applied sciences

MDPI

Article

Palmprint False Acceptance Attack with a Generative Adversarial Network (GAN)

Fei Wang [1], Lu Leng [1,2,*], Andrew Beng Jin Teoh [2] and Jun Chu [1]

[1] School of Software, Nanchang Hangkong University, Nanchang 330063, China; wangfei0496@sina.com (F.W.); chuj@nchu.edu.cn (J.C.)

[2] School of Electrical and Electronic Engineering, College of Engineering, Yonsei University, Seoul 120749, Korea; bjteoh@yonsei.ac.kr

* Correspondence: leng@nchu.edu.cn or 1816085212014@stu.nchu.edu.cn; Tel.: +86-791-8645-3251

Received: 1 November 2020; Accepted: 25 November 2020; Published: 29 November 2020

Abstract: Biometric-based authentication is widely deployed on multimedia systems currently; however, biometric systems are vulnerable to image-level attacks for impersonation. Reconstruction attack (RA) and presentation attack (PA) are two typical instances for image-level attacks. In RA, the reconstructed images often have insufficient naturalness due to the presence of remarkable counterfeit appearance, thus their forgeries can be easily detected by machine or human. The PA requires genuine users' original images, which are difficult to acquire in practice and to counterfeit fake biometric images on spoofing carriers. In this paper, we develop false acceptance attack (FAA) for a palmprint biometric, which overcomes the aforementioned problems of RA and PA. FAA does not require genuine users' images, and it can be launched simply with the synthetic images with high naturalness, which are generated by the generative adversarial networks. As a case study, we demonstrate the feasibility of FAA against coding-based palmprint biometric systems. To further improve the efficiency of FAA, we employ a clustering method to select diverse fake images in order to enhance the diversity of the fake images used, so the number of attack times is reduced. Our experimental results show the success rate and effectiveness of the FAA.

Keywords: false acceptance attack; palmprint; naturalness; clustering; diversity enhancement; generative adversarial network

1. Introduction

Today, people are enjoying variety of internet services that are associated to the advancement of telecommunication, smart devices, small IoT devices, and social media. For the growth of multimedia in future, multimedia security should be braced with the supporting technologies, such as identity management. Unlike traditional identity management approaches that require users to supply their own credentials and/or known-knowledge for authentication, biometric systems offer better usability [1,2] and have become versatile [3]. However, biometric systems are vulnerable to several attacks, such as image-level attack. In image-level attacks, the attackers try to find or artificially counterfeit the fake biometric images that can successfully cheat the systems, which can be used to impersonate genuine users [4]. Two typical instances are reconstruction attack (RA) [5] and presentation attack (PA) [6].

In RA and PA, only "similarity" is considered while additional significant evaluation of "naturalness" is neglected. "Similarity" refers to the closeness of two biometric templates in terms of a distance metric. In image-level attacks, the two biometric templates are generated from a genuine users' original biometric image and a found/counterfeited fake biometric image. If "similarity" is satisfied, the image-level attack is successful; i.e., the genuine user is impersonated successfully.

On the other hand, "naturalness" refers to a requirement where a found/counterfeited fake image must look natural, which implies the image should not have strong noise or look artificial. The counterfeited image without sufficient naturalness can be easily detected by a human operator or artificial intelligence machine.

"Naturalness" means an image seems natural rather than counterfeited. If an image has strong noise or noiselike appearance, it seems remarkably counterfeited. An image without sufficient naturalness can be easily detected and resisted against. The three biometric image-level attacks, namely RA, PA, and FAA, are discussed in terms of the two aforementioned evaluations and other performance, as follows.

RA is shown in Figure 1. A biometric image is reconstructed from a genuine user's target feature template in feature domain. Some evolution algorithms, such as the genetic algorithm (GA) or hill-climbing (HC) algorithm, are used to iteratively modify the fake image in image domain and continuously enhance the similarity in feature domain until RA is successful. Typically, if RA is successful, the target feature template and fake feature template are similar, while the target image and the fake image are dissimilar, because the similarity in feature domain does not ensure the similarity in image domain. In addition, since the naturalness is not considered in RA, the reconstructed fake images typically have insufficient naturalness; i.e., they have a counterfeit appearance that reveals they are not captured in natural environments. Furthermore, the evolution algorithms in RA become invalid in biocryptosystems if the extracted/recovered bio-key is strictly protected with one-way function. The correlation between the input and output is completely damaged by one-way function, so the evolution algorithms in RA cannot enhance the similarity in feature domain.

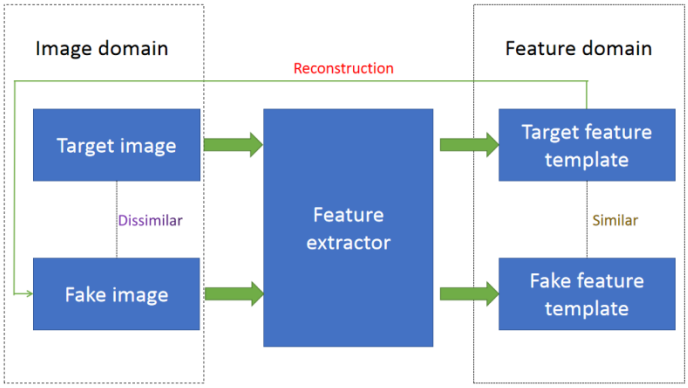


Figure 1. Reconstruction attack.

PA is shown in Figure 2. In PA, the attackers must have a genuine user' original target biometric image, and counterfeit a fake biometric image on some spoofing carriers, including print the image on a piece of paper, display the biometric image on a monitor, counterfeit a mask for a face or a glove for palmprint. They use the spoofing carriers containing the genuine users' original target biometric images, such as the paper, monitor, mask, and glove, to cheat the biometric system. It is easy to capture genuine users' original target face images or obtain them on internet social networks, but sometimes it is difficult to gain genuine users' original target images of other biometric modalities, such as palmprint. Some biometrics, such as veins or electrical biosignals, can resist PA and be used for liveness detection due to their concealed nature [7].

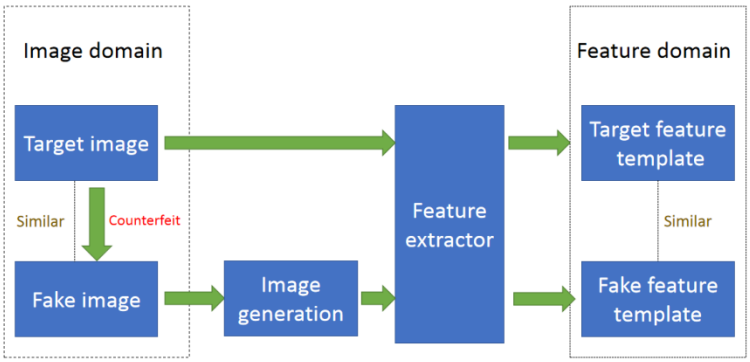


Figure 2. Presentation attack.

FAA is shown in Figure 3, which does not have the aforementioned issues that were presented in RA and PA. FAA does not require the genuine users' images, and it generates a large number of fake palmprint images with image generation technologies, such as generative adversarial network (GAN) and variational autoencoder (VAE), to impersonate genuine users. The fake images used to impersonate genuine users consist of the fake image set. The attackers try to find the fake image in fake image set to satisfy the similarity in feature domain; i.e., the fake image found can generate the fake feature template that is similar to the target feature template.

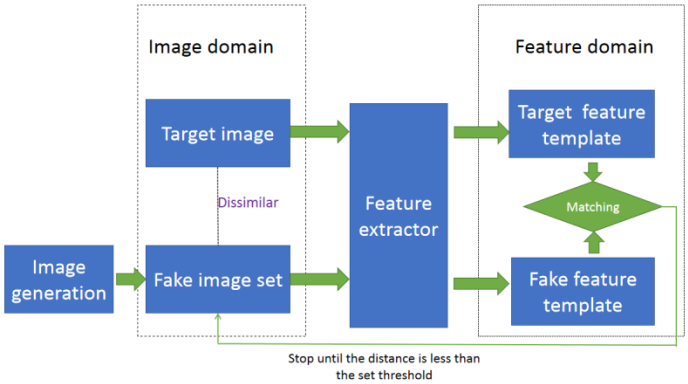


Figure 3. False acceptance attack.

Although biometrics is a powerful tool widely deployed in various security systems, biometric characteristics are largely immutable, resulting in permanent biometric compromise when a feature template is stolen. Thus, the usage of feature templates without protection should be forbidden. Cancellable biometric and biocryptosystem are two main pipelines for biometric template protection, whose frameworks are shown in Figures 4 and 5, respectively. The similarity between the feature templates in feature domain is approximatively preserved between the cancellable templates in cancellable domain, so the evolution algorithms in RA are valid for a cancellable biometric [8]. In biocryptosystems, a bio-key can be extracted/recovered and protected with a one-way function, such as hash function. RA becomes invalid because one-way functions completely damage the correlation/linkage between the input and output. However, PA uses the spoofing carriers containing the genuine users' original target biometric images to cheat biometric systems; while FAA uses the fake image set to cheat biometric systems. Neither PA nor FAA requires the data in feature domain, cancellable domain, and hash domain. Thus, PA and FAA are still valid in biocryptosystems. If a fake feature template is similar enough to a target feature template, i.e., the similarity in feature domain is satisfied, the bio-key in bio-key domain can be extracted/recovered from the fake feature template.

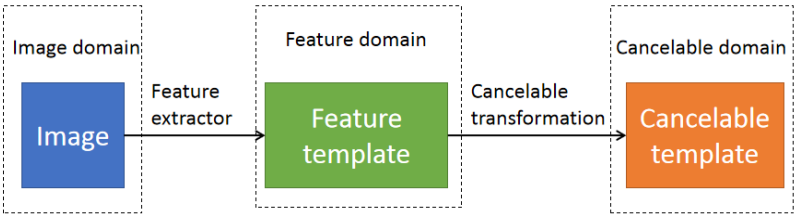


Figure 4. Cancellable biometric framework.

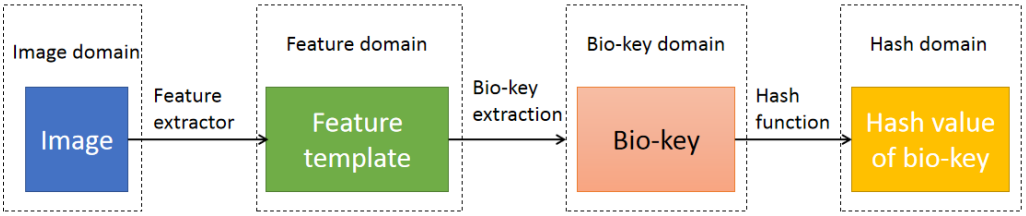


Figure 5. Biocryptosystem framework.

The three image-level attacks are compared in Table 1, which demonstrates the advantages of FAA.

Table 1. Comparison of three image-level attacks counterfeiting biometric image.

Attack Methods	Similarity in Feature Domain	Naturalness in Image Domain	Original Target Image	Cancellable Biometric	BioCryptosystem
Reconstruction attack	√	×	Required	Valid	Invalid
Presentation attack	√	√	Not required	Valid	Valid
False acceptance attack	√	√	Not required	Valid	Valid

Palmprint refers to the inner surface from the fingers to the wrist, which contains rich unique personal features, such as ridges, minutiae, and textures, so it is discriminative, noninvasive, stable, acceptable, and has good privacy. In addition, many feature extractors of other biometric modalities are suitable for palmprint, so palmprint is an important and representative biometric modality. In this paper, we develop false acceptance attack (FAA) for a palmprint biometric. The contributions of this paper include:

- We develop FAA for palmprint biometrics and demonstrate its feasibility against coding-based palmprint biometric systems. The FAA is free from the issues found in RA and PA.
- FAA does not require genuine users' images, and it can be launched simply with the synthetic images with high naturalness, which are generated by the generative adversarial networks. The naturalness of the reconstructed images is neglected in PA, so the FAA is a more fraudulent attack than RA.
- To further improve the efficiency of FAA, we employ a clustering method to select diverse fake images in order to enhance the diversity of the fake images used, so the number of attack attack times is reduced; i.e., the attackers can quickly find the fake image in a fake image set, which can cheat the system successfully.

2. Related Works

2.1. Biometric Image-Level Attacks

Biometric image-level attacks, including RA, PA, and FAA, counterfeit biometric images to impersonate genuine users. The basic goal is "similarity," that is the attacks are successful only when

the similarity is satisfied. Another important goal is "naturalness" that is neglected. The naturalness can be briefly divided into three levels, namely low, medium, and high levels, as shown in Figure 6. The fake images with low naturalness seem noiselike (random) or incomplete. The fake images with medium naturalness are complete but have a somewhat counterfeit appearance that reveals they are not captured in natural environments. The fake images with high naturalness are similar to real natural images.

(**a**) Low (**b**) Medium (**c**) High

Figure 6. Counterfeited fingerprint images with the naturalness of different levels.

The state-of-the-art biometric image-level attacks are summarized and compared in Table 2.

Table 2. Existing biometric image-level attacks.

Ref.	Year	Modality	Naturalness Level	Methodology
[9]	2004	Fingerprint	Low	Reconstruct fingerprint minutiae image using a hill-climbing (HC) algorithm.
[10]	2007	Fingerprint	Low	Reconstruct the direction, category, and ridge of the original fingerprint ridge from the fingerprint minutiae template.
[11]	2004	Face	Low	Reconstruct face image using HC.
[12]	2019	Palmprint	Low	Reconstruct image from cancellable biometric template using a genetic algorithm (GA).
[13]	2016	Iris	Medium	Generate iris image using generative adversarial network (GAN).
[14]	2011	Fingerprint	Medium	Reconstruct phase image from the fingerprint minutiae template and then converted into a gray image.
[15]	2015	Fingerprint	Medium	Encode the prior knowledge of fingerprint ridge structure through the direction patch and continuous phase patch dictionary, and then reconstruct the direction field and ridge pattern.
[16]	2010	Face	Medium	Reconstruct face image using HC based on Bayesian adaptation.
[17]	2014	Face	Medium	Reconstruct the real-valued template from the binary template using perceptual learning, and then use HC to iterate out the real-value template that meets the conditions.
[18]	2018	Face	Medium	Reconstruct face image from a deep face template using neighbor deconvolutional neural network.
[19]	2010	Iris	Medium	Divide the initial template into blocks of the same size and modify the pixel value in units of blocks.
[20]	2011	Iris	Medium	Generate feature texture from the iris template and embed it into a real iris image.
[21]	2013	Iris	Medium	Reconstruct real-value template from binary template using GA.
[22]	2018	Fingerprint	High	Reconstruct fingerprint image from fingerprint minutiae template using conditional adversarial networks.
[23]	2019	Iris	High	Reconstruct fingerprint image using RasGAN.

2.2. Coding-Based Palmprint Recognition

Palmprint has many advantages. In addition, many feature extractors of other biometric modalities are suitable for palmprint, so palmprint is an important and representative biometric modality [24,25]. Many palmprint recognition methods were proposed based on subspace, statistic, deep learning [26], coding, etc. Compared with the others, coding-based methods have low computation complexity, low storage cost, and can be free from training [27]. Meanwhile, coding-based methods are insensitive to illumination variances. Coding-based methods are popular for palmprint recognition, so FAA is conducted on six coding-based palmprint recognition methods in this paper, namely palm code (PC) [28], fusion code (FC) [29], competitive code (CC) [30], ordinal code (OC) [31], robust line orientation code (RLOC) [32], binary orientation co-occurrence vector (BOCV) [33], double orientation code (DOC) [34], and discriminative and robust competitive code (DRCC) [35]. Please note that the FAA developed is also suitable for other palmprint recognition methods.

2.3. Palmprint Template Protection

Biometric protection can be briefly categorized into cancellable biometric and biometric cryptosystems.

Cancellable biometric refers to the intentional and systematically repeatable distortion of biometric features in order to protect sensitive user-specific data. If a cancellable feature is compromised, the distortion characteristics are changed, and the same biometric is mapped to a new template, which is used subsequently [36]. Three goals of cancellable biometric follow.

Changeability: It is also reusability/revocability or diversity, i.e., straightforward revocation and reissue in the event of compromise. In addition, no same cancellable features can be used across various applications, therefore a large number of protected templates from the same biometric feature are required.

Noninvertibility: Noninvertibility of template computation is to prevent the recovery of original biometric image.

Accuracy: The protection should not deteriorate the recognition accuracy, in other words, the accuracy of the protected templates should approximate that of the original feature templates.

Some cancellable palmprint methods were proposed for palmprint template protection. The parameters of filters are randomly disturbed to generate cancellable palmprint templates [37]; however, the noninvertibility is not satisfactory. PalmHash Code and PalmPhasor Code are two important coded cancellable palmprint templates [38]. The security of PalmPhasor Code is higher than PalmHash Code, while its computational complexity is also higher than PalmHash Code [39]. Actually, the correlation between the adjacent entries in the cancellable template should be low to resist statistical analysis attack, so the filtered texture feature matrix before 2D cancellable transformation was transposed to suppress the vertical correlation between the adjacent entries in the cancellable template [40] and improve the accuracy [41]. Since the horizontal correlation between the adjacent entries is absent in 2DPalmHash Code and 2DPalmPhasor Code, horizontal-shift matching can be ignored. Therefore, the multiple-shift matching can be greatly simplified. This simplified matching has three advantages, namely reduction of matching complexity, enhancement of changeability performance, and improvement of verification performance [42]. Although the cancellable transformations are noninvertible, they are not strictly one-way. The similarity between two feature templates in feature domain is typically preserved between two cancellable templates in cancellable domain, so RA is valid for a cancellable biometric [8].

In biometric cryptosystems, the extracted/recovered bio-keys are used as the authenticators. Fuzzy commitment and fuzzy vault are two mainstream biometric cryptosystems. The palmprint cryptosystems were successfully developed based on fuzzy commitment and fuzzy vault [43,44]. The extracted/recovered bio-keys can be protected with a one-way hash function; accordingly, there is no available correlation between output and input of the hash function, so RA is disabled for the biometric cryptosystem.

3. Methodology and Evaluation

3.1. Framework

The framework of palmprint FAA with deepconvolutional GAN (DCGAN) is shown in Figure 7. The region of interest (ROI) is localized and cropped from the original palmprint image for recognition. DCGAN is employed to generate a large number of fake ROI palmprint images. The fake image set consists of the fake images used to impersonate a genuine user. FAA is successful once one fake image can impersonate the genuine user; that is, the similarity in feature domain is satisfied.

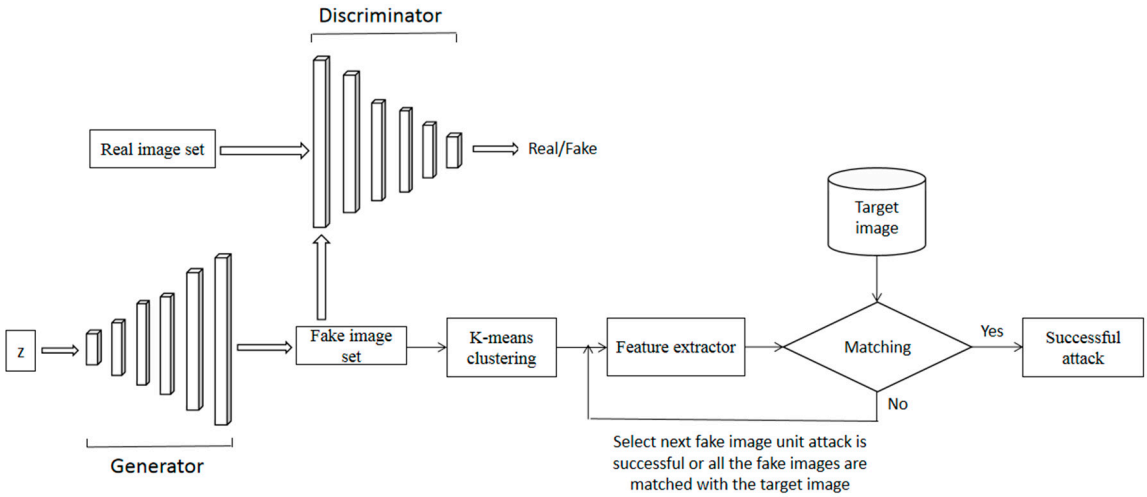


Figure 7. Framework of palmprint false acceptance attack with deepconvolutional GAN (DCGAN).

3.2. Image Generation

We selected DCGAN to generate the fake palmprint images used for FAA because of the following advantages:

- DCGAN is stable in training in most cases, so it is suitable for palmprint image generation if the number of the palmprint training images is not very large. In addition, the batch normalization in DCGAN can effectively suppress overfitting and accelerate convergence.
- DCGAN can generate the fake images with high resolution.
- The main hypothesis of this work is that the features (after feature extraction) of fake palmprints, which are generated from the DCGAN, are diverse. This is because if the fake palmprint feature templates are similar (lacking of diversity), then it is difficult for FAA to attack successfully. In other words, the greater the diversity of fake images, the higher the success rate of FAA. This hypothesis is experimentally confirmed by the red curves (imposter fake) in Figure 11. The distances between the fake palmprint templates are large, which demonstrates that the feature templates of the fake palmprint images, which are extracted from the DCGAN, are highly dissimilar; i.e., the diversity in feature domain is high.

DCGAN employs several techniques for optimization:

- Fully convolutional neural network—strided convolution is used instead of spatial pooling, which allows the network to learn more appropriate spatial downsampling methods.
- Avoidance of the fully connected layer after the convolution layer—although the fully connected layer increases the stability of the model, it also slows the convergence speed.
- Batch normalization is used in all the layers except for the output layer of generator and the input layer of discriminator. Even if the initialization is poor, batch normalization can ensure that the gradients in the network are strong enough.

- Effective activation functions—for the generator, Tanh and ReLu are used as the activation functions of the output layer and other layers, respectively. For the discriminator, leaky ReLU is used as the activation function.

The configuration of DCGAN in this paper is shown in Table 3.

Table 3. Configuration of DCGAN; 4 × 4 conv1 represents the size of the first layer of convolution kernel and 512 represents the size of the output feature map.

Layer	Generator	Discriminator
1	Input:1 × 1 × 128 4 × 4 convTrans1: 512, stride = 2 BatchNormalization ReLU	Input: 128 × 128 4 × 4 conv1: 16, stride = 1 BatchNormalization LeakyReLU
2	4 × 4 convTrans2: 256, stride = 2 BatchNormalization ReLU	4×4 conv2: 32, stride = 2 BatchNormalization LeakyReLU
3	4 × 4 convTrans3: 128, stride = 2 BatchNormalization ReLU	4×4 conv3: 64, stride = 1 BatchNormalization LeakyReLU
4	4 × 4 convTrans4: 64, stride = 2 BatchNormalization ReLU	4 × 4 conv4: 128, stride = 2 BatchNormalization LeakyReLU
5	4 × 4 convTrans5: 32, stride = 2 BatchNormalization ReLU	4 × 4 conv5: 256, stride = 1 BatchNormalization LeakyReLU
6	4 × 4 convTrans3: 16, stride = 2 Tanh( )	4 × 4 conv3: 16, stride = 2 LeakyReLU

3.3. Clustering for Diversity Enhancement

Quickly finding the fake image that can impersonate the genuine user successfully is desired. In FAA, if one fake image fails to attack, it is highly probable that its similar fake images also fail to attack. Thus, the fake image set with low dissimilarity, i.e., the fake image set in which the fake images are highly similar to each other, commonly leads to a large number of idle attacks. The attack times can be calculated by how many fake images are used to impersonate the genuine user until FAA is successful. For example, 10,000 fake images are used to impersonate the genuine user, the 10,000th fake image impersonates the genuine user successfully while the former 9999 fake images fail, and then the number of the attack times is 10,000. In practical attacks, attackers want the number of attack times to be as small as possible; they can then quickly find the fake image that can successfully impersonate the genuine user.

Since DCGAN also suffers from a mode collapse problem as in other GAN models, the diversity of the fake images is insufficient and can be further enhanced. If one fake image cannot impersonate the genuine user successfully, then it is highly probably that its similar fake images cannot impersonate the genuine user successfully either. If the diversity in the fake image set is enhanced, the attack times can be reduced.

Thus, K-means clustering is conducted on the fake image set as follows to enhance the diversity and accordingly reduce the number of attack times.

Input: The original dataset contains 40,000 fake images.

Output: The clustered dataset contains 20,000 fake images that are selected from the original dataset.

Step 1. Randomly select 20,000 fake images from the original dataset as the centroids of 20,000 classes.

Step 2. Compute the distance between each fake image in the original dataset and each centroid. If the distance is less than a threshold, this fake image is considered as a sample of the class of this centroid.

Step 3. Recompute the centroids of the 20,000 classes.

Step 4. If the 20,000 centroids before and after Step 3 are sufficiently close, i.e., the distance between the centroid before Step 3 and its corresponding centroid after Step 3 is less than a threshold, the state is converged and the algorithm is stopped; otherwise, repeat Steps 2–4.

After K-means clustering, 40,000 fake images are clustered to 20,000 classes. The first fake image of each class is selected, and the selected 20,000 fake images reconstitute the fake image set with diversity enhancement. Since the diversity is enhanced, the number of attack times is accordingly reduced.

In general, image-level attacks can be conducted in either online or offline mode. Online attacks can easily trigger blocking the ID after a few failed attack attempts. In offline attacks, repetitive attacks are allowed. FAA is in offline mode and not for real-time deployment. The needed time depends on the number of attacks until the first successful attack. For example, if the system is attacked first successfully by the n-th fake image, then the number of attacks is n. The computational complexity of every time attack is the same as that of every time matching operation.

3.4. Evaluation

The similarity goal in feature domain is that the reconstructed fake image can generate the fake template that is similar to the genuine user's target template. However, the reconstructed fake images typically do not have sufficient naturalness; that is, they have a remarkable counterfeit appearance that reveals they are not captured in natural environments. In other words, the existing RA methods only consider similarity in feature domain, while neglecting the naturalness in image domain.

"Similarity" means that the distance between two templates is less than a set threshold.

$$\mathrm{dis}(\mathbf{F1},\mathbf{F2}) \leq \tau \tag{1}$$

where **F1** and **F2** are two templates and τ is the set threshold.

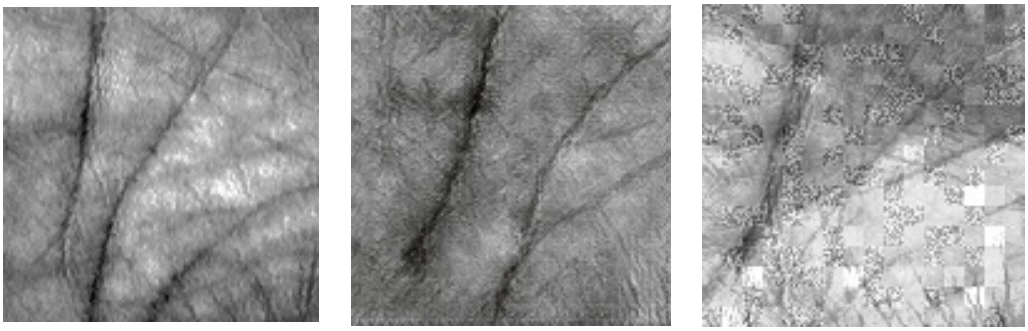
"Naturalness" means an image seems natural rather than counterfeit. Counterfeiting typically damages correlation and reduces the correlation coefficient, so the correlation coefficient can be used to measure the naturalness. The correlation coefficient is:

$$\rho = \frac{\mathrm{Cov}(X, Y)}{\sqrt{\mathrm{Var}(X)\mathrm{Var}(Y)}} \tag{2}$$

where X and Y are the variances of two adjacent pixels in an image, respectively. Cov() and Var() denote covariance and variance functions, respectively, and $\varrho \in [-1, 1]$. If an image has strong noise or noiselike appearance, it seems remarkably counterfeited and its correlation coefficient is low. An image without sufficient naturalness can be easily detected and resisted against. A smaller ϱ indicates a stronger counterfeit appearance (i.e., noise or noiselike appearance).

Figure 8 shows the naturalness of three image samples, namely, target images (real image), fake images in this paper, and fake images reconstructed with GA [21]. The fake images (Figure 8b) and (Figure 8c) are indeed very different from the target image (Figure 8a); however, their feature templates are highly similar. Thus, (Figure 8b) and (Figure 8c) can cheat a palmprint biometric system since the similarity measure takes place in feature domain rather than in image domain. The similarities in image domain and feature domain are nonequivalent. Neither (Figure 8b) nor (Figure Figure 8c) satisfies the similarity in image domain, but they both satisfy the similarity in feature domain.

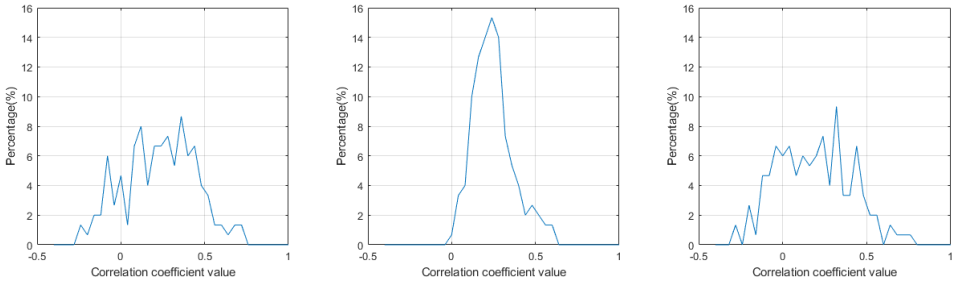
Some RA methods, including the GA used to create Figure 8c, combine a noiselike fake image and a real image to improve naturalness; i.e., the fake image is the fusion of a noiselike image and a real image at image level. The noiselike image has good similarity while the real image has good naturalness, so the fake image as a combination/fusion is a compromise between similarity and naturalness, and accordingly has a lower counterfeit appearance. It is desired that the system can automatically identify these fake images in terms of naturalness.



(**a**) Target image (**b**) Fake image using DCGAN (**c**) Fake image using GA

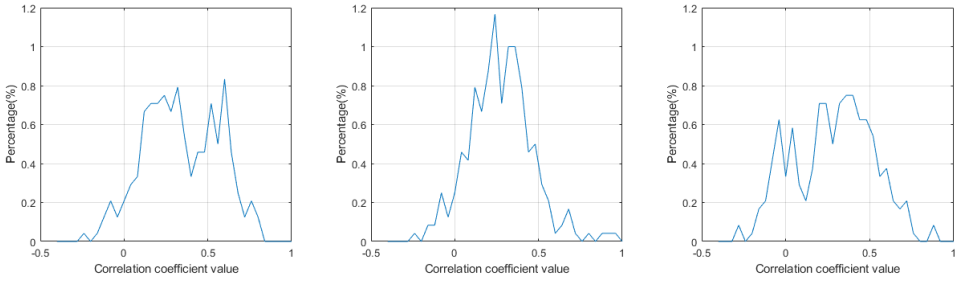
Figure 8. Image samples in three image sets.

The correlations in different parts of Figure 8c are highly different, so the average correlation coefficient of the whole image in Figure 8c is approximate to those of Figure 8a,b. Thus, the correlation is calculated in each block of an image to better detect and discriminate the counterfeit appearance. The ROI image size and block size are 128 × 128 and 8 × 8, respectively, so the block number is 16 × 16 = 256. Figure 9 shows the histograms of the correlation coefficient of the whole image in three image sets. Figure 10 shows the histograms of the correlation coefficient of the block in the three image sets.



(**a**) (**b**) (**c**)

Figure 9. Histograms of the correlation coefficient of the whole image in three image sets. (**a**) Target images, (**b**) fake images using DCGAN, and (**c**) fake images using GA.



(**a**) (**b**) (**c**)

Figure 10. Histograms of the correlation coefficient of the block in three image sets. (**a**) Target images, (**b**) fake images using DCGAN, and (**c**) fake images using GA.

In Figure 9, it is difficult to distinguish (Figure 9c) from (Figure 9a). The abscissa range of (Figure 9b) is narrower than (Figure 9a), which implies that the correlation coefficients in (Figure 9b) also exist in (a), so it is also difficult to distinguish (Figure 9c) from (Figure 9a).

In Figure 10, (Figure 10c) shows more blocks in an image with small correlation coefficients than (Figure 10a) and (Figure 10b). For example, there are more blocks in (Figure 10c) that have small (less than 0) correlation coefficients than (Figure 10a) or (Figure 10b).

According to our observation and analysis above, two thresholds are used to measure the naturalness; i.e., an image is real or fake. T1 is the correlation threshold and T2 is the number threshold. D(T1,T2) means an image has at least T2 blocks whose correlation coefficients are less than or equal to T1. A smaller T1 and a larger T2 means that more blocks in an image have lower correlation coefficients, and then it is more likely that the image is fake.

4. Experiments and Discussion

4.1. Dataset

All experiments were tested on the public palmprint dataset, the PolyU dataset, containing 7752 palmprint images from 386 different palms collected in two sessions. Each palm provided around 20 images, each person provided around 40 images.

Four thousand images of 200 palms were used as the training images to train DCGAN. One hundred fifty images in the remaining 186 palms were selected as the target images to compose the FAA test set. The 150 target images were of 25 palms; i.e., each palm had six images.

4.2. Matching Distance Distributions

Normalized Hamming distance was used as the matching distance to measure the dissimilarity. One hundred fifty fake images were randomly selected from the fake image set, which corresponded to 150 classes/palms. Four distance distributions were calculated, as shown in Table 4. The four distance distributions of different coding-based palmprint recognition methods are shown in Figure 11.

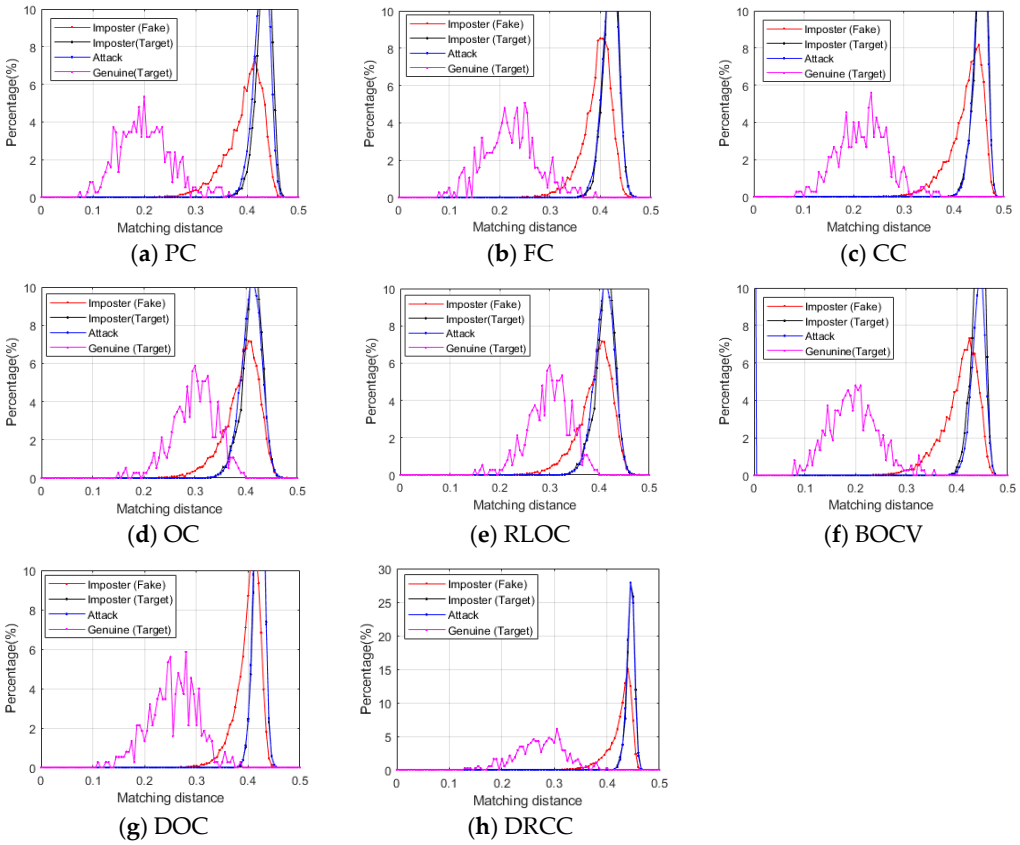


Figure 11. Four distance distributions. (**a**) palm code (PC), (**b**) fusion code (FC), (**c**) competitive code (CC), (**d**) ordinal code (OC), (**e**) robust line orientation code (RLOC), (**f**) binary orientation co-occurrence vector (BOCV), (**g**) double orientation code (DOC), and (**h**) discriminative and robust competitive code (DRCC)

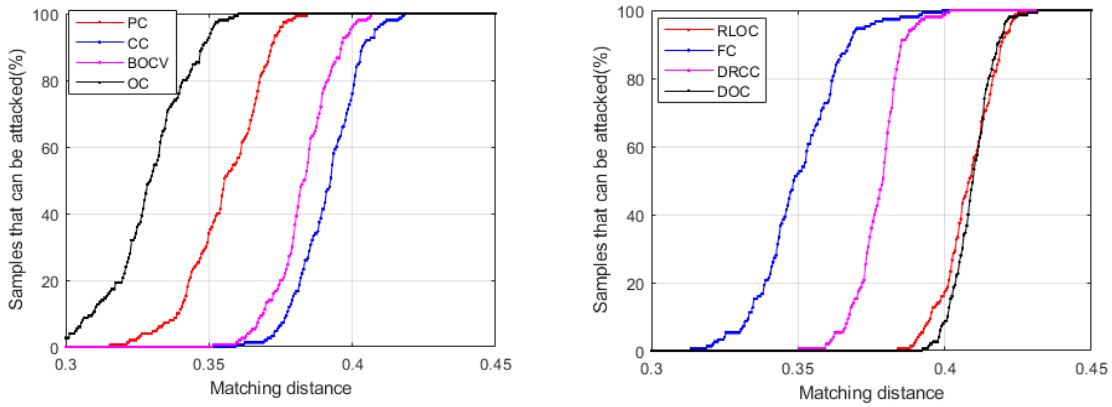
Table 4. Four distance distributions.

Distributions	Matching between
Imposter (Fake)	Two images in 150 fake images
Imposter (Target)	Two images of the different classes in 150 target images
Attack	One image in 150 fake images and one image in 150 target images
Genuine (Target)	Two images of the identical class in 150 target images

Imposter (Fake) distribution is on the right of Genuine (Target) distribution, so the diversity of fake images is good. However, Imposter (Fake) distribution is on the left of Imposter (Target) distribution, so the diversity of fake images is worse than that of target images. When the fake images are used for FAA, Attack distribution and Imposter (Target) distribution almost totally overlap, so the Attack distribution approximates the Imposter (Target) distribution.

4.3. Success Rate

The success rates of FAA, i.e., the ratios between the target images attacked successfully and the total target images, are shown in Figure 12. The eight palmprint coding methods are divided into two groups for clear comparison The success rates of FAA increase with the increment of distance threshold.

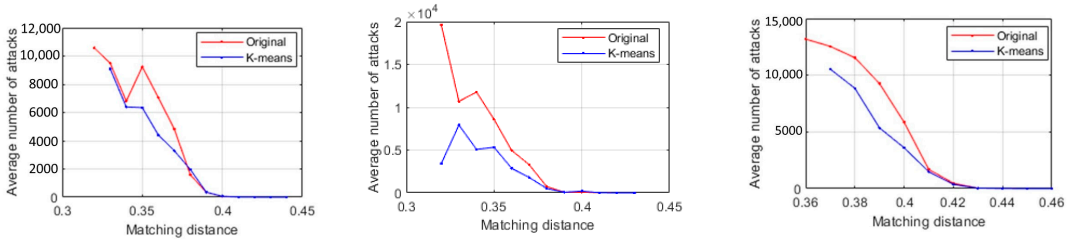


(**a**) (**b**)

Figure 12. Success rates of FAA. (**a**) Group 1; (**b**) Group 2

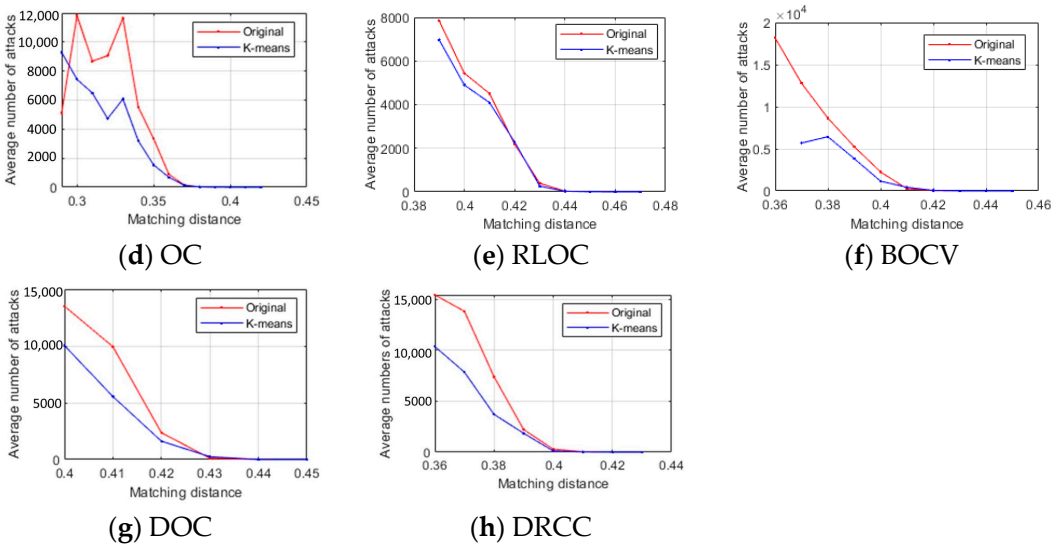
4.4. Reduction of Number of Attack Times

The attack times can be calculated by the number of the fake images used to impersonate the genuine user until FAA is successful. The original results are tested on a fake image set containing 40,000 fake images, while the K-means results are tested on the fake image set after K-means clustering, which contains 20,0000 fake images. The comparisons in Figure 13 confirm that the clustering can effectively reduce the number of attack times.



(**a**) PC (**b**) FC (**c**) CC

Figure 13. *Cont.*



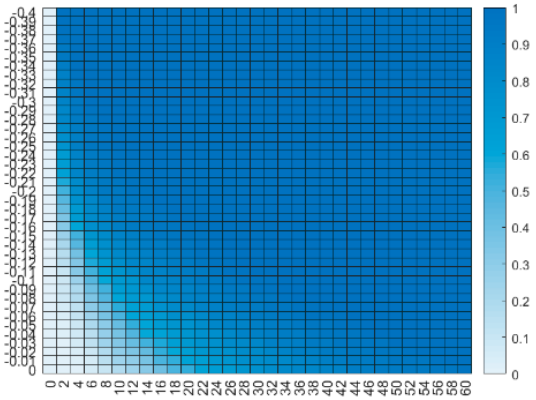
(**d**) OC (**e**) RLOC (**f**) BOCV

(**g**) DOC (**h**) DRCC

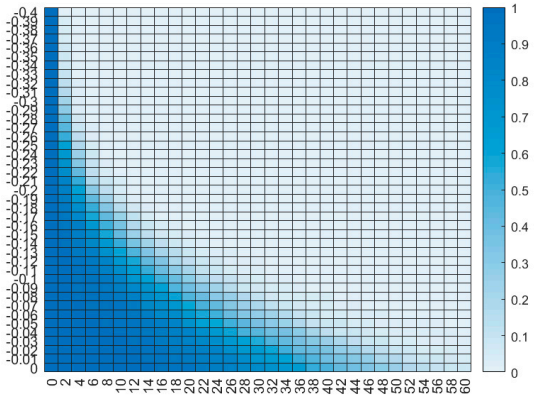
Figure 13. Attack times.

4.5. Naturalness

The naturalness is tested on three image sets, including the target images and fake images in this paper; fake images are reconstructed with GA [21]. Figure 14 shows the accuracies of real/fake detection according to D(T1,T2). Row indices and column indices correspond to T1 and T2, respectively.

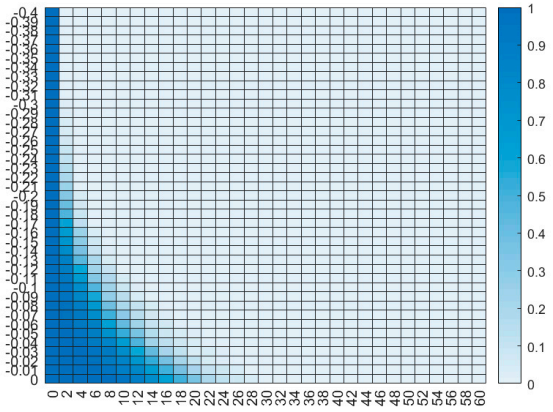


(**a**) Target image



(**b**) Fake image using DCGAN

Figure 14. *Cont.*



(**c**) Fake image using GA

Figure 14. Real/fake detection accuracy.

When T1 = −0.06 and T2 = 18, equal error rate (EER) minimizes at 23%; i.e., 76.67% of the target images are correctly judged as real images, while 76.67% of the fake images using GA are correctly judged as fake images. However, 97.33% of the fake images using DCGAN are judged as real images. Actually, a fake image using GA in [21] is the fusion of a noiselike image and a real image at image level, so it has better naturalness than the fake images in most other RAs. It is challenging to judge the fake images in [21] as to their being either real or fake. However, compared with the fake images in [21], more fake images with DCGAN in this paper are judged as real images, which demonstrates that the fake images in this paper have better naturalness, so FAA in this paper outperforms [21] in terms of naturalness.

5. Conclusions and Future Works

Palmprint has several advantages and is a representative biometric modality. Thus, we develop FAA for palmprint biometrics and demonstrate its feasibility against coding-based palmprint biometric systems. The FAA is free from the issues found in RA and PA. FAA does not require genuine users' images, and it can be launched simply with the synthetic images with high naturalness, which are generated by the generative adversarial networks. The naturalness of the reconstructed images is neglected in PA, so the FAA is a more fraudulent attack than RA. To further improve the efficiency of FAA, we employ a clustering method to select diverse fake images in order to enhance the diversity of the fake images used, so the number of attack attack times is reduced; i.e., the attackers can more quickly find the fake image in the fake image set, which can cheat the system successfully. In our future work, we will modify and improve GAN to enhance diversity to further increase the attack success rate. We will also try to develop more strategies to decrease the number of attack times.

Author Contributions: Conceptualization, L.L. and F.W.; methodology, L.L., F.W. and A.B.J.T.; software, F.W.; validation, L.L. and J.C.; formal analysis, L.L., F.W. and A.B.J.T.; investigation, L.L. and F.W.; resources, L.L. and F.W.; data curation, F.W.; writing—original draft preparation, F.W.; writing—review and editing, L.L., J.C. and A.B.J.T.; visualization, F.W.; supervision, L.L.; project administration, L.L.; funding acquisition, J.C. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Natural Science Foundation of China (61866028, 61663031), Key Program Project of Research and Development (Jiangxi Provincial Department of Science and Technology) (20171ACE50024, 20192BBE50073) Foundation of China Scholarship Council (CSC201908360075).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Jain, A.K.; Nandakumar, K.; Ross, A. 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recognit. Lett.* **2016**, *79*, 80–105. [CrossRef]

2. Teoh, A.B.J.; Leng, L. Editorial: Special issue on advanced biometrics with deep learning. *Appl. Sci.* **2020**, *10*, 4453. [CrossRef]
3. Li, Q.; Dong, P.; Zheng, J. Enhancing the security of pattern unlock with surface EMG-Based biometrics. *Appl. Sci.* **2020**, *10*, 541. [CrossRef]
4. Faundez-Zanuy, M. On the vulnerability of biometric security systems. *IEEE Aerosp. Electron. Syst. Mag.* **2004**, *19*, 3–8. [CrossRef]
5. Shao, R.; Lan, X. Multi-adversarial discriminative deep domain generalization for face presentation attack detection. In Proceedings of the Conference on Computer Vision and Pattern Recognition, Long Beach, CA, USA, 16–20 June 2019; pp. 10023–10031.
6. Maiorana, E.; Hine, G.E.; Campisi, P. Hill-climbing attacks on multibiometrics recognition systems. *IEEE Trans. Inf. Forensics Secur.* **2014**, *10*, 900–915. [CrossRef]
7. Pititheeraphab, Y.; Thongpance, N.; Aoyama, H.; Pintavirooj, C. Vein pattern verification and identification based on local geometric invariants constructed from minutia points and augmented with barcoded local feature. *Appl. Sci.* **2020**, *10*, 3192. [CrossRef]
8. Wang, H.; Dong, X.; Jin, Z. Security analysis of cancellable biometrics using constrained-optimized similarity-based attack. *arXiv* **2020**, arXiv:2006.13051.
9. Uludag, U.; Jain, A.K. Attacks on biometric systems: A case study in fingerprints. In Proceedings of the IEEE International Conference on Electronic Image, San Jose, CA, USA, 22–25 June 2014; pp. 622–633.
10. Ross, A.; Shah, J.; Jain, A.K. From template to image: Reconstructing fingerprints from minutiae points. *IEEE Trans. Pattern Anal. Mach. Intell.* **2007**, *29*, 544–560. [CrossRef]
11. Adler, A. Images can be regenerated from quantized biometric match score data. In Proceedings of the IEEE International Conference on Electrical and Computer Engineering, Niagara Falls, ON, Canada, 2–5 May 2004; pp. 469–472.
12. Dong, X.; Jin, Z.; Jin, A.T.B. A genetic algorithm enabled similarity-based attack on cancellable biometrics. *arXiv* **2019**, arXiv:1905.03021.
13. Salimans, T.; Goodfellow, I.; Zaremba, W. Improved techniques for training GANs. *NeurIPS* **2016**, *265*, 2234–2242.
14. Feng, J.; Jain, A.K. Fingerprint reconstruction: From minutiae to phase. *IEEE Trans. Pattern Anal. Mach. Intell.* **2010**, *33*, 209–223. [CrossRef] [PubMed]
15. Cao, K.; Jain, A.K. Learning fingerprint reconstruction: From minutiae to image. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 104–117. [CrossRef]
16. Galbally, J.; McCool, C.; Fierrez, J. On the vulnerability of face verification systems to hill-climbing attacks. *Pattern Recognit.* **2010**, *43*, 1027–1038. [CrossRef]
17. Feng, Y.C.; Lim, M.H.; Yuen, P.C. Masquerade attack on transform-based binary-template protection based on perceptron learning. *Pattern Recognit.* **2014**, *47*, 3019–3033. [CrossRef]
18. Mai, G.; Cao, K.; Yuen, P.C. On the reconstruction of face images from deep face templates. *IEEE Trans. Pattern Anal. Mach. Intell.* **2018**, *41*, 1188–1202. [CrossRef]
19. Rathgeb, C.; Uhl, A. Attacking iris recognition: An efficient hill-climbing technique. In Proceedings of the IEEE International Conference on Pattern Recognition, Istanbul, Turkey, 23–26 August 2010; pp. 1217–1220.
20. Venugopalan, S.; Savvides, M. How to generate spoofed irises from an iris code template. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 385–395. [CrossRef]
21. Galbally, J.; Ross, A.; Gomez-Barrero, M. Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms. *Comput. Vis. Image Underst.* **2013**, *117*, 1512–1525. [CrossRef]
22. Kim, H.; Cui, X.; Kim, M. Reconstruction of fingerprints from minutiae using conditional adversarial networks. In Proceedings of the International Workshop on Digital Forensics and Watermarking, Jeju Island, Corea, 10–13 August 2018; pp. 353–362.
23. Yadav, S.; Chen, J.C. Synthesizing iris images using RaSGAN with application in presentation attack detection. In Proceedings of the Conference on Computer Vision and Pattern Recognition, Long Beach, CA, USA, 16–20 June 2019.
24. Leng, L.; Zhang, J.S.; Khan, M.K.; Chen, X. Khaled Alghathbar. Dynamic weighted discrimination power analysis: A novel approach for face and palmprint recognition in DCT domain. *Int. J. Phys. Sci.* **2010**, *5*, 2543–2554.

25. Leng, L.; Li, M.; Kim, C.; Bi, X. Dual-source discrimination power analysis for multi-instance contactless palmprint recognition. *Multimed. Tools Appl.* **2017**, *76*, 333–354. [CrossRef]
26. Izadpanahkakhk, M.; Razavi, S.M.; Taghipour-Gorjikolaie, M.; Zahiri, S.H.; Uncini, A. Deep region of interest and feature extraction models for palmprint verification using convolutional neural networks transfer learning. *Appl. Sci.* **2018**, *8*, 1210. [CrossRef]
27. Leng, L.; Yang, Z.Y.; Min, W.D. Democratic voting downsampling for coding-based palmprint recognition. *IET Biom.* **2020**, *9*, 290–296. [CrossRef]
28. Zhang, D.; Kong, W.; You, J.; Wong, M. Online palmprint identification. *IEEE Trans. Pattern Anal. Mach. Intell.* **2003**, *25*, 1041–1050. [CrossRef]
29. Kong, A.W.; Zhang, D. Feature-Level Fusion for effective palmprint authentication. In Proceedings of the 1st ICBA Conference on Biometric Authentication, Hong Kong, China, 15–17 July 2004; Springer: Berlin/Heidelberg, Germany; pp. 761–767.
30. Kong, A.K.; Zhang, D. Competitive coding scheme for palmprint verification. In Proceedings of the 17th International Conference on Pattern Recognition, 23–27 September 2004; pp. 1051–4651.
31. Sun, Z.; Tan, T.; Wang, Y. Ordinal palmprint represention for personal identification [represention read representation]. In Proceedings of the IEEE International Conference on Computer Vision & Pattern Recognition, San Diego, CA, USA, 20–25 June 2005; pp. 1063–6919.
32. Jia, W.; Huang, D.; Zhang, D. Palmprint verification based on robust line orientation code. *Pattern Recognit.* **2008**, *41*, 1504–1513. [CrossRef]
33. Guo, Z.H.; Zhang, D.; Zhang, L.; Zuo, W.M. Palmprint verification using binary orientation co-occurrence vector. *Pattern Recognit.* **2009**, *30*, 1219–1227. [CrossRef]
34. Fei, L.; Xu, Y.; Tang, W.; Zhang, D. Double-orientation code and nonlinear matching scheme for palmprint recognition. *Pattern Recognit.* **2016**, *49*, 89–101. [CrossRef]
35. Xu, Y.; Fei, L.; Wen, J.; Zhang, D. Discriminative and robust competitive code for palmprint recognition. *IEEE Trans. Syst. Man Cybern. Syst.* **2018**, *48*, 232–241. [CrossRef]
36. Ghammam, L.; Karabina, K.; Lacharme, P.; Thiry-Atighehchi, K. A cryptanalysis of two cancelable biometric schemes based on index-of-max hashing. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 2869–2880. [CrossRef]
37. Leng, L.; Zhang, J.S.; Khan, M.K.; Chen, X.; Ji, M.; Alghathbar, K. Cancelable PalmCode generated from randomized Gabor filters for palmprint template protection. In Proceedings of the Conference on Image and Vision Computing, Queenstown, New Zealand, 8–9 November 2010; pp. 1–6.
38. Leng, L.; Zhang, J.S. PalmHash Code vs. PalmPhasor Code. *Neurocomputing* **2013**, *108*, 1–12. [CrossRef]
39. Leng, L.; Teoh, A.B.J.; Li, M.; Khan, M.K. A remote cancelable palmprint authentication protocol based on multi-directional two-dimensional PalmPhasor-fusion. *Secur. Commun. Netw.* **2014**, *7*, 1860–1871. [CrossRef]
40. Leng, L.; Teoh, A.B.J.; Li, M.; Khan, M.K. Analysis of correlation of 2DPalmHash Code and orientation range suitable for transposition. *Neurocomputing* **2014**, *131*, 377–387. [CrossRef]
41. Leng, L.; Teoh, A.B.J.; Li, M.; Khan, M.K. Orientation range of transposition for vertical correlation suppression of 2DPalmPhasor Code. *Multimed. Tools Appl.* **2015**, *74*, 11683–11701. [CrossRef]
42. Leng, L.; Teoh, A.B.J.; Li, M. Simplified 2DPalmHash code for secure palmprint verification. *Multimed. Tools Appl.* **2017**, *76*, 8373–8398. [CrossRef]
43. Leng, L.; Zhang, J.S. Dual-key-binding cancelable palmprint cryptosystem for palmprint protection and information security. *J. Netw. Comput. Appl.* **2011**, *34*, 1979–1989. [CrossRef]
44. Leng, L.; Teoh, A.B.J. Alignment-free row-co-occurrence cancelable palmprint Fuzzy Vault. *Pattern Recognit.* **2015**, *48*, 2290–2303. [CrossRef]