Research Article

Trace Attack against Biometric Mobile Applications

**Sanaa Ghouzali,¹ Maryam Lafkih,² Wadood Abdul,³ Mounia Mikram,⁴
Mohammed El Haziti,⁵ and Driss Aboutajdine²**

¹Information Technology Department, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia

²LRIT, CNRST Associated Unit, URAC 29, Faculty of Sciences, Mohammed V-Agdal University, 10090 Rabat, Morocco

³Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia

⁴The School of Information Sciences, 10170 Rabat, Morocco

⁵Higher School of Technology, 11060 Salé, Morocco

Correspondence should be addressed to Sanaa Ghouzali; sghouzali@ksu.edu.sa

Received 7 February 2016; Accepted 13 March 2016

Academic Editor: Miltiadis D. Lytras

Copyright © 2016 Sanaa Ghouzali et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the exponential increase in the dependence on mobile devices in everyday life, there is a growing concern related to privacy and security issues in the Gulf countries; therefore, it is imperative that security threats should be analyzed in detail. Mobile devices store enormous amounts of personal and financial information, unfortunately without any security. In order to secure mobile devices against different threats, biometrics has been applied and shown to be effective. However, biometric mobile applications are also vulnerable to several types of attacks that can decrease their security. Biometric information itself is considered sensitive data; for example, fingerprints can leave traces in touched objects and facial images can be captured everywhere or accessed by the attacker if the facial image is stored in the mobile device (lost or stolen). Hence, an attacker can easily forge the identity of a legitimate user and access data on a device. In this paper, the effects of a trace attack on the sensitivity of biometric mobile applications are investigated in terms of security and user privacy. Experimental results carried out on facial and fingerprint mobile authentication applications using different databases have shown that these mobile applications are vulnerable to the proposed attack, which poses a serious threat to the overall system security and user privacy.

1. Introduction

It is inevitable that the use of the PIN (personal identification number) as the sole secret to control authenticated access will become obsolete due the exponential growth and accessibility of handheld devices. As an alternative solution, biometric-based authentication techniques on mobile devices can efficiently verify the identity of a person, not just for unlocking the device but also for approving payments and as part of multifactor authentication services. Biometrics refers to physiological/behavioral traits, such as fingerprint, iris, face, and keystroke dynamics. Unlike a password, biometrics cannot be forgotten or stolen. This makes biometric modalities more suitable for authentication applications, especially from

the perspective of the users. Biometric-based authentication applications consist of two stages. The first stage is *enrollment* where the system extracts biometric features of the user and stores these features as a template. In the *authentication* stage, the user presents his or her biometric trait as requested. The user is authenticated if the extracted feature set from the given request is sufficiently close to the stored template set.

Although biometrics can increase the security of mobile applications over existing classical authentication techniques, these technologies have some drawbacks and are vulnerable to several attacks that undermine the authentication process by either bypassing the security of the system or preventing the functioning of the system [1, 2]. However, several attacks are mostly concerned with obtaining touch-input

FIGURE 1: Attack types and levels in a biometric authentication system.

information from the touch screen of a mobile device [3, 4]. The impostor can use, for example, fingerprint traces of a legitimate user collected on a touched object. Facial images can also be stolen from mobile devices or recovered from the user’s online identity shared via social media [5]. Moreover, many smartphone users are not aware of security issues of mobiles and give privileges to malicious software that they willingly install on their devices, allowing the attacker to gain access to sensitive resources such as the device’s camera.

In this paper, we present a new attack on biometric mobile applications based on the alteration of user images. We suppose that the impostor has modified versions of the user’s images and uses them to gain unauthorized access. This type of alteration has not yet been presented in literature and has not been applied to biometric mobile applications. We evaluated the effect of this attack on the security of fingerprint and facial biometric mobile applications and user privacy using different types of image alterations.

The rest of the paper is organized as follows. Section 2 provides related works to the proposed attack on biometric mobile applications. The proposed attack is presented and explained in Section 3. The experimental results are reported and discussed in Section 4. Section 5 concludes the paper and presents a number of future works.

2. Related Works

Biometric-based applications are vulnerable to several types of attacks, which can be classified into direct and indirect attacks as shown in Figure 1. Ratha et al. [1] identified eight points or levels of attacks against biometric applications (Figure 1). The first type of attack is named *sensor attack* or direct attack, consisting of presenting synthetic or fake biometric traits to the sensor. This attack can be carried out in several ways, such as spoofing and alteration attacks. In spoofing attacks, the impostor presents a fake biometric trait (i.e., silicon finger, face mask, etc.) to the biometric mobile application in order to gain unauthorized access. In the case of alteration, the impostor presents his own biometric trait with modifications using obliteration, distortion, imitation, or falsification [6–10]. In order to tackle this attack, approaches for altered biometric data detection have been proposed in [11, 12].

Indirect attacks can be launched on the interface between modules or on the software modules. In the case of the interface between modules, the attacker can resubmit previously

intercepted biometric data before extraction or after extraction of biometric features (replay attack). The transmission channel between the comparator and database can be altered, and the result of the comparator can also be compromised [13, 14]. In the case of attacks on software modules, the feature extractor module and comparator module can be modified through injection of malware (Trojan horse) to return the desired results. Moreover, the database can be attacked, and the biometric templates stored in the database can be disclosed or modified [15, 16].

For the mobile biometric application, spoofing is by far the most used direct attack. The impostor can use information from mobile data (left unwatched or stolen) to gain illegitimate access to the mobile applications. In [17], the authors discussed a spoofing attack on mobile phones using facial biometric authentication and proposed a spoofing attack detection method based on image distortion analysis. In [18], different cases of spoofing attacks in automatic speaker mobile verification systems are perfectly summarized. Spoofing attacks on iris-based mobile applications are also discussed in [19]. In mobile applications based on signatures, authors have tested the falsification attempt to evaluate the security of their proposed algorithm [20]. These works highlighted the vulnerabilities of mobile biometric applications against sensor attacks.

In the case of indirect attacks, several studies have concluded that the majority of mobile application users do not understand permission warnings when a malicious software (e.g., backdoor) is installed, allowing the attacker to gain system privileges and remotely access the device’s camera [21, 22]. Phishing attacks are also considered dangerous on biometric mobile applications where the attacker tricks the user into downloading a malicious mobile application that looks harmless, while giving unauthorized access to the impostor [23]. Further, biometric mobile applications can be attacked using the biometric traces of fingerprints or facial photographs, which can increase the security and privacy concerns of these applications.

3. Description of the Proposed Attack

Despite active research in recent years in the evaluation of biometric-based mobile applications, very few studies have focused on the effect of alteration on the security and robustness of these systems. Alteration of fingerprints has been used to hide the identity of the impostor and gain unauthorized access to the biometric system [12, 22]. This alteration is classified into three categories: obliteration, distortion, and imitation. In the case of facial authentication, the alteration is applied on the face via plastic surgery or prosthetic make-up [10]. With advances in technology, a hacker was able to clone a politician’s fingerprint using pictures taken at different angles with a standard photo camera [24].

In this paper, we present other types of alterations that can be applied on different biometric authentication systems, especially biometric mobile applications. This attack can be applied using different modalities, making it dangerous not only in the case of mobile applications based on fingerprint or facial authentication but also in iris- and voice-based mobile

FIGURE 2: Difference between sensor attacks and the proposed attack in a biometric authentication system.

FIGURE 3: Samples of altered images from the FVC2002 and Yale database.

applications. Unlike the alterations in [12, 22], the goal of the impostor in the proposed model is to gain unauthorized access to the system using an altered version of the real user's images (Figure 2).

The modified version of the user image can be recovered from biometric traces using, for example, the user's picture or traces of the fingerprint left on a touched surface. The impostor can use this image as a request to gain unauthorized access or to acquire some information about the user, which affects the user's privacy. We have focused on six categories

of alteration based on the changes made on the reference images, as shown in Figure 3; they are as follows:

- (i) *Alteration based on luminosity:* the impostor has modified versions of the user's image with different levels of luminosity. In order to change the luminosity, arbitrarily selected values are added to or subtracted from the user's image.
- (ii) *Alteration based on noise:* Gaussian noise varying between 0 and 100 (the normalization percentage) is

added to the user's image in order to generate several noisy images.

- (iii) *Alteration based on blur*: the blurred images are obtained using a 2D Wiener filter, and the variation of the blur is varied between 1 and 7.
- (iv) *A part of the user's image*: the impostor has only a part of the user's reference image.
- (v) *A mosaic image*: the impostor combines several parts of the user's images to create a new complete image that is presented as a request.
- (vi) *A negative image*: the impostor has a negative image of the user (e.g., a negative image of the user's photo or a medical image of the fingerprint, which can give high contrast of the fingerprint due to the black background).

3.1. Security Evaluation. In order to evaluate the security of biometric mobile applications against the proposed attack, we defined the criterion to measure the percentage of acceptance of the impostor who used altered images in order to gain illegitimate access. We named this criterion *correct matching using alteration (CMA)*, which is measured using (1) for fingerprint authentication and (2) for facial authentication for different types of alterations where R and A are the reference and the altered images, respectively:

$$CMA_{\text{Fingerprint}} = \text{Matching Score}(R, A) \quad (1)$$

$$CMA_{\text{Face}} = \text{Number of Corresponding Associations}(R, A). \quad (2)$$

3.2. Privacy Evaluation. Since biometric information is very sensitive data, the potential to misuse or abuse it poses a serious menace to the user's privacy. Therefore, we analyze the effect of the alteration attack on the privacy of the user. We suppose that the impostor does not know the system parameters. Our goal is to quantify the amount of information on reference images that can be gained from altered images. To this end, we consider an information theory analysis under various kinds of alteration attacks, and we examine the information content in biometric data. We use mutual information [25] (see (3)) to measure the amount of information leaked concerning the user's reference image when one or several biometric images of the same user are fully or partially altered. The mutual information $I(R, A)$ is measured in bits, where R and A are the reference and the altered images, $H(R)$ and $H(A)$ are the marginal entropies, and $H(R, A)$ is the joint entropy of R and A :

$$I(R, A) = H(A) + H(R) - H(R, A). \quad (3)$$

4. Experimental Results

We test the different categories of the proposed attack against fingerprint and facial mobile applications using different databases. Both applications are evaluated at two levels: security and privacy. To evaluate the security, we calculate the

matching score and the number of matched associations of the altered images used by the impostor to gain unauthorized access. At the privacy level, we evaluate the amount of information leaked by the impostor concerning the reference image.

4.1. Alteration Attack against Fingerprint Authentication System. The fingerprint authentication application is implemented based on four stages (Figure 4) [26]; the first one is image preprocessing using image enhancement to make the image clearer. Two methods are then used for image enhancement: histogram equalization and fast Fourier transform. Histogram equalization attempts to distribute the gray levels in the fingerprint image, whereas the Fourier transform connects some false bleeding points on ridges and removes the false connection between ridges. Next, the binarization and the segmentation are applied in order to extract the region of interest in the fingerprint image. The second stage is the minutiae extraction, which is based on ridge thinning to eliminate the redundant pixels and minutiae marking to extract the minutiae set. Since these approaches introduce some errors, which create false minutiae, the postprocessing stage is then needed to eliminate additional minutiae; this phase is based on removal of H-breaks, isolated points, and false minutiae. Finally, matching is carried out to measure the similarity between minutiae sets of different fingerprints. This stage is based on two steps, the alignment to arrange one fingerprint's minutiae according to another followed by the matching to find the percentage of matched minutiae between two fingerprint images. Given reference fingerprint I_1 with minutia set m_i and request for fingerprint image I_2 with minutia set m_j , we consider both minutiae matched if the spatial difference D between them is smaller than the selected threshold ϵ and their direction difference Dir is smaller than θ_0 where

$$D(m_i, m_j) = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \quad (4)$$

$$\text{Dir}(m_i, m_j) = \min(|\theta_i - \theta_j|, 360 - |\theta_i - \theta_j|).$$

Let us consider the function $S(m_i, m_j)$, which returns 1 if both minutiae are matched as follows:

$$S(m_i, m_j) = \begin{cases} 1, & D(m_i, m_j) \leq \epsilon, \text{Dir}(m_i, m_j) \leq \theta_0 \\ 0, & \text{otherwise.} \end{cases} \quad (5)$$

We calculate the total number of matched minutiae based on

$$\text{correct matched}(m_i, m_j) = \sum S(m_i, m_j). \quad (6)$$

The final matching score is calculated as follows:

$$\text{Matching Score} = \frac{\sum S(m_i, m_j)}{\text{number of minutiae}} * 100. \quad (7)$$

To analyze the effect of the proposed attack on the fingerprint matching score, FVC2002 and FVC2004 [27] fingerprint databases are used for experimentations. We consider the

FIGURE 4: Continued.

FIGURE 4: Different steps of minutia point extraction.

FIGURE 5: Alteration based on luminosity for fingerprint authentication applications.

FIGURE 6: Alteration based on blurring for fingerprint authentication applications.

reference database with 10 users. Then, for each user, 10 images with different alteration levels are created based on different types of alterations mentioned in Section 3. Next, based on the verification process (i.e., a 1:1 relation), the altered images are tested as requests against the reference images and then the matching score is calculated according to the system threshold.

4.1.1. Security Evaluation. At first, in order to show the effect of the level of alteration on the security of the biometric mobile application, we evaluate the security of the fingerprint-based mobile application against an alteration attack for all the users according to the alteration levels. Figure 5 presents the matching score for FVC2002 and FVC2004 databases with respect to the luminosity levels. We notice that the percentage distribution of the matching score increases when the luminosity level is decreased to -100 . This vulnerability can be explained by the ridge detection in the case of minimal luminosity where the ridge is highlighted in black. On the other hand, even if the level of luminosity is altered when the images are much degraded (i.e., less

than -80 or greater than 60), the matching score is always high, which explains why the fingerprint mobile application is always vulnerable to luminosity variations.

To evaluate the effect of blurring on the fingerprint authentication system based on FVC2004 and FVC2002 databases, blurred images are used. As shown in Figure 6, the distribution of the matching score is decreased when the blur level is increased. The percentage of matching can reach 55% for both databases if the impostor uses images with high blurring levels. For example, if the level of blurring is minimal, the matching score can reach 75%.

In order to study the effect of noise alteration, we first calculate the peak signal to noise ratio (PSNR) [28] to measure the similarity between the reference and noisy images. Instead of comparing the extracted features, we compare the images without taking into account the biometric system. When the level of noise is increased (i.e., interval $[45, 100]$), the PSNR value decreases toward zero, and when the level of noise is decreased (inferior to 48), the PSNR value is increased. Hence, the images with less noise are considered similar to the reference image of the user (Figure 7).

FIGURE 7: PSNR with respect to noise level using fingerprint images.

FIGURE 8: Alteration based on noise for fingerprint authentication applications.

Moreover, we also consider the case of biometric mobile applications where images are preprocessed and then post-processed. Hence, we compare the extracted features from noisy images and the reference image of the user.

We present the variation of the matching score depending on the noise levels. We notice that the matching score is increased, even if the percentage of noise is higher in altered images (Figure 8). This can be explained by the minutiae extraction process where the biometric system can consider many fake minutiae (extracted due to the noise) as veritable. Consequently, a very noisy image may be matched against the reference image with high probability compared to the less noisy image. Thus, the impostor can be accepted if presenting an altered image with high levels of noise.

When the impostor possesses a partial reference image of the real user, he/she can use a partial attack to gain unauthorized access to the biometric authentication system. To illustrate this attack scenario, we use different parts of

FIGURE 9: Alteration based on part of user's image for fingerprint authentication applications.

FIGURE 10: Alteration based on negative image for fingerprint authentication applications.

the user image and calculate the matching score between the extracted features from the partial altered image and the complete reference image (Figure 9). We notice that the impostor can get a high matching score when the level of alteration is minimal, whereas, in FVC2002, the matching score reaches 52% and, for FVC2004, the matching score can reach 58%.

In the case of alteration using a negative image, as shown in Figure 10, the chance of the impostor being accepted can reach 90% to 95% for both databases. This is due to the detection of the ridges in the fingerprint images, where the ridges are highlighted with black and the furrows with white. The negative image can highlight the image appearance in the sensor because of the black background, which results in an increased number of extracted features. The vulnerability due to this alteration can be increased using the threshold.

FIGURE 11: Alteration based on mosaic image for fingerprint images.

For alterations based on a mosaic image, we combine four different parts of the user's biometric trait images to create a mosaic image. As shown in Figure 11, the matching score increases according to the threshold to reach almost 85% for both databases. We notice that the impostor can get an even higher score due to the apparition of additional features. However, the percentage of acceptance is related to the combined parts because the biometric features can be formed or distorted based on the number of used parts and the quality of the generated image (i.e., mosaic image).

4.1.2. Privacy Leakage. A second point that we evaluate in this paper is the privacy concern under different types of alterations. To test the effect of information leakage on the user's privacy, we first measure the amount of information leaked for each user. Then, for each type of alteration, we calculate the average mutual information using all altered images at different levels for FVC2002 (Figure 12) and FVC2004 (Figure 13) databases.

For each user, the impostor can leak more information about the reference image using altered images, especially in the case of noisy images and increased luminosity. This vulnerability varies from one user to another. Hence, the attack effect is not the same for all users. This can be explained by the difference of image quality between different users and interclass variability.

4.2. Alteration Attack against Facial Authentication System. To create the face-based authentication application, we calculate the number of associations between the reference and request images. At first, local features are detected and extracted using scale-invariant feature transform (SIFT) [29]. Each image I is described by a set of invariant features $X(I)$. The matching process is based on the comparison of the two images I_1 and I_2 using the measure of similarity between the reference feature set $X(I_1)$ and the request set $X(I_2)$. Given

two key points $x \in X(I_1)$ and $y \in X(I_2)$, we note that x is associated with y if

$$\begin{aligned} d(x, y) &= \min_{\{z \in X(I_2)\}} d(x, z), \\ d(x, y) &\leq C d(x, y'), \end{aligned} \quad (8)$$

where d represents the Euclidean distance between the SIFT descriptors, C is the threshold selected arbitrarily, y' is the point of $X(I_2)$ with distance greater than $d(x, y)$, and the minimum distance to x is defined by the following equation:

$$d(x, y') = \min_{\{z \in X(I_2), d(x, z) > d(x, y)\}} d(x, z). \quad (9)$$

In other words, x is associated with y if y is the closest point from x in $X(I_2)$ according to the Euclidean distance between SIFT descriptors and if the second smallest value of this distance $d(x, y')$ is significantly greater than $d(x, y)$. Since the necessary gap between $d(x, y)$ and $d(x, y')$ is encoded by the constant C , we consider the key point y of the request matched with the reference key point y if x is associated with y and y is associated with x .

Figure 14 shows an example of the facial authentication system based on the SIFT descriptor. We analyze the security of a facial authentication system against our proposed attack using the Yale [30] and AR [31] databases.

4.2.1. Security Evaluation. Figure 15 shows the effect of luminosity alteration on the facial mobile applications. We notice that the number of matched associations between the altered and reference images is higher when the altered image is not very degraded. If the level of luminosity is increased, the number of corresponding associations between reference images and the altered image decreases. Hence, when the luminosity level is significantly increased or decreased, image quality is degraded and then the probability to accept the impostor is also decreased.

Figure 16 shows the effect of blurring on the facial authentication system based on the AR and Yale databases. We notice that the distribution of the number of associations is decreased when the blur level is increased. The number of correspondences can reach 150 for the AR database, if the impostor uses images with high blurring levels. In the case of minimal blurring levels, the number of corresponding associations can reach 225 for the AR database and 100 for the Yale database.

In the case of noise alteration, we first calculate the difference between the reference and altered images without considering the biometric authentication application (Figure 17). Our results show that the PSNR is increased when the noise is minimal and can be decreased successively when the noise level is increased. This means that the image with less noise level is the image with the best quality.

On the other hand, considering the facial authentication application, we notice in Figure 18 that the number of matched associations is increased to reach 300/313 for the AR database and 150/163 for the Yale database when the noise level is almost 50%. If the level of alteration is greater than

FIGURE 12: Average of mutual information for FVC2002 database.

FIGURE 13: Average of mutual information for FVC2004 database.

FIGURE 14: SIFT-based facial authentication system.

FIGURE 15: Number of associations using luminosity alteration for facial authentication applications.

FIGURE 16: Number of associations using blurring alteration for facial authentication applications.

FIGURE 17: PSNR with respect to the noise levels.

FIGURE 18: Number of associations using noise alteration for facial authentication applications.

50%, the number of associations decreases progressively. This can be explained by the processing due to feature extraction where the face-based mobile application can consider false points as veritable features. Thus, the biometric system gives additive associations between noisy and reference images. Hence, we conclude that, unlike PSNR, biometric authentication systems can consider the noisy image similar to the reference image due to false extracted features.

In order to illustrate the effect of partial images on the face-based mobile application, we measure the number of matched associations between different partial images and the reference image of the user (Figure 19). We notice that the number of matched associations between the partial images and the reference image of the user is decreased when the level of alteration is minimal. Hence, if the level of alteration is minimal, the impostor can have 229/303 matched associations for the AR database and 71/98 for the Yale database, which ensures access to the system.

FIGURE 19: Number of associations using partial alteration for facial authentication applications.

FIGURE 20: Number of associations using mosaic alteration for facial authentication application.

In the case of alteration using mosaic images, we notice in Figure 20 that the number of matched associations is arbitrarily distributed; this can be due to the quality of the mosaic image that is constructed using a combination of four different user image parts. If the mosaic image has a high quality, the number of matched associations can increase for some users, as shown for the AR and Yale databases.

For negative images, using the facial authentication application based on the SIFT descriptor, the devices cannot accept the negative image attack. This is due to the SIFT process, where the associations are randomly matched. The failure to match using the negative image cannot be generalized to all face-based authentication devices. This type of attack can be successful for facial authentication devices based on other biometric feature extraction processes. Figure 21 describes the dissimilarity between the key points of the original image and the negative image of the user, which result in a low number of associations between both images.

FIGURE 21: Matching of the original and the negative image.

4.2.2. Privacy Leakage. In order to test the privacy consequence for face-based mobile applications, we calculate the mutual information between the reference and altered images. The average of mutual information for each user is measured using all altered images of each user for every type of alteration.

It can be clearly noted that, as shown in Figure 22, for the AR database, for the face-based authentication system, the impostor can leak important information about the user, especially in the case of noise, blurring, and luminosity alterations. In the case of the Yale database (Figure 23), we notice that the privacy concern is increased where the impostor can have more information (average mutual information exceeds 2) about the real user, which affects user privacy. We also note that the negative image has a serious effect on the privacy of the user, especially in the Yale database.

This can be explained by the nature of the Yale facial database, which contains grayscale images, unlike the AR facial database, which has RGB color images. Moreover, we notice that even if the impostor who used negative images cannot be accepted by the system, he/she can gain important information about the user, which represents a privacy concern.

4.3. Result Summary. Tables 1 and 2 summarize the success probability of an impostor who has used an alteration attack based on user image traces for different alteration levels for fingerprint and facial authentication systems. It is clearly shown that the levels of alteration have an important effect on the matching score in fingerprint authentication systems and on the number of matched associations in facial authentication systems. On the other hand, we notice that alteration affects the number of extracted features, which can be increased or decreased compared to the number of extracted features from the reference image. Hence, poor quality fingerprints and facial images can lead to incorrect or spurious biometric features and also can remove real biometric features, which can deceive the effectiveness of the biometric system. The minutiae can be added or removed depending on the type of alteration. We also notice that when using alterations, such as part of a user image and blurred images, the level of alteration can affect the number of extracted features from altered images. Hence, if the quality of an altered image is significantly degraded (very high or low alteration levels), the number of extracted features is decreased.

FIGURE 22: Average of mutual information using different types of alterations for the AR database.

FIGURE 23: Average of mutual information using different types of alterations for the Yale database.

TABLE 1: Results of fingerprint authentication application.

Fingerprint authentication application				
Alteration	Levels	Matching score	Number of features in	
			Reference image	Altered image
FVC2002 database	Blur	1		273
		2	403	345
		6		352
	Noise	1.45		807
		49.9	162	490
		82.29		210
	Luminosity	-84.8		598
		-12.25	360	681
		50		418
	Part of user image	31.16		672
		93.5	600	321
		115.83		196
	Mosaic	—	287	1,167
		—	700	1,071
		—	505	658
FVC2004 database	Blur	—	505	1,728
		—	700	1,216
		—	527	1,147
	Noise	1		703
		2	476	623
		6		405
	Luminosity	1.45		801
		49.9	518	370
		90.36		598
	Part of user image	-84.8		34
		-12.25	356	518
		50		51
	Mosaic	80		612
		120	339	490
		160		108
	Negative	—	339	875
		—	176	629
		—	237	531
	Negative	—	518	528
		—	339	503
		—	231	233

5. Conclusion

In this paper we have presented, to the best of our knowledge, the first alteration attack on biometric mobile applications. This attack is based on image trace using altered versions of reference images of the user in order to gain illegitimate access to biometric mobile applications. We have distinguished between six types of alteration attacks and their effects on face- and fingerprint-based authentication mobile applications. We have altered the user's image using the modification of luminosity, noise, blurring, and negative images. We have also considered the case when an

impostor has a part or several parts of the user's image(s). Experiments are conducted on fingerprints using FVC2002 and FVC2004 databases and on face-based authentication applications using the Yale and AR databases. We have evaluated the matching score of both systems using the alteration attack and then studied the effects on user privacy. The experimental results show that biometric-based mobile applications based on fingerprint and facial images are vulnerable to the proposed attack. Furthermore, using this attack, the impostor can gain more information about the user's reference image, which compromises the user's privacy. In future work, we intend to extend this work and study the

TABLE 2: Results of face authentication application.

Face authentication application				
	Alteration	Levels	Number of associations	Number of associations in
				Reference image Altered image
Yale database	Blur	1	103	134
		2	65	106
		6	12	43
	Noise	1.45	65	169
		49.9	75	170
		90.36	119	123
	Luminosity	−44.61	86	118
		−15.64	114	126
		31	104	118
	Part of user image	48	68	118
		96	61	99
		240	36	60
	Mosaic	—	65	110
		—	35	113
		—	8	150
AR database	Blur	1	158	169
		3	133	152
		6	81	121
	Noise	1.4	137	314
		49.62	189	248
		90.36	140	198
	Luminosity	−44.61	181	194
		−15.64	190	195
		31	151	192
	Part of user image	48	147	204
		144	130	179
		240	105	164
	Mosaic	—	151	305
		—	146	451
		—	131	245

effect of trace attacks on protected biometric mobile devices using template protection algorithms, such as fuzzy vault and fuzzy commitment.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This research project was supported by a grant from the “Research Center of the Female Scientific and Medical Colleges,” Deanship of Scientific Research, King Saud University.

References

- [1] N. K. Ratha, J. H. Connell, and R. M. Bole, “An analysis of minutiae matching strength,” in *Proceedings of the International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA '01)*, pp. 223–228, Halmstad, Sweden, June 2001.
- [2] A. K. Jain, A. Ross, and U. Uludag, “Biometric template security: challenges and solutions,” in *Proceedings of the 13th European Signal Processing Conference (EUSIPCO '05)*, pp. 1934–1937, Antalya, Turkey, September 2005.
- [3] S. Sagioglu and G. Canbek, “Keyloggers: increasing threats to computer security and privacy,” *IEEE Technology and Society Magazine*, vol. 28, no. 3, pp. 10–17, 2009.
- [4] D. Damopoulos, G. Kambourakis, and S. Gritzalis, “From keyloggers to touchloggers: take the rough with the smooth,” *Computers and Security*, vol. 32, pp. 102–114, 2013.
- [5] M. Aresta, L. Pedro, C. Santos, and A. Moreira, “Online identity analysis model: analysing the construction of the self in digital environments,” *International Journal of Knowledge Society Research*, vol. 4, no. 3, pp. 89–102, 2013.
- [6] S. Yoon, J. Feng, and A. K. Jain, “Altered fingerprints: analysis and detection,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 34, no. 3, pp. 451–464, 2012.

- [7] T. van der Putte and J. Keuning, "Biometrical fingerprint recognition: don't get your fingers burned," in *Proceedings of the 4th Working Conference on Smart Card Research and Advanced Applications*, pp. 289–303, 2000.
- [8] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial "gummy" fingers on fingerprint systems," in *Proceedings of the SPIE Optical Security and Counterfeit Deterrence Techniques IV*, vol. 4677, pp. 275–289, San Jose, Calif, USA, January 2002.
- [9] J. Feng, A. K. Jain, and A. Ross, "Detecting altered fingerprints," in *Proceedings of the 20th International Conference on Pattern Recognition (ICPR '10)*, pp. 1622–1625, IEEE, Istanbul, Turkey, August 2010.
- [10] N. Erdogmus, N. Kose, and J.-L. Dugelay, "Impact analysis of nose alterations on 2D and 3D face recognition," in *Proceedings of the IEEE 14th International Workshop on Multimedia Signal Processing (MMSP '12)*, pp. 354–359, Banff, Canada, September 2012.
- [11] R. Josphineleela and M. Ramakrishnan, "A new approach of altered fingerprints detection on the altered and normal fingerprint database," *Indian Journal of Computer Science and Engineering*, vol. 3, no. 6, pp. 818–821, 2012.
- [12] A. K. Jain and S. Yoon, "Automatic detection of altered fingerprints," *Computer*, vol. 45, no. 1, pp. 79–82, 2012.
- [13] J. Galbally, J. Fierrez, J. Ortega-Garcia, C. McCool, and S. Marcel, "Hill-climbing attack to an eigenface-based face verification system," in *Proceedings of the 1st IEEE International Conference on Biometrics, Identity and Security (BIdS '09)*, pp. 1–6, IEEE, Tampa, Fla, USA, September 2009.
- [14] A. Adler, "Sample images can be independently restored from face recognition templates," in *Proceedings of the Canadian Conference on Electrical and Computer Engineering (CCECE '03)*, pp. 1163–1166, May 2003.
- [15] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: issues and challenges," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948–959, 2004.
- [16] A. Ross, J. Shah, and A. K. Jain, "Towards reconstructing fingerprints from minutiae points," in *Proceedings of the Biometric Technology for Human Identification II*, vol. 5779, pp. 68–80, Orlando, Fla, USA, March 2005.
- [17] D. Wen, H. Han, and A. K. Jain, "Face spoof detection with image distortion analysis," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 746–761, 2015.
- [18] N. Evans, T. Kinnunen, and J. Yamagishi, "Spoofing and countermeasures for automatic speaker verification," in *Proceedings of the INTERSPEECH*, pp. 925–929, 2013.
- [19] A. F. Sequeira, J. Murari, and J. S. Cardoso, "Iris liveness detection methods in the mobile biometrics scenario," in *Proceedings of the International Joint Conference on Neural Networks (IJCNN '14)*, pp. 3002–3008, IEEE, Beijing, China, July 2014.
- [20] J. Liu, L. Zhong, J. Wickramasuriya, and V. Vasudevan, "uWave: accelerometer-based personalized gesture recognition and its applications," *Pervasive and Mobile Computing*, vol. 5, no. 6, pp. 657–675, 2009.
- [21] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: user attention, comprehension, and behavior," in *Proceedings of the ACM Symposium on Usable Privacy and Security*, p. 3, ACM, Washington, DC, USA, July 2012.
- [22] A. Nagar, K. Nandakumar, and A. K. Jain, "Biometric template transformation: a security analysis," in *Proceedings of the SPIE, Electronic Imaging, Media Forensics and Security II*, vol. 7541, San Jose, Calif, USA, January 2010.
- [23] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in *Proceedings of the Conference on Human Factors in Computing Systems (CHI '06)*, pp. 581–590, April 2006.
- [24] "Politician's fingerprint 'cloned from photos' by hacker," December 2014, <http://www.bbc.com/news/technology-30623611>.
- [25] T. M. Cover and A. T. Joy, "Entropy, relative entropy and mutual information," in *Elements of Information Theory*, pp. 12–49, Cover & Thomas, 1991.
- [26] A. El-Sisi, "Design and implementation biometric access control system using fingerprint for restricted area based on Gabor filter," *International Arab Journal of Information Technology*, vol. 8, no. 4, pp. 355–363, 2011.
- [27] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, Berlin, Germany, 2009.
- [28] S. Arora, J. Acharya, A. Verma, and P. K. Panigrahi, "Multilevel thresholding for image segmentation through a fast statistical recursive algorithm," *Pattern Recognition Letters*, vol. 29, no. 2, pp. 119–125, 2008.
- [29] M. Bicego, A. Lagorio, E. Grosso, and M. Tistarelli, "On the use of SIFT features for face authentication," in *Proceedings of the Computer Vision and Pattern Recognition Workshop (CVPRW '06)*, p. 35, June 2006.
- [30] P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman, "Eigenfaces vs. fisherfaces: recognition using class specific linear projection," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 19, no. 7, pp. 711–720, 1997.
- [31] A. Martinez and R. Benavente, "The AR face database," Tech. Rep. CVC 24, 1998.