ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

FACE SPOOF DETECTION USING EFFICIENT LOCAL BINARY PATTERN(ELBP)

ChithaBargavi ,Divyabharathi.D , FarhinShahira S.A
4th Year ECE, Magna college of engineering
bargavi.chitha@gmail.com,farhin221@gmail.com
MsShwedha.R (M.E. Applied Electronics) Asst. Professor,

Abstract—Automatic face recognition is now widely used inapplications ranging from de-duplication of identity to authenticationof mobile payment. This popularity of face recognitionhas raised concerns about face spoof attacks (also known asbiometric sensor presentation attacks), where a photo or videoof an authorized person's face could be used to gain access tofacilities or services. While a number of face spoof detectiontechniques have been proposed, their generalization ability hasnot been adequately addressed. The proposed approach analyzesthe texture of the facial images using efficient localbinary patterns (ELBP). Compared to many previous works,our proposed approach is robust, computationally fast anddoes not require user-cooperation. In addition, the texturefeatures that are used for spoofing detection can alsobe used for face recognition. This provides a unique featurespace for coupling spoofing detection and face recognition.Extensive experimental analysis on a publicly availabledatabase showed excellent results compared to existingworks.

1. INTRODUCTION

AS a convenient user authentication technique, automaticface recognition has attracted increasing attention in variousaccess control applications, especially for mobile phoneunlocking. With the release of face unlocking functionalityin the Android mobile operating system, face recognitionbecomes another biometric authentication technique for mobilephones, similar to fingerprint authentication (Touch ID)in the iOS system. Unlike fingerprint authentication, facerecognition does not require any additional sensor since allsmart phones come equipped with a front facing camera.However, similar to other biometric modalities weneed to address concerns about face spoof attacks on facerecognition systems, particularly in unconstrained sensing anduncooperative subject scenarios .

It is relatively easier to acquire a person's face image orvideo (e.g., with a digital camera or from social media) thanit is to acquire other biometric traits such as fingerprint,palm print, and iris. Further, the cost of launching a facespoof attack, such as a printed photo, displayed photo, orreplayed video is relatively low (see Fig1).

Fig. A genuine face image (a) of a subject in the Idiap databases and three examples of spoofs of the same subject using a (b) printed photo, (c) displayed photo (on a tablet screen), and (d) 3D face mask.

A spoofing attack occurs when a person tries to masquerade as someone else by falsifying data and thereby gainingillegitimate access and advantages. For instance, one canspoof a face recognition system by presenting a photograph,a video, a mask or a 3D model of a targeted person in frontof the camera. While one can also use make-up or plasticsurgery as other means of spoofing, photographs are probablythe most common sources of spoofing attacks becauseone can easily download and capture

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

facial images.Inspired by image quality assessment, characterizationof printing artifacts and by differences in light reflection, wepropose to approach the problem of spoofing detection fromtexture analysis point of view. Indeed, face prints usuallycontain printing quality defects that can be well detected usingmicro-texture patterns. Furthermore, human faces andprints reflect light in different ways because a human face isa complex non rigid 3D object whereas a photograph can beseen as a planar rigid object. This may cause different specularreflections and shades. The surface properties of realfaces and prints, e.g. pigments, are also different. Hence, we present a novel approach based on analyzing facial imagetextures for detecting whether there is a live person or aface print in front of the camera. Compared to many previousworks, our proposed approach is robust, computationally fast and does not require user-cooperation. In addition,the texture features that are used for spoofing detectioncan also be used for face recognition. This providesa unique feature space for coupling spoofing detection andface recognition.The proposed approach analyzes the texture of the facialimages using efficient local binary patterns (ELBP)and encodes the micro-texture patterns into an enhancedfeature histogram . The results are then fed to a linear square supportvector machine (SVM) classifier which determineswhether there is a live person in front of the cameraor not. Extensive experiments on a publicly availabledatabase (NUAA Photograph Imposter Database containingseveral real and fake faces showed excellent resultscompared to previous works.

2. RELATED WORK

Without anti-spoofing measures most of the state-of-theartfacial biometric systems are basically vulnerable to attacks. Even a simple photograph of the enrolled person's face, displayed as a hard-copy or on a screen, will fool thesystem. Short surveys of previous attempts against spoofingattacks can be found in . Typical countermeasureagainst spoofing is liveness detection that aims at detectingphysiological signs of life such as eye blinking, facialexpression changes, mouth movements etc. For instance,Pan*et al.* exploited the observation that humans blink once every 2-4 seconds and proposed an eye blink-basedanti-spoofing method. It uses Conditional Random Fieldframework to model and detect eye-blinking. Kollreider*etal.*presented an optical-flow based method to captureand track the subtle movements of different facial parts, assumingthat facial parts in real faces move differently than on photographs. In another work ,Bao*et al.* also usedoptical flow for motion estimation for detecting attacks producedwith planar media such as prints or screens. Experimentson a private database showed a 6% false-alarmagainst about 14% false-acceptance.Another category of anti-spoofing methods are based onthe analysis of skin properties such as skin texture and skinreflectance. For instance, Li *et al.* described a methodfor detecting print-attack face spoofing. The method isbased on the analysis of 2D Fourier spectra, assuming that photographs are usually smaller in size and they would containfewer high frequency components compared to realfaces. Such an approach may work well for down-sampledphotos but is likely to fail for higher-quality images. Thedatabase used in the experiments is unfortunately not publiclyavailable.In a recent work, Tan *et al.* considered the Lambertianreflectance to discriminate between the 2D images offace prints and 3D live faces. The method extracts latent reflectancefeatures using a variationalretinex-based methodand difference-of-Gaussians (DoG) based approach. Thefeatures are then used for classification. The authors reportedpromising results on a database composed of realaccessesand attacks to 15 subjects using both photo-qualityand laser-quality prints. The database, the NUAA PhotographImposter Database, is made publically available. Thisprovides a valuable resource for fairly comparing the resultsof different methods. Hence, our current work also considersthis database.Other countermeasures against face spoofing attacks includemulti-modal analysis and multi-spectral methods. Asystem combining face recognition with other biometricmodalities such as gait and speech is indeed intrinsicallymore difficult to spoof than uni-modal systems. Multispectralimages can also be used for analysing the reflectanceof object surfaces and thus discriminating livefaces from fake ones .It appears that most of the existing methods for spoofingdetection are either very complex (and hence not verypractical for real-world face biometric systems requiringfast processing) or using non-conventional imaging systems(e.g. multi spectral imaging) and devices (e.g. thermal cameras).We therefore propose in this work a computationallyvery fast approach based on highly discriminative texturefeatures, using conventional images and requiringno user-cooperation.

3. SPOOFING DETECTION USING TEXTURE ANALYSIS:

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

Face images captured from printed photos may visuallylook very similar to the images captured from live face. Consequently, all these images would be largelyoverlapping in the original input space. Therefore a suitablefeature space is needed for separating the two classes(live vs. fake face images). The main issue is how to derivesuch a feature space. Our method aims at learning thefine differences between the images of real face and those of face prints, and then designing a feature space which emphasizesthose differences. A close look at the differences between real faces andface prints reveals that human faces and prints reflect lightin different ways because a human face is a complex nonrigid 3D object whereas a photograph can be seen as a planarrigid object. This may cause different specular reflectionsand shades. The surface properties of real faces andprints, e.g. pigments, are also different. In addition, faceprints usually contain printing quality defects that can be detectedwith micro-texture patterns. Furthermore, spoof attackswhen executed with face prints tend to engender someoverall image blur.Inspired by the observations above, and particularly byimage quality assessment and characterization of printingartifacts, we derive a facial representation (or a featurespace) that is able to capture typical characteristics of realand fake face images. Hence, the key idea of our approchis emphasizing the micro-texture differences in the featurespace.Our method adopts the local binary patterns , a powerfultexture operator, for describing not only the microtexturesbut also their spatial information. The vectors inthe feature space are then fed to an SVM classifier whichdetermines whether the micro-texture patterns characterizea live person or a fake image. Fig. 2 shows examples of twoimages (a live face and a face print) in the original spaceand the corresponding LBP images (using basic LBP as featurespace). We can notice that the printed photo looks quitesimilar to the image of the live face whereas the LBP imagesdepict some differences. We describe below our enhancedLBP feature space.

Figure3 Examples of two images (a live face and a face print) in the original space and the corresponding LBP images using basic LBP as a feature space.

3.1. Discriminative Feature Space Using LBP

The LBP texture analysis operator, introduced by Ojalaet al. , is defined as a gray-scale invariant texture measure,derived from a general definition of texture in a localneighborhood. It is a powerful means of texture descriptionand among its properties in real-world applications areits discriminative power, computational simplicity and toleranceagainst monotonic gray-scale changes.The original LBP operator forms labels for the imagepixels by thresholding the 3×3 neighborhood of each pixelwith the center value and considering the result as a binarynumber. Fig. 3 shows an example of an LBP calculation.

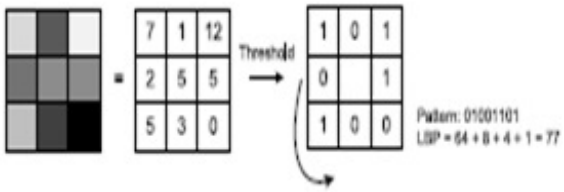


Figure 2The basic LBP operator.

LBP as a feature space.

The histogram of these 28 = 256 different labels can thenbe used as a texture descriptor.The operator has been extended to use neighborhoods ofdifferent sizes. Using a circular neighborhood and bilinearlyinterpolating values at non-integer pixel coordinatesallow any radius and number of pixels in the neighborhood.The notation (P,R) is generally used for pixel neighborhoodsto refer to P sampling points on a circle of radius R.The calculation of the LBP codes can be easily done in asingle scan through the image. The value of the LBP codeof a pixel (xc, yc) is given by:

$$\mathrm{LBP}_{P,R} = \sum_{p=0}^{P-1} s(g_p - g_c)2^p,$$

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

wheregc corresponds to the gray value of the center pixel(xc, yc), gp refers to gray values of P equally spaced pixelson a circle of radius R, and s defines a thresholding functionas follows:

$$s(x) = \begin{cases} 1, & \text{if } x \geq 0; \\ 0, & \text{otherwise.} \end{cases}$$

Another extension to the original operator is the definitionof so called uniform patterns. This extension was inspiredby the fact that some binary patterns occur more commonlyin texture images than others. A local binary pattern iscalled uniform if the binary pattern contains at most twobitwise transitions from 0 to 1 or vice versa when the bitpattern is traversed circularly. In the computation of theLBP labels, uniform patterns are used so that there is a separatelabel for each uniform pattern and all the non-uniformpatterns are labeled with a single label. This yields to thefollowing notation for the LBP operator: $LBP^{u2}_{P,R.}$ The subscriptrepresents using the operator in a (P,R) neighborhood.Superscript u2 stands for using only uniform patternsand labeling all remaining patterns with a single labelEach LBP label (or code) can be regarded as a microtexton.Local primitives which are codified by these labelsinclude different types of curved edges, spots, flat areas etc.The occurrences of the LBP codes in the image are usuallycollected into a histogram. The classification can be thenperformed by computing histogram similarities. For an efficientrepresentation, facial images are first divided into severallocal regions from which LBP histograms are extractedand concatenated into an enhanced feature histogram. Sucha representation is shown to be very adequate for face recognition. Our investigations have shown, however, thatmicro-texture details that are needed for discriminating areal human face from fake ones, can best be detected usinga combination of different LBP operators. Therefore, tobetter capture the differences between real human faces andfake ones, we derive an enhanced facial representation usingmulti-scale LBP operators. The proposed representation
is depicted in Fig. 4.

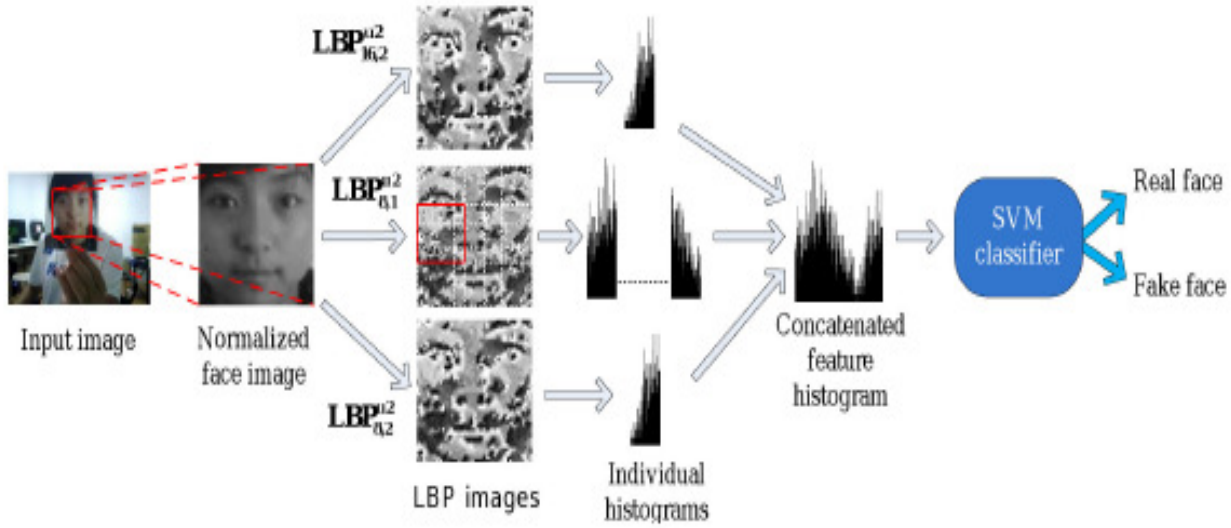


figure:4 spoof detection using efficiect local binary pattern

As illustrated in Fig. 4, our proposed representation computesLBP features from 3 × 3 overlapping regions to capturethe spatial information and enhances the holistic descriptionby including global LBP histograms computedover the whole face image. This is done as follows: theface is first detected, cropped and normalized into a 64×64pixel image. Then, we apply $LBP^{u2}_{8,1}$ operator on the normalizedface image and divide the resulting LBP face imageinto 3 × 3 overlapping regions (with an overlapping size of14 pixels). The local 59-bin histograms from each regionare computed and collected into a single 531-bin histogram.Then, we compute two other histograms from the wholeface image using $LBP^{u2}_{8,2}$ and $LBP^{u2}_{16,2}$ operators, yielding59-bin and 243-bin histograms that are added to the 531-binhistogram previously computed. Hence,

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

the length of the finalenhanced feature histogram is 833 (i.e. 531+59+243).

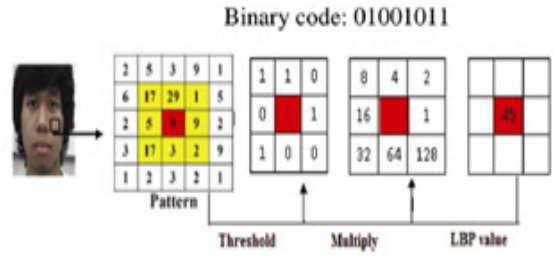
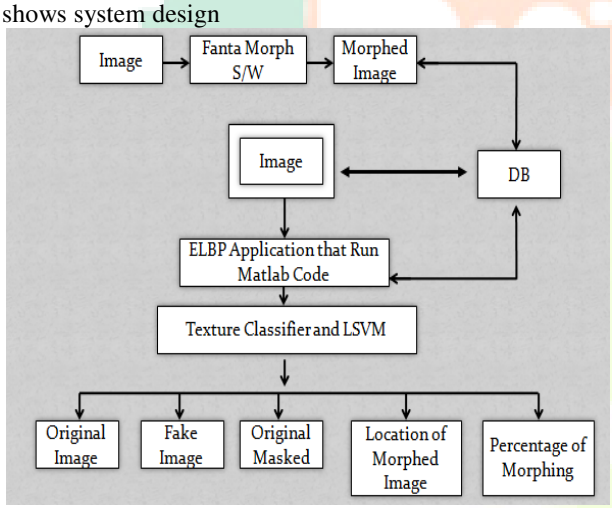


Figure 5 Example of LBP calculation.

3.2. Classification

Once the enhanced histograms are computed, we use a linear SVM classifier with radial basis function kernelfor determining whether the input image correspondsto a live face or not. The SVM classifier is firsttrained using a set of positive (real faces) and negative (fakefaces) samples. The following figure shows system design



4. Conclusion

Current face biometric systems are very vulnerable tospoofing attacks and photographs are probably the mostcommon sources of spoofing attacks. Inspired by imagequality assessment, characterization of printing artifacts andby differences in light reflection, we proposed an approachfor spoofing detection based on learning the micro-texturepatterns that discriminate live face images from fake ones.Indeed, face prints usually contain printing quality defectsthat can be well detected using micro-texture patterns. Furthermore,human faces and prints reflect light in differentways because a human face is a complex non rigid 3D objectwhereas a photograph can be seen as a planar rigidobject. This may cause different specular reflections andshades. The surface properties of real faces and prints,e.g. pigments, are also different. Our proposed approachused efficient local binary patterns (ELBP) to encode themicro-texture patterns into an enhanced feature histogram.

The results are then fed to a support vector machine classifierwhich determines whether there is a live person infront of the camera or not. Extensive experiments on apublicly available database containing several real and fakefaces showed excellent results. Compared to many previousworks, our proposed approach is robust, computationallyfast and does not require user-cooperation. In addition, thetexture features that are used for spoofing detection can alsobe used for face recognition. This provides a unique featurespace for coupling spoofing detection and face recognition.We have also evaluated our approach in a real world application(face based access control) by performing various2D face spoofing attacks using good quality face prints andalso high resolution displays. The results were promising.We believe that our approach can also be extended to detectspoofing attacks using masks or 3D models of the face becauseskin has a very particular texture with, for example,pores whereas fake faces have seldom such a level of detail.

5.REFERENCE:

- K. Nixon, V. Aimale, and R. Rowe, "Spoof detection schemes,"in*Handbook of Biometrics, A. Jain, P. Flynn, and A. Ross, Eds.*New York, NY, USA: Springer-Verlag, 2008, pp. 403–423.
- B. Biggio, Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, "Security evaluation of biometric authentication systems under real spoofing attacks," *IET Biometrics, vol. 1, no. 1, pp. 11–24, Mar. 2012.*
- J. Bai, T.-T. Ng, X. Gao, and Y.-Q. Shi, "Is physics-based liveness detection truly possible with a single image?" in *Proc. IEEE ISCAS,* May/Jun. 2010, pp. 3425–3428.
- J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

fourier spectra," *Proc. SPIE, vol. 5404, pp. 296–303,* Aug. 2004.

- J. Maatta, A. Hadid, and M. Pietikainen, "Face spoofing detection from single images using micro-texture analysis," in *Proc. IEEE IJCB,* Oct. 2011, pp. 1–7.