15th IAPR International Conference on Machine Vision Applications (MVA)
Nagoya University, Nagoya, Japan, May 8-12, 2017.

Histogram of Oriented Gradients based Presentation Attack Detection in Dorsal Hand-Vein Biometric System

Shruti Bhilare*, Vivek Kanhangad† and Narendra Chaudhari‡
Indian Institute of Technology Indore
{phd12110103*, kvivek†, nsc‡}@iiti.ac.in

Abstract

Biometric recognition, which is an integral part of the present-day security solutions, faces a major threat from presentation or spoofing attacks. In this paper, we present a novel presentation attack detection (PAD) approach for dorsal hand-vein based recognition system. The proposed approach performs Laplacian of Gaussian filtering on the acquired images, followed by extraction of histogram of oriented gradients (HoG) features at multiple scales. A linear SVM is employed for each scale and the final decision is obtained by combining individual decisions using the majority voting scheme. Experiments were carried out on 624 real images and 624 artefacts (spoof samples) collected from left and right hands of 52 subjects. Artefacts were generated independent of the enrollment images, by employing an off-the-shelf smartphone camera to capture the vein patterns from users' hands. These images were displayed using two different display devices and presented as artefacts to the biometric sensor. The experiments were carried out in the same-device and the cross-device scenarios. Our approach achieves average error rate of 0.16% and 0.8% in the same-device and the cross-device experiments, respectively and outperforms local binary patterns (LBP) based baseline algorithm.

1 Introduction

Due to the inherent advantages of using biometric traits for authentication over the traditional ways like passwords, biometric technology has emerged as a leading solution for physical identity and access management. Biometric solutions have been deployed in a wide range of applications like banking, e-commerce, border security and law enforcement. Moreover, there is an increasing interest to incorporate biometrics in various commercial products like mobile and wearable devices. With increasing number of deployments, safeguarding biometric systems against potential attacks is very crucial. Several studies have been conducted to assess the vulnerability of the face [1], iris [2], palmprint [3] and hand geometry based biometric systems. Researchers have also successfully spoofed fingerprint protected smartphones using a printed artefact [4]. These studies conclude that the biometric recognition systems are highly vulnerable to presentation attacks, which involve presenting a fake sample to the biometric sensor. Thus, in the past few years researchers have focused on developing anti-spoofing or PAD techniques to counter the presentation attacks.

Considering the vulnerability of the traditional biometric traits, researchers have explored vascular biometric traits such as palm-vein, finger-vein and dorsal hand-vein for biometric recognition [5]. Since these patterns are hardly visible in visible light, an NIR light source and an image sensor with sensitivity in the NIR spectrum are required to capture these vascular patterns. Hence, owing to the effort required to acquire the vein patterns, reproducing them is difficult if not impossible, making forgery of the vascular biometric systems tougher compared to the non-vascular biometric systems. Nonetheless, it has been shown that it is possible to spoof the vascular biometric systems with a very high false acceptance rate [6], [7]. It may be noted, however, that in most of the previous works [6], [7], the artefacts were generated using the real samples in the enrollment database. This method of artefact generation is practically very difficult to realize. Besides, with the prevalence of camera enabled mobile phones, the possibility of carrying out presentation attacks using them cannot be overruled. Hence, for artefact generation we have used an off-the-shelf smartphone camera having a sensitivity in the NIR spectrum coupled with an NIR light source.

In this work, we present a PAD approach to mitigate the effect of presentation attacks on dorsal hand-vein verification system. The paper is organized as follows. Section 2 and 3 detail the proposed PAD approach and the database used in this work. Section 4 presents the experimental results and section 5 concludes the paper.

2 Proposed PAD approach

In this section, we describe the major computational stages of the proposed PAD approach. Figure 1 shows the overview of the proposed approach. Firstly, the region of interest (ROI) is extracted from the dorsal hand image and is normalized using contrast limited adaptive histogram equalization (CLAHE). The ROI is then re-sized to 100×100 pixels and filtered using a Laplacian of Gaussian filter of size 5×5 pixels and variance 1.4. Figure 2 shows the resulting images of a real and two artefact samples belonging to a subject from the database. As can be observed from this Figure, there is a noticeable difference between the filtered images of real and fake samples. In particular, the vein pattern is more clearly visible in the real image while there is a lot of noise in filtered artefact images. This can be attributed to the use of smartphone camera to generate artefacts. Owing to the limited capabilities of the smartphone image sensor, the acquired images are considerably more noisy than their real counterparts which are acquired using the biometric sensor. Nevertheless, they can be employed to spoof the system with considerably high spoof false acceptance rate (SFAR) as shown in section 4. In the proposed approach, HoG [8] features are extracted from the filtered images at three different scales. Specifically, the images are par-

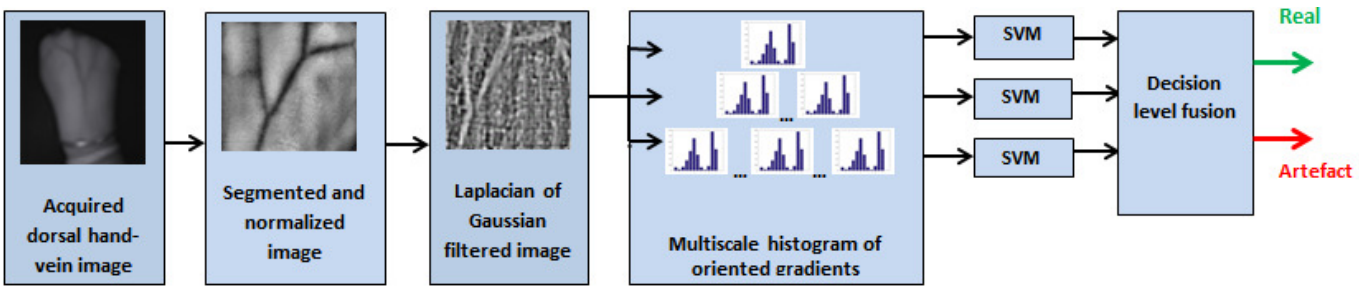


Figure 1. Overview of the proposed PAD approach

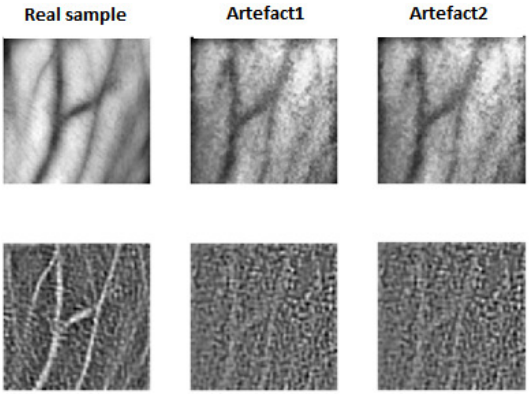


Figure 2. ROIs extracted from real sample and artefacts (top row). Corresponding Laplacian of Gaussian filtered images (bottom row)

titioned into cells of sizes 4×4, 25×25 and 50×50 pixels. These cells are grouped into blocks of size 2×2 cells with an overlap of 50% between adjoining blocks. The histogram of oriented gradients with 12 bins is computed for every cell in the image and histograms computed within a block are concatenated to form a feature vector representing the image at that scale. The above discussed process is performed for the three scales producing three feature vectors of length 27648, 432 and 48. In the final stage, the proposed approach employs linear SVMs, which utilize features extracted at three scales for classification of real images and artefacts. Further, the majority voting based decision level fusion is performed to obtain the final decision.

3 Database description

The enrollment database used for the dorsal hand-vein verification system consists of 624 images with six images each, acquired from left and right dorsal hands of 52 subjects. The images were acquired in an office space under no illumination condition. To minimize the effect of ambient light variations, a wooden box closed from all but the front side was used. Four LEDs with the peak wavelength of 850 nm were fixed on the upper four corners of the inside of the box. The imaging sensor, MvBlueFox-IGC with sensitivity in the visible and NIR spectrum was fixed on top of the box and was connected to a laptop with a USB cable. For each image capture, the subject placed his hand on the base of the box with the dorsal region of the hand facing upwards.

3.1 Artefact generation

In this work, we present the performance of the proposed PAD approach for two kinds of display artefacts. These artefacts were generated without assuming any access to the real images in the enrollment database. Instead, a more realistic approach was adopted in which a smartphone camera was used to acquire the vascular patterns from dorsal hands. Owing to the easy availability of smartphones, this way of attacking is highly plausible and also very effective as shown by the study in [9]. For artefact generation, the subjects were requested to place their hands on a flat surface and a ring of NIR LEDs was employed to illuminate the dorsal hand surface. Three images of dorsal hands acquired in this manner using a smartphone camera (HTC One E8) were displayed one by one on two devices and presented to the biometric sensor as artefacts. A smartphone (HTC One E8) with a screen size of 5 inches and resolution of 1080×1920 pixels and a tablet (Asus Fonepad 7) with screen size of 7 inches and resolution of 600×1024 pixels were used as display devices to generate two kinds of artefacts namely, artefact1 and artefact2, respectively.

4 Experimental results and discussion

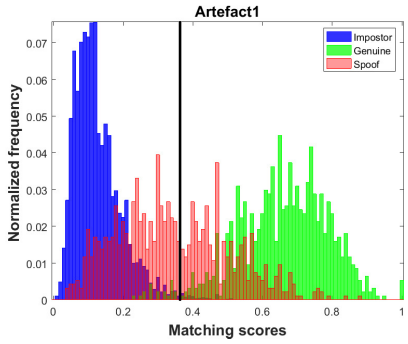
In this section we elaborate on the experimental protocols and results. Here, a study to show the vulnerability of the reference verification system is presented followed by performance evaluation of the proposed PAD approach.

4.1 Vulnerability study

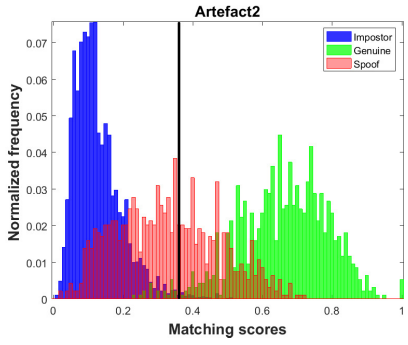
Firstly, we analyze how the performance of the biometric verification system is affected by the presentation attacks. In order to evaluate the biometric performance, the dataset was divided into training and testing partitions such that the first three real images per subject constituted the training partition and the remaining three samples constituted the test set. For matching, SIFT descriptors were computed at the keypoints in the images. In order to obtain the (dissimilarity) matching score between the two images, a distance vector comprising the euclidean distances between the SIFT descriptors extracted at matching keypoints was obtained. The root mean square value of the distance vector was then used as the distance score between two

images. The equal error rate (EER) for the biometric system was found to be 2.04%. Further, in order to assess the vulnerability of the system, the artefact samples were compared with the real samples from the training set to generate the spoof matching scores. Figure 3 shows the distributions of genuine, impostor and spoof matching scores. The threshold corresponding to the EER is indicated by the vertical solid line in Figure 3. The spoof distribution lying to the right of the line contributes to successful presentation attacks. The spoof false acceptance rate (SFAR) which represents the number of falsely accepted artefacts was found to be 42.62% and 45.72%, for artefact1 and artefact2, respectively.

It may be noted that the artefacts were not generated directly from the enrollment database, instead an intermediate step of image acquisition using the smartphone camera was employed, which deteriorated the quality of artefacts to a great extent. However, more than 40% of the generated artefacts qualified as the real samples which signifies high vulnerability of the hand-vein verification system to display based artefacts. Thus, it is imperative to employ a PAD technique prior to biometric verification.



(a)



(b)

Figure 3. Score distribution of the dorsal hand-verification system under attack

4.2 PAD performance evaluation

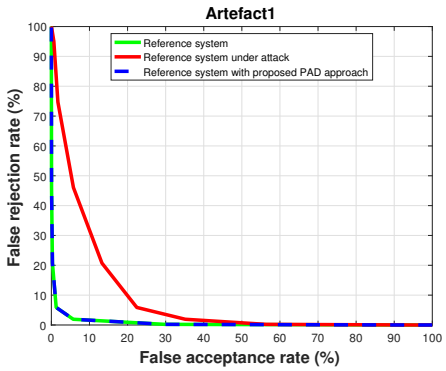
This section presents the performance of the proposed PAD approach in the same-device and cross-device scenarios. To the best of our knowledge there is no prior work for presentation attack detection in dorsal hand-vein biometrics. Hence, we compare the performance of our approach with LBP which is the most widely used PAD technique for biometric traits like iris and face[10]. Error rates defined in ISO/IEC WD 30107-3, attack presentation classification error rate (APCER), normal presentation classification error rate (NPCER) and average classification error rate (ACER) are reported for performance comparison.

4.2.1 Experiment 1: same-device scenario

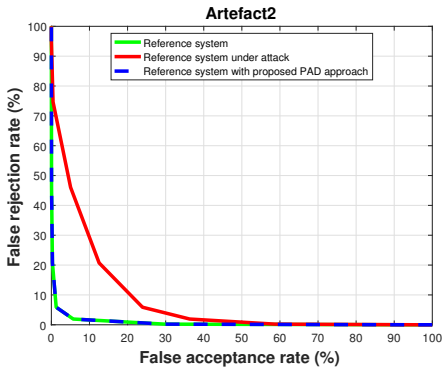
In the same-device scenario, three image samples per subject were considered from both real and artefact datasets and samples from first 50% of the subjects were used for training while remaining were used for testing. Table 1 shows the performance comparison of the proposed technique with 59 dimensional uniform LBP feature vector as employed in [10] for PAD. From the Table 1 it can be observed that the ACER for our approach is consistently better than LBP.

Table 1. Performance comparison of the proposed approach and LBP in same-device scenario

Attack	Method	APCER	NPCER	ACER
Artefact1	LBP	1.92	1.92	1.92
	Proposed	0.00	0.00	0.00
Artefact2	LBP	0.64	0.64	0.64
	Proposed	0.00	0.64	0.32



(a)



(b)

Figure 4. PAD performance

4.2.2 Experiment 2: cross-device scenario

In this set of experiments, artefacts generated from two different devices were used for training and testing to analyze the robustness of the proposed approach

to new display artefacts. Experimental protocol remains the same as in same-device scenario, except during the testing phase, artefacts belonging to the class other than the one used for training were used. Thus, when the artefacts belonging to artefact1 were used for training, testing was performed using the samples from artefact2 and vice-versa. Results shown in the Table 2 clearly demonstrate the superiority of our approach compared to LBP in the cross-device scenario as well. The DET curve in Figure 4 shows the effect of presentation attacks on the reference biometric system and the performance of the proposed PAD approach. In order to plot the curve, error rates were obtained from the real samples and artefacts from the second half subjects i.e. last 26 subjects. There is an evident increase in error rates when the verification system is exposed to presentation attacks. It may be noted that on employment of the proposed approach, the performance is nearly the same as that of the reference system under no attack. APCER achieved in our results clearly demonstrates that the approach completely bypasses the attack presentations thereby making the approach very useful for high security biometric solutions.

Table 2. Performance comparison of the proposed approach and LBP in cross-device scenario

Attack (Training)	Attack (Testing)	Method	APCER	NPCER	ACER
Artefact1	Artefact2	LBP	1.28	1.28	1.28
		Proposed	0.00	0.64	0.32
Artefact2	Artefact1	LBP	2.56	2.56	2.56
		Proposed	0.00	2.56	1.28

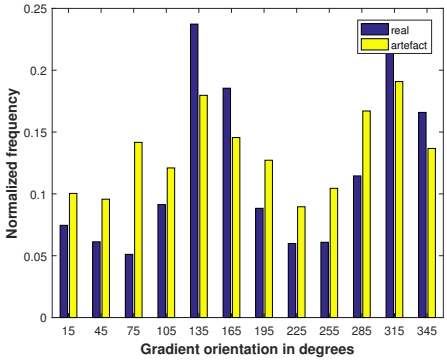


Figure 5. Histograms of oriented gradients for LoG filtered image of real sample and artefact

The high performance of the proposed approach can be attributed to the disparity in the orientation of the gradients obtained from the LoG filtered images. Figure 5 shows the histograms of gradients obtained from a block at scale 3 (cell size=4×4 pixels). As can be observed from the Figure, the histograms of the gradients from real images are more oriented in a specific direction depending on the vessel information than those from the artefacts which are more uniformly spread out and have smaller directional orientations. This may be associated with the blurring and noise induced in the artefacts during artefact generation and presentation.

5 Conclusion

This paper presents a presentation attack detection approach for the dorsal hand-vein biometric verification system. To the best of our knowledge this is the first work in presentation attack detection for dorsal hand-vein biometric. A database of left and right hands of 52 subjects was used in this study. The artefacts were collected independently of the real images in the enrollment database using a smartphone camera. Later these images were displayed on two display devices to generate two sets of display artefacts. The proposed approach is evaluated for both the artefacts in the same-device as well as cross-device scenarios. The proposed approach is also compared with LBP. Our approach outperforms LBP in most cases. In the worst case, our approach achieves average classification error rate of 0.32% compared to 1.92% for LBP in the same-device scenario. Also, in the cross-device scenario, our approach performs better than LBP with average classification error of 1.28% compared to 2.56% in the worst case. Thus, the results obtained in this work are encouraging and suggest employing a PAD module prior to deployment of the dorsal hand-vein verification system. Further, we plan to assess the applicability of the proposed approach for other vascular biometric traits.

References

[1] R. Raghavendra. et al.:"Presentation attack detection for face recognition using light field camera," *IEEE Trans. Image Process.*, vol.24, no.3, pp.1060–1075, 2015.

[2] R. Raghavendra. et al.:"Robust scheme for iris presentation attack detection using multiscale binarized statistical image features," *IEEE Trans. Inf. Forensics Security*, vol.10, no.4, pp.703-715, 2015.

[3] V. Kanhangad. et al.: Antispoong for display and print attacks on palmprint verication systems. In: SPIE Defense+Security. (2015) 94570E-94570E

[4] http://www.biometricupdate.com/201603/researchers-at-msu-spoof-a-fingerprint-protected-smartphone-using-an-inkjet-printer

[5] Y. Wang. et al.: "An automatic physical access control system based on hand vein biometric identification," *IEEE Transactions on Consumer Electronics*, vol.61, no.3, pp.320–327, 2015.

[6] P. Tome. et al.: On the vulnerability of palm vein recognition to spoofing attacks. In: ICB. (2015) 319-325

[7] P. Tome. et al.: On the vulnerability of finger vein recognition to spoofing. In: BIOSIG. (2014) 1-10

[8] N. Dalal. et al.: Histograms of oriented gradients for human detection. In: CVPR. (2005) 886-893

[9] I. Patil. et al.: Assessing vulnerability of dorsal hand-vein verication system to spoong attacks using smartphone camera. In: IEEE International Conference on Identity, Security and Behavior Analysis (ISBA). (2016) 1-6

[10] I. Chingovska. et al.: On the effectiveness of local binary patterns in face anti-spoofing. In: BIOSIG. (2012) 1-7