Face Biometric Authentication System for ATM Using Deep Learning

Dhanusree S, Saeeda Aseema M, Santhiya R, Mathumitha M*

**Asst.Prof, M.A.M College of Engineering and Technology*

ABSTRACT- Face Biometric authentication technologies have become more popular as the banking industry's need for stronger security measures has increased. Everyone uses automated teller machines, or ATMs, on a daily basis these days. Enhancing security in the banking sector is an important necessity. The ATM has grown unsafe due to a sharp rise in criminal activity and the quantity of offenders. An access card and PIN are currently the only identity verification methods used by ATMs. The risky scenario at the ATM has been much improved by recent advancements in biometric identification technologies, such as finger printing, retinal scanning, and facial recognition. This study suggests a security paradigm for automated teller machines that combines electronic facial recognition with a physical access card via Deep Convolutional Neural Network. Both their accounts and faces would be secured if this technology were to become widely used. In order to remotely certify an unauthorized user, a face verification link will be created and provided to them by certain artificial intelligence agents. Even though it is evident that human biometric traits cannot be duplicated, this idea will significantly address the issue of account security by enabling the account owner to be the only one with access to their accounts.

Keywords: Face Detection, Deep Learning, Image Processing, Neural networks, User Security, Real time monitoring

I.INTRODUCTION

A facial recognition system is a technology that compares a digital image or video frame with a database of faces to identify a person's face. Primarily used for user authentication and identification, this type of device detects and measures facial features from an image. Similar methods were first developed as computer applications in the 1960s. Since then, facial recognition systems have been applied more broadly in robotics, smartphones, and other technological fields. Facial recognition software is classified under biometrics, as it utilizes computerized facial recognition to analyze physiological traits of humans. While iris recognition is considered more accurate than facial recognition and fingerprint recognition, its adoption is limited by its contactless nature. Facial recognition systems have been widely deployed in advanced human-computer interaction, video surveillance, and automatic image indexing. Today, both public and private organizations worldwide use facial recognition technology. However, its effectiveness varies, and some systems have been abandoned due to lack of success. The use of facial recognition technology has sparked controversy due to allegations of privacy infringement, frequent misidentification of individuals, promotion of racial profiling and gender norms, and failure to protect individuals' rights Photographs serve as the foundation for face recognition systems based on deep learning. CNNs excel at understanding spatial hierarchies of information, enabling them to capture complex variations and aspects of the face. By leveraging multiple layers of convolution, pooling, and non-linear activation functions, CNNs can extract high-level representations of faces. This capability enables accurate recognition even in challenging environments. The research introduces a novel method that utilizes deep learning techniques to develop a Face Biometric Authentication System (FBAS) aimed at enhancing ATM security. The proposed system employs CNNs, a type of deep learning technique, to reliably identify and verify users based on their facial traits. The CNN architecture can effectively distinguish between authorized users and imposters because it has been trained on facial image data. Additionally, the system employs techniques like data augmentation and transfer learning to improve generalization and adaptability to various facial features and environmental conditions. Face detection, feature extraction, and authentication are key components of the proposed system. CNN algorithms are utilized for face detection to locate and extract facial regions from input images. These extracted faces then undergo feature extraction using a pre-trained CNN model. For authentication, these attributes are fed into a classifier, typically a softmax layer. The results demonstrate excellent precision, reliability, and robustness in the face of numerous challenges such as changing lighting conditions, occlusions, and facial expressions. The proposed system is well-suited for deployment in ATM environments due to its scalability, efficiency, and real-time processing capabilities. All things considered, the Face Biometric Authentication System

described in this paper is a major improvement over traditional authentication techniques like PINs or passwords, offering consumers a smooth and safe authentication process while reducing associated risks.

A. Background:

A reliable and safe way to confirm people's identities in a variety of contexts, from access control to financial transactions, is biometric authentication. Facial recognition has drawn a lot of interest among the various biometric modalities because it is simple to use and non-intrusive. Automated Teller Machines (ATMs) are crucial points of contact for consumers in the financial services industry to conduct banking operations such cash withdrawals, deposits, and balance inquiries. Facial biometric authentication system integration into ATMs has been suggested as a workable way to improve security and convenience. Personal Identification Numbers (PINs) and magnetic stripe cards are the mainstay of the traditional ATM identification mechanism; however they are susceptible to fraud, theft, and illegal access. The development of deep learning algorithms and the accessibility of high- resolution cameras has led to a rise in the dependability and accuracy of facial recognition technologies. Biometric systems are able to reliably identify people and provide access to their accounts by taking pictures of and examining facial traits like skin texture, iris patterns, and distinctive identifiers like facial landmarks. There are numerous essential parts and procedures involved in the implementation of a face biometric authentication system for ATMs. First, to take user faces during the authentication procedure, high-definition cameras are mounted at the ATM terminals. Deep learning techniques are then used to examine and analyze these photos. These algorithms are trained on enormous databases of face image data in order to precisely identify and validate people. The user's access to the ATM services is granted upon the successful authentication process, provided that the match falls below a predetermined level of resemblance. Convenience and user- friendliness rank among face biometric authentication's main benefits. Users may authenticate themselves more quickly and easily by presenting their faces rather than having to carry physical cards or remember complicated PINs. Facial recognition technology also provides improved security measures because biometric identifiers are by nature distinct and challenging to copy or fake. All things considered, the addition of facial biometric authentication systems to ATMs is a noteworthy development in banking technology that provides users with more security, dependability, and simplicity while making financial transactions.

B. Motivation:

The goal of this project development is to improve financial transaction security and convenience. PINs and magnetic stripe cards are examples of conventional ATM authentication techniques that are vulnerable to fraud and theft. The need for stronger security measures is urgent given the development in advanced hacking techniques. A potential answer is provided by face biometric authentication, which uses distinctive facial traits to confirm identity. Artificial intelligence's deep learning subgroup has demonstrated impressive results in facial recognition challenges, sometimes even outperforming human ability. ATMs can reliably recognize people based on their facial features by using deep learning algorithms, enabling a safe and effective identification process. Furthermore, by lowering the possibility of unwanted access, face biometric authentication improves security. To access an account, a fraudster would still need to get past the face recognition system, even if they manage to steal the victim's ATM card or PIN. The distinct biological characteristics of every person's face pose a significant challenge for counterfeiters seeking to trick the system, so offering an extra degree of security against identity theft and fraudulent transactions. Additionally, the use of facial biometric authentication is consistent with the growing trend in a variety of industries towards biometric-based security systems. When compared to conventional methods of verification, biometrics—such as fingerprints, iris scans, and facial recognition—offer a more dependable and user-friendly solution. As technology develops, incorporating biometric authentication into ATM systems is a proactive way to keep ahead of security risks and satisfy changing customer demands. The overall goal of utilizing deep learning to develop a Face Biometric Authentication System for ATMs is to improve customer experience, convenience, and security during banking transactions. ATMs may improve authentication procedures and reduce the possibility of fraud by utilizing deep learning algorithms, which would ultimately increase consumer confidence and trust.

RELATED WORKS

Pablo negri investigate the addition of several discriminative and generative models to the Probabilistic Linear Discriminant Analysis (PLDA) methodology. The goal of these models is to separate identification from other alterations in the face (such as those brought on by aging). Therefore, they can enhance the features of age invariance of the most advanced deep face embeddings. In this study, we experiment with the Pairwise Support Vector Machine (PSVM), a non- linear version of PLDA, and a standard PLDA. As a novelty, we also introduce a nonlinear version of PSVM called NL– PSVM. Our experiments also demonstrate the efficacy of both PLDA and its proposed extensions in mitigating the age sensitivity of the facial features, particularly in cases where age differences between the compared images are substantial (greater than ten years) or where age-related changes in the face are more noticeable, like in the transition from childhood to adolescence or from adolescence to adulthood. Additional testing on three common cross-age benchmarks (MORPH2, CACD-VS, and FG-NET) validates the efficacy of the suggested models. [1].

Zuolin Dong proposes a cascaded intelligent face identification method focused on videos that develops a deep learning network layer by layer by cascading various features, such as edge, contour, local, and semantic information. The information of the input data is gathered to accurately achieve face detection under non-ideal conditions, based on the final semantic features. The approach exhibits excellent resistance against spinning faces and good detection performance for both single and multi-face images, according to simulation findings. Simultaneously, the algorithm exhibits speed and meets the necessary requirements for real-time face detection. [2].

Xiang Wang These days, it's common practice to outsource facial recognition to a service provider. However, given the sensitivity of facial data, it raises serious questions regarding the outsourcing server's privacy. Thus, this study presents a framework for identity authentication based on privacy-preserving facial recognition

technologies. The extraction of facial features is done via the convolutional neural network. A secure nearest neighbor method that can compute the cosine similarity over encrypted feature vectors is suggested to address the privacy leak problem. Furthermore, by transferring some processes from the cloud to the edge of the Internet, edge computing is included in our framework to improve the efficiency of authentication. [3].

Hasini Gunasinghe introduce a biometrics- based authentication system that protects user privacy that allows users to authenticate to various service providers from their mobile devices without involving identity providers in the transaction. Three-factor authentication is used for authentication, which is accomplished by zero-knowledge proof of knowledge based on a cryptographic identification token that encapsulates the user's biometric identifier and a secret that they have supplied. Our method relies on a machine learning-based classification algorithm that uses the features derived from the user's biometric image to create a unique, repeatable, and revocable biometric identifier from the biometric image. A prototype of the suggested authentication system has been put into practice, and its security, privacy, and performance have all been assessed. The assessment was carried out using a publicly available data set of images [4].

Yukun Mal proposes a facial verification method that is encrypted. In this work, deep neural networks are used to extract facial traits, which are subsequently encrypted using the Paillier technique and stored in a data set. Three parties make up the system's framework: the client, the data server, and the verification server. The client is in charge of gathering requester information and forwarding it to the servers, the data server stores the encrypted user features and user ID, and the verification server handles verification. Since the data is shared in cipher text, only the verification server and the other parties are aware of the private keys. Two deep convolutional neural network architectures are used to test the suggested approach on the labeled faces in the Faces and Wild data sets. The comprehensive experimental results, which encompass results for both identification and verification tasks, demonstrate that our method can improve a recognition system's security while minimizing accuracy loss. As a result, the suggested approach is effective in terms of high verification accuracy as well as security. [5].

PROBLEM STATEMENT

Ensuring the security of personal banking information is paramount. Traditional authentication systems like

passwords and PINs are susceptible to fraud, theft, and unauthorized access. To mitigate these risks, there is a growing interest in employing biometric authentication methods for secure access to automated teller machines (ATMs). Facial recognition technology offers a practical and secure authentication method. However, current facial recognition technology for ATMs has several limitations. It often relies on weak learning strategies that are unreliable and inaccurate in real-world scenarios. Moreover, these systems can be vulnerable to spoofing attacks, where unauthorized individuals attempt to deceive the system with images or other methods. This project aims to enhance security and convenience by leveraging facial recognition technology to address these issues. Deep learning is a branch of artificial intelligence (AI) that simulates how neural networks in the human brain work. It has shown impressive results in a number of computer vision applications, including facial recognition. The suggested method will evaluate and authenticate user faces taken by the ATM's camera using deep learning algorithms. The system can accurately validate the identification of the user by matching the taken face image with a pre- registered template that is kept in the database. By doing away with the necessity for users to memorize and enter PINs, this biometric authentication procedure lowers the possibility of unwanted access considerably while improving user experience.

SYSTEM ARCHITECTURE

The suggested solution incorporates facial recognition technology to improve banking operations' security and user experience. Fundamentally, this technology uses deep learning algorithms to identify and verify people using only their face traits. This system's architecture is made up of multiple essential parts that cooperate to provide dependable and smooth authentication. First, the system collects real-time facial photographs using a powerful data collecting module. To aid with supervised learning, matching identification labels have been tagged into these photos. Second, convolutional neural networks (CNNs), which excel in extracting features from images, are used during the training phase. These CNNs are taught discriminative facial traits that are particular to each person using the gathered dataset. Multiple forward and backward pass iterations are used in the training process to optimize the network's parameters and reduce classification error. The deep learning model is installed on the ATM terminals and used as the authentication engine after it has been trained. Using a camera built into the ATM terminal, the technology takes a real-time picture of the user's face when they approach the machine to complete a transaction. The installed deep learning model for facial recognition then receives this image as input. In order to recognize an image, it must first be compared to the learnt representations that are kept inside the parameters of the model. The system evaluates whether the user's identity matches the one linked to the ATM card by comparing the similarity between the input image and the stored representations. Finally, the user is given access to their account so they can complete transactions after their authentication is successful. Appropriate error handling techniques are used in the event of a mismatch or inability to authenticate in order to maintain security and stop unwanted access. the use of deep learning methods to the development of a facial biometric authentication system for ATMs, with a focus on MySQL database management and Python programming. For the system to be deployed in ATM situations, real-time camera capture must be integrated with the created model. Real-time face detection and recognition from the webcam feed can be accomplished with Python tools like OpenCV. Python is a great option for constructing the face biometric authentication system's backend logic because of its large library and frameworks. Developers can easily incorporate real-time face detection and recognition capabilities into the ATM system by utilizing frameworks like TensorFlow and OpenCV. Strong image processing features offered by OpenCV enable the system to effectively extract faces from the ATM's video feed. Conversely, TensorFlow makes it easier to build and use deep learning models for tasks involving facial recognition. The user's face should be correctly recognized by the system, which will subsequently authenticate them using the enrolled database. Users who have enrolled

can have their biometric data safely stored using the MySQL system. The facial features of each user can be saved in the database with their associated account details as feature vectors or embedding.

PROPOSED SOLUTION

1) Face Detection:

The first phase in the biometric authentication process is face detection, in which the system searches for and

recognizes human faces in pictures or video feeds. Real-time facial detection is essential for precisely identifying users in the context of an ATM authentication system. Convolutional Neural Networks (CNNs), one of the deep learning algorithms that are frequently used for this job, are effective in detecting faces in a variety of lighting conditions and orientations. The ATM's camera input is processed by the face identification module, which then extracts and identifies faces for additional analysis.

2) Preprocessing:

In order to increase the precision of the ensuing processing stages, preprocessing entails cleaning and refining the facial pictures acquired during face detection. To provide consistent input for the feature extraction module, this may entail operations like noise reduction, scaling, and normalization. Preprocessing helps reduce lighting, position, and face expression fluctuations that may have an impact on the authentication system's effectiveness.

3) Feature Extraction:

A crucial step in face biometric authentication is feature extraction, which involves identifying facial traits being taken out and condensed into a format that can be compared. Deep learning methods are used to extract discriminative characteristics from preprocessed facial photos, such as facial landmark detection and deep feature extraction networks. These traits, which are used for identification verification, capture distinctive elements of the face, such as the placement of the mouth, nose, and eyes used for identity verification.

4) Face Recognition:

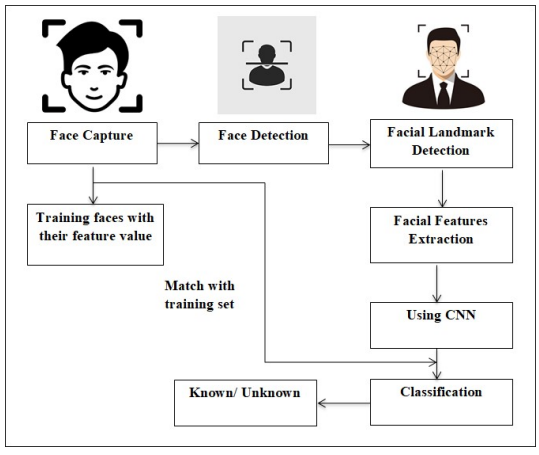
In order to confirm the user's identification, face recognition compares the retrieved facial features with those kept in the system's database. To assess whether a match exists, facial feature vectors are compared using deep learning-based face recognition algorithms like Siamese networks or triplet loss networks. A confidence score or probability reflecting the possibility of a successful authentication is output by the facial recognition module.

5) User Enrollment and Database Management Module:

Enrolling users in the system and maintaining the database containing their facial biometric information are the responsibilities of this module. Users' facial photos are taken at enrollment, processed, and generated into biometric templates that are safely kept in the database with matching user identifiers. In addition to putting security measures in place to safeguard sensitive biometric data, the database administration component makes sure that user records are retrieved and updated efficiently.

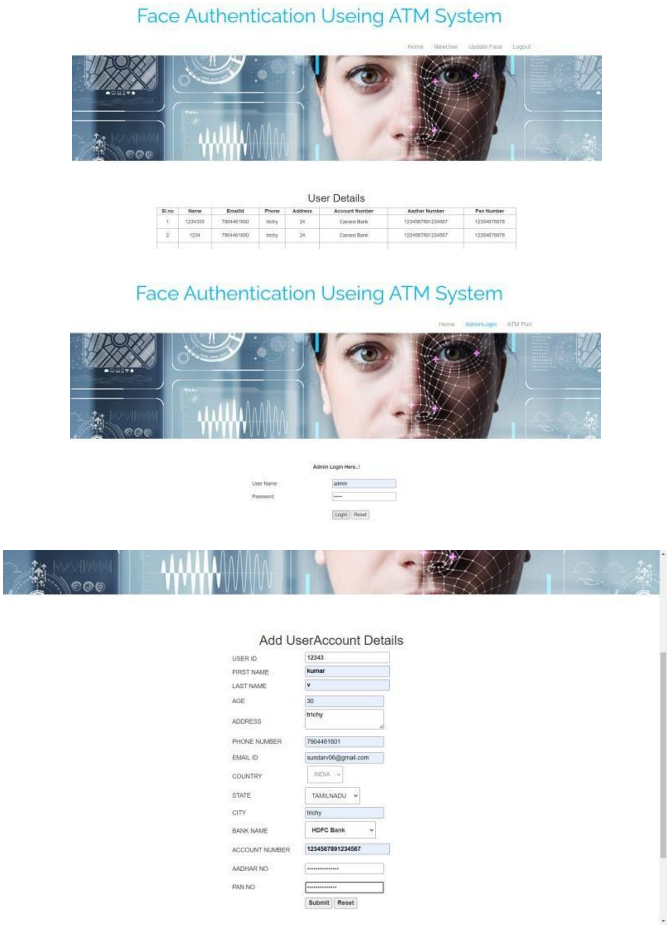
6) Integration with ATM Interface Module:

The ATM's user interface and the face biometric authentication system can be seamlessly integrated thanks to the integration module. This entails creating user-friendly interfaces for taking facial pictures, showing the authentication status, and giving users feedback while they authenticate. User authentication is made frictionless by integration with the ATM interface, negating the need for extra hardware or difficult setup processes.



Proposed Architecture Diagram

RESULT AND DISCUSSION



CONCLUSION

A major improvement in ease and security for banking operations is the deep learning-based integration of face biometric authentication systems in ATMs. A notable achievement in financial transaction security measures is the creation and deployment of a Face Biometric Authentication System for ATMs utilizing deep learning technology. Compared to conventional authentication techniques, this approach has a number of significant benefits, such as improved accuracy, ease of use, and fraud resistance. First off, the system can consistently and precisely identify people based on their facial traits by utilizing deep learning algorithms. This simplifies the authentication procedure for users and improves security by guaranteeing that only authorized users can access their accounts. It also does away with the need for tangible tokens or passwords.. Furthermore, by utilizing deep learning, the system can adjust and get better over time, continuously honing its recognition skills to better discern between authentic users and any imposters. The system's ability to adapt to changing security threats is ensured by its dynamic nature. Furthermore, customers can benefit from a high degree of ease when facial biometrics are used at ATMs. Rather than needing to carry out complicated password entry or remember them, users can expedite the authentication procedure by just presenting their faces. This lessens the possibility of forgotten passwords or login issues while also improving the user experience overall. Additionally, because the system relies on facial biometrics, it is naturally resistant to several types of fraud, like password theft and card skimming. Users can transact with better peace of mind because the risk of unlawful access is greatly decreased due to the distinctiveness and difficulty of each person's face features.

FUTURE WORK

In order to increase the efficacy, security, and usability of the Face Biometric Authentication System for ATM using Deep Learning, there are a number of important aspects that need to be expanded upon and improved in the future. First, more study and improvement may be done to raise the deep learning models' accuracy and resilience in face recognition. This involves investigating sophisticated neural network topologies, like capsule networks or attention mechanisms, to handle lighting, position, and face expression fluctuations and better capture facial information. Incorporating multi-factor authentication techniques is another way to improve the security of the authentication system. This could entail adding extra security features like speech recognition or behavioral biometrics, or merging facial recognition with other biometric modalities like fingerprint or iris detection. Moreover, to guarantee real-time performance on ATM hardware with constrained processing power, the computational efficiency of the deep learning methods must be maximized. This could entail using methods like compression, pruning, or model quantization to lower the models' computational complexity while keeping their accuracy high. The creation of a user-friendly ATM authentication system interface is a crucial component of upcoming work. This entails creating user-friendly interfaces for face enrollment and authentication procedures and giving users unambiguous feedback regarding the outcome of their authentication efforts.

REFERENCES

[1] Negri, Pablo, SandroCumani, and Andrea Bottino. "Tackling age- invariant face recognition with non- linear PLDA and pairwise SVM." IEEE Access 9 (2021): 40649-40664.

[2] Dong, Zuolin, Jiahong Wei, Xiaoyu Chen, and PengfeiZheng. "Face detection in security monitoring based on artificial intelligence video retrieval technology." Ieee Access 8 (2020): 63421-63433.

[3] Wang, Xiang, HeyuXue, Xuefeng Liu, and Qingqi Pei. "A privacy-preserving edge computation-based face verification system for user authentication." IEEE Access 7 (2019): 14186-14197.

[4] C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of ELECTRICAL ENGINEERING, Vol.63 (6), pp.365-372, Dec.2012.

[5] C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011.

[6] C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor & Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011.

[7] C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.

[8] G.Nagarajan C., Neelakrishnan G., Akila P., Fathima U., Sneha S. "Performance Analysis and Implementation of 89C51 Controller Based Solar Tracking System with Boost Converter" Journal of VLSI Design Tools & Technology. 2022; 12(2): 34–41p.

[9] G.Nagarajan, G.Neelakrishnan, R. Janani, S.Maithili, G. Ramya "Investigation on Fault Analysis for Power Transformers Using Adaptive Differential Relay" Asian Journal of Electrical Science, Vol.11 No.1, pp: 1-8, 2022.

[10] G.Neelakrishnan, K.Anandhakumar, A.Prathap, S.Prakash "Performance Estimation of cascaded h-bridge MLI for HEV using SVPWM" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:750-756

[11] G.Neelakrishnan, S.N.Pruthika, P.T.Shalini, S.Soniya, "Perfromance Investigation of T-Source Inverter fed with Solar Cell" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:744-749

[12] C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007

[13] M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022

[14] M Suganthi, N Ramesh, CT Sivakumar, K Vidhya, "Physiochemical Analysis of Ground Water used for Domestic needs in the Area of Perundurai in Erode District", International Research Journal of Multidisciplinary Technovation, pp: 630-635, 2019

[15] Gunasinghe, Hasini, and Elisa Bertino. "PrivBioMTAuth: Privacy preserving biometrics-based and user centric protocol for user authentication from mobile phones." IEEE Transactions on Information Forensics and Security 13, no. 4 (2017): 1042-1057.

[16] Ma, Yukun, Lifang Wu, XiaofengGu, Jiaoyu He, and Zhou Yang. "A secure face-verification scheme based on homomorphic encryption and deep neural networks." IEEE Access 5 (2017): 16532-16538.