IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

BANK LOCKER SECURITY SYSTEM USING FACE RECOGNITION AND LIVELINESS DETECTION

Dr. Poonam Lambhate1 Aarshin Inamdar2, Rucha Gaikwad3, Vaishanavi Madane4, Mayuri Khedkar5,

Department of Computer Engineering JSPM's JSCOE, Savitribai Phule Pune University , Maharashtra, India

Abstract:

A smart locker for the banking industry has been created in the current work. This work's key feature allows users to determine whether their facial expressions are normal or abnormal before opening a locker if they are. Your photograph will be compared to the information already present in the database by the smart lock application. After verifying the identity of the user, if the user's face appears weird, the locker is not open. The process of determining whether a previously detected object is a known or unknown face is known as face recognition.

Keywords-: Keywords: CNN, speech detection, and facial recognition.

Introduction

A rising interest in biometric approaches is a feature of current authentication systems. Among these methods are the face, facial thermogram, fingerprint, hand geometry, hand vein, iris, retinal pattern, signature, and voiceprint. The distinctiveness, durability, measurability, performance, user acceptability, and robustness against circumvention of each of these strategies vary. The objective of this system is to develop a hybrid biometric system that is independent of all biometric hardware. Biometric authentication, as opposed to password-based or token-based authentication, uses a person's particular biological traits to confirm their identification. Because users do not need to carry a physical token that may be easily misplaced or stolen or remember passwords, it is more difficult to spoof and, generally speaking, more convenient for users. Part of the individual is the authenticator. Speaker recognition is a sort of voice recognition technology. Whilst it is similar to speech recognition, which is utilised in speech-to-text applications, it is not the same. Facial recognition is a form of biometric technique in which a person is recognised by comparing a live image capture with the person's previously recorded data. Differentiating the feature space into live and nonliving is the act of liveliness. Imposters will attempt to insert numerous fake biometrics into the system.A biometric system's

performance will increase with the aid of liveliness detection. The determination of a biometric system's credibility in terms of security against spoofing is a crucial and difficult topic. The typical assault techniques in face recognition can be divided into a few different groups. The classification system is based on the verification evidence that is provided to the face verification system, such as a stolen photo, stolen face photos, recorded video, and 3D face models with the ability to blink and move their lips. Face recognition technology has improved to the point where it is already being tested in actual environments [2].

Literature Survey

To reduce the time and space complexity, the research [1] introduces an enhanced LBP (local binary pattern) system, coding-based feature extraction approach. Using the VAD (voice activity detection) approach, the algorithm's efficacy is increased while the misjudgement ratio for voice endpoints is decreased. In this work, we build and create a multimodal Android-based biometric identification system that uses speech and facial recognition. An authentication system that

has been developed may successfully implement identity authentication in a variety of scenarios and achieve management operations with high security applications. To achieve identity identification, only voice and facial biometrics are taken into consideration; many additional biometrics are not researched. The user experience will be lowered because the registration process requires an excessive amount of training data. The purpose of this effort is to create a system that can manage an office's main entrance utilising speech to text and face recognition [2]. (The system enables staff to open the front door using face recognition rather than tag-keys or cards. An employee is sent a randomly generated code, which must be entered into the screen in order to prevent spoofing attacks and boost security. We used GUI for this project. It allows for the quick display of information for system users and also provides instructions on how to access the office. Both the employee and the visitor find it more pleasant to visualise the data. 1) The prototype works well in an office setting, however facial recognition and speech to text will take longer if it is connected to a slower internet connection. 2) Because the system is cloud-based, an internet connection was always necessary for it to function.The Internet of Things (IoT) is used in this study to be incorporated on the system that has been created for a number of functionalities, including input reception, data storage, and even data processing [3]. While it functions similarly to the fingerprint approach in terms of accuracy and response time, the face recognition method provides greater customer satisfaction. Enrolling the user takes a long time. The image was taken, the facial data was extracted, and the image cache was rebuilt using a separate software. In this paper, a multimodal biometric system is suggested. Our multimodal biometric authentication system is based on the iris, voice, and visage as three different IDs. The first voice recognition described is mel-cepstral. Then, SIFT-based features are used to approach facial authentication [4]. The iris recognition approach based on LAB is then suggested. The decision module is the level at which the biometric fusion is carried out. The feature extraction stage varies between the three recognition systems, albeit they all use comparable supervised classification methodologies.

Problem Statement-:

Create a system that uses facial data to provide locker security.Our project's primary goal is to recognise faces and assess facial expressions. If the face locker opens, it will do so automatically; if not, a notification will be sent.

System Architecture -:

The registration module and the authentication module are the two key modules that make up the developed system. Enter the user name first to check if the user has been registered or not. Otherwise, collect its voice and visage and start the registration process. If not, the user must carry out the authentication process. Then, we may input the voice and face biometric data into the established authentication system to apply the matching fusion and establish if the authentication was successful or not. Face image and audio voice datasets are accepted as input. Output - Output to locate Matched Fusion and determine whether a person is authenticated or not.

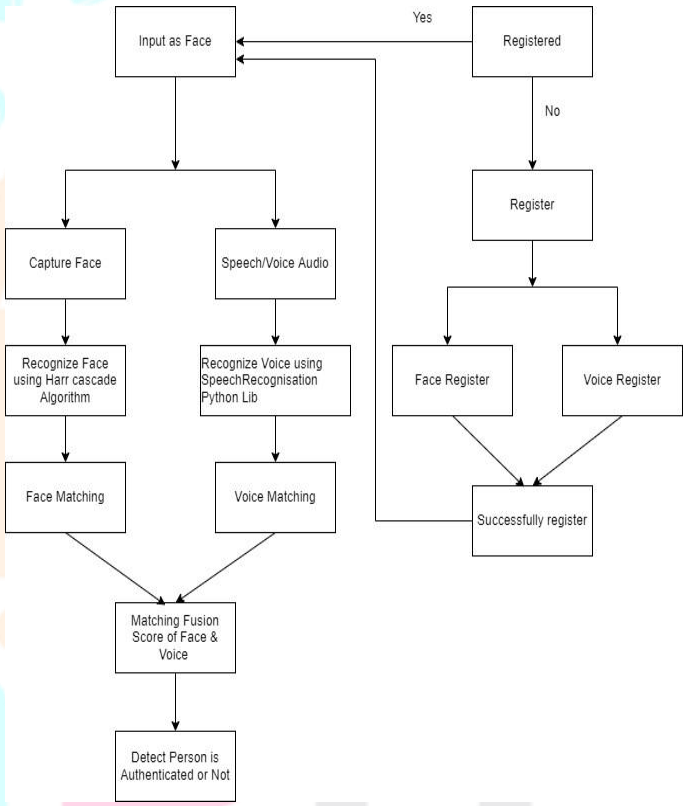


Figure 1.System Architecture

A. Methodology

Using test data, the system is tested to determine its accuracy. The system is put into use in the manner described below:

1) Dataset - Supply dataset (This requires that the data be uniform and understandable for a machine that does not perceive data the same way that humans do.

2) Pre-processing - Real-world data frequently includes noise, missing values, and may be in an unsuitable format, making it impossible to build machine learning models on it directly. Data pre-processing is a necessary step for cleaning the data and preparing it

for a machine learning model, which also improves the model's accuracy and effectiveness.

3)Feature Extraction - By generating new features from the ones that already exist in a dataset, feature extraction tries to reduce the quantity of features in a dataset (and then discarding the original features). The majority of the information contained in the original collection of characteristics should therefore be able to be summarised by this new, smaller set of features.

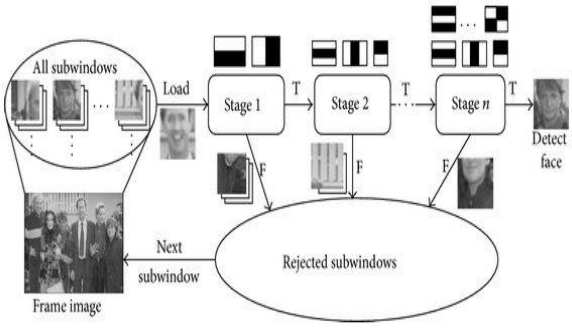
4)Classification - The Classification algorithm, which uses supervised learning to categorise new observations in light of training data, is used to recognise new observations. In classification, a programme makes use of the dataset or observations that are provided to learn how to categorise fresh observations into various classes or groups. The algorithm will determine how many faces are present. the entire description applied to the suggested work.

Algorithm Description

For face detection and face identification in our project, we use two algorithms: the CNN algorithm and the Harr cascade method.

1] **Harr cascade Algorithm:**

We'll use the Haar Cascade classifier to put our use case into practise. The Haar Cascade classifier, developed by Paul Viola and Michael Jones, is a successful object detection strategy. This method essentially uses machine learning, where a cascade function is learned using a large number of both positive and negative images. It is then used to detect the things in the other images based on the training.



Step 1: The image is cut up into smaller pieces before being transmitted to the classifier (or subwindows as shown in the illustration)

Step 2: We arrange N detectors in a cascade fashion, with each one learning a mixture of several feature types from images that are passed through (such as lines, edges, circles, and squares). Allegedly, each sub-part is given a confidence rating after feature extraction is complete.

Step 3: The images (or sub-images) with the highest confidence in being face images are accepted and delivered to the accumulator. As a result, the cascade retrieves the subsequent frame or image, if any, and resumes the process.

CNN Algorithm-:

CNN is utilised in image classification, object detection, face recognition, and image recognition. An image is processed by CNN image classification. Basic object recognition comes after the shape and features of the face are recognised. Afterwards, in order to ascertain its fundamental qualifications, the features of the face are further studied. The shape of the nose, the texture and tone of the skin, the existence of scars, hair, or other surface imperfections are a few examples. The total of these qualifications is then added to the image data analysis of a particular person's appearance. This process involves looking at a lot of samples, each of which presents the topic in a different way.

Results and Evaluation:

There is a critical need for security safeguards against spoof attacks for the general population. The security industry's fastest-growing subset is biometrics. Facial recognition, fingerprint recognition, handwriting verification, hand geometry, retinal and iris scanners are a few of the well-known methods foridentification. Face recognition technology is one of these methods that has advanced quickly in recent years. Face recognition algorithms typically struggle to distinguish between live and dead faces, which is a serious security concern. Face recognition algorithms can be easily tricked using facial images like portrait photos. A secure system needs liveness detection to prevent this spoofing.

Conclusion

This system develops a biometric authentication system that uses voice and face biometrics. In order to reduce time and space complexity and recognise voice, this system introduces an improved LBP coding-based feature extraction method. determining a person's authorization using voice and face recognition. This

technology offers a straightforward development path for the creation of unique face liveness detection methods for bank locker security in the future. This bank locker security system will work well to prevent illegal access and increase dependability through the usage of liveness facial recognition. Compared to the current systems, which are attackable, it may be utilised for user authentication successfully..

References

1) "A New'Method of Finger Veins Detection," International Journal of Bio- Science and Bio Science and Bio Technology, Vol. 1, No. 1, December 2009. Dana Hejtmankov'a, Radim Dvo'rak, Martin Drahansk'y, and Filip Ors' ag.

2) "A finger-vein imaging and liveness detection for identity identification utilising 2-axis MEMS scanner," International Conference on Optical Mems and Nanophotonics (OMN) 2016, Jaekwon Lee, Seunghwan Moon, Juhun Lim, Kwanghyun Kim, Jong-Hyun Lee, Min-Joo Gwak, and KyungSu Kim.

3) Amit Verma, "A Multi Layer Bank Security System," International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), 2013.
4) A Multi Layer Bank Security System by Amit Verma, published in 2013's International Conference on Green Computing, Communication, and Energy Conservation (ICGCE).
5) K. D. Kulat, A. G. Keskar, and V. R. Satpute. "A novel methodology based on 2D—DWT and variance method for people detection and tracking in video surveillance applications" IEEE, 2014. 9th International Conference on Industrial and Information Systems (ICIIS).

6) In 2014, Srivatsan Sridharan published a paper at the ICICES S.A. Engineering College in Chennai, Tamil Nadu, India titled "Authenticated Secure Biometric Based Entry to the Bank Safety Lockers." 318abab6c at overleaf.com/project/638025ea23c1703

7) Amit Verma and Neeraj Khera The Next Generation Information Technology Summit (Confluence), 5th International Conference, "Development of an Intelligent System for Bank Security," 2014.

8) Intelligent Systems and Information Management (ICISIM), 2017 1st International Conference on, IEEE. Ragade, Rupali R. "Embedded home surveillance system with pyroelectric infrared sensor using GSM."

9) Avinash D. Harale, Bhakti B. Bhaganagare, and. "Iris as biometrics for security system," IEEE, 2017's Second International Conference on Electrical, Computer and Communication Technologies (ICECCT).

10) P. P. Gangal et al. "Object recognition and tracking utilising 2D—DWT and variance approach," IEEE, 2014 Students Conference on Engineering and Systems (SCES).