IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, August 2023

Detection of Real and Spoofed Faces based on Handcrafted Features using Support Vector Machine

Dr. Shivaprasad. K. M[1] and Meena[2]
Professor, Department of Electronics and Communication Engineering,
R L Jalappa Institute of Technology, Doddaballapur, India[1]
Technical Assistant, Department of ECE, Gitam University, Bangalore Campus, India[2]

Abstract: *Infringement in biometric authentication is one of the crucial concern in today's scenario. Many of the robust authentication systems fall prey to crude spoofing attacks and their performance had been drastically dropped due to several unseen attacks owing to technological advancementsavailable at no cost. The objective of the proposed work is to design a robust spoof detection system which can sustain even the worst undetectable unseen interference that can fool a state of art authentication technique. The work comprise of four stages and consists of removing artifacts (contrast measurement and correction system, filtering with automatic face cropping), extracting the optimum features conventionally (statistical coarse and the window based fine features), reducing the dimensionality of the feature vector (Principal Component Analysis) and the classification system (Support vector Machine). The 75:25 percent train: test analysis showed that selecteddimension of the handcrafted features usingGaussian kernel of Support Vector Machinewas able to produce remarkable results over IDIAP dataset*

Keywords: Face Biometric, spoofing attacks, real and the fake images, contrast measurement and correction, statistical features, automatic face cropping and principal component analysis.

I. INTRODUCTION

Extracting handcrafted features from images for classification is not a new approach. Today deep learning and machine learning approaches have overtaken the traditional approach. In conventional approach, the hard part lies in optimally selecting the best feature extraction technique to broaden the disparities between classes and reducing the time plus computational complexity. Both the former and the later techniques used for feature extraction have pros and cons and requires effective pre-processing of the input data. Several noises including gaussian, speckle, shot and white noises tends to interfere as a cause of sensor materials, electronic devices and complex circuits. Illumination effects is another cause of concern when traditional features are used. Images subjected to improper lightening without efficient preprocessing may not be able to provide distinguishable features to discriminate the bonafied images from the images which are made to alike them. Enhancement using Laplacian filters [1], noise removal using normal and modified Divergence of Gaussian filtering (DOG) [2], eliminating partial light effects using gamma correction [3] are some preprocessing techniques found in the literature.

A spoofed face is pruned to variety of distortions which carries surface distortions, distortion through color, overlapping of digital grids, and face misalignments due to micro and macro bends in the original photo images [4]. On the other hand, motion analysis requires accurate segmentation of the face region along with upliftment of facial landmark points [5-6]. The key points are successful in handling print attacks at the cost of estimation through successive frames analysis but lacks ability to compensate the replay attack. Many work had been concentrated on textural information of the image, but they failed to capture the liveliness (e.g. blood movement in the facial nerves or movement over the face skin) properties over the face region thereby lacking the generalization capability [7-8]. These techniques were fast but remained restricted to dedicated dataset which they considered. For a chrominance image, the depth information is substantial and its estimation requires reliable techniques since attacks tends to diminish the low

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, August 2023

frequency components thus raising the high frequency ones [9-10]. Most of the techniques used over 3D photos make use of this property to distinguish real and fake images.

Our work is concentrated to cover all the above aspects. Most of the distortions especially illumination effects were mitigated by correcting the contrast of the input image for obtaining best quality features. The region of interest (face only) was segmented to as to reduce the background overheads regarding complexity and feature extraction. More than 5000 plus features were extracted using various descriptors to uplift textural, structural and depth details from the images. Experiments were carried to select the best combinations of features from available feature set and the optimum features were chosen. The dimensionality of the selected features was then reduced to considerable extent before inputting it to the classifier.

II. RELATED WORK

The first anti-spoofing dataset specifically designed for research was NUAA (2010) Photograph Imposter Database experimented over 15 subjects with 500 2D images with print attack. Another dataset CASIA-FASD (2012) included three presentation attacks and was an extension to the NUAA dataset with increased complexity. A complete set with accurate protocol containing 50 printed photos of different subjects was introduced by PRINT- ATTACK dataset (2011) and provided train, test and evaluation samples. More presentation attacks were incorporated in REPLAY-ATTACK (2012) dataset for fair comparison. Other datasets which joined the face anti-spoofing datasets were the MSU-MFSD (2014), MSU-USSA (2016), Msspoof (2015), UVAD (2015), and Replay-Mobile (2016). The latest being introduced in 2019-2022 are WFFD, SiW-M, CASIA-SURF ((2019)), SWAX, CelebA- Spoof, CASIA-SURF (2020), 3D-Mask CASIA-SURF and HiFiMask (2021).

Initially, common techniques focussed onhandcrafted features like LBP [11-12], DoG, SURF,SIFT [13], Wavelet based features and classifier including LDA and SVM. Illumination sensitivities were compensated using different color spaces such as HSV, Ycbcr and other frequency domain spectrums. Due to the fact that fake faces encompasses low or poor image quality, these approaches resulted limited performance. Conventional and temporal based schemes were restricted to single dataset and showed no generalization ability towards cross datasets due to non-matching in features spaces among diverse domain. The temporal methods imply detection of movements due to mouth or eye blinks from consecutive video frames [14-16].

Work suggested in [17] improved detection generalizability using mutual information and discriminating power analysis. They used texture difference as mutual difference based on color between the real and the fake images to obtain inter channel chromatic co-occurrence LBP (CCoLBP) and intra channel facial textures. A softmax classifier was used to discriminate real and spoof images from cross datasets (MSU MFSD, CASIA FASD, Replay Attack, Replay Mobile and OULU-NPU). Similar work was proposed in [18] where CCoLBP was combined with ensemble learning. The HOG-LPQ combination of features to use its blur invariant property over rectangular regions with Fuzzy-SVM classifier was used in [19] to efficiently recognize different genuine and spoofed attacks with low time complexity. Some of the related work employing detection based on color descriptors were introducedin [20-21]. The work proposed in [20] extracted texture information in the Ycbcr domain from color residue obtained using discrete wavelet filter. The high frequency components were processed to obtain a discriminative color residual image. The performance was evaluated over inter and intra dataset samples considering four datasets, FASD, MSU, ROSE-YOUTU and ROSE. Whereas, authorsin [21] mad use of SURF features on individual colorbands of the images. The rotation invariant SURF features were concatenated and reduced indimension (PCA and Fisher vector encoding). The descriptor were obtained around a point of interest on RGB, HSV and YCbCr color spaces using a haarwavelet on a 4x4 blocks or sub-regions. They concluded that their approach with limited training set showed interesting generalization performance.

III. PROPOSED METHOD

The proposed system comprises of pre-processing, feature extraction, dimension reduction and classification. The input real or spoofed image is pre- processed using contrast correction and filtering and the outputs from both the parallel process are averaged. The region of interest (the face region eliminating the background) is found by Bounding Box Algorithm and the face is resized to fixed size for obtaining equal feature dimension. Variety of features are extracted and 2060 values for each face region is obtained using variety of descriptors. The feature length of 2060 elements is

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, August 2023

reduced by two successive stages which includes principal component analysis (PCA) and then averaging of 25 elements obtained using PCA. Finally, the SVM is trained using randomly chosen 75% of samples from the available samples and remaining 25% samples were subjected to test. The following sub-sections deals with all stages in brief:
The IDIAP Replay Attack dataset considered consists of 4000 real and 9950 spoofed images belonging to 80 real and 199 fake subjects respectively converted from videos [22]. We have considered 50 images from each folder subject. The figure 1 and 2 shows real face images and spoofed face images for the same person. The block diagram for the proposed work is shown in the figure 3 below.

Fig.1. Real images extracted from the dataset videos

Fig. 2. Spoofed images extracted from the dataset videos

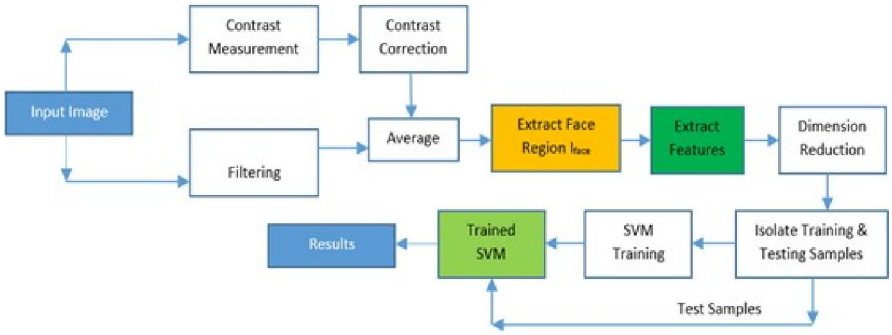

Fig. 3. The proposed system

The efficient preprocessing stage is the heart of this work. Many such patch based and global based contrast measurement methods are listed in the literature. The contrast of the image is influenced by illumination, color, contents, viewing distance, resolution etc. The perceived contrast is the difference measure between the brightest and the darkest point in the image. Tadmor and Tolhurst [23] method uses the modified DoG based filtering method to compute the image contrast and therefore used in this work followed by correcting the contrast. The result showed improved and acceptable contrast over the parent images. The following expressions (1 to 3) were used for contrast correction and the resultis depicted in figure 4. All the color frames R, G andB were subjected independently to contrast measurement and correction.

$$M = 255 * CM \quad (1)$$

$$Factor = 259 * \frac{(M+255)}{(255*(259-M))} \quad (2)$$

$$G = (Factor * (I - 128)) + 128 \quad (3)$$

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, August 2023

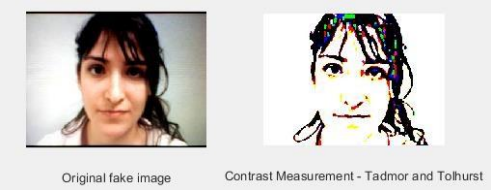

Fig. 4. Contrast measurement using Tadmor and Tolhurstmethod

When using suitable filter to reduce the effect of aliasing and uplifting weak edges, we select Beltrami filter [24] in parallel to the contrast correction and measurement. The filter uses only two tuning parameters, viz. includes the time step for stability and number of iterations. The time step parameter which is usually set to the reciprocal of the squared number of dimension was set to 0.5 and iterations at 20 after experimental analysis. The Beltrami filter have the capability to enhance edges while preserving them. Even though the loss due to filtering effect and the contrast correction is minimum, we considered the mean image obtained from both parallel operation to compensate the loss due to both operations. The mean image was then segmented using Bounding Box algorithm to extractthe face region thus discarding the unwanted background region. Considering C_i and G_i to the images obtained through contrast correction and filtering respectively, the mean image is obtained using the following expression (4).

$$II = {}^{1}[G +] \quad (4)$$

$$- \quad i \quad i$$

As seen from the figure 5, the perceived images in the first and the last column seem alike, but the peaksignal to noise ratio reflects the difference due to theoperations carried to enhance the original image. Forhigher detection accuracy, it is essential to uplift thesignificant features restricted to the region of interest. Also, due to varying face sizes, we resized the region of interest to [120 120 3] dimension for equal feature dimension. Figure 6 represent the extraction of region of interest (face) using the Bounding Box algorithm. The region *Iface* was extracted using bounding box algorithm in MATLAB covers head to neck portion

Fig. 5. The preprocessing stage. Original input image, Filtered image, Contrast corrected image and the Averaged image. The PSNR valuesreflects pixel value changes in each stages.

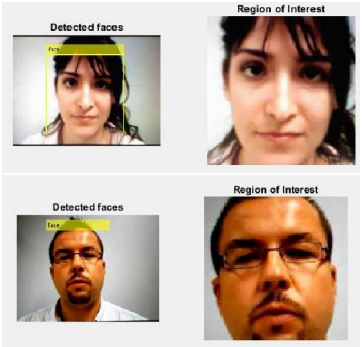

Fig. 6. Region of Interest (FACE) using Bounding Box Algorithm

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, August 2023

We obtained wide variety of fine and coarse featuresto improve the classification accuracy and analyzedthe performance using various combinations of the obtained features. The redundant features were eliminated and optimum features were considered based on the training and testing SVM accuracy. Thefeature set includes the following features:

The *Iface* image was converted to grayscale and 640 features were extracted using Gabor [25]. The parameters used for Gabor filtering were:

Downsampling rows and columns = 39, number of scales and orientations = 5 and 8. Averaging 8 features considering 8 directions, four-second order gray level co-occurrence matrix based features (contrast, correlation, energy and homogeneity) were obtained for 64 intensity levels. First order statistical features as a function of probabilities of pixel intensities in the facial region were extracted from the *Iface* image which basically included mean, variance, standard deviation, skewness and kurtosis

The probability *P* corresponding to each of theintensity level is evaluated by the following expression (11) first and then mean, variance, standard deviation, skewness and kurtosis areevaluated using expressions (5) to (11).

Wavelet coefficients provide fine details of texture

information. Taking into account the property of wavelets, we considered six different mother wavelets for extracting magnitude and energy of wavelet components including three bior (*bior 3.1, bior 3.5 and bior 3.7*), debauchees 3 (*db3*), symlet 3(*sym3*) and *haar* after level one decomposition oververtical and diagonal components. Expression (12) and (13) represents the magnitude and the energy measures. For each of the mother wavelet, the grayscale *Iface* image is decomposed to level 1 wavelet transform.

$$W_E = \frac{1}{p*q}\left(\sum_{r=1}^{p}\sum_{c=1}^{q} ab(W_x)^2\right) \qquad (13)$$

Where, *p* and *q* are the row and column dimension of the wavelet components. W_x is either W_v or W_d andcorresponds to vertical and diagonal components.

Selecting 16 binary levels, we obtained normalized histograms from *RGB Iface* image and the *Lab* color space *Iface* image. The expressions (14) and (15)below are used to extract color features. The color features from *RGB* and *Lab* color space were thenconcatenated.

For *RGB Iface* image,

$$H_{(x \in R,\, G,\, B)} = \frac{1}{M*N} H\left(I_{face}(x)\right)_{(bins = 16)} \qquad (14)$$

For *Lab* I_{face} image,

$$H_{(y \in L,\, a,\, b)} = \frac{1}{M*N} H\left(I_{face}(y)\right)_{(bins = 16)} \qquad (15)$$

These essential features are the novelty of our work.

The color *Iface* was decomposed to 4 level using'haar' mother wavelet. LBP features were extracted

from all three frames of original color image and allframes at decomposed levels. The features obtained from all frames of the original image were averaged and similar operation is carried for all decomposed level components. The final feature set is the average from all such components. This ensures that none ofthe detail is lost and thus will help to distinguish between the real and the spoofed image. We considered HOG features on *Iface* image and on each color component of *Iface* image. We combined all four HOG features by averaging them and obtained them with cell size set to [16 16]. The complete feature set consisting of coarse and fine features are indicated in the figure 7 below

A 'Gaussian' kernel with 'L1QP' solver was used in SVM on MATLAB 2021b, i5, 2.17 GHz, 6 core processor, 16 GB RAM and 128 GB SSD. The feature dimension of 2060 was reduced by two subsequent stages, former by selecting significant columns obtained through PCA and later by averaging 25 samples along the dimension. We experimented by selecting number of features from each set. We selected preceding 10 features for training and testing. The samples were segregated into training and testing set with 75% of data for training and remaining 25% of data for testing from each category.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, August 2023

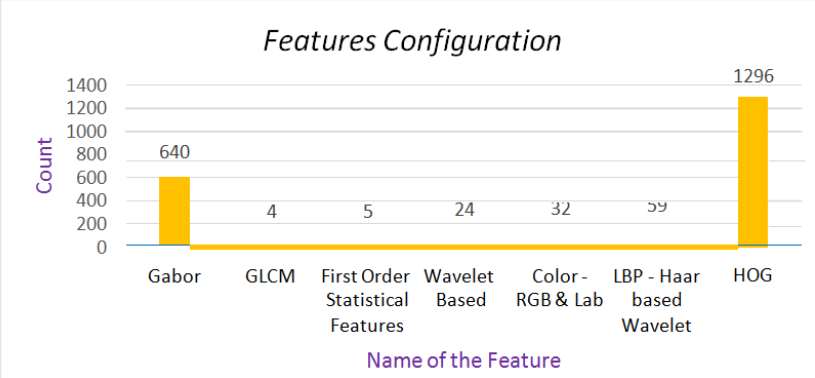

Fig. 7. Dimension of each features

IV. RESULTS AND DISCUSSION

The significant part includes the pre-processing stage involving contrast measurement and correction along with edge preserving filter operation and the traditional coarse (GLCM, Color, First order Statistical, and wavelet features) and patch based (Gabor, HOG and LBP features) quality features. The effect of uneven illumination was mitigated and the edges were secured from the original image without significant loss. The feature extractions operators contributed positively in obtaining a robust feature set. The complexity in terms of time and computation were reduced by reducing the dimension of the features samples. The images belonging to a subject differed with respect to lightning conditions only while the person remaining the same. Therefore, 50 samples were used for each subject (real and spoofed) and so they were reduced to 2 samples using averaging for 25 samples after PCA.

We obtained 100% accuracy in detecting either real or spoofed faces from 25% of the samples used for test purpose. The training and the testing samples were randomly chosen from the set each time the system was run. Depth, chrominance frequency components, textural properties, statistical components are combined so that discriminative values supersedes the common features and the classifier can accurately judge the test samples in the intra-dataset.

V. CONCLUSION

The work proposed here only consider images subjected to replay attack with spoofed images as a result of hand based support conditions and real images from the videos carrying controlled and adverse illumination conditions. An efficient preprocessing, choice of significant features, reduction in dimensionality of selected features and proper tuning of SVM played significant role in achieving best accuracy over the test samples. The proposed work can be tested for other types of unseen attacks and cross datasets. The real world problem keeps altering every day due to advancement in technologies made freely available for creating spoof images. It is thus required to cope with latest problems of unseen attacks that may peep into most robust authentication biometric systems and walk as a freeman. Many such complicated problems are been handled using sophisticated classifiers especially with deep learning models. The real or the spoofed image is directly fed inside and the model is the able to do all those task which are traditionally done exclusively except the classification.

REFERENCES

[1] Chen B., Qi X., Zhou Y., Yang G., Zheng Y. and Xiao B., "Image splicing localization using residual image and residual-based fully convolutional network," Journal of Visual Communication and Image Representation, vol. 73, 2020, Article ID 102967.

[2] Md Rezwan Hasan, S. M. Hasan Mahmud and Xiang Yu Li., "Face Antispoofing using texture based techniques and filtering methods," Journal of Physics: Conference Series 1229, 2019.

[3] Cheng Xin, Wang Hongfei, Zhou Jingmei, Chang Hui, Zhao Xiangmo and Jia Yilin, "DTFA-Net: Dynamic and Texture Features Fusion Attention Network for Face Antispoofing, Complexity," volume 2020, 2020.

[4] Patel Keyurkumar, Han Hu and Jain Anil Kumar, "Secure Face Unlock: Spoof Detection on Smartphones," IEEE Transactions on Information Forensics and Security, volume 11(10), 2016, October 2016, pp. 2268-2283.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, August 2023

[5] Bharadwaj S., Dhamecha T. I., Vatsa M. and Singh R., "Computationally efficient face spoofing detection with motion magnification," in Proceeding of the CVPR Workshops, June 2013, pp. 105–110.
[6] Pan G., Sun L., Wu Z. and Lao S., "Eye blink-based anti- spoofing in face recognition from a generic webcamera," in Proceedings of the 11th International Conference on Computer Vision (ICCV), Oct. 2007, pp. 1–8.
[7] Chingovska I., Anjos A. and Marcel S., "On the effectiveness of local binary patterns in face anti- spoofing," In Proceedings of the IEEE International Conference of Biometric Special Interest Group (BIOSIG), Sep. 2012, pp. 1–7.
[8] Maatta J., Hadid A. and Pietikainen M., "Face spoofing detection from single images using micro-texture analysis," in Proceedings of the International Joint Conference on Biometrics (IJCB), October 2011, pp. 1–7.
[9] Bao W., Li H., Li N. and Jiang W., "A liveness detection method for face recognition based on optical flow field," in Proceedings of the IASP, April 2009, pp. 233–236.
[10] Marsico M. De, Nappi M., Riccio D. and Dugelay J. L., "Moving face spoofing detection via 3D projective invariants," in Proceedings of the International Conference on Biometrics (ICB), Mar./Apr. 2012, pp. 73–78.
[11] Määttä, J.; Hadid, A.; Pietikäinen, M. Face spoofing detection from single images using micro-texture analysis. In Proceedings of the 2011 International Joint Conference on Biometrics (IJCB), Washington, DC, USA, 11–13 October 2011; pp. 1–7. 10.
[12] Freitas Pereira, T.d.; Komulainen, J.; Anjos, A.; De Martino, J.M.; Hadid, A.; Pietikäinen, M.; Marcel, S. Face liveness detection using dynamic texture. EURASIP J. Image Video Process. 2014, 2014, 2. [CrossRef]
[13] Patel, K.; Han, H.; Jain, A.K. Secure face unlock: Spoof detection on smartphones. IEEE Trans. Inf. Forensics Secur. 2016, 11, 2268–2283. [CrossRef]
[14] Kollreider, K.; Fronthaler, H.; Faraj, M.I.; Bigun, J. Real- time face detection and motion analysis with application in "liveness" assessment. IEEE Trans. Inf. Forensics Secur. 2007, 2, 548–558. [CrossRef]
[15] Pan, G.; Sun, L.; Wu, Z.; Lao, S. Eyeblink-based anti- spoofing in face recognition from a generic webcamera. In Proceedings of the 2007 IEEE 11th International Conference on Computer Vision (ICCV), Rio De Janeiro, Brazil, 14–21 October 2007; pp. 1–8.
[16] Sun, L.; Pan, G.; Wu, Z.; Lao, S. Blinking-based live face detection using conditional random fields. In Proceedings of the International Conference on Biometrics (ICB), Seoul, Republic of Korea, 27–29 August 2007; pp. 252– 260.
[17] Peng F., Qin L. and Long M.. "CCoLBP: Chromatic Co- Occurrence of Local Binary Pattern for Face Presentation Attack Detection," 27th International Conference on Computer Communication and Networks (ICCCN), 2018, pp. 1-9.
[18] Peng F., Qin L. and Long M., "Face presentation attack detection based on chromatic co-occurrence of local binary pattern and ensemble learning," Journal of Visual Communication and Image Recognition, volume 66, 2020, 102746.
[19] K. Mohan, P. Chnadrashekhar and K. V. Ramanaiah, "Object-specific face authentication system for liveness detection using combined feature descriptors with fuzzy- based SVM classifier," International Journal of Computer Aided Engineering and Technology, volume 12(3), 2020, pp. 287-300.
[20] Du Yuting, Qian Tong, Xu Ming and Zheng Ning, "Towards face presentation attack detection based on residual color texture representation," Security and Communication Networks, Volume 2021, 2021.
[21] Boulkenafet Zinelabidine, Komulainen Jukka and Hadid Abdenour, "Face Antispoofing using Speeded-Up Robust Features and Fisher Vector Encoding," Signal Processing Letters, IEEE, volume 24(2), 2017, pp. 141-145.
[22] Pereira Tiago de Freitas, Komulainen Jukka, Anjos Andre, Martino Jose Mario De, Hadid Abdenour, Pietikainen Matti and Marcel Sebastien, "Face liveness detection using dynamic texture," EURASIP Journal on Image and Video Processing, volume 2, 2014.
[23] Tadmor Y. and Tolhurst D., "Calculating the contrasts that retinal ganglion cells and LGN neurones encounter in natural scenes," Vision Research, volume 40(22), 2000, pp. 3145–3157.
[24] Wetzler A. and Kimmel R., "Efficient Beltrami Flow in Patch-Space," in Scale Space and Variational Methods in Computer Vision. SSVM 2011. Lecture Notes in Computer Science, volume 6667. Springer, Berlin, Heidelberg, 2012, pp. 134-143.
[25] Haghighat M., Zonouz S. and Abdel-Mottaleb M., "CloudID: Trustworthy cloud-based and cross-enterprise biometric identification," Expert Systems with Applications, volume 42(21), 2015, pp. 7905-7916.