiao Q., "Security issues in biometric authentication," *Proc. IEEE, Information Assurance Workshop, IAW'05*, pp. 8 – 13, June 2005.
- [2] Arun A. Ross, Karthik Nandakumar, Anil K. Jain, "Handbook of Multibiometrics," Springer, 2006.
- [3] Nagar A., Nandakumar K., Jain A. K., "Multibiometric Cryptosystems Based on Feature-Level Fusion," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 255 – 268, Feb. 2012.
- [4] Nageshkumar M., Mahesh P. K., M. N. Shanmukha, "An Efficient Secure Multimodal Biometric Fusion Using Palmprint and Face Image," *IJCSI International Journal of Computer Science Issues*, vol. 2, Aug. 2009.
- [5] Jain A. K., Uludag U., "Hiding Biometric Data," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 25, no. 11, pp. 1494 – 1498, Nov. 2003.
- [6] Won-gyum Kim, HeungKyu Lee, "Multimodal biometric image watermarking using two-stage integrity verification," *ELSEVIER Signal Processing*, vol. 89, no. 12, pp. 2385 – 2399, Dec. 2009.
- [7] Ruud M. Bolle, Jonathan H. Connell, Sharath Pankanti, Nalini K. Ratha, Andrew W. Senior, "Guide to Biometrics", *Springer*, 2003.
- [8] Hartung F., Kutter M., "Multimedia watermarking techniques," *Proc. IEEE*, vol. 87, no. 7, pp. 1079 – 1107, Jul. 1999.
- [9] A. K. Jain and U. Uludag, "Hiding Fingerprint Minutiae in Images," *Proc. Third Workshop on Automatic Identification Advanced Technologies (AutoID)*, pp. 97 – 102, Mar. 2002.
- [10] Nalini K. Ratha, Jonathan H. Connell, Ruud M. Bok, "Secure data hiding in wavelet compressed fingerprint images," *Proceedings of ACM Multimedia Workshops*, pp. 127 – 130, 2000.
- [11] Jain A. K., Uludag U., Rein-Lien Hsu, "Hiding a Face in a Fingerprint Image," *Proc. IEEE, 16th International Conference on Pattern Recognition*, vol. 3, pp. 756 – 759, 2002.
- [12] Umut Uludag, Bilge Günsel, Meltem Ballan, "A Spatial Method for Watermarking of Fingerprint Images," *Proc. 1st Intl. Workshop on Pattern Recognition in Information Systems*, 2001.
- [13] Yusra AI-Najjar and Alaa Sheta, "Minutiae Extraction for Fingerprint Recognition," *5th International Multi-Conference on Systems, Signals, and Devices*, 2008.
- [14] F. Chen, J. Zhou, and C. Yang, "Reconstructing Orientation Field From Fingerprint Minutiae to Improve Minutiae-Matching Accuracy," *IEEE Transactions On Image Processing*, vol. 18, no. 7, July 2009.
- [15] M. Turk and A. Pentland, "Eigenfaces for Recognition," *Journal of Cognitive Neuroscience*, vol. 3, no. 1, 1991.
- [16] Otsu, N., "A Threshold Selection Method from Gray-Level Histograms," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 9, no. 1, pp. 62-66, 1979.
- [17] Gonzalez, Rafael C. & Woods, and Richard E, (2002). Thresholding. In *Digital Image Processing*, pp. 595–611. Pearson Education.
- [18] Libor Masek and Peter Kovesi, "MATLAB Source Code for a Biometric Identification System Based on Iris Patterns," The School of Computer Science and Software Engineering, The University of Western Australia, 2003.
- [19] Welstead and Stephen T., "Fractal and wavelet image compression techniques," *SPIE Publication*, pp. 155–156, 1999.