Face Liveness Detection

Abstract

Face spoofing is considered to be one of the prominent threats to face recognition systems. However, in order to improve the security measures of such biometric systems against deliberate spoof attacks, liveness detection has received significant recent attention from researchers. For this purpose, analysis of facial skin texture properties becomes more popular because of its limited resource requirement and lower processing cost.The traditional method of skin analysis for liveness detection was to use Local Binary Pattern (LBP) and its variants. LBP descriptors are effective, but they may exhibit certain limitations in near uniform patterns. Thus, in this paper, we demonstrate the effectiveness of Local Ternary Pattern (LTP) as an alternative to LBP.In addition, we adopted Dynamic Local Ternary Pattern (DLTP), which eliminates the manual threshold setting in LTP by using Weber's law. The proposed method was tested rigorously on four facial spoof databases: three are public domain databases and the other is the Universiti Putra Malaysia (UPM) face spoof database, which was compiled through this study. The results obtained from the proposed DLTP texture descriptor attained optimum accuracy and clearly outperformed the reported LBP and LTP texture descriptors.

Introduction

Spoofing attacks upon face recognition systems involve presenting artificial facial replicas of authorized users to falsely infer their presence in order to bypass the biometric security measures. Such attacks can be carried out easily by means of printed photographs or digital images displayed on tablet, smart phones, etc. In order to distinguish real face features from fake faces, face liveness detection is a commonly used countermeasure approach. It is aimed at detecting physiological life signs in an identity [1]. Face liveness detection algorithms can be classified into two methods: intrusive and non-intrusive [2]. In intrusive methods, the involvement of the user is required to exhibit certain response to the system such as rotating head, performing few actions or mouth movement by uttering some words according to the system's instructions. While in non-intrusive methods, the system does not require any user involvement nor are users required to give any performance in any manner for liveness detection.Furthermore, these two methods are subdivided into three categories. The first category includes analysis of skin properties and frequency reflectance from the texture of the presented face in front of the sensor. In other words, for this approach, face liveness detection is carried out via analyzing and differentiating textural properties of real skin from spoof counterparts. The second category involves the use of dedicated sensors that can detect the evidence of liveness such as infrared or thermal cameras are deployed. However, such devices are expensive and thus the approach is often limited to highly secure applications. The third category of face liveness detection schemes is based on challenging response methods or motion analysis.For this approach, the liveness detection techniques are based on actions that are deliberately performed by the user in front of the cameras according to the system's instructions, such as head and lip movement. This approach may be viewed as intrusive to the users as they are required to be cooperative with the system. It also involves complicated liveness detection algorithms that would exhume the computing resources [3–5]. In recent research, non-intrusive analysis that falls under the category of skin texture analysis has been shown to be very effective for face liveness detection. For extraction of texture features, a number of algorithms have been proposed to achieve a good classification rate.

Experimental Setup

Experimental SetupIn this subsection, we evaluate the performance of the proposed method on our collected UPM face spoof database [26] and, for comparison, we adopt three publicly available databases: CASIA Face Anti-Spoofing Database [27], the Replay-Attack database [28] and the NUAA database [11] face spoof database. The details of the all the databases are discussed below. Face liveness detection is a binary classification problem, in which the result must be either positive (genuine face) or negative (spoof face). The Support Vector Machine (SVM) with liner kernel was chosen to separate positive and negative face spoofing samples. The SVMclassifier with linear kernel is used for each training dataset of all the databases with parameters optimized by cross-validation.The tenfold cross validation is used in every experimental setup with a fixed value of optimal cost (C = 10) and applied on UPMface spoof, CASIA, Replay-Attack and NUAA databases. Furthermore, the proposed method is compared to a single scale technique, namely LTP [29]. The value of patch size P, and radius R for LTPP, R and DLTPP, R were set as eight and two, respectively, for each pattern window. Through both techniques, we computed a 59-bin histogram for normalizing the values of the image.For evaluating and obtaining high performance from both feature descriptors, we applied six different threshold values for LTP for evaluating the developing dataset and obtaining the best threshold value for calculating the difference in patterns between live face and spoof face image. The histograms are computed from the feature extraction stage and then passed to an SVM for classification into the fake and real faces. In all experiments, the performance is measured in accuracy of system, Half Total Error Rate (HTER), False Acceptance Rate (FAR) and False Rejection Rate (FRR) in percentage.

UPM Face Spoof Dataset

The UPM face spoof database is collected and compiled during this research work. In our experiment, we follow the standard of data gallery independence in which the first 10 subjects are utilized for training dataset and the images of the remaining 20 subjects are utilized for testing the model. The training and developing set consists of 4500 genuine sample images, and 18,000 sample images are utilized to develop the testing dataset. For spoof attacks, 1500 sample images from all type attacks are designed per subjects. In this manner, 7500 samples images are utilized for training and developing datasets, while the remaining 30,000 fake sample images of 20 subjects are used for testing protocol. These 30 participants are from different ethnicities, between the ages of 20 and 50. Facial images were frontal shots captured using a single view camera, with spatial resolution of 1440 1080 pixels.

The imaging and recording conditions was an indoor environment under uncontrolled illumination. During each session, several variables were considered such as facial expressions, eye blinks, and wearing a scarf. The high resolution image consumes more memory with high computation and time. Therefore, we cropped the region around the frontal faces to 345 400 resolution, while retaining the maximum quality for printing photographs. Fake faces played a very important role in enhancing the challenges for face anti-spoofing algorithms.

For this purpose, the spoof database is compiled based on variations in terms of textures. We have introduced four different types of paper material in photo attacks: common A4, matt, laminated, and without lamination paper. Furthermore, this study utilized different digital screens such as iPhones, laptops, and tablet PCs for different resolution quality attacks. To make the collected database more challenging in terms of attacks, the images are captured from different distances. Tilted and bended images are also captured in order to increase the level of difficulty.

NUAA Dataset

The publicly available NUAA Photograph Imposter Database contains images of both real client access and photo attacks. The face image of each individual is collected in three different sessions, with an interval of approximately two weeks, whereby in each session, the environmental and illumination conditions are varied. There are 500 images for each subjects' recording. The images in the database are captured using conventional webcams, with resolution of 640 × 480 for 15 subjects. Even subjects that appeared in test and training sets are quite different. As it is explained in [11], six out of nine subjects do not appear in the training set for live human case and six out of 15 subjects do not appear in the training set for photo case.

Replay-Attack Database

photo The Replay-Attack database consists of real access and spoof attacks of 50 subjects. The database was comprised of a total of 1200 video recordings. These included real attempts, print attacks, phone attacks and tablet attacks of 200, 200, 400 and 400 videos, respectively. The dataset is subdivided into three sets named the training, development and testing set. Identities for each subset were chosen randomly, but do not overlap, i.e., people that are on one of the subsets do not appear in any other set. The training subset contains 360 videos of 60 real access and 300 videos of attacks. The development (validation) set was comprised of 360 videos of 60 real and 300 attack attempts. The testing group consist of 480 videos of 80 real-access and 400 attack videos. For performance evaluation, the train set utilized to train the classifier and typically the usage of the development set was used to adjust the parameters of classifier for good performance. For evaluating the performance of a model, the test set is intended to be used.

Conclusions

This paper introduced a new texture descriptor known as Dynamic Local Ternary Pattern (DLTP) in the face liveness detection method. By following Weber's law, in DLTP, the threshold value sets dynamically instead of by a manual setting. Comparison of DLTP is performed with Local Ternary Pattern (LTP) and systematically examined and compared these two techniques in relation to variation of their threshold values. For benchmarking, the performance evaluation is carried out on both publicly available face spoof databases (NUAA, Replay-Attack and CASIA), and our self collected UPM face spoof database. A best threshold value of LTP is utilized to compare the performance of DLTP for face spoof attacks.

The comparative analysis of both techniques also shows that DLTP out-performed LTP and other state-of-the-art approaches for face pattern analysis in a face liveness detection method. The dynamic threshold in DLTP was found to be more robust for noise with a central pixel value and invariance with respect to illumination transformation and texture variations as compared to LTP and other texture descriptors

REFERENCES

1. Chingovska, I.; Nesli, E.; André, A.; Sébastien, M. Face Recognition Systems under Spoofing Attacks. In Face Recognition across the Imaging Spectrum; Bourlai, T., Ed.; Springer: Berlin/Heidelberg, Germany, 2016; pp. 165–194.

2. Parveen, S.; Ahmad, S.M.S.; Hanafi, M.; Azizun,W.A.W. Face anti-spoofing methods. Curr. Sci. 2015, 108, 1491–1500.

3. Yi, D.; Lei, Z.; Zhang, Z.; Li, S.Z. Face anti-spoofing: Multi-spectral approach. In Handbook of Biometric Anti-Spoofing; Marcel, S., Nixon, M.S., Li, S.Z., Eds.; Springer: London, UK, 2014; pp. 83–102.