A Review on Type of Attacks on Fingerprint Image and Watermarking Techniques

IOP Conf. Series: Materials Science and Engineering **551** (2019) 012071 doi:10.1088/1757-899X/551/1/012071

A Review on Type of Attacks on Fingerprint Image and Watermarking Techniques

Mohamed Lebcir[1], Suryanti Awang[1]

[1]Soft Computing & Intelligent Systems Research Group (SPINT), Faculty of Computer Systems & Software Engineering, University Malaysia Pahang, UMP, Lebuhraya Tun Razak 26300, Kuantan, Pahang, Malaysia.

E-mail: mlebcir78@gmail.com, suryanti@ump.edu.my

Abstract. Fingerprint image watermarking techniques have several advantages over traditional security systems that based on token or knowledge. However, they are also vulnerable to attacks that can decrease their security. In this regard, this paper presents a study of a number of research studies on the attacks of fingerprint images watermarking techniques. The attacks can be categorized into intentional and unintentional. We study several attacks based on that category and several fingerprint image watermarking methods. We produce a comprehensive comparison of those methods to show how the methods able to prevent the attacks. We also discuss the advantages and disadvantages of the methods. Therefore, based on that, we can see what are the common attacks on the fingerprint image and what are the methods that efficient in preventing the attacks.

1. Introduction

Biometrics are an expanding area that focus on identifying and verifying individual identity using their anatomical (e.g. fingerprint) or behavioral (e.g. voice) characteristics. Since biometrics are permanently attached to the persons, they are more efficient than the normal authentication methods for example token-based or knowledge-based that can be forgotten, stolen or lost [1].

According to their uniqueness and immutability, fingerprint is the most widely used in biometric-based systems for user identification process that known as fingerprint recognition. Most of the fingerprint recognition systems are based on minutiae matching in the recognition step. Minutiae matching is based on minutiae points in the fingerprint pattern which is will be fingerprint features.

In order to increase the protection system, digital watermarking can be used to verify the authenticity of a fingerprint sample [2]. The basic idea of the digital watermarking approach is to embed watermark data into the original image fingerprint to protect fingerprint ownership. In addition, the watermark data can be encrypted before embedding the watermark, as a second layer of protection [3]. Therefore, the user's secret key which prevent the watermark from tempering or unauthorized access by attackers.

Although fingerprint image watermarking systems have several advantages over traditional protection systems, they also suffer from different attacks when they are used for achieving authentication. Those attacks can decrease their security considerably. Thus, it's needing to protect the transmitted content between the sender and receiver against those attacks and several measures that can be utilized to decrease the probability of such attacks. In this paper, we discuss about the attacks and the watermarking techniques that have been implemented to prevent the attacks.

2. Types of Attacks on Fingerprint Image Watermarking System

There are some attacks on fingerprint image watermarking systems that jeopardized the safety of that fingerprint image. Therefore, in this section we will discuss about the type of attacks based on a number of research studies that have analysed these attacks on fingerprint images watermarking techniques. In general, the attacks are broadly classified into two groups: unintentional and intentional attacks [4].

2.1. The unintentional attacks

the unintentional attacks can be defined as attacks that occur during normal fingerprint image processing operations such as printing, scanning, compression, transcoding, filtering, noise, gamma correction, geometric transforms and cropping. The attacks on a watermarked fingerprint image known as image processing attacks and geometric attacks. In the Geometric attacks like rotation, scaling, translation, cropping, row-column blanking, warping etc. attempt to destroy synchronization of detection, thus, making the detection process difficult and even impossible. For example, rotation or scaling can change pixel values and will damage the minutiae points and watermarks data.

2.2. The intentional attacks

The main threat to any assets protected by a biometric system is that of an impostor impersonating another person who is enrolled and gaining access to the protected assets[5]. The threats discussed by [6], include four major scenarios to attack a matching system, namely: use of a fingerprint dummy made e.g. from gelatin, use of latent fingerprint on sensor, use real finger of a biometric lookalike and use of the real finger of the victim.

fingerprints can be extracted from photos or copied from touched objects like coffee cups, keyboards, and other things. To test the device against this threat, [5] have developed two experiments.

Firstly, they reviewed the pictures taken and selected the most promising one in terms of image quality. Afterward, extracting a suitable fingerprint dummy using the following steps:

1. Crop the image area covering the whole fingerprint
2. Apply grayscale conversion, then color inversion
3. Crop and scale the relevant fingerprint area with respect to the physical and digital sensor size, e.g. 11×11mm, 192×192 pixel, 508dpi
4. Improve brightness, contrast, and gamma.

Using their tools, embedded the extracted fingerprint dummy into the recorded communication payload and uploaded this to the FPGA(Field-Programmable Gate Array). When activating the card, the FPGA injected the custom fingerprint created from the latent prints on the card. This way has successfully bypassed the authentication in a repeatable fashion.

Another, more passive way to extract the biometric data can be done by using pictures of the actual user covering his fingerprints. These pictures can be created by the attacker from a distance or can be found on the web as discussed by Starbug in Chaos Communication Congress 2014[7]. To evaluate this scenario, Fietkau et al. created multiple pictures covering the test person while showing his fingers and, set up an increasing target distance respectively to 3, 4, 5, 6 and 7 meters. The pictures were taken using a Canon EOS-D1 X with a 200mm lens in an outdoor daylight setting. After taking the pictures, starting the extraction process similar to the previous one. The main difference is in fact that we had to flip the image horizontally and further scale the area depending on the target distance.

Again, injected the obtained fingerprints into the recorded communication payload. defined a maximum amount of 3 attempts per image, which has given us the freedom to slightly improve the image gamma, brightness, and contrast. Under these constraints, 3 out of 5 dummies caused a valid authentication and could successfully bypass the matching algorithm

Due to these attacks, an efficient watermarking technique is needed to be implemented on a fingerprint image to prevent the attacks. We will discuss about the watermarking techniques that have been implemented by many researchers. The advantages and disadvantages of each watermarking technique is explained in that section as well**.**

3. Trend of preventing the attack on fingerprint image watermarking techniques

In fingerprint image watermarking techniques, the main consideration is the evaluation of the robustness and effectiveness of the watermarking method through measurement of the impact of different attacks upon the watermarked fingerprint image. The subsequent section will discuss on the fingerprint image watermarking techniques of preventing the attack.

Bousnina et al. introduced a new method of embedding watermark into a fingerprint image. This involves the use of a secretly generated key to identify which pixels to be watermarked. Thus, preserving the fingerprint minutia points and increase security when extraction step for watermark by attackers. After that, 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 [8]. This proposed method of watermarking biometric fingerprint was verified mainly against conventional watermarking attacks notable for digital images. This includes median filter, Speckle noise, Gaussian noise and Poison noise. In addition, this proposed method succeeded in preventing the intentional attacks which attackers are needed of secret key to extract watermark. Hence, its resistance strength was not investigated against other potential attacks such as geometric attacks.

In a particular research, a technique for inserting two watermarks into fingerprint images was proposed by Alkhathami et al. The technique makes use of Discrete Cosine Transform (DCT) algorithm [9]. Although their approach was blind, means that the extraction stage of watermark does not require the original fingerprint image, but the robustness was tested using only noise attacks which may have a more vulnerable image while placing it on the sensor. It is however necessary that the robustness of the technique needs to be verified against different type of attacks especially geometric attacks. Although, this method is blind, robust for compression attacks and succeeded payload capacity which help to add more authentication factors based on the watermark messages and to protect the ownership of the fingerprint image against piracy. However, its low robustness against geometric attack such as rotation.

In another study, a technique which is based on DCT and a fuzzy-Particle Swarm Optimization was put forward by Bansal et al. for fingerprint watermarking. This technique was applied to secure the fingerprint image of an individual by watermarking its analogous face image [10]. 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 which may lead to distortion of watermark or features for fingerprint.

Similarly, a technique for fingerprint watermarking was put forward by Cao et al. wherein (Contourlet Transform) and TC (Texture Complexity) is used for choosing the optimum blocks where the watermark may be embedded [11]. The watermarking algorithm is robust to JPEG compression, Gaussian noise and filtering attacks. However, it is generally known that there are possibilities for watermarked fingerprint images to be affected by several other attacks such as geometric attacks.

A blind algorithm in the Contourlet domain for watermarking was put forward by Kumar et al. 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 in a fingerprint image [12]. However, the influence of the extraction of biometric features that are important to compare between them were not evaluated, and noise adding attacks were only used 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. [13]. 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 so as to hide the face image's pixel data. However, this approach cannot be certified capable of retaining original fingerprint features as it was not verified against most of the conventional geometric and digital watermarking attacks.

An approach based on wavelet was introduced by Ghany et al. for embedding DNA data based multi-bit watermark into fingerprint images using DWT [14]. The method was robust and

straightforward, but it requires the original fingerprint template at the extraction stage (non-blind). Therefore, this method succeeded in imperceptibility and robustness but low security due to need the original fingerprint at the extraction step of watermark that may lead to the attackers can easily use the original secure data to attack the system.

Alkhathami et al. developed a watermarking algorithm to be embedded into fingerprint images with unique minutiae in order to prevent it from possible effects of the embedded watermark [4]. 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. Therefore, 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. [15]. 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 certain type of attacks like noise addition and histogram equalization, but not tested against other possible attacks such as different other image processing or geometric attacks. Therefore, the robustness was not completely evaluated to justify its capability to better robust than other approaches.

A comparative study was carried out by Haddada et al. on the choice of domain whereby the watermark may be inserted such that the minutiae could be preserved both in terms of its number and its positions [16]. that mean this technique combined between robustness and imperceptibility. The approach presents a new biometric fingerprint watermarking technique that 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 was not completely evaluated to justify its capability to preserve the numbers and positions of the minutiae, better than other approaches.

In a separate research, a watermarking technique was proposed by Alkhathami et al. 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 [4]. 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 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. In addition, based on the results that were recorded in fingerprint image watermarking techniques, most of them cannot know its strong or weakness against intentional attacks but stay just analysis expected based on its algorithm and tools used in this technique.

4. Conclusion

In general, the attacks on watermarking fingerprint image are broadly classified into two groups: unintentional and intentional attacks.

Although, most of watermarking technique as show in previous section were able to achieve good robustness against some unintentional attacks such as image processing. However, they failed to perform well against other types of attacks such as geometric transformations like translations or rotations.

Based on the results that were recorded in fingerprint image watermarking techniques, Geometric attacks such as rotation, scaling and translation are the most common type of challenge attacks in digital watermarking. In intentional attack cannot know strong or weakness of this fingerprint image

watermarking techniques as reviewed in this paper. This is still just analysis expected based on its proposed algorithm and tools used in this technique. Thus, the attacks are important to be evaluated to measure the robustness. This would help to provide higher security and robustness of watermarked fingerprint image.

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

References

[1] Awang S *et al* 2013 *Proc. -2013 Int'l Conf. on Signal-Img. Tech. & Internet-Based Sys.* 706–713
[2] Noore A *et al* 2007 *Forensic Science International* **169** 188–194
[3] Mousavi S M *et al* 2014 *Journal of Digital Imaging* **27** 714–729
[4] Alkhathami M *Watermarking techniques for genuine fingerprint auth.* PhD (RMIT University)
[5] Fietkau J *et al* 2018 *WOOT'18 Proc. of the 12th USENIX Conf. on Offensive Tech.* 5
[6] Henniger O *et al* 2010 *Int'l Biometric Performance Testing Conf.* 1–10.
[7] Starbug 2014 *Ich sehe, also bin ich ... du* (31C3) [Online] https://events.ccc.de/congress/2014/Fahrplan/events/6450.html.
[8] Bousnina N *et al* 2016 *12th Int'l Conf on Innovations in Info. Tech.* 127–131.
[9] Alkhathami M *et al* 2013 *Proc. of the 2013 IEEE 8th Conf. on Ind. Elec.and App.* 1151–1155.
[10] Bansal R *et al* 2013 *IEEE Int'l Conf. on Fuzzy Systems*
[11] Cao Y *et al* 2010 *Int'l Symposium on Intelligent Signal Proc. and Comm. Sys., Proc.* 10–13.
[12] Kishore Kumar N K *et al* 2012 *3rd Int'l Conf. on Comp., Comm. and Networking Tech.*
[13] Bansal R *et al* 2012 *Information Security Journal* **21** 88–101.
[14] Ghany K K A *et al* 2014 *2014 International Conference on Informatics, Electronics & Vision*
[15] Abraham J *et al* 2016 *Data Mining and Advanced Computing Int'l Conf.* 145–149.
[16] Haddada L R *et al* 2017 *IPAS 2016 - 2nd Int'l Image Proc., App. and Systems Conf.* 1–6.