Security System Uses CCTV Camera as Facial Image Recognition using Face-API

Olga Engelien Melo
Information Engineering
Polytechnic State of Manado
Indonesia

Harson Kapoh
Information Engineering
Polytechnic State of Manado
Indonesia

Ventje Ferdy Aror
Electrical Engineering
Polytechnic State of Manado
Indonesia

Ali Akbar Ramchie
Electrical Engineering
Polytechnic State of Manado

ABSTRACT
Security is a problem that cannot be separated from human life. Whether at home, on the go or at work. Currently, many implementations have been tried for security, especially in accessing a place or room. Several ways to ensure security, especially for people who are not supposed to be in certain places, are to limit the access rights of a person or group of people by giving keys, cards or pins to certain people using various technologies. CCTV cameras or Close Circuit Television can be used to monitor security. However, CCTV for monitoring security is still considered ineffective if there is an intrusion in a room, house, office or certain place because there must be an operator watching. This study aims to produce a system that will be used to recognize someone from their face so that it can be known and verified whether the person is registered and has access rights or is in a certain room and location without having to always be supervised by an operator. The method used is the javaScript module, namely face-api.js in the form of an open source machine learning framework with varying facial recognition test results, especially at distances above 300 cm. The decrease occurs varies, at a distance of 350 cm one face has 60% accuracy, at a distance of 400 cm the accuracy is only 50%. On 2 faces at the same time the accuracy level on the first face is 350 cm the accuracy level is 70% and the second face is 60%, at a distance of 400 cm the accuracy level on the first face is 50% and the second face is 90%.

General Terms
Face recognition

Keywords
Cctv, face detection, face recognition, face-api

1. INTRODUCTION
Security is an issue that cannot be separated from human life. Whether at home, on the go or at work. Currently there are many implementations that have been tried for security, especially in accessing a place or room. Some ways to ensure security, especially for people who are not supposed to be in certain places, are to limit the access rights of a person or group of people by giving keys, cards or pins to certain people using various technologies such as RFID [1]. This is necessary as an effort to increase the level of security or prevent crime. [2] The problem is that access right holders can forget pins, passwords or forget to bring access cards.

Biometrics is a solution to be able to access by identifying and verifying a person or group of people has access rights to a certain place [3][4].

CCTV cameras or Close Circuit Television can be used to monitor security [5]. But CCTV to monitor security is still considered ineffective if there is an intrusion in a room, house, office or a certain place because there must be an operator watching [6].

Currently there are many face recognition methods that can be applied so that a system can recognize a person's face and can determine whether that person has the right to access a room, has the right to be in a certain room or location such as methods such as Support Vector Machines (SVM). [11], Linear Discriminant Analysis (LDA) [10], Independent Component Analysis (ICA) [9], Principal Component Analysis (PCA) or Eigenface [8], and Hidden Markov Models (HMM) [12] and many studies also use facial recognition Local Binary Pattern Histogram (LBPH) method [5][13].

This research aims to produce a system that will be used to recognize someone from their face using machine learning so that it can be known and verified whether the person is registered and has access rights or is in a certain room and location without having to always be supervised by an operator.

2. RESEARCH METHODE
2.1 Research Planning
Stages or research procedures carried out using several methods such as Waterfall

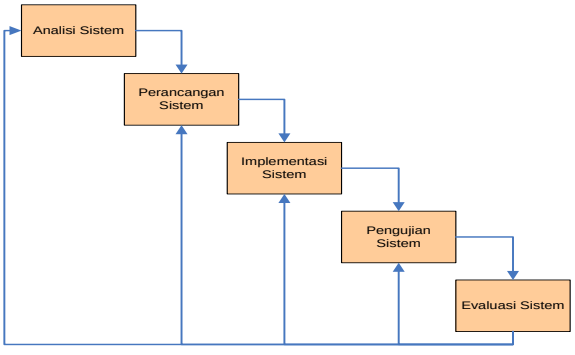

Figure 1. Waterfall

At the analysis stage the system requires data so that it is necessary to collect qualitative data, namely primary data. The stages of research include carrying out activities or activities to study which data sources are from books and other sources of information related to research activities and needs. The technique of taking and collecting data carried out is:

2.1.1 Observation

Observation is an activity carried out by observing the object under study. This activity is carried out either directly or indirectly in order to obtain data from research.

2.1.2 Interview

Interviews were conducted to obtain data and information related to the problem under study. In this study interviews were conducted with parties in the electrical engineering department to obtain data and information.

2.1.3 Literature Study

Theoretical references are needed for the literature related to the research being conducted.

3. CONCEPTUAL FRAMEWORK

Conceptual Framework is a form of thought framework that can be used as an approach in solving problems. Usually this research Framework uses a scientific approach and demonstrates relationships between variables in the analysis process.

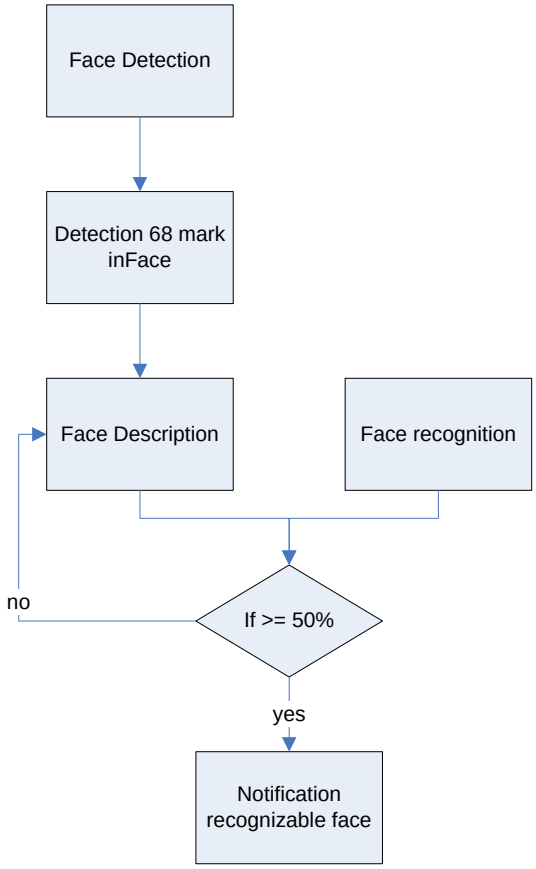

Figure 1. Face recognition conceptual

On fig. 1 is a conceptual face recognition system with the starting stage of the system recognizing faces by detecting 68 signs on the face from the results of the face detection. The system will describe the results of detecting 68 marks on the face and matching them with faces that have been registered using the face recognition method and if there is a match of greater than 50% then the face is considered registered.

3.1 System Architecture

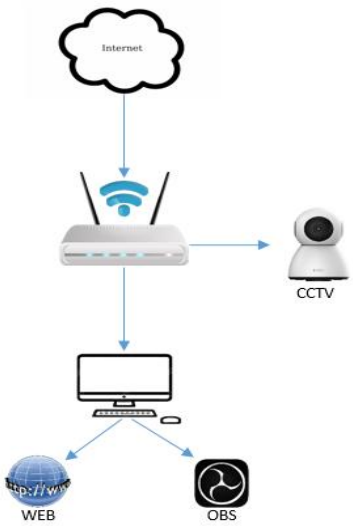

Figure 2. Architecture

Fig. 2 is the architecture of the system that describes the system requirements, namely CCTV, Access Point, Internet, PC/Laptop,OBS dan WEB.

Figure 3. Block diagram

Fig. 3 is a block diagram that illustrates that the system input is CCTV connected to the Access Point so that the CCTV IP can be known. The process occurs on a PC which is also connected to an Access Point which is in the same network segment as CCTV so that it can be connected to OBS which is also connected to WEB. The output from the system is in the form of notifications on the WEB.

4. IMPLEMENTATION TECHNOLOGIES

The facial image recognition security system using CCTV cameras uses several technologies that are integrated to produce a system that can recognize the face of a person or several people.

In general, the facial recognition method uses face-api.js which is a machine learning framework built on top of TensorFlow to help build a web application that can support face recognition[15].

4.1 Face Detection

Face detectors aim to obtain high accuracy in detecting faces in a face bounding box with low inference time.

Face detection, in this study implemented several face detection methods namely;

SSD (Single Shot Multibox Detector) based on MobileNetV1. The neural net will be connected to a face or every detected face then calculates the location of each face in an image and will return the bounding box along with the probabilities for each of these faces.

Tiny Face Detector which is a detector that performs very well with processing data in real time, the process is much

faster, smaller, and more resource efficient compared to the Mobilenet V1 SSD face detector, the drawback is that its performance is slightly less good at detecting faces small. This model has the advantage of being highly mobile and web-friendly, so it can become a GO-TO face detector on mobile devices and clients using only limited resources. The quantized model size is only 190 KB (tiny_face_detector_model).

MTCNN (Multi-task Cascaded Convolutional Neural Networks) is one such detection using neural networks representing face detectors as an alternative to SSD Mobilenet v1 and Tiny Yolo v2, which have more space for configuration. Like setting on the input parameters. MTCNN is very good at implementing detection of various sizes of face bounding boxes. MTCNN is a CNN having 3 cascading stages, the way it works is it simultaneously returns 5 face landmark points which is also done along with the bounding box and displays the score for each face. The size of the model is only 2MB.

4.2 68 Point Face Landmark Detection Models

This model implements a facial landmark detector by identifying 68 points on the face very lightly and quickly, but accurately. This model defaults to only 350 kb in size.

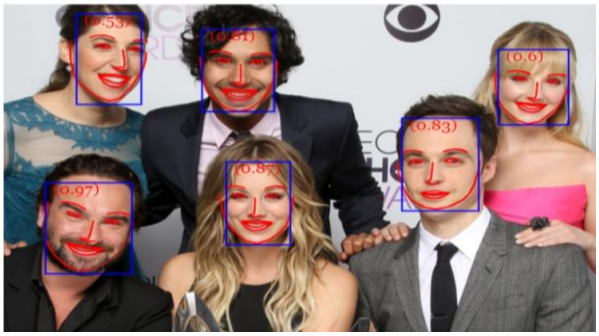

Figure 4 Landmark detection model

4.3 Face Recognation

Facial image recognition systems are generally divided into two types, namely feature-based systems and imaged-based systems. In the feature-based system, features (eyes, nose, mouth, etc.) are used which are components of the extracted facial image which then models the relationship between these features geometrically. Meanwhile, imaged based systems use image pixels as raw information which is then represented in certain methods.

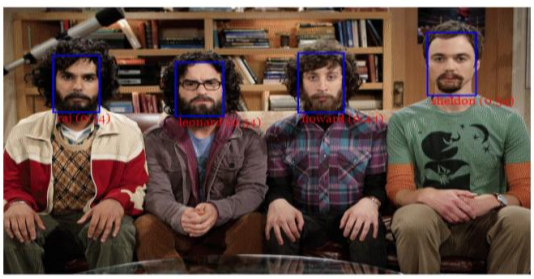

Figure 5. Face Recognation

Face recognition implemented with an architecture like ResNet-34 is used to recognize face images by calculating a face descriptor (a feature vector with a value of 128) from any given face image. It is used to describe the facial characteristics of a person. The facial models used are not limited to the set of faces used for training. Anyone can use it for anyone's facial recognition, for example ourselves. You can compare descriptors and determine the similarity of two arbitrary faces to their faces, for example by calculating the euclidean distance or using another classifier of your choice.

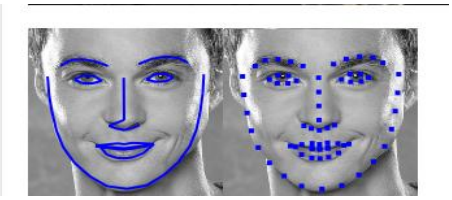

Figure 4. Face landmark detectioan

4.4. Biometrica System

Human behavior or parts of the human body can be used as self-identification in a system called a biometrics system. A self-recognition system is a system that automatically uses a computer to recognize a person's identity. The database is reference data that has been registered and prepared beforehand so that it can help the system to find and match a person's identity. The purpose of a self-recognition system is to increase system security so that recognizing targets can be done precisely and this is very important in a biometrical system [13].

4.4 Open Broadcaster Software

Open broadcaster software or OBS is an application that can be used on various platforms to improve video quality when live. The goal of optimizing real-time video and also streaming quality can be done with the help of OBS. Currently, OBS is much needed, such as being used for Instagram, YouTube and live on Twitch. OBS is an application that is classified as open source, which means you can use it for free on various devices.

5. RESULT OF RESEARCH

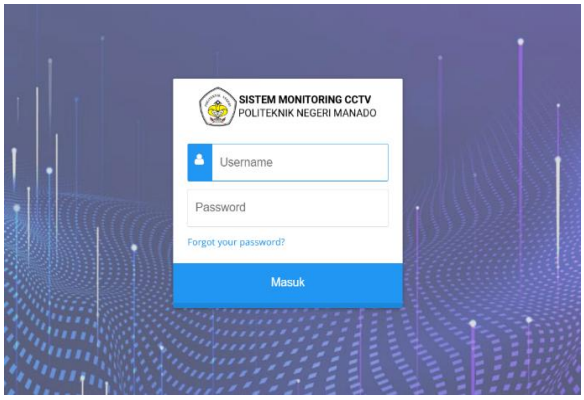

Figure 5. Form login

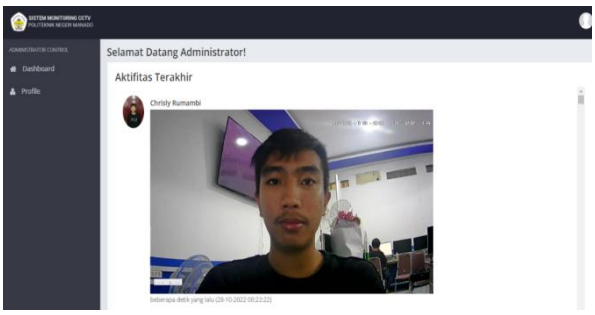

Figure 6. Face detection

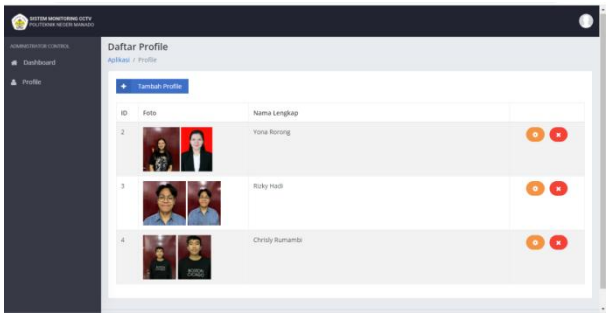

Figure 7. Face dataset database

Fig 7. is a facial dataset database that is used to compare with the results of facial descriptions from face detection using CCTV.

5.1 Testing

Testing was carried out to find out whether the system built was as expected, namely being able to recognize detected and registered faces or not.

Conduct testing by first entering facial data into the system database which will later become a reference for comparison with facial data input from detection using CCTV. The photo formats used are .jpg, .png and .jpeg

5.2 Result of Testing

Tests were carried out with several variables such as faces and face distance from CCTV

Table 1. Testing one person's face based on distance

Face distance from CCTV	Result 1	Result 2	Result 3	Result 4	Result 5
50 cm	√	√	√	√	√
100 cm	√	√	√	√	√
150 cm	√	√	√	√	√
200 cm	√	√	√	√	√
250 cm	√	√	√	√	√
300 cm	√	√	√	√	√
350 cm	√	√		√	
400 cm		√	√		

Face distance from CCTV	Result 6	Result 7	Result 8	Result 9	Result 10
50 cm	√	√	√	√	√
100 cm	√	√	√	√	√
150 cm	√	√	√	√	√
200 cm	√	√	√	√	√
250 cm	√	√	√	√	√
300 cm	√	√	√	√	√
350 cm	√		√	√	
400 cm	√	√	√		

In table 1 the test uses 1 face with 10 tests with the result that when the test is carried out with a distance above 300 cm, namely 350 cm and 400 cm the system begins to be unable to detect faces which are marked by no continuous border appearing.

Table 2. Testing the faces of 2 face based on distance

Face distance from CCTV	Result 1		Result 2		Result 3		Result 4	
	First face	Second face	First face	Second face	First face	Second face	First face	Second face
50 cm	√	√	√	√	√	√	√	√
100 cm	√	√	√	√	√	√	√	√
150 cm	√	√	√	√	√	√	√	√
200 cm	√	√	√	√	√	√	√	√
250 cm	√	√	√	√	√	√	√	√
300 cm	√	√	√	√	√	√	√	√
350 cm	√	√	√		√			
400 cm	√	√		√	√	√		

Face distance from CCTV	Result 5		Result 6		Result 7	
	First face	Second face	First face	Second face	First face	Second face
50 cm	√	√	√	√	√	√
100 cm	√	√	√	√	√	√
150 cm	√	√	√	√	√	√
200 cm	√	√	√	√	√	√
250 cm	√	√	√	√	√	√
300 cm	√	√	√	√	√	√
350 cm	√	√			√	√
400 cm	√	√		√	√	√

Face distance from CCTV	Result 8		Result 9		Result 10	
	First face	Second face	First face	Second face	First face	Second face
50 cm	√	√	√	√	√	√
100 cm	√	√	√	√	√	√
150 cm	√	√	√	√	√	√
200 cm	√	√	√	√	√	√
250 cm	√	√	√	√	√	√
300 cm	√	√	√	√	√	√
350 cm	√	√	√		√	√
400 cm	√	√		√		√

In table 2, the experiment using 2 faces can be seen that when the test was carried out with a distance above 300 cm, namely 350 cm and 400 cm, the system also began to be unable to detect faces which were marked by no continuous border appearance.

Testing the accuracy of the system

$$\text{Accuracy} = \frac{\text{True result}}{\text{The number of trials}} \text{ x } 100\%$$

Table 3. Accuracy of one face

Face distance from CCTV	Accuracy
50 cm	100%
100 cm	100%
150 cm	100%
200 cm	100%
250 cm	100%
300 cm	100%
350 cm	60%
400 cm	50%

The level of accuracy shows that at a distance of 350 cm the level of accuracy becomes 60% and 400 cm the level of accuracy becomes 50%.

Table 4. Accuracy of 2 face

Face distance from CCTV	Accuracy	
	First face	Second face
50 cm	100%	100%
100 cm	100%	100%
150 cm	100%	100%
200 cm	100%	100%
250 cm	100%	100%
300 cm	100%	100%
350 cm	70%	60%
400 cm	50%	90%

In the experiment using 2 faces also showed an accuracy rate at a distance of 350 cm on the first face 70% and the second face 60%. At a distance of 400cm the first face is 50% and the second face is 90%.

6. CONCLUSION

Research that has been done using distance and face variables. 10 times taking faces at each distance of 50 cm, 100 cm, 150 cm, 200 cm, 250 cm, 300 cm, 350 cm and 400 cm shows that face recognition can be done from the system that was developed with results at a distance of under 300 cm for one face or 2 faces show 100% accuracy. Whereas at a distance above 300 cm there is a decrease in the level of accuracy of the facial recognition system. The decrease occurs varies, at a distance of 350 cm one face has 60% accuracy, at a distance of 400 cm the accuracy is only 50%. On 2 faces at the same time the accuracy level on the first face is 350 cm the accuracy level is 70% and the second face is 60%, at a distance of 400 cm the accuracy level on the first face is 50% and the second face is 90%. Experimental variables need to be added, such as moving faces, time and lighting.

7. ACKNOWLEDGMENT

Thanks to Manado State Polytechnic who has given the opportunity to do this research.

8. REFERENCES

[1] Pratomo. H. A, Florestyanto. M, Sari. N. I, 2019, Pengenalan Wajah untuk Pemantauan Kehadiran Pegawai Menggunakan Metode Viola Jones dan Euclidean Distance Prosiding Seminar Nasional Komunikasi dan Informatika #3:69-78

[2] Rufendhi, B. C. 2014. Penerapan Euclidean Distance Pada Eigenface Untuk Monitoring Ruangan Secara Realtime Berbasis Webcam Dengan Pencocokan Wajah (Phd Thesis). Universitas Islam Negeri Maulana Malik Ibrahim.

[3] A. Yudhana, S. Sunardi, and P. Priyatno, 2018, "Perancangan Pengaman Pintu Rumah Berbasis Sidik Jari Menggunakan Metode UML," J. Teknol., vol. 10, no. 2, pp. 131–138, [Online]. Available: https://dx.doi.org/10.24853/jurtek.10.2.131-138.

[4] A. Yudhana, S. Sunardi, and P. Priyatno, "Development of Door Safety Fingerprint Verification Using Neural Network," J. Phys. Conf. Ser., vol. 1373, no. 1, 2019, doi: 10.1088/1742-6596/1373/1/012053..

[5] Bayu, S., Hendriawan, A., and Susetyoko, R."Penerapan Face Recognition Dengan Metode Eigenface Dalam Intelligent Home Security" Eepis Final Project. 2009. Retrieved From Http://Repo.Pens.Ac.Id/Id/Eprint/624

[6] Histogram Sunardi , Anton Yudhana , Muhamad Alwi Talib, 2022, Perancangan Sistem Pengenalan Wajah untuk Keamanan Ruangan Menggunakan Metode Local Binary Pattern , *Vol 13, No 2* .

[7] M. Turk and A. Pentland, 2002 "Eigenfaces for Recognition," J. Cogn. Neurosci., vol. 3, no. 1, pp. 71–86, Jan. 1991, doi: 10.1162/jocn.1991.3.1.71.

[8] M. S. Bartlett, J. R. Movellan, and T. J. Sejnowski, "Face Recognition by Independent Component Analysis," IEEE Trans. Neural Networks, vol. 13, no. 6, pp. 1450–1464, doi: 10.1109/TNN.2002.804287.

[9] J. Lu, K. N. Plataniotis, and A. N. Venetsanopoulos, 2003 "Face recognition using LDA-based algorithms," IEEE Trans. Neural Networks, vol. 14, no. 1, pp. 195–200, doi: 10.1109/TNN.2002.806647.

[10] B. Heisele, P. Ho, and T. Poggio, 2001, "Face recognition With Support Vector Machines: Global Versus Component-based Approach," Proc. IEEE Int. Conf. Comput. Vis., vol. 2, no. July, pp. 688–694, doi: 10.1109/ICCV.2001.937693.

[11] A. V. Nefian and M. H. Hayes, "Hidden Markov Models for Face Recognition," in Proceedings of the 1998 IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP '98 (Cat. No.98CH36181), 1998, vol. 5, no. 4, pp. 2721–2724, doi: 10.1109/ICASSP.1998.678085.

[12] T. K. Vamsi, K. C. Sai, and M. Vijayalakshmi, "Face Recognition Based Door Unlocking System Using Raspberry Pi," nternational J. Adv. Res.

[13] Darma Putra. C, Widya Hermawan. 2016, Sistematika Biometrika : Konsep Dasar, Tekhnik Analisis Citra Dan Tahapan 175 | JURNAL TEKNIK INFORMATIKA VOL 9 NO. 2

[14] Aris Budi: Pengenalan Citra Wajah…. 166-175 ISSN 1979-9160 Membangun Aplikasi Sistem Biometrika, Yogyakarta: Penerbit Andi, 2009.