Fingerprint Image Watermarking in Spatial, Frequency and Multiresolution domain: Techniques and challenges

Mohamed Lebcir
Faculty of Computer Systems & Software Engineering.
University Malaysia Pahang, UMP
Lebuhraya Tun Razak 26300, Kuantan, Pahang, Malaysia
mlebcir78@gmail.com

Suryanti Awang
Faculty of Computer Systems & Software Engineering.
University Malaysia Pahang, UMP
Lebuhraya Tun Razak 26300, Kuantan, Pahang, Malaysia
suryanti@ump.edu.my

Abstract— Fingerprint biometric system has been used as a personal authentication in many fields including law enforcement, business, *etc*. Fingerprint digital watermarking technique is implemented to increase the fingerprint security in terms of its originality. Thus, a number of related research studies have been analyzed in this paper. Three embedding domains are more commonly studied which are spatial domain, frequency domain and the multiresolution domain. These are used to implement the watermarking technique in fingerprint images. The strength and weakness of each technique in these embedding domains are discussed in this paper. This paper is categorized based on the domains. The most appropriate domain to implement the digital watermarking in fingerprint image combines between frequency and multiresolution due to the two domain advantages. The challenges of the fingerprint digital watermarking implementation are discussed in this paper as well based on the finding of the strength and weakness. We can conclude that the main challenges of this implementation are blind and more robust against a geometric attack like translations or rotations with the aim to provide higher security and robustness without corrupting minutiae points. This is because the fingerprint features can be easily affected by the incorporated watermark. In addition, a different set of features may be introduced due to displacements and rotations of the fingerprints.

Keywords— Fingerprint Image; Digital Watermarking; Computational Intelligence

1. INTRODUCTION

Biometric is a growing field which is associated with distinguishing individuals. Through biometrics, individuals can be easily identified based on their biological (such as fingerprint) or physiological (such as voice) features. Biometrics is more reliable compared to the conventional verification approaches such as the knowledge-based or the token-based methods. This is because the conventional methods can be easily lost, forgotten or even stolen [1].

One of the most commonly used biometric-based identification techniques is the fingerprint recognition method. This is due to its high dependability and uniqueness. During the recognition step, a large proportion of fingerprint-based authentication processes often apply minutiae matching. This approach depends primarily on the features and patterns of minutiae points present in the fingerprint.

It is worthy of note that despite the very many advantages of the fingerprint authentication approach, it faces certain shortcomings [2]. For instance, there is possibility of using false or forged fingerprint images to gain access to a system through some spoofing techniques [3]. Moreover, if by chance an authentic fingerprint sample which was initially used in an application is altered, it can present serious issues to every other application used by the sample. This is mainly due to the fact that it is impossible to either cancel or replace the fingerprint features.

Interestingly, the use of digital watermarking can help to certify the credibility of fingerprints [4]. The fundamental principle of digital watermarking technique is to insert watermark data into the authentic fingerprint image in order to safeguard the fingerprint. In another vein, a second protection later may be incorporated by encoding the watermark data prior to inserting the watermark [5]. Therefore, this would help to protect the watermark from being altered by unauthorized persons or attackers. As such, the originality of the fingerprint image is preserved and any alterations to the image of the watermarked-fingerprint can be observed by checking for changes in the watermark. In general, the notable characteristic features of the watermarking technique include good stability, large capacity and imperceptibility [6]. Good stability, otherwise called robustness denotes the ability of watermarking algorithm to conserve the watermark data regardless the nature of attacks. The possible types of attack include cropping, scaling, rotation and translation. Watermarking algorithm exhibits large capacity in the sense that there is a possibility to embed large numbers of bit into original image without deteriorating it. On the other hand, imperceptibility means that messages on the watermark are often beyond the human visual perception [6,7]. Therefore, based on its potentials, there are increasing interests on the use of watermarking techniques to protect and preserve the originality of fingerprint images.

2. FINGERPRINT WATERMARKING TECHNIQUES

One of the widely investigated approaches for protecting fingerprint images is digital watermark algorithm. However, a good watermark method should exhibit some specific characteristic features as reported in literature [8]. Consequently, some notable challenges have been recently identified in connection with the available techniques for fingerprint watermarking. The main aim of this paper is to review various approaches which have been used to embed watermark into fingerprints. The subsequent sections will present these domains in connection to different techniques which have been used for fingerprint watermarking.

A. The Fingerprint Watermarking Embedding Techniques in Spatial Domain

The spatial domain of embedding fingerprint watermark represents the domain for direct application of watermark images into the pixels of the host image. In this case, image of the watermark is directly embedded into the pixels of the host image [9]. One notable approach which is commonly used for watermarking in the spatial domain involves the substitution of the least significant bits (LSBs) with more significant bits in the image pixel [10].

Among the notable researches on this domain is a fragile authentication technique is watermarking fingerprint images was proposed by Pankanti and Yeung [11]. In their research, an authentication key is used to embed a watermark into a fingerprint image in the spatial domain. The method proposed has the ability to pinpoint any part of the image which has been altered. The conclusion from their study states that their watermarking approach does not present observable loss to the process of the fingerprint authentication. However, the technique is not suitable for protected fingerprint sample transmission over network that are not secure. This is due to the high vulnerability of embedded watermarks towards attackers [11].

In another research, a method was presented by Gunsel *et al*. [12] and Uludag *et al*. [13]. This method safeguards the orientation of the quantized gradient in the domain of the embedded watermark. Two techniques for fingerprint image watermarking in the spatial domain were described by Gunsel *et al*. [12]. The first approach makes use of gradient orientation analysis during the process of embedding the watermark. Hence, none of the features extracted by making use of gradient information is altered. Likewise, the second technique conserves the singular points within the fingerprint image. Therefore, there is no disruption to the classifications of the fingerprint image that is watermarked using this approach. In similar manner, Uludag *et al*. [13] put forward a spatial method for embedding watermarking fingerprint images without ruining the features of the fingerprint. With this approach, the characteristic features of the fingerprint are first detected. The watermark is then embedded into the fingerprint image in such a way that the fingerprint features are not distorted by the watermark. Actually, it is not fully understood if this method could trigger potential changes in the features of the fingerprint after the incorporation of the watermark data, or whether the features shall be retained. However, the entire single points as well as features of the fingerprint which are extracted using gradient information are secured within the fingerprint image.

In a different research, incorporation of a facial image was proposed to be hidden in the fingerprint image Jain *et al*. [14]. This method involves inserting a user face's eigenface coefficients in the fingerprint image. Hence, during the process of decoding, the recovered facial image may be used to ascertain the originality of the image. In their research, the information from the user face is primarily used to verify the fingerprint image. A secret key is randomly generated and one bit stream of the coefficients of the eigenface is then inserted into the pixels of selected fingerprint image [14]. The process of embedding the face is done in the spatial domain. Hence it does not depend on the original image in order to extract the watermark (blind). The main shortcoming of this approach is the fact that it mainly works in the spatial domain and as such, the embedded watermarks is highly vulnerable to attack. This is because spatial domain uses direct values of image pixels.

In a similar approach, a scheme of watermarked spatial fingerprint which used eigenfaces was proposed [15]. The watermark is embedded into the fingerprint through steganography in the 'sailboat' image. The solution is aimed at inscribing black squares around the minutiae in order to denote the ones that need to be dodged during the watermarking phase. After evaluation, this technique is proven to reveal good performance especially towards authentication and protection of fingerprint minutiae following the watermarking process. In addition, the use of steganography is found to curtail fingerprint piracy. There is challenge computational complexity. This is mainly due to the fact that a long duration of time would be required to process a combined watermarking and steganography procedure. Another drawback of this approach is that the spatial embedding domain is not sufficiently resistant to factors such as compression, noise as well as filtering attacks [16]. This is associated with the fact that the pixels are changed thereby sacrificing the image quality.

Furthermore, Bousnina *et al*. [17] introduced a new method of embedding watermark into fingerprint. This involves the use of a secretly generated key to identify which pixels to be watermarked. After this, the face features (watermark) is then inserted into the fingerprint image (cover) such that the fingerprint minutia points are preserved through the help of Orthogonal Locality Preserving Projections (OLPP) method [17]. This method was verified mainly against watermarking attacks notable for digital images. This includes median filter, Speckle noise, Gaussian noise and Poison noise. Hence, its resistance strength was not investigated against other potential attacks such as geometric attacks. It is well known that for digital watermarking, the most common form of attack is the geometric attack. Geometric attach could be in form of either scaling, rotation, scaling or translation [18]. Hence, geometric attacks should necessarily be evaluated in order to reduce the strength or robustness of the approach.

Based on information gathered here, it may be noted that spatial domain methods manifest less complications coupled with high payload. Unfortunately, they are not sufficiently robust against the common forms of image processing attacks such as compression. In addition, this approach is highly vulnerable to piracy attacks as the watermark can be easily modified during the process of watermarked image transmission between a sender and a receiver.

B. The Fingerprint Watermarking Embedding Techniques in Frequency Domain

The frequency domain denotes the rate of change in the values of pixel at the spatial domain. In the frequency domain, insertion of watermarks is made into the image transform coefficients. Herein, an inverse transformation is used to rebuild the watermarked image [9]. The commonly used watermarking transformation techniques in frequency domain are the Fast Fourier Transform (FFT) technique, and the Discrete Cosine Transform (DCT) [9]. The subsequent section will present a review on the available techniques of embedding watermark into fingerprint in the frequency domain.

In a particular research, a technique for inserting two watermarks into fingerprint images was proposed by Alkhathami *et al*. [8]. The technique uses Discrete Cosine Transform (DCT) algorithm [8]. Although their approach is blind, but the robustness was tested using only noise attacks. It is however necessary that the robustness of the technique needs to be verified against different type of attacks especially geometric attacks.

In another study, a technique which is based on a Fuzzy-Particle Swarm Optimization was put forward by Bansal *et al*. [19] for fingerprint watermarking. This technique was applied to secure the fingerprint image of an individual by watermarking its analogous face image [19]. Verification of the robustness of this approach was only confirmed for certain potential watermarked image attacks such as noise, JPEG compression and sharpening. However, it was not verified against other possible attacks especially the geometric ones such as rotations and translations.

Therefore, the use of DCT algorithms for embedding watermark into fingerprint image does not reveal sufficient robustness against geometric transformations such as rotations or translations. Unfortunately, this transformation often affects coefficient of many DCT algorithms. Hence fingerprint watermarking through DCT algorithm in the frequency domain is limited in its efficiency.

C. The Fingerprint Watermarking Embedding Techniques in Multiresolution Domain

The multiresolution domain is a term which is used mainly in the context of spatial frequency. It is referred as the (inverse of the) periodicity in respect to changes in the intensity values of the image. In general, high spatial frequency image characteristics (such as edges) are the ones wherein there is a great change in the intensity within a short image distance [20]. In short, multiresolution domain transformation presents an embedding domain to the watermark both in the spatial as well as the frequency domain. The notable transformations used in the multiresolution domain are the contourlet transform (CT), and the Discrete Wavelet Transform (DWT) [9]. The subsequent paragraphs present the notable studies on the technique used for embedding watermark in the multiresolution domain.

An embedded watermarking procedure in the wavelet domain was presented by [21]. A watermark is inserted into a compressed wavelet scalar quantization (WSQ) fingerprint image. During the WSQ encoding, individual coefficients of the wavelet transform are changed with consideration on the potential image degradation. It is interesting that this approach is a blind method, with the added advantage of operating in multiresolution domain. However, the major shortcoming of this technique is that security data are vulnerable to attackers [21]. Since attackers can gain easy access to security data under this technique, it is believed that it is only hidden by the secrecy of the algorithm.

Similarly, a watermarking approach which is based on wavelet was proposed by Zebbiche *et al*. in which watermarks are inserted into DWT coefficient via quantization [22]. The method is considered blind and it has high robustness to additive noise and compression. In fact, it has reasonable moderate linear mean filtering resilience. Notwithstanding the method was not verified against rotation and other common geometric attacks.

An algorithm was proposed by Noore *et al.* [23]. which uses DWT and capable of multiple fingerprint watermarking especially in the texture regions. In their study, face and text information were used as watermark [23]. However, their technique is resilience against common attacks such as noise, compression and filtering. It was not verified against geometric attacks.

Similar to this, a technique for fingerprint watermarking was put forward by Cao *et al*. wherein CT and TC (Texture Complexity) are used for choosing the optimum blocks where the watermark may be embedded [24]. Comparison of fingerprint face accuracies was mainly used to evaluate the robustness of their watermarking algorithm [24]. However, it is viewed that there are possibilities for watermarked fingerprint images to be affected by several other attacks.

A blind algorithm in the contourlet domain for watermarking was put forward by Kumar *et al*. [25] and the algorithm does not depend on original template of the fingerprint at extraction. In their approach, Iris code was primarily used as the watermark [25]. However, the influence of the extraction of biometric feature was evaluated only by adding noise attacks to verify the robustness of their algorithm. Therefore, testing of the robustness of their algorithm is considered incomplete.

In a different approach, a Particle Swarm Optimization (PSO) method was used by Bansal *et al*. [26]. The underlying principle behind their approach is the use of PSO to identify the best coefficients of DWT where there is possibility of embedding the facial image data to hide the face image’s pixel data. However, this approach cannot be certified is capable of retaining original fingerprint features as it was not verified against most of the conventional geometric and digital watermarking attacks.

In a research by Ma *et al* [27], a technique for watermarking which is based on wavelet quantization was proposed. In their approach, information is robustly inserted into fingerprints without jeopardizing the characteristic features [27]. This Significant Difference Parity Quantization (SDPQ) method is able to enhance the insertion of robust information especially in cases which require high data payload and good robustness. However, this approach is thought to be too complex as it requires more than one framework of authentication step in order to the security of the biometric system. Hence it is considered time wasting due to the long processing time required.

An approach based on wavelet was introduced by Ghany *et al*. for embedding DNA data based multi-bit watermark into fingerprint images [28]. The method is robust and straightforward, but it requires the original fingerprint template at the extraction stage (non-blind). The attackers can use the original secure data to attack the system.

Alkhathami *et al*. developed a watermarking algorithm to embed into fingerprint images with unique minutiae in order to prevent it from possible effects on embedded watermark [29]. This technique uses a new Dual-tree Complex Wavelet Transform (DTCWT) and it presents desirable advantages especially for protecting the fingerprint minutiae from potential embedded watermark effects. However, this algorithm is non-blind. So the original image is needed to extract the watermarks. This exposes the original data to be easily accessed by potential attackers during process of transmitting the watermarked image from sender to the receiver.

A simple blind technique which uses DWT for watermarking and digital image detection was put forward by Abraham *et al*. [30]. The proposed method is blind as the original fingerprint template is not required at the extraction stage (blind). In addition, the robustness of embedded information in this approach is reasonable. However, it can only withstand some specific types of attacks like noise addition and histogram equalization. There is no complete evaluation of robustness.

A comparative study was carried out by Haddada *et al*. [9] wherein the watermark may be inserted such that the minutiae could be preserved both in terms of its number as well as its positions. The approach presents a new biometric fingerprint watermarking technique which uses the facial Gabor characteristic features which are reduced by the Direct Linear Discriminant Analysis Technique (DLDA) method. However, the flaw of this proposed method is that it was not tested under rotation and other geometrical attacks. Therefore, the robustness is not completely evaluated to justify its capability to preserve the numbers and positions of the minutiae, better than other approaches.

In general, it was observed that the highlighted techniques offers better robustness and higher image imperceptibility. Specifically, the DWT has been more regularly used in digital image watermarking. This is based on its time/frequency decomposition characteristics which is considered similar to the visual systems of human theoretical models as against the other transform from previous methods [9]. However, as stated in the previous paragraphs, most of the approaches did not present complete evaluation of the robustness especially against rotation and the other geometric attacks.

D. The Fingerprint Watermarking Embedding Techniques in Hybrid Domain

Asides the general approach of embedding watermark in a single domain, there are other studies wherein two domains (hybrid domain) have been explored. For example, hybrid spatial and frequency domain, hybrid spatial and multiresolution domain or hybrid frequency and multiresolution domain [31, 32]. The subsequent paragraphs will present notable among the available fingerprint watermarking procedures in hybrid domain.

In a particular research, an approach was put forward by Vasta *et al.* which combines DWT and Least Significant Bit (LSB) methods to embed watermark into fingerprint. In their approach, a facial image was inserted into the fingerprint image through the use of combined LSB and wavelet techniques [33]. Notably, the approach based on wavelet is particularly robust against frequency related attacks. On the other hand, LSB is susceptible to geometric attacks. The proposed algorithm was verified for its recognition accuracy with respect to different forms of image operation. These operations include transformation, Gaussian noise, JPEG 2000 compression, rotation, resizing, median filtering rotation, and cropping. The result revealed that the algorithm is robust against most of the evaluated potential attacks. However, the security at the spatial domain is not strong enough to resist easy access of secret data by attackers.

In another study, Zebbiche *et al*. [34] put forward a digital watermarking technique which is based on DCT and DWT to insert an identification number into fingerprint images. It was observed that the technique was not fully blind. In addition, a complex technique known as decoding is involved in the extraction stage. Specifically, the technique was tested against a number s possible attacks like compression noise adding and filtering. However, it was not verified against rotation and the other notable geometric attacks.

In a separate research, a watermarking technique was proposed by Alkhathami *et al*. [29] which combines the features of DWT and DCT techniques. These were combined incorporate the fingerprint owner's grayscale facial image and other identification details in the model of binary text image, into the fingerprint image [29]. The results obtained from this study indicated that incorporation of more than one watermark images of different sizes did not corrupting the minutiae. However, it is often necessary to evaluate the robustness of the proposed algorithm against various potential image attacker of such algorithm. Hence, the algorithm may be considered good if it achieves high payload without corrupting the minutiae points.

Based on the review presented, it can be inferred that watermarking in hybrid domain of combined frequency and multiresolution domains helps to preserve the minutiae points. Hence it is more desirable compared with other hybrid domain systems. However, this approach requires original data for the extraction step which means it is not blind. Due to this, there is less security to the fingerprint such that it is not protected from piracy during transmission between sender and receiver. Hence, the original data can be easily detected and modified.

3. CONCLUSION

Based on aforementioned, most of the existing fingerprint image schemes demonstrate robustness against some categories of attacks. However, they failed to perform well against other types of attacks such as geometric transformations like translations or rotations. This is because the watermarking properties exhibit contradicting characteristic features. Therefore, an increase in the robustness of a watermark would typically lead to reduction in its ability to preserve the minutiae points. This may be attributed to the imposition of higher watermark energy on the fingerprint image. Hence, increasing of payload to embedding watermarks would corrupt its minutiae points because more modifications the fingerprint image are needed to embed the watermark. Based on the results that were recorded in fingerprint image watermarking techniques, both multiresolution and hybrid (frequency / multiresolution) domains are the best especially due to their capability to preserve the minutiae number at the extraction stage. These embedding domains offer good verification performances. In addition, it presents a desirable compromise between robustness and imperceptibility. However, the underlying challenge now is on how to enhance the robustness of the fingerprint watermarking procedure against most of the geometric attacks such as translations or rotations without a need for the original fingerprint template at the extraction stage (blind). This would help to provide higher security and robustness without corrupting minutiae points.

ACKNOWLEDGMENT

We would like to show our gratitude to University Malaysia Pahang (RDU vote number RDU180380) for supporting this study.

REFERENCES

[1] S. Awang, R. Yusof, M.F. Zamzuri, R. Arfa, “Feature level fusion of face and signature using a modified feature selection technique,” in: Proceedings - 2013 International Conference on Signal-Image Technology and Internet-Based Systems, SITIS 2013, 2013: pp. 706–713.

[2] N.K. Ratha, S. Chikkerur, J.H. Connell, R.M. Bolle, “Generating cancelable fingerprint templates,” IEEE Transactions on Pattern Analysis and Machine Intelligence. 29 (2007) 561–572.

[3] T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, “Impact of artificial gummy fingers on fingerprint systems,” in: Proceedings of Society of Photo-Optical Instrumentation Engineers, SPIE 2002, 2002: pp. 275–289. A. Noore, R. Singh, M. Vatsa, M.M. Houck, “Enhancing security of fingerprints through contextual biometric watermarking,” Forensic Science International. 169 (2007) 188–194.

[4] A. Noore, R. Singh, M. Vatsa, M.M. Houck, “Enhancing security of fingerprints through contextual biometric watermarking,” Forensic Science International. 169 (2007) 188–194.

[5] S.M. Mousavi, A. Naghsh, S.A.R. Abu-Bakar, “Watermarking techniques used in medical images: a survey,” Journal of Digital Imaging. 27 (2014) 714–729.

[6] V.M. Potdar, S. Han, E. Chang, “A Survey of Digital Image Watermarking Techniques,” International Conference on Industrial Informatics. (2005) 709–716.

[7] M.S. Subhedar, V.H. Mankar, “ScienceDirect Current status and key issues in image steganography: A survey,” Computer Science Review. 13–14 (2014) 95–113.

[8] M. Alkhathami, F. Han, R. Van Schyndel, “Fingerprint image protection using two watermarks without corrupting minutiae,” in: Proceedings of the 2013 IEEE 8th Conference on Industrial Electronics and Applications, ICIEA 2013. (2013) 1151–1155.

[9] L.R. Haddada, I.H. Trimech, N.E. Ben Amara, “A biometric watermarking approach of fingerprint images by DLDA Gabor face features without altering minutiae,” in: Proceedings of IPAS 2016 - 2nd International Image Processing, Applications and Systems Conference. IPASC 2017. (2017) 1–6.

[10] F.Y. Shih, S.Y.T. Wu, “Combinational image watermarking in the spatial and frequency domains,” Pattern Recognition. 36 (2003) 969–975.

[11] M.M. Yeung, S. Pankanti, “Verification watermarks on fingerprint recognition and retrieval,” Journal of Electronic Imaging. 9 (2000).

[12] B. Gunsel, U. Uludag, A. Murat Tekalp, “Robust watermarking of fingerprint images,” Pattern Recognition. 35 (2002) 2739–2747.

[13] U. Uludag, B. Günsel, M. Ballan, “A Spatial Method for Watermarking of Fingerprint Images,” in: Proceedings of the 1st International Workshop on Pattern Recognition in Information Systems, PRIS 2001. (2001) 26–33.

[14] A. K. Jain, U. Uludag, R.-L.H.R.-L. Hsu, “Hiding a face in a fingerprint image,” Object Recognition Supported by User Interaction for Service Robots. 3 (2002) 756–759.

[15] A.K. Jain, U. Uludag, “Hiding biometric data,” IEEE Transactions on Pattern Analysis and Machine Intelligence. 25 (2003) 1494–1498.

[16] J.R. Aparna, S. Ayyappan, “Image watermarking using Diffie Hellman key exchange algorithm,” Procedia Computer Science. 46 (2015) 1684–1691.

[17] N. Bousnina, S. Ghouzali, M. Lafkih, O. Nafea, M. Mikram, W. Abdul, D. Aboutajdine, “Watermarking for protected fingerprint authentication,” in: Proceedings of 12th International Conference on Innovations in Information Technology. IIT 2016. (2016) 127–131.

[18] P. Singh, R. Chadha, “A Survey of Digital Watermarking Techniques, Applications and Attacks,” International Journal of Engineering and Innovative Technology. 2 (2013) 165–175.

[19] R. Bansal, P. Sehgal, V. Bhasin, P. Bedi, “Multi-agent system for intelligent watermarking of fingerprint images,” IEEE International Conference on Fuzzy Systems. (2013) 1-8.

[20] R. Fisher, S. Perkins, A. Walker, E. Wolfart, “Hypermedia image processing reference,” England: John Wiley & Sons Ltd. (1996).

[21] N.K. Ratha, J.H. Connell, R.M. Bolle, “Secure data hiding in wavelet compressed fingerprint images,” in: Proceedings of the 2000 ACM Workshops on Multimedia. (2000) 127–130.

[22] K. Zebbiche, L. Ghouti, F. Khelifi, A. Bouridane, “Protecting fingerprint data using watermarking,” in: Proceedings of the Adaptive Hardware and Systems, 2006. AHS 2006. (2006) 451–456.

[23] A. Noore, R. Singh, M. Vatsa, M.M. Houck, “Enhancing security of fingerprints through contextual biometric watermarking,” Forensic Science International. 169 (2007) 188–194.

[24] Y. Cao, W. Gong, M. Cao, S. Bai, “Robust biometric watermarking based on Contourlet transform for fingerprint and face protection,” in: Proceedings of ISPACS 2010 - 2010 International Symposium on Intelligent Signal Processing and Communication Systems. ISPACS 2010. (2010) 10–13.

[25] N.K. Kishore Kumar, V.S. Sheeba, “Blind biometric watermarking based on contourlet transform,” in: Proceedings of 2012 3rd International Conference on Computing, Communication and Networking Technologies, ICCCNT 2012. (2012).

[26] R. Bansal, P. Sehgal, P. Bedi, “Securing Fingerprint Images Using PSO-Based Wavelet Domain Watermarking,” Information Security Journal. 21 (2012) 88–101.

[27] B. Ma, C. Li, Y. Wang, Z. Zhang, D. Huang, “Enhancing Biometric Security with Wavelet Quantization Watermarking based Two-stage Multimodal Authentication,” International Conference on Pattern Recognition. (2012) 2416–2419.

[28] K.K.A. Ghany, G. Hassan, A.E. Hassanien, H.A. Hefny, G. Schaefer, A.R. Ahad, “A Hybrid Biometric Approach Embedding DNA Data in Fingerprint Images,” in: Proceedings of the 2014 International Conference on Informatics, Electronics & Vision, ICIEV 2014. (2014) 1–5.

[29] M. Alkhathami, “Watermarking techniques for genuine fingerprint authentication,” in: Proceedings of the 12th International Conference on Innovations in Information Technology, IIT 2015. (2015) 127-131.

[30] J. Abraham, V. Paul, “A blind watermarking method for fingerprinting digital images,” in: Proceedings of 2016 International Conference on Data Mining and Advanced Computing, SAPIENCE 2016. (2016)145–149.

[31] R. Thanki, K. Borisagar, “ScienceDirect Sparse Watermarking Technique for Improving Security of Biometric System,” Procedia - Procedia Computer Science. 70 (2015) 251–258.

[32] U.H. Panchal, R. Srivastava, “A comprehensive survey on digital image watermarking techniques,” in: Proceedings of the 2015 Fifth International Conference On Communication Systems and Network Technologies, CSNT 2015, (2015) 591–595.

[33] M. Vatsa, R. Singh, A. Noore, M.M. Houck, K. Morris, “Robust biometric image watermarking for fingerprint and face template protection,” IEICE Electronics Express. 3 (2006) 23–28.

[34] K. Zebbiche, F. Khelifi, A. Bouridane, “An efficient watermarking technique for the protection of fingerprint images,” Eurasip Journal on Information Security. 2008 (2008).