Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 225 (2023) 2126–2135

Procedia Computer Science

www.elsevier.com/locate/procedia

27th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems (KES 2023)

Usability study of various biometric techniques in bank branches

Arkadiusz Harasimiuk[a*], Andrzej Czyżewski[a*]

[a]*Gdańsk University of Technology, Faculty of Electronics, Telecommunications and Informatics, Department of Multimedia Systems, 11/12 Narutowicza Street, Gdansk 80-233, Poland.*

Abstract

The purpose of the presented research was to evaluate the performance of the prepared biometric algorithms and obtain information on the opinions and preferences of their users in bank branches. The study aimed to determine users' attitudes towards particular modalities and preferences on how to use biometrics after the bank customers had practical experience with the operation of the prototype solutions. The research results allow a better understanding of users' needs and expectations, which can help to increase the knowledge of the need for biometric solutions in banking. Making appropriate changes based on the research results can help improve user satisfaction. The experiments included the collection of biometric sample collection and verification processes conducted by bank customers assisted by employees. The study collected biometric samples and questionnaires from 365 people, and 179 complete verifications were conducted. About 95% of those surveyed expressed acceptance of the implemented solutions for handling transactions using biometrics. The HandVein-FaceImage (hand vein scanning and face recognition) modality pair was rated highest in 70% of cases in the studied population.

© 2023 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0)
Peer-review under responsibility of the scientific committee of the 27th International Conference on Knowledge Based and Intelligent Information and Engineering Systems

Keywords: biometrics; authorization techniques; data fusion methods; opinion surveys

1. Introduction

Biometrics are becoming increasingly common in the banking sector as a tool for customer authentication. However, to ensure the success of implementing such a system, it is essential to understand customers' views on biometrics in banking and their preferences for biometric verification methods. The completed research project, the results of which are briefly presented in this paper, deals with today's exceptionally rapidly developing field of

* Corresponding author. Tel.: +48 58 347 13 01
E-mail address: arekh@multimed.org

1877-0509 © 2023 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0)
Peer-review under responsibility of the scientific committee of the 27th International Conference on Knowledge Based and Intelligent Information and Engineering Systems
10.1016/j.procs.2023.10.203

biometrics. A multimodal biometric authentication center embedded in cloud computing was set as part of the project. Unlike known biometric solutions, the proposed solution is comprehensive. That is, it not only compares biometric samples to determine similarity but controls the entire biometric authentication process, from the registration of samples to their parameterization and comparison with stored templates. The system to was tested in 10 branches of Polish largest bank.

Several years ago, a similar project was carried out by a team from the Multimedia Systems Department of the Gdansk University of Technology, and the results were published [1][2][3]. The new project differs from the previous one. A special biometric kiosk has been constructed and replicated to conduct experiments in natural conditions. The learning algorithms rather than deterministic decision-making ones were used. The method was developed for performing biometric fusion so that individual modalities can be simultaneously considered during biometric authentication rather than only a selected one.

Nowadays, biometric methods are so developed, and the number of publications on them is so great that it is impossible in this short article to review the numerous technologies that make up a complex biometric system. However, it may be helpful to point to cite articles such as [4], which addresses various biometric methods, or [5], which deals with biometric fusion methods. Proprietary work in this area was published in 2022 [6]. Reviewing facial recognition technology is included in the article [7]. The results of the described project in the methods for extracting distinctive features for speech biometrics include publications [8][9]. The current project further includes behavioral biometrics [10], which has been incorporated in the form of eye-gaze modality.

The research coordinated by the authors of this paper used a multimodal approach to user authentication. Fragmented methods of biometric identity verification exist on the market, but they are mostly limited to using one modality in a selected situation. Meanwhile, the developed solution assumes the use of several modalities simultaneously and then performs a fusion of individual extracted parameters (biometric data) to confirm the user's identity. A vital research element in the context of the need for fusion at the stage of analyzing the acquired information is the fusion and interpretation of multimodal data, allowing minimization of the resulting authentication error rates of both FRR (false rejections) and FAR (false acceptances) types. Furthermore, as a result of using several modalities, a scenario in which the customer cannot or does not want to use the offered modalities is also acceptable. In such a case, the biometric data fusion algorithm planned for development during the study will adapt to the current information coming in from each classifier. As the primary data fusion algorithm, it was designed to use a convolutional neural network in the implementation. This network was built based on available programming libraries and trained based on data acquired during experimental research in bank branches and with the participation of mobile bank customers.

The research experiment carried out was based on scenarios involving the use of biometric modalities, based on the use of the following sensors: palm vein scanner (hand vein), microphone track for voice authentication, RGB camera, depth camera (3D), eye-tracking device/to test eye movements.

1.1. Description of used biometric modalities

The remainder of this chapter will briefly discuss the various biometric modalities used.

1.1.1. Facial image biometrics

A developed application installed on a biometric workstation integrated with a graphical user interface is used to record biometric samples of facial images. Upon receiving a message, the service reads the stored samples and uses a neural network to generate a parametric representation of facial images as vectors of 128 floating-point numbers. The parameterization process of facial image samples is carried out in two stages. First, an algorithm detects a face in each image frame using a histogram of oriented gradients (HOG). Then, after detection, a neural network transforms the face image into a parametric representation. Before that, the face image is subjected to an affine transformation that matches the size of the detected face region to the size of the defined network input. The network is a so-called Siamese network for embedding face parameters in a multidimensional space. The network was trained with a collection of faces of about 2,500 people from publicly available biometric databases containing more than 2,500 images. The prepared algorithm for identity verification based on facial image analysis was tested

on a set of about 2,300 people, containing five images for each person. The study shows that the performance measures, TAR (True Acceptance Rate) and FAR (False Acceptance Rate), are 99.14% for FAR=0.1%, respectively.

1.1.2. Voice biometrics

As with the other modalities, an application located on the biometric workstation is used to record voice biometric samples, which the client operates through a graphical user interface. A correctly recorded speech sample is subjected to parameterization. Mel-cepstral coefficients (MFCC -Mel-Frequency Cepstral Coefficients) are used for parameterization. They are formed from the cepstrum of the signal represented on the mel scale (mel-cepstrum).
A vector of mel-cepstral parameters is a vector of cepstrum coefficients in the corresponding mel bands. They are designed to reflect the natural response of the auditory system to stimulation by speech sounds. Mel-cepstral parameters are characterized by low sensitivity to noise and are, therefore, often used in speech recognition. The choice of MFCC as a parameterization method was supported by results from studies using other parameterization methods.
In order to verify identity using a speech sample, a comparison is made between the recorded sample and a pattern in the biometric database. After decryption, the sample is passed to a neural network based on an architecture similar to the DeepSpeaker network. All the training collections included in this corpus, about 960 hours of recordings, were used for training. The number of samples for each speaker varies and ranges from a few to dozens of samples for a single speaker. For the presented model, an Equal Error Rate of 0.0208 and a True Positive Ratio of 0.8421 were obtained. With a False Acceptance Rate of 0.1%, the True Acceptance Rate was 98.29%.
The voice modality work also included preliminary work on testing the vulnerability of the trained model to attacks using a voice cloning algorithm. The experiment consisted of launching an attack on the currently best-trained model using crafted biometric data impersonating other people. The conclusions of the study indicate that work on attack resilience is needed to secure this authentication solution fully.

1.1.3. Gaze tracking biometrics

The biometric data collection process begins by performing a simplified eye-tracking camera calibration for each customer. Next, a message is displayed on the screen informing the customer that their task is to focus their eyes on the points displayed on the screen. In the next step, a starting point (with an increased diameter compared to the test points) is displayed in the center of the screen for a period of 3 seconds. At the same time, the process of downloading data from the eye-tracking camera is started. Subsequent test points are displayed on the screen, the display time for each is 1.5s. At the moment, the procedure contains a total of 27 test points. In the end, the endpoint (analogous to the start point) is displayed. With these assumptions, the data recording time is about 35 seconds. However, it will be possible to shorten the procedure assuming a reduction in the number of test points. This will depend on the analytical results obtained from the data verification process.
Once registration is complete, the collected biometric data is analyzed, and the parameters are calculated for each test point reflecting delayed saccadic movements, the average and maximum speed of saccade movements, the maximum acceleration (absolute value) of saccadic movements, maximum movement speed during fixation, the area of the polygon for fixation, the perimeter of the polygon for fixation, and others. Based on the above scenario, a pilot study was carried out, which yielded a collection containing 111 samples registered on a model test bench. In addition, 146 samples recorded on additional workstations where users worked unsupervised and also on older models of the eye tracking camera were taken. Verification is done by comparing the currently submitted samples with previously recorded reference samples. It was demonstrated that a low-frequency gaze tracker, refreshing data with a time resolution of 30 ms, is sufficient to achieve EER in the range of 6.76%-8% with adequate feature extraction and an XGBoost classifier employed.

1.1.4. Three-dimensional facial imaging

In addition to the usual RGB image, the depth map is an additional standard signal in modern cameras. The signal containing the depth map is obtained by various techniques, among which ToF (Time of Flight) or stereovision are the most commonly used. Two scenarios were considered for the operation of the modality of 3D face imaging. The first assumed a combination at the level of individual frames of RGB and depth images, such that a unified (cropped) set of points representing the colors and spatial distances of the pixels is produced. The resulting 4-channel signal was used to train the neural network. The second variant envisioned treating the depth data as a separate signal, considered independent of the RGB visible signal. In the final implementation, after running the

MOST WIEDZY Downloaded from mostwiedzy.pl

RGB streams and depth map from the 3D camera, the pixel coordinates of each incoming depth map frame are aligned using geometric transformations to match the RGB frame. A face is then detected in the RGB image frame. As such, the images are fed to the input of a parameterized implemented using a deep neural network, whose output is a vector of 1024 floating-point numbers. An additional element in processing a 3D face image is the detection of convexity in the face area based on the depth map. If the area is too flat, the samples are discarded. Finally, parameterized samples are sent to a server, where a comparison is made with reference samples, and a verification score for that modality is determined.

1.1.5. Hand Vein Modality

A palm scan is the first biometric activity when a registered customer comes into contact with a biometric kiosk (named "biometric island"). It was decided to use a PalmSecure reader from Fujitsu. As part of the efficiency study, analyses were made of the time required for a query and response based on the system running at the bank's headquarters. The times needed to send a query and get a response from the server to oscillate around 700 ms. The time required to apply the hand to the reader correctly should be added to the given time. Analyses of the identification speed of the pilot system operating in the bank show that the time of user service from palm application to opening does not exceed 2s. Reducing the time required to get a response from the server is possible by using a more efficient computing infrastructure (increasing the number of processors).

1.2. Hardware implementation of the biometric kiosk

Biometric islands were designed, manufactured, and replicated as part of the project. The following figures show the appearance of the fabricated biometric island, indicating the elements responsible for each modality (Fig. 1).
The kiosk ("biometric island") is the place of the customer's first contact with the system. It is a stationary position in the bank's branch in the form of an interactive kiosk where the customers can register and confirm their identity.

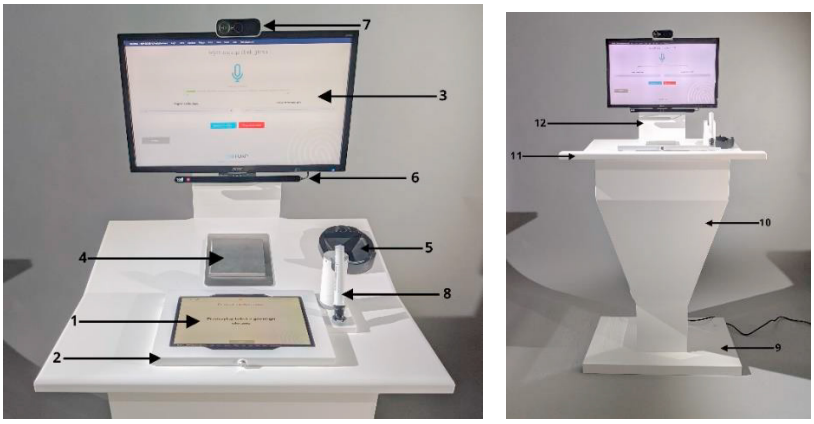

Fig. 1. Appearance of the biometric island. Components: 1. computer, 2. anti-theft case, 3. monitor, 4. ID card scanner, 5. hand vein scanner, 6. eye-tracking device, 7. 2D/3D camera, 8. biometric pen, 9. desktop, 10,12. column, 11. console.

1.3. Fusion of biometric modality results

Fusion uses an algorithm for inference-related calculations using Dempster-Shafer (DST) premise combination theory. The algorithm was developed and verified, primarily on simulated data. An earlier biometric data fusion article described the algorithm and the results obtained [6].

2. Collected surveys and their analysis

Surveys of participants in the conducted sample complemented the project's modality-specific research.
The survey was divided into two parts. To collect survey data, a system prepared for the study was used to handle the various modalities and the surveys in question. The statistical data study was designed to collect information about the people who participated in the study. The data collected included the following aspects: gender, age - given in one of 4 indicated ranges, education, and place of residence. How the surveyed responses were selected was due to both the specificity of biometric solutions and the link between them and their potential use in banking

products. In addition, the final form of the questions was prepared in such a way that they could be completed in the shortest possible time. The survey was geared to handle modalities, and the survey data was a supplement, and for this reason, simplification was taking place in possible aspects. The survey of statistical data included the questions indicated in Tab 1.

Tab. 1 Demographic data of subjects

Question	Answers
1 – Gender	- Female - Male
2 - Please specify age in years	- Below 18 - 18-30 - 31-51 - above 51
3 - Education	- primary - vocational - secondary - higher
4 - Residence	- up to 1000 inhabitants - from 1001 to 300,000 inhabitants - above 300,000 inhabitants

In the case of missing survey data resulting from an interruption in the service process, such a participant was not counted as having passed the biometric sample registration correctly. In addition to a survey on statistical data, a questionnaire was available to collect information on biometrics preferences and applications after using the system. Tab 2. includes items provided as part of the electronic version made available to clients.

Tab. 2 Statistical data survey

Question	Subject
1	In your opinion, does the tested solution increase the security of using the services offered by the bank?
2	Do you accept the use of biometric data in this form for activities performed at the bank?
3	Is the biometric enrollment process intuitive?
4	Is biometric authentication convenient?
5	Does the tested solution provide a sufficient level of discretion when recording biometric data?
Summary	Which modality are you most likely to use in the future to approve banking activities - Handvein - Voice recognition - Face recognition

2.1. Test results

As part of the research conducted, data related to master samples and verifications were collected. Since not all customers were willing to perform verifications, some data collected are limited to submitted master samples alone. In addition, some clients did single verification, and some the full verification. Despite these limitations, however, the usefulness of each case should be noted.

Based on the above data, it is possible to deduce the trend of increasing the number of verifications carried out in the final days of the stages. The verification results obtained met the requirements of the project. It should also be noted here that two aspects were verified as part of the testing:

- correctness of operation of prepared biometric authentication algorithms in real conditions
- correctness of the use of the solution

The following conclusions were drawn during these tests:

- The training process must be careful, and the facilitators themselves must go through the entire process of using the various modalities multiple times
- Prepared solutions from the point of view of operation should be simplified as much as possible for the sake of future self-service
- An important aspect of biometric solutions is to ensure discretion

MOST WIEDZY Downloaded from mostwiedzy.pl

Fig. 2 illustrates the distribution of authentication results

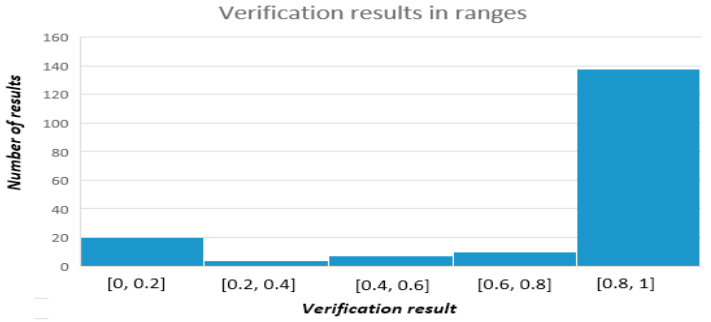

Fig. 2. Distribution of verification results – numbers of results in particular ranges

As the results indicate, most are in the expected upper quartile area. The correctness of the prepared algorithms, and the cases in the first quartile were analyzed, and the impact of the initial lack of understanding of the operation of the various modalities and how to use them could be observed.
Fig. 3 show the verification results related to the sequence and timing of execution.

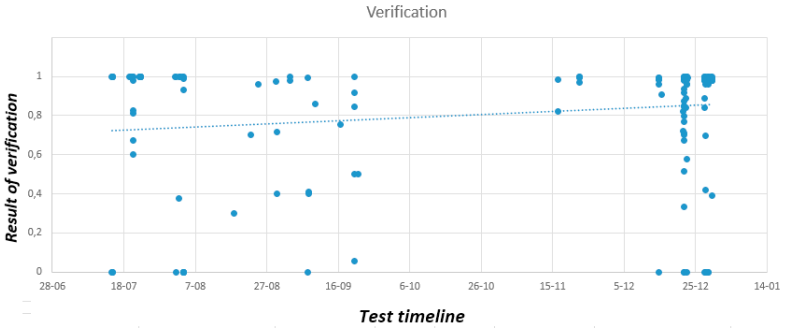

Fig. 3. Distribution of biometric verification results based on test timeline

The charts show the trend of increasing verification results obtained as the term of the study progressed. This has been driven by improving the skills of bank branch personnel in instructing customers.

2.2. Quantitative data from surveys

The users' preferences were analyzed based on the results of the main question from the survey concerning their preferred biometric modality. Tab. 3 and Fig. 4 illustrate the preference results for users who submitted samples and went through the verification process.

Tab. 3 Preferred modalities for those who have gone through the verification process

Preferred modality	Number
FACE	27
GAZE	2
HAND	86
VOICE	5
NO INFO	58
ERROR	1
Total	**179**

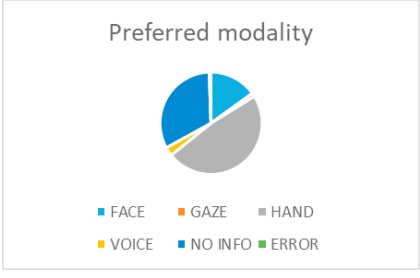

Fig 4: Distribution of verification results that passed the verification process

Tab. 4 and Fig. 5 illustrate the preference results for users who only submitted samples, combined with those who submitted samples, and also went through the verification process.

Tab. 4 Preferred modalities for all people who used the system

Preferred modality	Number
FACE	75
GAZE	9
HAND	246
VOICE	29
ERROR	6
Total	**365**

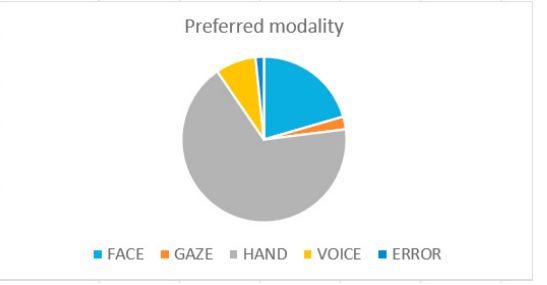

Fig. 5. Distribution of modality preferences for clients using the system

Comparing the results for those who went through the verification process and those who performed only the submission of master samples, excluding those who did not complete the questionnaire, it should be noted that results are similar, not changing with regard to the preferences of individual modalities. It means that a broader familiarization with the modalities does not change the preferences. Based on this information, the following preferred modalities were identified:

- biometry of the hand vein system
- facial image biometrics
- voice analysis biometrics
- eye-gaze tracking biometrics

The survey did not distinguish between a facial image and a three-dimensional image because, from the point of view of handling the process, it was the same functionality.

2.3. Analysis of the correlation of biometric fusion results with individual survey questions

The following comparative analysis in Tab. 5 shows the dependence of verification results on the level of education, considering the number of people in each area.

Tab. 5 Verification quantities and average scores in relation to education

Education	Number of verifications	Verification average
BASIC	8	0.787
HIGHER	105	0.812
MEDIUM	44	0.804
MEDIUM_PRACTICAL	10	0.978
TBD	12	0.708
Total	**179**	**0.811**

This characteristic indicates a majority with secondary and higher education. However, the verifications carried out show no significant discrepancies between the groups. On this basis, it is possible to conclude the acceptability of biometric solutions regardless of education. The following comparative analysis in Tab.6 shows the gender dependence of verification results with the number of people in each area.

Tab. 6 Verification quantities and average scores by gender

Gender	Number of verifications	Verification average
F	95	0.837
M	75	0.795
NO INFO	9	0.666
Total	**179**	**0.811**

The following comparative analysis in Tab.7 shows the age dependence of verification results with the number of

MOST WIEDZY Downloaded from mostwiedzy.pl

people in each area.

Tab. 7 Verification quantities and average scores in relation to age

Age	Number of verifications	Verification average
<18	5	0.912
>51	58	0.759
18-30	34	0.836
31-51	73	0.852
NO INFO	9	0.666
Total	**179**	**0.811**

The following comparative analysis in Tab. 8 looks at the dependence of verification results on the place of residence, considering the number of people in each area.

Tab. 8 Verification quantities and average scores in relation to place of residence

Residence	Number of verifications	Verification average
CITY	146	0.811
NO INFO	9	0.666
NULL	2	0.995
TOWN	16	0,804
VILLAGE	6	0.989
Total	**179**	**0.811**

The above cross-sectional analyses allow relating the results of the obtained verifications to the analyzed behavioral parameters. These data firstly indicate the structure of customers appearing in branches. The majority of customers are urban, with higher education, both genders and over 30 years of age. While the place of residence should be linked to the branches where the surveys were conducted, the other parameters fully reflect the bank customers' structure. For age-related data, we can observe weaker results in the highest age group, which is a rationale for appropriate further development of the service in terms of these users. For other parameters, the verification results obtained for all parameters do not differ significantly, which means that the solutions have been prepared adequately for potential customers' needs.

2.4. Discussion

Questionnaires have been collected, supporting the document handling process by biometric solutions. The following summaries were prepared cross-sectionally for two different cases. The first is a separate subgroup of results for users who submitted samples and went through the verification process. The second case for which survey data was collected is all users who submitted samples, including those who underwent the verification process.

The following Fig.6 illustrate the survey results on the following issues on which customers commented:

1. In your opinion, does the tested solution increase the security of using the services offered by the bank?
2. Do you accept the use of biometric data in this form for activities performed at the bank?
3. Is the biometric enrollment process intuitive?

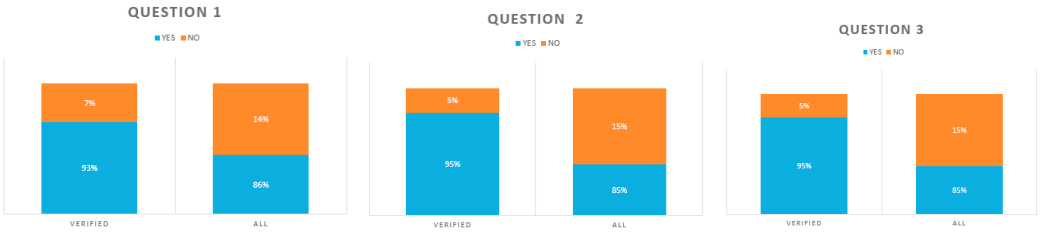

Fig. 6. Results of answers to question 1, 2 and 3

A trend was indicated regarding issues related to understanding the importance of biometrics in enhancing security, acceptance of biometric solutions in biometric activities, and intuitiveness.

While the first two aspects are related to the participants' feelings, the last one indicates that even a single repetition of using the modality was already able to raise positive attitudes toward the solution.
Fig.7 addresses issues from the surveys collected:
4. is biometric authentication convenient?
5. does the tested solution provide sufficient discretion when recording biometric data?

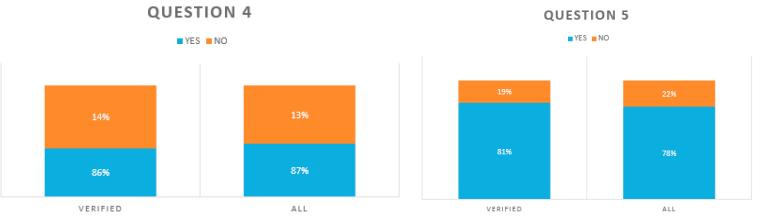

Fig. 7. Results of answers to question 4 and 5

Information regarding the convenience of the solution and discretionary issues did not vary between users who only submitted samples and those who went through the verification process.
The work included verifications of camera positioning, particularly in areas where changing lighting conditions caused the cameras to malfunction. According to the quantitative data shown earlier, the voice modality was not often used. For this modality, the aspect of discretion was raised by respondents. If the work continues, this should be one aspect to be addressed in two threads: a separate room for the submission of master samples and setting up the biometric kiosk in such a way that banking activities, including the handling of biometrics, are carried out with the expected level of discretion.

2.5. Analysis of modality pairs used for fusion verification

Tab. 9 shows the results of the combined modalities in terms of the average scores obtained, taking into account the number of participants

Tab. 9 Quantities and average scores of verification obtained in pairs of each modality

Education	Number of verifications	Verification average
Face3D-HandVein	1	0.985
FaceImage-Face3D	3	1.000
FaceImage-HandVein	11	0.953
HandVein-Face3D	15	0.686
HandVein-FaceImage	127	0.854
HandVein-Voice	19	0.660
Voice-FaceImage	1	0.000
Voice-HandVein	2	0.350
Total	**179**	**0.811**

Based on the results presented, it can be seen that the most common modality pair is Handvein-FaceImage. This result also coincides with the preferred modalities indicated by the respondents. The best results from the average verification results were obtained for the FaceImage-FaceImage3D pair. The above results are one of the elements for the developed recommendations resulting from the project.

3. Conclusions

The research used a multimodal approach to user authentication using several biometric modalities simultaneously, and then performing fusion allowed the solution to be verified under experimental conditions. The usability tests verified the practicality of the biometric modalities prepared as part of the project using biometric kiosks installed in bank branches. Furthermore, the results obtained from both collected samples supplemented by surveys and direct contacts allow us to confirm the effectiveness of the solution and recommend further work and improvements.
Studies have shown that the preferred modalities: hand vein and facial images, are best perceived by users and most often used in fusion, yielding good results. For this reason, they are recommended for implementation first.
These indications come from the numerical results of the modality pairs and the analysis of user feedback.

MOST WIEDZY Downloaded from mostwiedzy.pl

It is recommended that work continues implementing voice biometrics, which in light of documented studies, has achieved high resistance to attacks using the popular voice cloning method [6].

4. Acknowledgments

This research was funded from the budget of project no. POIR.01.01.01-0092/19 entitled: "BIOPUAP - a biometric cloud authentication system," financed by the Polish National Centre for Research and Development (NCBR) from the European Regional Development Fund.

References

[1] P. Szczuko, A. Czyzewski, P. Hoffmann, P. Bratoszewski, M. Lech, Validating data acquired with experimental multimodal biometric system installed in bank branches, Journal of Intelligent Information Systems, 2017, IF:1.294, 10.1007/s10844-017-0491-2.

[2] P. Szczuko, A. Czyzewski, M. Szczodrak, Variable length sliding models for banking clients face biometrics. Multimedia Tools and Applications Multimedia Tools and Applications (2019) 78: 7749. https://doi.org/10.1007/s11042-018-6432-4

[3] A. Czyzewski, P. Hoffmann, P. Szczuko, A. Kurowski, M. Lech, M. Szczodrak, Analysis of results of large-scale multimodal biometric identity verification experiment. IET Biometrics (Vol. 8, 1, 2019) DOI: 10.1049/iet-bmt.2018.5030

[4] Sabhanayagam T., et al., A Comprehensive Survey on Various Biometric Systems. Int. Journ. of Applied Engineering Research, Volume 13, Number 5 (2018) pp. 2276-2297.

[5] Singh M., et al., A comprehensive overview of biometric fusion. Information Fusion 52 (2019) pp. 187-205.

[6] Szczuko, P., Harasimiuk, A., Czyzewski, A. Evaluation of Decision Fusion Methods for Multimodal Biometrics in the Banking Application. Sensors 2022, 22, 2356. https://doi.org/10.3390/s22062356

[7] Introna L. D., Nissenbaum H., Facial Recognition Technology: A Survey of Policy and Implementation Issues. Lancaster University. https://www.researchgate.net/publication/228275071

[8] Zaporowski S., Czyżewski A., Audio feature optimization approach toward speaker authentication in banking biometric system. doi: The Journal of the Acoustical Society of America 150, A349 (2021); https://doi.org/10.1121/10.0008549

[9] Piotrowska M., Korvel G., Kostek B., Ciszewski T., Czyzewski A.. Machine Learning-based Analysis of English Lateral Allophones. International Journal of Applied Mathematics and Computer Science. 2019;29(2): 393-405. https://doi.org/10.2478/amcs-2019-0029

[10] Liang Y., Behavioral Biometrics for Continuous Authentication in the Internet-of-Things Era An Artificial Intelligence Perspective. IEEE Internet of Things Journal, Vol. 7, No. 9, Sept. 2020