Real Time Access Control Based on Face Recognition

Ylber Januzaj[a], Artan Luma[a], Ymer Januzaj[a] and Vehbi Ramaj[b]

***Abstract*— Nowadays the number of thefts and identity fraud has become a serious issue. In order to avoid these thefts and identity fraud, a face recognition system must be established. The scope of this project is to develop a security access control application based on face recognition. The haar-like features is used for face detection and PCA algorithm is used for face recognition. In order to achieve a higher accuracy and effectiveness we use OpenCV libraries and python computer language. Training and identification is done in embedded device known as Raspberry Pi. During our paper we focus on accuracy increment by controlling parameters such as background, light and number of trainings. During our paper we also explicate cost issues of our application compared with commercial applications.**

***Index Terms*— Recognition, Raspberry Pi, OpenCV, PCA.**

I. Introduction

([1], [3], [4]) During the past few years, it has become necessary to have a reliable security system, which can secure our assets in the best and safest way possible. Traditional security systems require the user a key, a security password, an RFID card, or and ID card to have access to the system. However, these security systems have deficiencies, for example, they can be forgotten or stolen from unauthorized people ([2], [6]). As a result, there is a need to develop a software that guarantees a higher security level.

Face recognition is one of the most popular methods of biometric technology ([5], [9]). When compared to other biometric technologies, like fingerprint, voice recognition, and retinal scan, face recognition can be considered more natural. Face recognition also allows access to more than one person, while only giving access privileges to certain people.

In our device, we will be using a Pi Camera, which will provide our entry data, as images. The pictures taken will be saved in a folder called 'positive'. After being saved, the images will be converted in numeric images, as XML file. When the camera scans a person trying to be authenticated, it compares the image to the earlier ones saved in the database. The Raspberry equipment will be used to control the signals sent out to the magnetic lock. If the scanned face is recognized, the system will send a signal to open the magnetic lock for a period of 5 seconds, which will automatically lock after that. Except the magnetic lock, we have used other electronic elements to ensure the proper function of the device. We have used a TIP120 transistor, which allows the connection of the magnetic lock and current through the Raspberry, and a 10 kΩ resistor connecting the button that accepts the signal to activate the recognition process.

Although our project was designed to be used in home and other building's entry systems, that does not limit our project to be used on other environments like detecting unauthorized people, surveillance systems, and courts.

A. *Statement of the Problem*

Security systems are getting more important every day ([2], [9], [16]). These changes are happening proportionally to the number of thefts reported. Based on the reports of my country Police, in my city, during 2014 there have been over 150 thefts reported, in homes and other buildings, therefore there is a need for a higher level of security.

Traditional systems mentioned are not reliable since they can be stolen or forgotten ([7], [8]). For example, password and ID cards can be forgotten/lost or even stolen from unauthorized people.

As a result, access security systems need to develop to be more secure. There is always a need to eliminate traditional systems' flaws. Biometrical technology is considered one of the most secure authentication systems available, by providing a higher level of security than traditional systems ([13], [18], [19]). It is considered this secure since a face cannot be stolen, borrowed or forged in any way to gain access to a building.

We have used the PCA (Principal Component Analysis) algorithm. We have carefully chosen this specific algorithm, since it is easy to use, and more efficient than other algorithms. Using PCA, we have minimized the analysis and development required, by analyzing only some of the similar images from our database.

II. LITERATURE REVIEW

The reason there is a demand to implement an access security system, is to control the people entering and going out of different buildings. As mentioned above, we need to be cautious about the privacy of the building. We have used a magnetic lock as a device to control the entrance of the building.

The magnetic lock consists of a magnet, and a metal bar, which is controlled from the magnet ([10], [11]). The magnetic lock uses 12V current. When the controller is charged with current, the magnet releases the lock, and opens the door, and when it is not charged, the magnet does not release the bar, therefore the door stays locked. It is considered that the magnetic lock is made of a strong material, so the physical security of the door is not a concern, since it is considered almost impossible for the door to be opened without being released from the magnetic lock.

The magnetic lock can operate in different ways, but there are three more basic and efficient methods ([10], [12]). The first method is the magnetic lock connected with a keypad, which requires a password for the magnetic lock to open. The second method is used more for businesses, where it requires

[a]Faculty of Contemporary Sciences, South East European University, Tetovo, R. of Macedonia [a]{yj16535, a.luma, yj11263}@seeu.edu.mk [a]mob: +38649666626
[b]Faculty of Economics, University of Pristina, Pristina, Kosovo, vehbiramaj@yahoo.com [b]mob+37744278990

http://dx.doi.org/10.15242/IAE.IAE0615004

a card which works on frequency radio ([12], [13], [14]). These cards are known as smart cards, and, when a card is identified as a known one from the device, the magnetic lock opens. The third and the most secure method, is through biometric technology, like, fingerprint, retina scan, voice recognition, or the one we will be using, face recognition.

A. Access through password

The most basic access control system is through password combination ([15], [17], [22]).When dealt with a higher security level, there is a need for frequent password update. Another way to get a more secure system, is combining more numbers in the password, to make it harder to guess. It is necessary for the generated password to be kept secret, and not be shared with people who aren't authorized access. This is not considered a very secure system, since, as mentioned above, the password can be forgotten, or stolen from unauthorized people.

B. Access through RFID

Accessing the security system through smart cards, allows authorized people to enter the building ([19], [20], [21]). The system can be designed to allow access to only certain parts of the building. The privileges of entering certain doors, are determined by the data of certain authorizations. There are two kinds of cards, the ones that need physical contact with the base to access the info, and the ones that transmits the data to the base through radio waves.

C. Biometric Technology

([1], [22], [23]) Using the method of identifying physical features of humans, biometric technology has a wide range of use in security systems, and is considered one of the safest methods. In Figure 1, we show the classifications of biometrics. It is divided into two categories, physical and behavioral. The physical part includes physical features like, face, fingers, hands, retina, and DNA, while ability features are unique features like, passwords, signature, and voice ([12], [13], [17]).

Because every person possesses unique features, biometric based security systems are recommended to be used in environments that need a high security level. In ([14], [15]), it is stated that biometrics is the safest technology because features like: face, fingers, and voice, cannot be borrowed or stolen. While applying biomedical technology, at the same time we would be able to find out if a person is using two or more identities.

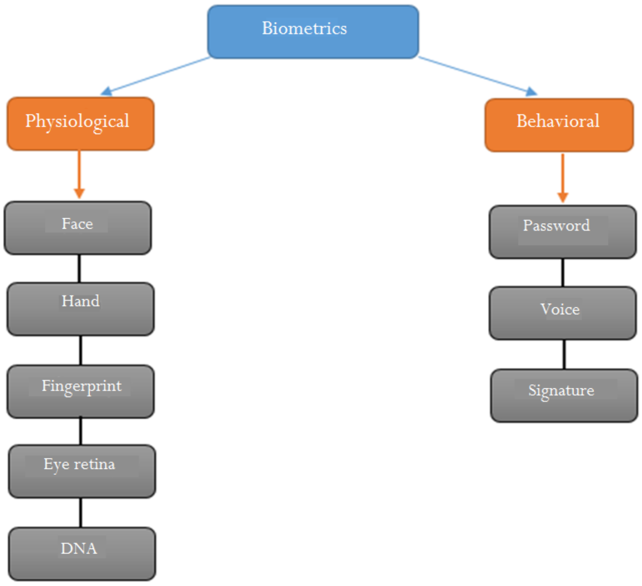

Figure 1. Biometrics

Based on the research done, we have illustrated the differences between biometric technologies. The comparison was made based on 4 factors: accuracy, cost, necessary equipment, and acceptability. We have ranked these factors in three categories: Low (L), Medium (M), and High (H).

TABLE I: BIOMETRIC TECHNOLOGY COMPARISONS

Method	Accuracy	Cost	Equipment	Acceptability
Face	M	L	Camera	M
Hand	M-L	M	Scanner	M
Fingerprint	H	M	Scanner	M
Retina	H	H	Camera	L
ADN	H	H	Test Equip.	L
Voice	M	M	Microphone	H
Signature	L	M	Optic Pen	H
Password	H	L	Keypad	L

Table 1 shows the comparison between biometric technologies. We compared 8 biometric methods. We notice that face recognition has a medium level of accuracy when compared to other methods. This accuracy can get higher when other features are checked, like the background, lighting, and the position of the head. Cost wise, face recognition is cheaper than other methods, that being one of the reasons we have chosen to develop this certain system ([18], [19], [20]). A key component to developing such a system is a camera, and of course, the server that will develop and identify the faces. In the last category, the acceptability, when compared to other methods, face recognition shows medium level acceptance. To lower the acceptance, we have taken three steps. First, we have used an AT&T Database from the 90s, for negative images. These images will train our system to be more accurate when dealt with new images. Second step, was saving a larger number of images per person, in different positions. We have used 5 positions, and for each one of them, we have recorded 10 images, resulting in 50 positive images per person. And the last step we have used to lower the acceptance of unauthorized people, is lowering the positive limit. Since our system gives out low values for known people (the lower the value, the more reliable the person is), we have tried using minimal values as a positive result for our system. Based on ([5], 6], [7]) and the comparisons we have made, we can conclude that our face recognition security system has an accuracy scale of over 62%. Such high accuracy scale has been accomplished by constantly checking the background, lighting, and the position of the head. Other things that played a big role in achieving over 62% accuracy, is the use of many images for an authorized person, using an existing database with images which helps the system to become more smart, and the use of minimal values as a condition for authorization for new people trying to get access to the building.

III. Face Recognition

To implement such a project, the main and most important step was finding the hardware to use for the device. The elements that our device uses are: Raspberry Pi B+ Microcontroller, Camera Pi 5MP, magnetic lock, TIP120 Transistor, 10 kΩ resistor, a button, and a board where the elements were mounted.

We have chosen a Raspberry Pi B+ microcontroller to use in our device. We have done a lot of research, and compared elements in different microcontrollers, like, cost, processing, and user friendliness. The main reasons why we have chosen this specific element, are the high processing capacity, relatively low price, and its ability to adapt in different programming modes. The device uses Linux as an operating system, which has access to a large number of libraries and applications compatible with it. Raspberry Pi has an Ethernet port allowing us a network connection, as long as we are in the same subnet with the device we want to access and manage, 4 USB ports used to connect devices like a keyboard, mouse, camera, and other devices that connect through a USB port, and an HDMI port giving us access to the interface of the operating system installed, and can also be used the first time while installing the devices. It has 40 pins that allow us to receive and send signals. They are divided in half into two groups: the 3V, and the 5V group. Therefore, one side of the microcontroller gives a voltage of 3V, and the other 5V. Besides the 40 voltage pins, it has pins that are used to receive signals, which in our case was used to connect the button, that will send the signal for the face identification. Raspberry Pi does not have an operating system previously installed, but that can be downloaded from the Raspberry website, and transferred to an SD card, preferably larger than 4GB. Figure 2 shows the device along with its components. Later we will give description for each component that is used in our project.

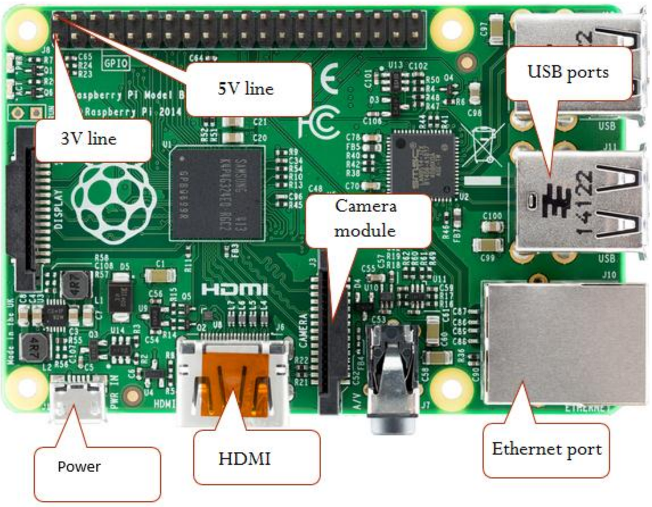

Figure 2. Raspberry Pi B+ microcontroller

A. *Pi Camera*

For our device, we have chosen the Raspberry Pi Camera, which can be integrated directly in the microcontroller. This connection is done through CSI (Camera Serial Interface) bus, which offers an extremely high return of the data, in our case, transfer of the image pixels ([2], [3]). Its dimensions of 25mm x 20mm, and weighing only 3g, makes it very compatible for our project. With a 5MP sensor, this camera offers static images with a resolution of 2592x1944 pixels, and video with 1080p30 and 720p60 resolution [4].

B. *Tranzistor TIP120*

This transistor was used to control the current that is sent to the magnetic lock. Since the magnetic lock gets the current directly from the outside, it is necessary to use this transistor to control the current through the microcontroller. TIP120 transistor has 3 pins, base, collector, and emitter. The base pin is connected directly from the microcontroller, and when the application recognizes a face, it sends a signal to the transistor for a period of 5 seconds, where the magnetic lock is also charged for the same amount of time. After 5 seconds, the signal sent at the base of the transistor stops, and does not allow current to be sent to the magnetic lock.

C. *10KΩ resistor*

To stabilize the circuit we have used a 10kΩ resistor. As mentioned before, the microcontroller has pins that are used to receive signals. In our case, the receiving pin was used to record images when the person is facing the camera. The signal has a voltage of 3V, and it is necessary to use this kind of a resistor to stabilize the voltage in the circuit. It has a resistance of 10kΩ, and a power of 0.25Wat, with a tolerance of 1%.

IV. Application Programming

The software part of the device is done in the Raspberry device. It is divided into three major parts: recording the images, their training, and most important face recognition. Next, we explain how these software parts work together.

A. *Recording the images*

After the application starts, it is necessary for the images that will get access to open the door, to be recorded. The user

http://dx.doi.org/10.15242/IAE.IAE0615004

has to go through a few steps to record the images into the system. The explanation of these steps is below in Figure 3.

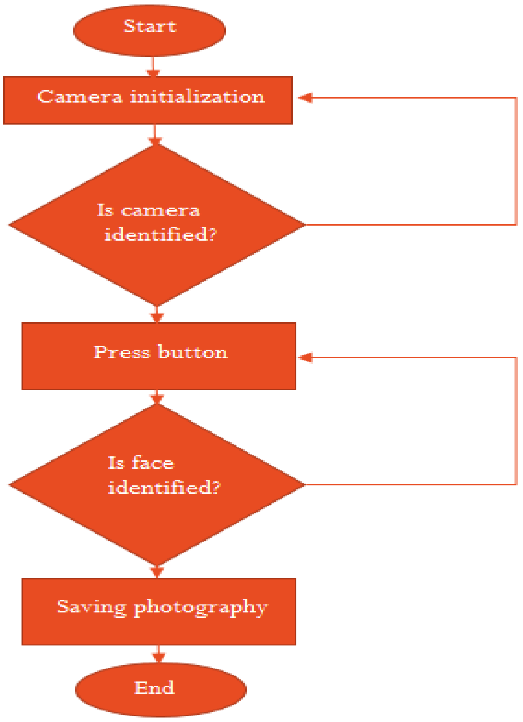

Figure 3. Application process graph

When the application is ready to work, it offers two ways to do the recording, one way through the button connected to the device, and the other through "C" character in the keyboard if available. When recording the images, it is preferred to take 30 pictures for one person, in different positions and different lighting. Next we show how the device is more accurate when raising the number of images. For every picture taken, the application tells if it has managed to identify the face, and if it has, it will be saved in the positive folder. If it can't recognize the face, it will tell that identification wasn't possible.

B. *Image training*

The second most important phase of our application is the image training phase. This includes the process of saving the images into numeric vectors. Later, these values will be used to identify the faces. First, the application reads the two destinations, the one for negative images, and the one for positive images. Both the destinations will be read throughout the training process, and final values will be exported to an XML file called training.xml. During this process the application reads grayscale images, which are later formatted to be used for face recognition. After they are formatted, vectors are set based on X and Y coordinates. After that process, the application continues to save the images in numeric values, and in the end, it will send a message telling that the savings have been successful. All images will be saved in three models, medium, positive, and negative.

C. *Face recognition*

The last step of the application is recognizing the new faces that come to get identified in order to be granted access to the building. Since our previous images have already been saved to numeric values, every new face that comes to be identified, will be recorded as an image, converted to numeric values, and compared to the existing data. If the new data resembles the old ones in the system, it will be considered as a known face and will be granted access to the building, and if not, it is considered as a negative image, and does not have access to the building. This process makes sure that hardware is known to the system, and the training is complete.

One of the novelty of our application is that training and identification is done in embedded device such as Raspberry Pi B+ microcontroller. As we mentioned above it is an appropriate device while it offers interoperability to the users in few aspects. After we finished the programming part we were required to prepare the box of our application. In Figure 4 we can see the box of our application which acts independently from any other device.

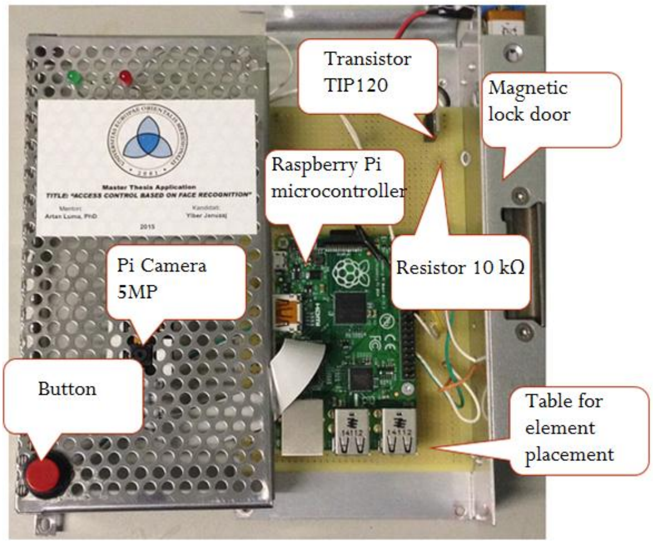

Figure 4. Completed equipment

As we can see here all elements are attached on our device. In this condition the equipment is considered ready to be used in any environment especially in objects that we want to have a more secure control. Next we see two cases when the users arrives to open the door with registered face, and we see the case when the users is identified as negative result. In Figure 5 we have the case when the user is identified. As we can see here the user is required to be in front of camera and press the button, in the moment that he press the button the process of identification starts. If the system identifies the face as positive then microcontroller send signal to the magnetic lock and the door will be open in period of 5 seconds, after this period the user is required to be identified in order to unlock the door. It is preferred to take pictures in different positions such as: smiling, serious, nervous and surprised. We will be informed for the door station by leds which are integrated in our application, as we can see when the user is identified the green led is turned on, otherwise the red led shows the lock state of the door.

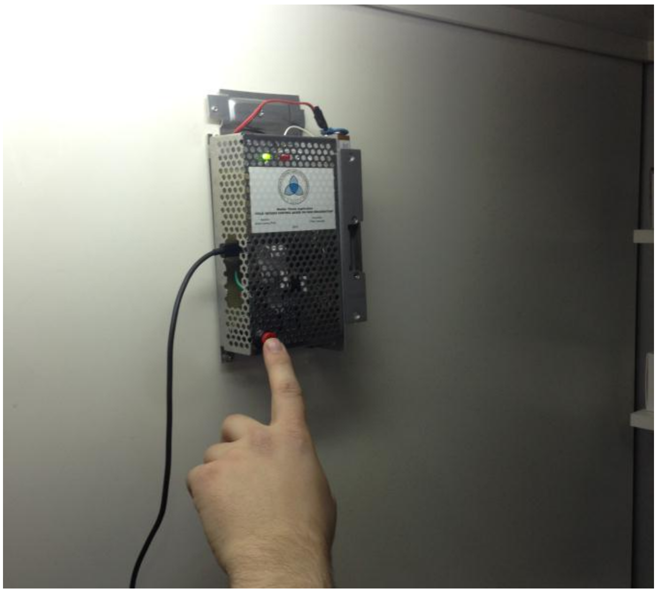

Figure 5. Positive case

In Figure 6 we can se the case when the user is identified as negative from the system. In this case the user is allowed to try 5 times in order to become identified. After 5 times of failure the system will turn a lought siren to inform others that is a fraud case. Also if a user fails more than 5 times, his photos will be saved on a specific folder as a frauder, and the administrator or object owner can see who is this person.

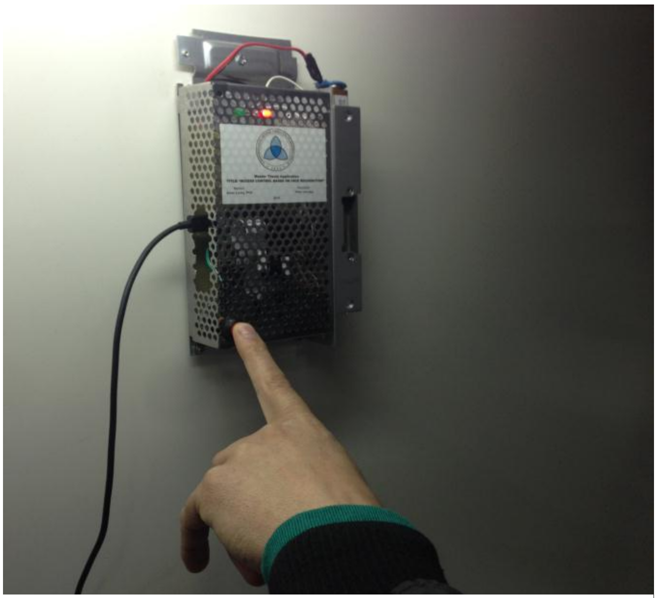

Figure 6. Negative case

As we can in above we have to cases when the user is identified as positive and negative. Next we see results which are derived by tests which are done by us. As we can see we prepared a special box for our application which can be mound in every place that we want.

V. Results

In this chapter we analyze our application based on different factors. We test the application in a controlled and not controlled background, light and no light situations. So our application is more accurate, we will test it with a number of pictures. We will record images in different positions, with each person having a minimum of 30 images, and a maximum of 50 images. We will also test the application through people already registered in our database as positive images, to see its accuracy. All these analysis and results will be presented in a table. The accuracy percentage has been calculated with the formula:

Accuracy = (Face recognition / total number of tests) x 100

Table II: Overall Analysis

Nr	Background	Light	Nr of photos	Accuracy
1	Uncontrolled	Uncontrolled	30	39%
2	Controlled	Uncontrolled	40	46%
3	Controlled	Controlled	40	56%
4	Controlled	Controlled	50	62%

We see in Table II that accuracy of our application grows up from 39% to 62%. The minimum of accuracy is reached when no parameter is controlled and the number of photos in our database is at least 30. And the maximum of accuracy in our application is reached when all parameters are controlled and the number of photos is at least 50. In Figure 4 we can see the graph of our accuracy, and we observe a linear growth of accuracy of our application.

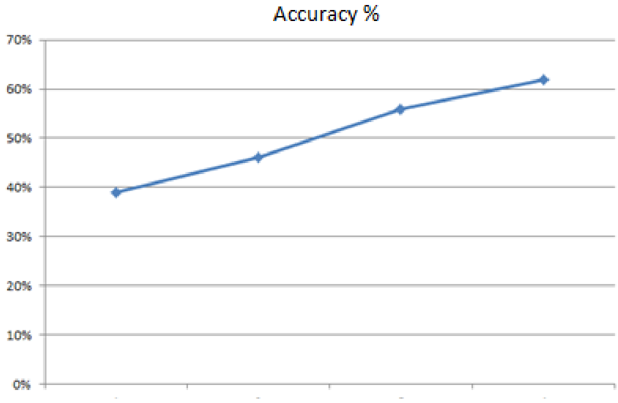

Figure 7. Accuracy of our application

This linear growth of our application accuracy becomes when parameters are controlled. Thus we recommend controlling these parameters in order to have a successful application. As we can see in above pictures we have light in the ambient where the application is places because it is one of our parameters which needs to be controlled.

VI. Conclusion

Throughout our project we have explained the implementation of an application that will control access to a building. We have seen how the accuracy level is higher when factors like: background, lighting, and the number of images are controlled. We have noticed that if all factors are controlled, the accuracy level will be higher. Therefore, as a conclusion it is preferred to control factors like background, lighting, and to have a minimum of 50 images for a person, considering that the device has enough memory. If you manage to control all the factors, our system offers an accuracy of 62%.

The first aim of our project was training and identification in embedded devices. While our device can do the training and the identification independently, without being connected to any other machine we conclude that our goal was achieved. As we know that there are many equipments like this in market, but we choosed to implement this kind of application by the reason of cost. Based on the comparisons our equipment is offered with lower price than commercial equipment.

The second aim of our project was the implementation of a face recognition application using PCA (Principal Component Analysis) algorithm. This particular algorithm is very suitable and fast. Its use allows us to reduce the number of images in our database. In addition the usage of this algorithm enables us to use simple camera which are offered with low price. As a result, we can conclude that our goal, to implement a face recognition system using PCA (Principal Component Analysis) has been achieved.

REFERENCES

[1] Nazeer, S.A., Omar, N., and Khalid, M., "Face Recognition System using Artificial Neural Networks Approach," *International Conference on Signal Processing, Communications and Networking.* ICSCN. 2007. 420-425, 22-24 February 2007 http://dx.doi.org/10.1109/icscn.2007.350774.

[2] Liu, S., and Silverman, M., "A Practical Guide to Biometric Security Technology," *IT Professional*, 27-32, 2001. http://dx.doi.org/10.1109/6294.899930

[3] Jain, A. K., Ross, A., and Prabhakar, S., "An Introduction to Biometric Recognition," *IEEE Transaction on Circuits and System for Video Technology,* 4-20, 2004.

[4] Faundez-Zanuy, M., "Biometric Security Technology," *IEEE Transaction on Aerospace and Electronic System,* 15-26, 2006. http://dx.doi.org/10.1109/MAES.2006.1662038

[5] Kar, S., Hiremath, S., Joshi, D.G., Chadda, V.K, and Bajpai, A.,"A MultiAlgorithmic Face Recognition System," *International Conference on Advanced Computing and Communication*, 321-326, 2006.

[6] Agarwal, M., Agarwal, H., Jain, N., and Kumar, M., "Face Recognition Using Principle Component Analysis, Eigenface and Neural Network," *International Conference on Signal Acquisition and Processing,* 310-314, 2010. http://dx.doi.org/10.1109/icsap.2010.51

[7] Riddhi, C., and Neha, P., "Details Study on 2D Face Recognition Technique Using Local and Global Features," *Indian Streams Research Journal*, 1-17, 2013.

[8] Juwei, L., Plataniotis, K.N, and Venetsanopoulos, A.N, |Regularization Studies of Linear Discriminant Analysis in Small Sample Size Scenarion with Application to Face Recognition," *Pattern Recognition Letter,* 181-191, 2005.

[9] Xueguang, W., and Xiaowei, D., "Study on Algorithm of Access Control System Based on Face Recognition," *International Colloquium on Control and Management*, 336-338, 2009. http://dx.doi.org/10.1109/cccm.2009.5267908

[10] Çarıkçı, M., and Özen, F., "A Face Recognition System Based on Eigenfaces Method," *Procedia Technology*. 118-123, 2012.

[11] Chaoyang, Z., Zhaoxian, Z., Hua, S., and Fan, D. Comparison of Three Face Recognition Algorithms. *International Conference on Systems and Informatics.* May 19-20, 2012.

[12] Kirby, M., and Sirovich, L., "Application of the Karhunen-Loeve Procedure for the Characterization of Human Faces," *IEEE Transaction on Pattern Analysis and Machine Intelligence*, 103-108, 1990. http://dx.doi.org/10.1109/34.41390

[13] Sirovich, L. & Kirby, M., "Low-Dimensional Procedure for the Characterization of Human Faces," *Journal of the Optical Society of America A*, 519-524, 1987. http://dx.doi.org/10.1364/JOSAA.4.000519

[14] Lih-Heng, C., Aslleh, S.H., and Chee-Ming, T., "PCA, LDA and Neural Network for Face Identification," *IEEE Conference on Industrial Electronics and Applications,* 1256-1259, 2009. http://dx.doi.org/10.1109/iciea.2009.5138403

[15] Eleyan, A., and Demirel, H., "PCA and LDA based Neural Networks for Human Face Recognitio," *In: Delac, K., and Grgic, M. Face Recognition System.* Austria: I-Tech Education and Publishing. 93-106, 2007.

[16] Martinez, Aleix M.; Kak, A.C., "PCA versus LDA," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 228-233, 2011.

[17] Kim K., "Face recognition using principal component analysis," *Department of Computer Science, University of Maryland College Park,* 2003.

[18] Bill Ballad, Tricia Ballad and Erin Banks, "Access Control, Authentication, and Public Key Infrastructure," *Book, Jones & Bartlett Learning,* Chapter 1, pp. 13-15. 2011.

[19] Dhiren R. Patel, "Information Security: Theory and Practice." *Book, Prentice-Hall,* Chapter 1, pp. 9-10. 2008.

[20] Sadeque Reza Khan. "Development of Low Cost Private Office Access Control System (OACS)." *International Journal of Embedded Systems and Applications (IJESA)* Vol.2, No.2. 2012.

[21] Muhanad Hayder Mohammed. "SECURE ELECTRONIC LOCK USING PIC 16F628A MICROCONTROLLER.*"International Journal of Research in Computer Science*, 2 (5): pp. 43-47. 2012. http://dx.doi.org/10.7815/ijorcs.25.2012.047

[22] Si Tong Sun et al. "The Design of Electronic Code Lock," *Advanced Materials Research* (Volume 267), Manufacturing Systems and Industry Application: pp. 1001-1004, 2011.

[23] Inderpreet Kaur. "Microcontroller Based Home Automation System With Security." (IJACSA) *International Journal of Advanced Computer Science and Applications,* Vol. 1, No. 6, 2010. http://dx.doi.org/10.14569/IJACSA.2010.010610

[24] Li Hui, Yang Hong-tao, Li Xiu-lan. "Design and application of new kind of electronic and mechanical antitheft lock using DSP". *International Conference on Computer, Mechatronics, Control and Electronic Engineering (CMCE),* 2010.

Ylber A. Januzaj has graduated the Faculty of Contemporary Sciences and Technologies in South East European University. He holds a BSc diploma in Computer Sciences from 2012, and now he is master student in South East European University, in Database Management programme. Currently he is full-type job in a network company, in Kosovo, working as a Network Administrator, and at the same time as a Database Administrator. He has developed many application linked with database, and configured many servers with terabytes capacities.

Artan E. Luma has graduated the Faculty of Contemporary Sciences and Technologies in South East European University in Tetovo. He holds a PhD diploma in Computer Sciences from 2010. From Dec 2010 he is Assistant Professor in South East European University, type of sector: Education and Research. He is author of many publications and many books in the field of Computer Sciences. His work is focused on cryptography field.

Ymer A. Januzaj has graduated the Faculty of Contemporary Sciences and Technologies in South East European University. He holds a MSc diploma in Computer Sciences from 2014. Currently he is full-type job in a network company, in Kosovo, working as an IT director.