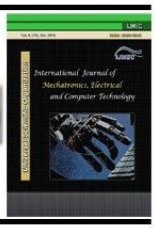
Vol. 5(17) Oct. 2015, PP. 2398-2407

Contents list available at IJMEC

International Journal of Mechatronics, Electrical and Computer Technology (IJMEC)

Journal Homepage: www.aeuso.org

PISSN: 2411-6173 - EISSN: 2305-0543



An Eye Blinking Password Based Liveness Monitoring System to Improve the Detection of Video Spoofing

A. Asaduzzaman[1], A. Mummidi[2] and Fadi N. Sibai[3]

[1]*EECS Department, Wichita State University, Wichita, Kansas, USA*

[2]*Facilities Planning Department, Saudi Aramco, Dhahran, Saudi Arabia*

***Corresponding Author's E-mail:** fadi.sibai@aramco.com*

Abstract

Contemporary protocols in the TCP/IP suite may be very vulnerable to spoofing attacks when extra precautions are not taken to verify the identity. There are several ways to spoof the facial recognition such as using photograph, three-dimensional (3D) model, and video clip of a valid user. Studies show that there have been significant improvements in detecting photograph and 3D model spoofing. However, there is no such improvement in detecting video spoofing. Recent studies also show that liveliness monitoring using the facial features has potential to improve security, especially in biometric systems. In this paper, an efficient method to detect video spoofing using liveliness monitoring is introduced. An eye blinking password system using ultrasonic range sensing module is developed for liveliness detection of the users. In the proposed system, local facial features like eye blinking and chin movement pattern are used via a real-time generic web-camera. The system is tested by conducting experiments using 20 valid users and 100 different users' appearances. According to the experimental results, the proposed system achieves 100% face recognition accuracy and 100% liveliness detection performance.

Keywords: *Eye blinking password, liveliness monitoring, network security, ultrasonic method, video spoofing*

1. Introduction

Facial recognition is proven to be very useful to providing user authentication which helps one to protect information. Research in this field has a growing encouragement from many government agencies and universities. People are frustrated in using passwords for protecting their personal information and/or personal identification numbers for their automated teller machines (ATMs). Recent developments have been made to utilize biometric sensors in ATM cash points where fingerprint analysis is required to authorize their account. Such a biometric security makes people more confident that their information is secure. The facial recognition uses digital image or video processing techniques for authentication. In spite of the fact that the complex algorithms are required for processing images and videos, facial recognition techniques have proven to be very useful for contemporary security applications [1]. Although facial recognition has potential to identify facial features, it encounters several challenges in providing accurate results. The most common challenges occur due to improper lighting, viewing angles, and spoofing alerts. When the user is subjected to improper lighting conditions, the same user can appear noticeably different [2]. There is also a difference between the indoor and outdoor lighting conditions [3]. This makes the system hard to identify the users. A constant lighting is required so that the facial recognition system can identify

Article History:

Received Date: Jun. 23, 2015

Accepted Date: Sep. 08, 2015

Available Online: Sep. 12, 2015

the user in any situation [4]. The system also requires proper viewing angles for user identification, as the user may appear different from various viewing angles [5]. Additionally, the user must stand in front of the system at an appropriate angle to get accurate results. Spoofing attacks are considered as a major threat because they are implemented with the sole purpose of fooling the system while obtaining the required authentication information from the user. This can be of national importance if any sensitive information is in the wrong hands. Consequently, preventing such spoofing attacks is of primary importance [6]. A photograph of a valid user can be bent, rotated, and/or shifted accordingly before the camera to spoof the authentication system. That makes photographic spoofing a simple and cheap way of fooling the facial recognition system [7]. Video spoofing [8], on the other hand, poses a greater threat than any other spoofing techniques as it provides many physiological clues to the system like blinking, head movement, etc. Another way of spoofing is through a 3D model of a valid user. This way of spoofing does not pose much of a threat because a 3D model lacks the physiological information of the face and the realism of a live person [9].

There are distinct points on a face that make them distinguishable. These points can be called as nodal points. A typical facial recognition system measures these nodal points to identify the facial structure of a face. Common nodal points include the distance between the eyes, width of the nose, depth of the eye sockets, shape of the cheekbone, and the length of the jaw line. These nodal points are measured using numerical code called faceprint [10]. They can be measured and processed in three different approaches: Image input normalization, geometric approach, and elastic face matching. In certain situations, neural networks are used to match these parameters. These approaches use different algorithms to process the image data and match it to the image uploaded in the database. The disadvantage with such filtering algorithms is that they do not check if the image or video is reliable as it cannot distinguish between a live feed of the camera and a video clip placed in front of the camera. Such flaws are the source for the spoofing attacks.

For the past few years, many algorithms have been provided to identify spoofing attacks [11]. Many of such theories have been successful in identifying photograph spoofing with great accuracy [12]. The same could not be said in the case of video spoofing. When a video clip of a valid user is placed in front of a camera, it can easily deliver the necessary data to measure the nodal points of a face which makes it a challenge to identify such spoofing attacks. The lack of verification is misused and utilized for spoofing. If a proper security layer is added for better verification of the user, the threats of spoofing can be minimized. Existing technologies use software-implemented security but do not provide the reliability that the users expect. In our proposed model, we provide a hardware-implemented security that would eliminate the existing flaws in detecting the spoofing possibilities. The rest of the paper is organized as follows: Section II summarizes some related published articles. Some popular existing anti-spoofing techniques are discussed in Section III. Section IV describes the proposed video spoofing detection method. The proposed method is evaluated in Section V. Finally, this work is concluded in Section VI.

2. Literature Survey

In general, any facial recognition system utilizes either two-dimensional (2D) or 3D images. A 2D system processes a single 2D image of a face [13][14]. In a 3D system, various technologies such as patterned illumination light or paraxial viewing can be used to develop a 3D representation of a face [15]. The 3D sensors are used to capture information about the shape of a face. This information is then used to identify distinctive features on the surface of a face, such as the contour of the eye sockets, nose, and chin. One advantage of 3D facial recognition is that it is not affected by changes in lighting like other techniques [16]. Facial recognition systems utilize several popular recognition algorithms including principal component analysis using eigenfaces, local binary patterns, and elastic bunch graph matching [17].

A computational model of face recognition is developed by Turk et al. [18]. They suggest that an information theory approach of coding and decoding of face images may provide an insight in the

facial features. A simple approach of capturing these facial features is by capturing a variation in the collection of face images. In mathematical terms, they obtain the eigen vectors of the facial component. The eigen vectors are characterized as a set of features that, as a collection, depict the variation between the face images. These eigen vectors are taken as a ghostly face called eigenfaces. They initially acquire the training set of images and calculate the eigenfaces. When a new image is obtained, they calculate its eigenfaces. The eigen faces of the training set image and the new image are compared. If the weights match, then it is classified as a known person. If the weights do no match and it is repeatedly encountered then it recalculates the characteristic weight pattern and thereby giving the system to self-learn.

A facial recognition algorithm using facial bunch graph matching is proposed by Wiskott et al. [19]. Elastic bunch graph matching is an algorithm used for object recognition. It requires two important parameters to calculate the visual data. The visual features based on Gabor wavelets and dynamic link matching is necessary for facial recognition. The testing images are taken and the facial features of these images are depicted using Gabor wavelets. The real image of the user is then obtained and similar analysis of the features is obtained. Both Gabor wavelets are then compared with dynamic link matching. If there are enough reasonable valid similarities between the two wavelets, the user is qualified as known and is authorized.

3. Existing Anti-Spoofing Techniques

A. Photographic Spoofing

In photo spoofing, any image of a valid user can be used to fool the facial recognition system. Many algorithms have been proposed to prevent such attacks. Such an approach to detect such spoofing is proposed by Pan et al. [20]. They propose a blinking-based liveliness detection method, where the blinking of the eye can prove the system that it is not an imposter image. They create a system with no hardware addition which adds to the cost factor and yet they have a complex underlying algorithm to keep track of the eye blinking sequence. They use eye closity algorithm for quick and accurate recognition of eye blinking. An average person blinks every 2 to 4 seconds. Any generic camera can capture in no less than 15 frames per seconds. This means that the camera can capture about two or more frames per eye blink. This makes eye blinking a more prominent feature to identify a live face and it is a more non-intrusive approach in identifying spoof attacks. The most typical way for the system to learn eye blinking is by classifying the opening and the closing of the eye lids. For their training period, they provide about 1,016 images of closed eyes and 1,200 images of open eyes without providing any details whether they are left or right eyes. All the images have base resolution of 24x24 pixels. They show promising results in identifying the eye blinking. Three different approaches are used to measure the detection rates. They are one eyed detection rate, two eyed detection rate, and clip detection rate. Each of these approaches have their own advantages. Although this approach is reliable, the system could be affected by strong glass reflection making it difficult to determine the eye blinking.

An improved method to detect face spoofing using micro texture analysis is proposed by Maatta et al. [21]. In their method, they are able to distinguish the real image from the fake photograph by differences in the reflection of light. They also point out the texture differences between the real face and the fake image. They analyze the surface properties which show the difference in pigments. From these observations, they adopt local binary patterns to distinguish between the real face and the fake image and prevent spoofing. The local binary pattern is texture operator that helps in describing the microstructures and their spatial information. The vector data they obtain from the operator is then fed to support vector machine classifier which characterizes the micro-texture patterns. They provide results from an experimental setup, where images of 15 subjects are used as separate sets for training and test purposes. They setup two sessions for training and one for the test purpose. For the training session, 1,743 images of 9 real clients and 1,748 images of the imposter images are taken. During the test session, only 3 clients are qualified. In order to add complexity to

the testing, they introduce 6 more clients. They consider a 64x64 pixel image. Their results are promising in determining the spoofing but their system can be flawed if a high resolution image is used to fool the system. In such a situation, distinguishing the texture is more of a challenge.

Another approach of classifying captured and recaptured images to detect photograph spoofing is proposed in [22]. The approach relies on contrast and texture characteristics of images to detect spoofing. They initially use difference of Gaussian (DoG) filter to obtain the frequency band which could help discriminate the real and photo images. Their experimental setup involves the same training and testing sessions. A set of client and imposter images are taken into consideration for these sessions. The different conditions are under illumination condition, effect of DoG filtering and global matching method in recaptured face image detection. In the illumination condition, it provide an accuracy of 88.03%. Under the effect of DoG filtering, the error is reduced to 11.97%. The error is 23.46% when DoG filtering is not used. For the global matching method, they use local binary pattern variance algorithm which not only provide texture characteristics, but also provide the contrast characteristics of images. This helps in the classification of the captured and the recaptured images. Experiments indicate that this approach provide more accurate results compared to other spoof detection systems.

The photographic spoof detection approaches are efficient and yet they have certain weaknesses which still need to be corrected. The most efficient and reliable data can be obtained through video processing. Spoofing is still possible in video processing.

B. Video Spoofing

A typical video based face detection system automatically detects the face regions, extracts facial features, and recognizes facial identity. Facial recognition of video processing is preferred over still images as motion helps in eliminating possible photograph spoof, despite facing some challenges such as low video quality, small face images, and body parts characteristics. The approaches used for eliminating photographic spoofing could not be said for video spoofing.

A method to identify video spoofing though visual rhythm analysis is proposed by Allan da Silva Pinto et al. [23]. In any image or video processing technique, the data has to be sent through an analog to digital converter to process the signals. During this conversion, it is more likely that noise would be generated in the system. These noise signals are distinct to the camera from which the video is obtained and the surrounding it captures. If a live video is captured, then from the noise generated we can identify its source from the generic camera implemented. In case of video spoofing, a video clip from a different camera is given as live feed to the system. After analog to digital conversion, the noise generated is likely to vary as the noise is subjected to camera feed. This variation in noise rhythm is used to identify the spoof threat. Their experimental setup involves video spoof data from previous attacks and using the same data to spoof the current setup of facial recognition system. The results prove to be encouraging because of their high accuracy. The disadvantage is that if spoofed video is created using the same camera as the one used for the facial recognition system then the accuracy fails again.

Video Spoofing is considered as a high threat when compared to photographic spoofing because there are very few and very less efficient approaches in identifying video spoofing when compared to photograph spoofing.

4. Proposed Method

We introduce the liveliness monitoring technique to eradicate the spoofing threats. The purpose of eye blinking module is to set a password with the blinking effect. For instance, four blinks can be set as a password for a particular user and the system only then recognizes that person as a valid user with four blinks in front of the camera. The eye ball depth is an important nodal point in distinguishing the user, because it is unique to every human being. Prior to running the facial matching algorithm, we identify the eye ball depth of the user in front of the camera. The use of

acoustics handles the task of measuring the eyeball depth. Ultrasonic range sensing modules are said to have better accuracy and precision to determine the distance between the two points. The purpose of measuring these values is to make sure that a valid user is standing in front of the generic camera by checking the depth irregularities with the depth of an eyeball. These depth irregularities cannot be spoofed by any other video displaying devices like a cell phone or mini digital display devices. Thus, if the video clip of any person is placed in front of the camera, this design will detect a video spoofing alert. In such a way, user authentication is improved and spoofing threats are also eliminated. Although this approach seems to be valid, adding a contingency to the existing technique would provide better accuracy and would completely eradicate the spoofing threats. The proposed model utilizes hardware-based security to eliminate spoofing threats. The use of ultrasonic range sensing module brings the microcontroller unit into picture. Figure 1 illustrates the inter-actions of various components of the proposed system using a block diagram.

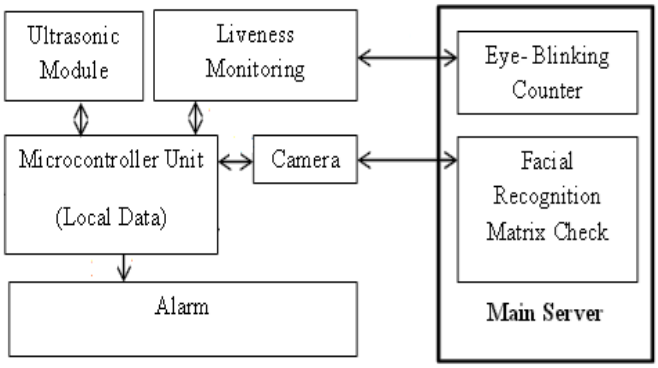


Fig. 1: Block diagram of the proposed model

A. Hardware: Microcontroller Unit

The microcontroller unit (MCU) used is an Arduino Leonardo. Arduino is an open source platform based single board microcontroller. Arduino Leonardo is a microcontroller board based on ATmega32u4. It has 20 digital input/output pins, of which 7 can be used a PWM outputs and 12 as analog inputs; a 16MHz crystal oscillator; a micro USB connection; a power jack; an ICMP header; and a reset button. External (non-USB) power can come either from an AC-to-DC adapter (wall-wart) or battery. The board can operate on an external supply of 6 to 20 Volts. The ATmega32u4 has 32 KB memory (with 4 KB used for the boot-loader). It also has 2.5 KB of SRAM and 1 KB of EEPROM. The ATmega32U4 provides UART TTL (5V) serial communication, which is available on digital pins 0 (RX) and 1 (TX). The 32U4 also allows for serial (CDC) communication over USB and appears as a virtual com port to software on the computer. The chip also acts as a full speed USB 2.0 device, using standard USB COM drivers.

B. Hardware: Ultrasonic Module

Ultrasonic range sensing module HC-SR04 is used in this experiment. The ultrasonic modules (UMs) provide 2cm-400cm non-contact measurement function, the ranging accuracy can reach 3mm. The modules include ultrasonic transmitters, receiver and control circuit. One only needs to supply a short 10uS pulse to the trigger input to start the ranging, and then the module will send out an 8 cycle burst of ultrasound at 40 kHz and raise its echo. The echo is a distance object that is pulse width and the range in proportion. The timing diagram of HC-SR04 is provided in Figure 2. One can calculate the range through the time interval between sending trigger signal and receiving echo signal. The formula is given as: µS / 58 = centimeters or µS / 148 = inch; or: the range = high level time * velocity (340M/S) / 2. We suggest to use over 60ms measurement cycle, in order to prevent trigger signal to the echo signal. It has quiescent current less than 2 mA, working current requirement less than 15 mA, measuring angle of 30 degrees, and trigger input pulse width of 10 micro seconds.

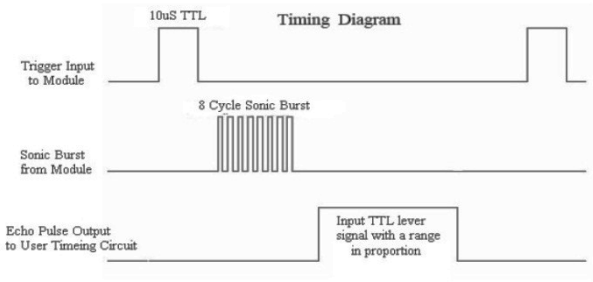


Fig. 2: Timing diagram for HC-SR04

C. Software: Integrated Development Environment

Arduino integrated development environment (IDE) version 1.0.5 is used for code development and uploading it to the MCU board. Arduino IDE comes with a software library called "Wiring" which facilitates common input/output operations. Most Arduino boards have an LED and load resistor connected between pin 13 and ground; a convenient feature for many simple tests. Arduino IDE uses the GNU toolchain and AVR Libc to compile programs and avrdude to upload programs to the board.

D. Work-Flow

At the beginning, Arduino Leonardo is preloaded with the measurement values of the valid user and it is given an accuracy factor of 0.5. The work-flow of the proposed system is illustrated in Figure 3. The ultrasonic range sensing module measures the eyeball depth of the valid users. This measurement data is sent to the microcontroller unit for further processing. If the values (ultrasonic distances) match, the liveliness detection monitoring comes into picture and goes to the eye blinking phase. (If the measurements do not match, then the microcontroller unit signals the buzzer indicating that it is a threat.)

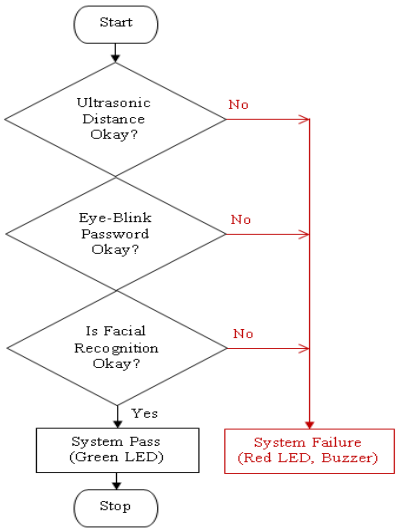


Fig. 3: Flow Chart of the proposed model

Each user is given a different eye password according to their eye blinking. The user, after the acceptance of eyeball value measurements, is validated for liveliness monitoring. The liveliness monitoring detects the eye blinking of the valid user. Each valid user has an eye blink pattern as a password to distinguish from other users. The liveliness monitoring algorithm requires better processing power and thus, it is sent to a nearest server that contains the database of the valid user information related to the facial recognition system. Clip based detection is used to identify the eye

blinking as it promises better accuracy and efficiency. If the eye blinking password does not match then it again buzzes, indicating a threat.

Only after the eye blinking criterion is met, the system then moves to the facial recognition method for the true authentication of the user. In a way, it is acting as a security measure to better improve the reliability. The ultrasonic module requires only the processing power of the microcontroller and thus it can be kept isolated from the database. In this regard, it is providing proper isolation to restrict threats like hacking the main server to access information. For the liveliness monitoring, the proposed algorithm includes identifying the outline of the eye (the left and right most positions of the eye are identified), matching the position of the eye (with the standard eye position), and calculating the difference between the position of the top of an eye outline and that of the standard opened eye.

The proposed system faces some challenges. The system depends on ultrasonic range sensing, making proper arrangement of these sensors are necessary for efficient operation. Moreover, it uses eye blinking as a password, hence proper lighting conditions are required to provide optimum lighting to detect the eyelid movement. These requirements are also the common challenges of any biometric facial detecting system and these conditions should be satisfied for proper operation [24].

5. Evaluation

The system evaluates only one user at a time for face recognition. Handling multiple users may increase hardware complexity. For the measurement of eyeball depth, initially 20 users are taken into consideration. These users are the only ones who are authorized to unlock the system. Users are considered for both training and testing stages. The circle in Figure 4 indicates the ultrasonic eyeball depth values of one of the 20 valid users. The values represent the top, center, and the bottom depth of the eyeball.

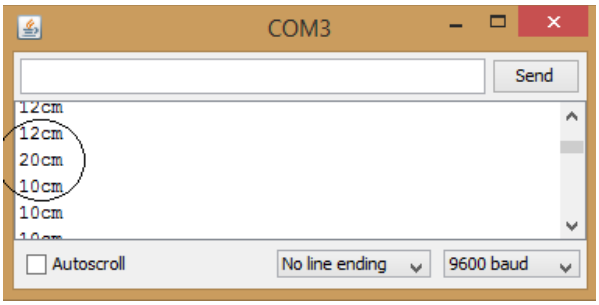


Fig. 4: Eye-ball measurement of 1 of the 6 valid users

The eye ball depth measurement values of all 20 valid users are shown in Table I. The values are unique for each user. The values of eyeball depth for User 1 are (12, 20, and 10), where 12 represent the upper, 20 represent the center, and 10 represent the bottom depth of the eyeball. After these values are taken, they are kept aside in a database along with the facial matrix of each user. These values are preloaded in the microcontroller unit for testing.

After the training stage is completed, the system is ready to test users. First, it is verified whether the microcontroller unit can identify the valid users with the preloaded values of the eye ball depth measurement. During the test stage, all the valid users show full accuracy and the microcontroller system is capable of identifying the users every time. 100 different attempts are made to authenticate the system by measuring their eyeball depth values. These values and experimental results are summarized in Table II. The system recognizes the valid users (and the invalid users). In order to further improve the system performance, we introduce liveliness monitoring which also improves accuracy.

Table 1: Valid Users Ultrasonic Distance Measurements

Valid User	Ultrasonic Distance (top, center, bottom)
User 1	(12, 20, 10)
User 2	(13, 10, 11)
User 3	(12, 12, 11)
User 4	(14, 10, 13)
User 5	(14, 11, 12)
User 6	(15, 13, 12)
User 7	(11, 10, 10)
User 8	(13, 11, 12)
User 9	(12, 10, 11)
User 10	(12, 9, 11)
User 11	(11, 11, 9)
User 12	(15, 11, 10)
User 13	(13, 12, 13)
User 14	(11, 9, 10)
User 15	(14, 13, 10)
User 16	(10, 10, 9)
User 17	(11, 10, 9)
User 18	(12, 11, 11)
User 19	(13, 8, 12)
User 20	(11, 10, 11)

Table 2: Comparison between Valid And Invalid Users

Person	Ultrasonic Distance	Check Database (Pass/Fail)	Valid/Invalid User
Person 1	(14,10,13)	Pass	Valid (User 4)
Person 2	(13,10,11)	Pass	Valid (User 2)
Person 3	(12,11,14)	Fail	Invalid
Person 4	(15,13,12)	Pass	Valid (User 6)
Person 5	(12,15,11)	Fail	Invalid
Person 6	(12,12,11)	Pass	Valid (User 3)
Person 7	(14,11,12)	Pass	Valid (User 5)
Person 8	(12,20,10)	Pass	Valid (User 1)
Person 9	(11,11,12)	Fail	Invalid
Person 10	(10,12,12)	Fail	Invalid
Person 11	(10,10,11)	Fail	Invalid
Person 12	(13,12,13)	Pass	Valid (User 13)
Person 13	(11,10,10)	Pass	Valid (User 7)
Person 14	(11,10,11)	Pass	Valid (User 20)
Person 15	(9,9,10)	Fail	Invalid
……	……	……	……
Person 99	(14,13,10)	Pass	Valid (User 15)
Person 100	(13,13,12)	Fail	Invalid

If a spoofing attempt is made in the system by showing the video of a valid user, the ultrasonic ranging module measures for the eyeball depth but it receives distance values between the video display screen and the module whose value is different from that of the eyeball depth of the user. The system identifies it as a spoofing attempt and declines authentication. Table III shows the comparison between the verification of User 1 with a “live attempt” and a “video attempt”. User 1 is first verified through the eyeball depth measurements and the system recognizes User 1 as a valid user. When the system is attacked by showing the video of User 1, it receives a different set of eyeball depth measurement values and thus does not authenticate it.

Table 3: Comparison Between Live and Spoof Videos

Live/Video Attempt	Ultrasonic Distance	Check Result (Pass/Fail)	Valid/Invalid User
Live	(12, 20, 10)	Pass	Valid (User 1)
Video Spoof	(11, 20, 9)	Fail	Invalid

Conclusions

For facial recognition using video clips, additional protections are required to successfully verify users' identification because the common protocols in the TCP/IP suite are vulnerable to video spoofing attacks. In this work, liveliness monitoring is introduced while verifying the users' identification to enhance the performance and accuracy of the security system. An eye blinking password system is developed using ultrasonic range sensing module for liveliness detection of users. A real-time generic web-camera is used in the system to implement the local facial features such as eye blinking and chin movement. It is expected that the proposed system should offer better accuracy as it can identify video spoofing and perform an improved facial recognizing algorithm. In this experiment, 20 different valid users are used for training and testing purposes; 100 different users' appearances are tested in the experiments. Based on the experimental results, 100% face recognition accuracy and 100% liveliness detection performance are achieved. The proposed facial recognition system is robust in natural environments in the presence of noise and illumination changes. The proposed system may suffer from improper lighting or viewing angles to operate properly. Next generation security systems should have the capability of recognizing people in real-time with less constrained conditions. We plan to improve the algorithm for faster execution of the liveliness monitoring and test the proposed system with hundreds of valid and invalid users in our next endeavor.

REFERENCES

[1] W. Zhao, R. Chellappa, P.J. Phillips, and A. Rosenfeld, "Facial Recognition: A Literature Survey," ACM Computing Surveys, Vol. 35, No. 4, pp. 399–458, 2003.

[2] P.J. Phillips, P.J. Flynn, T. Scruggs, K.W. Bowyer, J. Chang, K. Hoffman, J. Marques, J. Min, and W. Warek, "Overview of Facial Recognition Grand Challenge," IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2005.

[3] X. Tan and B. Triggs, "Enhanced Local Texture Feature Sets for Face Recognition under Difficult Lighting Conditions," 3rd International Workshop on Analysis and Modelling of Faces and Gestures (AMFG'07), 2007.

[4] P.N. Belhumeur, "Ongoing Challenges in Facial Recognition," Department of Computer Science, Columbia University.

[5] K.W. Bowyer, K. Chang, and P. Flynn, "A Survey of approaches and challenges in 3D and multi-modal 3D+2D face recognition," Computer Vision and Image Understanding 101, 2006.

[6] T. Ahonen, A. Hadid, and M. Pietikäinen, "Facial Recognition with Local Binary Patterns," Computer Vision – ECCV 2004, Volume 3021, pp 469-481, 2004.

[7] B.G. Nalinakshi, S.M. Hatture, M.S. Gabasavalgi, and R.P. Karchi, "Liveliness Detection Techniques for Prevention of Spoof Attack in Face Recognition System," ISSN 2250-2459, ISO 9001:2008 Cetrified Journal, Volume 3, Issue 12, December 2013.

[8] G. Pan, L. Sun, Z. Wu, and S. Lao, "Eyelink-based Anti-Spoofing in Face Recognition from a Generic Webcamera.," Computer Vision ICCV 2, 2007.

[9] N. Erdogmus and S. Marcel, "Spoofing Face Recognition with 3D Masks," IEEE Transactions on Information Forensics and Security, 2014.

[10] Y. Lee, D. Terzopoulos, and K. Waters, "Realistic Modelling for Facial Animation," Computer Graphics and interactive Techniques, pp 55-62, 1995.

[11] T.d.f. Pereira1, A. Anjos, J.M.D. Martino, and S. Marcel, "Can face anti-spoofing countermeasures work in a real world scenario?," IDIAP Research Institute.

[12] A. Rocha, W. Scheirer, and S. Goldenstein, "Vision of the Unseen: Current Trends and Challenges in Digital Image and Video Forensics," ACM Vol V, 2009.

[13] V.V. Starovoitov, D.I. Samal, and D.V. Briliuk, "Three Approaches for Facial Recognition Systems," 6-th International Conference on Pattern Recognition and Image Analysis, Velikiy Novgorod, Russia, pp. 707-711, 2002.

[14] J. Komulainen, A. Hadid, and M. Pietikäinen, "Facial Spoofing Detection using Dynamic Texture," Computer Vision ACCV 2012 Workshop, Volume 7728, 2013.

[15] I.A. Kkadiaris, G. Passalis, G. Toderici, M.N. Murtaza, Y. Lu, N. Karampatziakis, and T. Theoharis, "Three Dimensional Face Recognition in the prescence of Facial Expressions:An Annotated Deformable Model Approach," Pattern Analysis and Machine, Volume 29, April 2007.
[16] J. Komulainen, A. Haidid, M. Pietikainen, A. Anjos, and S. Marcel, "Complementary countermeasures for detecting scenic face spoofing attacks," Biometrics ICB, 2013 International Conference, June 2013.
[17] C.-L. Lai, J.-H. Hsu and C.-H. Chu, "Spoofing face detection based on spatial and temporal feature analysis," Consumer Electronics GCCE, IEEE 2nd Global Conference, October 2013.
[18] M.A. Turk and A.P. Pentland, "Face Recognition using Eigenfaces," IEEE, 1991.
[19] L. Wiskott, J.-M. Fellous, N. Kruger, and C.v.d. Malsburg, "Face Recognition by Elastic Bunch Graph Matching," Intelligent Biometric Techniques in Fingerprint and Face Recognition, Chapter 11, pp. 355-396, 1999.
[20] G. Pan, Z. Wu, and L. Sun, "Liveness Detection for Face Recognition," Recent Advances in Facial Recognition, pp. 236, 2008.
[21] J. Maatta, A. Hadid, and M. Pietikainen, "Face Spoofing Detection From Single Images Using Micro-Texture Analysis," IEEE, 2001.
[22] N. Kose and J.-L. Dugelay, "Classification of Captured and Recaptured Images to Detect Photograph Spoofing," Multi Media Department, Sophia-Antipolis, France.
[23] A.d.s. Pinto, H. Pedrini, W.R. Schwartz, and A, Rocha, "Video-Based Face Spoofing Detection through Visual Rhythm Analysis," 25th IEEE Conference on Graphics, Patterns and Images (SIBGRAPI), pp. 221-228, 2012.
[24] K.A. Nixon, V. Aimale, and R.K. Rowe, "Spoof Detection Schemes," Handbook of Biometrics, Springer, 2007.