2020 International Conference on Computational Performance Evaluation (ComPE)
North-Eastern Hill University, Shillong, Meghalaya, India. Jul 2-4, 2020

Ameliorated Anti-Spoofing Application for PCs with Users' Liveness Detection Using Blink Count

Arpita Nema
Department of Computer Science and Engineering
Jabalpur Engineering College
Jabalpur, India
nemaarpita2012@gmail.com

***Abstract*— The paper proposes "Anti-spoofing application for desktop". This application uses a face recognition approach along with the use of eye-blink count to detect liveness. Main phases of application are namely, face detection and recognition, and determination of liveness status of user. Liveness detection is proven to prevent the video play-back attacks and use of printed photograph in order to compromise the security. Webcam captures the user's image after every short interval of time. Image captured after passing authentication process is checked for liveness. In case of security breach, countermeasures are executed. This include capturing image of adversary and system logoff or exit. This paper proposes an additional functionality which uses HOG feature descriptor of user image along with passcode. It uses SVM classifier that gives performance metric of 100% accuracy. The experimental results of the ameliorated functionality show the effectiveness of the proposed approach.**

Keywords: Histogram of Oriented Gradients; Anti-spoofing; Face recognition; Eye-blink count; Passcode

I. INTRODUCTION

Face recognition as biometric technology is astonishingly versatile. This dominates the broad range of applications from law enforcement agencies to consumer applications. Technique of face recognition is used to control the access of restricted areas, safe boxes or high-tech computing systems.

This paper proposes the use of face recognition for desktop user authentication. This makes logging procedure easier and faster. In order to get unauthorized access to system, adversary may use printed photographs or video playback attack. Many approaches to the problem involve use of auxiliary devices like thermal sensor, flashlight, 3-D camera or more than one 2-D camera. This increases the complexity and the cost of the system. Thus, to cope with this our method proposes use of eye blink count to detect liveliness of the system's user. This does not use any specialized hardware. The use of passcode by the user gives accuracy of 100% and saves the original biometric that could be leaked. The Histogram of Oriented Gradients (HOG) as a feature descriptor is the fastest method for face detection on general-purpose CPU [2]. This is covered under the ameliorated functionality module.

The proposed methodology along with the related works are illustrated in the following sections of the paper. Section II mentions about the cognate work of some desktop security applications. It withal discusses methods to detect liveness in face apperception. Section III illustrates the proposed approach to detect face liveness utilizing blink count with ameliorated functionality. Section IV devises the obtained performance results on ORL and CASIA face dataset. Section V gives the conclusion of the paper.

II. RELATED APPROACHES

This section discusses the present applications that provide security to desktop or laptop system. Also, it mentions the anti-spoofing techniques with liveness detection in existing works.

A. Some desktop security applications that work on similar concept of face recognition and detection

- **True key (Intel security).** [8] uses multi-factor authentication. The True Key app protects passwords by scrambling them with AES-256 and uses fingerprint as biometric modality. One can decrypt and access information with the factors they choose. User is always verified by at least two factors before being signed in. It shows efficient performance on Apple's macOS and Microsoft's Windows 10.

- **Rohos Face Logon.** Based on neural network technology, [9] provides user identification by face recognition in an automatic continuous process. It gives greater security to standard windows logon procedure, making it easier.

- **FastAccess Anywhere.** [10] is a cross platform application that works from Windows to iPhone and Google Android tablets and smartphones. It starts with face recognition engine. It only uses face for faster and easier logging.

- **KeyLemon.** [7] uses its patented webcam face recognition technology. It also retrieves information about those who try to gain unauthorized access to the PC. KeyLemon works fine on windows and OSX. Its usage is discontinued now.

B. Methods to detect liveness in face recognition

- **3D Face Analysis.** [6] discusses facial 3-Dimensional structure-based approach to detect liveness. This method processes 3D curvature of the acquired data to differentiate a photo from a real human face. An optoelectronic stereo system

978-1-7281-6644-5/20/$31.00 ©2020 IEEE

acquires the scans of 3D face. Thus, it requires an external device to detect liveness. The advantage, this biometric system offers, all facial encodings are utilized.

- **Pupil Tracking.** Eye area is extracted in [4] using a real-time camera that uses Haar-Cascade Classifier with a pre-trained classifier to detect eye region. To get a stable ocular perceiver region and minimize user's head kinetics, feature points are extracted and traced by employing the Kanade-Lucas-Tomasi approach. A square frame has consummately eight LEDs for each direction. To activate the culled direction's LED, a signal is sent to Arduino. A desultory direction is selected by a spoofing algorithm after a couple of stable frames that have eye pupils. It is recorded whether the position of LED matches with the eye direction, after activation of culled LED. Liveness information is returned by the algorithm if the docility requisite is gratified. This is a user cooperative approach that also requires a contrivance hardware device.

- **Fourier spectra analysis predicated on hair.** In this method [5] 2-Dimensional Fourier Spectra is analyzed. The corresponding frequency dynamics descriptor (FDD) and high-frequency descriptor (HFD) are quantified. To heighten the distinction between a playback video attack and a live person, the use of flashlight is specified. High-frequency components measure the hair details precisely to compare spoof video or image with the authentic user. Approach [5] requires an auxiliary device but advantages include low cost of implementation and computational intricacy.

- **Recaptured feature extraction.** [3] analyzes the distinctions between fake images and original face images. Blurriness, Hue channel distribution, and specular reflection ratio are used as feature descriptors.

III. Proposed Methodology

This section discusses the modules of our proposed system. Our system monitors the user using webcam for authentication. Software scripts are kept in system startup folder, which starts executing right after the boot process. Anti-spoofing measures are implemented when adversary is encountered.

A. Face Detection and Recognition

The script enables capturing of images (video) in the form of frames, by the desktop or laptop webcam. Face Detection is applied on every alternate frame to get the face co-ordinates and the corresponding face sub-matrix. The face sub-matrix is converted into a face code using face encoding.

For every profile added in the system a corresponding face code exists which is loaded when the system is initiated. The captured face encoding is compared with the profile image encoding. In case the face encoding and profile encoding match, proper functioning resumes otherwise "Unknown User Detected" message flashes on screen and the system aborts. The phases are depicted in fig. 1.

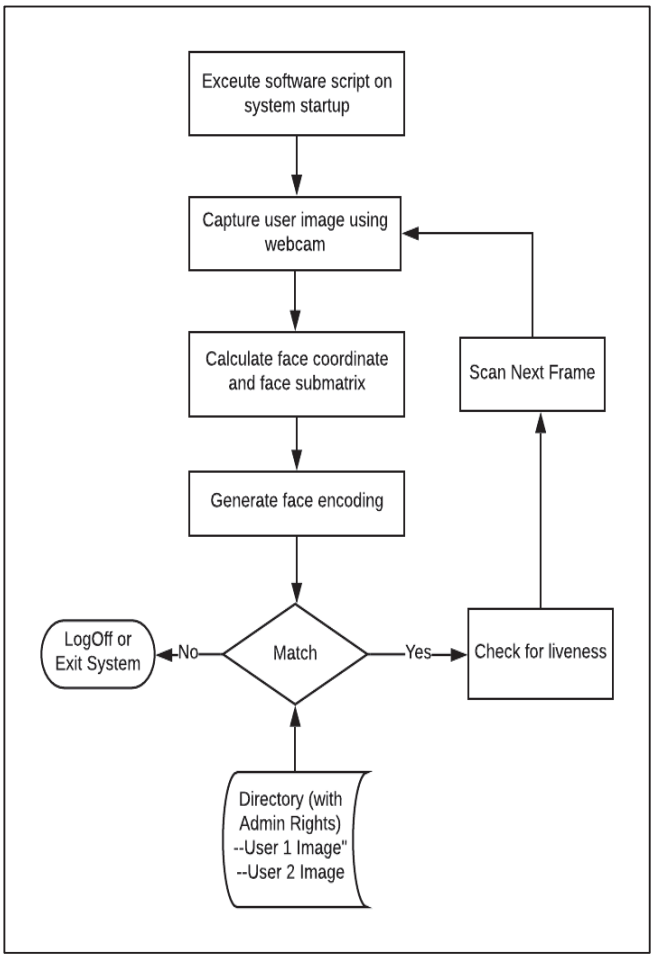

Fig. 1. Face detection and recognition stages.

B. Liveness Detection

The application includes a liveness detector capable of spotting fake faces in the face recognition system. After face recognition, convex hull is applied to enclose face landmarks, for example, the left and the right eye in a face. A blink count marks a blink of an eye. As the area of the convex hull enclosing an eye decreases beyond a certain threshold, the blink count is increased by one. The blink count is figured and is compared with the anterior one for a fine-tuned number of iterations. In case the current blink count is equal to the previous one, the fake flag is set, otherwise, the current blink count is set as previous and the computation continues. The process is depicted in fig. 2.

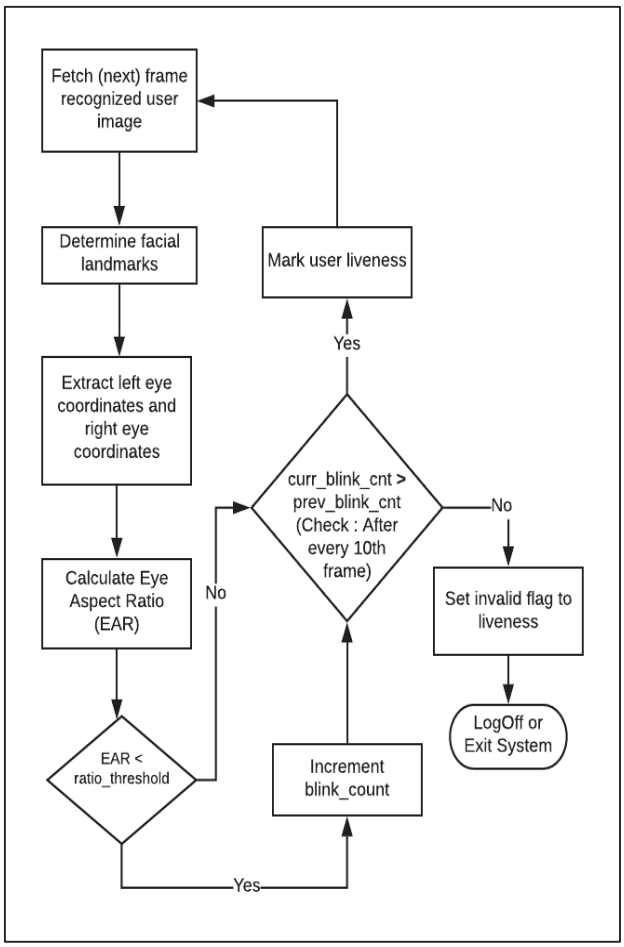

Fig. 2. Steps for liveness detection using eye-blink count.

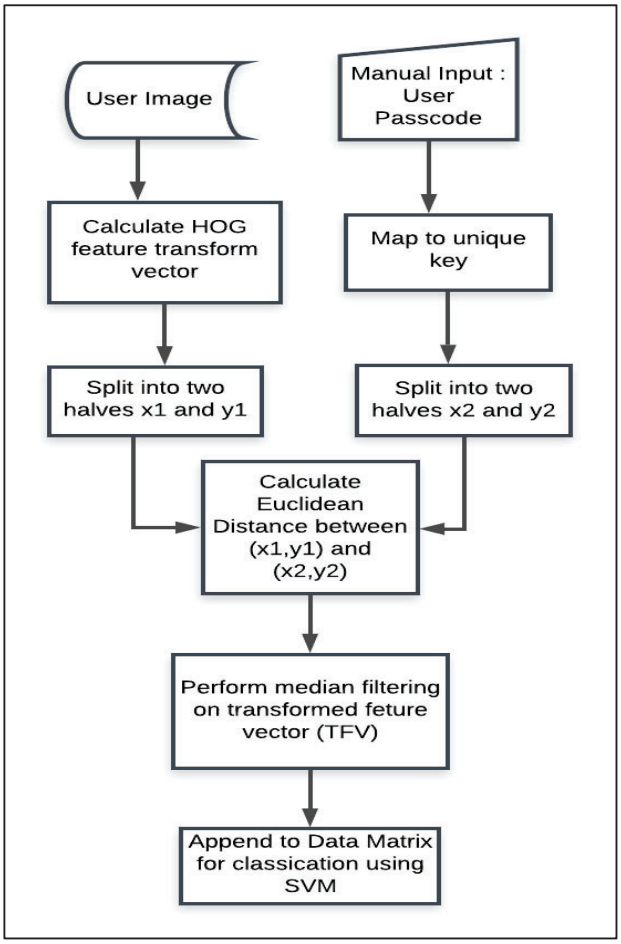

Fig. 3. Transformation of original face image using Passcode.

C. Ameliorated functionality

Feature Extraction. A user profile in the system consists of user images and a password. This module applies Histogram of Oriented Gradient (HOG) function on every profile image to obtain a corresponding HOG feature array. In the HOG feature descriptor, the distributions (histograms) of directions of gradients (oriented gradients) are used as features. The user passcode is mapped to a key. The size of a key is equal to the number of features obtained after applying HOG.

The HOG feature array and the key is divided into two halves (x1, y1) and (x2, y2) respectively. The Euclidean distance between (x1, y1) and (x2, y2) is computed to generate a vector on which median filter is applied to obtain a Transformed Feature Vector (TFV). For all system users, the TFV of all their images is appended to data matrix. The process is depicted in fig. 3. This step helps to transform the original biometric sample such that it cannot be retrieved. Thus, preventing accidental leakage of original biometric to unauthorized user.

Classification. The support vector machine (SVM) learning model is employed as the classifier. Here, the classification task is to predict the category or label (user) of the target given the input data. Since a target is provided, we have labeled data, it is supervised learning.

To obtain a hyperplane in n-D space is the aim of SVM [1]. The data points are distinctly classified by n features. There are numerous hyperplanes that could be opted to segregate data points of two different categories. A hyperplane is so chosen that it maximizes the span between data points of two different classes as shown in fig. 4, the main objective of this classification model. To relegate future data points confidently, providing reinforcement, the marginal distance is maximized. The decision borders are formed by the culled hyperplane. The data points attribute to distinct classes fall on different sides of the plane. The data points which are more proximate to the hyperplane are called 'Support Vectors'. The hyperplane's orientation and position are influenced by these.

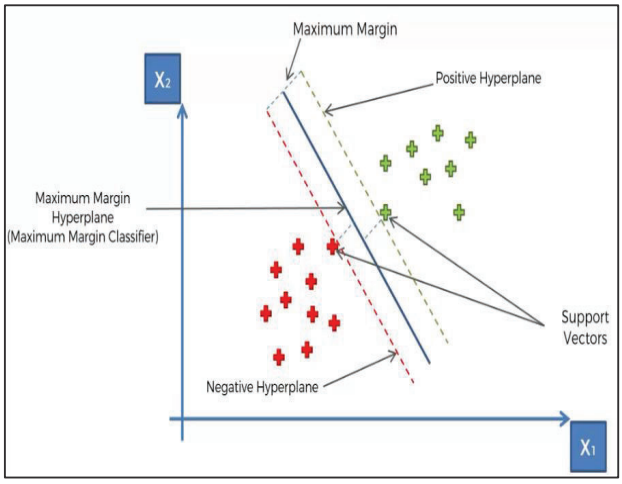

Fig. 4. SVM classifier intuition

IV. Result Analysis

Software script is implemented using python which makes it multi-platform application. 10-fold cross-validation is employed to evaluate the ameliorated functionality of the proposed system on the ORL and CASIA face database.

A. Dataset

ORL Database.
Captured within April 1992 and April 1994, this database [11] is composed of facial images. Vision, Robotics and Speech Group of the Engineering Department, Cambridge University uses this database in various face recognition projects.

For each of the 40 different individuals, 10 distinct images were taken. Images were captured by varying face details and expressions and at various intervals of time. This makes it an apt choice to get incorporated into the recognition task.

CASIA Database.
Collection of correspondent Near Infrared (NIR) images and mugshots is present in CASIA 2.0 dataset [12]. This database is registered by the Chinese Academy of Science (CASIA). It contains 5-50 NIR facial and 1-22 VIS for 725 individuals. Only mugshots images are used to evaluate the performance of the functionality proposed.

B. Performance Measure

We evaluated the performance under three cases:
Case 1 - When each user uses a unique passcode
Case 2 - Same passcode is used by all users
Case 3 - When users' original HOG features are used for classification

TABLE I. Matching Performance Accuracy (%) for ORL Database

fold	*Case 1*	*Case 2*	*Case 3*
1.	100.0	92.5	100.0
2.	100.0	77.5	97.5
3.	100.0	92.5	100.0
4.	100.0	90.0	97.5
5.	100.0	87.5	100.0
6.	100.0	100.0	97.5
7.	100.0	87.5	92.5
8.	100.0	72.5	90.0
9.	100.0	82.5	95.0
10.	100.0	77.5	92.5
Average	100.0	86.0	96.25

TABLE II. Matching Performance Accuracy (%) for CASIA Database

fold	*Case 1*	*Case 2*	*Case 3*
1.	100.0	77.6	94.41
2.	100.0	86.3	95.93
3.	100.0	82.7	96.44
4.	100.0	84.3	95.93
5.	100.0	78.7	95.43
6.	100.0	85.8	95.43
7.	100.0	82.7	97.96
8.	100.0	84.8	93.90
9.	100.0	83.2	95.93
10.	100.0	82.2	95.93
Average	100.0	82.8	95.73

As expected, when a unique passcode mapped key is used, the performance is comparably high. Same passcode used by more than one user does not help in authentication step and degrades the performance. Original HOG feature performance metric, without use of any passcode mapped key is comparable to mapped ones.

V. Conclusion

Liveness detection using eye-blink count enhances the reliability of the face recognition application. The approach proposed is a multi-platform application to enhance the security of the desktop system. This is automatic and low-cost solution that does not require any user cooperation. The application testing is conducted in adverse conditions on authentic data that demonstrate the sturdiness and efficacy of the work proposed. The performance evaluation of the ameliorated functionality on ORL and CASIA dataset using SVM as classifier have satisfying result.

VI. Future Enhancement

Prospective efforts will be aimed to get more accurate eye points and bringing amendments in the algorithm employed to locate eyes. Precise eye locations will make execution more expeditious and robust.

Acknowledgment

I would like to express gratitude to Rishika Kohli for her assistance in developing the GUI of application for advancement of this research work.

References

[1] Sun Z., Hu K., Hu K., Liu J., Zhu K., "Fast Multi-Label Low-Rank Linearized SVM Classification Algorithm Based on Approximate Extreme Points", IEEE Access, vol. 6, July 2018.

[2] Wang H., Zhang D., Miao Z., "Fusion of LDB and HOG for face Recogntion", IEEE, 37th Chinese Control Conference, Wuhan, China, July 2018

[3] Luan X., Wang H., Ou W., Liu L., "Face lineness detection with recaptured feature extraction", IEEE International Conference on Security, Pattern Analysis, and Cybernetics, Shenzhen, China, Dec. 2018.

[4] Killioglu M., Taskiran M., Kahraman N., "Anti-Spoofing in Face Recognition with Liveness Detection Using Pupil Tracking", IEEE 15th International Symposium on Applied Machine Inteeligence and Informatice, Herl'any, Slovakia, January 2017.

[5] Weiwen Liu, "Face Liveness Detection using analysis of Fourier Spectra Based on Hair", International Conference on Wavelet Analysis and Pattern Recognition, Lanzhou, July 2014.

[6] Lagario A., Tistarelli M., Cadoni M., Fookes C., Sridharan S., "Liveness detection based on 3D face shape analysis", International Workshop on Biometrics and Forensics, Lisbon, Portugal, April 2013.

[7] 3 Webcam Face Recognition Security Software and Biometric Password Manager, November 2019. Retrieved from https://www.geckoandfly.com/4068/webcam-face-recognition-security-software-and-password-manager-program/

[8] Intel True Key. Retrieved from https://www.truekey.com/#features

[9] Rohos Face Logon. Retrieved from https://www.rohos.com/products/rohos-face-logon/

[10] Sensible Vision Patent , "System and method for providing secure access to an electronic device using continuous facial biometrics", United States Patent, February 2013.

[11] The Database of Faces, AT&T Laboratories Cambridge. Retrieved from http://cam-orl.co.uk/facedatabase.html

[12] CASIA NIR-VIS 2.0 Database. Retrived from https://pythonhosted.org/bob.db.cbsr_nir_vis_2/