FINGERPRINT LIVENESS DETECTION BASED ON GUIDED FILTERING AND HYBRID IMAGE ANALYSIS

[1]Mrs S.Mounika, [2]D.Gaurav Kumar, [3]Kurella Bharat, [4]Ravula Kamalakar

[1]Assistant Professor, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

Mounikashetti1992@gmail.com

[2]BTech student, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,
gauravrockzz73@gmail.com

[3]BTech student, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,
bharathchan2@gmail.com

[4]BTech student, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,
saikamalakar07@gmail.com

Abstract: *Fingerprints are widely used for biometric recognition. However, many spoofing attacks based on an artificially made fingerprint occur. In this study, the authors propose an approach to detect fingerprint liveness which uses the guided filtering and hybrid image analysis. This study deals with the problem of ignoring the contribution that is brought by the sharp features when analysing the denoised image. The method described utilises both the enhanced sharp features and denoised features from the hybrid images to get better results. The input fingerprint is pre-processed by region of interest extraction and then is filtered by a guidance image for obtaining the denoised image. Then, histogram equalisation is introduced to eliminate the impact of illumination condition. The authors extract the co-occurrence of adjacent local binary pattern features from both the cropped images and the denoised images. Whilst concatenating both the features together to form a long feature, t-Distributed Stochastic Neighbour Embedding is applied to reduce the data dimension. The authors consider the fingerprint liveness detection as a two-class classification problem and use support vector machine with radial basis function kernel to solve this problem. The authors evaluate the experiments on three benchmark data sets. Experimental results demonstrate that the accuracy of the proposed method can outperform most of the state-of-art methods.*

Keywords: *Biometric recognition, Fingerprint liveness detection, t-Distributed Stochastic Neighbour Embedding.*

I. INTRODUCTION

Biometric methods mean recognizing a person based on a physiological or behavioural characteristic. Biometric data varies from each other. Therefore, the biometric system has been extensively used for personal identification and authentication. Moreover, the biometric system has been used effectively for more than a decade. During the past few years, many biometric traits have been applied in the security domain, ranging from fingerprint to face, to Iris, and, more recently, to vein and blood flow. Nowadays, the fingerprint has become the most widely used among these traits because of its uniqueness and easiness to collect [1].

The fingerprint-based system has many applications, such as fingerprint unlock, and fingerprint payment and the second generation of identity authentication. However, with its widespread use, fingerprint authentication systems are facing being increasingly challenged by counterfeit attacks, and the systems are vulnerable to the attacks. The general fake attack is to make artificial replicas and forge real user fingerprint verification through latex, gelatine, silicone, play-both and other materials. With the purpose of dealing with the spoofing attacks, many fingerprint liveness detection techniques have been developed to distinguish the captured fingerprint image whether real or not. There has been a host of research papers with regard to fingerprint liveness detection. At the same time, some relevant competitions being intended to further promote its development are organized as well. Fig. 1 shows typical example of real and fake fingerprint images that can be obtained from the public database used in the Liveness Detection Competition (LivDet) in the years of 2011 and they all are from the Sagem device.

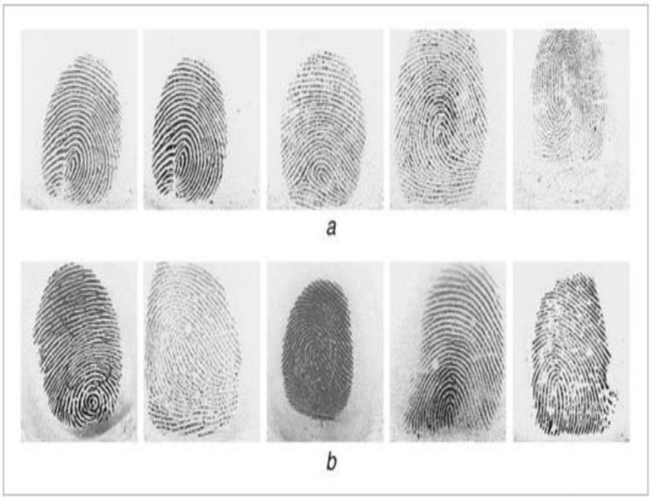


Fig.1 Sample images of LivDet2011

Samples are from the Sagem device. The top row stands for live samples, while the bottom row presents fake samples. The spoof materials are gelatine, latex, PlayDoh, silicone and wood glue from left to right

(a) Live fingerprint images, **(b)** Fake fingerprint images

At present, many deep neural networks have demonstrated their power in many computer classification applications. So, there exist an increasing number of papers studying the deep neural network applied to the detection, and their performances can surpass many traditional spoof detection algorithms [2]. However, deep learning is strict with the demand for the computation resource. These deep learning techniques are not practical in many applications because of the limited computation. In, the convolutional neural network (CNN) is applied to fingerprint liveness detection. The authors of utilize transfer learning to make the trained CNN model solve the two-class classification and achieves remarkable results. While exhibits an experimental conclusion that the CNNs tend to learn first-layer features, akin to either Gabor filter or color blobs when trained on the image. Gabor filter is a linear filter used for texture analysis.

It can extract edge in image processing. Differing from the denoising filters in saving the whole image information, the Gabor filter is used to keep the detailed information. By making the first-layer features resemble Gabor filters in CNNs can we get excellent performance, and this operation reminds that great attention should be paid to the detail information in the spatial domain, equal to the high-frequency information in the frequency domain. It is also recommended that the sharp feature in original images should not be ignored whilst detecting fingerprint liveness. However, there have been many researchers of fingerprint liveness detection mainly concentrating on using multiple texture operators for feature concatenation of the denoised images, ignoring the effect of sharp features in original images. For instance, in [3], researchers propose a method by combining low- level feature, which includes SURF, PHOG, and textures from Gabor wavelet about the denoised image. This method based on the complementarity of texture features achieves some results. However, the shortcomings of this method are also obvious. Denoised images often lose the sharp information of the image, ignoring the contribution of this information to the recognition of the fingerprint living detection. Additionally, the features of multifeatured fusion have higher dimensionality, which would bring high time complexity of recognition and verification. While in another paper [4], Zhang *et al.* propose a novel fake fingerprint detection based on wavelet analysis and local binary pattern (LBP). They realise the significance of sharp information. Thus, their approach applies wavelet analysis to obtain the denoised image and the residual image between the denoised image and the original image. However, the shortcoming of this approach is that there is no need to compute the residual images. The residual images share redundant information with the original images. We can simplify the computation by not doing the subtraction operation to get residual images, replacing it with utilising the original image and the denoised image directly.

MOTIVATION

Biometric methods mean recognizing a person based on a physiological or behavioural characteristic. Biometric data varies from each other. Therefore, the biometric system has been extensively used for personal identification and authentication. Moreover, the biometric system has been used effectively for more than a decade. During the past few years, many biometric traits have been applied in the security domain, ranging from fingerprint to face, to Iris, and, more recently, to vein and blood flow. Nowadays, the fingerprint has become the most widely used among these traits because of its uniqueness and easiness to collect.

II. LITERATURE SURVEY

ChiachiaG et al. [5] In some cases, the urgent need for unattended authentication has influenced a significant implementation of biometric architectures in recent years. This, in turn, has exposed security issues particularly associated with biometric systems. Presentation Attacks (PA, i.e., device login attempts using fake biometrics feature or Presentation Attack Tool) pose an excessive threat to device security: someone may eventually want to manufacture or order a rubber finger or face mask to impersonate someone else. In this context, we present a unique fingerprint attack detection (PAD) scheme based on 1) a novel capture device capable of collecting snapshots in the shortwave infrared (SWIR) spectrum and 2) intensity analysis of fully based strategies. On the literal and in-depth knowledge of abilities. The technology is evaluated against a database of more than 4,700 samples drawn from 562 unique subjects and 35 Presentation-Proprietary Attack Tool (PAI) types. The effects show the strength of the proposed approach with a detection equal error rate (D-EER) of only 1.35%, even in the practical scenario where five unique types of PAI are considered the most effective for validation purposes. (No unknown attacks).

DubeyR et al.[6] Anonymous people can impersonate authorized users to complete various authentication processes, thus disrupting the lifestyle system and causing great economic loss to society. , known as Fingerprint Life Detection (FLD), has been exploited. Compared with the handcrafted function methods, the deep convolutional neural network (DCNN) can automatically investigate the higher-level semantic element through the supervised learning rule set without professional history information. However, one of the drawbacks of extreme CNN models is that fixed-scale images (e.g., 227 x 227) matter in the input layer. Although dimensional problems can be solved by cropping or scaling operations by resampling an image of any scale to a hard and fast scale, it may cause some loss of key texture statistics and image resolution degradation to impair the generalization performance of the model classifier. This paper proposes a new FLD approach called advanced DCNN with an image scale equation to keep texture records and maintain image resolution. In addition, in this article, an adaptive method of obtaining price knowledge has been used. In performance appraisal, a confusion matrix is implemented in FLD for the first time as an indicator of performance. Experimental result amounts based entirely on the LivDet 2011 and LivDet 2013 scoring units also confirm that the detection performance of our technique is superior to other strategies.

ZhangY et al.[7] Fingerprint reputation systems are widely used in our daily life, including door security, identification, and phone verification. However, the prevalent problem is that fingerprint recognition systems are easily fooled by using fake fingerprints for collaboration. Therefore, it is necessary to design a module for the lifetime detection of fingerprints in fingerprint reputation structures. To solve the above problem and distinguish between real and fake fingerprints, a unique, fully software-based activity detection technique that uses a uniform near-binary sample (ULBP) in a spatial pyramid for fingerprint activity detection is implemented. Fingerprints on this document. First of all, the pre-treatment process for each fingerprint is basic. Then, to solve the image rotation and size invariance, three-layer spatial fingerprint pyramids were added in this paper. Then, the texture records of the 3-layer spatial pyramids are determined using a standardized neighborhood binary pattern to extract specific fingerprint capabilities. The accuracy of our proposed method has been compared to several new techniques in detecting the age of fingerprints. Experiments were performed based on recent databases taken from the 2013 Life Detection Competition of 4 different fingerprint sensors. Finally, the fully dependent classifier version is trained on features extracted using the SVM classifier. Experimental effects show that our proposed approach can gain very common accuracy compared to other techniques.

NogueiraR et al. [8] It is well known that fingerprints can be easily superimposed to deceive identity structures. This paper recommends a completely new method with preserved fingerprint templates for life-detector identification. The fingerprint recognition platform should contain a list of saved sample fingerprints to compare with new fingerprints seeking access to the device. Therefore, instead of simply detecting a lifetime of probe fingerprints, the proposed approach uses matching template fingerprints and probe fingerprints via convolutional neural networks to perform lifetime selection containing type-serial convolutional neural networks. The proposed approach can be built on existing life detection methods to increase accuracy without a huge leap in computation time. The evaluation of the LivDet dataset indicates that the proposed fingerprint age detection technology can provide superior accuracy.

III. PROPOSED METHODOLOGY

In order to utilise the information from both the denoised image and the original fingerprint image, we extract features from the two images directly. The procedure of fingerprint liveness detection is presented as follows. First, the ROI extraction method is used to crop the useless background and put the fingerprint in the centre position. A guided image filtering operation is applied to the extracted ROI to get a denoised version of the input image. In order to get rid of the impact of different illumination conditions, we apply the contrast-limited adaptive histogram equalisation (CLAHE) to both the original ROI and the smoothed one. Finally, the co-occurrence of adjacent LBPs (CoALBPs) features is extracted separately from the original and the filtered images. Both of these features are concatenated together, and the dimension is reduced via the t-SNE method. The fingerprint liveness detection is implemented via the linear support vector machine (SVM) algorithm with the radial basis function (RBF) kernel. The whole algorithm flow is illustrated in Fig. 2.

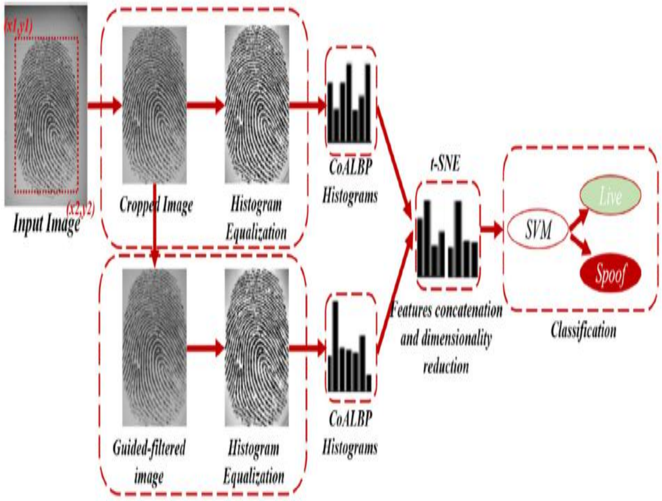


Fig.2 Framework of the proposed fingerprint liveness detection scheme

Pre-processing operation

This pre-processing operation includes ROI extraction, guided filtering, image equalisation. Many fingerprints captured from the optical device are usually not in the centre position of the image, and the background takes up a large part percentage of the image. We want to increase the ratio that the foreground accounts for in the whole image. There are two choices for us to realise the target that is to discard the useless background information and let the input image comprise most of the foreground. One is the fingerprint segmentation or matting and the other is the image cropping. Even though both the ways above is effective to drop the useless information that the background provides, the traditional fingerprint segmentation such as OSTU algorithm does not fit the fingerprint images like Fig. 3, having the low image contrast. In Fig. 3, the first two images show the original images, while the last two images present the corresponding segmentation images being dealt with OSTU algorithm. When the grey level of the background has a little difference with the foreground, the traditional algorithm OSTU will mistake the background as the foreground. In order to balance the effect and the computation loads, we decide to do some more simple but straightforward operations on the fingerprint segmentation results. The proposed method to extract the ROI is based on the OSTU algorithm and utilises the characteristics of the interwoven appearance of the ridges and valleys. The approach is depicted in Algorithm 1 (see Fig. 4). After transforming the original image to the binary image using OSTU, we visit each pixel in the binary image from top to down and left to right. Since we determine the cropping box coordinate via the number of the black pixel changing to the white pixel and the white pixel changing to the black pixel.

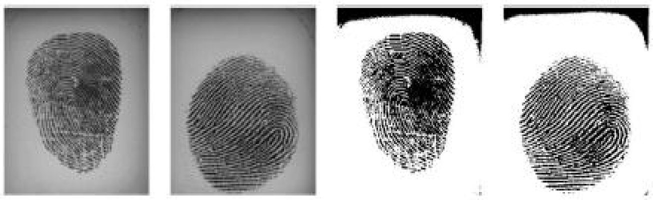
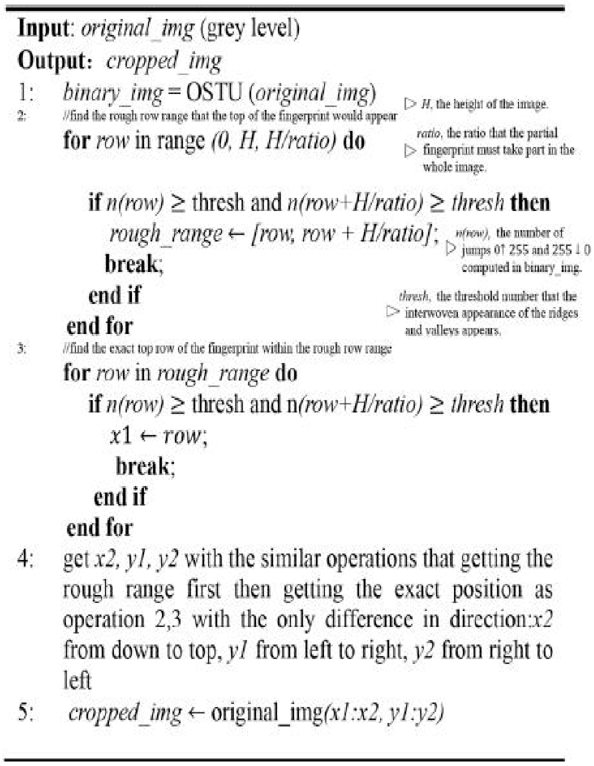


Fig.3 Sample images of mistaken segmentation



```
Input: original_img (grey level)
Output:  cropped_img
1:   binary_img = OSTU (original_img)                          ▷ H, the height of the image.
2:   //find the rough row range that the top of the fingerprint would appear
     for row in range (0, H, H/ratio) do                       ▷ ratio, the ratio that the partial
                                                                 fingerprint must take part in the
                                                                 whole image.
         if n(row) ≥ thresh and n(row+H/ratio) ≥ thresh then
             rough_range ← [row, row + H/ratio];               ▷ n(row), the number of
             break;                                              jumps 0↑ 255 and 255 ↓ 0
                                                                 computed in binary_img.
         end if                                                ▷ thresh, the threshold number that the
     end for                                                     interwoven appearance of the ridges
                                                                 and valleys appears.
3:   //find the exact top row of the fingerprint within the rough row range
     for row in rough_range do
         if n(row) ≥ thresh and n(row+H/ratio) ≥ thresh then
             x1 ← row;
             break;
         end if
     end for
4:   get x2, y1, y2 with the similar operations that getting the
     rough range first then getting the exact position as
     operation 2,3 with the only difference in direction:x2
     from down to top, y1 from left to right, y2 from right to
     left
5:   cropped_img ← original_img(x1:x2, y1:y2)
```

Fig.4 Algorithm 1: Fingerprint image cropping algorithm for extracting ROI

Feature extraction

Feature extraction is of considerable significance to future classification. The performance of classification is determined by the extracted features. LBPs is a type of texture descriptor generally used for classification in computer vision. In its original version, the LBP operator assigns a label to every pixel of an image by thresholding the 3 × 3-neighbourhood of each pixel with the centre pixel value. The label of the centre pixel is then represented as an 8-bit integer, where each bit is the pixel state in its neighbourhood.

However, in the original LBP descriptor, the packing of LBP patterns into histogram tends to discard the spatial information among the patterns. It considers only the magnitude relation between the centre and the neighbouring pixel intensities. To exploit the spatial relationship among the patterns, we take the CoALBPs [20] into account. It is defined as an index of how often their combination occurs in the whole image. The proposed feature is robust against variations in illumination and can simultaneously retain more details of the image. In [20], an approach is proposed that modify the LBP configuration to consider sparser configurations, and it can reduce the cost of computation.

Feature dimension reduction

The denoised image is obtained via guided image filtering where the cropped image itself is considered as the guidance image. For the CoALBP features are extracted separately from the ROI images and the smoothed images, we concatenate the features together to form a long feature. The future aim is to apply the concatenated feature to reduce the high-dimensional feature into a relatively lowdimensional subspace.

The PCA is commonly used for the data dimension reduction. However, PCA is linear, and it cannot demonstrate the complex polynomial relationship among the features. In this paper, we use the t-SNE for dimension reduction, which is faster than PCA and can preserve the local and global structure of the data at the same time.

The t-SNE algorithm is based on SNE and is easier to optimise compared to SNE. It produces significantly better visualisation than SNE as well. The difference between the two algorithms is the cost function. The t-SNE uses a symmetrised version of the SNE cost function with simpler gradients, and it uses a student-*t* distribution rather than a Gaussian to compute the similarity between two points in the low-dimensional space. By doing this, t-SNE can handle the crowding problem and the optimised problems in the SNE method. The t-SNE method is particularly vital for high-dimensional data that lie on several different but related low-dimensional manifolds. Therefore, we choose the algorithm to do with the dimensionality reduction, and the following experiments show the effectiveness.

Classification

After the features are extracted and the dimension of the features is reduced, SVM is used to distinguish fake fingerprints from real fingerprints. In the training procedure, we choose the Gaussian RBF as the kernel of the SVM method. SVM with RBF kernel has slightly better performance than the linear kernel. We apply the kernel to map the obtained feature vector to a higher space and to classify better. The kernel function is determined by five-fold subject-disjoint cross-validation. In addition, SVM is utilised to make a decision in the test stage.

Experiment analysis

We evaluate the effectiveness of our approach in liveness detection of fingerprint on three benchmark data sets: LivDet2011, LicDet2013, LivDet2015.

Data sets and performance metrics

We used the data sets provided by the LivDet in the years 2011, 2013 and 2015. LivDet2011 is made up of images from four different devices: Biometrika, Digital Persona, Italdata and Sagem. There are 4000 images for each of these devices, 2000 live images and 2000 spoof images (400 of each of five spoofs materials). LivDet2013 consists of images from four different devices: Biometrika, Crossmatch, Italdata and Swipe. There are 4000 or more images for each of these devices as detailed explained. Also, LivDet 2015 consists of four different optical devices: Green Bit, Biometrika, Digital Persona and Crossmatch. There are >4000 images for each of these devices which is described in detail explained. Fig. 5. shows typical examples of real and fake fingerprint images that can be obtained from the public database used in LivDet 2011 and they are from different devices. Since it was known that it might be affected by an acquisition problem for the Crossmatch . data set of LivDet2013 [8], we avoid using it in our experiments. In all data sets, the Real/Fake fingerprint ratio is 1/1 and they are equally distributed between training and testing sets. The classification results were evaluated by the accuracy

IV. RESULTS

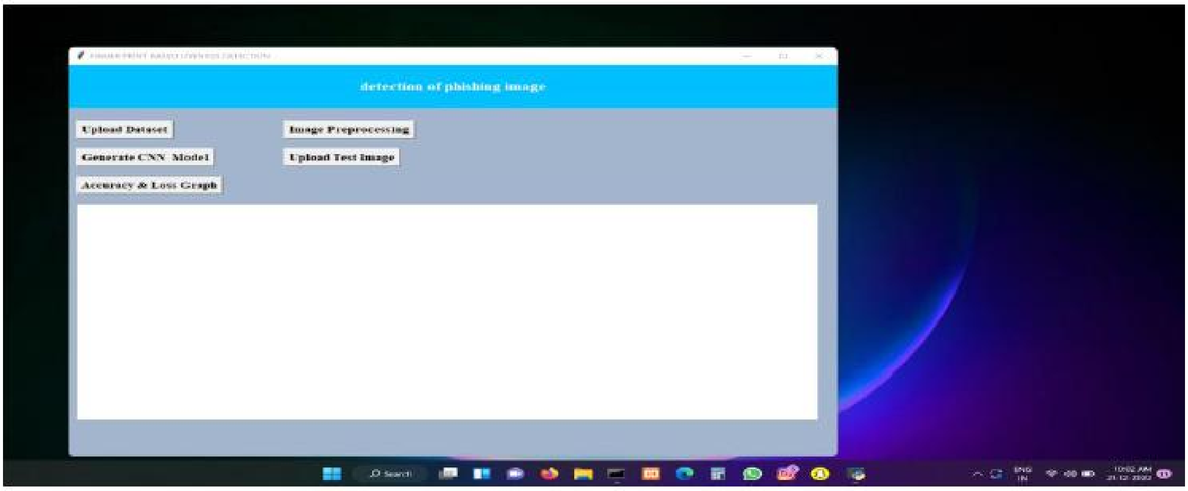


Fig.5 In above screen click on _Upload Dataset ‘button to upload dataset

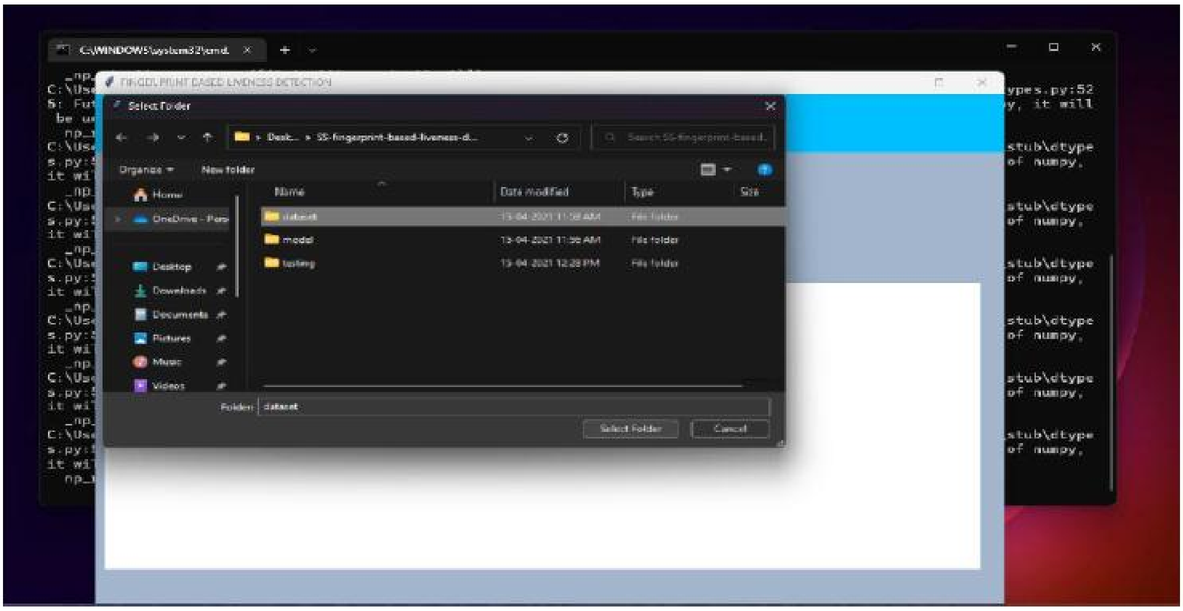
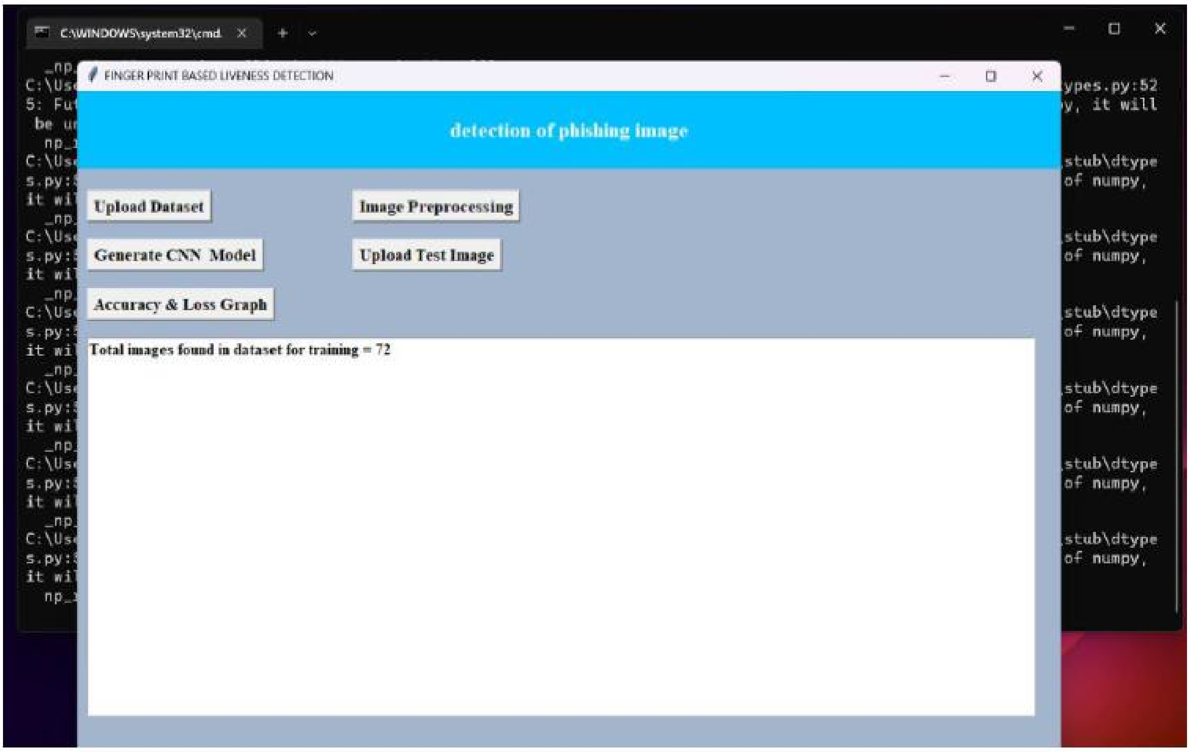


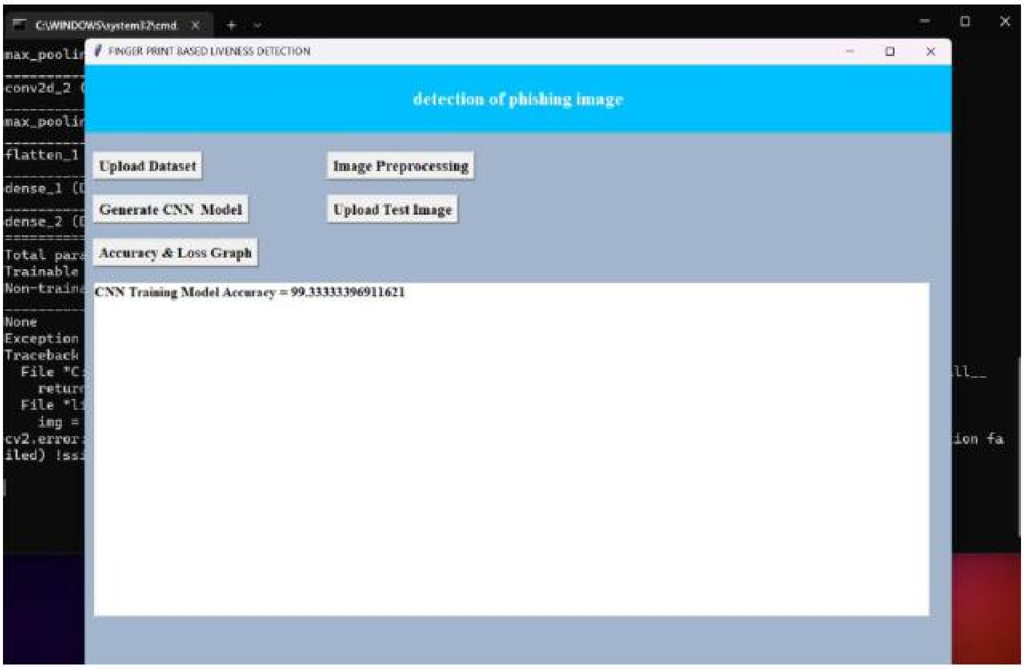
Fig.6 In above screen selecting and uploading _dataset�' file and then click on _Open' button to load dataset.



```
ypes.py:52
y, it will
stub\dtype
of numpy,
```

Total images found in dataset for training = 72

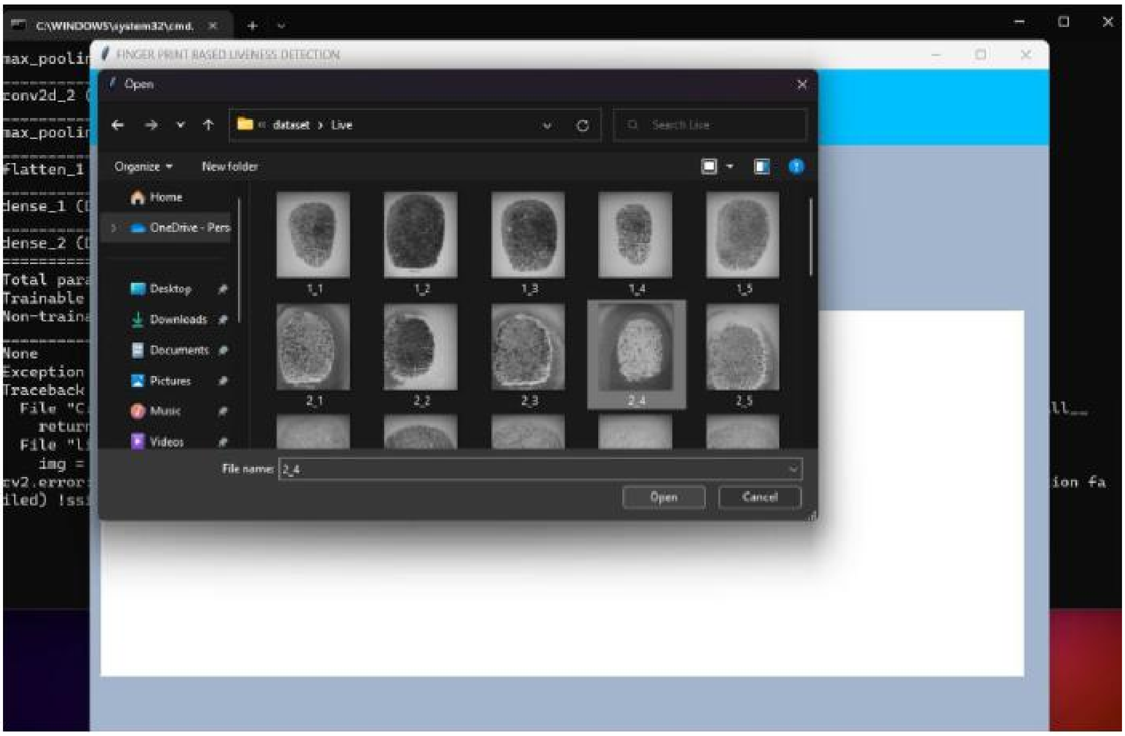
Fig.7 In above screen dataset loaded and now click on _Image Preprocess' button to read and process dataset and to get below screen.



```
max_poolin
conv2d_2 (
max_poolin
flatten_1
dense_1 (D
dense_2 (D
Total para
Trainable
Non-traina
None
Exception
Traceback
  File "C:
    return
  File "li
    img =
cv2.error:
iled) !ssi
```

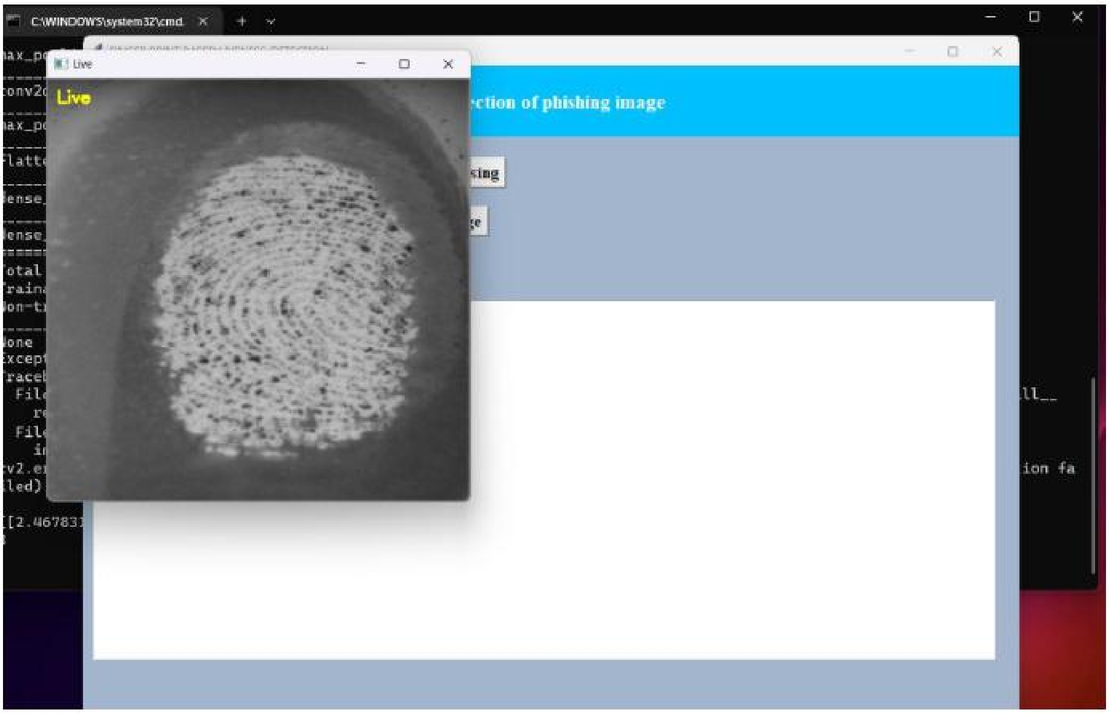
CNN Training Model Accuracy = 99.33333396911621

Fig.8 In the above slide we click _generate CNN model‘ for obtaining the accuracy of the image as shown and click upload test image to get below slide



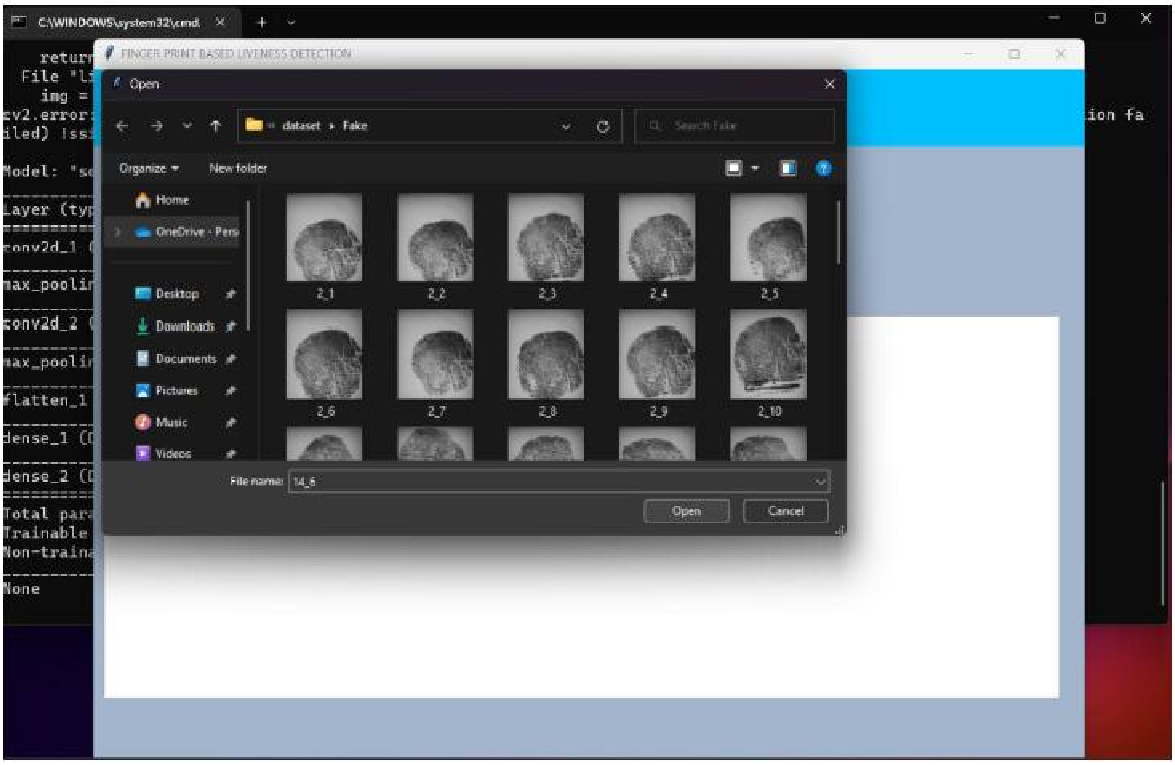
```
max_poolin
conv2d_2 (
max_poolin
flatten_1
dense_1 (D
dense_2 (D
Total para
Trainable
Non-traina
None
Exception
Traceback
  File "C
    return
  File "L
    img =
cv2.error:
iled) !ss
```

Fig.9 Select any image from the dataset with finger imprints and click the button open



```
ax_p
conv2
ax_p
flatt
ense_
ense_
otal
rain
on-t
one
xcep
racel
 Fil
   r
 Fil
   i
v2.e
led)

[2.467832
```

Fig.10 The output is displayed as live if the fingerprint has liveness from the selected dataset

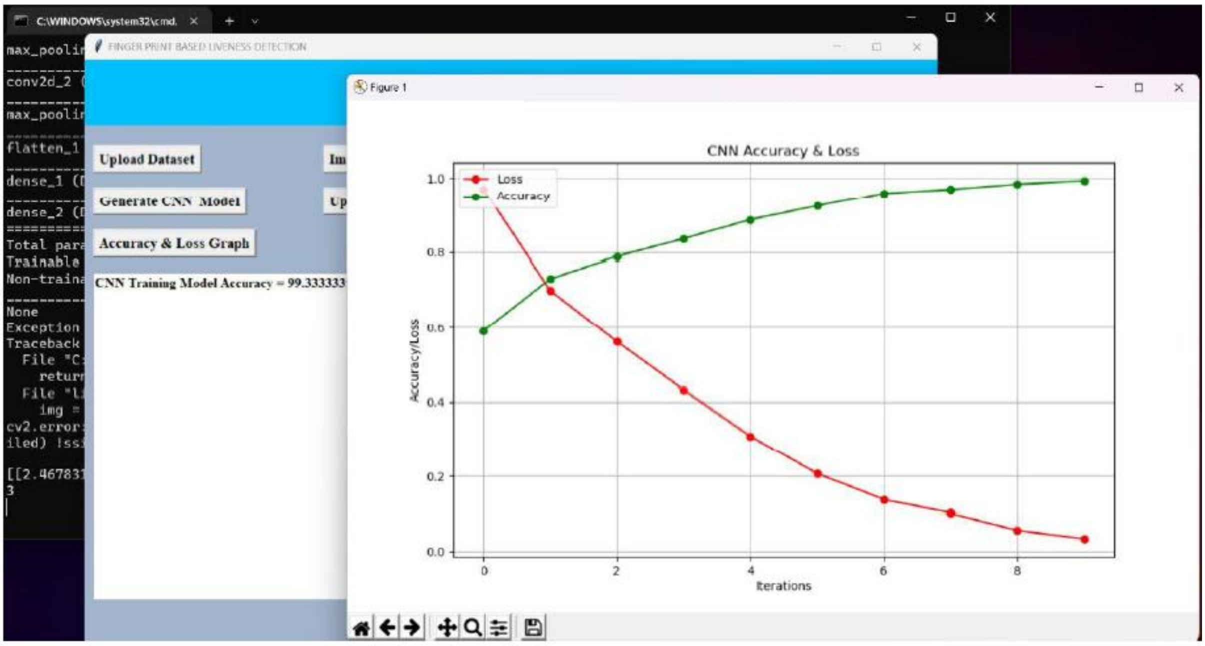


```
  retur
 File "li
  img =
cv2.error
iled) !ssi

Model: "se

Layer (typ
==========
conv2d_1 (

max_poolir

conv2d_2 (

max_poolir

flatten_1

dense_1 (I

dense_2 (I
==========
Total para
Trainable
Non-traina

None
```

```
ion fa
```

File name: 14_6

Fig.11 If the fingerprint is selected from the _fake‘ dataset then the images are fingerprint spoofs and displayed as FAKE



```
max_poolin
conv2d_2 (
max_poolin
flatten_1
dense_1 (I
dense_2 (I
==========
Total para
Trainable
Non-traina

None
Exception
Traceback
  File "C:
    return
  File "li
    img =
cv2.error
iled) !ss

[[2.467831
3
```

CNN Training Model Accuracy = 99.333333

Fig.12 CNN Accuracy & Loss

V. CONCLUSION

In this paper, a fingerprint liveness detection method based on the guided filter and hybrid image analysis is proposed.

ISSN: 2366-1313

This method uses the concatenated CoALBPs features extracted from the hybrid images, i.e. both the original and the filtered image, to improve the performance of fingerprint liveness detection. By comparing the structure of CNNs and the traditional processing methods, we find the crucial significance of the sharp information of the original images. In addition, the experiments also verify the efficiency of the sharp information. We divide the whole algorithm into four steps. First, we do the pre-processing operation to get the image that has the most useful information. Second, we utilise the CoALBPs descriptor to obtain the features of the original imageand the denoised image. Third, we apply the t-SNE algorithm to realize the dimension reduction of the concatenated features which belong to the original image and the smoothed image. At last, SVM with RBF kernel is used to train the classification.

REFERENCES

[1] Menotti, D., Chiachia, G., Pinto, A., et al.: _Deep representations for iris, face, and fingerprint spoofing detection ', IEEE Trans. Inf. Forensics Sec., 2014, 10, (4), pp. 864–879

[2] Dubey, R.K., Goh, J., Thing, V.L.L.: _Fingerprint liveness detection from single image using low-level features and shape analysis ', IEEE Trans. Inf. Forensics Sec., 2016, 11, (7), pp. 1461–1475

[3] Zhang, Y., Fang, S., Xie, Y., et al.: _Fake fingerprint detection based on wavelet analysis and local binary pattern '. Biometric Recognition, Shenyang, People's Republic of China, 2014, pp. 191–198

[4] Nogueira, R.F., Lotufo, R.D.A., Machado, R.C.: _Fingerprint liveness detection using convolutional neural networks ', IEEE Trans. Inf. Forensics Sec., 2016, 11, (6), pp. 1206–1213

[5] Schuckers, S., Abhyankar, A.: _Detecting liveness in fingerprint scanners using wavelets: results of the test dataset '. Biometric Authentication, ECCV 2004 Int. Workshop, BioAW 2004, Prague, Czech Republic, 2004, vol. 3087, pp. 100–110

[6] Schuckers, S.A.C., Parthasaradhi, S.T.V., Derakshani, R., et al.: _Comparison of classification methods for time-series detection of perspiration as a liveness test in fingerprint devices ', IEEE Trans. Syst. Man Cybern. C, 2005, 35, (3), pp. 335–343

[7] Yambay, D., Ghiani, L., Denti, P., et al.: _Livdet 2011—fingerprint liveness detection competition 2011'. Proc. 5th

IAPR Int. Conf. Biometrics (ICB), New Delhi, India, March/April 2012, pp. 208–215.

[8] Ghiani, L., Yambay, D., Mura, V., *et al.*: 'Livdet 2013 fingerprint liveness detection competition 2013'. Proc. IAPR Int. Conf. Biometrics, Madrid, Spain, June 2013, pp. 1–6

[9] Mura, V., Ghiani, L., Marcialis, G., *et al.*: 'Livdet 2015 fingerprint liveness detection competition 2015'. Proc. IEEE Int. Conf. Biometrics Theory, Applications and Systems, Arlington, VA, USA, September 2015, pp. 1–6

[10] Kim, S., Park, B., Song, B.S., *et al.*: 'Deep belief network based statistical feature learning for fingerprint liveness detection', *Pattern Recognit. Lett.*, 2016, **77**, (C), pp. 58–65

[11] Pala, F., Bhanu, B.: 'Deep triplet embedding representations for liveness detection', in Bhanu, B., Kumara (Ed.): *'Deep learning for biometrics', Advances in Computer Vision and Pattern Recognition* (Springer, Cham, Switzerland, 2017), pp. 287–307