IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 4, April 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 4, April 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1004092|

A Review on Bank Locker Security System using Machine Learning with Face & Liveness Detection

Prof.Aditi D Wangikar, Aditya Sasane, Sourav Kaushal , S. Anudeep, Pramod dhoot

Department of Computer Engineering, JSPM'S Jayawantrao Sawant College of Engineering, Pune, India

ABSTRACT: Assuring the security of transactions is currently one of the most difficult challenges confronting financial systems. Because of its convenience and appeal, biometric verification of customers attracts enormous quantities of money from banks all over the industry. Particularly in offline settings, where virtual selfies are matched to face images from identification documents. In fact, comparisons of selfies with IDs are currently being used in a variety of larger initiatives, such as automated immigration. One of these processes is quite tough because of the disparities between comparative facial photos due to their unique origins. For cross-area matching problems, we propose a single architecture based on deep functions extracted from two properly-referenced Convolutional Neural Networks (CNN). The results of the data gathered, dubbed Face bank, indicate the power of the suggested face-to-face evaluation hassle and its inclusion in actual banking security systems, with over 93 percent accuracy.

KEYWORDS: Convolutional Neural Networks (CNN), Face Financial Institution, Computerized Immigration Management

I. INTRODUCTION

The technique of identifying anything that has already been identified as a regarded or unknown face is known as face reputation. The challenge of facial identification is frequently perplexing, as is the hassle of facial reputation. Face reputation decides whether a "face" is well-known or unknown, depending on the character who uses facial data to verify this facial expression. Face recognition has piqued the curiosity of academics in disciplines ranging from security to photo processing to computer imaginative and prescient since the early 1970s. Face recognition has also shown to be beneficial in the processing of multimedia data. Human face identification is the most promising of several image processing topics, with a large area of research-oriented real-life applications.

II. FACE AWARENESS

DIFFERENT METHODS OF FACE RECOGNITION:

Face recognition can be divided into two categories: geometry (element supported) and photometric (based on visual). As the researcher's interest in facial recognition grows, he develops a variety of algorithms, three of which are well-studied in facial textbooks. There are two primary types of visual algorithms.

Geometry: The geographic position of face characteristics is based on the geometric relationship between landmarks. This means that the essential geometric aspects of the face, such as the eyes, nose, and mouth, are identified initially, and the face is divided based on geometric distances and angles between the elements.

Photometric stereo is a technique for detecting an object's composition from numerous images taken in varied lighting situations. A gradient map, which is made up of the mass of a normal surface, defines the shape of the object.

A. motivation

• The program's main goal is to identify the user.

• Face detection saves time when looking for the user.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 4, April 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1004092|

• Identifies unauthorised users.

MOTIVATION

In recent years, liveness detection has become a popular study topic in the fingerprint and iris reputation communities. However, techniques for dealing with this difficulty in face recognition are severely limited. The act of separating the feature area into stay and non-living is known as liveness. Imposters will attempt to use a wide range of forged biometrics in gadgets. The total performance of a biometric machine will increase with the help of liveness detection. It's a crucial and difficult problem that defines the security of biometric systems against spoofing.

III. LITERATURE SURVEY

[1] Gang Pan et al. The automated exploitation is the current spoofing in opposition to the picture in the visible notion of physical exploitation in real-time bodily acquisition. To avoid spoofing attacks in an innovative way, this solution only requires a regular camera and no additional technology. The blink of an eye is a convenient way to open and close bottles rapidly. Repetition is essential. A normal camera records fifteen frames per second, yielding two face frames that have been utilised in spoofing attacks. 2 framed captives are thought-about frames, respectively. HMM creates possibilities from a small number of countries. The standard HMM active blast exploitation detects spoofing attacks.Anjos et al. [2] describe how to provide modifications for the user's physical state before or after the adjustment. There are two types of movement detection in this method. The relationship between the user's head rotation and its domain is how this method works. Using a good movement guide, examine the author's relationship. The direction of movement is tracked using visible flow. This method is simple, but it requires many frames to examine the physical properties, thus the user must collaborate. The acquisition of physical assets [3] is intended to improve the face recognition system's reliability and security. With completely different approaches, the false face is distinguished from the one with the 000 exploitation tricks. With this research, we offer a single face identification approach based on frequency analysis and discriminatory texture of 2-D paper masks on a live face for assisted face detection.

We used a power spectrum to analyse frequency, and we used an established way of operation [4] that not only exploited low frequency data but also shared data between high frequency regions. It is also commonly utilised in Binary Pattern (LBP) [5]. Quality attack tactics in face recognition can be divided into numerous groups. The notion of differentiation is determined by the type of illuminated image, refined facial images, video recording, and 3D facial models with the capacity to blink and move lips offered by the facial verification system. 3D facial models featuring a variety of expressions, for example [6].

The major goal of this article is to design and build a bank security protection system that uses RFID and GSM technology that may be used in banks, secure offices, and private residences. In both cases, the genuine individual was discovered in a bank township with cash. The RFID reader reads the id list from the entry tags and sends it to the microcontroller. If the id list is active, the microcontroller sends an SMS request to the specified cell range, allowing the first calculator to open the bank lock. If these 2 passwords are similar to a locker unlocked otherwise it will remain in a locked area [7].

Proposed system

Figure 1 shows the system architecture.

• A database must be downloaded from the database and uploaded to our workspace.

• Photographs of the train will be included.

• Individual information must now be separated from data testing and training.

• Cropped and grayscale photos must be downloaded.

• Image elements are now used to extract training databases, which are then calculated and stored.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 4, April 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1004092|

ADVANTAGES

• protection against vulnerabilities such as spoofing, tampering, and masquerade assault, among others.

• Neither the template nor the image is saved.

• enhanced authentication and security assurance Maintaining confidentiality and privacy.

• It can be done in large-scale utilities and public areas with the proper permission.

IV. CONCLUSION

We propose a machine learning-based face detection-recognition and liveness detection system for bank lockers in this study. The user will use a bank locker in this project, which will employ facial detection and liveness techniques. This face-detected locker is superior to typical lockers in that it does not require a traditional key to open. It is a highly dependable strategy for safeguarding our assets.

REFERENCES

1. G. Pan, L. Sun, Z. Wu, and S. Lao, "Eyeblink-based anti-spoofing in face identification from a generic webcamera," in Proc. IEEE 11th Int. Conf. Comput. Vis. (ICCV), pp. 1–8, Oct. 2007.
2. "Motion-based countermeasures to photo attacks in face recognition," IET Biometrics, vol. 3, no. 3, pp. 147–158, Sep. 2014.
3. Pan, Gang, Lin Sun, Zhaohui Wu, and Yueming Wang are the authors of this article. "By combining eyeblink and scene context, monocular camera-based facial liveness detection." 215-225 in Telecommunication Systems 47, no. 3-4 (2011).
4. H. S. Choi, R. C. Kang, K.T. Choi Multiple static features are used to detect fake fingerprints. 48(4), Optical Engineering, 2009.
5. M. Pietikainen and T. Ojala Local Binary Patterns for Multiresolution Gray-Scale and Rotation Invariant Texture Classification. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 24
6. J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on fourier spectral analysis," SPIE vol. 5404, pp. 296-303, 2004.
7. Abhishek Jha, ABES Engineering College, Ghaziabad, "Class Room Attendance System Using Facial Recognition System," The International Journal of Mathematics, Science, Technology, and Management (ISSN: 2319-8125), Vol. 2 Issue 3 (July/August).
8. S. SAYEED, J. HOSSEN, S.M.A. KALAIARASI, S.M.A. KALAIARASI, S.M.A. KALA
9. V. JAYAKUMAR, I. YUSOF, and A. SAMRAJ, "Real-Time Face Recognition For Attendance Monitoring System," Journal of Theoretical and Applied Information Technology, Vol. 95, No. 1, January 15, 2017.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details