INTENSIF, Vol.5 No.1 February 2021
ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v5i1.14435

The Office Room Security System Using Face Recognition Based on Viola-Jones Algorithm and RBFN

Sistem Keamanan Ruang Kantor Menggunakan Fitur Pengenalan Wajah Berbasis Algoritma Viola-Jones dan RBFN

Received:
31 May 2020
Accepted:
27 December 2020
Published:
1 February 2021

[1*]Andree E. Widjaja, [2]Hery, [3]David H. Hareva
[1,2,3]Universitas Pelita Harapan
[1,2,3]Tangerang, Indonesia
E-mail: [1]andree.widjaja@uph.edu, [2]hery.fik@uph.edu, [3]david.hareva@uph.edu
*Corresponding Author

Abstract—The university as an educational institution can apply technology in the campus environment. Currently, the security system for office space that is integrated with digital data has been somewhat limited. The main problem is that office space security items are not guaranteed as there might be outsiders who can enter the office. Therefore, this study aims to develop a system using biometric (face) recognition based on Viola-Jones and Radial Basis Function Network (RBFN) algorithm to ensure office room security. Based on the results, the system developed shows that object detection can work well with an object detection rate of 80%. This system has a pretty good accuracy because the object matching success is 73% of the object detected. The final result obtained from this study is a prototype development for office security using face recognition features that are useful to improve safety and comfort for occupants of office space (due to the availability of access rights) so that not everyone can enter the office.

Keyword—Office Security, Face Recognition, Prototyping, Database

Abstrak—*Universitas sebagai salah satu institusi pendidikan dapat menerapkan teknologi untuk meningkatkan keamanan kantor dosen dan staf. Pada saat ini, sistem keamanan kantor dosen dan staf yang terintegrasi dengan data dosen ataupun staf akademik secara digital masih terbatas, sehingga ditemukan kendala utama yaitu berupa keamanan barang-barang penting dan bersifat rahasia tidak terjamin karena dengan bebasnya pihak luar masuk ke dalam ruang kantor. Oleh karena itu, penelitian ini bertujuan untuk mengembangkan sistem keamanan ruang kantor menggunakan fitur pengenalan wajah berbasiskan algoritma Viola-Jones dan Radial Basis Function Network (RBFN). Berdasarkan hasil pengujian, sistem yang dibuat menunjukkan pendeteksian objek dapat berjalan dengan cukup baik dengan tingkat pendeteksian objek individu 80%, dan sistem ini memiliki akurasi yang cukup baik karena keberhasilan mencocokan objek individu yang terdeteksi mencapai 73% dengan data objek individu yang tersimpan dalam database. Hasil akhir yang diperoleh dari penelitian adalah prototype sistem keamanan ruang kantor menggunakan fitur pengenalan wajah yang bermanfaat untuk meningkatkan keamanan dan kenyaman bagi penghuni ruang kantor, karena adanya hak akses ke dalam ruang kantor, sehingga tidak semua orang dapat memasuki ruang kantor tersebut.*

Kata Kunci—*Sistem Keamanan Ruangan, Pengenalan Wajah, Prototyping, Database*

I. INTRODUCTION

In today's modern era, the security aspect is essential because a high-security level can increase individuals' peace and comfort [1]. People can do various ways to improve security, ranging from the direct or physical human involvement in the form of guarding by security officers to using technology support, for example, information security systems [2-3], home security systems [4], digital rights management [5], and data distribution security systems [6]. Also, the use of technology in the security system applied can be the use of biometrics such as fingerprints, CCTV installation, and various other things [7].

As an educational institution, the university can significantly apply technology in the campus environment to increase the office space's security (workspace) of lecturers and staff. Based on observations in the campus environment, few office security systems are currently integrated with digital data from lecturers or academic staff. Therefore the main obstacle is possible, namely the security of essential and confidential items that are not guaranteed security because outsiders enter office room freely.

At this time, the application of room security systems can be carried out with technological support in the form of the Internet of Things (IoT) using Arduino hardware, integrated with a database to maximize room security systems [8]. The use of Arduino is increasing with the need for a microcontroller device that is affordable and supported by the development of work automation using a device that can be controlled via a mobile application [9]. Several previous studies regarding security systems have been carried out by M. K. Syabibi and A. Subari, [10], namely by using a webcam to create a web-based monitoring system for home security. Previous research aims to monitor activities that occur at home via the web. In contrast, this research seeks to create a security system for office doors, especially to control access of people in and out of the room.

Another research was carried out by M. Arihutomo [11] to make a guard robot for guarding. The difference with this research is that previous research made robots a security system, whereas this study produced a security system in-room access rights. Other facial recognition research was also carried out by Yuliana Y. and Nurhaida I. [12]. The analysis uses a webcam to detect and perform facial recognition and tests to improve a person's face's detection and recognition accuracy. The research that is currently being conducted aims to implement an office security system using facial recognition features. Furthermore, several previous studies related to this research topic are summarized in table 1 below.

Table 1. SOME OF THE PREVIOUS RESEARCH RELATED

No.	Author	Research Conducted
1	D. E. Kurniawan, K. Adi, and A. F. Rohim [13]	developed a facial biometrics system to recognize faces with an accuracy rate of up to 97.5%. This study used the Gabor KPCA method and Mahalanobis Distance.
2	N. Saubari, R. Isnanto, and K. Adi [14]	developed a face detection system using the Haar-Like Feature method and Artificial Neural Network Backpropagation. The facial recognition accuracy of the developed system reaches 80.8%.
3	I, K. S. Widiakumara, I K. G. D. Putra, and K. S. Wibawa [15]	developed an Android application to identify faces. The method used is the Eigenface method, which is stored in the MySQL database system. The accuracy (success) of this facial recognition Android application is 68%.
4	N. V. de Lima, L. Novamizanti, and E. Susatio [16]	developed a 3-dimensional facial recognition identification system based on template matching, the Iterative Closest Point (ICP) method, and the Support Vector Machine (SVM) classification. The developed system accuracy is 97.30%.
5	R. Wiryadinata, U. Istiyah, R. Fahrizal, Priswanto, dan S. Wardoyo [17]	developed facial recognition software for presence using the Eigenface algorithm, Provincial Component Analysis, and facial expressions. The developed system accuracy reaches 86.67%

The research being conducted aims to develop an office security system using facial recognition features. Researchers will build this system with the use of a camera device, namely an IP camera. It functions to take the faces of individual objects. Then process them for facial recognition based on the Viola-Jones algorithm and the Radial Basis Function Network (RBFN), and the application of the Arduino NodeMCU ESP8266 hardware, which is used to control the door lock to open and close office doors. In this study, the Arduino used was the ESP8266 MCU node. The ESP8266 MCU node is a microcontroller that is integrated with the ESP8266 WIFI module [18].

II. RESEARCH METHOD

A. Research Stages

This study uses the prototyping method in developing office space security systems. The stages in this research are shown in Figure 1 below.

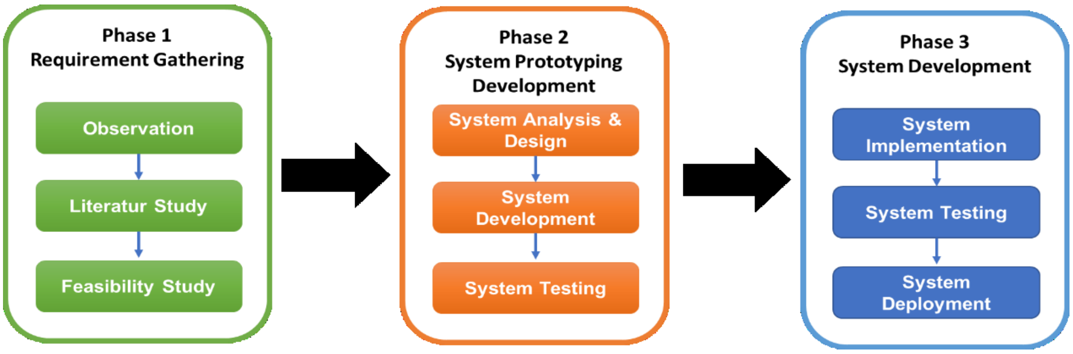

Figure 1. STAGES OF THE RESEARCH

This research consisted of 3 phases, namely, requirement gathering, the second phase building a prototyping system, and system deployment for the final step. In this prototyping system, the user will try the system to get feedback and become an evaluation to produce prototype improvements. This process is repeated until analysts, users, and related parties agree on the resulting prototype [19].

B. Viola-Jones Algorithm

Face detection is an early stage in facial recognition systems. One of the algorithms that can be used to detect objects is the Viola-Jones algorithm. The Viola-Jones algorithm works by using a simple Haar-like feature that quickly evaluates a new image representation [20]. Viola-Jones processes feature sets with integral imagery and boost algorithms to reduce time complexity and perform a classifier's cascade classifier. The detection is carried out using the Viola-Jones algorithm, as shown in Figure 2.

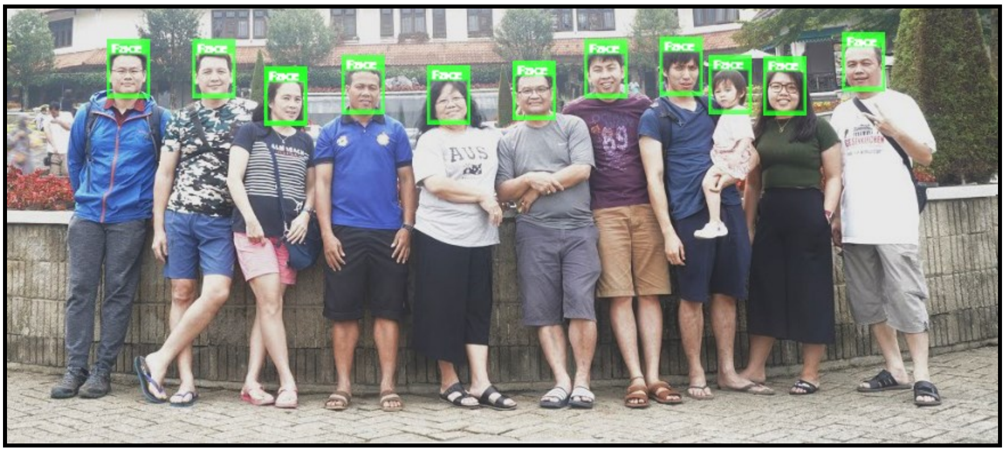

Figure 2. INDIVIDUAL OBJECT DETECTION WITH VIOLA-JONES ALGORITHM

Object detection is carried out, namely, detecting the existence of objects that are human individuals. The results of the detection of individual detected items will then be focused and processed on the face. The effects of the processing carried out by the Viola-Jones algorithm produce a box shape in the form of a face area on the front. Furthermore, the system will carry out matching individual object faces with the data they have.

C. Radial Basis Function Network

Radial Basis Function Network (RBFN) is a neural network-based algorithm used for decision making. The RBFN model consists of 3 layers, namely the input layer (input layer), hidden layer (hidden layer), and output layer (output layer) [11]. The input layer receives an input vector A, which is then taken to the hidden layer, which will process the input data non-linearly with the activation function. The output from the hidden layer is then processed linearly

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v5i1.14435

at the output layer [21]. Radial Basis Function Network architectural modeling is seen in (Figure 3).

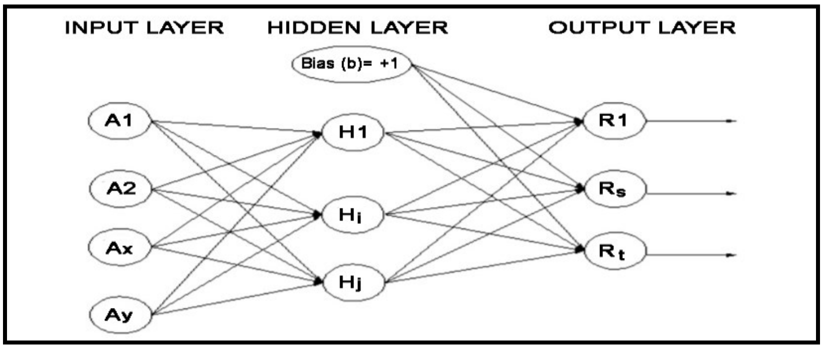

Figure 3. MODELING RADIAL ARCHITECTURE BASED ON FUNCTION NETWORK

Network training is divided into two stages: first, the weights from the input to the hidden layer are determined, and then the consequences from the invisible to the output layer are calculated. The training or learning process of RBFN is known to be very fast. A typical configuration of RBFN for input point Ay with hidden layer Hj and output point Rt [22]. The RBFN model uses the base function as an activation function for each neuron in the hidden layer. In this study, the radial basis function used is the Gaussian function. You can see the equation for the Gaussian function in equation (1) below:

$$\emptyset(|| A - A_c ||), \emptyset(z) = exp\left[-\frac{(z)^2}{2\sigma^2}\right] \qquad (1)$$

Information:

$(z)^2 = distance\ of\ each\ point\ to\ the\ center$

$\sigma^2 = variant\ of\ center$

D. Block Diagram of Built Office Security System

The block diagram of the office security system built is presented in Figure 4.In the diagram shown, two processes are the training process and the facial recognition process.

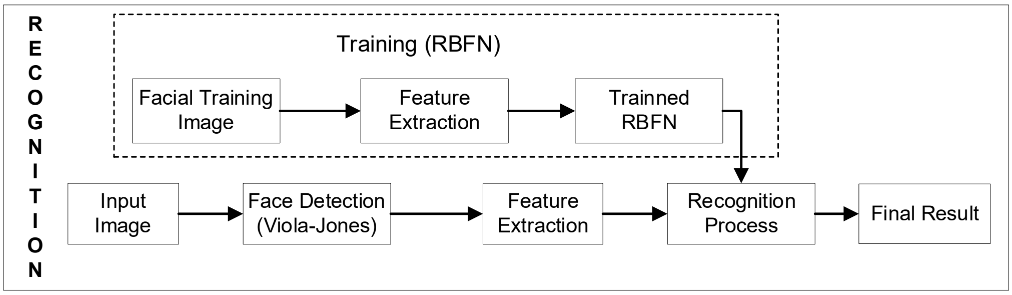

Figure 4. DIAGRAM BLOCK OF THE BUILD OFFICE SECURITY SYSTEM

III. RESULT AND DISCUSSION

A. Research Prototyping Results

After conducting this research, the results obtained are in the form of a prototype of an office security system using facial recognition features. The structure built is a pilot project of the smart campus master plan that will be developed. The resulting prototype uses an Arduino NodeMCU ESP8266 microcontroller, wireless router, electronic door lock access, CPU server, and IP camera. How the office security system works using the facial recognition feature can be seen in Figure 5.

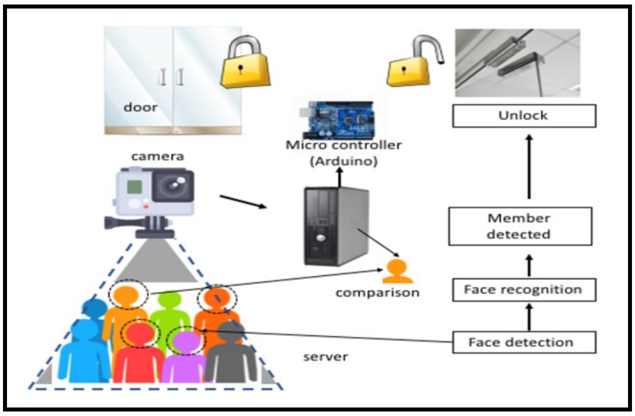

Figure 5. HOW TO WORK AN ARDUINO-BASED OFFICE SECURITY SYSTEM USING FACE RECOGNITION FEATURES

The workings of the resulting prototype, namely:

1. When someone approaches the office door with a distance of about 1-2 meters, the IP camera will detect individual objects in front of them.
2. Then the captured individual objects will be sent via the wireless network to the CPU Server for matching individual faces captured by the IP camera with personal object data that has been stored in the database with the Radial Basis Function Network.
3. Suppose the matching process finds matching results on individual object data in the database. In that case, the CPU Server sends an order to the Arduino NodeMCU ESP8266 microcontroller to access the door lock to open the lock so that the person at the office room door can enter the room. After the person enters, the Arduino NodeMCU ESP8266 microcontroller will access the door lock by closing the activity so that the office door is locked again so that the office space's security is well maintained.
4. Conversely, suppose the matching process does not find matching results on individual data objects in the database. In that case, the CPU Server does not give orders to the Arduino microcontroller so that the person who is in front of the office door cannot open the office door to enter because the door lock is locked.

Next, we will discuss the documentation for implementing a prototype office security system using the facial recognition feature. The office space security system created is then implemented for testing the system being built. Figure 6 shows the office space security system prototype in the form of an Arduino NodeMCU ESP8266 device and an IP Camera that has been completed and is connected to a wifi network and a CPU Server.

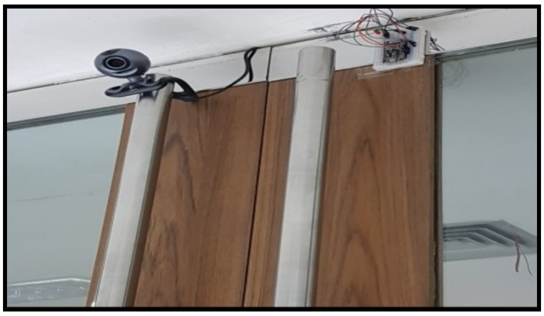

Figure 6. ARDUINO-BASED OFFICE SECURITY SYSTEM PROTOTYPE USING FACE RECOGNITION FEATURES

In Figure 7, the documentation for the office room door of the lecturer and staff of the Faculty of Computer Science is closed. The office door has been installed with an office security system so that no one can enter the room. It is done to maintain room security because there are essential and confidential items such as important documents such as exam questions, lecturers' research items, and a PC server that stores all the records of the Faculty of Computer Science.

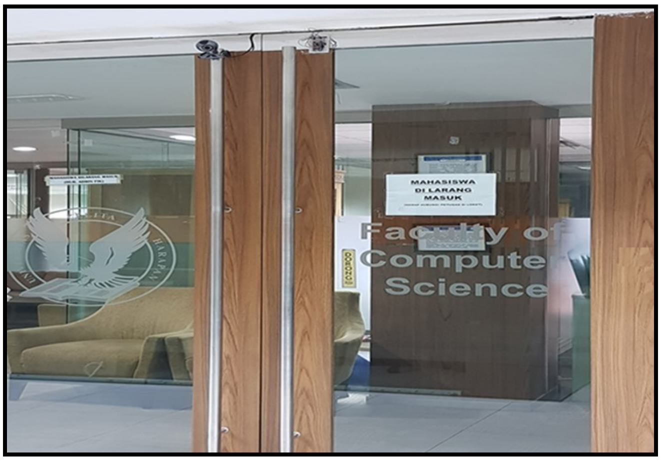

Figure 7. DOCUMENTATION OF INSTALLATION OF ARDUINO-BASED OFFICE SECURITY SYSTEMS USING FACE RECOGNITION FEATURES IN F BUILDING

In (Figure 8), when someone approaches the office door, the IP camera will detect individual objects in front of them. Furthermore, in Figure 9, the room security system will carry out the facial recognition process before the individual opens the door.

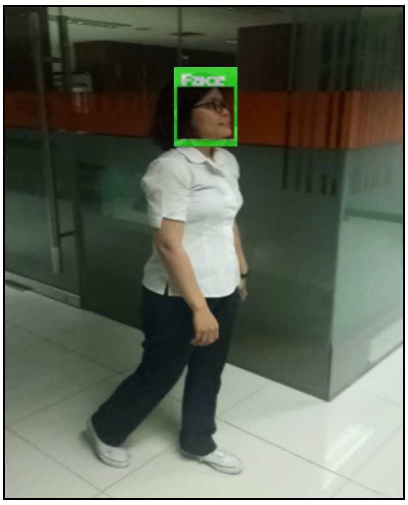

Figure 8. TESTING PHOTO STEP 1

Figure 9. TESTING PHOTO STEP 2

Figure 10 is the process of recognizing the face of individual objects by comparing the faces of particular objects with training data in the database carried out by the room security system.

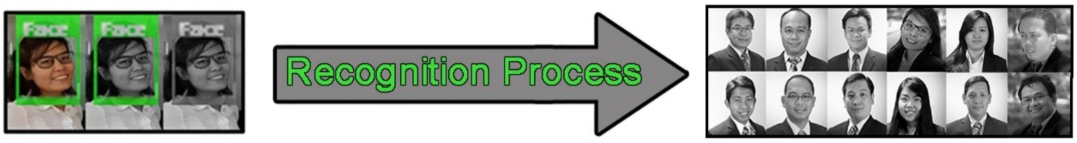

Figure 10. PROCESS OF RECOGNITION OF INDIVIDUAL OBJECT FACES WITH TRAINING DATA THAT IS IN DATABASE STORED ON THE CPU SERVER

In Figure 11, after successfully matching individual objects' faces, the CPU Server via the wireless network sends commands to the Arduino NodeMCU ESP8266 microcontroller to access the door lock to perform the unlock command. In Figure 12, the person in front of the door can push the door to open the door because the door lock is already open.

Figure 11. TESTING PHOTO STEP 3

Figure 12. TESTING PHOTO STEP 4

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v5i1.14435

In Figure 13, the person in front of the door opens the door, enters the faculty and staff office room, and then closes the door. In Figure 14, the closed door will be automatically locked so that the office space's security is well maintained.

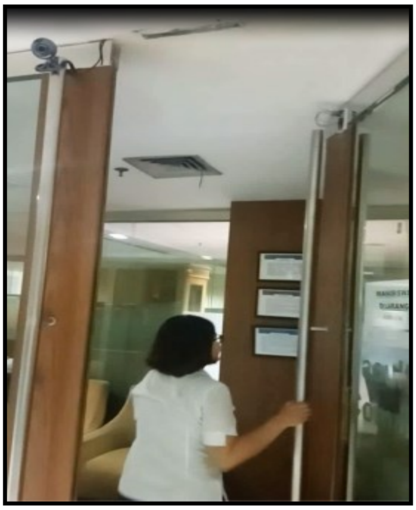

Figure 13. TESTING PHOTO STEP 5

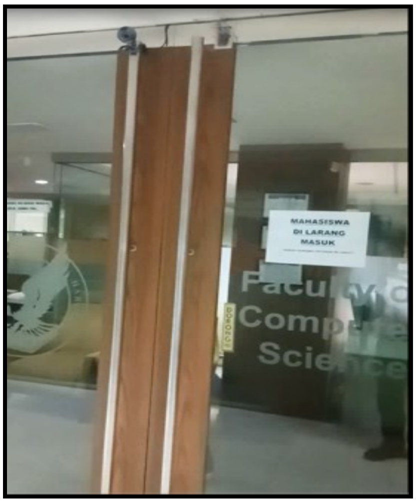

Figure14. TESTING PHOTO STEP 6

B. Testing Result

In this office space security system research, there are two main processes: detecting objects by the camera at a distance of 1-2 meters and matching individual items captured by the camera with personal object data stored in the database. Tests are carried out on the Arduino-based office security system using the facial recognition feature to ensure that it runs well and is stable. The office space security system test was conducted 30 times to determine its ability to detect objects. The results of testing the office security system to detect individual objects are seen in Table 2:

Table 2. RESULTS OF OFFICE SPACE SECURITY SYSTEM TESTING FOR OBJECT DETECTING

Testing	Object Detection Duration	Detection Status Results	Testing	Object Detection Duration	Object Detection Results
1	7 seconds	Successfully Detect	16	1.3 seconds	Successfully Detect
2	8 seconds	Successfully Detect	17	> 15 seconds	Failed
3	11 seconds	Successfully Detect	18	4 seconds	Successfully Detect
4	8 seconds	Successfully Detect	19	> 15 seconds	Failed
5	9 seconds	Successfully Detect	20	7 seconds	Successfully Detect
6	7 seconds	Successfully Detect	21	12 seconds	Successfully Detect
7	> 15 seconds	Failed	22	9 seconds	Successfully Detect
8	5 seconds	Successfully Detect	23	10 seconds	Successfully Detect
9	7 seconds	Successfully Detect	24	11 seconds	Successfully Detect
10	8 seconds	Successfully Detect	25	9 seconds	Successfully Detect
11	13 seconds	Successfully Detect	26	6 seconds	Successfully Detect
12	> 15 seconds	Failed	27	6 seconds	Successfully Detect
13	> 15 seconds	Failed	28	8 seconds	Successfully Detect
14	8 seconds	Successfully Detect	29	> 15 seconds	Failed
15	5 seconds	Successfully Detect	30	12 seconds	Successfully Detect

After 30 experiments, researchers found that the system succeeded in detecting individual objects 24 times, and six times it failed to detect particular objects. It shows that the system has relatively good stability because it manages to catch 80% of individual things in front of the camera.

After the first stage of testing is carried out, the second stage of testing is carried out. Namely, the office space security system matches the individual objects detected with the personal object data stored in the database. This office space security system test was carried out 30 times to determine the system's ability to match individual objects' faces that have been detected. You can see the results of testing the office security system to fit the detected particular objects in Table 3.

Table 3. Results Of Office Space Safety System Testing - Individual Object Matching Detected

Testing	Object Match Duration	Object Matching Status Results	Testing	Object Match Duration	Object Match Detection Results
1	10 seconds	Successfully Matched	16	5 seconds	Successfully Matched
2	8 seconds	Successfully Matched	17	7 seconds	Successfully Matched
3	9 seconds	Successfully Matched	18	8 seconds	Successfully Matched
4	15 seconds	Failed to Match	19	11 seconds	Failed to Match
5	12 seconds	Successfully Matched	20	18 seconds	Successfully Matched
6	8 seconds	Successfully Matched	21	17 seconds	Successfully Matched
7	17 seconds	Failed to Match	22	16 seconds	Failed to Match
8	13 seconds	Successfully Matched	23	14 seconds	Successfully Matched
9	7 seconds	Successfully Matched	24	17 seconds	Successfully Matched
10	9 seconds	Successfully Matched	25	13 seconds	Successfully Matched
11	10 seconds	Failed to Match	26	8 seconds	Failed to Match
12	7 seconds	Successfully Matched	27	6 seconds	Successfully Matched
13	20 seconds	Successfully Matched	28	7 seconds	Successfully Matched
14	15 seconds	Failed to Match	29	5 seconds	Failed to Match
15	12 seconds	Successfully Detect	30	11 seconds	Successfully Matched

After 30 experiments, researchers found that the system succeeded in matching the detected object 22 times. It shows that the system has relatively good accuracy, with the success of matching objects is 73%. The constraints found in this study were the process of matching detected objects that had not been maximally successful. It can occur due to various factors, including the light intensity in the room's form of lighting. It is not always the same. The individual objects detected have considerable noise and the position of individual objects' faces against the camera so that the angle of taking personal items can affect particular objects' results.

It can overcome the current obstacle by increasing the lighting in the room for maximum light intensity. The camera can get individual objects properly and pay attention to the object's angle by adding several cameras to cover a wider area and angle. Besides, to produce better results, researchers can pay attention to the image extraction process. The improved image extraction process can help the recognition process to be more accurate [13]. It is estimated that the next researchers will solve this problem by developing a more modern face detection algorithm with a higher accuracy level.

IV. CONCLUSION

This research concludes that the office space security system prototype using facial recognition features works well (80% successful detection of individual objects). As for the face matching process, the office space security system developed has good accuracy because matching objects' success reaches 73%. Suggestions for future research are that in implementing an office security system that uses facial recognition features, it is necessary to apply a combination of methods and other face recognition algorithms to increase accuracy and fast processing times. This research concludes that facial recognition technology is currently still under development by experts to obtain a high level of accuracy. People can maximally realize the result of smart living, smart city, smart home, and intelligent campus.

ACKNOWLEDGMENTS

We would like to thank Pelita Harapan University, LPPM Pelita Harapan University, Faculty Leaders and fellow lecturers, and all those involved in Pelita Harapan University's internal research with Research No: P-018-FIK / VI / 2018.

REFERENCES

[1] L. Lestary and H. Harmon, “Pengaruh Lingkungan Kerja Terhadap Kinerja Karyawan,” J. Ris. Bisnis dan Investasi, 2018, doi: 10.35697/jrbi.v3i2.937.

[2] I. A. Dianta and E. Zusrony, “Analisis Pengaruh Sistem Keamanan Informasi Perbankan pada Nasabah Pengguna Internet Banking,” INTENSIF, 2019, doi: 10.29407/intensif.v3i1.12125.

[3] R. Umar, I. Riadi, and E. Handoyo, “Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI),” J. Sistem Informasi Bisnis, 2019, doi: 10.21456/vol9iss1pp47-54.

[4] A. Setiawan and A.E. Purnamasari, “Pengembangan Smart Home dengan Microcontrollers ESP32 dan MC-38 Door Magnetic Switch Sensor Berbasis Internet of Things (IoT) Untuk Meningkatkan Deteksi Dini Keamanan Perumahan,” J. Rekayasa Sistem dan Teknologi Informasi, 2019, doi: 10.29207/resti.v3i3.1238.

[5] A. Kurniawan, “Digital Rights Management Sebagai Solusi Keamanan Dokumen Elektronik,” J. Sistem Informasi, 2012, doi:10.21609/jsi.v4i2.251.

[6] S. Widodo, E. Sediyono, and Suhartono, “Desain Sistem Keamanan Distribusi Data Dengan Menerapkan XML Encryption dan XML Signature Berbasis Teknologi Web Service,” J. Sistem Informasi Bisnis, 2011, doi: 10.21456/vol1iss1pp47-57.

[7] E. Yuliza and T. U. Kalsum, “Alat Keamanan Pintu Brankas Berbasis Sensor Sidik Jari Dan Password Digital Dengan Menggunakan Mikrokontroler Atmega 16,” J. Media Infotama, 2015, doi: 10.37676/jmi.v11i1.247.

[8] L. Louis, "Working Principle of an Arduino and Using It," Int. J. Control. Autom. Commun. Syst., 2016, doi: 10.5121/ijcacs.2016.1203.

[9] N. David, A. Chima, A. Ugochukwu, and E. Obinna, “Design of a Home Automation

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v5i1.14435

System Using Arduino," Int. J. Sci. Eng. Res., 2015.

[10] M. K. Syabibi and A. Subari, "Rancang Bangun Sistem Monitoring Keamanan Rumah Berbasis Web Menggunakan Raspberry Pi B+ Sebagai Server Dan Media Kontrol," Gema Teknol., vol. 19, no. 1, p. 22, 2016, doi: 10.14710/gt.v19i1.21959.

[11] M. Arihutomo, A. Budikarso, and Setiawardhana, "Rancang Bangun Sistem Penjejakan Objek Menggunakan Metode Viola Jones Untuk Aplikasi Eyebot," EEPIS Final Proj., 2010, Accessed: Nov. 02, 2016. [Online]. Available: http://repo.pens.ac.id/id/eprint/311.

[12] Y. Yuliana and I. Nurhaida, "Rancang Bangun Aplikasi Pengenalan Wajah menggunakan Metode Viola-Jones dan Algoritma PCA," J. Telekomun. dan Komput., 2018, doi: 10.22441/incomtech.v8i3.3385.

[13] D. E. Kurniawan, K. Adi, and A.F. Rohim, "Sistem Identifikasi Biometrika Wajah Menggunakan Metode Gabor KPCA dan Mahalanobis Distance," J. Sistem Informasi Bisnis, 2014, doi: 10.21456/vol2iss1pp006-010.

[14] N. Saubari, R. Isnanto, and K. Adi, "Jaringan Syaraf Tiruan Perambatan Balik untuk Pengenalan Wajah," J. Sistem Informasi Bisnis, 2016, doi: 10.21456/vol6iss1pp30-37.

[15] I K. S. Widiakumara, I K. G. D. Putra, and K. S. Wibawa, "Aplikasi Identifikasi Wajah Berbasis Androdi," J. Ilmiah Teknologi Informasi, 2017, doi:10.24843/LKJITI.2017.v08.i03.p06.

[16] N. Vd. Lima, L. Novamizanti, and E. Susatio, "Sistem Pengenalan Wajah 3D Menggunakan ICP dan SVM," J. Teknologi Informasi dan Ilmu Komputer, 2019, doi: 10.25126/jtiik.2019661609.

[17] R. Wiryadinata, U. Istiyah, R. Fahrizal, Priswanto, and S. Wardoyo, "Sistem Presensi Menggunakan Algoritma Eigenface dengan Deteksi Aksesoris dan Ekspresi Wajah", J. Nasional Teknik Elektro dan Teknologi Informasi, 2017, doi: 10.22146/jnteti.v6i2.319.

[18] M. R. Hidayat, C. Christiano, and B. S. Sapudin, "IoT-Based Home Security System Design Using NodeMCU ESP8266, HC-SR501, PIR Sensor AND Smoke Detector Sensor," Kilat, 2018, doi: 10.33322/kilat.v7i2.357.

[19] A. Aileen, Hery, A. E. Widjaja, J. T. Purba, and K. G. Simanjuntak, "Recording application with managerial prediction features for skenoo business," in IOP Conference Series: Materials Science and Engineering, 2019, doi: 10.1088/1757-899X/508/1/012133.

[20] M. Chaudhari, S. sondur, and G. Vanjare, "A review on Face Detection and study of Viola-Jones method," Int. J. Comput. Trends Technol., 2015, doi: 10.14445/22312803/ijctt-v25p110.

[21] J. Wang, B. Wang, Y. Zheng, and W. Liu, "Research and implementation on face detection approach based on cascaded convolutional neural networks," in Proceedings - 2017 International Conference on Vision, Image and Signal Processing, ICVISP 2017, 2017, vol. 2017-Novem, pp. 34–39, doi: 10.1109/ICVISP.2017.10.

[22] K. Ganapathy, V. Vaidehi, and J. B. Chandrasekar, "Optimum steepest descent higher-level learning radial basis function network," Expert Syst. Appl., 2015, doi: 10.1016/j.eswa.2015.06.036.

[23] S. Lukas, A. R. Mitra, R. I. Desanti, and D. Krisnadi, "Student attendance system in the classroom using face recognition technique," 2016 International Conference on Information and Communication Technology Convergence, ICTC 2016, 2016, doi: 10.1109/ICTC.2016.7763360.