Anti-spoofing for Display and Print Attacks on Palmprint Verification Systems

Vivek Kanhangad[a], Shruti Bhilare[b], Pragalbh Garg[a], Pranjalya Singh[a], and Narendra Chaudhari[b]

[a]Discipline of Electrical Engineering
[b]Discipline of Computer Science and Engineering
Indian Institute of Technology Indore
Indore, India 453441
Email: kvivek@iiti.ac.in, phd12110103@iiti.ac.in, nsc@iiti.ac.in

ABSTRACT

A number of approaches for personal authentication using palmprint features have been proposed in the literature, majority of which focus on improving the matching performance. However, of late, preventing potential attacks on biometric systems has become a major concern as more and more biometric systems get deployed for wide range of applications. Among various types of attacks, sensor level attack, commonly known as spoof attack, has emerged as the most common attack due to simplicity in its execution. In this paper, we present an approach for detection of display and print based spoof attacks on palmprint verification systems. The approach is based on the analysis of acquired hand images for estimating surface reflectance. First and higher order statistical features computed from the distributions of pixel intensities and sub-band wavelet coefficients form the feature set. A trained binary classifier utilizes the discriminating information to determine if the acquired image is of real hand or a fake one. Experiments are performed on a publicly available hand image dataset, containing 1300 images corresponding to 230 subjects. Experimental results show that the real hand biometrics samples can be substituted by the fake digital or print copies with an alarming spoof acceptance rate as high as 79.8%. Experimental results also show that the proposed spoof detection approach is very effective for discriminating between real and fake palmprint images. The proposed approach consistently achieves over 99% average 10-fold cross validation classification accuracy in our experiments.

Keywords: Biometrics, Anti-spoofing, Surface Reflectance, Statistical Features, Palmprint Verification

1. INTRODUCTION

Automated palmprint authentication systems utilize discriminatory features extracted from low resolution palmprint images for personal verification. It is one of the biometric traits that enjoy a very high user acceptance as the characteristics can be acquired in a non intrusive and completely contact-free manner, causing very little inconvenience to the user. Palmprint based biometric systems have been extensively studied in the literature and several approaches have been proposed. Thus far, the research on palmprint biometrics has primarily focused on improving the matching performance. However, with increasing deployments of the biometrics based access systems, the threat of spoof attacks on these systems is on the rise. The threat is even more severe in unsupervised installations of the biometric systems. Therefore, there is an urgent need to develop reliable spoof detection techniques that are capable of reducing the vulnerability of palmprint authentications systems to such attacks. Possible attacks on a biometric system can be broadly classified into eight types[1] , including attacks at sensor level, replay attacks on data transfer channel between the sensor and feature extraction module, and attacks on the database. Among these, the most common and easiest way of circumventing a biometric system is to present fake biometric sample to the sensor, known as spoof attack. Specifically, in a palmprint based biometric system, the sensor level spoof attack may involve presenting fake hand in the form of a hand image displayed on a portable display or image of the hand printed out on a piece of paper.

Researchers have attempted to address the problem of spoof attacks and proposed several anti spoofing techniques for fingerprint[2–5] , face[4,6,7] and iris[4] based biometric systems. Interestingly, there has been very little effort in the literature towards developing counter measures for hand based biometrics such as hand geometry

Biometric and Surveillance Technology for Human and Activity Identification XII, edited by Ioannis A. Kakadiaris, Ajay Kumar, Walter J. Scheirer, Proc. of SPIE Vol. 9457, 94570E
 · doi: 10.1117/12.2180333

and palmprint systems; despite the fact that the threat of spoof attacks are equally severe in these systems. The threat is clearly evident from the results reported in[8] , where authors have demonstrated how easily commercially available hand geometry based biometric systems can be circumvented. The work reported in[9] analyses on a small scale, vulnerability of 2D palmprint systems to spoof attacks. Experimental results presented in[9] show that 2D palmprint based biometric system can be circumvented by presenting photographs of the users' hand (fake biometric sample) to the acquisition device. Researchers have proposed approaches based on the analysis of multi spectral responses[10] or use of 3D (depth) features[11,12] to enhance the inherent robustness of palmprint systems to sensor level attacks. However, such approaches do not explicitly perform spoof detection. Moreover, the major drawback of these techniques is the requirement of additional sensor and increased complexity in data acquisition and processing. Anti-spoofing techniques based on local binary patterns (LBP), which capture local textural differences between real and spoof samples (e.g. arising from printing artefacts), have been shown to be quite effective for spoof detection in face and iris based biometric systems. Authors in[13] investigated the effectiveness of LBP based features for spoof detection in palmprint matching systems. However, their experiments were conducted on a subset of a publicly available palmprint dataset. Moreover, they addressed the problem of spoof detection using only print based spoof samples.

The key objective of this work is to develop an efficient spoof detection technique for palmprint systems based on the estimation of surface reflectance. We also perform assessment of vulnerability of palmprint systems to sensor level attacks, which employ displayed and printed spoofs of hand images to circumvent the system. The rest of the paper is organized as follows. Section 2 gives the detailed description of our anti-spoofing approach. Section 3 presents the experimental results and finally, section 4 concludes the paper.

2. PROPOSED APPROACH

The block diagram of the proposed spoof detection approach is shown in figure 1. Major computational stages of our approach include extraction of region of interest (yielding a palmprint sub-image) for the hand image, followed by sub-band decomposition using discrete wavelet transform (DWT). Discriminating information extracted from the distributions of sub-band coefficients and the pixel intensities of the palmprint sub-image is used to train a binary classifier, which determines whether the hand presented to the system is real or a fake one. Detailed descriptions of these stages of processing are provided in the following sections.

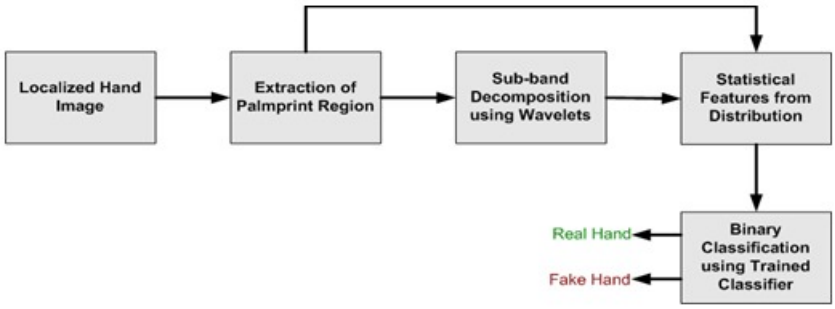


Figure 1. Overview of the proposed spoof detection approach

2.1 Region of Interest Extraction

Pre-processing stage of the proposed approach performs the task of localization and subsequent extraction of the region of interest, i.e. palmprint, from the acquired hand image. For this purpose, we adopt the method presented in[11] , which is based on the localization of local minima that correspond to finger valleys on the hand contour. Coordinates of the finger valleys thus obtained are used as reference for extraction of the palmprint region. Palmprint sub-images are then normalized to images of size 150 x 150 pixels. Figure 2 shows sample images of real and fake palmprints for two users in IITD Touchless Palmprint Database.[14] The first column shows the real images. The second and third columns show display and printed spoofs respectively. As can be observed in this figure, palmprints captured from printed photographs and display generated spoofs look very

similar to palmprints captured from users' hands or the real samples. Although it is expected that fake palmprint images would contain printing artefacts, reflections and other kinds of noises arising from printing (or display) and the subsequent imaging process, we have observed that it is extremely difficult to discriminate between real and fake palmprint images with naked eyes.

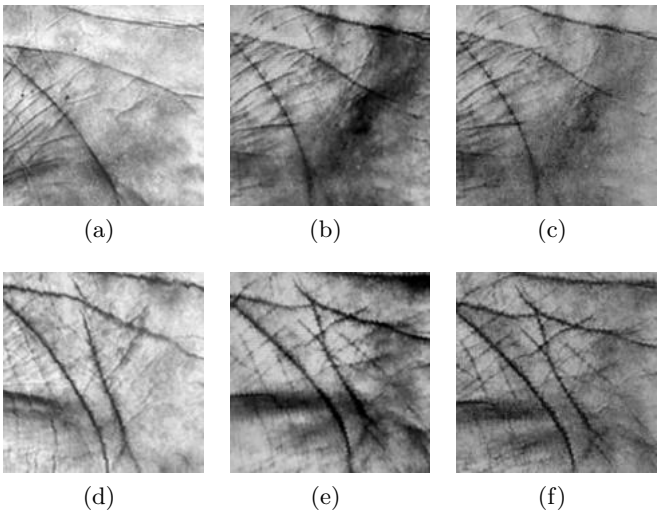


Figure 2. Palmprint images acquired by the camera from the real human hands (a),(d); from images displayed on display (b),(e); and from printed photographs (c),(f) for two users in IITD dataset

2.2 Feature Extraction

Our approach to palmprint spoof detection is based on the idea that estimation of surface reflectance can greatly help in discriminating between materials with different surface properties. However, the problem of accurately estimating the surface reflectance by analysis of a single acquired image is a non trivial task. The authors in[15] developed a machine learning approach for determining relationships between surface reflectance and image features. Their approach is based on a set of first and higher order statistical features computed from the distributions of pixel intensities and sub-band wavelet coefficients. It may be noted that their approach does not explicitly estimate the surface reflectance. Instead, through extensive experimentation, it is established that there exists a relationship between surface reflectance and statistical features extracted from the image. Inspired by the work in[15] , we explored the statistical features and came up with a feature set consisting of following features that characterize the distributions: *mean, variance, skewness, kurtosis,* 10^{th}*,* 50^{th} *and* 90^{th} *percentile of the image pixel intensities, variance of wavelet coefficients in the first and second level vertically oriented sub-bands and their ratio, and the kurtosis of the second level vertically oriented sub-band.* Therefore, we have an 11 dimensional feature vector, F that effectively captures differences in the distributions of pixel intensities and their sub-band coefficients for discrimination of real and spoof image samples. F can be represented as $F = [F_1, F_2, F_3, F_4, F_5, F_6, F_7, F_8, F_9, F_{10}, F_{11}]$. Let the extracted palmprint image of size $M \times N$ be denoted by I. Then the features can be described as follows:[16]

F_1 denotes the mean or average value of the pixel intensities of the palmprint image.

$$F_1 = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} I(i,j)}{M \times N} \tag{1}$$

F_2 denotes the variance of pixel intensities of the palmprint image.

$$F_2 = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} (I(i,j) - F_1)^2}{M \times N} \tag{2}$$

F_3, F_4 and F_5 represent the 10^{th}, 50^{th} and 90^{th} percentiles of distribution of pixel intensities, respectively. The p^{th} percentile of a distribution is a number such that approximately $p\%$ of the values in the distribution are equal to or less than that number. $F6$ denotes the skewness of the intensities in the palmprint image and it is defined as the ratio of the third central moment and the third power of its standard deviation. It measures the asymmetry of the distribution. A positive value indicates a distribution skewed to the right while a negative value indicates a negatively skewed distribution.

$$F_6 = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(I(i,j) - F_1)^3}{(M \times N).(F_2)^{\frac{3}{2}}} \tag{3}$$

F_7 denotes the kurtosis of the distribution of the intensity values in the palmprint image which is defined as the ratio of the fourth central moment and the fourth power of its standard deviation. It measures the peakedness of a distribution. A value greater than 3 indicates a more peaked distribution compared to the normal distribution while a value less than 3 corresponds to a curve that is flatter than the normal distribution.

$$F_7 = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(I(i,j) - F_1)^4}{(M \times N).(F_2)^2} \tag{4}$$

Let C_1 and C_2 denote the vectors representing the coefficients of the vertical sub-bands at the first and second levels of decomposition respectively and let μ_1 and μ_2 represent the mean of C_1 and C_2 respectively. Variances of the filter outputs at the two scales are an approximate measure of the spectral power in different frequency bands.[15] F_8 and F_9 represent the variances of the vertical sub-bands at first and second levels of the wavelet decomposition respectively.

$$F_8 = \frac{\sum_{i=1}^{|C_1|}(C_1(i) - \mu_1)^2}{|C_1|} \tag{5}$$

$$F_9 = \frac{\sum_{i=1}^{|C_2|}(C_2(i) - \mu_2)^2}{|C_2|} \tag{6}$$

F_{10} denotes the ratio of the two variances of the vertical subbands at first and second levels of the wavelet decomposition namely F_8 and F_9.

$$F_{10} = \frac{F_8}{F_9} \tag{7}$$

F_{11} denotes the kurtosis of the second finest vertical sub-band of the wavelet decomposition.

$$F_{11} = \frac{\sum_{i=1}^{|C_2|}(C_2(i) - \mu_2)^4}{|C_2|.(F_9)^2} \tag{8}$$

2.3 Classification

The set of features described in the previous section are used to train a classifier, which (during the testing phase) determines whether the input hand image belongs to a real hand or a fake one. In this work, we employ support vector machine (SVM) for classification. Specifically, we use linear soft margin formulation of SVM, which finds an optimal linear separating hyper-plane while performing a trade-off between training error and the model complexity. Details of this technique can be found in.[17] In this work, the implementation of SVM in MATLAB is used for classification.

3. EXPERIMENTS

In this section we provide detailed description of plamprint database and generation of the spoof palmprint images. Later in the section, we present the results of two sets of experiments to ascertain the effectiveness of the proposed feature set for spoof detection.

3.1 Database and Spoof Generation

IITD dataset contains two sets of images, acquired from left and right hands of 230 users. We use 1300 right hand images of 230 users in this dataset. These images were acquired in an unconstrained and contact-free manner under controlled background and lighting conditions. Due to non existence of a benchmark dataset for spoof hand images, we generated the spoof samples corresponding to the real images in the dataset. Table 1 presents detailed specifications of devices employed in this work. The following section provides the details of spoof generation.

3.1.1 Display Spoof Generation

For generating display based spoof images, an automated system consisting of a laptop with 4GB RAM, i3 processor @2.40 GHz and a Microsoft LifeCam studio webcam was developed. The webcam is connected via a USB port to the laptop which runs a MATLAB program to display the hand images sequentially on the display screen, while the web camera synchronized with the laptop acquired images of the displayed palmprints.

3.1.2 Print Spoof Generation

For generating print based spoof images, we use palmprint images of 230 users from IITD database. Fake hand samples (in this case, photographs) are generated by printing these images on matte A4 size sheets of paper using a Canon ImageRunner 3225 laser printer with a printing resolution of 1200 dpi x 1200 dpi. Microsoft LifeCam studio webcam, with a resolution of 1280 x 720 pixels, was used to capture images of the printed palmprints.

Table 1. Specifications of the devices considered in the experiments for creating spoof samples

Device / Manufacturer	Specifications	
Printer		
Canon ImageRunner 3225 laser printer	Printing Resolution	1200 dpi x 1200 dpi
Display		
Toshiba	Screen Type	LED Screen (Glossy)
	Resolution	1920 x 1080 pixels
	Refresh Rate	60 Hz
Camera		
Microsoft Lifecam Studio	Resolution	1280 x 720 pixels

3.2 Vulnerability Assessment

In the first set of experiments, the objective is to assess the vulnerability of palmprint matcher when fake palmprint images are presented for matching. For this purpose, we adopt the palmprint matching algorithm,[18] which uses Gabor filters oriented at six different directions to extract the dominant direction of palm lines. The orientation information is then binary coded and stored as a feature. A Hamming distance based measure is used for comparing a pair of binary features. We perform two verification experiments in the following two scenarios.[19]

3.2.1 Licit Scenario

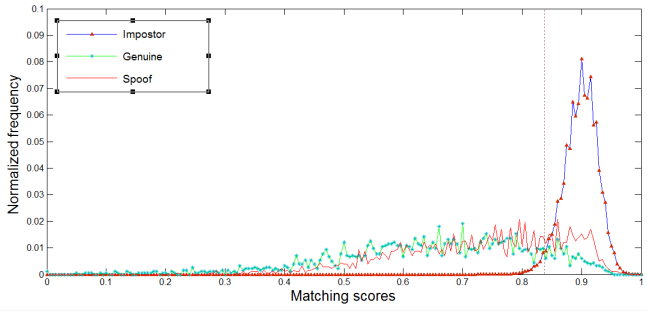
In this experiment we only consider real palmprint images. The dataset is divided into independent training and testing sets. For each user in the database, the first three images are used for enrolment (training), while authentication (testing) is performed using the rest. Using this method a set of genuine and impostor matching scores are generated. Two error rates involved in this scenario are false acceptance rate (FAR) and false rejection rate (FRR). The decision threshold (t) is determined as the operating point where FRR equals FAR. This error, termed as equal error rate (EER) is 9.5572 in our case.

3.2.2 Spoof Scenario

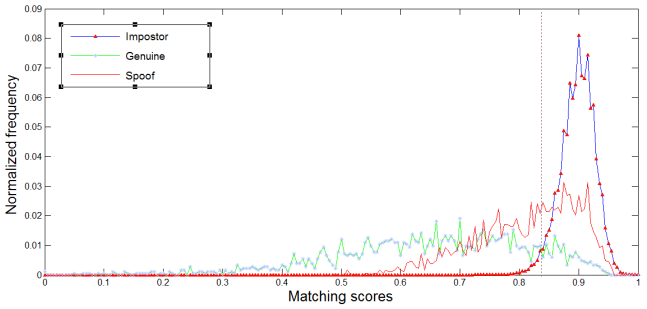
In this experiment, our objective is to compute the vulnerability of the palmprint matcher. For this purpose, we calculate spoofing false acceptance rate (SFAR)[20] which is defined as the percentage of spoof attacks that are successful in circumventing the system. The decision threshold (t), computed in the licit scenario is used as a threshold to accept or reject the spoof test samples. Since it is a verification scenario, the palmprint matching is performed between users' spoof and corresponding real samples to calculate the spoof attack scores. The real samples are the ones used for training in the licit scenario while the spoof samples are the spoof counterparts of the test samples used in the licit scenario. SFAR obtained for display and print based spoof attacks are reported in table 2.

Table 2. Vulnerability assessment of the palmprint matcher in the spoof scenario

Spoof Type	**SFAR (%)**
Display based spoof	79.80
Print based spoof	60.51



(a)



(b)

Figure 3. Genuine, impostor and spoof distributions a) for the display based spoof attack b) for the print based spoof attack

High SFAR suggests that the palmprint verification systems are highly vulnerable to both the kinds of spoof attacks. It may be noted that display based spoof attack is more effective (as it leads to higher SFAR) than the print based one. This may be due to the fact that the process of generation of display based spoof images does not involve printing and as a result, the distortions that are usually caused by printing will not be present in these images. It may be noted that parameters of the palmprint matcher (e.g. parameters of Gabor filter) have not been optimized in our implementation and therefore the matching performance may possibly be improved. The value of SFAR depends on the decision threshold and in turn on EER. Therefore, it can be argued that a better palmprint matcher with lower EER will result in increased number of successful spoof attacks leading to higher SFAR.

Figure 3 shows distribution of genuine, impostor and spoof matching scores. It is clearly evident from the

figure, that the distribution of dissimilarity scores for the spoof samples overlap with both genuine and impostor distributions. Specifically, there is significant overlap between genuine and spoof distributions. It may also be noted that the spoof distribution to the left of the decision threshold contributes to the spoof attacks that successfully spoof the system; while the spoof distribution to the right of the decision threshold corresponds to the failed attempts.

3.3 Anti-spoofing

In the second set of experiments, we evaluate the performance of the proposed spoof detection approach for display and print based spoof images. Three experiments are performed. Firstly, we consider anti-spoofing for display based attacks. Secondly, we investigate anti-spoofing for print based attacks; and finally, we assess the performance in the presence of both kinds of spoof attacks. To quantify the errors in the anti-spoofing framework, two error rates, namely, false living rate (FLR) and false fake rate (FFR) are utilized.[21] FLR denotes the fraction of spoof samples falsely accepted as living or real while FFR denotes the fraction of real (live) samples mistaken as spoof. Based on these two rates we computed the accuracy of the system. To this end, we perform 10-fold cross validation for each of the three experiments and report the average accuracy and area under the ROC curve (AUC). In our case we plot ROC between FLR and 1-FFR. The accuracy is computed as the number of test samples that are correctly classified out of the total number of test samples. Let N_f be the number of fake test samples and N_r be the number of real test samples. Then the Accuracy is computed as follows:

$$Accuracy = \max_t (1 - \frac{FFR(t) \times N_f + FLR(t) \times N_r}{N_f + N_r}) \tag{9}$$

Finally, in order to perform a comparative evaluation, we present experimental results for LBP based anti-spoofing technique.[13] For this purpose, we implemented the approach presented in[13] and evaluated its performance on our database of palmprint images. Table 3 presents the anti-spoofing performances for display and print based attacks using the proposed as well as the LBP based approach. As can be seen, our approach consistently outperforms LBP based approach. Another key advantage of the proposed approach is shorter feature length as compared to the LBP based approach, resulting in higher computational efficiency.

Table 3. Performance of the proposed and LBP based approach for display, print and combined (display + print) spoof attacks

Spoof Type	**Proposed Approach**		**LBP based approach[13]**	
	Accuracy (%)	**AUC**	**Accuracy (%)**	**AUC**
Display	99.68	0.0013	91.82	0.0339
Print	99.60	0.0014	89.07	0.0593
Display+Print	99.62	0.0014	89.93	0.0510

4. CONCLUSION

This paper presents an anti-spoofing approach for palmprint based biometric systems. We consider two different types of sensor level attacks, namely, print and display based attacks. The proposed approach is based on the analysis of acquired hand images for estimating surface reflectance. First and higher order statistical features computed from the distributions of pixel intensities and sub-band wavelet coefficients form the feature set. A trained binary classifier makes use of these features to determine whether the hand presented to the sensor is real or fake. Experiments on a database of 1300 hand images from 230 subjects yield promising results, which demonstrate that the proposed technique is effective in discriminating high quality palmprint spoof images. As part of future work, we plan to generate fake hand images using another publicly available database - CASIA palmprint database, in order to further validate the proposed approach. In addition, we plan to investigate whether the proposed approach works effectively in detecting spoofs created using other kinds of printers and cameras.

REFERENCES

1. Ratha, N. K., Connell, J. H. and Bolle, R. M. "An analysis of minutiae matching strength," Proc. Springer Audio-and Video-Based Biometric Person Authentication, 223-228, (2001).
2. Reddy, P. V., Kumar, A., Rahman, S. M. K. and Mundra, T. S., "A new method for fingerprint antispoofing using pulse oximetry," Proc. IEEE Int. Conf. Biometrics, Theory and Applications, Washington D. C., 36-41, (2007).
3. Setlak, D. R., Fingerprint sensor having spoof reduction features and related methods, US Patent No. 5, 953, 441, (1999).
4. Nixon, K. A., Aimale, V. and Rowe, R. K. [Spoof Detection Schemes, Handbook of Biometric], Springer US, 403-423, (2008).
5. Derakhshani, S. T. V., Hornak, R., Parthasaradhi, L. A. and Schuckers, S. A. C., "Time-series detection of perspiration as a liveness test in fingerprint devices," IEEE Trans. Systems, Man, and Cybernetics 35(3), 335-343, (2005).
6. Zhang, Z., Yi, D., Lei, Z. and Li, S. Z., "Face liveness detection by learning multispectral reflectance distributions," Proc. Int Conf. on Face and Gesture 436-441, (2011).
7. Maatta, J., Hadid, A. and Pietikinen, M., "Face spoofing detection from single images using micro-texture analysis," Proc. International Joint Conference on Biometrics (IJCB), Washington, D.C., USA, (2011).
8. Chen, H., Valizadegan, H., Jackson, C., Soltysiak, S. and Jain, A. K., "Fake hands: Spoofing hand geometry systems," Proc. Biometric Consortium, Washington, D.C., (2005).
9. Zhang, D., Kanhangad, V., Luo, N. and Kumar, A., "Robust palmprint verification using 2D and 3D features," Pattern Recognition 43(1), 358-368, (2010).
10. Nixon, K. A. and Rowe, R. K., "Multispectral fingerprint imaging for spoof detection," Proc. SPIE 5779 Biometric Technology for Human Identification, 214-225, (2005).
11. Kanhangad, V., Kumar, A. and Zhang, D., "A unified framework for hand verification using 2D and 3D features," IEEE Trans. Information Forensics Security 6(3), 10141-1027, (2011).
12. Li, W., Zhang, D., Lu, G. and Yan, J., "Efficient joint 2D and 3D palmprint matching with alignment refinement," Proc. IEEE Conf. on Computer Vision and Pattern Recognition (CVPR), 795-801, (2010).
13. Kanhangad, V. and Kumar, A., "Securing palmprint authentication systems using spoof detection approach," Proc. SPIE 9067 Int. Conf. on Machine Vision, 90671M, (2013).
14. Kumar, A., "Incorporating cohort information for reliable palmprint authentication," Proc. IEEE Indian Conf. Computer Vision, Graphics and Image Processing, 583-590, (2008).
15. Dror, R. O., Adelson, E. H. and Willsky, A. S., "Estimating surface reflectance properties from images under unknown illumination," Proc. SPIE 4299 Human Vision and Electronic Imaging IV, 231-242, (2001).
16. Walck, C., [Handbook on Statistical Distributions for Experimentalists], University of Stockholm Internal Report SUF-PFY/96-01, (2007).
17. Kecman, V., [Learning and Soft Computing: Support Vector Machines, Neural Networks, and Fuzzy Logic Models], MIT Press, (2001).
18. Kong, A. W. K. and Zhang, D., "Competitive coding scheme for palmprint verification," Proc. Int. Conf. Pattern Recognition, Washington, D.C., 1051-4651, (2004).
19. Chingovska, I., Anjos, A. and Marcel, S., "Anti-spoofing in action: joint operation with a verification system," Proc. IEEE Conf. Computer Vision and Pattern Recognition Workshops (CVPRW), 98-104, (2013).
20. Johnson, P., Tan, B. and Schuckers, S., "Multimodal fusion vulnerability to non-zero effort (spoof) imposters," IEEE Int. Workshop on Information Forensics and Security (WIFS), 1-5, (2010).
21. Erdogmus, N. and Marcel, S., "Spoofing face recognition with 3D masks," IEEE Trans. Information Forensics Security 9(7), 1084-1097, (2014).