Indian Journal of Science and Technology, *Vol 8(S8), 523–535, April 2015*

ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Liveness Detection in Face Identification Systems: Using Zernike Moments and Fresnel Transformation of Facial Images

Farhood Mousavizadeh[1], Keivan Maghooli[1]*, Emad Fatemizadeh[2] and Mohammad Shahram Moin[3]

[1]Department of Biomedical Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran; k_maghooli@srbiau.ac.ir

[2]Sharif University of Technology, School of Electrical Engineering, Biomedical Signal and Image Processing Laboratory (BiSIPL), Tehran, Iran

[3]IT Faculty, ICT Research Institute (Iran Telecom Research Center), Tehran, Iran

Abstract

There are many ways to cheat Biometric facial recognition systems such as recorded movies or portrait photographs. Hence, these systems need Liveness detection in order to guard against such attacks. We have proposed a new real time and single image Liveness detection and face identification approach utilizing Zernike moments and Fresnel Transformation. The advantages of using Fresnel transformation and Zernike moments to express the facial features are investigated in both face identification and Liveness detection scopes. A publically available PRINT-ATTACK database is used for evaluation of our Liveness detection method. Some of the conventional Liveness detection systems use 3D or IR cameras that are costly and may decrease the facial features that are important in face recognition. Multimodal biometric systems use several independent biometrics, like face and voice, simultaneously. Such methods need extra equipment and algorithms that may be expensive and time-consuming. Thanks to the ability of digital Fresnel transformation and Zernike moments to describe and differentiate the light intensity reflections and the aliasing characteristics, a common digital camera is used instead of 3D or IR cameras. The Fresnel transformation of the facial images is extracted and the Zernike moments are then calculated as the features for both face recognition and Liveness detection. A support vector machine classifier is used for Liveness detection and the hamming distance between the extracted feature vectors and the average of registered samples are calculated for face recognition. We obtained an accuracy of 94.0% in separation of the original face pictures and fake ones and 97.16% in face identification. Our methodology proposed a new generative rotation and scale invariant facial anti-spoofing approach that can be used instead of the state of the art features like LBP and Gabor wavelets.

Keywords: Face Liveness Detection, Fresnel Transformation, Zernike Moments.

1. Introduction

Biometric identification is a common technique that uses biometric features to identify and authenticate human beings. Face, voice, fingerprint and retina-scan recognition are conventional biometric techniques. They are used for the authentication or recognition of an individual identity[1–5]., but the critical issue is to protect the system against the stolen and hacked samples. So the presence of some extra algorithms and equipment is necessary for detection of Liveness existence in biometric samples, namely, Liveness detection. Some Liveness detection systems use 3D cameras or several independent biometric methods simultaneously[6–8].

*Author for correspondence

Such methods need extra equipment and algorithms that may be expensive and time-consuming since several independent algorithms are necessary to be run. In Some recent Liveness detection systems, biometrics like iris and finger print are considered to distinguish the fake and real samples. Galbaly et al. applied the finger print Liveness detection method based on quality related features to obtain the information for Liveness judgments[9] and the latest (known to us) researches of Iris-based Liveness detection are published by Czajka and Zhang et al.[10,11]. Their proposed strategy is based on quality related features of Iris images. Tan et al. used a method based on the difference between surface properties of a live human face and a photograph[12]. The method was based on the analysis of Image illumination. The surface of a photograph has normal and mostly constant illumination and is different from the real face. Chanderkant et al. presented a fake face detection method based on facial skin elasticity in which a set of face images are captured after asking the user to do some face movement activities[13]. The method needs a sequential set of face images and some extra subject cooperation, while our approach is based on single face image using a conventional camera and without any user cooperation. In this paper, we investigate the difference of intensity and spatial frequency between a 3D live face and a flat printout spoofing picture. The light reflected intensity and the spatial frequency properties are then analyzed with Zernike moments discriptors[14]. The Fresnel transformation shows different aliasing properties related to different sampling rates between the live and printout fake pictures that are useful for Liveness detection. The changes in the object sampling rate and reflection characteristics may cause differences in the intensity and spatial frequencies of the images. Zernike moments have the ability to distinguish the differences between the intensity and spatial properties of the pictures captured by two different optical systems[15]. The ability of Fresnel transformation to provide the images similar to the original images but different in reflection intensity and aliasing properties, leads to the goal of Liveness detection simultaneously with face recognition. The remainder of this paper is organized as follows: Section 2 discusses our model and the proposed algorithm on Liveness detection and face recognition using a publically available database. The feature extraction and experimental results in Liveness detection and face recognition are described in section 3. The Setup and Classification results can be found in section 4. The competitive advantages of our method and the new prospective of facial Liveness detection methods are summarized in section 5 and 6.

We first explain the model and the reason of using Fresnel transformation and Zernike moments and then focus on the Liveness detection algorithm.

2. Model

In this paper we use Fresnel Transformation of Facial Images and their Zernike moments to identify two real and fake optical subjects. In accordance to our investigation, these two transformations are able to differentiate between the real face images and fake printout pictures. The Fresnel transformation pictures of fake and real are shown in Figure 1.

Figure 1. Examples of Fresnel transformed images of real and fake samples.

Visible differences in aliasing and intensity can be easily seen on the corners and lateral regions of fake and real images.The aliasing commonly occurs in shifted-Fresnel diffraction in short propagation distances. In this paper, such aliasing is investigated as distinctive feature

that is applicable in differentiation between live and spoofing images. The reason is described bellow: Fresnel diffraction with Fast Fourier Transform (FFT) cannot set different sampling rates between source and destination plane, however, the aliasing may be incurred in Fresnel diffraction in a short propagation distance.
Recent researches concentrate on elimination of these effects since they are unwanted in holography image reconstruction[16].

The aliasing condition has not been already investigated as a conventional feature for classification and analysis of facial images. However, the live and fake pictures have different aliasing effects that can be used as proper features for Liveness detection. This is because of the difference between the sampling rate of the picture taken from a real face and the image taken from a printout face photograph. As can be seen in Figure 2, despite of the real images in which the sample rate relates only to the digital camera taking picture from the real face, there are three sample rates in the spoofing images:
The first is the sample rate taken by the digital camera that captures the picture from the original real face, the second is related to the sample rate of the printer that prints out the fake picture and the third is the sample rate of the camera that takes the picture from the printout photograph.

The next stage is Zernike moments extraction. As discussed earlier and also can be seen in the corners and lateral regions of the Fresnel transformed images, there are valuable information on the images obtained by Fresnel transform. The Fresnel transformed images are divided into nine overlapping windows and the Zernike moments for the whole face image and all nine overlapping windows are extracted. The use of multi windowing technique is helpful and practical due to the differences in texture properties between the real and fake images. There are significant differences in the corner and lateral regions. We consider windowing technique and compute features from 3 × 3 overlapping regions to extract and analyze both the detail spatial information on lateral regions and the holistic descriptions computed over the whole face image. Zernike moments, taken from Fresnel transformed images, are used as the features for identifying of the fake and real faces. It is because of Zernike moments capability in a wide range of applications such as pattern recognition applications[17–19], content-based image retrieval[20–22], biometrics[23,24] and Diagnostic Medical Imaging Programs[25–27].
Such performances are useful for two reasons:
1. The nature of aliasing differences that is discussed before in Fresnel transformed images.
2. The different of the light reflection between a real face and fake printout picture.

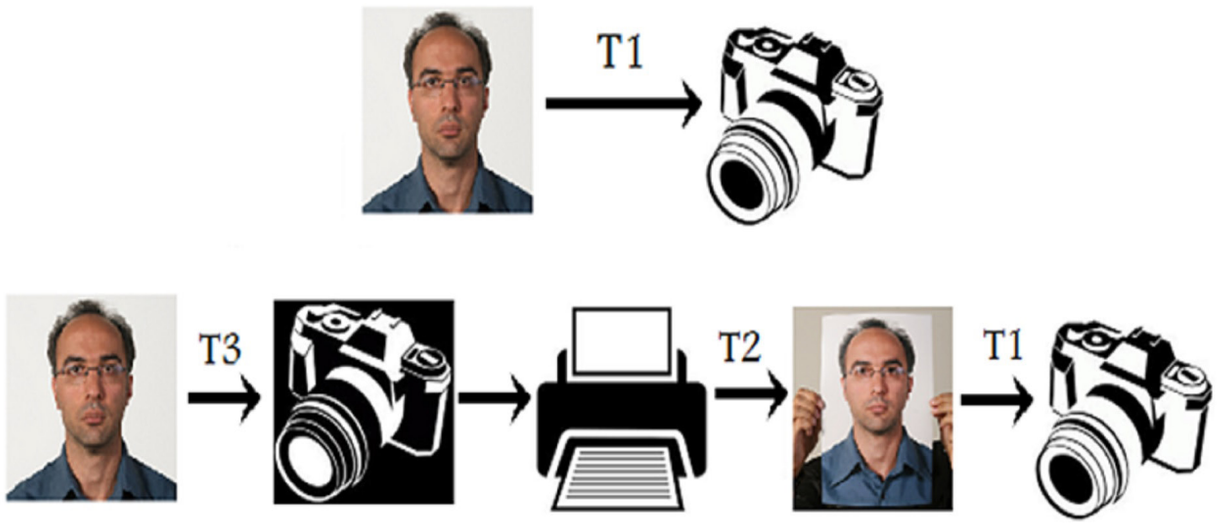

Figure 2. Real face image sample rate T1 and the fake one that T1, T2 and T3 affect the overall sample rate.

The Fresnel transformed intensity is affected by both the light scattering amplitude and the aliasing malfunctions that can be easily analyzed by Zernike moments amplitude.The data base and the algorithm are described in the following sections. Figure 3 shows the algorithm and the stages of separating the original picture from the fake one.

2.1 Database

The proposed algorithm is tested on the publicly available PRINT-ATTACK database that contains 200 videos of both real client accesses and spoof printed photographs. Hence, we have 400 videos of real and spoof attempt videos of 50 subjects in the data base.

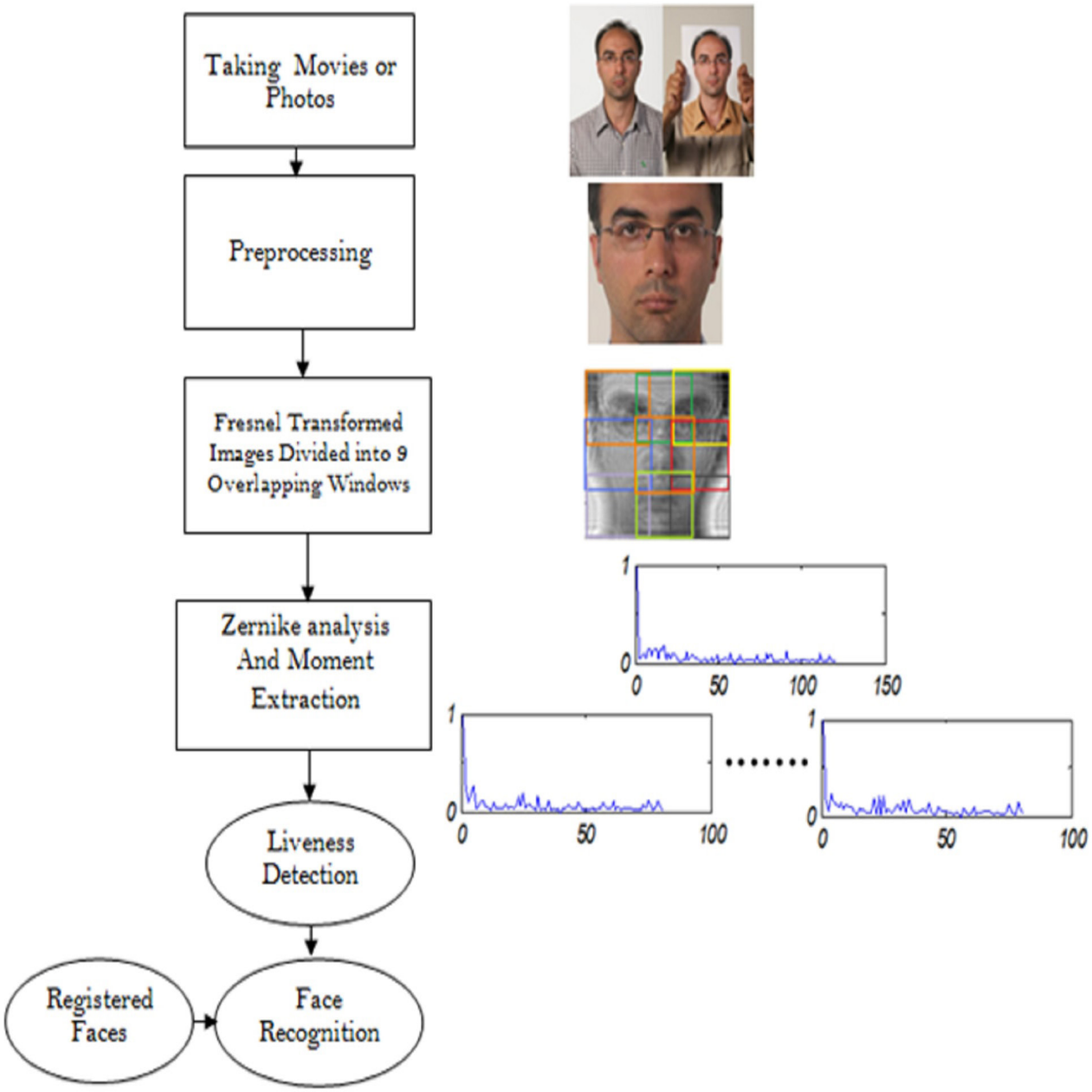

Figure 3. Liveness detection and face recognition Algorithm.

The videos are captured under two different record conditions: the first condition has a uniform background scene and a fluorescent lamp as light source called controlled videos, and the second case which is called adverse video with the non-uniform background scene and the day light illumination. The real videos are captured with a resolution of 320 by 240 pixels at 25fps and are 15 seconds each (375 frames). A technician displays the printout of each client's picture, the spoofing video clips are then generated under the same sampling setup and resolution of real-client accesses and in about 10 seconds. There are two different attack modes for each spoof attempt: the first mode that the operator holds the printed photograph called hand-attack, and the second mode that the prints are glued to the wall called fixed-attack. We use[24] frames of each video with the same frame intervals, 9 for real client accesses and 7 for the spoofing videos. Figure 4 illustrates some examples of real, hand-attack and fixed attack samples.

2.2 Preprocessing

The faces are first detected using a cascade of classifiers based on a variant of Local Binary Patterns (LBP)[28] referred to Modified Census Transform (MCT)[29]. The detected faces are then cropped and normalized into 64×64 pixel images.

2.3 Fresnel Transform

Fresnel transformation of 2D images is appropriate for propagation measurement of input field $E(x_0, y_0)$ along the general z-direction and results in the output field $E(x, y)$ [16,30]. As can be seen in Figure 5, we consider the geometry of Figure 5, where $E(x_0, y_0)$ is the input field on the input plane.

$\sum_0$ Propagates along the general z-direction and results in the output field $E(x, y)$ on the output plane Σ.

Then the output field could be written as:

$$E(x,y,z) = -\frac{ik}{2\pi}\iint_{\Sigma_0} E_0(x_0,y_0)\frac{\exp((ikr))}{r}dx_0dy_0,$$

$$-\frac{ik}{2\pi z}\iint_{\Sigma_0} E_0(x_0,y_0)exp\left[ik\sqrt{(x-x_0)^2+(y-y_0)^2+z^2}\right]dx_0dy_0$$

.....(1)

The approximation of $r \approx z$ in the denominator is used, but not in the exponent.

Equation 1 is a convolution:

$E(x,y;z) = E_0 * S_H(2)$ .....(2)

With the kernel:

Figure 4. Examples of real faces, fake photos hand-attack and fake photos fixed-attack.

$$S_H(x,y;z) = -\frac{ik}{2\pi z} exp\left[ik\sqrt{x^2+y^2}\right] \quad (3)$$

That could be referred to as 'the point spread function (PSF)'. (More precisely, this is a coherent spread function).

2.4 Zernike Moments

We proposed a new generative facial anti spoofing approach based on the Zernike moments invariants as the features of Liveness detection.

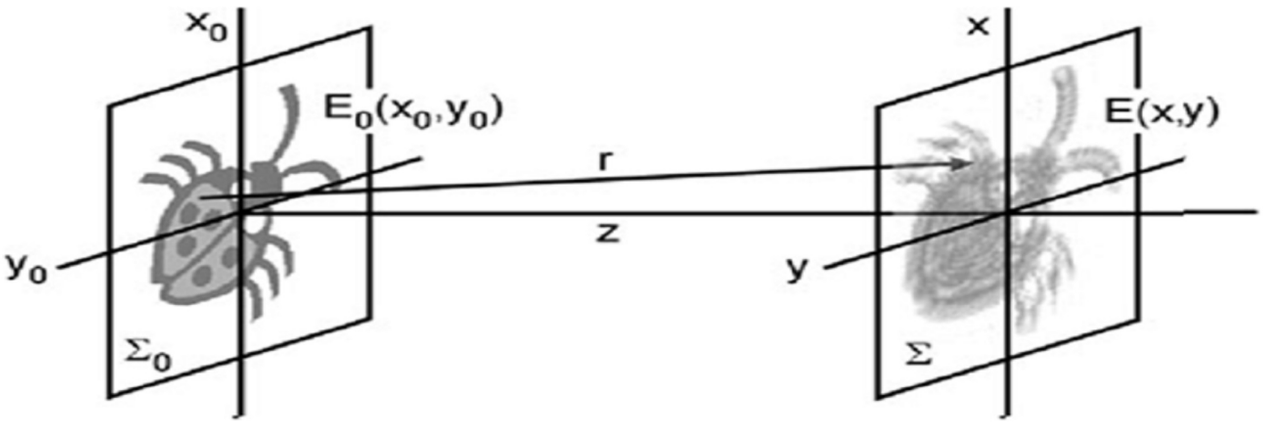

Figure 5. The input field $E(x_0, y_0)$ propagates along the general z-direction and results in the output field $E(x, y)$.

The equation 1 could be written as a paraxial approximation. We often use paraxial, or Fresnel, approximation of the PSF to make theoretical advancements and for other purposes.

$$r = \sqrt{(x-x_0)^2+(y-y_0)^2+z^2} \approx z + \frac{(x-x_0)^2+(y-y_0)^2}{2z(4)} \quad (4)$$

Which is valid for $z^3 \gg k/8\,[(x-x_0)^2+(y-y_0)^2]_{max}^2$ then the Fresnel PSF is:

$$S_F(x,y;z) = (X,Y;Z) = -\frac{ik}{2\pi z} exp(ikz) exp\left[\frac{ik}{2z}(x^2+y^2)\right](5)$$

And the spherical wave-front can be approximated with a parabolic wave-front, or a 2D chirp function. The diffraction field is expressed with a single Fourier transform of spatial frequencies

$$k_x = k\frac{x}{z}\ ;\quad k_y = k\frac{y}{z} \quad (6)$$

$$E(x,y;z) = -\frac{ik}{2\pi z}\exp(ikz) \times \iint_{\Sigma_0} E_0(x_0,x_0) exp\left\{\frac{ik}{2z}[(x-x_0)^2+(y-y_0)^2]\right\} dx_0\ dy_0, = -\frac{ik}{2\pi z}\exp(ikz)\ exp\left[\frac{ik}{2z}(x^2+y^2)\right] \times$$

$$\iint_{\Sigma_0} E_0(x_0,x_0) exp\left[\frac{ik}{2z}(x_0^2+x_0^2)\right] exp\left[-\frac{ik}{z}(xx_0+y_0)\right] dx_0\ dy_0,$$

$$= -\frac{ik}{z}\exp(ikz)\ exp\left[\frac{ik}{2z}(x^2+y^2)\right] \times$$

$$f\left\{E_0(x_0,y_0) exp\left[\frac{ik}{2z}(x_0^2+y_0^2)\right]\right\}[k_x,k_x] \quad (7)$$

$$E(x,y;z) = 2\pi exp\left[\frac{ik}{2z}(x^2+y^2)\right] f\{E_0(x_0,y_0)S_F(x_0,y_0;z)\}[k_x,k_x] \quad (8)$$

Where $f\{\cdot\}$ is the Fourier transform.

Using the Zernike moments have proven to be an strong features for facial recognition and verification[23,24].

The advantage of using Zernike moments in comparison with other facial recognition methods like Local Binary Pattern (LBP), is its flexibility in terms of size and detail of local description with the same computational complexity. These advantages motivate us toward utilizing Zernike moments invariants for facial Liveness detection and anti-spoofing systems. In the present research, this ability is used to differentiate live and fake samples. The Zernike moments could introduce a set of orthogonal polynomials that are interior of the unit circle. These polynomials could be written as:

$$V_{nm}(x,y) = V_{nm}(\rho,\theta) = R_{nm}(\rho)\exp(jm\theta \quad (9)$$

Where:

n positive integer or zero

mpositive or negative and $|m| \le n \;\; n - |m|$ is even

ρ Length of vector from origin to (x,y) pixel

θ Angle between vector and x axis on counter clockwise direction

$R_{nm}(\rho)$ Radial polynomial defined as:

$$R_{nm}(\rho) = \sum_{s=0}^{n-\frac{|m|}{2}} (-1)^s \cdot \frac{(n-s)!}{s!\left(\frac{n+|m|}{2}-s\right)!\left(\frac{n-|m|}{2}-s\right)!}\rho^{n-2s}$$

.....(10)

The Zernike moment of order n and m for a digital image is:

$$A_{nm} = \frac{n+1}{\pi}\sum_{x}\sum_{y} f(x,y)V_{nm}^{*}(\rho,\theta), x^2 + y^2 \le 1 \quad (11)$$

Where $A_{nm}^{*} = A_{n,-m}$

The important point here is the accurate and efficient estimation of n as the high order Zernike moment. The idea to find the best n is that we assure the number n has the ability of picture representation. We could estimate the proper n with a simple method. Let's assume f_i that is a picture and $\widehat{f_i}$ is the reconstructed picture of f_i with $n = i$, then we have $H(\widehat{f_i}, f)$ where H is the hamming distance between $\widehat{f_i}$ and f_i . If $H(\widehat{f_i}, f_i) \le \varepsilon$ where is a pre-selected threshold, we can assure that a good reconstruction is occurred. The Zernike moment magnitudes are normalized to achieve the features that are scale and translation invariant in addition to Zernike moments rotation invariance property[15].

3. Liveness Detection and Face Recognition

In the most Liveness detection researches, the authors assume that the Liveness detection has been previously completed and now the face recognition is important. Therefore, suggesting an algorithm with the ability to meet both goals of Liveness detection and face recognition simultaneously and with using the same features can be worth while because there is no need for the extra hardware or software. Moreover, such systems may use face recognition systems and algorithms that may be costly and time consuming. Classification starts with extracting the Zernike moments of the Facial Images Fresnel transformation. Zernike moments and Fresnel transformation are used together because Zernike moments help to find the major and important texture properties of the facial images and Fresnel transformation makes visible intensity differences in live and fake images. As illustrated in Figure 3, the facial Fresnel transformed images are divided into nine overlapping regions. We calculate Zernike moments of order n=20 yielding 121 Zernike moments for the whole face image and of order n=10 yielding 35 Zernike moments for each overlapping region. Hence, we have a set of 435 (i.e. 120+9×35) orthogonal Zernike moments as the feature vectors for both Liveness detection and face recognition (the magnitude of the Zernike moment is the same for all images and is not considered as a pattern feature15). In addition to aliasing properties, one of the major differences between the real and fake pictures is the light reflected from the curvatures of a real face and a flat fake picture that influences the amplitude of the Zernike moments. As will be seen later in the results, the Zernike moments of real pictures are different from fake ones and are suitable for our intentions. The Zernike moments amplitude of the face pictures in low and middle spatial frequencies are proper features for the Liveness detection. The middle and high frequencies related to face features that are different from one person to another are suitable features for the face recognition. In this paper the whole spatial frequency range is applied to have both Liveness detection and face recognition ability together. Using the Fresnel transformation and the Zernike moments is a strong operator for describing not only the facial detail textures but also the spatial information. The computed features are then fed to SVM classifiers.

4. Setup and Classification Results

In this section, the separability of the features between two classes of live and fake samples is evaluated. The separability indices like and Fisher's discriminant ratio (FDR) are used. The results show good discrimination between two classes in comparison with the state of the art features like LBP.
The scatter matrices like and are needed to calculate the separability indices.as the Within-class scatter matrix is calculated as follow:

$$S_w = \sum_{i=1}^{M} P_i \partial_i \qquad (12)$$

Where is the covariance matrix for class w_i

$$\partial_i = E\left[(x - \mu_i)(x - \mu_i)^T\right] \qquad (13)$$

Pi is the a priori probability of class . That is, where is the number of samples of class , out of a total of N samples. Obviously, trace { } is a measure of the average, over all clas follow:

$$S_b = \sum_{i=1}^{M} P_i(\mu_i - \mu_0)(\mu_i - \mu_0)^T \qquad (14)$$

And the Trace { } could be calculated as the measure of average (over all classes) distance of the mean of each individual class from the respective global value.
And the Mixture Scatter matrix is:

$$S_m = E\left[(x - \mu_0)(x - \mu_0)^T\right] \qquad (15)$$

S_m is the covariance matrix of the feature vector and it could be also shown as:

$$S_m = S_b + S_w \qquad (16)$$

J_1 could be calculated as:

$$J_1 = \frac{trace\{S_m\}}{trace\{S_w\}} \qquad (17)$$

J_1 takes large values when samples are well clustered around their mean, within each class, and the clusters of the different classes are well separated. We could see values of two classes of live and fake samples using our method and LBP in Table 1. As can be seen our features are better clustered and are separable using Zernike moments of Fresnel transformation. We also calculated Fisher's Discriminant Ratio (FDR) to quantify the separability capabilities of our individual features. The FDR is calculated as follow:

$$FDR = \frac{(\mu_1 - \mu_2)^2}{\sigma_1^2 + \sigma_2^2} \qquad (18)$$

Figure 6 shows the FDR values related to the first 100 features sorting in descending order. For the fair comparison, we took the same feature dimension as the LBP features by changing the number of Zernike moments and also normalized the features of both methods. As can be seen in Figure 6 our features are well separated into two classes and the FDR values of our features shows better separation of classes than the LBP. Although the dimension of our features could

be reduced using the main features that are sorted by FDR but we did not decrease our feature's dimension because these features may be usable for face identification. Figure 1 illustrates the real and fake images and the corresponding Fresnel transformation of facial images that was explained before. Significant differences are observed between the real and fake images because of the aliasing and also differences between the coordinates of a flat photo and a complex 3D human face. A ten-fold cross-validation is used, and averaged scores are reported for our Liveness detection method. The entire set of 50 subject video images is divided into ten equal sets. Nine of them are used for the training, one for testing. The real access video set consists of two adverse and controlled videos. Therefore, every subject has 4 real access videos. The spoofing set consists of four types of attack: Fixed-adverse, Fixed-controlled, Hand-adverse and controlled videos. As explained before, 24 frames of each video are used for making the image data set. Hence, each individual fold has 5×4×24 images for real access clients and the same number of images for spoofing attacks. We evaluate our texture operator by comparing with two common Liveness detection operators: multi-scale local binary patterns (LBP)[31] and Gabor wavelets[32]. As discussed before, the dimension of our features is 435 and it is nearly the half size of LBP features that could be an advantage for our approach. The features are computed applying three operators to all ten-folds described earlier. The same optimal polynomial SVM classifier, database and protocol are used for having a fair comparison.

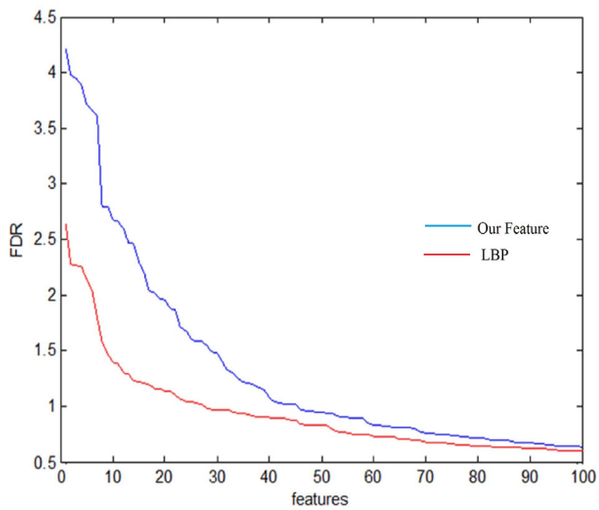

Figure 6. FDR values related to the first 100 features sorting in descending order.

Table 1 presents a classification comparison between our approach and the results applying LBP and Gabor wavelets operators. The results show clearly that our method is as competitive as the state of the art techniques in Liveness detection and also better results in comparison to LBP and Gabor wavelets operators. The Region of Convergence (ROC) curves of three spoofing features (our method, LBP and Gabor wavelets) can be seen in Figure 7. It can be clearly seen that the three anti spoofing approaches performed satisfactory in discriminating live face images from fake photos. The outstanding superiorities of our purposed method can be explained by two facts:
1. The ability of Fresnel transformation to illustrate the different aliasing properties related to the different sample rates.
2. The light reflection intensity that is completely different in the flat surface of a fake picture versus a 3D real face.

Table 1. Ten folds classification accuracy (Our method, LBP and Gabor)

Fold Number	Our method%	LBP %	Wavelet Gabor%	J1 Our method	J1 LBP
1	92.2	87.0	85.5	1.48	1.43
2	94.2	89.3	85.8	1.98	1.53
3	94.3	93.6	87.1	1.82	1.47
4	93.0	91.0	85.0	1.67	1.49
5	95.5	96.3	93.7	2.09	1.81
6	97.7	97.5	91.5	1.98	1.57
7	95.2	94.1	84.7	2.31	1.61
8	95.3	95.6	90.8	2.05	1.62
9	90.1	90.2	88.6	1.37	1.38
10	92.9	93.5	85.3	1.93	1.60
Average	**94.0**	**92.8**	**87.8**	-	-
Standard Deviation	2.10	3.35	3.19	-	-

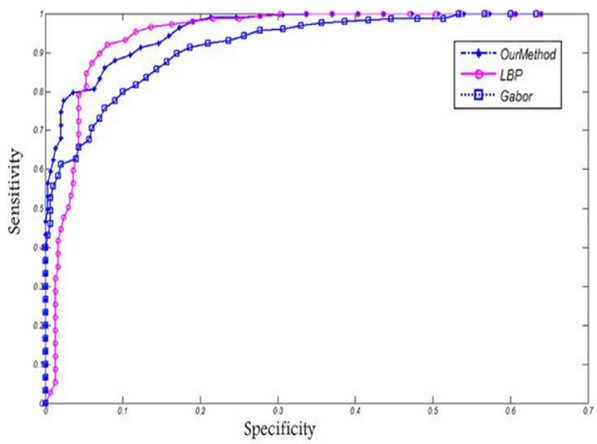

Figure 7. ROC curves of three texture operators (Our Method, LBP, and Gabor wavelets operator).

The equal error rate of our method is 4.5% versus 5.1% for LBP and 11.62% for Gabor wavelets operators. In accordance to the graph depicted in Figure 8, our method achieves the performance 94% at 0.16% FAR. Figure 9 shows the ROC curves for the different numbers of the first Zernike moments, defined as N, that are used in Liveness detection and Table 2 summarizes the Area Under Curve (AUC) results taking the same classifiers. As we can see, increasing the number of Zernike moments significantly improves the performance of Liveness detection. Nevertheless, we did not observe any significant changes in AUC and ROC curves for N more than 35, because the higher order of Zernike moments are related to the higher spatial frequencies that are not useful in Liveness detection.

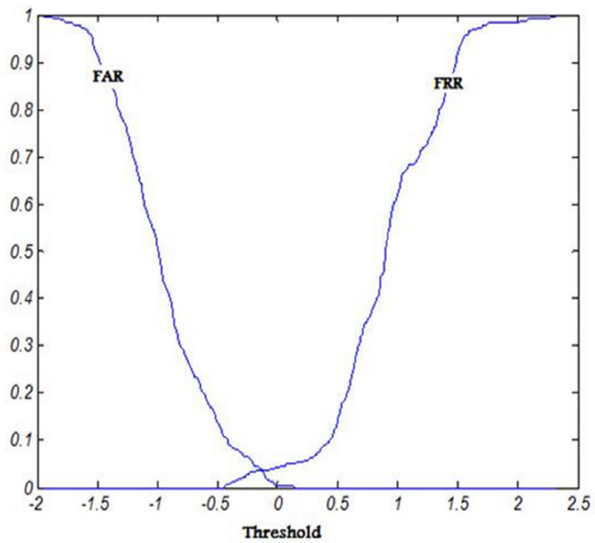

Figure 8. Our method Equal Error Rate (EER) estimation using FAR and FRR graphs.

As discussed before, the N number for the whole face image is not decreased because the spatial details in the face images a In our approach, face recognition and Liveness detection features are the same. A Zernike moment based algorithm is used, which identifies whether an image, acquired by a client, matches one of the suspects or not. re useful for face recognition. As mentioned before, 8 capturing mode and 24 frame images of 50 persons have been used. Hence, our facial database consists of overall 9600 (i.e.50×24×8) images. A ten-fold cross-validation is used and each subject 192 video images is divided into ten equal sets. Finally, each fold has approximately 19×50 images and the remaining images used for training as registered images.

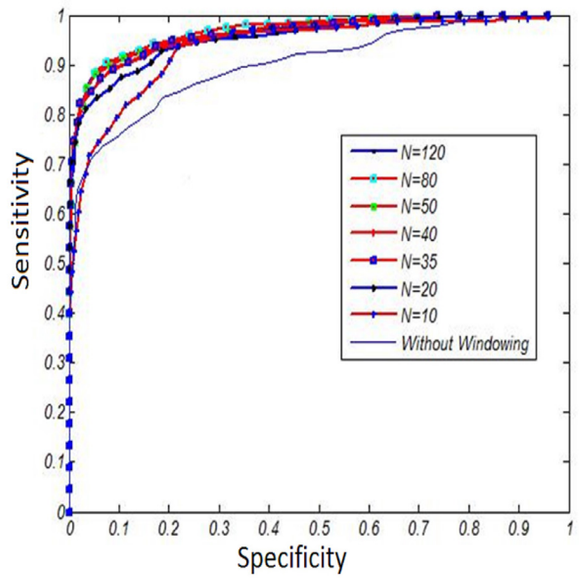

Figure 9. The ROC curves for the different number s of the first Zernike moments.

Table 2. Feature size and AUC for different numbers of the first Zernike moments

N	Feature size	AUC
Without Windowing(N=0)	120	.90
10	210	.93
20	300	.95
35	435	.96
40	480	.96
50	570	.96
80	840	.96
120	1200	.96

For face recognition, we measure the hamming distance between the extracted feature vectors of each sample and the average of registered samples using a threshold for the acceptance. Table 3 Presents Ten-fold results on face recognition datasets.

The results show that our method appeared to be suitable for feature extraction in face recognition systems.It should be noted that the major goal of this research is the Liveness detection and a brief report of the face identification results is presented to evaluate the ability of our features for face recognition and Liveness detection at the same time.Satisfactory results have been obtained from application of Zernike moments of Fresnel transformation in both face recognition and Liveness detection. One of the advantages of having Liveness detection and face identification at the same time is knowing not only that the cheating has occurred but also whose picture is used, because the subject whom his picture is used may be in danger and needs to be helped.

Table 3. Ten folds face recognition Performance using our method VS. LBP

Fold Number	Our method	LBP
1	96.3	94.2
2	100	98
3	96.6	92.3
4	97.2	95.3
5	100	97
6	90.2	91.1
7	95.6	94.2
8	100	99
9	98.4	94.6
10	97.3	94
Average	**97.16**	**94.97**
Standard Deviation	2.94	2.45

The results show that our method appeared to be suitable for feature extraction in face recognition systems.

It should be noted that the major goal of this research is the Liveness detection and a brief report of the face identification results is presented to evaluate the ability of our features for face recognition and Liveness detection at the same time.

Satisfactory results have been obtained from application of Zernike moments of Fresnel transformation in both face recognition and Liveness detection. One of the advantages of having Liveness detection and face identification at the same time is knowing not only that the cheating has occurred but also whose picture is used, because the subject whom his picture is used may be in danger and needs to be helped.

5. Discussion

This paper presents a Liveness detection algorithm using single face images. The results show that using Fresnel transformation provides images that are different in aliasing malformation and light intensity between live 3D face and fake printout pictures and are suitable for face Liveness detection.The Fresnel transformation shows different aliasing properties related to different sampling rates between the live and printout fake pictures that are useful for Liveness detection. The changes in the object sampling rate and reflection characteristics may cause differences in the intensity and spatial frequencies of the images. Zernike moments have the ability to describe the intensity and spatial properties of the pictures captured by two different optical systems. They are well known and widely used in pattern recognition and image analysis.

The high quality and resolution color printers have been used to ensure the fake pictures are exactly like the real face pictures in size and details. The Light beams reflected from a real face are different from a flat planar picture. Therefore the spatial frequencies and intensity of the reflected light of a real face is quite different than that provided by a flat printout picture. These frequency properties are investigated by the Liveness detection methods like Gabor wavelet and Fourier spectra analysis.

LBP Liveness detection methods concentrate on the light intensity and reflection differences between live and fake samples. Our method takes the advantage of using both frequency and intensity properties by using: A: Fresnel transformation and its ability to differentiate the spatial frequency properties of images.

B: Zernike moments and their ability to differentiate the images with different light reflected intensity.

The results show clearly that our method is as competitive as the state of the art techniques in Liveness detection and also produces better results in comparison with LBP and Gabor wavelets operators.

The results show that the Zernike moments of Fresnel transformed real pictures are different from fake ones and are suitable for our intentions. The Zernike moments' amplitude of a face picture in low and middle spatial frequencies is a proper feature for the Liveness detection. The middle and high frequencies that are different from one person to another are suitable features for the face recognition.

6. Conclusion

Using two different systems or algorithms for face recognition and Liveness detection is time-consuming and may need some additional equipments or facilities. Our research presents the same features and algorithm in Liveness detection and face recognition which can be run simultaneously. The dimension of our features is smaller than the other state of the art methods that can be a privilege for our approach.This paper proposes a single image-based face anti-spoofing method not only comparative with the state of the art Liveness detection methods, but also applicable in face recognition systems. The features are rotation, scale and translation invariant due to using the normalized Zernike moments.We assume that the fake pictures are stolen or hacked and the other types of biometric face attacks like statue or hypnotized subjects are not considered.

We can get help from the sequential pictures and motion analysis methods against these kinds of attacks.

7. Acknowledgment

The database of this paper used the Print-Attack Corpus made available by the Idiap Research Institute, Martigny, Switzerland.The authors would like to thank the financial support provided by Research Institute for ICT (formerly ITRC).

8. References

1. Bartlett MS, Movellan JR, Sejnowski TJ. Face recognition by independent component analysis. IEEE Trans Neural Networ. 2002; 13(6):1450–64.
2. Shah HNM, Ab Rashid MZ, Abdollah MF, Kamarudin MN, Chow KL, Kamis Z. Biometric voice recognition in security system. Indian Journal of Science and Technology. 2014; 7(2):104–12.
3. Long TB, Thai LH, Hanh T. Multimodal biometric person authentication using fingerprint, face features. PRICAI 2012: Trends in Artificial Intelligence. 2012; 7458:613–24.
4. Parvathi R, Sankar M. Fingerprint authentication system using hybrid classifiers. Int J Soft Comput Eng. 2012; 2:185–90.
5. Tabatabaee H, Jafariani H. Retinal identification system using Fourier-mellin transform and fuzzy clustering. Indian Journal of Science and Technology. 2014; 7(9):1289–96.
6. Chetty G, Wagner M. Multi-level liveness verification for face-voice biometric authentication. Biometric Symposium; 2006; Baltimore, Maryland.
7. Chetty G, Wagner M. Liveness detection using cross-modal correlations in face-voice person authentication. InterSpeech Conference; 2005; Lisbon, Portugal. p. 2181-4.
8. Bronstein M, Kimmel R. Three-dimensional face recognition. Int J Comput Vision. 2005; 64(1):5–30.
9. Galbally J, Alonso-Fernandez F, Fierrez J, Ortega-Garcia J. A high performance fingerprint liveness detection method based on quality related features. Future Gener Comp Sy. 2012; 28(1):311–21.
10. Zhang H, Sun Z, Tan T. Learning hierarchical visual codebook for iris liveness detection. The International Joint Conference on Biometrics; 2011. p. 11–3.
11. Czajka A. Database of iris printouts and its application: Development of Liveness detection method for iris recognition. The 18th International Conference on Methods and Models in Automation and Control (MMAR2013); 2013; Miedzyzdroje, Poland. p. 26–9.
12. Tan X, Li Y, Liu J, Jiang L. Face liveness detection from a single image with sparse low rank bilinear discriminative model. 11th European Conference on Computer Vision; 2010. p. 504–17.
13. Kant C, Sharma N. Fake face detection based on skin elasticity. Int J Adv Res Comput Sci Software Eng. 2013; 3(5):1048–51.
14. Trester S. Computer-simulated Fresnel holography. Eur J Phys. 2000; 21(4):317–31.
15. Khotanzad A, Hong Y. Invariant image recognition by Zernike moments. IEEE Trans Pattern Anal Mach Intell. 1990; 12(5):489–97.
16. Shimobaba T, Kakue T, Okada N, Oikawa M, Yamaguchi Y, Ito T. Aliasing-reduced Fresnel diffraction with scale and shift operations. J Opt. 2013; 15(7).
17. Wang L, Healey G. Using Zernike moments for the illumination and geometry invariant classification of multispectral texture. IEEE Trans Image Process. 1998; 7(2):196–203.
18. Broumandnia A, Shanbehzadeh J. Fast Zernike wavelet moments for Farsi character recognition. Image Vision Comput. 2007; 25(5):717–26.
19. Wang XF, Huang DS, Du JX, Xu H, Heutte L. Classification of plant leaf images with complicated background. Appl Math Comput. 2008; 205(2):916–26.
20. Kim YS, Kim WY. Content-based trademark retrieval system using a visually salient feature. Image Vision Comput. 1998; 16(12–13):931–9.
21. Kim WC, Song JY, Kim SW, Park S. Image retrieval model based on weighted visual features determined by relevance feedback. Inform Sci. 2008; 178(22):4301–13.
22. Li S, Lee MC, Pun CM. Complex Zernike moments features for shape-based image retrieval. IEEE Trans Sys Man Cyb. 2009; 39(1):227–37.
23. Lu C, Lu Z. Zernike moment invariants based iris recognition. Advances in Biometric Person Authentication. 2004; 3338:554–61.
24. Kim HJ, Kim WY. Eye detection in facial images using Zernike moments with SVM. ETRI Journal. 2008; 30(2):335–7.
25. Bharathi VS, Ganesan L. Orthogonal moments based texture analysis of CT liver images. Pattern Recogn Lett. 2008; 29(13):1868–72.
26. Liyun W, Hefei L, Fuhao Z, Zhengding L, Zhendi W. Spermatogonium image recognition using Zernike moments. Comput Meth Prog Bio. 2009; 95(1):10–22.
27. Iscan Z, Dokur Z, Olmez T. Tumor detection by using Zernike moments on segmented magnetic resonance brain images. Expert Sys Appl. 2010; 37(3):2540–9.
28. Ahonen T, Hadid A, Pietikainen M. Face recognition with local binary patterns. Computer Vision - ECCV 2004. 2004; 3021:469–81.
29. Froba B, Ernst A. Face detection with the modified census transform. IEEE International Conference on Automatic Face and Gesture Recognition; 2004. p. 91–6.
30. Kim MK. Diffraction and Fourier Optics. Digital Holographic Microscopy: Principles, Techniques and Applications. Springer; 2011.

31. Maatta J, Hadid A, Pietikainen M. Face spoofing detection from single images using micro-texture analysis. The International Joint Conference on Biometrics; 2011. p. 1–7.

32. Manjunath BS, Ma WY. Texture features for browsing and retrieval of image data. IEEE Trans Pattern Anal Mach Intell. 1996; 18:837–42.