Face anti-spoofing methods

Sajida Parveen[1,3,*], Sharifah Mumtazah Syed Ahmad[1,2], Marsyita Hanafi[1] and Wan Azizun Wan Adnan[1]

[1]Department of Computer and Communication Systems Engineering, and
[2]Wireless and Photonic Networks Research Centre of Excellence, Universiti Putra, Malaysia
[3]Department of Computer Systems Engineering, Quaid-e-Awam University of Engineering, Science and Technology, Nawabshah, Pakistan

In recent years, facial biometric systems have received increased deployment in various applications such as surveillance, access control and forensic investigations. However, one of the limitations of face recognition system is the high possibility of the system being deceived or spoofed by non-real faces such as photograph, video clips or dummy faces. In order to identify the spoofing attacks on such biometric systems, face liveness detection approaches have been developed. Thus, the current approach is to integrate liveness detection within facial biometrics by using life sign indicators of individual features. This article presents a review of state-of-the-art techniques in face liveness detection, which are classified into two groups, namely intrusive and non-intrusive approaches. Here, each technique is discussed in terms of its implementation, strengths and limitations, as well as indications on possible future research directions that can be studied.

Keywords: Biometrics, face recognition, intrusive, liveness detection, non-intrusive.

BIOMETRICS refers to technologies that measure and analyse human body characteristics[1]. Biometrics traits can be categorized into two classes, namely physical characteristics, such as fingerprints, faces or iris patterns and behavioural characteristics such as voice, signature or walking patterns (gait). However, one of the most predominant challenges in many biometric recognition systems is the possibility of identity theft, which is conceptually known as spoofing attack. Some stolen biometrics data can be easily exploited and mimicked by impostors to gain unauthorized access to the biometric system, without the consent of the genuine user. Examples of spoofing attacks on biometrics systems include the use of artificial fingers, contact lens with retinal patterns and recorded voice. Research efforts on identification of spoofing attack have been made from various perspectives. In this article, the state-of-the-art spoofing identification techniques for facial biometrics based on liveness detection are presented.

Generally, fake faces can be categorized into two classes: positive and negative. The positive class, also known as the genuine face, has limited variation, whereas the negative class includes the spoof faces on photographs, dummy or recorded videos. Figure 1 shows examples of fake faces made of silica gel, rubber, photo and video replay[2,3].

Facial biometrics spoofing techniques involve placing genuine photographs or dummies, playing video recording etc. in front of the camera. A human photograph represents planar objects with only one static facial expression. However, it lacks the three-dimensional (3D) information and provides less physiological clues than videos[3]. These limitations of still photographs are often exploited in liveness detection for facial biometrics. However, the challenges in facial detection increase for spoofing attacks that involve the use of video cameras. Nowadays, videos of a genuine user with facial expressions, eye blink and head movement can be easily captured using high quality cameras. As far as 3D structure is concerned, a 3D corporeal model of a user has detailed 3D information that photos and videos do not possess. The biometric system can be spoofed by using a 3D corporeal model which is known as synthesis attack. Dummy models can usually reproduce rigid head movement by rotation but cannot imitate the lip movement, eye blink and facial expressions[3,4].

Recently, studies on the face liveness detection have been widely explored in order to tackle the problem of spoofing attacks. Face liveness detection involves a process of verifying whether the face image presented to recognition system is real (i.e. alive) specimen or has been reproduced synthetically and is thus fraudulent.

This article mainly describes the state-of-the-art techniques in face liveness detection, which covers both intrusive and non-intrusive methods. It includes description on life sign classifications and provides critical review in terms of the financial and technical implementation of various techniques. The remaining article includes review on literatures according to the face liveness detection system architecture, categorization of face anti-spoofing techniques, anti-spoofing measures and discussion and conclusion.

Facial biometric liveness detection system architecture

The basic block diagram of a face liveness detection system is shown in Figure 2. To use an anti-spoofing system,

*For correspondence. (e-mail: engr_sajida@hotmail.com)

a user is required to present the relevant biometrics trait to the sensor, which is in this case a camera. The captured facial images is preprocessed into an acceptable form (e.g. such as through normalization and noise removal techniques) as such distinct 'live' facial features can later be extracted at the feature extraction module. The output of the feature extraction is a biometric template which contains prominent features which are able to distinguish live samples from spoofed counterparts. Only live samples will be processed for biometric identifications, whereas spoof authentication attempts are automatically rejected.

Sensor

A variety of acquisition sensors has been studied in different literature. Usually, the same type of sensors is used to provide input samples into the face liveness detection system and facial biometrics. Visible light cameras are among the most commonly used devices, as they are cheaper, faster, higher in resolution and easy to use. However, such cameras are limited to capturing only images that are in visible light spectrum[3,5–26]. In addition, several experiments have also utilized thermal and 3D sensors for face liveness detection[25,27,28]. Thermal sensors are not limited to only visible spectrum; hence, they can capture objects in dark area. However, interpreting the images can be a difficult task. In addition, the sensors are very expensive, hindering cheap biometrics solution. On the other hand, 3D sensors have high data acquisition rate, independent of ambient light, sub micron accuracy in micro ranges. 3D sensors may be affected by computation, measurement time, cost and quality expected from measurement. Table 1 illustrates a summary of different types of acquisition systems used in the literature for face liveness detection.

Figure 1. Examples of fake facial specimens. From left to right columns are silica gel, rubber, photos and video replay[2,3].

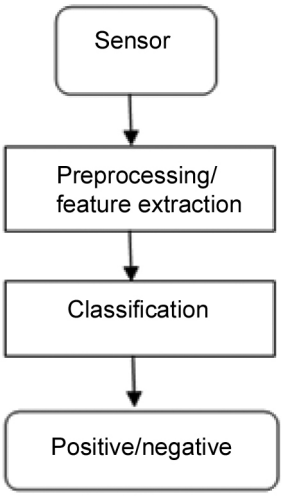

Figure 2. Basic block diagram, a face liveness detection system.

Preprocessing/feature extraction

Face liveness detection systems may be influenced by variability in lighting, pose and picture quality. To increase the effectiveness of liveness detection, several systems have adopted preprocessing. Preprocessing usually involves the removal of noise from the image and occasionally normalization steps in order to enhance the visual appearance of the facial images for feature extraction. The techniques may include smoothing, blurring, sharpen, edge detection or scaling. Then, the preprocessed samples are forwarded to the feature extraction module to extract the salient features in differentiating live specimens from spoof counterparts.

Several of commonly used techniques for feature extraction are presented in Table 2. Many have adopted local binary pattern for feature extraction to generate the users' template[15–18,20,24,26,29]. Detailed review of each technique is discussed here.

Classification

In the liveness detection process, the liveness verification of the queried biometric trait is evaluated by matching the queried feature vectors against those stored in the database collected during the enrolment stage. This process produces a binary response that states the status of the liveness verification, as either accepted as live or rejected as spoof samples. The commonly used classifiers in literature for face liveness detection are summarized in Table 3. It is observed that SVM classifier is one of the

Table 1. Types of sensors

Sensors	Reference
Visible	3, 5–13, 15–19, 21–27, 35, 36
Thermal	25, 27
Optoelectronic 3D scanner	28
MS Kinect (depth camera)	29
Optical stabilized	42

most popular approaches used in the state-of-the-art literatures.

Anti-spoofing categorization

According to the trends in previous studies, approaches on liveness detection can be mainly grouped into two categories, namely intrusive and non-intrusive. For the intrusive method, users are required to respond to the system in a constrained manner such as exhibiting a few actions, uttering words or rotating their head in a certain direction. On the other hand, a user's involvement is not required in the non-intrusive approach. Here, we gain some insight into the existing face liveness detection techniques, with regards to the mentioned categories.

Intrusive liveness detection

The intrusive approach usually requires the users to respond to a few actions specified by the system. The method presented by Frischholz and Werner[30] requires the users to rotate the head in a certain direction according to random instructions generated by the system. The pose estimation algorithm compares those real life movements with specified instructions. This method is capable of denying replay attacks using both photographs and videos and it also remained difficult for attackers to reproduce such different head poses. However, users need to pay attention to the system and follow the instructions; moreover, it is time consuming and may be cumbersome. Another intrusive technique was proposed by Kollreider *et al.*[5], in which users were asked to start uttering the specific digit sequence prompted randomly from 0 to 9 and each lip movement was recognized sequentially. Using optical flow features, the 10 lip movements of users were categorized into 10 different classes trained by SVM classifier. The proposed technique requires no preprocessing; therefore, it involves less computation. However, liveness verification with lip movement, but without audio recording can be attacked by using video or different photograph sequences. Moreover, some multi-modal approaches also employed interactive manner of speaking by using three traits like face, voice, and lip movements to improve recognition accuracy and security[31]. Likewise, Chetty[6] proposed a liveness checking technique based on cross-modal association models, which involve hybrid fusion of acoustic and visual speech correlation features. The technique measures the degree of synchronization between lips and voice extracted from the video. The lip movement used in this approach helps to overcome the problems associated with photos and voice recorded spoofing attacks.

The combination of more than one biometric trait integrated in one system is an innovative technique to enhance the security level of a facial biometrics anti-spoofing system[32]. Extensive research has been conducted to adjust the best way to combine information from several biometric traits, whether it is at the feature level or at the decision level. Multi-level liveness verification (MLLV) framework proposed by Chetty and Wagner[19] uncovered the static and dynamic relationship between voice and face. The MLLV comprised three levels, namely bimodal fusion (BMF), which was used to verify liveness for still photo attack and pre-recorded audio. Second level of liveness detection was based on cross-modal fusion (CMF) that detected video replay attacks and the third level used 3D multimodal fusion (3DF) for synthesis attacks. This system enhanced the face liveness detection and verification at multiple levels for all types of attacks, but somehow user involvement was required for voice trait.

Kant and Sharma[27] presented a method based on fusion of thermal imaging and skin elasticity of human face. In this approach, user was asked to chew and move forehead simultaneously. The correlation coefficients were calculated between the images captured by generic web camera sensor and thermal sensor. The facial skin elasticity was

Table 2. Approaches for feature extraction

Technique/approach	Reference
Conditional random field (CRF)	19, 20, 23, 25
Undirected CRF	10
Linear chain CRF	9
Local binary pattern (LBP)	15, 16, 18, 20, 24, 26, 29
3D Gaussian	21, 36
Raster flow	21
Cross model correlation (latent semantic analysis (LSA), factor analysis CFA	6, 25
Sparse logistic regression	11–13
Second order gradient	42
Focus function	22
Correlation coefficient and discriminant analysis	27
Bidirectional reflectance distribution function (BRDF)	3
Optical flow field	5, 7, 8
First order statistic	28

Table 3. Classification techniques

Classifiers	Reference
SVM	3, 8, 13, 15–17, 24, 29, 35, 42
Binary classifiers	17, 20
DoG filter	11, 12, 18, 19
Linear discriminant analysis	16, 17, 29
Ada boost	5, 9, 23
Weighted fusion	6
Hamming distance	36
Manhattan distance	26
LTV	11
HF	11
Difference degree calculation	7

calculated by using discriminant analysis to differentiate the human skin from other materials such as gelatin, rubber, cadaver, clay, etc. This technique is effective for liveness detection against various spoofing attacks mentioned previously. However, the performance of the system was significantly affected by user's age factor, due to the application of skin elasticity and the requirement of additional expensive hardware, i.e. thermal camera which may be impractical.

Non-intrusive liveness detection

Non-intrusive approach exploits the spontaneous physiological activities of face, such as properties of 3D geometry, eye blinking, skin texture, non-rigid deformation and thermogram. Normally, in non-intrusive systems, users are not aware of which clue of liveness is being used, tested and analysed in the face anti-spoofing system. In other words, the testing is invisible to the end users. The techniques used against photo spoofing attacks are devised based on assumptions that the photograph is a two-dimensional (2D) planar structure which can be differentiated from a live face 3D object. Choudhary *et al.*[33] differentiated between live persons and still photos by employing a structure from motion, which yields depth estimates for each of the features of a face. The drawback of this approach is the difficulty of estimating the in-depth information when the head is in still position and the technique is very sensitive to noise and lighting condition. Also, Lagorio *et al.*[28] proposed a method based on optoelectronic 3D scanning that relies on the assumption that a real face possesses characteristics of 3D structure. The technique was based on the estimation of the first order statistics of the surface curvature. Although surface curvature variations of face in printed pictures and computer screen was not evaluated in their experiment, the advantages of their approach are that, interaction with subjects is not required and it is robust to many spoofing attacks such as 3D synthesis and video playback. The main disadvantage of this approach is the cost since it requires the use of expensive optoelectronic 3D scanner.

Optical flow is the instantaneous speed of a moving spatial object's pixel movements on the projection plane. The instantaneous change rate of intensity on specific points in projection plane is defined as optical flow vector[34]. Bao *et al.*[7] described a method of optical flow in which they analysed the differences and properties of optical flow fields which are generated from 3D objects and 2D planes such as translation, rotation, moving in forward or backward and swing as shown in Figure 3.

It was also analysed that a face is an irregular 3D object, which means the optical flow field generated by head motion and facial expressions is irregular. The first three types of optical flow fields generated by 2D and 3D objects were quite similar but the fourth one for both 2D and 3D objects came up with more differences. On that basis, Bao *et al.*[7] assumed that the test region was a 2D plane. They obtained a reference field from the actual optical flow field data and distinguished between the real face and photograph by measuring the degree of differences between these two fields. No subject involvement and extra hardware were required in this method, but there was a problem with illumination changes that affected the result because this method relies on precise calculation of the optical flow field.

Kollreider *et al.*[8] proposed a method based on light weight optical flow, which is applicable in the face motion estimation based on the structure of a tensor. The basic idea was based on the assumption that a 3D face generates a special 2D motion which was higher in central face parts, e.g. nose as compared to the outer face regions, e.g. ears. Ideally, in terms of liveness detection, the outer and the inner parts move in opposite directions. For this scheme liveness of the face was evaluated by trajectory of several face parts using the optical flow of

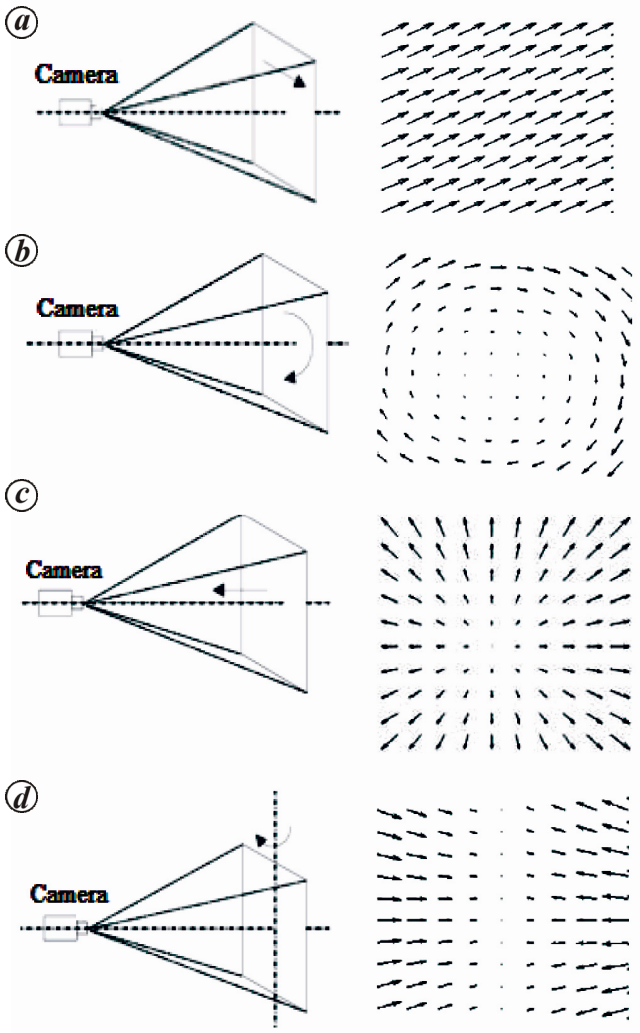

Figure 3. Four basic types of optical flow fields[7]. ***a***, Translation; ***b***, rotation; ***c***, moving forward or backward; ***d***, swing.

lines. The drawbacks of this technique lie in its sensitivity to background and illumination changes.

Several physiological activities can also be used as clues for non-intrusive liveness detection. Eye blink, for example, is a physiological activity which is an essential physiological function of the eyes. The eye blinking is an action that consists of two continuous sub actions that are from open to close and from close to open. The imposter can also produce eye blink motion by using videos of original live face. In order to overcome this problem, Pan *et al.*[9] proposed an eye blink-based face liveness detection approach using an adaptive boosting algorithm. The authors defined the real value of discriminative feature for eye image, called eye closity by measuring the degree of eyes closeness, which was constructed using linear binary classification and iterative procedure. The performance of liveness detection was measured using three types of detection rates. The one-eye-detection rate was first used to measure the ratio of correctly detected blinks to the total blinks in the test data. The second measurement was a two-eye-detection rate, where the ratio of the correctly detected blink activities to the total blinks activities in the test data. The third measurement was clip detection rate, in which the clip was considered as live face if any blink of a single eye in the clip was detected. Pan *et al.*[10] also extended their technique by using undirected conditional graphical model based on eye blink for face liveness detection.

Another eye blink based approach was proposed by Szwoch and Pieniazek[35]. This technique employed the usage of conditional random field (CRF) for eye blinks in face liveness detection. CRF is an interesting mechanism for recognition of context dependent phenomena in time series. The only drawback of CRF is the usage of the symmetrical context time window. One of the studies used the Hamming distance method to analyse the eye movement[36]. This method detected centre point of the eyes in the image sequences and calculated the variations of each eye region using a threshold to separate the fake face from live face. However, their approach is restrained only for photograph attacks.

Li *et al.*[37] described a method based on information of the structure and the movement of a face. The authors performed classification between live and fake faces using Fourier spectra, based on the assumption that high frequency components of photo are less than that of a live face. However, it was sensitive to the lighting effect and vulnerable to spoofing attacks using high quality photographs. Tan *et al.*[11] formulated a binary classification problem using a Lambertian model. The authors proposed two strategies to extract the information of different surface properties of a live human face or a photograph and developed two extensions to the sparse logistic regression model. The first extension was based on sparse low rank logistic regression and the second extension was based on nonlinear models via empirical mapping. In an operational scenario, the illumination conditions may vary greatly and may cause shadows on different parts of the face. These darker regions of the image may influence the spoof detection method. The method was further restricted to only photo spoof. However, to deal with such illumination changes, a technique was proposed by Peixoto *et al.*[12]. The method was an extension of the sparse logistic regression model. Difference of Gaussian (DoG) filter, which is a band pass filter that uses two Gaussian filters with different standard deviations as limits was used. The system does not require any extra hardware and it is capable of dealing with LCD screen based attacks.

An alternative anti-spoofing method is based on a set of low-level feature descriptors, which explores both spatial and temporal information using partial least squares regression, was proposed by Schwartz *et al.*[13]. This method differentiates between live specimens and spoof photo images or videos based on a feature weighting. The descriptors are extracted from a selected number of frames using colour frequency (CF), histogram of oriented gradients (HOG), histogram of shearlet coefficient (HSC), and grey level co-occurrence matrix (GLCM), and then concatenated to compose a feature vector. The experiment was evaluated on FSA video and NUAA datasets. A noticeable limitation in this approach is that the feature descriptor performed differently on the two datasets such as HSC performs better on FSA dataset; however, GLCM provides better results on NUAA dataset.

Local binary pattern (LBP) is a method based on texture analysis. It is a simple yet very efficient texture operator which labels the pixels of an image by thresholding the neighbourhood of each pixel and considers the result as a binary number as shown in Figure 4. LBP texture operator has recently become popular due to its discriminatory power and computational simplicity. Hadid and others[14,15] and Chingovska *et al.*[16] analysed the potential of texture features of the faces based on LBPs and multi-scale LBPs. These approaches provided the result that the system could be very simple and independent from user cooperation. The techniques were used only on photo and video based spoof attacks, while mask and 3D attack still reveal limitations.

Likewise, Pereira *et al.*[17] proposed another LBP-based approach, whereby, LBP operator was used from three

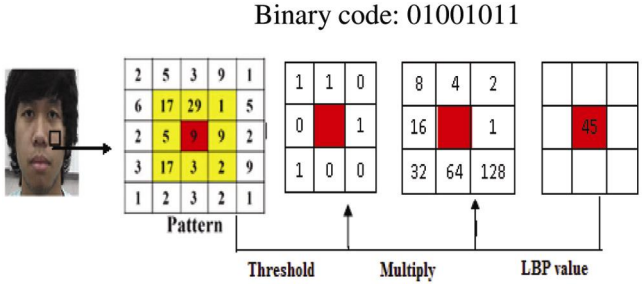

Figure 4. Example of LBP calculation.

orthogonal planes (LBP–TOP) that combines space and time information into a single descriptor with multi-resolution strategy using photographs and videos. The system was designed for detection of both photo and video spoofing attacks but the face detector relies on middle frame only, since it was not error free. In addition, Kose and Dugelay[18] calculated the characteristics of contrast and texture of captured and recaptured face images. In this approach, a DoG filter was used to obtain a special frequency band which provided considerable information to discriminate between live face and photo images and local binary pattern variance (LBPV) was used for feature extraction. The method is simple to implement, illumination invariant and not affected by the rotation of photographs at different angles. However, it was only capable of resisting photo spoofing attacks.

Pan *et al.*[20] presented a real-time face liveness detection system using a monocular camera. This approach was based on a combination of eye blinks and scene context. The authors used outside face clue of scene context called reference scene, which was similar to the background. When a human stands in front of a fixed camera of a face recognition system, the detecting model differentiated the input and reference scene. This technique is secured against dummy, photo, and 3D attacks, but may be vulnerable to video attacks. Kollreider *et al.*[21] proposed a method based on combination of eye blink and 3D properties of faces. The 3D properties such as mouth movement and eye blinking were extracted using 3D Gaussian and raster flow.

The initial means of spoofing the faces in biometric systems includes the use of simple still images. The materials used nowadays by an imposter to spoof can be any still photograph on a paper, fabric or video on a computer screen or a 3D model made up of clay, or gelatin. Most of these materials exhibit some level of spectral sensitivity, which can be detected using infrared or thermal sensors. In addition, this information can be contrasted with the vein map pattern underneath the skin or the temperature profile of a face to differentiate a live face. These sensors are costly for such applications that employ common cameras such as webcams or mobile phone cameras for capturing the biometric traits. More recently, a new approach was proposed by Sooyeon *et al.*[22], whereby the authors exploited the focus function in the camera. To identify the fake faces such as 2D pictures, the authors calculated the variations of pixel values by focusing two images sequentially taken in different focuses.

A summary of the intrusive and non-intrusive approaches in previous studies is presented in Table 4.

The table shows that studies on intrusive approaches are very limited. This is because the techniques for face liveness detection systems are dependent on user involvement such as head and lip movement. The deployment of anti-spoofing based on non-intrusive technique is costly for 3D and dummy attacks.

Anti-spoofing measures

Many types of anti-spoofing measures have been used to make the system robust to spoofing attacks. Smart cards, passwords, enrolling several samples, supervising face recognition process, multimodal biometric system and liveness detection are some examples[38].

In this article, we are focusing on face liveness detection and the liveness indicators are categorized into four classes[39].

(1) *Motion analysis* is based on the assumption that planar object such as 2D face moves differently from real face. The method calculates in-depth information between different frames in a video sequence to identify the real and fake faces.

(2) *Life sign detection* is based on analysing signs of life from the user's face such as eye blinking or lip movement. The algorithms in this class focus on the movement of certain part of the face.

(3) *Texture analysis* exploits the texture patterns that provide detectable information between the texture of real and fake faces. In this approach, features are extracted from the face images or sequence of images showing certain texture patterns that do not exist in the real faces.

(4) *Thermal sensor* uses the temperature profile of faces or vein pattern underneath the skin.

The performances of anti-spoofing systems are measured in the same manner as the biometric authentication systems. The following measures are defined for liveness detection[40].

False reject ratio (FRR) is the rate whereby a live specimen is rejected as a fake attack.

False accept ratio (FAR) is the rate whereby a spoof attack is accepted as live sample.

Failure to acquire (FA) is the rate whereby the system fails to collect samples.

Mean transaction time (MTT) is the average time required by the system to make a decision.

Receiver operating characteristic (ROC) plots are used to choose the operating threshold of the system with full knowledge of the probability of accepting a spoof biometric data as a live sample and vice versa. The ROC is

Table 4. Categorization of techniques

Categories	Types of attacks	Reference
Intrusive	Video	5, 6, 19
	Photographs	27
	Audio	5, 6, 19
Non-intrusive	Videos	8, 9, 12, 13, 16, 17, 20, 21, 23, 24, 26, 29, 28, 35
	Photographs	3, 7, 10–13, 15, 16, 18, 20–22, 24–26, 28, 36, 42
	3D	20
	Dummy	28

also a good evaluation measure for comparing heterogeneous approaches to spoof detection[41]. In Figure 5, we illustrate the categorization of related studies based on the described life sign indicators.

In recent years, a number of benchmark face anti-spoofing databases have been developed to provide a common platform for comparative evaluation of the effectiveness of the various liveness detection systems. With regards to this, several of the databases are available in the public domain. Other self-collected data used by different researchers in studying the accuracy of their face liveness detection techniques are listed in Tables 5–9. We have grouped the studies on the basis of Figure 5 and generated the tables for each life sign indicator. According to that, Table 5 shows that most of the research has been conducted on texture analysis in the last 3 years. This could be attributed to the simplicity in the algorithms coupled with the low cost and compatibility in utilizing any standard camera as the input device.

Other noticeable research that has been performed using lip movement liveness detection is shown in Table 6. Research in this aspect mainly started in 2006 and the task of improving the technique is still in progress.

Tables 7–9 list the anti-spoofing studies based on 3D face properties, head movement and eye blink respectively. It is observed that the studies are rather limited in all three domains.

The proposed anti-spoofing methods in the literature have shown encouraging accuracy results when tested on publicly available databases that measured in half of the total error rate (HTER), area under the ROC curve (AUC), performance of the system means efficiency and equal error rate (ERR) in percentages. We have summarized the achieved results in Table 10 of proposed approaches on publicly available databases such as NUAA, CAISA REPLAY ATTACK, XM2VTS, ZJU, etc.

The current publicly available face spoofing databases that contain images of texture variations have been used extensively in studying the effectiveness of liveness detection in identifying a variety of spoofing attacks from high-quality photo attacks to video-replays. However, due to the lack of the availability of other datasets of different nature in public domain such as those which contain videos of eye-blink, head and mouth movement,

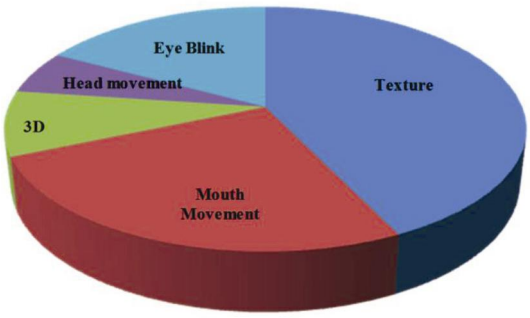

Figure 5. Life sign classification.

Table 5. Texture analysis based liveness detection

Databases	Year	Reference
Replay attack	2012	16
	2013	17
NUAA	2011	12, 13, 15
	2012	18
	2010	11
CAISA	2013	24
Self collected	2010	3
	2013	42
Yale data base	2011	12
XM2VTS	2009	8
FSA	2011	13
OTCBVS	2011	25
UCBN and AVOZES	2006	19
3D-MAD	2013	29
–	2013	22

Table 6. Mouth movement based liveness detection

Databases	Year	Reference
UCBN	2006	19
AVOZES	2006	19
XM2VTS	2007	5
VidTIMIT	2006	19
	2010	6
SC	2013	26
DaFEX	2010	6
ZJU	2008	21
–	2013	27

Table 7. 3D properties based liveness detection

Database	Year	Reference
ZJU	2008	21
SC	2013	28
	2009	7

Table 8. Head movement based liveness detection

Database	Year	Reference
ZJU	2008	21
SC	2013	28
	2009	7

Table 9. Eye blink

Databases	Year	Reference
ZJU	2007	9, 23
	2008	10, 21
	2010	20
	2012	35
SC	2005	36
	2013	26

Table 10. Performance evaluation on publicly available databases

Approaches	Databases	Reference	Performance evaluation			
			AUC (%)	HTER (%)	Accuracy (%)	EER (%)
Texture analysis	NUAA	11	0.95		87.5	–
		15	0.99	19.03	–	–
		12	–	–	93	–
		18	–	11.97 and 13.05	–	–
		16	–	18.32,19.03 and 13.17	–	–
	CASIA	15	–	18.17	–	–
		16	–	21.0, 18.1 and 18.2	–	–
		24	–	0	–	–
			–		–	–
	Replay attack	21	–	12.5	–	–
		15	–	15.16	–	–
		44	–	5.1	–	–
		16	–	17.1, 15.6 and 13.8	–	–
	Print Attack	21	–	0	–	–
		46	–	8.98	–	–
		43	–	9		–
		45	–	–	100	–
		24	–	–	–	0
	Yale	12	–	–	93	–
Mouth movement	XM2VTS	5	–	–	–	0.5
Eye blink	ZJU	21	–	–	96.9	–
		10	–	–	95.7	–
		35	–	–	84	–

Table 11. Classification of schemes

Cost of system	Liveness indicator	Advantages	Disadvantages
Low level	Texture	• Simple implementation. • Good result in known scenarios, • Possible decision from one frame. • No user collaboration needed (non-intrusive).	• Needs data that covers all possible attacks. • Problem with low textural attacks. • Low video or image quality.
Medium level	Motion and life sign	• Difficult to spoof. • Texture independent. • Low user collaboration needed (intrusive).	• Needs video sequence. • Needs high quality image. • Challenged by videos with low motion activity. • Illumination may affect on system performance
High level	Life sign and additional sensor device	• Impossible to spoof. • Texture independent. • Cover all types of attacks. • Good performance under bad illumination conditions. • Independent from user collaboration (non-intrusive)	• Depends on landmark detection in the face. • Needs video sequences. Need extra device.

benchmarking of such anti-spoofing algorithms cannot be carried out effectively.

Discussion

From the reviewed literatures, we inferred that non-intrusive approaches such as texture-based schemes are suitable for low-cost liveness detection systems. These systems require no extra hardware but compromise on image or video quality. Motion-based anti-spoofing schemes, which are classified as intrusive approach, are a good option for medium-cost face liveness detection systems. These schemes are very effective and independent of texture variations. The main disadvantage of such spoofing techniques lies in their sensitiveness to the illumination changes. The sensitiveness may be compensated by using high quality images or videos. To increase the security level and tackle the issues associated with low

and medium cost anti-spoofing schemes, the use of life indicators in an anti-spoofing system is an adequate solution. Such systems require extra hardware to produce high quality images or videos which make such systems expensive and hardware dependent, but the systems provide better performance and are very difficult to spoof. The earlier discussed liveness indicators are summarized according to the cost of systems in Table 11.

Conclusion

We have presented a review of different anti-spoofing techniques for face liveness detection systems. These approaches make face recognition systems resilient to various types of spoof attacks. Different anti-spoofing methods have been developed and implemented that may significantly raise the difficulty level for photo, video and synthesis attacks. To date, the outcome of research efforts on anti-spoofing appears to be making a significant progress, but the quest continues towards a more reliable and secure system. Liveness detection still remains a challenge for the face recognition systems. From the review of literature, it can be concluded that the use of ordinary generic cameras for video replay attacks in non-intrusive technique may lead us to some cost-effective face anti-spoofing systems. There is need for designing and deploying non-intrusive methods without using extra devices. The use of thermal camera as an extra hardware is promising for liveness detection approach, but it may be too expensive for practical applications. Also, anti-spoofing methods may need to include more life sign indicators for liveness testing. In addition, more testing is needed to assess their effectiveness and the impact on overall performance of face biometric system. Finally, no matter what security measures are in place, no system is spoof-proof. Anti-spoofing measures simply make it more difficult for intruders to attack face biometric systems.

1. Wayman, J. L., Jain, A., Maltoni, D. and Maio, D., *Biometric Systems Technology, Design and Performance Evaluation*, Springer Science Business Media, Springer-Verlag, London, 2005.
2. Zhang, Z., Yi, D., Lei, Z. and Li, S. Z., Face liveness detection by learning multispectral reflectance distributions. Automatic Face and Gesture Recognition and Workshop, IEEE, Santa Barbara, CA, 2011, pp. 436–441.
3. Bai, J., Ng, T. T., Gao, X. and Shi, Y. Q., Is physics-based liveness detection truly possible with a single image? In Proceedings of the IEEE International Symposium. Circuits and Systems (ISCAS), Paris, France, 30 May–2 June 2010, pp. 3425–3428.
4. Nixon, K. A., Aimale, V. and Rowe, R. K., *Spoof Detection Schemes. Handbook of Biometrics*, Springer, New York, 2008, pp. 403–423.
5. Kollreider, K., Fronthaler, H., Faraj, M. and Bigun, J., Real time face detection and motion analysis with application in liveness assessment. *Trans. Infor. Forensics and Security*, IEEE, 2007, **2**(part 2), 548–558.
6. Chetty, G., Robust audio visual biometric person authentication with liveness verification. In Intel Multimedia Analysis for Security Appl. SCI 282, Springer, 2010, pp. 59–78.
7. Bao, W., Li, H., Li, N. and Jiang, W., A liveness detection method for face recognition based on optical flow field. In International Conference on Image Analysis and Signal Processing IASP, IEEE, 2009, pp. 233–236.
8. Kollreider, K., Fronthaler, H. and Bigun, J., Non-intrusive liveness detection by face images. *Image Vision Comput*., 2009, **27**(3), 233–244.
9. Pan, G., Sun, L., Wu, Z. and Lao, S., Eyeblink-based anti-spoofing in face recognition from a generic Webcamera. In International Conference 11th Computer Vision (ICCV'07), IEEE, Rio de Janeiro, Brazil, 14–20 October 2007.
10. Pan, G., Wu, Z. and Sun, L., Liveness detection for face recognition. In *Recent Advances in Face Recognition* (eds Kremisir, D., Mislav G. and Marian Stewart Barlett), InTech, Austria, 2008, pp. 235–252; ISBN 978-953-7619-34-3.
11. Tan, X., Li, Y., Liu, J. and Jiang, L., *Face Liveness Detection from a Single Image with Sparse Low Rank Bilinear Discriminative Model*, Springer, 2010, pp. 504–517.
12. Peixoto, B., Michelassi, C. and Rocha, A., Face liveness detection under bad illumination conditions. In IEEE 18th International Conference on Image Processing (ICIP), 11–14 September 2011.
13. Schwartz, W. R., Rocha, A. and Pedrini, H., Face spoofing detection through partial least squares and low-level descriptors. In International Joint Conference on Biometrics (IJCB), 11–13 October 2011.
14. Hadid, A., *The Local Binary Pattern Approach and its Application to Face Analysis*, Image Processing theory, tools and applications, IEEE, 2008; 978-1-4244-3322-3.
15. Maatta, J., Hadid, A. and Pietik, M., Face spoofing detection from single images using micro-texture analysis. IEEE, Washington, DC, 2011, pp. 1–7.
16. Chingovska, I., Anjos, A. and Marcel, S., On the effectiveness of local binary patterns in face anti-spoofing. In Proceedings of International Conference on Biometric Special Interest Group (BIOSIG), IEEE, Darmstadt, 6–7 September 2012.
17. Pereira, T. F., Anjos, A., De Martino, J. M. and Sebastien Marcel, LBP-TOP based countermeasure against face spoofing attacks, ACCV 2012 Workshop, Part 1, LNCS 7728, Springer, Berlin, Heidelberg, 2013, pp. 121–132.
18. Kose, N. and Dugelay, J. L., Classification of captured and recaptured images to detect photograph spoofing. In APR International Conference on Informatics, Electronics & Vision IEEE, Dhaka, 2012, pp. 1027–1032.
19. Chetty, G. and Wagner, M., Multi-level liveness verification for face-voice biometric authentication. Biometrics Symposium, Baltimore, Maryland, 19–21 September 2006.
20. Pan, G., Sun, L., Wu, Z. and Wang, Y., Monocular camera-based face liveness detection by combining eyeblink and scene context. Science + Business Media, LLC, Springer, August 2010.
21. Kollreider, K., Fronthaler, H. and Bigun, J., Verifying liveness by multiple experts in face biometrics. In Computer Vision and Pattern Recognition Workshops. CVPRW 2008, IEEE, Anchorages, AK, 23–28 June 2008.
22. Sooyeon, K., Sunjin, Y., Kwangtaek, K., Yuseok, B. and Sangyoun, L., Face liveness detection using variable focusing. In International Conference on Biometrics (ICB), Madrid, Spain, 4–7 June 2013.
23. Sun Gang Pan, L., Zhaohui Wu and Shihong Lao, *Blinking-Based Live Face Detection Using Conditional Random Fields*, ICB 2007, Springer, pp. 252–260.
24. Komulainen, J., Hadid, A. and Matti, P., Face spoofing detection using dynamic texture. In Computer Vision-accv 2012 Workshops Lecture Notes in Computer Science, Springer, 2013, vol. 7728, pp. 146–157.

25. Sun, L., Huang, W. B. and Wu, M. H., TIR/VIS correlation for liveness detection in face recognition. In *Computer Analysis of Images and Pattern*, Springer, 2011, pp. 114–121.
26. Hatture, S. M. and Karchi, P. R., Prevention of spoof attack in biometric system using liveness detection. *Int. J. Latest Trends Eng. Technol.*, 2013, Special Issue-IDEAS-2013, pp. 42–49.
27. Kant, C. and Sharma, N., Fake face recognition using fusion of thermal imaging and skin elasticity. *IJCSCIJ*, 2013, **4**(1), 65–72; ISSN-0973-7391.
28. Lagorio, A., Tistarelli, M., Cadoni, M., Fookes, C., Clinton, B. and Sridha, S., Liveness detection based on 3D face shape analysis. In Proceedings of the 2013 International Workshop on Biometrics and Forensics (IWBF), IEEE, Lisbon, Portugal, 2013, pp. 1–4.
29. Erdogmus, N. and Marcel, S., Spoofing in 2D face recognition with 3D masks and anti spoofing with Kinect. In 6th International Conference on Biometrics: Theory, Applications and Systems (BTAS), IEEE, Arlington, VA, 2013.
30. Frischholz, R. W. and Werner, A., Avoiding replay-attacks in a face recognition system using head-pose estimation. In International Workshop on Analysis and Modeling of Faces and Gestures (AMFG'03), IEEE, 2003, pp. 234–235.
31. Pan, G., Wu, Z. and Sun, L., Liveness detection for face recognition. *Recent Adv. Face Recog.*, 2008; www.intechopen.com
32. Schuckers, S. A. C., Spoofing and anti-spoofing measures. *Inf. Security Tech. Rep.*, 2002, **7**(4), 56–62.
33. Choudhury, T., Clarkson, B., Jebara, T. and Pentland, A., Multimodal person recognition using unconstrained audio and video. In International Conference on Audio- and Video-based Biometric Person Authentication (AVBPA'99), Washington DC, 1999, pp. 176–181.
34. Barron, J. L., Fleet, D. J. and Beauchemin, S. S., Performance of optical flow techniques. *Int. J. Comput. Vision*, 1994, **12**(1), 43–77.
35. Szwoch, M. and Pieniazek, P., *Eye Blink based Detection of Liveness in Biometric Authentication Systems using Conditional Random Fields* (ed. Bolc, L. *et al.*), ICCVG, 2012, LNCS 7594, Springer, pp. 669–676.
36. Jee, H. K., Jung, S. U. and Yoo, J. H., Liveness detection for embedded face recognition system. *Int. J. Biol. Life Sci.*, 2005, **1**, 4.
37. Li, J., Wang, Y., Tan, T. and Jain, A. K., Live face detection based on the analysis of Fourier spectra. In Proceedings of Artical SPIE 5404, Biometric Technology for Human Identification, 25 August 2004, pp. 296–303.
38. Zhao, W., Chellappa, R. and Phillips, R., Face recognition: a literature survey. *ACM Comput. Surv.*, 2003, **35**, 399–458.
39. Kahm, O. and Damer, N., 2D face liveness detection: an overview. In International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, 2012, pp. 1–12.
40. Adler, A. and Schuckers, S., Security and Liveness, Overview, *Encyclopedia of Biometrics*, Springer, 2009.
41. Nixon, K. A. *et al.*, Novel spectroscopy-based technology for biometric and liveness verification. In Proceeding of SPIE 5404, Biometric Technology for Human Identification, 287, 25 August 2004.
42. Aruni, S., Tivari, S. and Kumar Singh, S., Face tempering detection from single face image using gradient method. *Int. J. Security Appl.*, 2013, **7**(1), 17–30.
43. Anjos, A. and Marcel, S., Counter-measures to photo attacks in face recognition: a public database and a baseline. In Biometrics (IJCB), International Joint Conference on IEEE, Washington, DC, 2011, pp. 1–7.
44. Komulainen, J., Anjos, A., Hadid, A., Marcel, S. and Pietikäinen, M., Complementary countermeasures for detecting scenic face spoofing attacks. In IAPR International Conference on Biometrics, ICB, Madrid, 2013.
45. Yan, J. *et al.*, Face liveness detection by exploring multiple scenic clues. Control Automation Robotics and Vision (ICARCV). In 12th International Conference on IEEE, Guangzhou, 2012, pp. 188–193.
46. Anjos, A., Chakka, M. M. and Marcel, S., Motion-based countermeasures to photo attacks in face recognition. *IET Biometrics*, 2013, **3**(3), 147–158.

Received 8 April 2014; revised accepted 26 January 2015