Available online at
http://www.pancaranpendidikan.or.id

PancaranPendidikan FKIP UniversitasJember
Vol. 07, Issue, 2, pp, 19-28, May, 2018

Pancaran Pendidikan

DOI:
10.25037/pancaran.v7i2.182

ISSN 0852-601X
e-ISSN 2549-838X

Implementation of Eigenface Method in Improving Security in a Smart Home Systems

Abdurrasyid[1]*, Riki Ruli Afandi Siregar[1], Indrianto[1], Meilia Nur Indah Susanti[1]
[1]Sekolah Tinggi Teknik PLN, Jakarta, Indonesia

email: *rasyid@sttpln.ac.id, riki.ruli@sttpln.ac.id, indrianto@sttpln.ac.id, meilia@sttpln.ac.id

ARTICLE INFO

Article History:
Received 1 Maret 2018
Received in revised form 10 April 2018
Accepted 17 April 2018
Published online 1 May 2018

Key Words:
Eigenface, Eigenvector, Eigenvalue, image vector, matrix covariance

ABSTRACT

Based on data that was extracted from Indonesia Central Bureau of Statistics there were has been theft cases as much as 125.869 times during 2015, consists of Crime against Property / Goods with Violence 11.856 cases, and Crimes against Property / Goods Non-Violent 114.013 cases[1], theft often occurs in empty homes that no occupants, theft is also common in homes that have security cameras, cameras that were installed cannot provide prevention or warning to homeowners. It can be anticipated if the homeowner gets information about the condition of the house in real time wherever he is. This technology is designed to created smart home system that was integrated by the security method especially in face recognition, Eigenface method as the image processing method used to detect home occupants to avoid thieves, the core of this method is to compare the eigenface value of the captured image with the eigenface value present in the database, the smaller difference between the eigenface training image in the database with the eigenface test face it can be concluded that the image has a higher similarity, greater differences, will make the system detect that an unknown person is entering the house, and will send a warning message to the homeowner via cell phone about danger that is occurs

INTRODUCTION

Based on data that was extracted from Indonesia's Central Bureau of Statistics there were has been theft cases as much as 125.869 times during 2015, consists of Crime against Property / Goods with Violence 11.856 cases, and Crimes against Property / Goods Non-Violent 114.013 cases[1], theft often occurs in empty homes that no occupants, theft is also common in homes that have security cameras, because the cameras installed cannot provide prevention or warning to homeowners, thus still give the chance to the thief to commit his crimes. Smart home system is an application system that is a combination of technology and services devoted to the home environment with specific functions that help the comfort and safety of its inhabitants. Smart home systems typically consist of control and automation of some devices or home appliances that accessible via smartphones. Smart home design never detached from microcontroller hardware like MyRio 1900[2], Siemens PLC[3], Raspberry[4].

Nowadays microcontroller becoming more popular because it could drive many innovations, sport simulation on archery [5], education [6], On the other hand various data communication could be used to communicate microcontroller and sensors to pass the data like lightweight UDP[7], communication media that was common Wi-Fi and SSL Technologies[8], Web Socket Protocol[9], etc. Smart home system could be created with various facilities, one of the important feature that we can offer is security, especially to secure the home from theft. Eigenface method is one of the face recognition that used Principal Component Analysis that finds a set of projection vectors designed such that the projected data retains the most information about the original data [10], in other hand it was a method for feature extraction that has been proven to be effectively applied in calculations for digital face recognition [11]. However the success of facial detection was affected by some noise factors such as salt & pepper noise, Gaussian noise or Poisson noise to every test image[12].

METHODS

Eigenface method is one of the face recognition methods that recognizes 3 (three) dimensional images into 2 dimensional images by using extracted values based on image vectors on faces obtained from various sides which then produce eigenvalues and eigenvectors. The Eigenvalue is the characteristic value of an n x n size matrix, while the Eigenvector is a non-zero column vector which, when multiplied by a n x n size matrix, will result another vector that has a multiple value of the Eigen vector itself.

The stages of this facial recognition algorithm begin by making the column matrix of faces entered into the database (Figure 1)

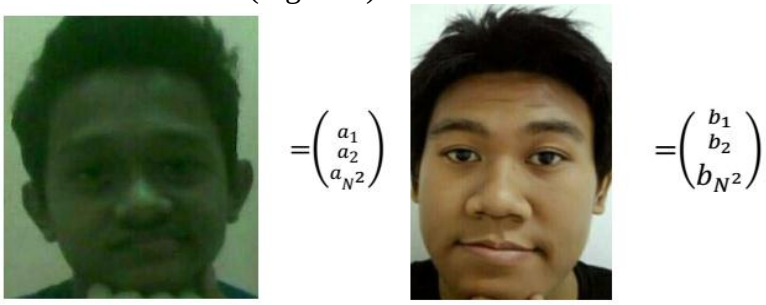

Figure 1. column matrix

a and b are the vectors obtained from the face image that have been broken down. After that, the vector will be put in column matrix, and continued by searching for the average image vector of the next column matrix by using Equation (1).

$$m = \frac{1}{M}\begin{pmatrix} a1 & b1 \\ a2 & b2 \\ a_{N^2} & b_{N^2} \end{pmatrix} \quad (1)$$

M is the number of facial images in the database. While m is the average of the image vector. After the average is obtained, then searched the difference of each matrix of image columns with use equation (2) as shown below.

$$a_m = \begin{pmatrix} a_1 - m_1 \\ a_2 - m_2 \\ a_{N^2} - m_{N^2} \end{pmatrix} \quad b_m = \begin{pmatrix} b_1 - m_1 \\ b_2 - m_2 \\ b_{N^2} - m_{N^2} \end{pmatrix} \quad (2)$$

After the difference is obtained, then the matrix covariance is searched for get the eigen value by using equation (3).

$$S = AA^T \quad (3)$$

Where S is the covariance to be sought, whereas A is the eigenvalue, and A^T is the eigenvector. Once the value is obtained covariance, then the eigen vector value is sorted by largest eigen values. Once sorted, the vector will be reduced by using equation (4).

$$Z_n = e_Z^T(Y_n - m_{n^2}) \quad (4)$$

After the calculation result obtained, then recalculate to get the value of the previously parsed facial image.

Figure 2 shown that this research consists of two parts, the first part is a series of tools, which is centred on Raspberry PI as a microcomputer that processes data and manage the work of each sensor, and the last is software embedded in the mobile smartphone in the form of sdk file.

This research uses Eigenface method as the method used to detect faces as security in smart home, shown in Figure 2, when the camera sensor is activated it will activate the alarm, so when the camera detects faces and faces detected not in accordance with the pattern of faces that have been registered on the database then it will activate the buzzer and send a message to the home owner smartphone.

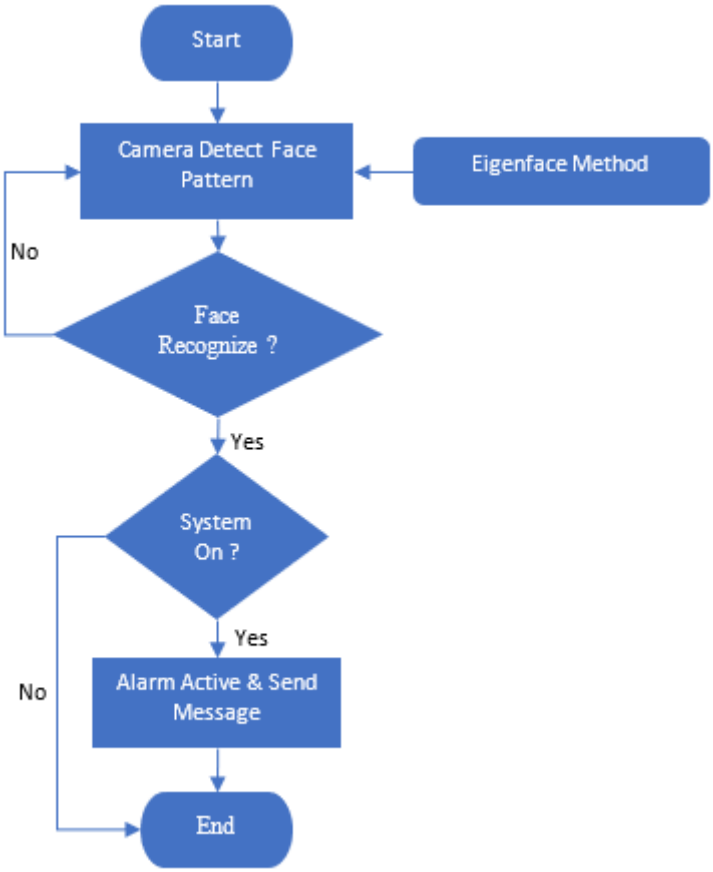

Figure 2. System Workflow

1.1. Hardware Design

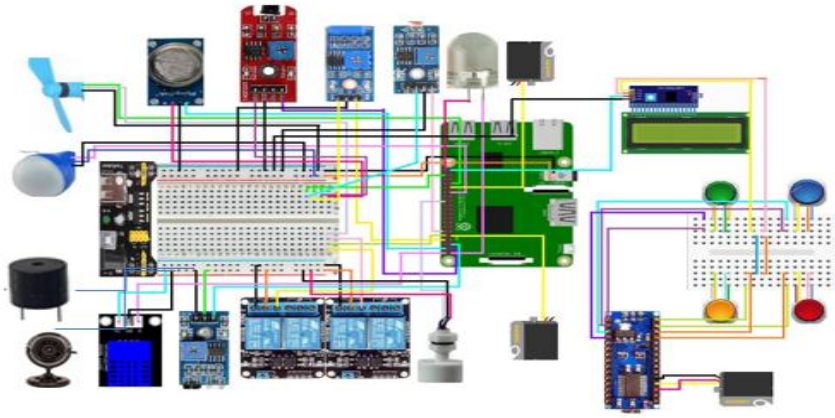

Figure 3. Hardware Block Diagram

Figure 3 above shown the block diagram of hardware, first is a PIR sensor that has been connected to the smart home using Arduino as its connecting media will detect the movement that is around the sensor. Then the camera will do face detection using eigenface method then find out whether the face pattern is recognized or not, if not then will send a message to the owner of the house and buzzer will sound. Once the message is received, the homeowner can immediately check who is detected by the security

sensor by using a camera that has been connected to Raspberry even when they are not at home.

Figure 3, describes how the existing sensors are assembled, there are 5 sensors mounted on the sensor circuit, that are fire sensor, gas sensor, water level sensor, PIR Sensor, vibration sensor, all of the sensors ware connected and controlled by two microcontrollers, Arduino as the sensors circuit centre and Raspberry PI as the data processor.

1.2. Eigenface Software Design Implementation

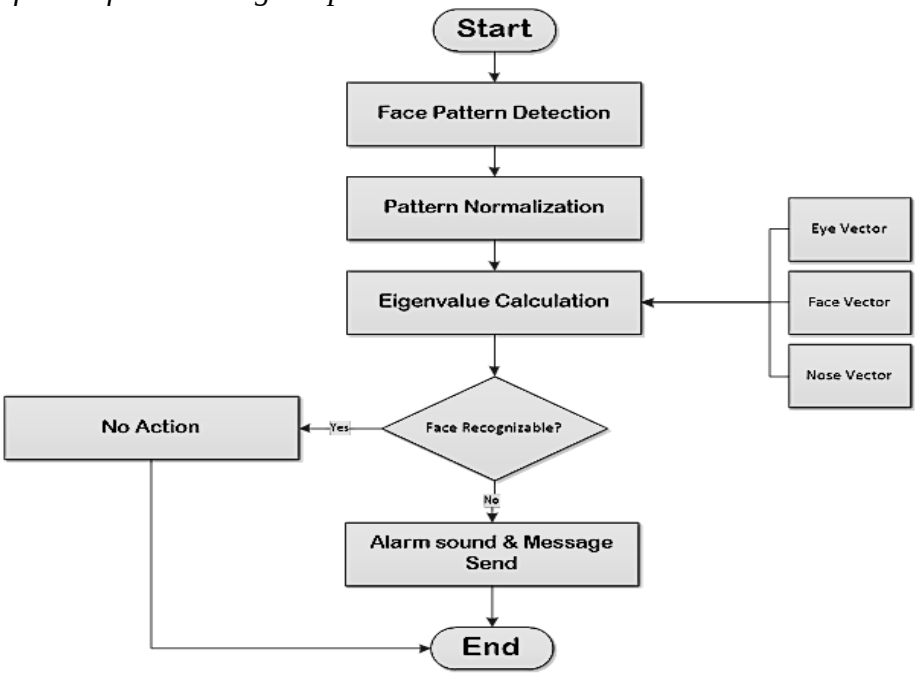

Figure 4. Face recognition workflow

Figure 4 describe how face recognition that implement eigenfece method work, Enable webcam to capture face image, once the camera detects a face pattern, the system will capture the face and face of the capture will appear in the application window that has been created. After the face was displayed in the application window, the system would normalized the image on the face, perform the calculation to get the eigenvalues and also the value of the eigen vector that will be used to obtain eigenface value based on the captured face.

Once obtained eigenface value, then the system will directly do the matching face into the database, whether there are faces that have the same value or near or not. Once matched, if it does not match the database, the alarm will sound and the device will send a warning message to the home owner. If the eigenface value matched in the database, then the system will not do anything.

RESULTS AND DISCUSSION

In this section is divided into 2 parts, the first is how the interface of the smart home model and the designed detection application and the second describes the steps passed on the eigenface method.

1.3. Smart home interface

Figure 5 below show home prototype in the form of a model and smart home application serves as a communication tool between users and home model. In making this smart home system model, the interface is user-friendly designed to be easy to use and understand by users shown in Figure 6.

Figure 5. Smart home model interface

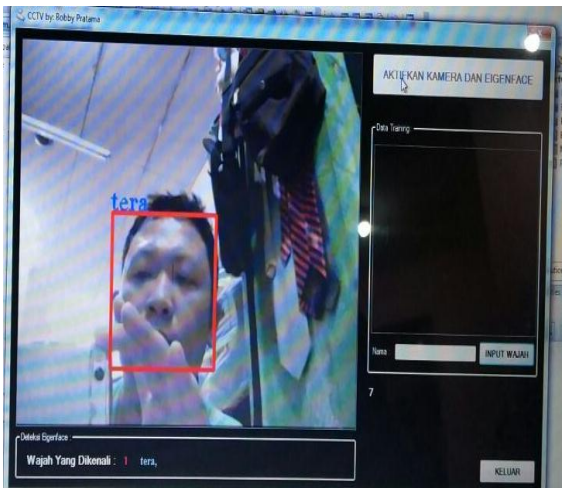

Figure 6. Face pattern recognition result

Figure 7 shows a message that will be sent to the homeowner when the camera sensor detects an unknown person entering the house

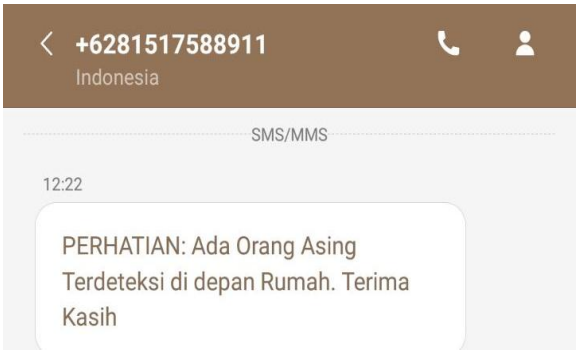

Figure 7. Message result

1.4. Eigenface Calculation

At this stage, the calculation is done to get the value of the eigenface to obtain the eigenface value of the human face by using image training. Here is a calculation of the eigenface method.

a. first is to get the vector value in image training.

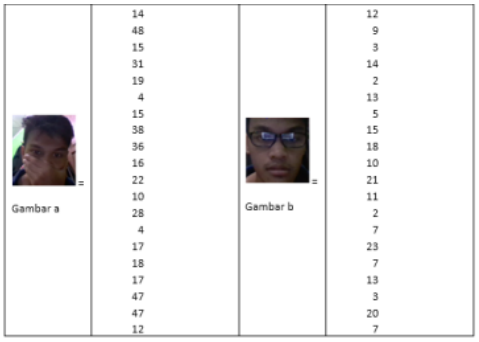

Figure 8. Image training vector value matrix

b. Once obtained, then do a search the average value with the formula as shown in equation 2.

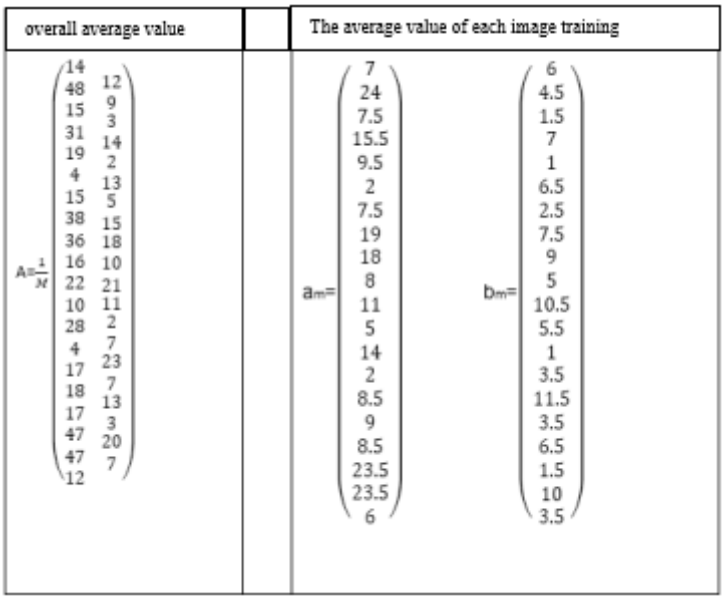

Figure 9. Image training vector value matrix

c. Matrix covariance searching to get the eigen value using equation $S = AA^T$
After obtaining the average value, then find the value of covariance by using the formula $S = AA^T$, and the result is as follows:

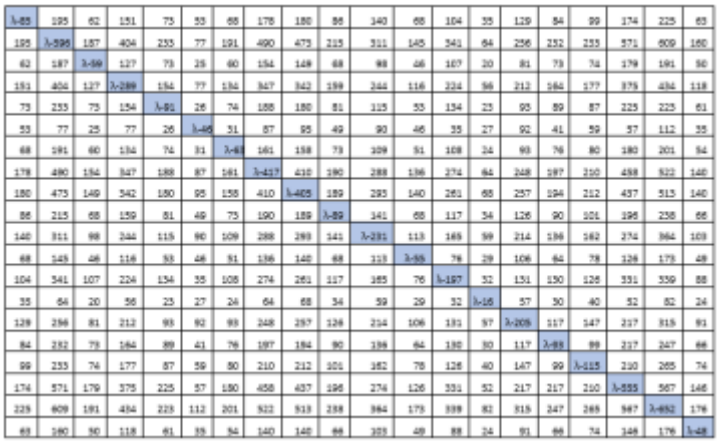

Figure 10. Covariant Value

d. Calculate eigenvalue and eigenvector to get eigenface value

After obtained covariant value next step is calculate eigenvalue with the equation $AV = \lambda V$

The formula of finding eigenvalues is $(\lambda I\text{-}A)\ V = 0$

The determinant results obtained are:

$190\lambda 2 - 38581\lambda + 990138 = 0$

$(190\lambda - 6451)\ (\lambda - 153)$

$\lambda 1=6451,\ \lambda 2=153$

After obtained the eigenvalue, next step is looks for the eigenvector value by entering the eigenvalue that already obtained into the equation $AV = \lambda V$.

After obtained the eigenvector value, next step is looks for the eigenface value we can find the value of eigenface in the training image used.

To get the eigenface value, the formula used is

$\mu = \sum V.\phi$

Information:

μ = eigenface value

$\sum V$ = the total value of the V eigen value

ϕ = Value

CONCLUSION

The research was conducted to produce a smart home system design that could help homeowner to secure homes from thieves, by detecting face patterns matched with data on the database, and send a message to the homeowner if the unidentified face is detected, eigenface method used as image processing methods to detect facial patterns through the stages of the method, in the other hand, this research equipped with several other sensors such as flame sensors, gas sensors, PIR sensors, vibration sensors, and temperature sensors, all of the sensors are coupled to the Raspberry PI and Arduino microprocessors and can be controlled via homeowner smartphone. Further research that can be developed is testing the eigenface method for smart home security by giving some noise factors such as salt & pepper noise, Gaussian noise or Poisson noise to every test image, and then see the results of the test.

REFERENCES

[1] Sub Directorate of Political and Security Statistics, "Criminal Statistics 2016," 2016.

[2] D. A. R.Wati and D. Abadianto, "Design of Smart Home Systems Prototype Using MyRIO," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 215, no. 1, 2017.

[3] C. Barz, S. I. Deaconu, T. Latinovic, A. Berdie, A. Pop-Vadean, and M. Horgos, "PLCs used in smart home control," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 106, p. 12036, 2016.

[4] F. Maulana, W. Soegijoko, A. Yamani, O. V Russkov, and S. E. Saradgishvili, "International Conference on Recent Trends in Physics 2016 (ICRTP2016)," *J.*

Phys. Conf. Ser., vol. 755, p. 11001, 2016.

[5] D. Rusjdi, A. Abdurrasyid, and D. A. Wulandari, "Calculation for simulation of archery goal value using a web camera and ultrasonic sensor," *AIP Conf. Proc.*, vol. 1867, 2017.

[6] Indrianto, M. N. I. Susanti, and D. Karina, "RESLanjut: The learning media for improve students understanding in embedded systems," *AIP Conf. Proc.*, vol. 1867, 2017.

[7] L. Yuan, H. Chen, and J. Gong, "International Conference on Recent Trends in Physics 2016 (ICRTP2016)," *J. Phys. Conf. Ser.*, vol. 755, p. 11001, 2016.

[8] M. Energy *et al.*, "International Conference on Recent Trends in Physics 2016 (ICRTP2016)," *J. Phys. Conf. Ser.*, vol. 755, p. 11001, 2016.

[9] N. Witthayawiroj and P. Nilaphruek, "The Development of Smart Home System for Controlling and Monitoring Energy Consumption using WebSocket Protocol," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 185, p. 12019, 2017.

[10] M. Slavkovic and D. Jevtic, "Face recognition using eigenface approach," *Serbian J. Electr. Eng.*, vol. 9, no. 1, pp. 121–130, 2012.

[11] J. R.-S. J. Ruiz-del-Solar and P. N. P. Navarrete, "Eigenspace-based face recognition: a comparative study of different approaches," *IEEE Trans. Syst. Man, Cybern. Part C (Applications Rev.*, vol. 35, no. 3, pp. 315–325, 2005.

[12] S. LEFKOVITS and L. LEFKOVITS, "Performance Analysis of Eigenface Recognition Under Varying External Conditions," *Sci. Bull. Petru Maior" Univ. Tîrgu Mureş*, vol. 11, no. 2, pp. 44–49, 2014.