Implementation Face Recognition Attendance Monitoring System for Lab Surveillance with Hash Encryption

F Hamami\textsuperscript{1}, I A Dahlan\textsuperscript{2}, S W Prakosa\textsuperscript{3}, K F Somantri\textsuperscript{4}

\textsuperscript{1}School of Industrial and System Engineering, Telkom University Bandung, Indonesia
\textsuperscript{2}Military Engineering Faculty, Indonesia Defense University Bogor, Indonesia
\textsuperscript{3}Electronic and Computer Engineering, National Taiwan University of Science & Technology, Taipei, Taiwan
\textsuperscript{4}Faculty of Mathematics and Science, Universitas Pendidikan Indonesia, Bandung, Indonesia

Abstract. Face recognition (FR) is becoming popular to identify people. In fact, using the FR scheme, surveillance tasks can be built by recognizing people from their faces. This paper presents the implementation of face recognition as a biometric method for smart attendance as well as we also proposed the integrated scheme from capturing data from edge devices (CCTVs), streaming data to the dedicated server, then presenting the real-time data through android mobile devices. In this scheme, we proposed to employ deep learning algorithms based on the Convolutional Neural Network (CNN). Through the CCTV data streaming, faces are captured and matched with the database. Therefore, it is considered as their logging attendance. Furthermore, it is marked and stored into the database. This system prototype is developed by big data technology to tackle this complexity of data. The recognized faces can be monitored in real time monitoring. Eventually, real time reports are delivered through the web and android device with API after the data transmission is secured with hash encryption.

1. Introduction

Face recognition system is a modern technology that is able to recognize and identify people from their faces. Face recognition is a matching technology similar to fingerprint technology, retinal scan, and speech recognition. The technologies above have the same goal for distinguishing specific people. Face recognition technology has pros and cons until now. The main issue is that face recognition can endanger the public’s privacy. This technology may take some pictures from someone without permission. Despite the current debate, this technology has begun to grow rapidly and is widely used in many sectors.

One example of face recognition implementation might not violate privacy is smart attendance. Face recognition technology is able to replace the fingerprint that previously existed for attendance data. When employees attend the office, they don't need to report attendance manually. The system will automatically capture their faces in real-time. The captured face will be matched with the database to check the employee’s identity. Attendance systems could be implemented in many sectors such as companies, universities, laboratories and others.

There are several ways to look at attendance such as by giving a signature on the attendance file. This technique is the most conventional method. There are also some studies that developed smart attendance using fingerprints [1]. Many institutions now apply this biometric method but when it comes to a lot of people this becomes a big problem when people are waiting in line to tap their fingers.
Several studies also proposed smart cards with RFID for smart attendance. Sharma et al, proposed RFID for monitoring company employees [2]. The disadvantage of this method is the same as the fingerprint method. On other hand, when the magnetic card is malfunction the system will not be able to recognize the identity provided by the card. Other studies are using smartphones to track the employees' attendance. Suwito et al, proposed smart mobile as employees’ attendances using voice recognition [3].

Research developments are continuing to use other biometric technologies that do not require someone to actively use a fingerprint or a card. One of them is using the unique face. Studies to develop systems that are able to recognize faces grow rapidly. Face recognition is the same as other biometric methods such as fingerprint, retina and speech has the same goal to identify a unique person. Several researchers presented algorithms to recognize faces. [4] proposed a hybrid face recognition algorithm by combining two face recognition techniques by integrating (PCA) principal Component Analysis, (LDA) Linear Discriminant Analysis. [5] proposed the Open CV comparing the ROC (Receiver Operating Characteristics) curve and implementing it in the attendance system. [6] proposed simple fast Principal Component Analysis to recognize some faces.

This research proposed to develop face recognition prototype for smart attendance with several additions such as big data technology to process its data, android and web for its server monitoring and report. The location used for the prototype is in the lab environment. When lab employees come to the laboratory, the system will take pictures in real time and recognize them. Report results will be sent to the web and Android devices.

2. Methods

This face recognition algorithm is using FaceNet model that is a system that directly learns a mapping from face image databases to a compact Euclidean space where distances directly correspond to a measure of face similarity.

\[ d_{ij}(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2} \] .........................(1)

It means that every candidate has different distances and it will have a similar distance’s score if they are one identity. FaceNet model is using triplet loss function to minimize the distance between a positive and an anchor while maximizing the distance between the anchor and a negative identification and it will be shown in formula 2.

\[ \sum_{i=1}^{N} [||f(x_i^a) - f(x_i^p)||^2 - ||f(x_i^a) - f(x_i^n)||^2] \] .........................(2)

\[ x_i = \text{Variable represents an image} \]
\[ f(x_i) = \text{Embedding Image} \]
\[ a = \text{Margins between positive and negative pairs} \]

The triplet loss involves comparing face embedding for three images, one being an anchor (reference) image, second one the positive image (matching the anchor) and the third one negative image (not matching the anchor).

![Figure 1. Triplet loss selection illustration](image-url)
FaceNet maps a face into a 128D Euclidean space. The L2 distance (or Euclidean norm) between two facial embeddings corresponds to its similarity. This is exactly like measuring the distance between two points in a line to know if they are close to each other. In addition, the scheme is illustrated as below:

![Figure 2. Triplet Loss Image](image)

Finally, the distance is measured and it is the main metadata for comparing images stored in our dedicated database. Therefore, from the measured distance, the judgment of similarity between captured images and our database is constructed. Eventually, the captured face is stored into the logging database as an attendance system with several categories such as name, position, datetime and photo logger. FaceNet model as a classification and recognition of people from their faces is illustrated in Figure 3.

![Figure 3. Face recognition step](image)

Before feeding the data for the face recognition step (FaceNet Model) in the bounding box, we must align using the Multi Cascaded Convolutional Neural Network (MTCNN).

![Figure 4. Align image step with MTCNN](image)

In training process, the faces of employees are collected in large numbers. The face position is also visible from the front and sides. Examples of collected employees face images from several points of view can be seen in Figure 5.

![Figure 5. Employee faces images](image)
Finally, K-Nearest-Neighbours (KNN) is used to ensure the classification and recognize the person who enter the lab is included the databases or not. KNN classifier is best suited for classifying persons based on their images due to its lesser execution time and better accuracy than other commonly used methods which include Hidden Markov Model and Kernel method as an attendance system [7].

When the model is deployed in the server, there is a special program for retrieving real time video from CCTV with RTSP protocol. The video consists of multiple images and cropped to get the available faces. The faces then inserted into the face recognition model to define and identify faces. The system architecture is shown in Figure 6.

![Figure 6. System Architecture](image)

After face’s employees have already been identified with a unique name, a query will be made to the SQL database with name keyword. Face details are stored in database and become historical data. This data can later be used to dig deeper knowledge related to attendance. Relational data is shown in Figure 7.

![Figure 7. Database storage flow](image)

Face recognition can be useful as an automatic attendance system to improve the quality of worker’s performance but if the data is leaked, it can cause disaster and other problems. The encryption is needed so only verified officer can access it. One way to keep data safe is to use a cryptographic system that makes the information content become unknown. The illustration of the use of encryption and decryption is shown in Figure 8.

![Figure 8. Encryption model](image)
Data can also be used for reports presented in the dashboard. Real time data such as employee arrivals can be directly displayed automatically on the web and android devices. In addition, employee attendance data can also be aggregated based on historical data on a daily basis.

3. Result and Discussion

Prototype has been tested in a laboratory environment. CCTV was installed in the top corner to take pictures of employees in the lab. At certain hours, CCTV will take pictures and stream the data to the server to process them in real time. Several faces have been trained to make the system understand and able to recognize employees. Web-based dashboard built for monitoring face recognition activity with NodeJS environment. The dashboard displays objects captured by the camera and marked with a rectangle. Every second the system will crop the face of the captured image and also display on the board as shown in Figure 9.

![Figure 9. Real time monitoring dashboard](image)

Finally, the system creates a real-time report based on the employee’s attendance. The report is visualized and presented on an android device. This will make the employer easy to monitor the employees' attendance from an Android-based smartphone.

![Figure 10. Real time face recognition report](image)

![Figure 11. Whitelist and blacklist face loggers.](image)
Moreover, the proposed smart attendance is also aimed to detect intruders by showing unknown or blacklist people as described in Figure 11. Besides, this system makes this laboratory safer and also integrally lessens the burden of human resource workers to assess the performance of employees. System is also able to create better insight in reports by aggregating data from employees captured by CCTV such as counted employees, counted unrecognized people, late employees, early out employees and absent employees. The detailed report can be seen in Figure 12 above.

![Real time face insight analytics](image)

**Figure 12. Real time face insight analytics**

4. Conclusion

Smart attendance is a smart way to check employees' attendance. A deep learning algorithm combined with big data technology can be proposed to create smart attendance with face biometric methods. The prototype is able to recognize the faces in real time and identify the details of employees with Hash Encryption. Reports are presented in the form of a dashboard on the web and android devices and easily monitored by company officials.

Thus, in the near future, we are concerned about creating a lightface recognition model as we understand that the acceleration of current approach is needed. This paradigm is to create a more user-centric algorithm and to improve user experience.

References

[1] O. Shoewu, L. A. Akinyemi, and N. T. Makanjuola, “Smart Attendance Management System (SAMSYS) for an Academic Institution,” no. June 2019, 2018.
[2] “Radio Frequency Identification (RFID) Based Employee Monitoring System,” vol. 4, no. 5, pp. 3441–3444, 2014.
[3] B. Soewito, F. L. Gaol, and F. E. Gunawan, “Smart Mobile Attendance System Using Voice Recognition and Fingerprint on Smartphone,” no. August 2019, 2016.
[4] N. R. Borkar and S. Kuwelkar, “Real-Time Implementation Of Face Recognition System,” no. Iccmc, pp. 249–255, 2017.
[5] I. Technology and C. Technology, “Implementation of Face Recognition Algorithm for Biometrics Based Time Attendance System.”
[6] J. G. Roshantharanga, S. M. S. C. Samarakoon, T. A. P. Karunarathe, and K. L. P. M. Liyanage, “Smart Attendance Using Real Time Face Recognition (SMART - FR ),” vol. 2013, pp. 41–44, 2013.
[7] M. Kaur, “K-Nearest Neighbor Classification Approach for Face and Fingerprint at Feature Level Fusion,” vol. 60, no. 14, pp. 13–17, 2012.