p-ISSN: 1979-5661
e-ISSN: 2622-321X

Spoof Detection Using Local Binary Pattern In Face

Anshika Shukla[a1],Vani Dave[b2],Ayush Mishra[a3]

Assistant Professor
[a]Department of computer science and Engineering,
Kanpur Institute of Technology, India
[1]anshikashukla4@gmail.com

Assistant Professor
[b]Master In Computer Application
Kanpur institute of technology
[2]vani_dave@rediffmail.com(corresponding author)

Research Scholar
[a]Department of computer science and Engineering,
Kanpur Institute of Technology,India
[3]ayush8stp@gmail.com

Abstract

Spoofing attack is an attempt to acquire some other's identity or access right by using a biometric evidence of authorized user. Among all biometric systems facial identity is one of the widely used method that is prone to such spoofing attacks using a simple photograph of the user.

The paper focuses and takes the problem area of face spoofing attacks into account by detecting spoof faces and real faces. We are using the local binary pattern (LBP) for providing the solution of spoofing problem and with the help of these patterns we inspect primarily two types of attacks i.e. printed photograph and photos displayed using digital screen. For this, we will use the local database maintained by us having the images labeled as real and spoof for the data required.

We conclude that local binary pattern will reduce the total error rate and will show the moderate output when used across a wide set of attack types. This will enhance the efficiency of the system for detection of spoofing by using the deep learning techniques.

Keywords :Spoofing ,Local Binary Pattern, CASIA, NUAA, Hyperplane, Support Vector machine

1. Introduction

Spoofing attack is a way of cyber attack in which a person tries to override the biometric authentication of a valid user by presenting a counterfeit biometric evidence .In this attack attacker does not need any knowledge about the algorithm used in the biometric system .The biometric based verification systems are mostly not resistant to spoofing attack due to the reason of their designing as they are designed only to recognize identities without checking their liveliness. Instead some authentication systems which are using biometric authentication are also not able to implement the anti spoofing scheme in a very sophisticated way.

Attacking on biometric system in different possible ways will require different level of difficulty for the attacker to create a spoof identity. In biometric systems like fingerprint recognition and iris recognition we require the artificial spoof evidence that can counterfeit the real identity and this requires a great expertise but the generation of fake evidence in face spoofing attack is easy and can be done by using a simple photograph of valid user . The biometric evidences can be easily by passed by either using these images or using a pre- recorded video.

As this kind of attack came into knowledge of the biometric community, various geeks provided their pay to check the liveliness of the person by adding various sensors to the biometric system. These systems detect the liveliness of person by asking user to perform some tasks or make a particular kind of gesture. But all

these sensors are external hardware that are required to perform this detection hence making a completely automated detection system is cheaper way as compared to these systems.
This approach we have opted in this is to find the Local Binary Patterns (LBP) in the given image data and extract the feature from that LBP image by creating the histogram from the LBP data . These histogram will be used to perform the training of the model to predict the real spoof facial evidence.

2. **Existing anti spoofing methods and techniques**

For the implementation of anti spoofing there are various techniques and methods used. These methods follow the three basic ways to perform the spoofing detection: The first one is by assessing the texture of the subject image captured by the sensor of the system as it checks the complete texture of image to find the variation between real and spoof image. The second one is by detecting the liveliness of the environment during the capturing of image which checks the scene if it is live or pre- recorded video clip. The third one is a combination in which we use the texture based technique and the liveliness based detection together. Taking the first approach into account the spoof detection method using feature texture of the image was made when this was mentioned in a paper that the text of real image and spoof image varies on the basis of frequency distribution. As in capturing of any image the two main process comes in account are Illumination and reflectance so the frequency distribution of any image completely depends upon the reflectance and this is found that the reflectance of recaptured image shows various difference between the real once captured scene on the basis of their frequency distribution . So the previous work is done by using this frequency distribution and training the classifier by this frequency distribution the image. These classifiers further give their prediction for the data.

3. Methodology and Experiments

The paper here presents the anti-spoofing method using the described same concept of texture analysis of the live captured frames/images. In this method we will primarily use three concept that will be required for the whole method to be implemented. As in this method we are using the Local Binary Patterns (LBP) to train the algorithm I.e. SVM . We will brief the information about the LBP, SVM and the dataset we will be using for the implementation of this method.

3.1 Local Binary Pattern (LBP)

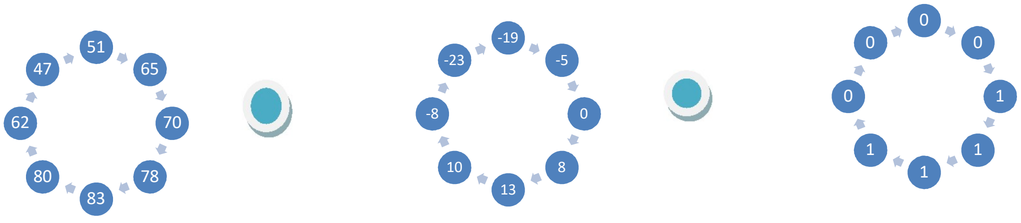
LBP is a pattern which is extracted from the image by processing its pixel in a specific logic format so that they change their value to binary values I.e. 0 & 1. LBP method provides the labeling of the pixels by finding the difference of neighborhood of each pixel and outputs that image area as the binary number. Because of its high discrimination power and an ease and simplicity in computation, This operator has got a better popularity in its approach to be used in various applications. It has become a very unique approach for textual analysis other than the traditionally used textual analysis approach. The one of the most important property or feature of LBP is that it shows its robust behaviour for the unicolor/bicolor in grey scale images.

p-ISSN: 1979-5661
e-ISSN: 2622-321X

For example, by the intensity difference in illumination .

The value of the LBP code of a pixel (x_c,y_c) is given by:

LBP$_{P,R}$= $\sum_{p=0}^{p-1} s(gp - gc)2^p$ s(x)=$\begin{cases} 1, if\ x >= o; \\ 0, otherwise. \end{cases}$



1.Sample 2.Difference 3.Threshold

1*1+1*2+1*4+1*8+0*16+0*32+0*64+0*128=15

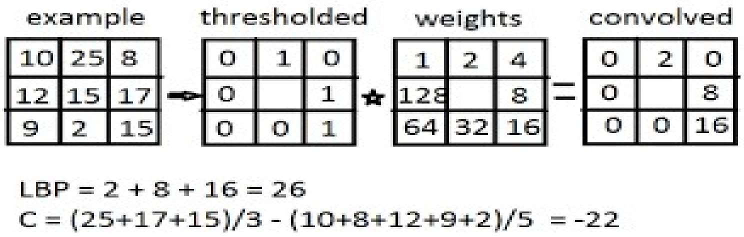
4. Multiply by powers of two and sum

The LBP algorithm we are applying here requires a total of four tunable parameters:

1. **Radius**: It is used to handle and create the round/circular LBP and decides to represent the radius of that around the centered selected pixel. The default and most probable value is taken as 1.
2. **Neighbors**: The total number of points that are considered to build the rounded local binary pattern are termed as number of neighbors. The increase in neighbor count will increase the computational cost hence to reduce the cost we use less neighbor sample. The default value is taken as 8.
3. **X-Set**: The number of blocks in the horizontal side I.e. x-axis. The more cells we will use, the better and finer the grid will become and the dimensions of the resulting feature vector will inhance and be raised. The default value is taken as 8.
4. **Y-Set**: The number of blocks in the vertical side I.e. y-axis. The more cells we will use, the better and finer the grid will become and the dimensions of the resulting feature vector will enhance and will be raised. The default value is taken as 8.

The logic and mathematics to form the Lbp image from original uses the radius and pixel to be considered as input to then get the metrics of image according to the given inputs. This is then calculated as per the logic

LBP(p,r) = sigma-in range p=0 to p-1(gp-gc)
Taking the base threshold as 2^p



example

10	25	8
12	15	17
9	2	15

thresholded

0	1	0
0		1
0	0	1

weights

1	2	4
128		8
64	32	16

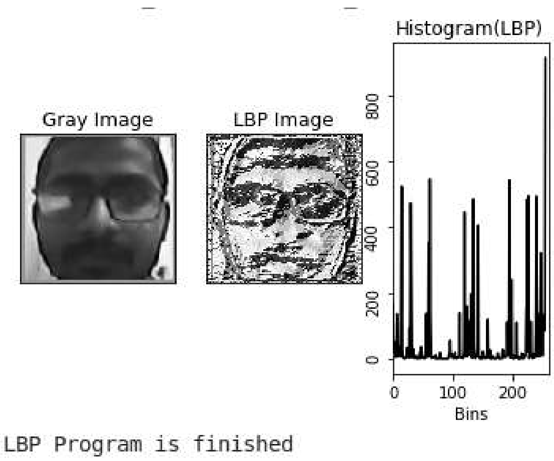
convolved

0	2	0
0		8
0	0	16

LBP = 2 + 8 + 16 = 26
C = (25+17+15)/3 - (10+8+12+9+2)/5 = -22

3.2 Extracting the histogram

The histogram is prepared on the basis of frequency distribution of lbp image formed from the actual image. This is done after the image is converted to LBP format and hence this is done in mainly two ways: By taking the frequency of the pixel value and plotting on a histogram or by taking the probability of the frequency of pixel value. In this paper we are using the first way to form the histogram which will be required as input data to feed the algorithm. This histogram will be made by using the pixel data provided after the image is converted to lbp.



```
LBP Program is finished
```

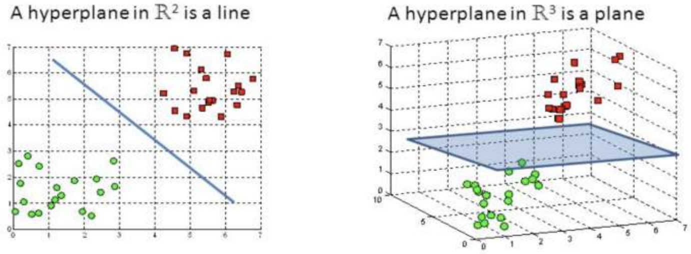
Now this LBP histogram will be used as an input feed for the algorithm and this histogram shows variation in frequency distribution of real image and recaptured image on the basis of reflectance.

3.3 Algorithm Used: Support Vector Machine (SVM)

The support vector machine algorithm helps to find a specific plane in an N-dimensional space that classifies the different data points in a distinct way. The N-Dimensional space refers to space having N features. To separate the two classes we have various planes available in the same feature set . The main objective of this algorithm is to find a specific plane that could provide the maximum possible margin between these data points, i.e. the distance between data points of the two different classes must be maximum. Maximizing this margin distance between two different classes data points creates reinforcement so that the next points that are to be tested gets more accuracy as per the last updated details.

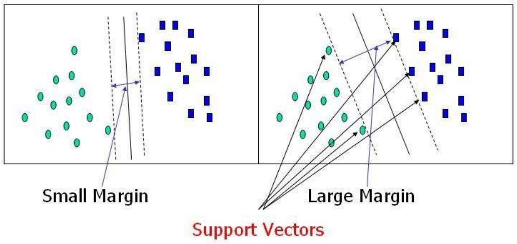
3.4 Hyperplane

Hyperplanes are the virtual boundaries made across the data points to classify their classes. These data points are provided to their specific classes as per their belonging to either side of the plane. As the planes are completely dependent upon the features provided hence the dimension is dependent upon the features . Lets assume that there are two features then we can consider a line as the hyperplane. In similar way if there are a total of three features then the hyperplane will be a plane. If we think of features more than the three then it will be a difficult task to decide the hyperplane of it.



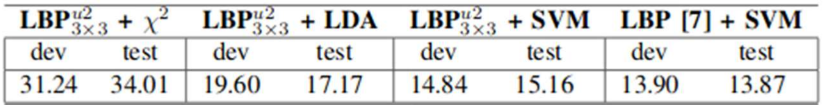
3.5 Support Vectors

The support vectors are the data points that are much nearby to the actual hyperplane and they provide the support to the hyperplane and adjust the position of hyperplane as per the accuracy. These support vectors are used to maximize the margin between the data points that is used in the classifier. If we will remove the support vectors the location of hyperplane will be automatically adjusted and that too with a bad accuracy and less margin. These support vector and hyperplane points help us in building our SVM as only a single linear vector i.e hyperplane can’t maximize the margin and hence these support vectors provide a support to our linear decision boundary to maximize the margin.



4. Training and Accuracy

The SVM is trained using the data that is provided as input feed in form of histogram. This data is input by the histogram associated with its label. The training and testing/validation will require a huge dataset as SVM requires a huge data for better accuracy. The data here will be feed in a specific format and after the training of algorithm the validation will be done using some other data to check its response to new or fresh data. This is done to check the EER% which can lead to a better and much accurate algorithm to be used.



$LBP^{u2}_{3\times3}$ + χ^2		$LBP^{u2}_{3\times3}$ + LDA		$LBP^{u2}_{3\times3}$ + SVM		LBP [7] + SVM	
dev	test	dev	test	dev	test	dev	test
31.24	34.01	19.60	17.17	14.84	15.16	13.90	13.87

This EER% clearly shows that the error rate is less if we use the SVM with the huge input data for feed and this can enhance the accuracy rate as well. The SVM used in this method is tested as per other algorithms and the comparison between the accuracy of dataset used is mentioned. These error rate and accuracy details are claimed in referred journal by author using the same classifier and databases. The accuracy of model/classifier varies as we switch from NUAA database to CASIA database. This accuracy is enhanced when SVM is used with the CASIA database and the outputs vary in a better way.

	NUAA		CASIA-FASD
	Dev	Test	Dev Test
LBP^{u2}_{3X3} + LDA	0.06	18.32	17.08 21.01
LBP^{u2}_{3X3} + SVM	0.11	19.03	16.00 18.17
LBP[7] + SVM *	0.11	13.17	15.43 18.21

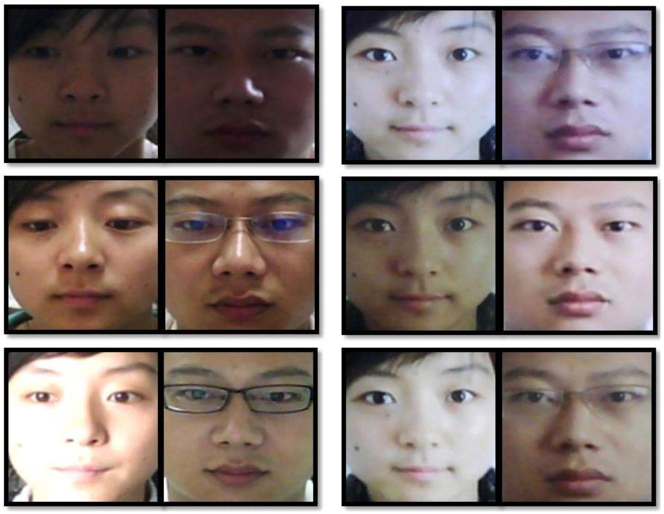
5. *Database*

As we know that any algorithm can work efficiently and with a good accuracy when is given a huge amount of data as input feed. Hence here we require a lot of data for the training and validation of the algorithm i.e. SVM. The data here is set of images having two classes that are: Real images that are taken live and can be considered as once captured images and the second class consist of images that are spoof and can be considered as fake/recaptured images.

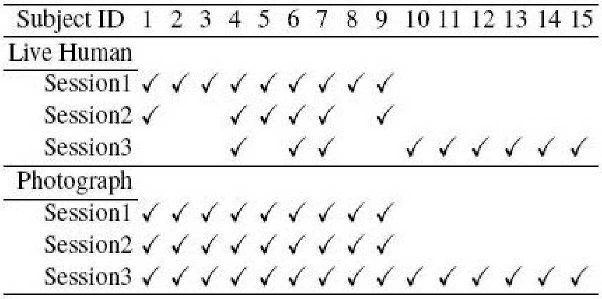
5.1 NUAA

The database used in some traditional methods was NUAA and it consist of 15 subjects in the dataset, every one of them consist of real face of the subject, and photograph of them. Real face is taken from webcam with natural expression and frontally face the camera, there is no movement such as eye blink, this is used to make the real face similar like the photograph.

p-ISSN: 1979-5661
e-ISSN: 2622-321X



Each column from the different section 1, section 2 and section 3. In each row, the left side image set are from a real human face and the right side image set from a photo. This dataset consist of various types of changes in the images of different subjects and these changes are like their gender variation, the intensity of light , use of spectacles etc . All the images in the dataset are of same resolution of 640 x 480 pixels.



Subject ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Live Human															
Session1	✓	✓	✓	✓	✓	✓	✓	✓	✓						
Session2	✓			✓	✓	✓	✓		✓						
Session3				✓		✓	✓			✓	✓	✓	✓	✓	✓
Photograph															
Session1	✓	✓	✓	✓	✓	✓	✓	✓	✓						
Session2	✓	✓	✓	✓	✓	✓	✓	✓	✓						
Session3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

5.2 CASIA

CASIA Face Image Database Version 5.0 (or CASIA-FaceV5) is the latest updated CASIA dataset for faces and it consists of a total of 2,500 colored facial images of 500 different subjects(persons). The images of faces in this dataset are captured in a single session using the specific Logitech USB camera. The subjects in this dataset are not professional research scholars but they are normal people like graduate students, workers, waiters etc . The images provided in this dataset consist of similar features as they all have the same format of BMP extension and they are 16 bit color images. The resolution of these images is 640*480. There are also some of the differences found in the images of this dataset and this is like intensity of light variation, the posture of person, the expression shown by subject, the distance etc.

The images of the dataset of CASIA are stored in a specific format and it provides the whole data into subsets and if we wish to download the cropped images we can get them within 150 MB and the downloaded data is also in specified format.
The actual dataset has a more detailed and complete images without cropped and this dataset is available in more than two forms , one of which is so small in size for the testing purpose of for the demo and the second one is cropped images and the real ones as well. These images differ in various aspects like size , quality etc.
This data is more relevant and appropriate that provides a better accuracy in prediction and this paper uses the CASIA dataset for a better quantity and quality of data.

6. CONCLUSION

This paper provides a way to study the approach to face anti-spoofing method using the CASIA database available for face biometric research and SVM classifier to work on that data. In here we have used the training images in LBP format which then is transformed to histogram having the frequency distribution for feeding the algorithm. The algorithm provides a better efficiency and a reduced error rate with efficient approach. In this we have used only the prediction for images and frames but it can be enhanced by using the video content in account for the training purpose as it will check the liveliness in a better way and the error rate can be further reduced and accuracy can be enhanced.

7. Acknowledgement

We would like to thank our deep sense of gratitude to college , that provided us an opportunity to write a paper . We are very thankful to the Management and the Director of the Institute for the help they provided us during the writing the content of this paper .We would also like to give special thanks to our HOD"s of CSE & IT & MCA Dept. and collogues of the college for their true encouragement and guidance in the completion of the paper.

References:

[1] Portions of the research in this paper use the CASIA-FaceV5 collected by the Chinese Academy of Sciences' Institute of Automation (CASIA) Images for Data set are referred from "CASIA-FaceV5, http://biometrics.idealtest.org/ "

[2] P. V. Reddy, A. Kumar, S. Rahman, and T. S. Mundra, "A new anti spoofing approach for biometric devices," Biomedical Circuits and Systems, IEEE Transactions on, vol. 2, no. 4, pp. 328–s337, 2008.

[3] S. Parveen, S. Ahmad, S. Mumtazah, M. Hanafi, W. Adnan, and W. Azizun, "Face anti-spoofing methods." Current Science (00113891), vol. 108, no. 8, 2015.

[4] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A face anti spoofing database with diverse attacks," in Biometrics (ICB), 2012 5th IAPR International Conference on. IEEE, 2012, pp. 26–31.

[5] J. Galbally and S. Marcel, "Face anti-spoofing based on general image quality assessment," in Pattern Recognition (ICPR), 2014 22nd International Conference on. IEEE, 2014, pp. 1173–1178.

[6] T. de Freitas Pereira, J. Komulainen, A. Anjos, J. M. De Martino,A. Hadid, M. Pietikäinen, and S. Marcel, “Face liveness detection using dynamic texture,” EURASIP Journal on Image and Video Processing,vol. 2014, no. 1, p. 2, 2014.

[7] J. Komulainen, A. Hadid, and M. Pietikainen, “Context based face anti-spoofing,” in Biometrics: Theory, Applications and Systems (BTAS),2013 IEEE Sixth International Conference on. IEEE, 2013, pp. 1–8.

[8] K. Patel, H. Han, and A. K. Jain, ‘‘Cross-database face anti spoofing with robust feature representation,’’ in Proc. Chin. Conf. Biometric Recognit . Cham, Switzerland: Springer, 2016, pp. 611–619

[9] Z. Wang, C. Zhao, Y. Qin, Q. Zhou, G. Qi, J. Wan, and Z. Lei, ‘‘Exploiting temporal and depth information for multi-frame face anti-spoofing,’’ 2018,arXiv:1811.05118. [Online]. Available: https://arxiv.org/abs/1811.05118

[10] Gang Pan, Zhaohui Wu and Lin Sun, Liveness Detection for Face Recognition, Recent Advances in Face Recognition, I-Tech, on Page(s): 236, December, 2008

[11] R. Duda, P. Hart, and D. Stork, Pattern Classification, 2nd ed. John Wiley & Sons, New York, 2001.

[12] D. Wen, H. Han, and A. K. Jain, “Face spoof detection with image distortion analysis,” Information Forensics and Security, IEEE Trans-actions on, vol. 10, no. 4, pp. 746–761, 2015.

[13] C.-C. Chang and C.-J. Lin, “LIBSVM: A library for support vector machines,” ACM Transactions on Intelligent Systems and Technology, vol. 2, pp. 27:1–27:27, 2011, software available at http://www.csie.ntu.edu.tw/ ∼ cjlin/libsvm.

[14] K. Kollreider, H. Fronthaler, and J. Bigun, Non-intrusive liveness detection by face images, Image and Vision Computing, vol. 27(3), pp. 233-244, 2009. Scholarpedia :