ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

Face Spoofing Detection Using Machine Learning Approach

Raghavendra R J[1], Dr. R Sanjeev Kunte[2]

Research Scholar, Department of Information Science & Engineering, JNN College of Engineering, Shimoga, Karnataka, India[1]

Professor, Department of Computer Engineering, JNN College of Engineering, Shimoga, Karnataka, India[2]

ABSTRACT: For face recognition systems, impostors can obtain legal identity authentication by presenting the printed images, the downloaded images or candid videos to the sensor. Since, the face is a unique biometric of the individual and face recognition is the superior identification method. This paper proposes a novel method for face spoofing detection by using features of Local Binary Pattern (LBP) and the popular machine learning approach SVM used as classifier. The LBP is applied to each 3x3 matrix obtained from detected face through Viola-Jones algorithm to get the features. The face image is segmented into number of different blocks and LBP Features are taken, then SVM (Support Vector Machine) is used for determining whether the input image corresponds to live or fake face. Our experimental analysis on a publically available NUAA face anti spoofing database following the standard protocols showed good results.

KEYWORDS: Face-spoofing attack, Local Binary Pattern, NUAA dataset.

I. INTRODUCTION

The Biometric authentication is an essential and power full system that gives more security at surveillance activities. Biometrics are the unique features of human body, cannot be stolen or copied by some other one. It is secured means of authentication technique to recognize and identify the individual. The applications of biometrics are very secured choice in person recognition and/or identification. Spoofing attack is the action of deceiving a biometric sensor by presenting a counterfeit biometric evidence of a valid user [1]. It is a direct attack to the sensory input of a biometric system and the attacker does not need previous knowledge about the recognition algorithm. These attacks typically include print attacks, and replay attacks.

The common approach to detecting spoofing attacks is to collect both real and fake data (spoofing attempts) and then try to learn a suitable classifier to predict whether a test sample is a real access or a spoofing attempt. The assumptions that the artificial biometric evidence can bypass a biometric recognition system, are not only magical. In [2] gives an interesting examplewhere eye-blinking and some extent of mouth movements can be well simulated using just two photographs. However, despite the great progress made in this direction [3-7], there are certain drawbacks to this approach.

On the other hand, face images captured from printed photos look similar to the images where captured directly from the sensor as shown in the below Figure.1. The first row shows real face images where the second row shows fake face image from NUAA database. There's no a clear difference between real face pictures and imposter face pictures. However, there's a difference between the two rows when we look at the images from textures point of view.

To cope with this problem, we present a novel descriptor for facial image spoofing which is based on local binary pattern (LBP); the features are extracted from the local facial image regions in order to tackle the problem of detecting fake facial biometric data. In this work we use SVM as a machine learning model for real/fake face classification. Our goal is to detect the spoofed face image from texture analysis point of view.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

Figure.1: Live Face vs. Imposter Face (Row1. Live Face, Row2. Imposter Face)

II. RELATED WORK

Face recognition systems are known to respond weakly to attacks for a long time [9, 10] and are easily spoofed using a simple photograph of the enrolled person's face, which may be displayed in hard-copy or on a screen. In this short survey, we focus on methods that present counter-measures to such kind of attacks. Anti-spoofing for 2-D face recognition systems can be coarsely classified into 3 categories with respect to the clues used for attack detection: motion, texture analysis and liveness detection [11]. Li et al. [14], used a Fourier spectra to compare the hardcopies of client faces and real accesses. This method works well for down-sampled of the print-photo attack identity, but it fails for higher-quality images sometimes.

Another category of anti-spoofing methods focus on detection of a live-face specific motion on the scene, such as eye blinking, mouth movements or head movements. Examples of methods using eye-blinking detection are proposed in [19, 20]. There are a number of publications which analyze specific properties of the human head as a 3D object and its movements, like [21,22]. Both methods use optical flow field for motion estimation and report EER of 0.5% and HTER of 10% respectively. A. Anjos et al. [23] states that in the case of an attack using a photograph, there should be high correlation between the total amount of movement in the face region and the scene background. The algorithm achieves HTER of 8.98%.

LBP [17,18] has emerged as one of the most prominent texture features and a great many new variants continue to be proposed. LBP's strengths include avoiding the time consuming discrete vocabulary pre-training stage in the BoW(Bag of Words)framework, its overall computational simplicity, its monotonic illumination invariance, its flexibility, and ease of implementation.

III. SPOOFING DETECTION USING LBP

In this section, we explain our approach of anti-spoofing used to differentiate between live faces and fake ones. The block diagram of our anti-spoofing approach is as shown in Figure. 2. First, the face is detected using Viola-Jones algorithm [17] and we then applied the Active Shape Models with STASM[18] to locate landmarks. These landmarks help us to adjust and crop the faces. After that we divided the face image into 3x3 overlapping regions, and we applied LBP operator on each region. Finally, we used a non-linear SVM classifier with radial basis function kernel for determining whether the input image corresponds to a live face or not. We describe below each step in detail.

A. *Viola-Jones algorithm:* To detect the faces we used STASM. A STASM is a software package for locating landmarks using Active Shapes Models (ASMs). When we used STASM directly on large images which have small faces the system fails to detect the faces. So, Viola-Jones [13] is applied first to detect the faces and then STASM is used in detected faces to locate landmarks (Shown in Figure.3).

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

B. ***Feature extraction using LBP****:* The LBP is an image operator which transforms an image into an array or image with more detail. The basic LBP introduced by Ojala et al.[12], was based on the assumption that texture has locally two complementary aspects, a pattern and its strength. The original LBP works in a 3x3 pixel block of image. The pixels in this block are thresholded by its center pixel value, multiplied by powers of two and then summed to obtain a label for the center pixel. As the neighborhood consists of 8 pixels, a total of 2^8=256 different labels can be obtained depending on the relative gray values of the center and its neighborhood as shown in Figure.4.

The $LBP_{(P,R)}$ operator used a circular neighborhood. The notation (P, R) is generally used for pixel neighborhoods to refer to sampling points and circle of radius. So the calculation of the $LBP_{(P,R)}$ codes can be easily done. The value of the LBP code of a pixel (x_c, y_c) is given by:

$$LBP_{P,R}=\sum_{p=0}^{P-1} s(gp - gc)2^p \quad (1)$$

where$g_c$corresponds to the gray value of the center pixel(x_c, y_c), $g_p$refers to gray values of P equally spaced pixels on a circle of radius R , and s defines a thresholding function as follows:

$$s(x) = \begin{cases} 1 & if\ x \geq 0 \\ 0 & otherwise \end{cases} \quad (2)$$

C. ***Classification:***A Support Vector Machine (SVM) performs classification by finding the hyper plane that maximizes the margin between two classes. The vectors (cases) that define the hyper plane are called the support vectors. In our experiments, once the enhanced histograms are computed and reduced, we use a nonlinear SVM classifier [23] with radial basis function kernel for determining whether the input image corresponds to a live face or not. The SVM classifier is first trained using a set of positive (real faces) and negative (fake faces) samples from the dataset.

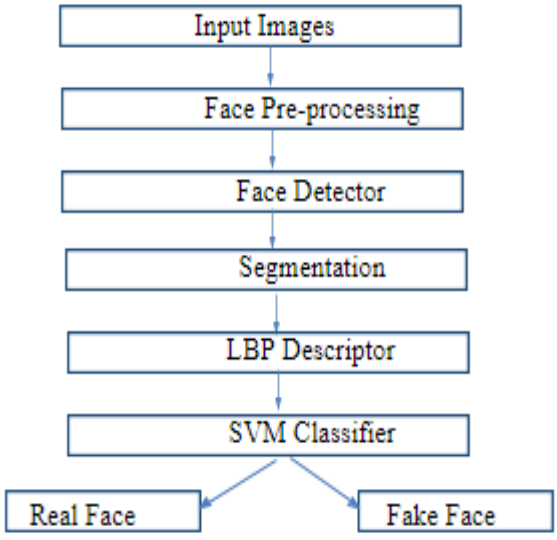

Figure.2: Steps in face spoofing.

D. ***Dataset :***The NUAA spoofing face Database [15] which plays an important role in static face liveness detection and is available to the public was published in 2010, and both the images of real client and imposter attacks are included. Each individual face image is collected in three different sessions of which each is held every two weeks and the environment and lighting conditions are different for each session. The NUAA Database uses traditional webcams whose resolution is 680×480 to obtain 15 persons images, and each person are captured almost 500 images. Only nine out of fifteen objects present in the training set under the live human circumstance and only three out of nine objects

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

present under the photo circumstance. Thus we can know that there is such a big difference between persons present in test and training sets. The training set contains 3099 images, the test set contains 2623 images, and does not overlap with the training set to form a database.

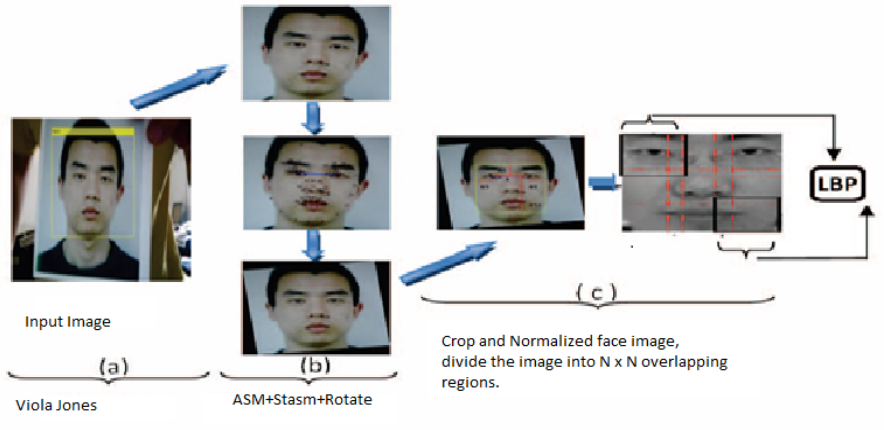

Figure.3: Face pre-processing.

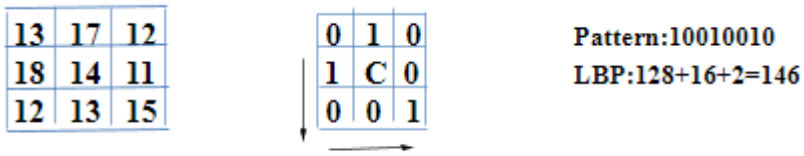

Figure.4: The basic LBP operator

IV. EXPERIMENTAL SETUP

We conducted experiments using the NUAA dataset[2]. First the image is pre-processed into gray scale. Viola-Jones is applied to detect face and it is normalized to size of 160 x 160 pixels. The normalized face is segmented into 100 blocks, each block is size of 16 x 16 pixels. Uniform Local Binary pattern (LBP) descriptor is applied to each block, extracting 59 features which is repeated for all remaining blocks to get 5900 features. This process is repeated for all the images of dataset including real and fake mages. The extracted features are collected in a file and the features are given as input to SVM classifier and trained with kernel function. During testing, the test image is also segmented as above and given as input to trained SVM classifier to decide give image is real/fake.

V. RESULTS AND DISCUSSIONS

The NUAA anti spoofing face database comprising 14 classes of real and spoof images. The original image of dataset is resized into 160x160 pixels. During training of SVM classifier 10 images were considered in each class and then tested. Later number of images were increased from to 20 and 100 in each class for training. The testing set comprising both real and spoof total of 1150 ad 1949 images respectively. For all classes, each image is divided into 100 blocks and each block is of size 16 x 16 pixels. For all images total number of LBP features extracted is 5900. It has been observed from Table I that as the number of training images in training set increases the percentage of recognition rate also increases (both for real and spoof images).

In the second experiment, number of training images remains constant with about 40 real and 40 fake faces. Each image of dataset is segmented into different block sizes, which is varying from 16 x 16 blocks to 160 x 160 blocks. For each different block size features are extracted. In 16 x 16 blocks, the LBP features extracted are 5900, which constitute very high recognition rate. The recognition rate is varying once the number features are decreased. It

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

has been observed in the Table II that, number of features increases, the recognition rate also increases. It indicates that more number of blocks/image, overall recognition rate also increases.

Sl. No.	No. of Train images	Number of test images		Number of correct recognition		Overall Recognition rate (%)
		Real	Spoof	Real	Spoof	
1	280	1150	1949	1098	1934	97.80
2	560	1150	1949	1110	1934	98.22
3	840	1150	1949	1111	1933	98.22
4	1120	1150	1949	1110	1934	98.22
5	1400	1150	1949	1107	1935	98.24
6	1680	1150	1949	1111	1935	98.28
7	1960	1150	1949	1114	1935	98.40
8	2240	1150	1949	1150	1937	99.61
9	2520	1150	1949	1150	1938	99.64
10	2800	1150	1949	1150	1944	99.83

Table I: Results of images whose Block size of 16 x 16

S.I No.	Block size	Number of Features	Number of test images		Number of correct recognition		Overall Recognition rate (%)
			Real	Spoof	Real	Spoof	
1	16 x 16	5900	1150	1949	1110	1934	98.9
2	32 x 32	1475	1150	1949	1132	1932	97.9
3	64 x 64	531	1150	1949	1126	1930	96.6
4	80 x 80	98	1150	1949	1106	1920	95.6
5	160x160	59	1150	1949	1097	1829	94.3

Table II: Results of 1100 images of different block size

VI. CONCLUSION

In this work, an approach for anti-spoofing detection using machine learning approach is presented that discriminate live faces from fake ones. An excellent description operator named Local Binary Patterns (LBP) are used to extract features from face images. The experimental results shows an encouraging recognition rate of more than 98%.

Compared with many previous methods, our proposed method is robust and non-intrusive, and user collaboration can be ignored. In addition, the computational time cost by this algorithm to recognize a single image can completely satisfy the real-time detection requirement

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

REFERENCES

1. K. Nixon, V. Aimale, and R. K. Rowe, “Spoof detection schemes” Handbook of Biometrics, 2008.
2. Joshi, T., Dey, S., Samanta, D ,“ Multimodal biometrics: state of the art in fusion techniques”, International Journal of . Biometrics Vol.1, No.4, pp. 393–417, 2009.
3. T. de Freitas Pereira, J. Komulainen, A. Anjos, J. M. De Martino,A. Hadid, M. Pietikainen, and S. Marcel, “Face liveness detection using dynamic texture,” Journal on Image and Video Processing, EURASIP ,Vol. 2, 2014.
4. S. Tirunagari, N. Poh, D. Windridge, A. Iorliam, N. Suki, and A. Ho, “ Detection of face spoofing using visual dynamics,”, in Proceedings of International conference on Information Forensics and Security, IEEE, vol. 10, no. 4, pp. 762–777, 2015.
5. J. Komulainen, A. Hadid, M. Pietikainen, A. Anjos, and S. Marcel, “Complementary countermeasures for detecting scenic face spoofing attacks”, in Proceedings of International Conference on Biometrics, Madrid, Spain, pp. 1-7, Jun. 2013.
6. J. Yang, Z. Lei, D. Yi, and S. Li, “Person-specific face antispoofing with subject domain adaptation,” in Proceedings of International conference on Information Forensics and Security, IEEE, vol. 10, no. 4, pp. 797–809, 2015.
7. J. Mtt, A. Hadid, and M. Pietikinen, “Face spoofing detection from single images using micro-texture analysis” ,in Proceedings of International Joint Conference on Biometrics (IJCB), pp. 1–7, 2011.
8. G. Pan, Z. Wu, and L. Sun, “Recent Advances in Face Recognition, chapter Liveness detection for face recognition”, InTech, pp. 235-252, 2008.
9. L. Thalheim, J. Krissler, and P.-M. Ziegler, "Body check: Biometric access protection devices and their programs put to the test", Heise Online, 2002.
10. N. M. Duc and B. Q. Minh, "Your face is not your password", in Proceedings ofBlack Hat Conference, 2009.
11. M. M. Chakka et al., “Competition on counter measures to 2-d facial attacks,” in Proceedings ofInternational Joint Conference on Biometrics, 2011.
12. T. Ojala, M. Pietikainen, and T. Maenpaa, “Multi-resolution gray-scale and rotation invariant texture classification with local binary patterns” in proceedings of Pattern Analysis and Machine Intelligence, IEEE, vol. 24, no. 7, pp. 971–987, 2002.
13. P. Viola and M. Jones, “Rapid object detection using a boosted cascade of simple features”, in Proceedings of Computer Vision and Pattern Recognition, Vol. 1, pp. 1-9. 2001.
14. J. Li, Y. Wang, T. Tan, and A. K. Jain, “Live face detection based on the analysis of Fourier spectra”, in Proceedings of Defense and Security. International Society for Optics and Photonics, pp. 296–303, 2004.
15. Tan X, Li Y, Liu J, et al. ,“Face liveness detection from a single image with sparse low rank bilinear discriminative model”, in Proceedings of European Conference on Computer Vision(ECCV), Springer-Verlag, pp. 504-517, 2010.
16. Parveen S, Ahmad S, Abbas N, et al. “Face Liveness Detection Using Dynamic Local Ternary Pattern (DLTP)”, Computers: Open Access Journal, Vol. 5, No.2, pp. 1-15, 2016.
17. Ojala T, Pietikainen M, Maenppaa T, ”Multiresolution gray-scale and rotation invariant texture classification with local binary patterns”, in Proceedings of Pattern Analysis Machine Intelligence. Vol. 24, No. 7, pp. 971–987, 2002.
18. Pietikainen, M, Hadid, A., Zhao, G., Ahonen, T,” Computer vision using local binary patterns”, Springer, London, UK, 2011.
19. G. Pan, Z. Wu, and L. Sun, “Liveness detection for face recognition: Recent Advances in Face Recognition”, Vienna, Austria, 2008.
20. H. K. Jee, S. U.Jung, and J. H. Yoo, “Liveness detection for embedded face recognition system”, International journal of computer and information Engineering, Vol. 2, No.6, 2008.
21. K. Kollreider, H. Fronthaler, and J. Bigun, “Non-intrusive liveness detection by face images”, in Journal of Image and Vision Computing, ELSEVIER, vol. 27, no. 3, 2009.
22. W. Bao et al. “A liveness detection method for face recognition based on optical flow field”, in Proceedings of International Conference on Image Analysis and Signal Processing, IEEE, 2009.
23. Anjos and S. Marcel, “Counter-measures to photo attacks in face recognition: a public database and a baseline” in Proceedings of International Joint Conference on Biometrics, pp. 1-7, 2011.
24. Y.Ma and X.Ding, “Face detection based on hierarchical Support Vector Machines”, in Proceedings of ICPR, pp. 222–225, 2002.
25. V. N. Vapnik, “The Nature of Statistical Learning Theory”, Springer, 1995.
26. J. Platt, “Probabilistic outputs for SVMs and comparisons to regularized likelihood methods. In Advances in Large Margin Classifiers”, MIT Press, 1999.
27. E. Boser, I. M. Guyon, and V. N. Vapnik,” A training algorithm for optimal margin classifiers”, In D. Haussler, editor, 5th Annual ACM Workshop on COLT, ,Pittsburgh, PA, ACM Press, pp. 144-152, 1992.
28. P. Viola and M. Jones, “Rapid object detection using a boosted cascade of simple features,” in Proceedings of Computer Vision and Pattern Recognition, CVPR, vol. 1., IEEE, pp. I–511, 2001.
29. S. Milborrow and F. Nicolls, “Locating facial features with an extended active shape model,” in Proceedings of Computer Vision–ECCV 2008. Springer, pp. 504–513, 2008.