Image Distortion Measures for Face Spoof Detection

Sannidhi Yatin Dixit
Department of Electronics and Telecommunication
K. J. Somaiya College of Engineering, Mumbai, India
sannidhidixit@gmail.com

Abstract - Automatic face recognition is widely used in today's world due to the de-duplication of the user. This has raised the concerns about the face spoof attacks where the authorized access is given to illegal user to the service or the facility where a person's photo or video is used for the same. Various face spoof detection algorithms have been proposed and implemented whose generalized ability has not been adequately addressed. The image distortion analysis is an efficient and robust method for face spoof detection. IDA feature vector extracts four features (specular reflection, blurriness, color diversity and chromatic moment feature). A classifier that consists of multiple SVM is trained for different faces and they are then used to classify between the genuine and spoofed faces. MSU database is used that has the pictures and videos clicked using Nexus 5 and MacBook Air and the types of spoofing attacks it covers are printed photo attack and replayed video.

Index words: Face recognition, spoof detection, image distortion analysis, feature

I. INTRODUCTION

"Fingerprints can't lie but liars can make fingerprints" is an old quoted paraphrase by Mark Twain which has been proven right in many occasions by now. The case is not true just for the fingerprints but also for other biometric traits such as face, iris, voice and gait.

Researchers from many different fields such as image processing, computer vision or pattern recognition have applied new techniques in each of these areas to improve the performance of biometric systems leading to the biometric paradigm, "Forget about keys and passwords, be your own key". It is a very well accepted fact that, with the development of the biometric systems which keeps growing year after year in different environments such as airports, laptops and mobile phones, the users are also becoming more and more familiar with their use in everyday life and hence the security weaknesses are better known to the general public. Nowadays, tutorials are easily available online which give detailed guidance on how to create fake masks, fingerprints or irises that may be used to fool biometric systems. Hence, we need to use the biometric traits of the user, which are extremely specific about the user.

In recent years, there has been an increasing interest on the evaluation of biometric systems security, which has led to creation of many and very diverse initiatives focused in this field. Among the different vulnerabilities analysed, intensive research efforts have been focused on the study of direct or spoofing attacks. In spoofing attacks, the intruders use some type of synthetically produced artefact (eg. face mask or a printed image) or try to mimic the behaviour of the original or a genuine user, to access the biometric system through fraud. In this way, spoofing takes place easily taking the advantage of the fact that our face, iris, voice and other data is publically available. Hence, the biggest disadvantage of biometrics is that the biometric traits are not secrets. Hence, spoofing is very dangerous because it transforms every user into a potential user.

Face anti-spoofing have the following challenges [1]:

(i) Non-invasive: these techniques should in no case be harmful or require an excessive contact with the user.

(ii) User friendly: users should not be reluctant to interact with them.

(iii) Fast: results should be generated in reduced lapse of time as users' interaction with the sensor should be kept as short as possible

(iv) Low-cost: wide use cannot be expected if the cost is excessively high

(v) Performance: in addition to a good fake decision rate, the protection scheme should not degrade the recognition performance of the biometric system.

Face anti-spoofing techniques are mainly classified into hardware and software approaches where the hardware approach needs an additional hardware to detect the illegal access. They analyze different score fusion techniques for the protection and authentication modules under a three-case classification scenario: clients, impostors and spoofing attacks. The software approaches are the techniques which do not require an additional hardware to detect spoofing.

Robustness and generalization ability, real time response and usability are the factors on which the software algorithms are classified. As per these factors the face spoof detection methods can be classified into the following four groups (i) motion based methods (ii) texture based methods (iii) methods based on image quality and (iv) methods based on other cues.

Motion Based Methods: The anti-spoofing techniques in this approach rely on the detection of motion over a face video sequence. This approach is based on trajectory analysis of specific face segments. Such dynamic features reveal valuable information to discriminate between real and spoofed static copies. This method is based on eye blink, mouth movement and head rotation. Since motion is relative to video frames this method has good generalization ability as compared to the texture methods. The facial motion frequency is limited which acts as a major drawback for this method and thus leading to longer time duration for identifying face spoof detection.

Texture Based Methods: Instead of the printed attacks and the replayed video attacks, this method extracts image artifacts in the images which are spoofed. Natural surfaces usually

exhibit some repetitive intensity variations or patterns that are generally referred to as texture. Analysis of texture information is important in machine vision. The texture features like linear binary pattern (LBP), Local ternary pattern (LTP), histogram of oriented gradients (HOG), difference of Gaussian (DoG), Lambertian model, co-occurrence of Adjacent local binary patterns (CoALBP), image block difference, local phase quantization (LPQ), scale invariant descriptor (SID), Moiré pattern, Radon transforms,etc are skilled to differentiate between spoofed images and genuine faces. The texture based methods are static methods in other words they need only a single image to detect a spoof though the generalization ability of these methods are poor. Since the texture methods use a single image, their computational ability is fast.

Methods Based on Image Quality: In this method, four features are used for detecting liveliness of the object. Their computational time is fast and they have a good generalization ability. The computational complexity of this method is low. The image quality methods include four methods namely blurriness, specular reflection, color diversity and chromatic moment feature [2].

Methods Based on Other Cues: These methods have an additional hardware requirements on the system and hence the application range is limited. While using 3D cues, the spoof response obtained takes time but this system is very robust. Upper body detection and the iterative closest point methods come under this method.

II. Features Of Image Distortion Analysis

In mobile applications and other such applications where the decision needs to be quick whether the user is an authorized user or not, the number of frames used should be less and preferable an algorithm should be used such that a single image suffices.

The proposed algorithm for the image distortion method is as shown below.

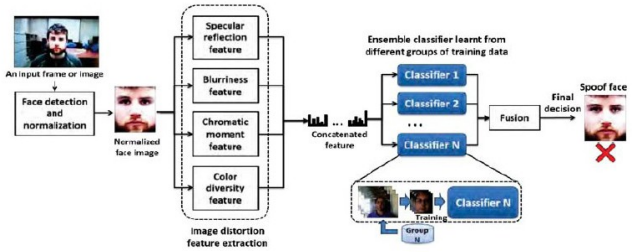

Figure 1 : IDA algorithm

The input frame of an image is first normalized. The image thus used for finding the features may be cropped into just the face of the person rather than using the entire image for further analysis. This image is then given to the IDA features like blurriness, specular reflection, chromatic moment and colour diversity. A concatenated feature is histogram is obtained from these features and then this is given to various classifiers and the decision is made [2].

The major distortions in the spoofed image includes the image blurriness due to the defocusing of the camera, the image chromaticity and contrast distortion arising due to imperfect color rendering of the display LED screen or the printer, the specular reflection from the printer or the display screen and the color diversity distortion due to limited color resolution of the printer and the LCD screen.

Other distortions are the geometric distortions and artificial texture patterns but these are illumination and camera dependent. Hence, focus is on the four basic sources of image distortion for detecting spoof.

A. Blurriness

In today's world, with the advancement in technologies, the cameras and the mobile phones give the best quality of images which leads to image correction algorithms to eliminate noise or compression artifacts. But when the corrections are made using the low pass filters, the high frequency content is lost too along with the smooth artifacts and thus leads to blurriness. Since blur is caused by the loss of high frequency content, it can be reproduced with a low pass filter.

When the original image is blurred with a low pass filter and the blurred picture is re-blurred with the same low pass filter, a high difference is observed in the loss of details between the original image and the first blurred image and a slight difference between the two blurred images.

As the number of times the image is re-blurred, the neighbouring pixels converge to the same gray level faster [3]. For a sharp picture, they gray levels of the neighbouring pixels will change with a great difference while if a gray image is blurred, the gray levels of the neighbouring pixels will still change but to a smaller extent in comparison.

Figure 2 : Original Image, Blurred image and re-blurred image

If a small blurred part is covered with a homogeneous area, the picture is apparent as a non-sharp picture even if only a small portion of the picture is blurred. Hence we take only the pixels which have changed after the blurring step.

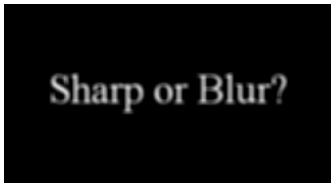

Figure 3: Blurred text over a flat area

The algorithm used to detect spoof using blurriness is as explained below with the assumption that the sharpness of the image is enclosed in the gray component. Let F be the luminance component of the image of an m x n pixel size frame. To calculate approximately the blur annoyance of F the

first step consists in blurred it in order to obtain a blurred image B. Horizontal and vertical strong low pass filters are chosen to model the blur effect and we obtain B_{Ver} and B_{Hor} given by the following equations.

$$h_V = \frac{1}{9} X [1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1]$$
$$h_h = transpose(h_v) = hv'$$
$$B_{Ver} = h_V * F \quad (1)$$
$$B_{Hor} = h_h * F$$

The absolute difference image are obtained by studying the variations of the neighboring pixels.
They are:

$$D\_F_{Ver}(i,j) = Abs(F(i,j) - F(i-1,j)) \quad for\ i=1\ to\ m-1;\ j=0\ to\ n-1$$
$$D\_F_{Hor}(i,j) = Abs(F(i,j) - F(i,j-1)) \quad for\ j=1\ to\ n-1;\ i=0\ to\ m-1 \quad (2)$$
$$D\_B_{Ver}(i,j) = Abs(B_{Ver}(i,j) - B_{Ver}(i-1,j)) \quad for\ i=1\ to\ m-1;\ j=0\ to\ n-1$$
$$D\_B_{Hor}(i,j) = Abs(B_{Hor}(i,j) - B_{Hor}(i,j-1)) \quad for\ j=1\ to\ n-1;\ i=0\ to\ m-1$$

If the variation of the neighboring pixels after the blurring step is high, the initial image was sharp while the initial image is blur if the variation is slight.

$$V_{Ver} = Max(0, D\_F_{Ver}(i,j) - D\_B_{Ver}(i,j)) \quad for\ i=1\ to\ m-1,\ j=1\ to\ n-1$$
$$V_{Hor} = Max(0, D\_F_{Hor}(i,j) - D\_B_{Hor}(i,j)) \quad for\ i=1\ to\ m-1,\ j=1\ to\ n-1 \quad (3)$$

For comparing the variations from the initial picture, the sum of coefficients of D_F_{Ver}, D_F_{Hor}, D_V_{Ver} and D_V_{Hor} as follows:

$$s\_F_{Ver} = \sum_{i,j=1}^{m-1,n-1} D\_F_{Ver}(i,j)$$
$$s\_F_{Hor} = \sum_{i,j=1}^{m-1,n-1} D\_F_{Hor}(i,j)$$
$$s\_F_{Ver} = \sum_{i,j=1}^{m-1,n-1} D\_V_{Ver}(i,j) \quad (4)$$
$$s\_F_{Hor} = \sum_{i,j=1}^{m-1,n-1} D\_V_{Ver}(i,j)$$

The result needs to be normalized within the range of 0 to 1.

$$b\_F_{Ver} = \frac{s\_FVer - s\_VVer}{s\_FVer}$$
$$b\_F_{Hor} = \frac{s\_FHor - s\_VHor}{s\_FHor} \quad (5)$$

Figure 4 : Flow Chart for Blur estimation

Finally the blur value is selected using,

$$blur\_F = Max(b\_FVer\ ,\ b\_FHor) \quad (6)$$

The flowchart for the above method is summarized as follows where 0 is the best quality and 1 is the worst quality in terms of the blur perspective.

B. Chromatic Moment Features

The digital images can be classified into photographs and graphics where the former are obtained using cameras and scanners and the latter using computers. The three major differences between photographs and graphics are (i) Graphics are composed of a single color with several regions while the photographs rarely have a single colored region. (ii) Photographs are taken from cameras which portray the objects in the real world. Because of the noise in the generation of photographs and the texture of the objects, the texture information of the photographs is different from that of the graphics. (iii) Highly saturated colors tend to appear more in the graphics as compared to the photographs.

Graphics have a set of colors that are larger in proportion than the photographs thus leading to the color difference being different in graphics and the photographs [4]. This color distribution is measured using the colored histogram having high dimension for color histogram. Hence, the chromatic moment feature is used because it also produces the compact indices and characterizes the color distribution.

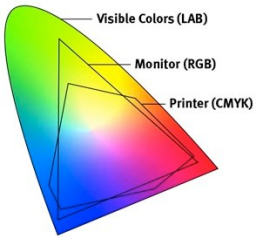

Figure 5: Color gamut of monitor and printer as compared to visible colors

The color distribution of the recaptured face images and the genuine face differ and this helps in identifying the spoof detection. This difference in the color representation is because of the imperfection color reproduction property and the display media. To implement this method, the first step is to convert the RGB color space to HSV color space. We generate a gray level vector and initialize a general histogram. We then calculate the mean, variance and skewness for each of the three channels namely H, S and V. Mean is the central value of the set. Variance is the average of the squared differences from the mean. Variance decides on how far the data is spread out from the mean. Skewness represents an imbalance and asymmetry from the mean of a data distribution. A skewed data can be either positive or negative. A positive skewed data means that the extreme data results are larger and the negative skewed means that the extremes are smaller.

HSV is the most common color space and is a cylindrical coordinate representation of points in RGB color model. HSV stands for hue, saturation and value. Hues are described by a number that specifies the position of the corresponding pure color as a fraction between 0 and 1. 0 refers to red, 1/6 is yellow and 1/3 is green. Saturation of a color described how white the color is. A pure red is fully saturated with a saturation of 1 while tints of red have saturation of 0. Value is also called as the lightness of the color which describes how dark the color is. A value of 0 is black with increasing lightness moving away from black.

III. Implementation

MSU Mobile Face Spoof Detection (MFSD) is used for face spoof detection which consists of various videos of around 50 clients. This dataset is produced at the Michigan State University which has both the real or the genuine faces and the spoofed faces. This dataset is produced using Nexus 5 and MacBook Air. As compared to other databases, MSU dataset has the following desirable properties:

- Mobile phone is used to capture both genuine faces and spoofed attacks, simulating the application of mobile phone unlocks.
- The printed photos used for attacks are generated by printing on a large sized paper. Hence the printed photos of the MSU database have much better quality than the printed photos like the CASIA database.

IV. Results

Table 1 shows the blur value for the real faces of different clients while Table 2 gives the blur values for spoofed faces of a certain set of clients.

TABLE I
Blur Values for Real Face

Scene Number	Blur Value
Client 1 (Android)	0.5004
Client 2 (Android)	0.5150
Client 24 (Android)	0.4797
Client 26 (Android)	0.3871
Client 30 (Android)	0.4617
Client 30 (Laptop)	0.5753
Client 42 (Android)	0.5547
Client 42 (Laptop)	0.5740

TABLE II
Blur Values for Attack Image

Scene Number	Blur Value
Client 23 (Printed)	0.4426
Client 24 (iPad)	0.4544
Client 24 (iPhone)	0.5919
Client 24 (Printed)	0.5029
Client 30 (iPhone)	0.4973
Client 32 (Printed)	0.5756
Client 42 (Android Printed)	0.5995
Client 42 (Laptop iPhone)	0.5785
Client 42 (Laptop Printed)	0.4724

Table 3 shows the chromatic moment values for the real faces of different clients while Table 4 gives the chromatic moment values for spoofed faces of a certain set of clients. Chromatic values are calculated with the mean, variance and skewness of each of the channel namely Hue, Saturation and value. In this method, the RGB color spaces are converted into H, S and V channels. This method gives better results as compared to the color histograms.

TABLE III
Chromatic Moment for Real Faces

Scene Number	Hue			Saturation			Value		
	Mean	Variance	Skewness	Mean	Variance	Skewness	Mean	Variance	Skewness
Client 1 (Android)	1.9240	0.6902	2.2972	4.0856	2.8799	0.6785	4.6857	3.7992	-0.0706
Client 2 (Android)	1.9151	0.4974	1.4075	5.2867	4.1271	-0.0873	3.6539	3.7030	0.2592
Client 24 (Android)	1.9400	0.2397	3.4711	4.4708	3.4559	0.5546	6.4877	3.6618	-1.1715
Client 26 (Android)	1.2965	0.2086	0.8910	4.8705	2.1961	0.1629	5.3367	2.9862	-0.3110
Client 30 (Android)	1.0942	0.0853	2.7783	5.3574	3.0165	0.2809	4.9861	4.3735	-0.0049
Client 30 (Laptop)	2.1789	5.0212	1.9827	3.8393	1.6964	0.8205	3.5995	2.3000	0.2736
Client 42 (Android)	1.2393	0.1820	1.2220	4.4292	2.7471	0.8387	5.8201	3.6869	-0.5538
Client 42 (Laptop)	2.0161	4.4902	2.2322	3.5949	0.9148	0.9408	3.9059	1.7001	0.1283

TABLE IV
Chromatic Moment for Attack Image

Scene Number	Hue			Saturation			Value		
	Mean	Variance	Skewness	Mean	Variance	Skewness	Mean	Variance	Skewness
Client 23 (Printed)	1.4042	0.2408	0.3906	3.3318	1.0190	0.8092	5.9269	2.0669	-0.1359
Client 24 (iPad)	1.2898	0.6568	5.9995	3.8306	6.0260	0.3942	6.5705	3.3283	-1.2973
Client 24 (iPhone)	1.7042	1.6520	2.4492	3.2595	4.4613	0.9402	6.1155	5.2588	-1.0373
Client 24 (Printed)	2.8235	4.0856	1.2892	2.4173	0.9331	0.9286	4.4117	1.8420	0.2793
Client 30 (Laptop iPhone)	2.4070	2.9546	1.4833	3.3921	4.6699	0.7930	4.6493	5.5671	-0.1514
Client 32 (Printed)	3.5332	6.3320	0.5947	3.1501	1.1171	0.5132	3.6415	2.3507	0.4184
Client 42 (Android Printed)	1.5770	2.9902	3.3221	3.0488	0.2666	0.2365	5.8500	1.0498	-0.1808
Client 42 (iPhone)	1.9756	3.3562	2.5270	3.6683	4.2468	0.5643	5.9112	4.9798	-0.6840
Client 42 (Laptop Printed)	2.3423	5.0986	1.8184	2.7970	0.6493	0.6601	3.6419	0.9246	0.1967

V. Conclusion

Blurriness leads to the loss of high frequency data along with the smooth edges. Hence the value of blurriness helps in estimating the difference between the genuine face and a picture face. In ideal case, the blurriness value of a genuine face or the real face tends to 0 while the spoofed face has its blurriness tending to 1. Practically, the blur value for the spoofed face is greater than the real face in most of the cases.

The range of hue is generally between 0 to 2 while the saturation and value have their values approximating 0 and 1. The mean for the real images is less for the real face and more for the spoof image. The variance and skewness of the spoof picture is greater than the genuine face.

References

[1] J. Galbally, S. Marcel and J. Fierrez, "Biometric Antispoofing Methods: A Survey in Face Recognition,"in IEEE Access, vol.2,no.,pp.1530-1552,2014.doi:10.1109/ACCESS.2014.2381273H. Simpson, *Dumb Robots*, 3rd ed., Springfield: UOS Press, 2004, pp.6-9.

[2] D. Wen, H. Han and A. K. Jain, "Face Spoof Detection With Image Distortion Analysis," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 4, pp. 746-761, April 2015. doi: 10.1109/TIFS.2015.2400395

[3] F. Crete, T. Dolmiere, P. Ladret, and M. Nicolas, "The blur effect: perception and estimation with a new no-reference perceptual blur metric," in Proc. SPIE: Human Vision and Electronic Imaging XII, 2007.

[4] Y. Chen, Z. Li, M. Li, and W.-Y. Ma, "Automatic classification of photographs and graphics," in Proc. ICME, 2006, pp. 973–976.

[5] M. Stricker, and M. Orengo, "Similarity of color images", in Proceedings of SPIE Storage and Retrieval for image and Video Databases Conference, pp. 381-392, 1995.