Frontiers in Health Informatics
ISSN-Online: 2676-7104
www.healthinformaticsjournal.com
2024; Vol 13: Issue 7
Open Access

Blockchain-Assisted Machine Learning For Securing Mobile Ad-Hoc Networks Against Black-Hole Attacks

Thirupathi Nanuvala[1],Baddam Rithika Reddy[2],Kanduri Sahith[3],Saroj Vihung[4], Samala Keerthi[5], Savarapu Omkaarini [6]

[1]Assistant Professor ,Department of CSE VNRVJIET, Hyderabad – 500090 Telangana, India
[2]Department of CSE VNRVJIET, Hyderabad – 500090 Telangana, India
[3]Department of CSE VNRVJIET, Hyderabad – 500090 Telangana, India
[4]Department of CSE VNRVJIET, Hyderabad – 500090 Telangana, India
[5]Department of CSE VNRVJIET, Hyderabad – 500090 Telangana, India
[6]Department of CSE VNRVJIET, Hyderabad – 500090 Telangana, India

Cite this paper as: Thirupathi Nanuvala,Baddam Rithika Reddy,Kanduri Sahith,Saroj Vihung, Samala Keerthi, Savarapu Omkaarini (2024). Blockchain-Assisted Machine Learning For Securing Mobile Ad-Hoc Networks Against Black-Hole Attacks. *Frontiers in Health Informatics*, *13 (7) 553-560*

Abstract—Biometrics, such as scanned fingerprints and irises have been revolving around the theme of identity cross verification for quite a while, however during such processes, performance and scalability find it difficult to scale especially when it comes to the vast data base sets. The research introduces new means of time capture whereby multi-face recognition technology would be utilized. The proposed method is in stark contrast with most biometrics as it provides rapid mass identification of several individuals as opposed to one at a time. The goals of this system are the integration of algorithms which perform facial recognition, spoof detection and the exact identification of the sought person. The system provides effective and robust means of capturing attendance and dealing with problems like identity theft and unauthorized attendance.

I. INTRODUCTION

Multi-faced attendance systems are the newest attendance tracking systems used to recognize one or more people simultaneously, and advanced computer algorithms further enhance their typical accuracy and scalability even in unsupportive environments with mixed lighting and facial expressions. The design of the system begins with the Haar Cascade classifier for face detection that restricts its focus to relevant areas. This is followed by usage of FaceNet to uniquely generate facial embeddings that could be then used to recognize multiple faces in one single frame.

Security will be ensured with Convolutional Neural Networks (CNN) identifying and blocking access frauds before it can be secured and attempted. The system is very much easy to use by schools, offices, and other industries and gives real-time attendance data to administrators. Thus, in the direction of its user-friendliness and privacy compliance, this system serves not only to ease attendance issues but also takes into account the ever-changing challenges biometric technology faces, in this dynamic world.

II. MODULES IN MULTI FACE RECOGNITION SYSTEM

2.1 Face Detection

When people come in front of the camera, the system isolates your face from the remaining area using bounding boxes. Red rectangular boxes are drawn around the faces to separate the faces from the captured frame. This is achieved using the Haar Cascade model.

Haar Cascade is an object detection model which uses the concept of Haar Features, which are rectangular features that capture the variation of intensity within images.These features, inspired by Haar wavelets, are created to convey patterns like edges, lines, and rectangles by evaluating the difference in intensity between distinct regions in the image.

To identify the most relevant features, the Haar Cascade uses the AdaBoost Algorithm based on boosting. This is an ensemble technique that is used to obtain a strong classifier by combining multiple weak classifiers. Adaboost iteratively considers those distinguished features which are present in positive examples and absent in negative examples to train the classifier.

During the object detection process, the image or frame is scanned using a sliding window. In this process, each window is analyzed by multiple classifiers and eventually the window is classified either as object present or object absent. This method is fast and is capable of detecting multiple objects within an image in various lighting conditions.

2.2 Face recognition

The entire process of face recognition with FaceNet has many distinct stages and uses advanced deep learning algorithms to become highly accurate and efficient. Initially, FaceNet uses the deep convolutional neural network (CNN) to extract features from face images. This is achieved through training the model on a huge dataset of labeled face images where the network learns how to transform the face images into a small and high-dimensional feature vector space. During training, the network learns and identifies those unique qualities that make up a particular individual, and therein lies the face, which subsequently will also be used to score the person. Such feature vectors are often referred to as embeddings but should keep the relation of proximity, such that similar faces should be clustered together within the vector space while dissimilar ones remain well apart.

The model runs on a loss function called triplet loss. In this way, it takes three images into account: an anchor image, a positive image (another image of the same person as the anchor) as a negative image (an image of another person). Minimizing the distance between the anchor and positive embeddings while maximizing the distance between the anchor and negative embeddings is the goal. The more such training samples feed into the model, it learns to create the clustered spaces of faces from a particular person and differentiate them from a completely different person.

An input image of a face undergoes the facial encoding through a trained model of FaceNet, and the generated embedding is compared against a known face embedding database using a similarity metric-the most commonly used metric being cosine similarity or Euclidean distance. The known face whose embedding is closest to that of the input face is identified as the matched person. This method allows FaceNet to perform very accurate and efficient face recognition, even under changes of pose, illumination, and expression.

The scalability and performance dimensions of FaceNet are thus among the best. The embedding space produced by FaceNet is very discriminative-it captures even small differences between faces. As a result, FaceNet can be used for the

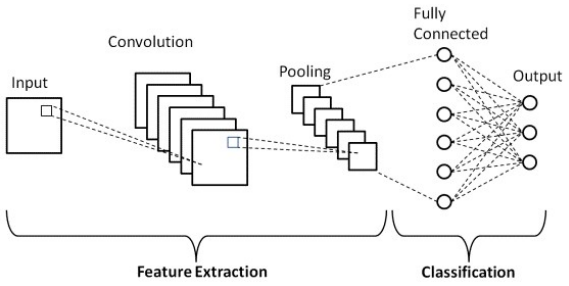
management of large-scale efficient face recognition tasks. Moreover, the embeddings can be used for various applications other than that in face recognition, such as face verification and face clustering. This makes FaceNet truly an all-in-one tool in the domain of computer vision.

2.3 Anti-spoofing model

Classification of images into a genuine or spoof using Convolutional Neural Network (CNN) has several processes that enables it to differentiate between both the genuine and artificially presented input into the system.

First, the feature extraction from the input image is obtained through a series of convolutional layers. These layers create small filters that collect different aspects of an input image, such as edges, textures, and patterns. The special usage for spoof detection there tends to be those kinds of qualities that indicate manipulation, like unnatural texture or an inconsistency that is present in images or videos viewed by the system instead of a live person. They are therefore made to present more complex features over time, such that the network can recognize even small differences between a real image and a spoof.

Following feature extraction, the CNN uses max pooling for spatial dimensions. This process actually condenses the feature maps, taking in maximum values from predetermined areas thereby emphasizing on more salient features while cutting back on computation. This becomes important, therefore, in optimizing the processes of data so that there would be not too much excess detail which has nothing to do with spoofing detection and overloads the whole network.



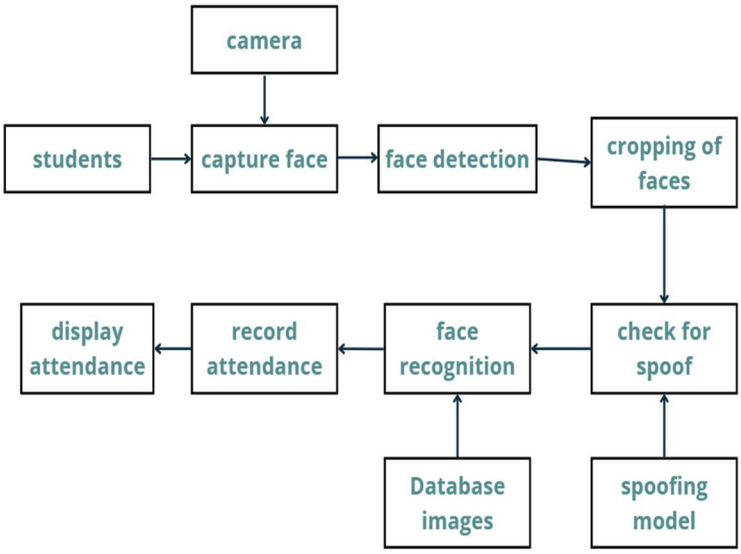
An Adaptive Average Pooling layer in the CNN takes care of the irregularity in image sizes so that all subsequent input will flow steadily through the network. The dimension of all output feature maps is standardized at a fixed size, e.g. 4x4 pixels irrespective of the actual dimension of the image. This standardization would ensure a similar good process for images that carry different sizes, clearing the image for the last classification process.

The processed features are given to the fully connected layers during the classification phase. These layers merge and comprehend the features and make predictions to determine if the image is a real or spoofed one. The output probabilities for the classes (genuine or spoofed) are obtained from the last fully connected layer using a sigmoid activation function. Conversion of this nature enables the network to ascertain whether an image is of a live person or is just a static photo or video, thus being classified as real or spoofed. The CNN makes precise classifications by understanding features and patterns signifying some anomalies with respect to spoofing; thus, it would make a great panacea for a secure and reliable

face recognition system.

III. ARCHITECTURE

The face-recognition-based attendance system starts with capturing the images of students entering the premises with the help of a camera. The algorithms used for this purpose may include Haar Cascade or others for face detection. The purpose of this step is to detect and locate the area of the image containing the face. Once this is done, the face is cropped so that only the region of interest, which is the face, remains, and the background information is discarded, thus making



the pictures suitable for further processing.

The cropped faces are then passed to the face recognition module using a pre-trained model-such as FaceNet. The model generates embeddings that are numeric representations of the extracted facial features corresponding to each captured image. These generated embeddings are then matched with the embeddings already stored in the database where information about all registered students is kept. The system matches each detected face to the appropriate identity in the database so as to recognize the students.

The system also provides an anti-spoofing mechanism for the faces captured. This is a critical step to avoid spoofing attempts for breaking into the system, such as pictures and videos. A deep learning model, able to distinguish between live faces and fake inputs, analyzes the cropped facial images. Fake faces are not considered for further steps.

Upon successful face authentication and match with a database entry, attendance for that specific student is recorded. Attendance is recorded in a database, which would be used for the administration purposes. The system also shows attendance on real-time models, allowing both students and administrators to verify the records made. This system architecture creates more robust and secured attendance automation while retaining higher accuracy and efficiency.

IV. TRAINING MODELS

The recognition system basically consists of a pre-trained FaceNet model that is designed to produce particular vector representation from facial images that are also prepared through face region detection by Haar cascade classifiers and crop-resizing to meet the input criteria of the FaceNet model. Training of such a system occurs with deep convolutional

neural networks (CNNs) which enable learning of those features that will describe the specific peculiar structure of someone's face. Data might be of the following three categories of images: the anchor image of a focal person, a positive image of the same person, and a negative image of another individual, thus training the model to ensure that both anchor and positive image embeddings are closer to one another while ensuring that negative image embedding is pushed far away. This indeed yields the most trustable and accurate facial recognition.

To accompany the whole system of recognition, an anti-spoofing model is used for added safety. The anti-spoofing model analyses pictures by means of convolutional layers that will base their functioning with respect to texture information in spoof identification. The model is constituted from an amalgamated real-and-fake face image data set, which enables the model to identify real users from a fraudulent contestant. It also enables the system to successfully block unauthorized entries under spoofing.

The model is trained over numerous epochs and modified in that manner for a long time to adjust the values within the model parameters for reducing errors. By the time training is done for the model, it will accurately recognize faces and detect spoofing attempts. It is this combination of accuracy and security that renders it well-suited for applications requiring stringent authentication.

V. OBJECTIVE

The primary purpose of this system is to provide a scalable and dependable system that uses advanced technologies to address the drawbacks of standard biometric methods such as fingerprints or eyes. Traditional systems offer advantages, but they frequently cause issues with scalability and efficiency, particularly in real-time systems with big populations. Because of their configuration, they are only intended to function with one person at a time, making them unsuitable for scenarios in which numerous persons must be identified fast. Furthermore, such systems are vulnerable to small concerns like identity theft and unauthorized attendance, which can skew the accuracy of attendance system statistics.

The purpose of this project is to develop a better system that can recognize numerous faces at once, which will be useful for marking students' attendance records. This technique solves some of the problems of traditional attendance systems, such as long waits. This system focuses on accuracy and robustness in detecting spoofing.

VI. EXPERIMENTAL SETUP AND RESULTS

7.1 Experimental Setup

This project employs a well-designed setup to realize some reliable anti-spoofing detection and facial identification. A face recognition model generates facial embeddings, which are compared with stored embeddings for identity verification. This mechanism ensures attendance is assigned to a very genuine person as it can effectively differentiate between the real and spoofed inputs. It can process a video feed in real-time and analyze a static image, which gives accurate and consistent results. To increase its reliability, the model uses datasets of authentic versus spoofed facial images during testing.

Tools and Libraries

The system is built using a wide range of tools and libraries.

- **Deep Learning Frameworks:**
  To build and train neural networks, for face recognition and face embeddings generation.

- **Image Processing Libraries:**
  The predominant function of these libraries is to detect facial features on video feeds and images along with enforcing validation workflows.

- **Numerical Computing Libraries:**
  These make such mathematical operations easier from dealing with arrays to processing models' input and output efficiently.

- **Pre-trained Models for Face Recognition:**
  They provide an efficient way to obtain embeddings and perform facial matching in both real-time and batch modes.

7.2 Results

The system performance was evaluated on the basis of misclassifications, looking at trends and areas where improvement is required.

It has been observed that the average inference time required to process a single frame-from face detection to spoofing and face recognition-was also measured. On GPU setups, the average processing time per frame was 100–300 ms, which could facilitate nearly real-time working. On CPU-only setups, the inference time averaged 400–1500 ms per frame, thus making it relatively more suited for a batch-mode processing or applications with less stringent demands for real-time operation. These findings show how extended efficiently functioning mechanisms could evolve based on the optimization of the hardware.

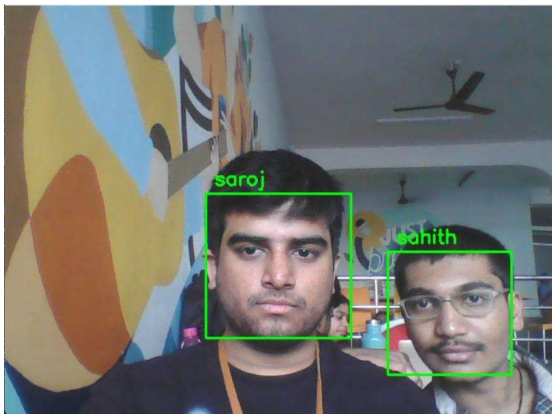


Fig 1 : Face recognition

Fig 1 shows two figures, namely 'saroj' and 'sahith,' identified via bounding boxes. The labels imply a face recognition system is tagging individuals in real-time.

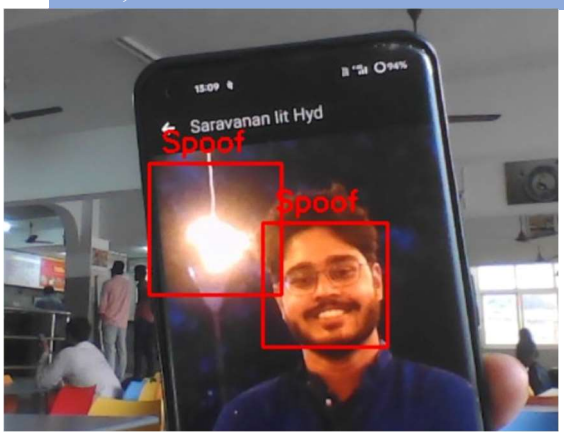


Fig 2: Spoof detection

Fig 2 illustrates a potential spoof detection system. It shows a phone screen with a face displayed and labeled with red bounding boxes marked as "Spoof."

Poor light conditions, such as weak or unevenly distributed illumination, were found to adversely affect the detection and recognition accuracy of faces. Similarly, extreme facial poses, other than nominal, such as faces taken at strange angles or which are only partially visible, increased misclassification rates. This indicates the necessity to improve the robustness of the model in critical scenarios.

VII. AREA FOR FUTURE WORK

Face recognition-based attendance systems have the potential to evolve far beyond their current capabilities, paving the way for significant innovations and enhancements. One key area for advancement is enhancing the system to handle challenging scenarios, such as distinguishing between identical twins or recognizing individuals with facial hair, caps, or masks. With the increasing use of masks in public settings and varied facial appearances, algorithms can be improved to account for these variations while maintaining high accuracy.

Another area of improvement involves adapting the system to work effectively under adverse conditions, such as poor lighting, occluded faces, or unconventional camera angles. Advanced deep learning techniques and diverse training datasets can enable the system to perform reliably in such real-world scenarios. Additionally, combining face recognition with other biometric methods, such as iris scanning or voice recognition, can make the system more secure and versatile. These systems can also expand their application in large-scale environments, such as smart cities or IoT-enabled spaces, where they could seamlessly integrate with other smart devices. This would enable real-time monitoring and management of attendance for thousands of individuals, catering to schools, workplaces, public gatherings, and beyond. Such advancements would make face recognition-based attendance systems more robust, scalable, and adaptable to diverse use cases.

VII. CONCLUSION

This model provides an efficient method for streamlined attendance monitoring using computer vision algorithms. This model uses Haar Cascade, FaceNet and CNN for achieving efficient attendance marking enabled with anti spoofing capabilities. This technique also solves common problems such as face expressions, lighting conditions as well as spoofing attempts. This system enables us to keep a track of the student attendance by storing the attendance along with their entry time. This approach can reduce the time consumed in the conventional process and reduce the chances of

proxies.

This system achieves a considerable amount of accuracy without compromising with the security. It records the attendance of only genuine faces by preventing any fake attendance attempts using Anti-spoofing. This system is much faster and reliable compared to the existing systems and can further be improved considering several other conditions such as considering masked faces, voices etc.

REFERENCES

[1] S. Hapani, "Automated Attendance System Using Image Processing," in Proceedings of IEEE Conference on Automated Systems, 2023.
[2] S. Sathyanarayana, "Automatic Student Attendance Management System Using Facial Recognition," in International Journal of Emerging Trends in Computer Science and Engineering (IJETCSE), 2023.
[3] N. Kanchan, "Attendance Management System Using Hybrid Face Recognition Techniques," in Proceedings of IEEE Conference on Hybrid Recognition Techniques, 2023.
[4] S. Chintalapati, "Automated Attendance Management System Based on Face Recognition Algorithms," in Proceedings of IEEE Conference on Face Recognition Algorithms, 2023.
[5] E. Vardharajan, "Automatic Attendance Management System Using Face Detection," in Proceedings of IEEE Conference on Face Detection Systems, 2023.
[6] "Face Recognition Attendance System Using Machine Learning and Deep Learning," in Proceedings of the Conference on Machine Learning and Deep Learning Techniques, 2023.
[7] "Intelligent Attendance System with Face Recognition Using the Deep Convolutional Neural Network Method," in Proceedings of the Conference on Deep Convolutional Neural Networks, 2023.
[8] "Automatic Attendance System Using Face Recognition Technique," in Proceedings of the Conference on Automatic Systems Using Face Recognition, 2023.
[9] "Face Recognition Attendance System Based on Real-Time Video Processing," in Proceedings of the Conference on Real-Time Video Processing, 2023.
[10] "Deep Facial Recognition Using TensorFlow," in Proceedings of the Conference on TensorFlow for Facial Recognition, 2023.
[11] "Face Recognition-Based Lecture Attendance System," in Proceedings of the Conference on Lecture Attendance Systems, 2023.
[12] "Face Detection and Recognition Using the Viola-Jones Algorithm, Principal Component Analysis (PCA), and Artificial Neural Network (ANN)," in Proceedings of the Conference on Face Detection Algorithms, 2023.
[13] "Appearance-Based Facial Detection for Recognition," in Proceedings of the Conference on Appearance-Based Detection Techniques, 2023.
[14] "Algorithm for Efficient Attendance Management: Face Recognition-Based Approach," in Proceedings of the Conference on Efficient Attendance Management Algorithms, 2023.