A Multimodal Face and Fingerprint Recognition Biometrics System

Maciej Szymkowski, Khalid Saeed

A Multimodal Face and Fingerprint Recognition Biometrics System

Maciej Szymkowski (✉), Khalid Saeed

Faculty of Computer Science,
Bialystok University of Technology, Bialystok, Poland

szymkowskimack@gmail.com
k.saeed@pb.edu.pl

Abstract. Biometrics helps protect users' data against hackers. There are two groups of biometrics features, the first contains physiological features and the second consists of behavioral traits. In the case of biometrics safety procedure the user does not need to remember his/her password because they always have them. It is proved that physiological biometrics can grant higher accuracy than systems that base on behavioral traits. One of the most popular physiological features are fingerprints and face. In the work presented in this paper, these two features are taken into consideration at the same time in a multimodal system. The accuracy of user identification is calculated for each of the two features individually and also for them when combined together.

Keywords: face, fingerprint, biometrics, physiological biometrics, identification, security systems, multimodal systems, fusion

1 Introduction

Recent research is showing that most of security systems are at the risk of breaking their hedges. To protect users' data, biometrics safety procedures introduce the possibility of increasing the system protection level. The main reason of using this kind of safety procedure is that the user does not need to carry the tokens or remember the password. People are simply recognized by the features showing 'what they are' - they are authenticated by their physiological or behavioral characteristics. In biometrics safety systems, simply, the user himself is the key. Fingerprints, retina, face or other measurable traits could play the role of the password, a key that is not as easy to break as the traditional one because human traits are not easy to imitate.

There are two groups of biometrics features. The first is a group that contains representatives of physiological traits. For instance, face, fingerprint, retina or hand geometry are classified as participants of this group. It means that these features are connected with how human organism is built. In the case of behavioral biometrics features, keystroke dynamics, voice or signature are connected with this group.

In the system described in this work, only physiological features are taken into consideration. It is connected with the fact that they are not easy to imitate and that each man have these features unique. On the other hand one can claim that behavioral traits are easier to implement because they, in the most of the cases, do not need any specialized hardware and could be collected without notifying the user. This statement is true but samples of behavioral traits differ from each other even within the same user and hence the repeatability is very low because it is hard to repeat proper activity each time in exactly the same manner. Moreover, physiological traits grant higher level of identification accuracy because of their uniqueness.

The system presented in this paper is multimodal. It means that at least two features are combined in order to check whether this combination gives higher accuracy than the data obtained from each of the selected traits separately. Another goal of the presented approach is to check whether more data to analyze can lead to more accurate classification. In the authors' approach fingerprint and face were chosen. Each of them can easily be collected because most of personal computers contain cameras whilst the fingerprint scanners are available and built-in scanners in the laptops and mobile phones are becoming more popular.

2 Known approaches

Lately more interest in the case of face and fingerprint recognition has been observed. To present the current state of the knowledge, the authors of this work selected a few different approaches that can be compared with the idea presented in this paper.

In [1] an idea that uses eigenvectors to identify user by his face is described. In 1987 the originators of this approach were Sirovich and Kirby although eigenvectors as a significant part of human recognition algorithm were firstly used by Matthew Turk and Alex Paul Pentland. Their algorithm mainly bases on principal component analysis (PCA), in which one of the most essential steps is the image conversion to vertical vector to be a part of the analyzed matrix. Then the mean value of each horizontal vector is calculated and finally the mean vertical vector is obtained to subtract from each of the matrix vertical vectors. The matrix values normalization is done to change all matrix values into 0 – 255 interval. Then main principal values of matrix and each of vertical vectors are calculated. Authors of this algorithm, have only described the processing method, they do not present or compare results.

Authors of [2] mostly based on the idea that was presented by Turk and Pentland in [1]. In the case of Eigenface technique one can easily observe that variation was maximized, while in Fisherface method, the main aim is to maximize mean distance between classes and to minimize variance within each class. Authors of this approach prepared an algorithm in which the Modified Fisher Linear Discriminant Model (MFLD) is used. This model consist of decomposition of Fisher Linear Discriminant into simultaneous diagonalization of the two within- and between-class scatter matrices. As the second part of the work Fuzzy Fisher Linear Discriminant (FFLD) was mentioned. One of the main goals of authors approach was dimensionality reduction of analyzed matrix by which algorithm could be more efficient. To measure distance between two samples, Euclidean metric was used. Authors claimed that by usage of MFLD, accuracy of user identification was 91.4% and for FFLD it equals 94.8%.

Completely different approach, one could observe in the method called Local binary pattern histograms (LBPH). In [1-2] whole image was taken into consideration in contrary to Eigenface and Fisherface techniques, in method that is presented in [3], image local features are taken into account. For each pixel, binary string is determined. It is created by comparison between analyzed pixel value and values of all his neighbors. Therefore each pixel is described by *p*-value binary string, where *p* is a number of neighbors that were taken into consideration in the comparison process. This string is called local binary pattern (LBP). The main idea of this algorithm is connected with dividing an input image into m different parts and calculating function LBP for each, previously separated part. Then for each region histogram that is created on the basis of calculated LBP and specific vector basing on histograms are prepared. For new sample that was not stored in the database, histogram vector is calculated and it is compared with all vectors that are in the database. Authors of this approach have only described the processing method, they do not present or compare results.

In the solution that was originally published in [4], one can observe that authors mainly focused on interesting processing algorithm for fingerprint feature extraction. In the case of this algorithm ridge bifurcations, ridge endings, core and deltas, as a kind of minutiae, are detected. Moreover authors presented their own idea by which all minutiae could be easily described. Feature vector of the whole fingerprint is prepared with usage of minutiae-type, their location and orientation. Authors of [4] claim that there is no such a need to begin fingerprint analysis with image preprocessing (for instance improving contrast or histogram alignment). The authors' algorithm starts with image analysis methods such as initial segmentation, orientation computation and ridge frequency computation. As the main purpose of this stage, localization of a fingerprint area on the image, orientation of each pixel and calculation frequency of ridges are mentioned. On the basis of [4] one could get into know that these steps are enough to prepare fingerprint image to filtration process. Moreover, in this paper authors presented an interesting idea by which spurious minutiae could be easily removed. As it was in the case of [1, 3] in this paper only processing method is described, authors do not present or compare obtained results.

Another solution that was originally published in [5], presents the processing algorithm that could be used to prepare two fingerprints to comparison procedure. One can easily observe that unlike algorithm presented in [4], this one is taking into account only two types of minutiae that are ridge ending and ridge bifurcation. This approach is using CN algorithm to detect different types of minutiae and different image analysis operations that have to prepare an image to minutiae classification. Feature vector consists of minutiae type and localization. Authors of this approach also described comparison method between two different fingerprints. They take into account number of minutiae in two compared images and by its usage determine matching score of analyzed fingerprints. Despite the fact that the whole comparison procedure was described, no information about accuracy of proposed approach were attached in this work.

The algorithm that is presented in [6], as the one described in [5], deals with two types of minutiae – ridge ending and ridge bifurcation but it also takes into consideration Core in fingerprint. Moreover in this solution is not described any specific identification algorithm. On the other hand on the basis of this algorithm, one

can easily prepare feature vector by which comparison between two fingerprint images will be done. In the case of this approach, additional image analysis operations are done on an image. These steps are used to obtain image from which minutiae could be extract.

Due to the fact that in this work authors deal with the problem of multimodal biometrics system, a few works about this kind of systems were also analyzed.

In [7] authors presented a system that bases on two behavioral features that are keystroke dynamics and mouse movement. The dynamics of moving and mouse button dwell times were taken into consideration. Authors prepared simple comparison method by which interesting results were obtained. As a classifier *k*-Nearest Neighbor was used. Authors measured the accuracy for different number of nearest neighbors and for each of the analyzed features separately and also for combination of keystroke dynamics and mouse movement. The best results were obtained in the case of combination of two features and accuracy was 68.8%. All accuracies for other traits were lower than in the case of fusion system.

In the literature there are several examples of multimodal biometrics systems. There are a few different ideas of how these solutions should work [8-10]. In the papers [8-9], no specific solution was presented. Only the main aim and the idea of multimodal biometrics systems were described.

Multimodal biometrics systems that combine face and fingerprint were presented in [11-12]. In [11] authors used face and fingerprint as the primary characteristics and gender, ethnicity, height as soft characteristics. Experiments were done on a database that consists of 263 users. Results show that the recognition accuracy of the primary characteristics can be improved by additional step that basis on soft characteristics.

Authors of [12] also presented the work about multimodal face and fingerprint biometrics system. Face verification module incorporates Gabor Wavelet texture features and face edges. For the fingerprint classification, authors prepared an algorithm that basis on minutiae detection and builds feature vector for each fingerprint from the database and for a new sample. Authors claimed that their system could be effectively used for people identification at airports.

3 Proposed approach

In order to measure accuracy of each of the proposed ways of user identification, an algorithm with its computer implementation in Java are presented. Two algorithms were implemented – one for face recognition and one for fingerprint classification. In the case of face recognition problem, Eigenface method [1] was used. This idea was selected due to the high accuracy level, effectiveness of processing process and simplicity of implementation. It was implemented with the usage of Java CV, which also provides methods by which programmer could easily grab current image from the camera connected to the computer.

Each of users in our database is described by three images of his fingerprint and by three images of his face. In the case of fingerprint classification, authors prepared their own approach that provides a procedure for fingerprint image processing. After image processing, feature vector is generated. Manhattan distance is

then followed with classic *k*-Nearest Neighbor algorithm. All steps of this approach are presented in the form of block diagram in Fig. 1.

At the beginning of fingerprint image processing the image is binarized. Different strategies of binarization were described in [13]. Authors decided to implement manual binarization with threshold set at 215. Pixel value is set to black if condition presented in (1) is satisfied, where x and y are the position of the X and Y axis respectively and R is red channel pixel value at the given location. Accordingly G is for green channel value and B is for blue. The results of this procedure and the original image are presented respectively in Fig. 2a and in Fig 2b.

$$\frac{R_{x,y} + G_{x,y} + B_{x,y}}{3} > threshold \tag{1}$$

As the second step of image preprocessing morphological closing is proposed. This step is connected with the quality of captured images. Due to the fact that these images are not in the best quality, small spaces in fingerprint are visible. Authors implemented this kind of morphological operation because it consists of image erosion preceded by image dilation. It causes that small spacing are filled with black pixels that represents elements belonging to fingerprint and then additional, redundant black pixels are removed. By this operation the fingerprint image quality is a little bit raised.

In Fig. 2c. fingerprint image after thinning procedure is presented. By this step all fingerprint lines are reduced to 1-pixel width. It was done due to the fact that redundant pixels could make significant impact on minutiae detection method. Additional pixels could be classified as pixels that belongs to minutiae but in fact they are not connected with the real one.

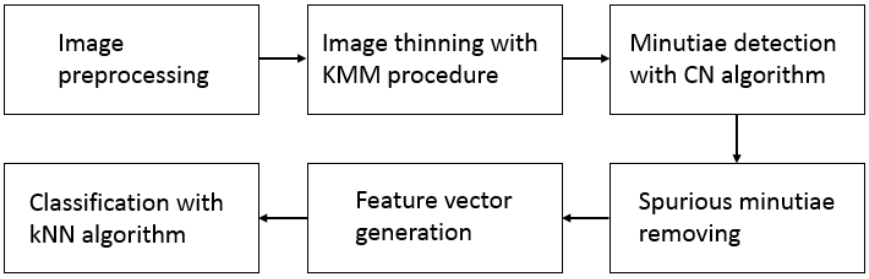

Fig. 1. Block diagram of fingerprint algorithm that was implemented in the application

(a) (b) (c)

Fig. 2. Original image (a) image after binarization procedure (b) and image after thinning procedure (c).

As the third step of image processing minutiae detection was done. All minutiae were extracted with usage of CN algorithm. This solution is a widely-used algorithm for minutiae detection. In this approach authors take into consideration 8 closest neighbors of analyzed pixels. Crossing number was calculated as in (2).

$$CN = \frac{1}{2} \cdot \sum_{i=1}^{8} |P_i - P_{i-1}| \tag{2}$$

By calculation of this number analyzed pixel could be properly classified. When CN = 0 it means that this pixel belongs to background, CN = 1 – means that analyzed pixel is ridge terminal, CN = 2 – points at ridge continuation and CN = 3 – return information that pixel is ridge bifurcation.

Due to the low quality of processed image, as another step spurious minutiae removing was presented. This step was done in the same way as it was described in [4]. It means that distance between minutiae and all of its neighbors is calculated. If this distance is too low, minutiae is classified as spurious and is removed. After removing all redundant minutiae, feature vector is generated. In the case of this approach it consists only of two simple information – number of ridge endings and number of ridge bifurcations. All steps of the processing algorithm are presented in Table 1.

In the case of classification, distances between new samples feature vector and all feature vectors of all samples that are stored in the database are measured. Then classification is done with classic *k*-NN algorithm. Classification procedure is presented in Table 2. In Table 3 description of multimodal system is provided.

Table 1. Fingerprint processing algorithm

Input: Image that is provided by the user.
Output: Feature vector that describes fingerprint.

1. Binarize input image with manual thresholding binarization method. Set binarization_threshold = 215.
2. Do morphological closing with 3x3 mask on the image obtained after step 1.
3. Do thinning with usage of KMM algorithm.
4. Detect all minutiae likely structures on the fingerprint image with usage of CN algorithm.
5. Remove spurious minutiae
    a. Set minutiae_threshold = 60.
    b. For each detected minutiae:
        i. Measure distance to all other minutiae
        ii. If at least one distance is lower than minutiae_threshold remove minutiae that is too close to analyzed one.
6. Count number of ridge bifurcations and ridge endings.
7. Create feature vector that consists of numbers established in step number 6.

Table 2. Fingerprint classification procedure

Input: Fingerprint image sample that is not stored in the database.
Output: Classification decision.

1. Create feature vector for the new sample with usage of fingerprint processing algorithm described in Table 1.
2. For each image in the database:
    a. Create feature vector for currently analyzed image.
    b. Measure distance between feature vectors of currently analyzed image and the new samples one.
    c. Add calculated value to the list with the information about image class.
3. Calculate with k-Nearest Neighbor algorithm the most probable class for the new sample.

Table 3. Multimodal system description

Input: Face and fingerprint images that are not stored in the database. **Output:** Classification decision 1. Create feature vector for fingerprint image and classify it with usage of classification procedure described in Table 2. 2. Classify face image with usage of Eigenface algorithm. 3. Compare classification decisions: a. If both algorithms return the same user class then user is recognized as the one pointed by both procedures. b. If classes returned by both algorithms are different then user is not recognized. 4. Return classification decision.

4 Results of the experiment

Authors' database consists of 50 users that are described by 3 fingerprint samples and 3 face samples each. Experiments were based on dividing the database into two 75-samples sets that were: test and learning set. Also different number of input samples modifications were taken into consideration. Accuracy was also measured for 5, 10, 20, 30, 40 and 45 users. Fingerprint images were obtained with Futronic® FS80 fingerprint scanner, face photos were done with Tracer® PC Prospecto Cam.

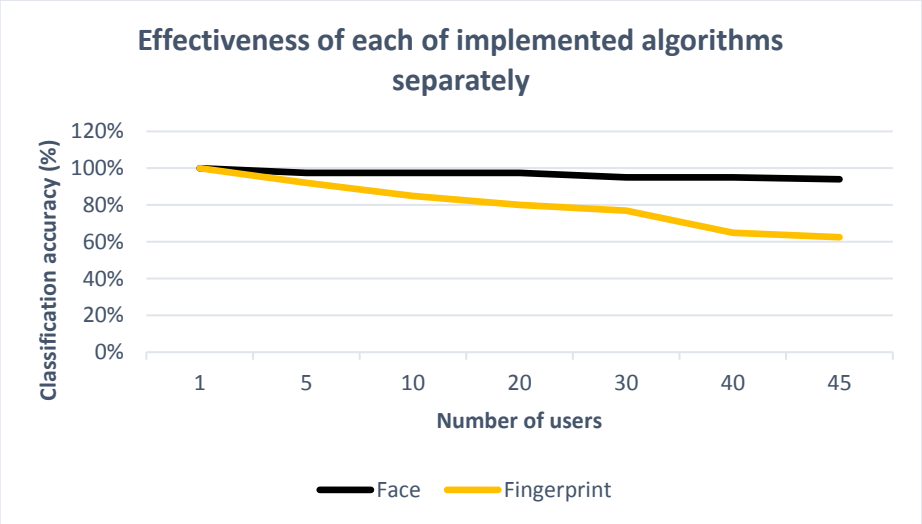

Fig. 3. Effectiveness of implemented algorithms

In Fig. 3 results of two implemented algorithms were presented. As one can observe better results were obtained with usage of face identification algorithm. Results of this way of identification was nearby 100% mostly for each of number of users. In the case of proposed fingerprint classification algorithm with increasing number of users, classification accuracy decreases. Probably it was connected with the fact that simple feature vector was used to describe each of sample. One can observe that by usage of more complex descriptor accuracy level could be higher.

In Fig. 4. the accuracy results of each of identification methods are presented in comparison with the approach when those two features are analyzed simultaneously. One can easily observe that combination of these two algorithms gives quite good results.

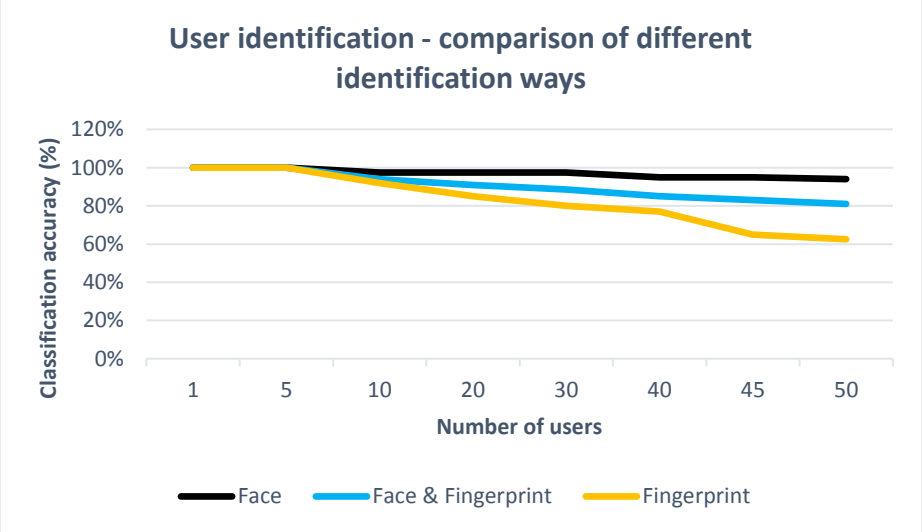

Fig. 4. Comparison of different identification ways

On the basis of the results that are presented in Fig. 4, one can observe that the best implemented algorithm was Eigenface that was used to recognize user by his face. On the other hand, the worst was fingerprint algorithm. As it was mentioned before, this results is caused by simple feature vector. It is observable that two fingerprints that have similar numbers of ridge bifurcations and ridge endings could be classified as fingerprints that belongs to one man. Results that were obtained with combination of these two features are quite good. These results present that user could be recognized on the basis of his face and fingerprint with the accuracy ratio that is nearby 81%.

5 Conclusions and future work

Biometrics security procedures provide new high standard of security methods that can be used in different programs or devices. One can observe that even if user knows how fingerprint or the face of other user looks like, it is really hard for him to imitate these features. What is more, recent cameras or fingerprint scanners take into consideration not only the form of analyzed feature but also its life span. For instance in the case of cameras, user have to move his head in the left and in the right side. By this step false faces, prepared by photos could be detected. Other solution is connected with fingerprints. Fingerprint scanners could also detect temperature of finger and its structure. By these ideas, false fingerprints created with the usage of different materials can also be tracked down.

As expected, combining of two human, physiological features allowed to obtain quite good recognition ratio in the case of user identification. It is easily observable that the accuracy of user identification for both of analyzed features was 81%. This result provides that proposed solution could be implemented in real circumstances. What is more combination of two features can assure better recognition ratio than relying on only one human trait. Proposed fingerprint algorithm accuracy ratio was 62.5%. It is easily observable that combination of face and fingerprint provided better recognition ratio than the approach based only on fingerprint.

The approach presented in this work, can be used in the case of user verification problem. Moreover, one can easily observe that biometrics safety procedure that were implemented in this program, assure satisfying verification accuracy level.

As future work the authors would work under more detailed fingerprint processing algorithm and more effective face identification model. These steps aim to increase accuracy of the presented idea. For instance, more complex feature vector could be used. Moreover different face identification algorithms will be tested. Authors' database is continuously expanding. In the near feature authors would work under detection of more minutiae types.

Acknowledgment

This work was supported by grant S/WI/1/2013 from Białystok University of Technology and funded with resources for research by the Ministry of Science and Higher Education in Poland.

References

1. Turk, M., Pentland, A.: “Face recognition using eigenfaces” – Computer Vision and Pattern Recognition, 1991, Proceedings CVPR 1991, IEEE Computer Society Conference on 1991
2. More, V., Wagh, A.: “Improved Fisher Face Approach for Human Recognition System using Facial Biometrics”, International Journal of Information and Communication Technology Research, Volume 2 – No. 2, 2012, p. 135 – 139
3. http://docs.opencv.org/2.4/modules/contrib/doc/facerec/facerec_tutorial.html#local-binary-patterns-histograms. Accessed 20 Jan 2017
4. Surmacz, K., Saeed, K., Rapta, P.: “An improved algorithm for feature extraction from a fingerprint fuzzy image”, Optica Applicata, Volume 43 – No. 3, 2013, p. 515 - 527
5. Ravi, J., Raja, K.B., Venugopal, K.R.: “Fingerprint recognition using minutia score matching”, International Journal of Engineering Science and Technology, vol 1, 2009, p. 35-42
6. Gnanasivam, P., Muttan, S.: “An Efficient Algorithm for Fingerprint Preprocessing and Feature Extraction”, Procedia Computer Science, vol. 2, 2010, p. 133 – 142
7. Panasiuk, P., Szymkowski, M., Dąbrowski, M., Saeed, K.: “A Multimodal Biometric User Identification System Based On Keystroke Dynamics and Mouse Movements”, K. Saeed, W. Homenda – “Computer Information Systems and Industrial Management, 15th IFIP TC8 International Conference, CISIM 2016, Vilnius, Lithuania, September, 14-16, 2016, Proceedings”, p. 672-681
8. Panchal, T., Singh, A.: “Multimodal Biometric System”, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, 2013, p. 1360 – 1363
9. Ross, A., Jain, A.: “Multimodal Biometrics: An Overview”, Proceedings of 12th European Signal Processing Conference (EUSIPCO), Vienna, Austria, September 2004, p. 1221 – 1224
10. Gavrilova, M., Monwar, M.: “Multimodal Biometrics and Intelligent Image Processing for Security Systems”, United States of America, 2013, ISBN: 978-1-4666-3646-0
11. Jain, A., Karthik, N., Xiaoguang, L., Park, U.: “Integrating Faces, Fingerprints, and Soft Biometric Traits for User Recognition”, Proceedings of Biometrics Authentication Workshop LNCS 3087, 2004, p. 259 – 269
12. Seralkhatem Osman Ali, A., Sagayan, V., Saeed Malik, A., Rasheed, W.: “A Combined Face, Fingerprint Authentication System”, Proceedings of The 18th IEEE International Symposium on Consumer Electronics (ISCE 2014), p. 127 - 129
13. Chaki, N., Hossain Shaikh, S., Saeed, K.: “Exploring Image Binarization Techniques”, Springer India 2014, Studies in Computational Intelligence, Volume 560, ISBN: 978-81-322-1906-4