*UDC 004.021*

# NEW ROBUST FACE ANTI-SPOOFING TECHNIQUE

Z.T. KHUDOYKULOV, Sh.Z. ISLOMOV, L.U. DAVRONOVA, U.R. MARDIEV

*Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Republic of Uzbekistan*

*Submitted 20 March 2019*

**Abstract.** Face recognition is one of the main areas of biometric identification and authentication. Face identification consists of face detection and recognition processes. There are a lot of attacks which they can spoof of faces on face detection process. In this paper all attack points between camera and user application are given. According to the attack points, there are three types of anti-spoofing methods. Based on feature level techniques robust anti-spoofing technique is proposed. When intruder uses photo of the registered person, proposed anti-spoofing technique easily detects. This anti-spoofing technique detects fake face based on pixel value between face and background space.

*Keywords:* face detection, face recognition, face identification, spoofing, sensor, anti-spoofing, score-level.

## Introduction

Identification and authentication techniques based on face are widely used in access control systems of organization. Face identification consists of two processes: Face detection, Face recognition. Face detection is a process finding face gradients and extraction faces from images. Based on detected faces are recognized person. Face detection and recognition processes is presented in Fig. 1.

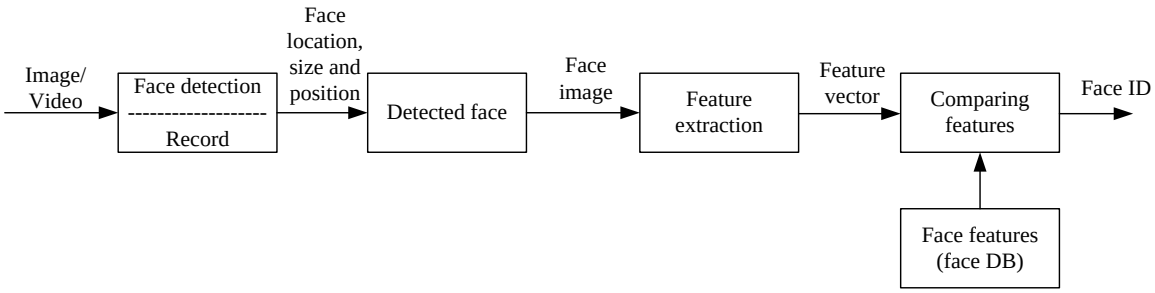



Fig. 1. Face detection and recognition processes

Here, first image is captures from web camera or video. Face detection detects faces from image and features which are extracted from detected faces. Extracted features compares with stored parameters in face database (face DB).

## Attack points

These processes are presented without any attacks. Also, there are a lot of types of attacks which is disturbed identification systems. In [1] eight attack points between scanner and identification applications is given. The main components of face identification system are given in Fig. 2.

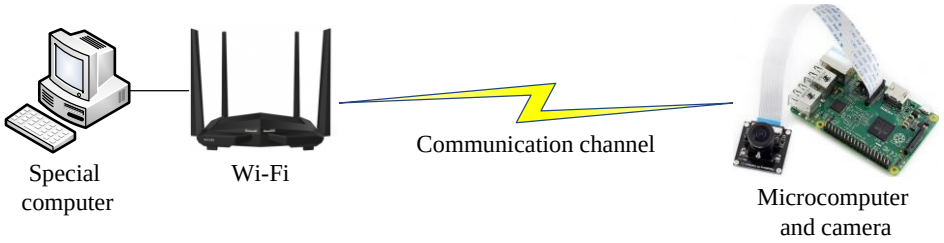



Fig. 2. Face identification system using microcomputers

The camera captures image and Wi-Fi, which supports microcomputer send it over the wireless communication channel. A special computer, which is used to detect faces and extract facial features to identify a person. Here, attack points are in web camera, communication channel and special computer. In Fig. 3 all attack points are given.

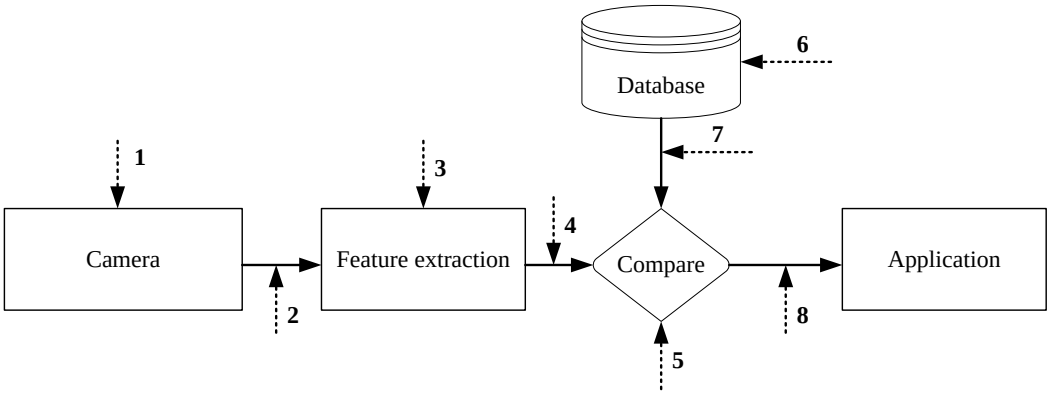



Fig. 3. Attack points

Point 1 attacker sends fake face image (photo, video or 3D mask) to the camera. Camera takes fake face image and sends to the special computer over the communication channel. For protection from spoofing faces anti-spoofing methods are used [2].

Point 2 captured image from camera sends to the special computer for preprocessing over the wireless channel. Channel is protected with cryptographic algorithms, but there are many cryptanalysis methods [3], which can interrupt encrypted packets. For protection from these attacks types strong and combined cryptographic methods are used.

Point 3, 4, 5, 6, 7 is directed to attack computer systems, programs and databases. Monitoring, filtering and access control tools are used for protection.

Point 8 these types of direct attacks to change packets, which saved identification results (like point 2).

## Proposed method

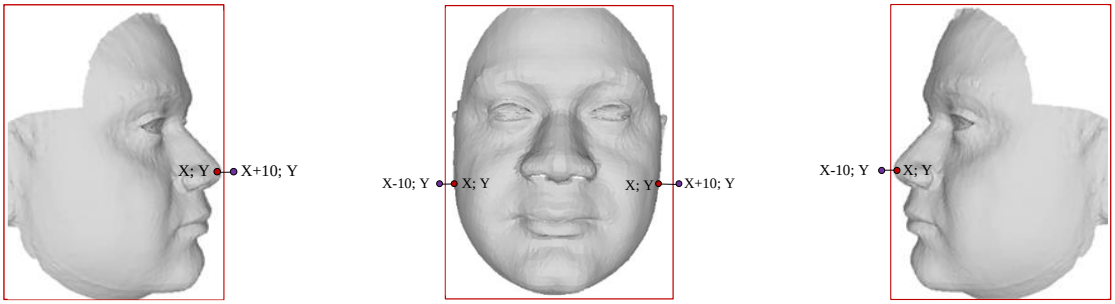
Three types of detection methods from attacks are used to detect spoofed faces: sensor, feature and score level techniques.

In sensor-level techniques special hardware to detect spoofing is used. These methods add some special device to the sensor in order to detect particular properties of a living trait (e.g., facial thermogram, blood pressure, fingerprint sweat, or special reflection properties of the eye).

In feature-level techniques special software to distinguish between real and fake traits which are extracted from the biometric sample are used. For instance, from just one single high resolution image of a face we may perform both face and iris recognition. In this particular case, a multimodal strategy is being applied at the feature extractor level, with no need of any additional hardware or sensing device.

Score-level techniques are used when two-type detection methods fall out. This technique is used in score level. For example, second type of biometric method is used for detection spoofing, or studied results of other type of anti-spoofing methods.

Proposed anti-spoofing pixel-based method is developed on feature-level techniques. When an attacker tries to use fake face photo, pixel based anti-spoofing method detects it easily. In this method comparing the background of the detected face and face gradients is used. In real face identification systems without spoofing background image and face gradients changes over time. If these pixels do not change, it means that face image is spoofed.




*a* *b* *c*

Fig. 4. Different views of faces: right (*a*), front (*b*), left (*c*)

In [4] triangle method for faster and accurately face detection is proposed. After detection face regions, we can distinguish pixel values between face space and background space. The value of *X* coordinate from face and value of *X*+10 coordinate from background comparison is shown. 3 positions of the faces are viewed in this method.

1. *Right.* In left side-face, in right side-background image pixels are situated (Fig. 4, *a*). Here, $A(X;Y)$ is detected from face space and $B(X+10;Y)$ is detected from background space. By $I=|A-B|$ formula is calculated differences between *A* and *B*. After 0,5 second is computed $I_1=|A-B|$. If following condition is done, then this face is real, else, spoofed face.

$|I - I_1| \geq 10$;

$A(X,Y)$ point in face;

$B(X+10,Y)$ point in background image;

$I=|A-B|$;

$I_1=|A-B|$ after 0,5 second;

$|I - I_1| \geq 10$ is real face, else fake.

2. *Front*. Here is applied Right and Left methods (Fig. 4, *b*).

3. *Left*. In right side-face, in left side-background image pixels are situated (Fig. 4. *c*). Here, $A(X,Y)$ is detected from face space and $B(X-10,Y)$ is detected from background space. By $I=|A-B|$ formula calculates differences between *A* and *B*. After 0,5 second is computed $I_1=|A-B|$. If following condition is done, then this face is real, else, spoofed face.

## Comparison and discussions

Proposed anti-spoofing method was analyzed with IQA [5], IDA [6] and DNN [7] methods. IQA (Image Quality Assessment) detects and finds spoofed faces based on image quality. IDA (Image Distortion Analysis) detects spoofed faces based on image distortion. DNN (Deep Neuron Network) detects spoofed faces based on spoof face databases. DNN presents high result, but it takes more time and resource to train face databases, also, it is difficult to collect spoofed faces. Presentation of accuracy of anti-spoofing techniques is in table 1.

Table 1. **Comparison of anti-spoofing techniques**

| Method | IQA | IDA | DNN | Proposed method |
|---|---|---|---|---|
| Accuracy | 0,86 | 0,9 | 0,98 | 0,95 |

## Conclusion

In one of the situations, the spoofed face was detected, and it was a fake face image. By applying this method for detecting fake faces in face recognition, the system is protected from spoofing without any special hardware or second type of biometrics.

## References

1. Rubal J., Chander K. // Int. J. of Advances in Scientific Research 2015. Vol. 1 (07) P. 283–288.
2. Galbally J., Marcel S., Fierrez J. // IEEE Access. 2014. T. 2. C. 1530–1552.
3. Moabalobelo T., Nelwamondo F., Tsague H. D. Survey on the cryptanalysis of wireless sensor networks using side-channel analysis. 2012.
4. Malikovich K.M. [et al.] // The J. of Multimedia Information System. 2018. Vol. 5. №. 1. P. 15–20.
5. Hanimol T.M., Vidhushavarshini S. Bio-Spoof and Anti-Spoofing Detection Based on IQA. 2015.
6. Wen D., Han H., Jain A.K. // IEEE Transactions on Information Forensics and Security. 2015. Vol. 10. №. 4. P. 746–761.
7. Wang M., Deng W. Deep face recognition: a survey. 2018.