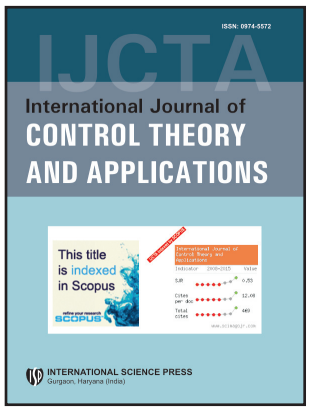

International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 9 • Number 44 • 2016

Detecting Face Spoof Using IDA Features and Colour Texture Analysis

Reshma Rajan[a] and Ani Sunny[b]

[a-b]Department of Computer Science and Engineering, M.A College of Engineering, Kothamangalam, Kerala, India. Email: [a]reshmarajan6666@gmail.com; [b]anisunny88@gmail.com

Abstract: In recent years, automatic face recognition has become a realistic target of biometrics research. The main applications ranges from de-duplication of identity to authentication of mobile payment. Face spoof attacks are really a threat to face recognition systems. Face spoof attacks are also called as biometric sensor presentation attacks, in which an attacker gain access to the services or facilities by using the photo or video of an authorized user's face. The existing Image Distortion Analysis (IDA) method uses different classifiers for different spoof attacks, which adds additional complexity to the system. So to overcome that, in the proposed method a multiclass SVM classifier is used which can also detect the type of attack. To improve the spoof detection rate, the proposed method considers colour texture analysis in addition to the IDA features (blurriness, chromatic moment and colour diversity). To choose the most appropriate feature set, proper feature ranking and selection is applied. Experimental results on MSU MFSD and Idiap Replay-Attack public domain face spoof databases shows that the proposed method outperforms the current face spoof detection method based on Image Distortion Analysis.

Keywords: Image Distortion Analysis, colour texture analysis, multiclass SVM, feature ranking and selection.

1. INTRODUCTION

In the past two decades, face recognition has been one of the most interesting and important research fields. Automated authentication is used widely in various access control applications in different sectors, varying from governments, airports, banking systems to personal devices. The existing common user verification processes like Personal Identification Numbers (PINs) and paired authentication (username and password) can be easily hacked, predicted by the attacker or even can be forgotten by the user. So automated authentication has been more directed towards using person's biometric traits for more robust recognition. Biometrics refers to metrics related to human characteristics. Biometrics is the measurement and statistical analysis of people's physical and behavioral characteristics. The technology is mainly used for identification and access control, or for identifying individuals that are under surveillance. Biometrics authentication is also called as realistic authentication. Some characteristics are distinctive to each person. Therefore biometric authentication is more reliable and robust when compared to other authentication techniques. Different types of biometrics such as iris, fingerprint and facial features are used as identification tools in many critical applications. Biometric traits such as fingerprint, palm

print and iris are difficult to acquire. A person's face image or video is relatively easier to acquire. Also. the cost of launching a face spoof attack is relatively low. Face recognition does not require any additional sensors as in the case of fingerprint authentication, since all smart phones are equipped with a front facing camera [2].

The different biometric attacks are broadly classified into direct and indirect attacks. The attacks which are performed outside the biometric system simply by presenting a biometric trait to the input sensor are called as direct attacks. The attacks which are performed inside the biometric system by intruders, such as cyber-criminal hackers are called as indirect attacks. The main countermeasure to face spoofing is liveness detection, which aims at detecting physiological characteristics, such as eye blinking, facial expression changes and mouth movements. Motion detection, texture analysis and liveness detection are the three main criterias considered for typical 2-D face anti-spoofing process[1].

Because of the natural and non-intrusive interaction, identity verification and recognition using facial information is one of the most active areas in computer vision research. Face recognition has several advantages over other biometric technologies: It is natural, nonintrusive, and easy to use. It does not consume high computation efforts.

The major type of face spoof attacks are photo attacks, video attacks and mask attacks. A printed attack is an attack in which the attacker shows a photograph of the genuine user on his smart device or displaying a printed copy to the camera. Replay attack is an attack in which the attacker replays the video of a genuine user from a phone or tablet facing the camera. The attack becomes easier if the resolution of the printer or display device is higher [3].

The main goal of this research is to propose an efficient and robust face spoof detection algorithm based on Image Distortion Analysis(IDA) and Colour Texture Analysis. For efficiently classifying the original and spoof images, a single multiclass SVM classifier is used. Feature ranking and selection is applied to choose the best features for classification. Experimental results on the public domain face spoof databases MSU MFSD and Idiap Replay-Attack shows that the proposed method achieves best performance compared to the existing method with a much lower error rate.

The rest of the paper is organized into four sections. SectionII deals with the related works. Proposed System is discussed in section III. Section IV involves the results and discussions and the conclusion of the work is given in section V.

2. RELATED WORKS

Based on the different types of cues, face spoof detection methods are classified into five groups. They are (1) Motion Based Methods (2) Texture Based Methods (3) Image Quality Analysis Based Methods (4) Image Distortion Analysis Based Methods (5) Methods Based On Other Cues.

A. Motion Based Methods

These methods are designed to counter printed photo attacks. These methods try to capture the subconscious motion of organs and muscles in a live face, such as eye blink [4], mouth movement [5] and head rotation [6]. In [4], the authors proposed a method for blinking-based liveness detection using Conditional Random Fields [CRF].CRF's accommodates long-range contextual dependencies among the observation sequence. Motion is a relative feature across video frames. Therefore, these methods have better generalization ability. The main limitation is that it takes relatively long time to accumulate the stable vitality features for face spoof detection. It is easy to confuse these methods by other irrelevant background motions.

B. Texture Based Methods

Texture based methods are designed to counter both replay video attack and printed photo attack. A single image is only required for the detection of spoof. These methods have poor generalization ability because these can be easily over-fitted to one particular illumination and imagery condition[21]. The basic advantages are fast response and low computational complexity. In [7], the authors proposed a component based face coding approach for liveness detection. In this method, a Holistic Face (H-FACE) is formed by expanding the detected face and dense low level features (e.g. LBP, LPQ, HOG, etc.) are extracted for all the components. They have used a component based approach which gives much better performance when compared to the methods that uniformly divide the image into grids.

C. Image Quality Analysis Based Methods

For designing informative features no face specific information has been considered in this method. This method aims at designing a generic liveness detection method across different biometric modalities. In [8], the authors proposed a biometric liveness detection method for iris, fingerprint and face images. Here 25 general image quality features are considered which includes full-reference and non-reference measures. This method has improved generalization ability, fast response and low computational complexity. The features are selected based on performance, complementarity, complexity and speed.

D. Image Distortion Analysis Based Methods

Based on the light reflectance of the object at specified location, the major distortions in a spoof face image include: (1) specular reflection from the printed paper surface or LCD screen (2) image blurriness due to camera defocus (3) image chromaticity and contrast distortion due to imperfect colour rendering of printer or LCD screen and (4) colour diversity distortion due to limited colour resolution of printer or LCD screen. In [2], the author proposed an efficient and rather robust face spoof detection algorithm based on image distortion analysis (IDA). Different classifiers are used for different face spoof attacks. Experimental results on two public-domain face spoof databases (Idiap REPLAY-ATTACK and CASIA FASD) and the MSU MFSD database created by the author shows that the proposed approach outperforms the state-of-the-art methods in spoof detection. The proposed approach could improve the generalization ability under cross-database scenarios.

E. Methods Based On Other Cues

Face spoof countermeasures using cues derived from sources other than 2D intensity image, such as 3D depth[23], IR image[24], spoofing context[25], and voice[26] have also been proposed. The main disadvantage of this method is that it impose extra requirements on the system or user. For example, the methods that use IR images require an additional IR sensor and the method based on voice requires a speech analyzer. Therefore these methods have a narrower application range. In [9], the author proposed a novel face liveness detection approach to counter spoofing attacks by recovering sparse 3D facial structure. From the given face video, they first detect facial landmarks and then select the key frames. The frames which are propitious to recover facial structure are called as key frames. From the selected key frames sparse 3D facial structures are recovered. Finally an SVM classifier is trained to distinguish between genuine and fake faces.

3. PROPOSED SYSTEM

The face spoof detection algorithm proposed in this work is based on Image Distortion Analysis (IDA) and Colour Texture Analysis. An image frame or image of a person's face is the input to the system. The input image is normalized after detecting the face. After normalization of the input image IDA features are extracted from the

normalized image and colour texture analysis is done to extract texture descriptions from each colour channel separately to form the feature vector. The extracted features are normalized to fall within a certain range of values. From the feature vector the most appropriate feature set is selected by applying proper feature ranking and selection. These features are given as input to the multiclass SVM classifier that is used to distinguish between genuine (live) and spoof faces. Figure 1 shows the proposed face spoof detection method using multiclass SVM classifier.

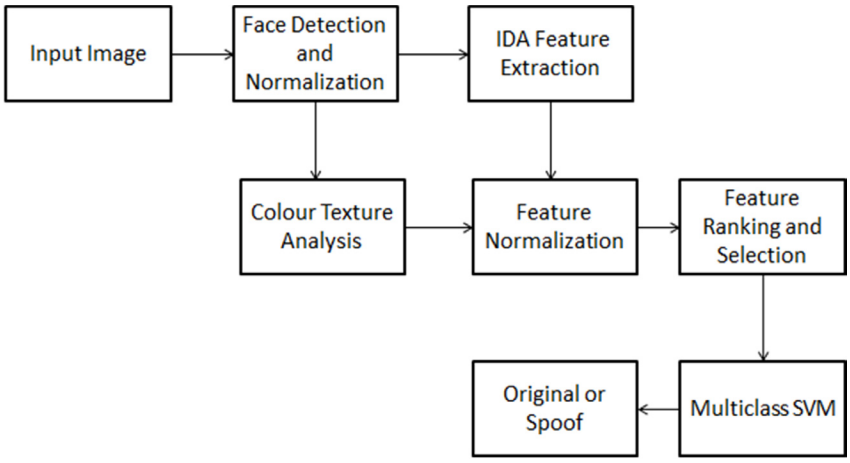

Figure 1: Block Diagram of the Proposed System

A. Face Detection and Normalization

The first step in this work is face detection. The algorithm automatically detects face from the input image. Then the features which could be used to identify the face as genuine or spoof are extracted from this face image. The detection process could be affected by many complexities such as background, illumination etc. An input face image frame, extracted from the collected video dataset is given as input to the face detection module. The classifier in a face detection system is trained with a set of face and non-face images. Training is done using the features extracted from both face and non-face images. So the system will be able to correctly classify the given input image as a face or non-face image. Viola-Jones face detection algorithm is used in this work for face detection. After face detection, the input image is cropped and normalized to 144×120 pixels.

In Robust Real Time Face Detection, Paul Viola and Michael J Jones[10] proposed the Viola Jones Face Detection Algorithm[11][12] which can efficiently classify face and non-face images. The main concepts in the algorithm are haar features, integral image, adaboost algorithm and cascading classifier. Haar features represent the characteristics of face. Each feature results in a single value. The input image is converted to integral image which is a new image representation used for fast feature evaluation and also as a means to speed up the classification task. Using Adaboost learning algorithm, a set of relevant features are selected. The features which performs better than random guessing and detects more than half the cases are selected as relevant features. Then a cascading classifier is built which is composed of stages each containing a strong classifier. Each stage has a certain number of features. This helps in quickly discarding the non-face images.

B. IDA Feature Extraction

According to Dichromatic Reflection Model [13], light reflectance of an object at a specific location can be decomposed into diffuse reflection and specular reflection components. In this we try to capture the image quality

differences which occurs due to the difference in the reflection properties of materials such as paper, facial skin and screen. In the proposed work three IDA features are extracted.

1. *Blurriness Features*: Spoofing medium usually have limited size. So in order to conceal the boundaries of the attack medium, the attackers have to place them close to the camera. So the spoof image may get defocused and blurriness occurs.

   Two types of blurriness features are extracted. The difference between the original input image and its blurred version is considered in the first feature[14]. If the difference is large it indicates that the blurriness is lower in the input image. The average edge width in the input image is considered in the second feature[15].

2. *Chromatic Moment Features*: Due to the imperfect color reproduction properties of printing and display media, recaptured face images show a different color distribution when compared to colors in genuine face images. To devise invariant features, the normalized face image is converted to HSV(Hue, Saturation and Value) space from RGB space. Then mean, deviation and skewness of each channel is computed[16].These three are considered as chromatic moment features. Two additional features are taken:(a)percentage of pixels in the maximal histogram bin (b)percentage of pixels in the minimal histogram bin.

3. *Color Diversity Features*: Color reproduction loss occurs during image/video recapturing process. Due to this, spoof faces tends to fade out. First color quantization is performed[16]. Then two features are taken:(a)Histogram bin count of the most frequently appearing colour (b)Number of distinct colours appearing in the normalized image.

C. Colour Texture Analysis

In the proposed work we extract joint colour texture information from both luminance and chrominance channels. Due to the spoofing medium dependent gamut and other imperfections in the colour reproduction, the recapturing process introduces inherent disparities in the colour information between a genuine face and a recaptured face image. The main limitation of texture analysis of gray scale images is that we can extract fine details only if the input image resolution is high.

In the proposed work, co-occurrence of adjacent local binary patterns are considered to extract the texture descriptions. First, we convert the image from RGB space to YCbCr colour space[18]. Then the texture descriptions are extracted from each colour channel separately and these descriptions are concatenated to get an overall facial representation. LBP patterns are constructed for each pixel. For each pixel in an image, by thresholding a circularly symmetric neighbourhood with the value of the central pixel, a binary code is computed[17].

$$\mathrm{LBO}_{\mathrm{P},\,\mathrm{R}(x,\,y)} = \sum_{n=1}^{\mathrm{P}} \delta\left(r_n - r_c\right) \times 2^{n-1} \tag{1}$$

where, $\delta(x) = 1$ if $x >= 0$, otherwise $\delta(x) = 0$. r_c and $r_n (n = 1, ..., \mathrm{P})$ denote the intensity values of the central pixel (x, y) and its P neighbourhood pixels located at the circle of radius R (R > 0), respectively.

To represent the image texture information, the occurrences of different binary patterns are collected into histogram. In this work the spatial information between adjacent LBP's are also considered. The concept of co-occurrence is used to consider the spatial relation. Co-occurrence of adjacent LBP's is defined as the count of how often their combination occurs in the whole image. To capture the correlation between the spatially adjacent patterns, four directions are considered: D = {(0, Δs), (Δs, 0), (Δs, Δs) and ($-\Delta s$, Δs)} where s is the distance between two adjacent LBP patterns. For each direction, auto-correlation matrices are generated.

D. Feature Normalization

Normalization is done to make the features comparable and to reduce the influence of one feature on the other. It also improves the accuracy and makes the training faster. All the features will get equal opportunity to influence the model. Min-max normalization is used. It is relatively simpler and can effectively suppress the effect of outliers.

$$\text{normalized}(x') = \frac{x - \min(x)}{\max(x) - \min(x)} \tag{2}$$

E. Feature Ranking and Selection

The main aim of feature ranking and selection is to reduce the dimensionality of the feature space. It also removes redundant, irrelevant and noisy data. It improves classification accuracy and reduces time constraints. Chi-square probability density function is used to rank the features. Chi-square probability density function is one of the characteristics of chi-squared distribution.

$$f(x;k) = \frac{x^{\left(\frac{k}{2}-1\right)} e^{\frac{-x}{2}}}{2^{\frac{k}{2}} \tau^{\frac{k}{2}}} \tag{3}$$

for $x > 0$. Otherwise 0. $\tau^{\frac{k}{2}}$ denotes the gamma function. k is the degree of freedom.

Feature selection is a process that chooses a minimum subset of features from the original set of features, so that the feature space is optimally reduced according to a certain evaluation criteria. The main steps of feature selection are: subset generation, subset evaluation, stopping criteria and validation. In practical problems, testing a given classifier on a number of feature subsets obtained from different ranking indices is the only way to make sure that the highest accuracy is obtained. Feature selection is done here by empirical method by selecting predefined number of features.

F. Classification

Multiclass learning is referred as the tasks in which labels are assigned to instances where the labels are taken from a finite set of elements in supervised machine learning tasks[19]. In existing system which is based on image distortion analysis different classifiers are used for different spoof attacks. Each classifier is trained with combining all genuine samples and a single group of spoof samples. The output from each of these classifiers have to be fused in order to get the final result. But fusion is a time consuming process and if output of any one of the classifiers is wrong it will affect the entire result. So in order to overcome this, in the proposed system a single multiclass SVM is used. A single multiclass SVM classifier[20] is used for training and testing purpose which can also identify the type of spoof attack. It classifies the output to three different classes: original, spoof-replay video attack and spoof printed photo attack.

4. RESULTS AND DISCUSSION

The analysis of the proposed method has been done in this section. The experimental analysis has been done using the public domain face spoof databases MSU Mobile Face Spoofing Database (MSU MFSD) and Idiap Replay-Attack Database[2]. By feeding the extracted features to the multiclass SVM classifier, the efficiency of the system has been computed. Then testing has been performed to get the response of classifier over the test dataset. The experiment was conducted by using MATLAB (R2013a). Then a comparison has been done with

the existing system which uses an ensemble SVM classifier scheme based on Image Distortion Analysis (IDA) and is referred to as IDA + SVM.

The performance metrics used for the comparison are:

$$\text{Detection Rate (TPR)} = \frac{TP}{TP + FN} \tag{4}$$

$$\text{False Rejection Rate (FRR)} = \frac{FP}{TN + FP} \tag{5}$$

$$\text{False Acceptance Rate (FAR)} = \frac{FN}{TP + FN} \tag{6}$$

$$\text{Overall Accuracy (OA)} = \frac{TP + TN}{TP + FP + TN + FN} \tag{7}$$

$$\text{HTER} = \frac{FAR + FRR}{2} \tag{8}$$

The evaluation method is based on calculating the Half Total Error Rate (HTER) which is the mean between False Acceptance Rate (FAR) and False Rejection Rate (FRR). False Acceptance Rate (FAR), also called as False Negative Rate (FNR), is the ratio of malicious attempts that were not correctly recognized by the system [22]. False Rejection Rate (FRR), called as False Positive Rate (FPR), represents the ratio of real accesses that were wrongfully classified as spoofing attacks. Sensitivity or True Positive Rate (TPR) or recall is the percentage of number of spoof images getting correctly classified as spoof. Overall accuracy rate is the number of images correctly classified as spoof or original.

A. Case 1: Using MSU MFSD Database

The training dataset contains 30 original images and 40 spoof images. The testing set also contains 30 original images and 40 spoof images. Table 1 shows the experimental results.

Table 1
Performance Evaluation in MSU MFSD Database

Method	*TPR (%)*	*FRR (%)*	*OA (%)*	*HTER (%)*
Proposed	90	13.3	88.5	13.3
IDA + SVM	82.5	16.6	82.8	17.05

From the observations it is clear that the proposed method has shown significant increase in spoof detection rate (TPR) approximately by 7.5% and overall accuracy (OA) approximately by a rate of 5.7%. Through proper feature ranking and selection, only the best features are fed to the classifier so that the classification accuracy can be increased. Because of that, the False Rejection Rate (FRR = 13.3%) and the False Acceptance Rate (FAR=10%) have been considerably reduced when compared with the existing system (FRR = 16.6% and FAR = 17.5%). So the HTER is also considerably reduced in the proposed method.

B. Case 2: Using Idiap Replay-Attack Database

The training set of data contains 30 original and 40 spoof images. The testing set of data contains 50 original images and 50 spoof images. Table 2 shows the results.

Table 2
Performance Evaluation in Idiap Replay-Attack Database

Method	*TPR (%)*	*FRR (%)*	*OA (%)*	*HTER (%)*
Proposed	86	8	89	11
IDA+SVM	78	16	81	19

The output shows that the proposed method has achieved great results in spoof detection rate (86%) and overall accuracy rate (89%). The False Acceptance rate (FAR = 14%) has been considerably reduced in the proposed system compared to the existing system (FAR = 22%). The main observation after performing this experiment is that the performance of the multiclass SVM classifier showed promising results, with a half total error rate minimized to 11%.

5. CONCLUSION

Anti-spoofing is becoming a vital issue in biometric authentication systems. It is highly critical for a system to correctly discover and prevent attackers especially with the diverse variation of attacks. In this work, a face spoof detection method based on Image Distortion Analysis (IDA) and Colour Texture Analysis was proposed. Feature ranking and selection is done to choose the best features. A single multiclass SVM classifier is used for classification. The public domain databases MSU MFSD and Idiap Replay-Attack was used in this work for conducting experiments. The evaluations conducted on the MSU MFSD database shows that the proposed method achieved best performance with a higher True Positive Rate (TPR=90%) and a much lower error rate (HTER = 13.3%).The evaluations conducted on Idiap Replay-Aattack database shows that the proposed system has achieved much better performance with a high True Positive Rate (TPR=86%) and a much lower error rate (HTER = 11%).

The future works on this study include :i) collect a large and representative database that contains the user demographics like age, gender. ii) consider multiple frames from a video for training and testing. iii) evaluation can be conducted in cross-database scenario.

REFERENCES

[1] JAVIER GALBALLY, SEBASTIEN MARCEL and JULIAN FIERREZ, “Biometric Antispoofing Methods: A Survey in Face Recognition”, Digital Object Identifier 10.1109/ACCESS.2014.2381273, 2, 1530–1552, 2014.

[2] Di Wen, Hu Han and Anil K. Jain, “Face Spoof Detection With Image Distortion Analysis”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY,10,746–761,2009.

[3] Galbally, J., R. Satta, M. Gemo, and L. Beslay (2014). “A jrc case study in 3d face recognition.”URL https://ec.europa.eu/jrc/en/publications-listJRC94041.

[4] Lin Sun, Gang Pan, Zhaohui Wu and Shihong Lao, “Blinking-Based Live Face Detection Using Conditional Random Fields”,in Proc. AIB, 2007, pp. 252–260.

[5] K. Kollreider, H. Fronthaler, M. I. Faraj, and J. Bigun, “Realtime face detection and motion analysis with application in ‘liveness’ assessment,” IEEE Trans. Inf. Forensics Security, Vol. 2, No. 3, pp. 548–558, Sep. 2007.

[6] W. Bao, H. Li, N. Li, and W. Jiang, “A liveness detection method for face recognition based on optical flow field,” in Proc. IASP, Apr. 2009,pp. 233–236.

[7] J. Yang, Z. Lei, S. Liao and S. Z. Li, “Face liveness detection with component dependent descriptor”, in Proc. IJCB, 2013, pp. 1–6.

[8]]. J. Galbally, S. Marcel and J. Fierrez, “Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition”, IEEE Trans. Image Process,23, pp. 710–724,2014.

[9] T. Wang, J. Yang, Z. Lei, S. Liao and S. Z. Li, "Face liveness detection using 3D structure recovered from a single camera", in Proc. ICB, 2013, pp. 1-6.

[10] Paul Viola and Michael J. Jones, "Robust Real-Time Face Detection", International Journal of Computer Vision, 57, pp. 137–154, 2004.

[11] O. H. Jensen, "Implementing the viola-jones face detection algorithm", in Informatics and Mathematical Modelling, 2008,pp. 1–33.

[12] J. S. Pierrard and T. Vetter, "Real-time hand tracking using the viola and jones method", Proc. International Conference on Image and Signal Processing, 2005.

[13] S. A. Shafer, "Using color to separate reflection components," Color Res. Appl., Vol. 10, No. 4, pp. 210–218, 1985.

[14] F. Crete, T. Dolmiere, P. Ladret and M. Nicolas, "The blur effect: Perception and estimation with a new no-reference perceptual blur metric", Proc. SPIE, 6492, pp. 64920I, 2007.

[15] P. Marziliano, F. Dufaux, S. Winkler and T. Ebrahimi, "A noreference perceptual blur metric", in Proc. ICIP, 3, pp. III-57III-60, 2002.

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

[17] T. Ojala, M. Pietikäinen, and T. Mäenpaa, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," *IEEE Trans. Pattern Anal. Mach. Intell.*, Vol. 24, No. 7, pp. 971–987.

[18] R. Lukac and K. N. Plataniotis, *Color Image Processing: Methods and Applications*, Vol. 8. New York, NY, USA: CRC Press, 2007.

[19] Kobics, K. C. and Y. Singer, "On the algorithmic implementation of multiclass kernel-based vector machines.",Journal of Machine Learning Research, 2001, pp.265292.

[20] Chih-Wei Hsu and Chih-Jen Lin, "A Comparison of Methods for Multiclass Support Vector Machines", IEEE TRANSACTIONS ON NEURAL NETWORKS, 13, pp.415-425, 2002.

[21] I. Chingovska, A. Anjos and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing", Proc. IEEE BIOSIG, 2012, pp.1–7.

[22] Keneilwe Zuva and Tranos Zuva, "EVALUATION OF INFORMATION RETRIEVAL SYSTEMS", International Journal of Computer Science and Information Technology,4, 2012.

[23] T. Wang, J. Yang, Z. Lei, S. Liao, and S. Z. Li, "Face liveness detection using 3D structure recovered from a single camera," in *Proc. ICB*, Jun. 2013, pp. 1–6.

[24] Z. Zhang, D. Yi, Z. Lei, and S. Z. Li, "Face liveness detection by learning multispectral reflectance distributions," in *Proc. FG*, Mar. 2011, pp. 436–441.

[25] J. Komulainen, A. Hadid, and M. Pietikäinen, "Context based face antispoofing," in *Proc. BTAS*, Sep./Oct. 2013, pp. 1–8.

[26] G. Chetty, "Biometric liveness checking using multimodal fuzzy fusion," in *Proc. IEEE FUZZ*, Jul. 2010, pp. 1–8.