JOURNAL OF ADVANCED APPLIED SCIENTIFIC RESEARCH-ISSN(O): 2454-3225
Snehal Datwase et al, JOAASR-Vol-6-3-May-2024:70-84

Palmprint spoofing detection by using deep learning technique on Multispectral database

Snehal Datwase[1], R R Deshmukh[1] †*

[1] *Dr Babasaheb Ambedkar*, *Marathwada University*, *Aurangabad*

Abstract

The protection of Biometric systems against attacks is crucial as biometric devices proliferate in the field of personal authentication. The presentation assault is the most prevalent type of attack on biometric systems; it entails presenting a fake copy (artefact) of the true biometric to the sensor in order to gain unauthorised access. The vulnerability in palmprint-based biometric systems has not received much attention despite the substantial threat posed by these assaults. In this research, we show how to detect a spoof palmprint image. Spoofing attacks involving faked images pose a significant threat to biometric systems. For the suggested method, we use the CASIA palmprint database, from which we constructed our own spoof database using printed photos. After that, we did some pre-processing to obtain the ROI image and a noise-free image for feature extraction using the SIFT approach. We use the convolution neural network for classification and the SVM for comparison. We obtained a result of 96.2% for our proposed palmprint system identification and 89% for SVM. But our main goal is to train the model for spoof detection, so we take some normal images and some spoof images for our train model and use the confusion matrix to calculate the accuracy of our model. We obtain an overall accuracy of 86% for our spoof detection by computing the confusion matrix.

1 Introduction

Biometric palmprint recognition has received a lot of attention over the past years from various studies. Modern human civilization is expanding quickly, which has increased the need for innovative and effective technology to support it. The use of highly trustworthy and widely available individual authentication and identity mechanisms became essential as security and privacy concerns also surfaced. In order to meet this demand, the science of biometrics has

*Corresponding author.
†E-mail: rrdeshmukh.csit@bamu.ac.in

developed. It now focuses on the physiological and behavioural traits of the human body in order to identify an individual's identity. The focus of biometric technology is on methods that automatically verify both fixed human qualities, like DNA, fingerprints , faces , iris scans, and palmprint, as well as human behavioural traits, including gait, voice, keystrokes, and signatures. Palmprint recognition has emerged as one of the key biometric technologies among them, garnering a lot of attention.

The evaluation of the resilience of biometric systems and the growing interest in security have emerged as important research areas in recent years. In the past, spoofing attacks were not an issue because biometric systems were solely intended to recognise IDs. A handful of the ways that biometric systems can be exploited include interfering with sensors, altering databases, assaulting the channel between databases and matching, and many more techniques (1).

The increased interest in investigating the so-called direct or spoofing assaults, particularly print and replay attacks among the various types of treats explored, has led to attempts in this crucial field of research. The print attack uses printed multimodal images of an identity to trick 2D recognition systems, whereas the replay assault uses replaying a live identity's video sequence on a fixed or portable screen to avoid liveness detection.

The biometric community has been forced to look into the weaknesses in modalities like the fingerprint, face, and even gait against such fraudulent acts. A significant difficulty in the field of biometrics is the spoofing of attack detection.

Techniques are typically separated into texture, motion, and liveness evaluations to prevent spoofing in recognition systems (2). In order to identify attacks, texture analysis tools primarily look for texture patterns like print errors and general image blur. Motion features utilised to overcome a reliance on specific texture patterns, such as optical flow, are referred to as motion analysis (3; 4) However, motion-based algorithms have limitations when there is minimal motion information in a video because of stagnant subject motions and low-resolution cameras. In contrast, liveness cues analyse spontaneous movements that are impossible to capture in an image in order to determine the vitality signals of a biometric feature. These indicators for 2D face identification include eye blinking, lip movement, and variations in facial expression. As a result, one solution may not necessarily be applicable to different attack types. Digital photographs are also susceptible to aberrations during capture, capturing, processing, transmission, and reproduction, which could cause a noticeable decline in image quality. For instance, pictures of faces taken with an electronic device are probably going to be over- or underexposed, while pictures of palmprints taken using a printed piece of paper are probably going to have more local acquisition artefacts like spots and patches. A large amount of research has recently been

put into creating quality assessment techniques that benefit from the known properties of the human visual system. Therefore, it is also necessary to identify the quality variations between authentic and false samples utilising a variety of image quality methodologies (IQM).

In this work we have focused on the printed photograph of palmprint images for spoofing detection in that we have Separate palmprint recognition systems, which are simple to replicate and have success potential.

2 Background

Because various sensors are used in the two circumstances of image acquisition, it is generally believed that false samples are different from true images and that an image sample's quality should differ from another sample taken with a different sensor. Intensity, brightness, colours, blurriness, and other changes may contribute to the quality difference. The concept of (5) justifies the 'quality discrepancy' between the real and faked samples. Describes a spoofing detection approach based on dorsal hansd vein pictures. It is expected that multimodal systems are inherently resistant to faked artefacts (6). The anti-spoofing strategy has also been proven for multibiometrics and fusion tactics (7; 8). Sajjad et al. (9) demonstrated a multimodal biometric system based on handcrafted fingerprint, palmprint, and facial modalities. High-level characteristics based on deep convolutional neural networks (CNN) can also be utilized to detect faking. The Google Net serves as the backbone for computing deep spoofing detection characteristics. The use of an electronic screen display in a spoofing attack is shown in another example (10). In recent years, researchers have worked to develop several anti-spoofing techniques for fingerprints in an effort to address the problem of presentation attack detection (11; 12). There are also biometric technologies based on voice, iris, and face (13; 14). Face biometrics are receiving increased attention from researchers, and (15) provides a detailed analysis of face biometric antispoofing techniques. The two main categories of anti-spoofing techniques are software-based and hardware-based techniques. To assess if a feature is alive (17), hardware-based or sensor-level techniques (16) use additional specialized equipment or sensors. Additionally, a variety of methods have been proposed to strengthen the built-in defences of biometric systems against sensor-level attacks, based on the multispectral response analysis or the use of 3D (depth) features (18; 19; 20; 21; 22). Although these techniques increase biometric security, their main drawback is the difficulty in collecting and processing the necessary data. The challenge-response-based spoof detection techniques (23; 24) fall under this group and look at how a person reacts to challenges or other external stimuli. These methods are not very

user-friendly because they typically demand a lot of human cooperation. Software-based or feature-level approaches, however, provide reasonably priced, user-friendly, and unobtrusive alternatives (25). Solutions In essence, these methods process the biometric sample to provide traits that aid in differentiating between real and fraudulent biometric data. The bulk of software-based face and iris biometrics methods that have been studied in the literature are based on an analysis of textural differences in real biometric data and artefacts. For instance, it has been shown that anti-spoofing techniques based on local descriptors, such as LBP, are effective for spoof detection in, respectively, iris- and face-based biometric systems. LBP-based histogram characteristics are also investigated for spoof detection in palmprint matching systems. However, the study was limited to a small number of fake samples, and the experimental evaluation made use of a small section of a palmprint dataset that was made available to the public. It is clear that little has been done to develop palmprint biometric systems' spoof detection methods in software.

3 Methodology

As depicted in Figure 1, this is the suggested methodology for our research. As per the procedure, we obtained a multispectral palmprint database from CASIA University. Once we obtained the database, we used the database's region of interest (ROI), where we had identified the hand valley, and selected the important locations to scale the image and create the optimal region of interest.

After that, we pre-processed the entire database by applying several filters to it in order to reduce the noise and obtain the clear palmprint feature needed to detect spoofing. After smoothing, lighting, and thresholding, we applied the feature extraction method to it in order to determine whether the valley points or not. From there, we took its derivative, applied the low pass filter, and obtained the local valley. We then applied the CHVD algorithm to obtain the three significant valleys, and obtained the histogram of the ROI image, from which we could obtain the distinct features of the palmprint during thresholding.

For the additional classification work, we divided the database in half, using 70% for training the model and 30% for testing it. Using convolution neural networks and deep learning techniques, we applied various layers to the model's training and provided x and y labels in order to calculate the training loss. We apply several layers and epochs to the CNN during the classification process, and we detect validation loss throughout. PCA and SVM are also used to compare the results. Utilizing the CMC curve, we measure identification.

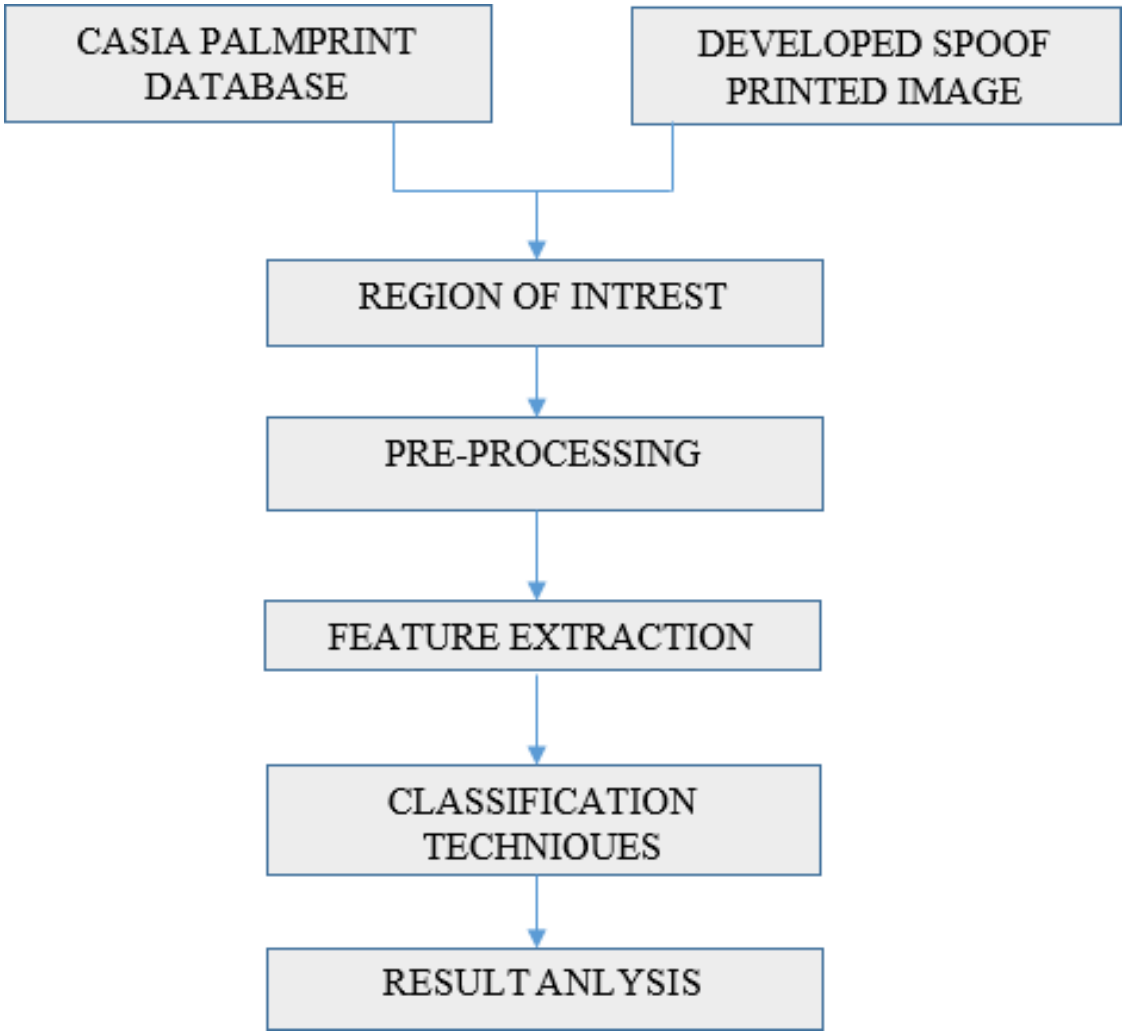

FIGURE 1

Proposed Methodology

After receiving the identification result, our primary goal in the process is to identify spoofs. To do this, we use the confusion matrix to calculate the accuracy of our model. Whereas, to determine the F1 score, we must compute the precision and recall for that confusion matrix.

4 Experimental Result

In the conclusion section, aside from wrapping up the research by reiterating the goal of the study and confirm the major results or outcomes and concrete recommendations be offered, there are some limitations of the current study. When similar works already reported; what new information the present work offers should be highlighted throughout the article in tune with the sections; in case of abstract it is novelty; in case of introduction, it is justification of present work; in case of results and discussion, it is the comparison how your data with previous

work and relate in tune with objectives; in the case of conclusion, it is take-home piece of new information to the readers; The authors should discuss these limitations from which research directions for future studies may be offered.

Using the multispectral palmprint database, we offer our experimental investigation of the suggested deep learning strategy in this section. Where we discovered the palmprint recognition and spoof detection. Additionally, we looked at how image quality affected anti-spoofing accuracy. We calculate error rate when we calculate the equal error rate in that biometric spoofing detection system (EER). We are determining whether or not the image is a fake using that EER.

4.1 Database

We are using the multispectral palmprint database from the CASIA University (28) in this part, which has a total of 7200 images. All of the photographs are 8-bit JPEG files with greyscale. This database was compiled during the course of two sessions, separated by a month. Each person provides six samples, and then all six photos are captured under six distinct lighting conditions. The CCD camera, which is mounted on the device's bottom, is used to capture this database.

After receiving the database from CASIA, we pre-process it, resize the original image, and obtain the ROI of the image as shown in Fig. 2 We have also taken the cropped image's threshold. Next, we obtain the coordinates, rotate the image, and select the precise palm region as shown in Fig. 3. In the end, we obtain the precise ROI image of the palm as displayed in Fig 4.

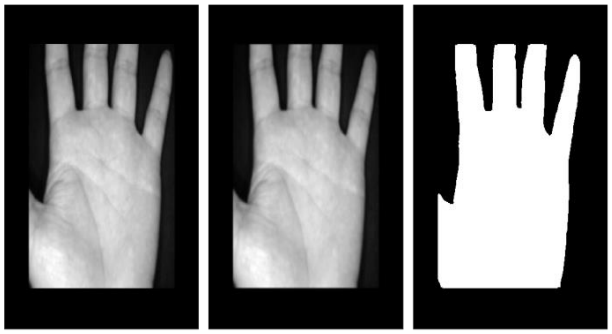

FIGURE 2

The palm's resized and threshold image.

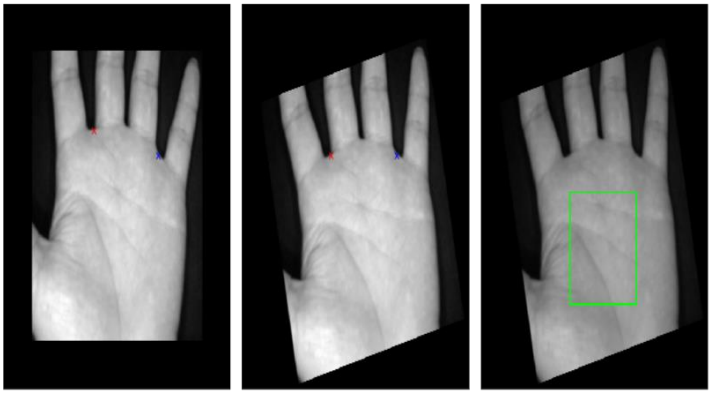

FIGURE 3

The palm's location and exact ROI region

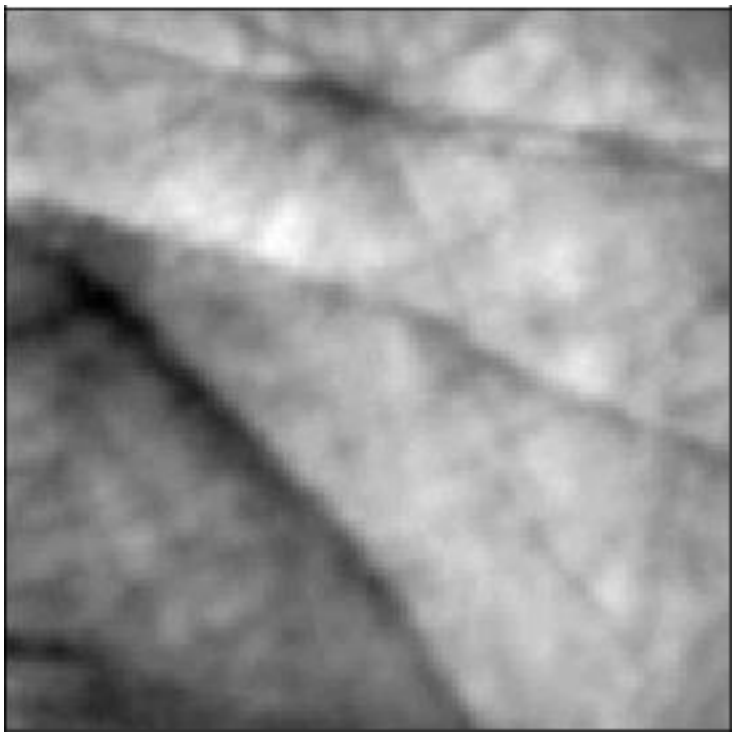

FIGURE 4

Extracted ROI image

4.2 Palmprint spoof database – printed palmprint images

Due to the lack of a spoof database, we developed our own in this section using information from the CASIA university database. We printed 500 copies of the palmprint database's paper In that 250 left and 250 right palm images are used. Printed images, which we then scanned using an HP Scanjet 200 to establish the spoof database on our own. In order to remove the noise from the palmprint spoof database, we applied various filters. We used Gaussian and medium filters in this process, as well as thresholding, to get the ROI of the ideal palmprint.

5 Feature Extraction

From a collection of reference photos, SIFT key points for objects are first collected and saved in a database. Each feature from the new image is individually compared to this database in order to identify an object in the image. Candidate matching features are then found based on Euclidean distance between their feature vectors. To exclude the best matches from the entire set of matches, subsets of critical points that concur on the item and its position, scale, and orientation in the new image are found. A quick implementation of the generalized Hough transform in a hash table allows for the quick detection of consistent clusters. Following more thorough model testing, outliers are eliminated for each cluster of three or more features that agrees on an item and its pose. Finally, given the accuracy of fit and number of likely false matches, the likelihood that a certain set of features indicates the presence of an object is determined. High confidence can be placed in identifying object matches as correct when they pass each of these conditions.

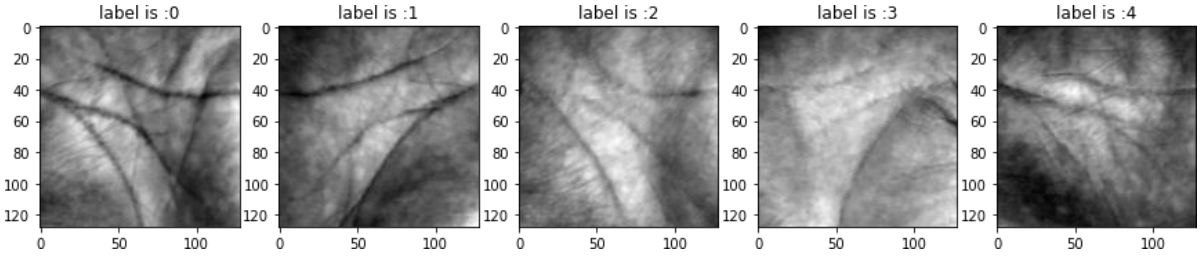

FIGURE 5

Feature extraction by using SIFT

6 Result and Discussion

After obtaining the ideal region of interest and removing the background and image noise, we tested our database using the palmprint database. We employed a convolution neural network for categorization for this portion of the palmprint. Whereas in that CNN classification, the model is trained using a database that has been split into two sections: 70% for training and 30% for testing. In order to train the CNN model, we also used the fake database that we had built from the printed image of the palmprint. For each batch of 64 iterations, we used the Euclidian distance to determine the training loss.

The network should be able to learn the image embedding (translation, rotation) in a reliable manner. Even if the images are aligned, illumination adjustments shouldn't significantly affect the embedding produced by the network. Therefore, using CNN is a good choice.

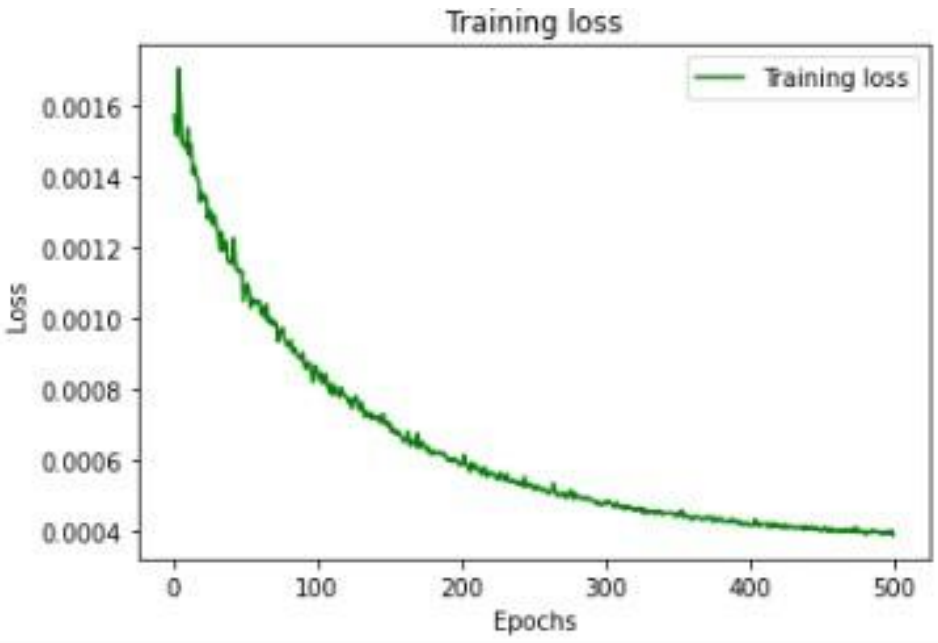

FIGURE 6

Training loss

The CNN will produce an embedding, which is a feature vector that represents the image. Triplet Loss is used to create well-defined embedding's between various classes.

Then, after splitting the database into train and validation sets, we used the CNN layers model, whose embedding size was 100, to train the model. This allowed us to calculate and improve the triplet loss. We experienced the triplet loss depicted in the fig. 6

The validation loss in that training model, as displayed in Fig 7. Has increased from 0.08140 to 0.07501. The losses are quite erratic in the early epochs. This, however, should not worry us because it just indicates that the initial learning rate is excessively high given the steep loss function terrain at the initialization weights. The fact that the validation samples are simpler to effectively distinguish from the training samples explains why the validation loss is lower than the training accuracy. Following all of that, let's test the model using various CNN empty layers and obtain weight from the training model to visualise the impact of embedding. To do this, we employ principal component analysis.

As seen in the fig.8 After 100 epochs, the class is not well separable, but we can still see some clusters. Let's not forget that we will use a non-linear classifier and show the data in two dimensions. Let's compare the performance of an SVM on the data acquired without using our triplet loss pipeline to the performance of an SVM on the embedding obtained with the triplet loss in order to truly determine whether having the embedding with triplet loss is beneficial.

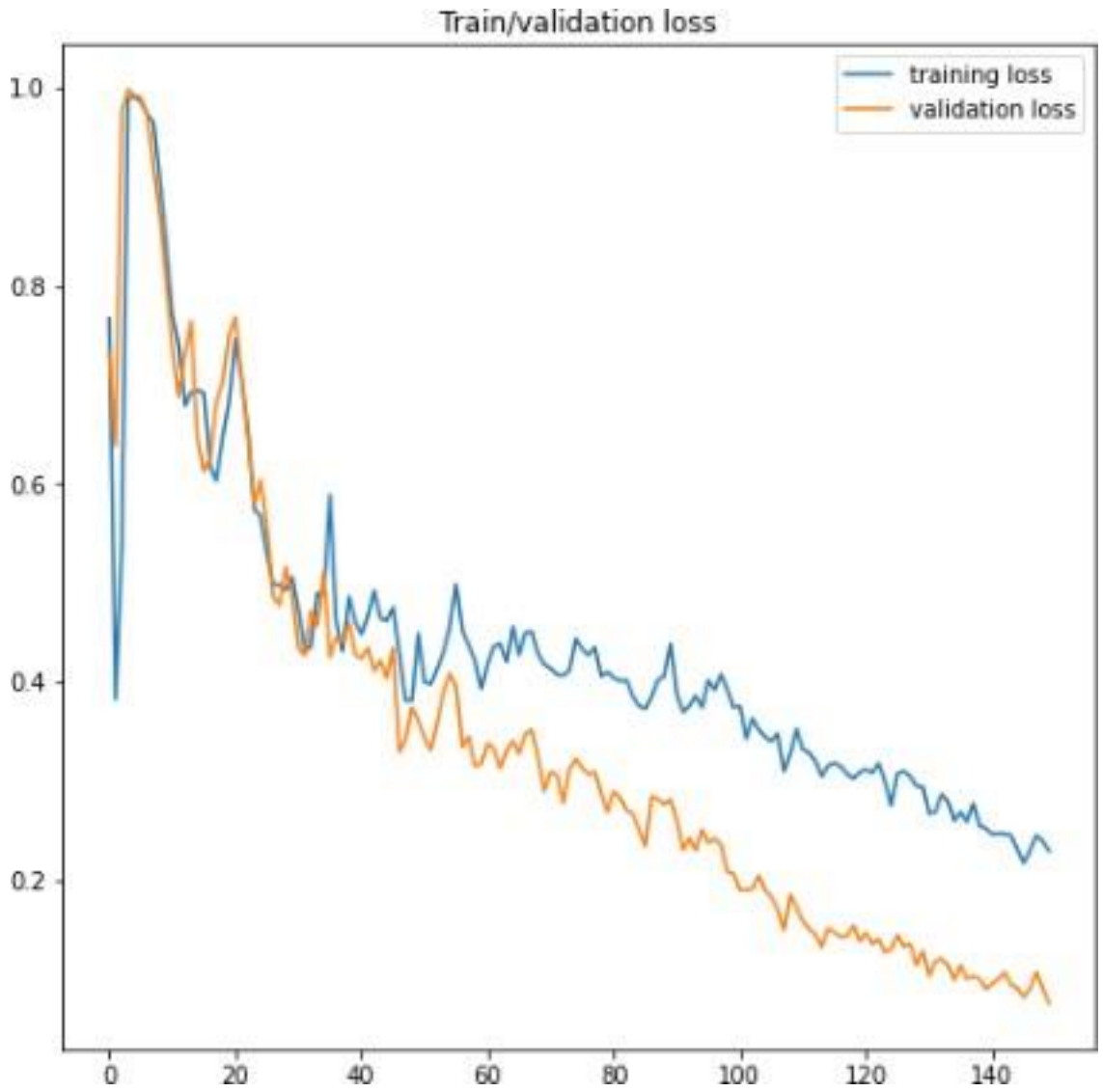

FIGURE 7

Training loss and validation

Let's test the SVM on the database after the entire process is complete. The result is 89.4%. And following embedding discovery, the accuracy percentage is 96.2%. Our pipeline obviously benefits, as is evident. But let's not forget that we are taking a biometrics course. The metric accuracy is not appropriate in an identifying scenario. Now, let's use several spoof ways to determine how well our pipeline is working. We have preserved the model predictions for all classes for each input label in the variable "pred." With a dataset of 100 classes, the spoof database has 500 test samples. The "pred" array is therefore shaped (500, 100). We will, for instance, have an array of probabilities for each of the 100 classes for the first input test sample.

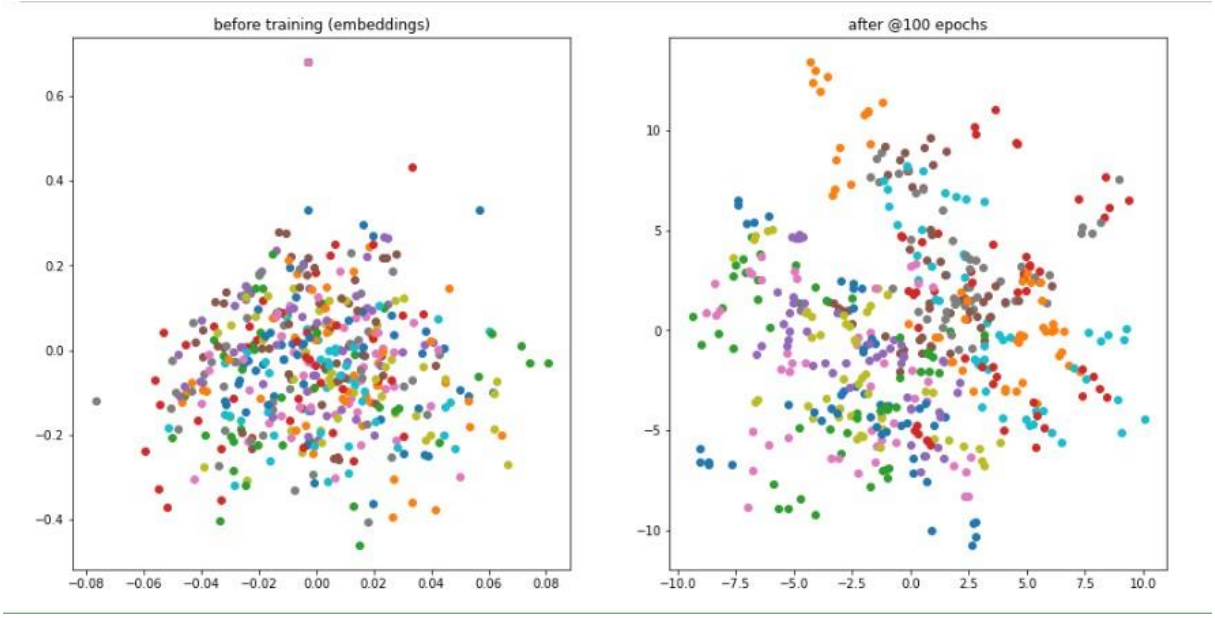

FIGURE 8

The effect of embedding using PCA.

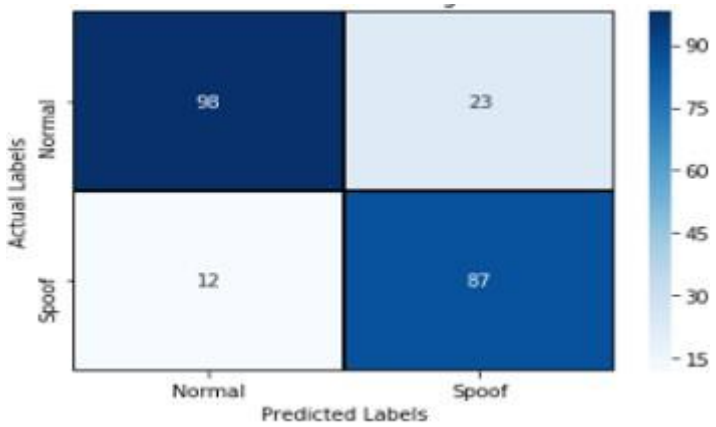

FIGURE 9

Confusion Matrix for our proposed model.

We use the confusion matrix throughout the entire computation procedure for our model's performance. As we calculate the precision and recall of the confusion matrix to generate the F1 score of the confusion matrix, we have taken into consideration the normal and spoof images detection to see if our model can detect the spoof image or not. The model's precision is 0.85 and recall is 0.89. The F1 Score we obtained is 0.86. This indicates that our model's spoof detection accuracy is 86%.

7 Conclusion

It has been shown that biometric verification systems are extremely susceptible to a variety of assaults that aim to defeat the system. Due to how simple they are to execute, presentation assaults provide the most security risk. Since palmprint authentication systems are not an exception, in this study we have created a palmprint-based biometric system anti-spoofing strategy. In that work, using the CASIA university database for our suggested approach, we generated our own printed Palmprint image database for the detection of the spoofing. We also performed some pre-processing on the database to remove the noise before using the SIFT feature extraction technique. Following that, we divided the database and trained the model for testing. To train the model, we employ deep learning methods like the convolution neural network. After that, we utilise a support vector machine to compare our model to others. In this case, the accuracy for identification is 96.2% for the CNN model and 89% for the SVM. Here, our suggested strategy for identification yields good results. The accuracy of our model is calculated using the confusion matrix, and as our major goal is to detect spoofing, we employ a combination of normal and spoof photos for this purpose. As a result, our model's accuracy is 86%.

Acknowledgment

This work is supported by Department of Science and Technology under the Funds for Infrastructure under Science and Technology (DST-FIST) with sanction no. SR/FST/ETI340/2013 to Department of Computer Science and Information Technology, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, Maharashtra, India. The authors would like to thank Department and University Authorities for providing the infrastructure and necessary support for carryout the research. The authors would like to thank Chhatrapati Shahu Maharaj Research Training & Human Development Institute (SARTHI) for the financial support in this work.

References

[1] N K Ratha, J H Connell, and R M Bolle. An analysis of minutiae matching strength. In *Audio-and Video-Based Biometric Person Authentication: Third International Conference*, *AVBPA 2001 Halmstad*, volume 3, pages 223–228. Springer, 2001.

[2] M M Chakka, A Anjos, S Marcel, R Tronci, D Muntoni, G Fadda, . . Pietikäinen, and M. Competition on counter measures to 2-d facial spoofing attacks. *2011 International Joint Conference on Biometrics (IJCB)*, pages 1–6, 2011.

[3] K Kollreider, H Fronthaler, and J Bigun. Evaluating liveness by face images and the structure tensor. *Fourth IEEE Workshop on Automatic Identification Advanced Technologies (AutoID'05)*, pages 75–80, 2005.

[4] K Kollreider, H Fronthaler, and J Bigun. Verifying liveness by multiple experts in face biometrics. *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, pages 1–6, 2008.

[5] J Galbally, S Marcel, and J Fierrez. Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. *IEEE transactions on image processing*, 23(2):710–724, 2013.

[6] I Patil, S Bhilare, and V Kanhangad. Assessing vulnerability of dorsal hand-vein verification system to spoofing attacks using smartphone camera. *2016 IEEE International Conference on Identity*, *Security and Behavior Analysis (ISBA)*, pages 1–6, 2016.

[7] C Shen, Y Chen, and G Yang. On motion-sensor behavior analysis for human-activity recognition via smartphones. *2016 Ieee International Conference on Identity*, *Security and Behavior Analysis (Isba)*, pages 1–6, 2016.

[8] B Biggio, G Fumera, G L Marcialis, and F Roli. Statistical meta-analysis of presentation attacks for secure multibiometric systems. *IEEE transactions on pattern analysis and machine intelligence*, 39(3):561–575, 2016.

[9] M Sajjad, S Khan, T Hussain, K Muhammad, A K Sangaiah, A Castiglione, . . Baik, and S W. CNN-based anti-spoofing two-tier multi-factor authentication system. *Pattern Recognition Letters*, 126:123–131, 2019.

[10] R Raghavendra and C Busch. Robust scheme for iris presentation attack detection using multiscale binarized statistical image features. *IEEE Transactions on Information Forensics and Security*, 10(4):703–715, 2015.

[11] P V Reddy, A Kumar, S M K Rahman, and T S Mundra. A new method for fingerprint anti-spoofing using pulse oxiometry. *First IEEE International Conference on Biometrics: Theory*, *Applications*, *and Systems*, pages 1–6, 2007.

[12] S T Parthasaradhi, R Derakhshani, L A Hornak, and S A Schuckers. Time-series detection of perspiration as a liveness test in fingerprint devices. *IEEE Transactions on Systems*, *Man*, *and Cybernetics*, *Part C (Applications and Reviews)*, 35(3):335–343, 2005.

[13] N Erdogmus and S Marcel. Spoofing face recognition with 3D masks. *IEEE transactions on information forensics and security*, 9(7):1084–1097, 2014.

[14] A Hadid. Face biometrics under spoofing attacks: Vulnerabilities, countermeasures, open issues, and research directions. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pages 113–118, 2014.

[15] H Zhang, Z Sun, T Tan, and J Wang. Learning hierarchical visual codebook for iris liveness detection. *International Joint Conference on Biometrics*, 1, 2011.

[16] R Raghavendra and C Busch, Presentation attack detection algorithm for face and iris biometrics, 2014.

[17] J Sanchez, I Saratxaga, I Hernaez, E Navas, D Erro, and T Raitio. Toward a universal synthetic speech spoofing detection using phase information. *IEEE Transactions on Information Forensics and Security*, 10(4):810–820, 2015.

[18] J Galbally, S Marcel, and J Fierrez. Biometric antispoofing methods: A survey in face recognition. *IEEE Access*, 2:1530–1552, 2014.

[19] P V Reddy, A Kumar, S M K Rahman, and T S Mundra. A new antispoofing approach for biometric devices. *IEEE transactions on biomedical circuits and systems*, 2(4):328–337, 2008.

[20] D Zhang, Z Guo, G Lu, L Zhang, and W Zuo. An online system of multispectral palmprint verification. *IEEE transactions on instrumentation and measurement*, 59(2):480–490, 2009.

[21] W Li, L Zhang, D Zhang, G Lu, and J Yan. Efficient joint 2D and 3D palmprint matching with alignment refinement. *2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, pages 795–801, 2010.

[22] N Kose and J L Dugelay. Countermeasure for the protection of face recognition systems against mask attacks. *10th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG)*, pages 1–6, 2013.

[23] G Pan, L Sun, Z Wu, and S Lao. Eyeblink-based anti-spoofing in face recognition from a generic webcamera. *IEEE 11th international conference on computer vision*, pages 1–8, 2007.

[24] M I Faraj and J Bigun. Audio-visual person authentication using lip-motion from orientation maps. *Pattern recognition letters*, 28(11):1368–1382, 2007.

[25] I Chingovska, A Anjos, and S Marcel. On the effectiveness of local binary patterns in face anti-spoofing. *2012 BIOSIG-proceedings of the international conference of biometrics special interest group (BIOSIG)*, pages 1–7, 2012.

[26] D Gragnaniello, C Sansone, and L Verdoliva. Iris liveness detection for mobile devices based on local descriptors. *Pattern Recognition Letters*, 57:81–87, 2015.

[27] V Kanhangad and A Kumar. Securing palmprint authentication systems using spoof detection approach. *Sixth International Conference on Machine Vision (ICMV 2013)*, 9067:321–325, 2013.

[28] http://biometrics.idealtest.org/