MSC 68T10 **DOI: 10.14529/jcem190103**

IMPROVED CONTINUOUS AUTHENTICATION SYSTEM WITH COUNTERFEIT PROTECTION

A. A. Kudinov[1], neverdark74@gmail.com,
S. M. Elsakov[1], elsakovsm@susu.ru
[1] South Ural State University, Chelyabinsk, Russian Federation

The article examines the possibility of improving the security of user workstations equipped with web cameras. This is achieved by implementation of continuous user authentication through face recognition. This method significantly increases a security level of the system from the threat of gaining access while the user is not at the workplace. In addition, various methods to protect the system from imitating the images of a genuine user were developed. Testing various approaches to solving the problem was performed and the reliability of the system was estimated.

Keywords: authentication; face recogniton; webcam; photo recogniton; Dlib library.

Introduction

While a user is not at his workplace, access to his computer or mobile device can be intercepted through input-output devices. Especially it concerns systems in high-risk environments, such as computers at the banks or management of important objects [1]. The standard protection consists in fixing of a certain time interval. If no user actions are detected during this interval, the computer is blocked and re-entering the password is requested. Otherwise, the computer is not blocked. An intruder can exploit this and perform an arbitrary input.

To increase the level of protection, we propose to use the system of continuous authentication, which is capable of verifying a user for authenticity in a short time period. Since it is futile to force a user to constantly enter a password or insert a token, the only possible suitable factor for continuous authentication is biometrics. A chosen authentication method is 2-dimensional recognition of face geometry using a standard webcam.

1. Related Work

Researches propose such solutions as recognition of the key typing [2], recognition of a user's finger movements on the touch screen of the mobile device (using the specially developed digital sensor glove) [3], and computer mouse movement analysis [4]. Their distribution is blocked by various factors: a clear keyboard handwriting is formed not by all users; scanning of finger movements requires a special glove, which will have to be purchased additionally; the movements of the computer mouse are subject to elementary falsification.

It was also proposed to identify the characteristics of the human heart: its tones [5] and geometry [6]. For these methods, a very high level of reliability is achievable since neither tones nor the geometry of the heart is practically impossible to falsify. The main disadvantage of these methods is the need to purchase additional expensive equipment.

Recognition of the geometric characteristics of the user's face was proposed by [1, 7, 8]. In [8], a continuous authentication system was developed using a three-dimensional RGB-D camera. It achieved very high reliability indicators (EER $\approx 0.8\%$). However, three-dimensional cameras are very rare at the moment.

In [1, 7], two-dimensional face recognition was proposed. In [7], the front camera of the smartphone is used to obtain the image, in order to detect the necessary facial features when the user conceals or leaves the boundaries of visibility. In [1], a standard webcam was used, but authentication is not really continuous, it works whenever a user attempts to perform any operation requiring access. In both works, acceptable reliability indicators were achieved, but there is no possibility to recognizing a photo of an authentic user that an intruder can show to a camera.

The paper considers the method of continuous authentication, which has the following advantages:

–to use this method of biometric authentication, only a web camera is required that is built-in most smartphones and laptops or can be purchased at a low price;

–by monitoring from a webcam, it is possible to activate the energy saving mode of the computer during the absence of the user, which will save energy;

–the ability to distinguish a living user from his photo.

This paper is organized as follows: Section 2 describes the algorithm used for face recognition. Section 3 shows the results of testing performance and system accuracy. Finally, Section 4 presents our conclusions and considers further perspectives followed by references.

2. Face Recognition

Face recognition is reduced to a process consisting of two stages:

–face localization on the image (i.e. detection);

–detection of key structures on the face surface.

To achieve this, we used the facial landmarks construction algorithm described in [9] and implemented in the Dlib library. To identify a face, it localizes and marks the following areas: the right eye, the left eye, the right eyebrow, the left eyebrow, the nose, the jaw.

The work uses the pre-trained convolutional neural network ResNet [12]. The layers that are responsible for the classification are cut off from the network, and only the convolutional layers remain that extract the key features from the image, i.e. structure of the face. In Dlib a modified version of this network is used – ResNet34.

The image is marked with the specific (x, y)-coordinates that surround each of the above facial structures. There are 68 such landmarks in total.

As a result, the network produces a vector d called a descriptor. Such descriptors will be extracted from an original user image and from an image received from the web camera.

The descriptors are used for face recognition: for this purpose, the Euclidean distance $e(d, c)$ (where d and c are two different descriptors) between them is calculated by

$$e(d, c) = \sqrt{\sum_{k=1}^{n} (d_k - c_k)^2}. \tag{1}$$

If this distance is less than some constant *threshold*, then it is considered that the

persons belong to the same user, therefore, the person's face is identified. Otherwise, the user s access to the system denied.

If a user's face is rotated, the affine transformation of the derived landmarks is performed.

3. Testing

To evaluate the effectiveness of continuous authentication, the following criteria are used:

–False Accept Rate (FAR) means the probability that the system recognizes another person (impostor) as a legitimate user;

–False Reject Rate (FRR) means the probability that the system recognizes legitimate user as an impostor;

–Equal Error Rate (EER) determines the accuracy of the recognition;

–RAM usage;

–CPU usage;

–Duration of one recognition procedure.

To get the EER, it is necessary to plot the FAR and FRR graphs. EER will be equal to that value of $FAR(threshold)$, at which it is equal to $FRR(threshold)$, i.e. EER is at the intersection of these graphs:

$$EER = FAR(threshold) = FRR(threshold). \tag{2}$$

3.1. Dataset

Video from 11 different videobloggers of different emotional expressiveness, various illumination level and duration from 10 to 220 minutes was used as a data set.

All the videos were taken from YouTube. Videoblogers were divided into two groups. Bloggers from the first group have weak emotional expressiveness and use a dark background. Bloggers from the second group have strong emotional expressiveness and use light or neutral background.

Videos from the first group:
https://www.youtube.com/playlist?list=PLjd1aefITwnGbaW0mBNna9e1qVBhNV4t0

Videos from the second group:
https://www.youtube.com/playlist?list=PLjd1aefITwnHiW9-9IB5V6tLDeVitb5Lh

3.2. Evaluation of Accuracy

Before testing, each blogger was registered in the system as a user with his login and received his own template. A template is a set of four manually taken images containing a face. On three images a face is turned towards the camera, and on the fourth one it is rotated 45 degrees to the side to test the quality of affine transformation the face landmarks. The descriptors d_1, d_2, d_3, d_4 are computed for all 4 images.

A FAR graph is plotted according to the following algorithm:

–$threshold$ takes values 0.01, 0.02, ..., 1.0.

–The descriptors d_1, d_2, d_3, d_4 are computed for a template of each user.

–The system consistently scans the videos of all other bloggers and processes 100 frames from the beginning of each blogger's video. When processing a frame, the system

looks for a face on it. If a face is found, the descriptor $d_{current}$ is calculated from it.

–Euclidean distance between each of $d_{1...4}$ and $d_{current}$ is calculated. The result is 4 values e_1, e_2, e_3, e_4. The average value e is calculated from them by $e = e_1 + e_2 + e_3 + e_4/4$;

–If $e < threshold$, then the value is considered erroneous.

–FAR for one $threshold$ value is the ratio of the number of erroneous values to the total number of values.

–Based on the 100 FAR values obtained, the $FAR(threshold)$ graph is plotted.

To calculate a FRR, the user's template is compared to the 100 frames from the beginning of video of the same user. Erroneous values should exceed the $threshold$. The remaining steps of the algorithm are the same as in the FAR calculation algorithm.

Consider the change of an EER when changing the following parameters, which can affect the quality of recognition:

–User s template;

–Video resolution;

–Illumination (brightness) of the template images.

The standard test was conducted on video with a resolution of 360p. The test results are shown in Fig. 1 (marked as FAR_1, FRR_1). FAR and FRR intersect at $threshold = 0.63$, and an EER of 0.87% is achieved. Next, the impact of various user's templates on an accuracy of the system was tested. Templates were obtained automatically directly from the video by reading every 100th of the processed frame as one of four images. Test results with the modified template are shown in Fig. 1 (marked as FAR_2, FRR_2). Changing the template has almost no effect on an accuracy: $EER = 0.88\%$. But FAR_1 and FRR_1 are less than FAR_2 and FRR_2 with same $threshold$ values.

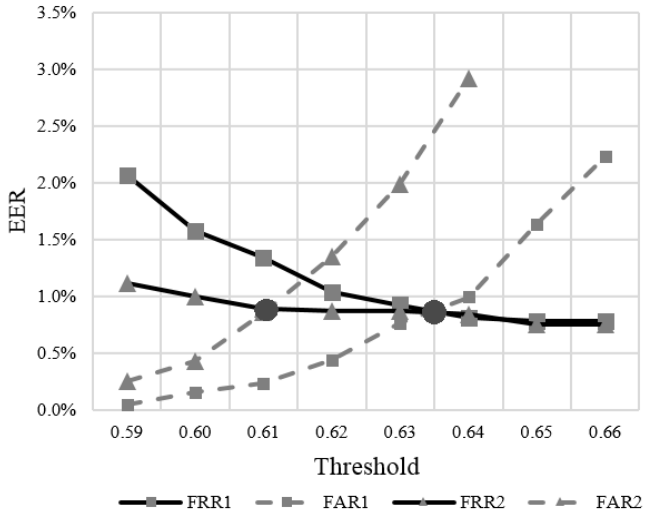

Fig. 1. Illustration of ratio FAR to FRR for the standard test and test with automatically obtained samples (fragment). Intersection points are marked by a circle.

As a rule, FAR is much lower than FRR in single-entry authentication systems (for example, 6.5% FRR and 0.1% FAR) [10]. This is justified since it is usually more important to block access for an impostor than allow it for a legitimate user. In the case of continuous authentication, it is highly likely that an already authorized user can

be incorrectly identified and denied access during the session. To solve this problem, we propose to keep FRR on balance with FAR.

Testing was also conducted for the two groups separately (see Fig. 2, first group is marked as FAR_1, FRR_1, second group marked as FAR_2, FRR_2). The first group was much easier to recognize than the second group: EER for the first group of 0.15% is achieved, at $threshold = 0.59$. EER for the second group of 1.31% is achieved, at $threshold = 0.68$. Therefore, an emotional expressiveness and background have a significant influence on the recognition accuracy.

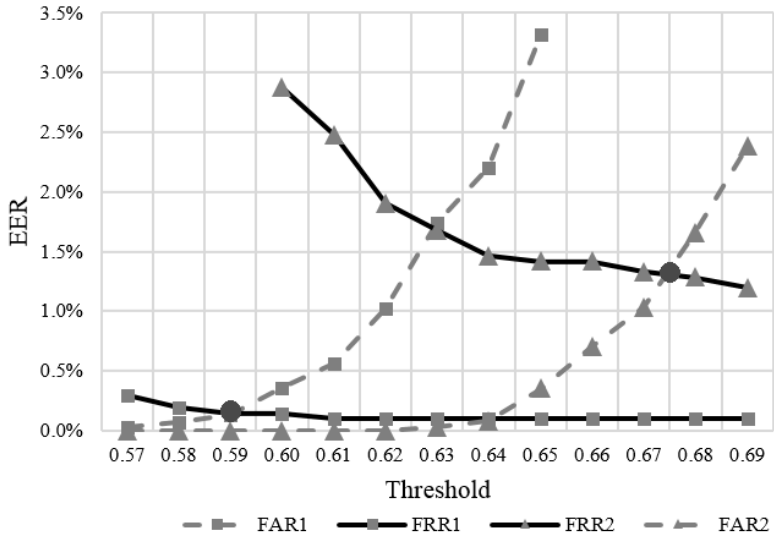

Fig. 2. Illustration of the ratio FAR to FRR for the first and second group videos (fragment). Intersection points are marked by a circle.

Now let's consider influence of resolution. All the video were consistently tested in the following resolutions: 240p, 360p (standard test), 480p, 720p. The results are shown in Fig. 3.

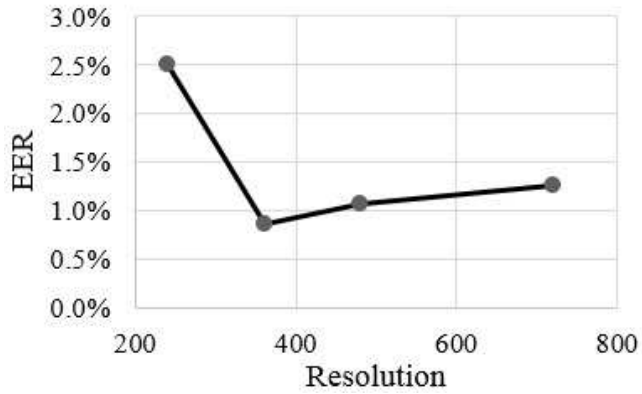

Fig. 3. The influence of different video resolution on EER. The minimum value = 0.87% for the standard test at 360 pixels, the maximum value = 2.5% at 240 pixels.

Testing demonstrates that the highest accuracy is achieved on the standard test at 360 pixels. With a strong reduction in resolution, the EER rises sharply to 2.5% at 240

pixels (this is due to low image clarity). However, when the resolution is increased, the EER also rises: to 1.10% at 480 pixels and 1.25% at 720 pixels.

The influence of illumination on recognition quality was tested. To simulate different illumination, all user's templates were taken with different brightness: -50%, -25%, 0% (standard test), +25%, +50%. The test results are shown in Fig. 4.

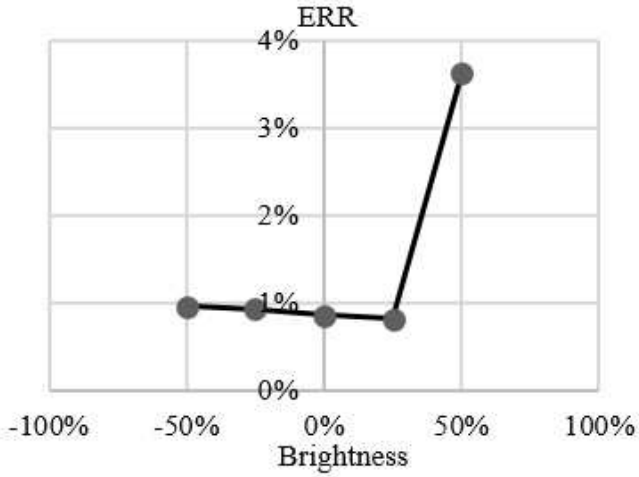

Fig. 4. The influence of different illumination level on EER. The minimum value = 0.86% with a brightness increase of 25%, the maximum value = 3.6% with a 50% increase. The dimming of templates had little effect on recognition quality.

Illumination negatively affects an accuracy only at high or very low intensity usually not used in reality [7]. Increasing the brightness by 25% reduced the EER to 0.86%, but it rises sharply to 3.6 at 50 percent. Therefore, The dimming had an insignificant effect on an EER - 0.92% with brightness of -25% and 0.96% with -50%. Therefore, lighter images are easier to recognize, but further brightening on the contrary reduces the accuracy.

3.3. Photo Classification

The standard vulnerability of any face recognition system is the possibility that an intruder can bypass the system protection by faking an image of a genuine user s face and showing it to a webcam (for example, using a photo). To protect against this, two different methods are considered.

Suppose that the intruder fixed the photo in front of the webcam for greater reliability. In this case, the difference between the face descriptors in different frames will tend to a minimum. The first method is based on this supposition. Euclidean distance between the previous and the current processed frame is calculated and compared with the constant $threshold_2$. If the distance is below $threshold_2$, then it is user's photo on image, not genuine user himself.

The second method is based on the differences in the movement of a real person and a photo in the frame. For its implementation, a convolutional neural network created with the Keras library was used. It includes three subsamples and convolution cascades. The convolutional part of the network is designed to highlight the characteristic features in the image. The convolutional part is followed by the fully connected part of the neural network, which is responsible for the classification. For this purpose, two fully connected

layers are used. The network was used for binary classification of the images. The first class is an images of the faces of living people, the second - an images of photos of people in front of a webcam.

To evaluate the accuracy of both methods, we used FAR and FRR. FAR is the probability that the system incorrectly recognizes the user's photo as his living face, and FRR is the probability of wrong recognizing of the legitimate user, but almost motionless user as his photograph. Testing was conducted using the camera "HDE 12 Megapixel". As a material for testing, 250 frames with 10 different live people and 250 frames with photos of 10 people in front of a webcam were taken.

The results for first method are shown in Fig. 5 (marked as FAR_1, FRR_1). EER of 3.5% is achieved at $threshold_2 = 0.1$. It should be noted that situations when a real user sits in the workplace almost motionless can occur very often. Therefore, we suggest to keep FRR higher than FAR, with a $threshold_2$ no more than 0.09, to avoid false recognition as a photograph.

Testing of the second classification method was conducted with the training sample of 500 frames for both classes. Figure 5 shows the test results of the second method (marked as FAR_2, FRR_2). $EER = 4.9\%$ is achieved with $threshold_2 = 0.11$.

Figure 5 demonstrates that FRR_1 is almost equal to FRR_2. Hovewer, FAR_1 value grows much faster than FAR_2.

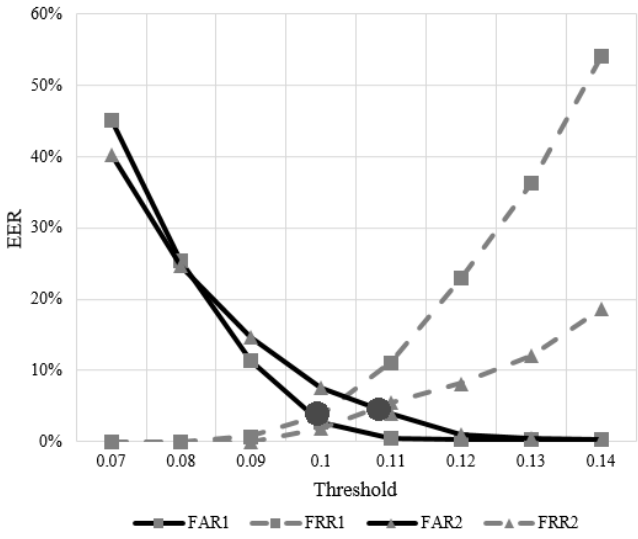

Fig. 5. Illustration of the ratio FAR to FRR for testing the photo recognition quality by the both methods (fragment). Intersection points are marked by a circle.

Testing was conducted with the training sample of up to 3000 different frames for both classes. Figure 6 shows the results of testing with its values of 500, 1000, 1500, 2000, 2500 and 3000 frames.

Increasing the size of the training sample improves accuracy. At 3000 frames, $EER = 1.3\%$ is achieved. It should be noted that the growth rate of accuracy decreases. Consequently, a further increase in the size of the training sample will have little impact on the growth of accuracy. A comparison of the two methods shows that with a sufficiently large size of the training sample, the second method demonstrates greater accuracy.

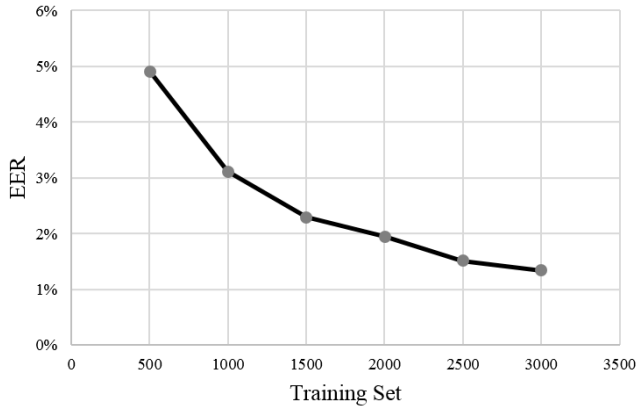

Fig. 6. The influence of different size of the training sample on EER. The minimum value = 1.3% with 3000 shots, the maximum value = 4.9% with 500 shots.

3.4. Total Accuracy

Let s consider the total accuracy of the system, taking into account the user recognition and the photo recognition. When processing a frame from a webcam or video, the following events may occur:

–image with the face of a legitimate user is on input (event A);

–image with the photo of a legitimate user is on input (event B);

–image with the face of an impostor is on input (event C).

The recognition system works according to the following algorithm. Firstly it recognizes the face for legitimacy, depending on the threshold t_1. If the result is greater than t_1, then the face is considered as an impostor, and access is denied (event D). Or it tries to recognize if the face is in the photo, depending on the threshold t_2. If the result is less than t_2, it is considered that the image is a photograph and the system denies access (event E). Or the user is considered to be alive and legitimate, and access is granted (event F).

Now let's determine the probability of a false reject of the system FRR_{total}. This is the probability of occurrence of any the events D or E, provided that event A occurred. Therefore, it is influented by the following events:

–The image contains the face of a legitimate user, the face is recognized as a user, recognized as a photograph (AE);

–The image contains the face of a legitimate user, the face is recognized as an impostor (AD).

Then FRR_{total} is calculated by

$$FRR_{total} = P(D|A) + P(E|A), \tag{3}$$

where

$$P(D|A) = (1 - FRR(t_1)) * FRR2(t_2), \tag{4}$$

$$P(E|A) = FRR(t_1). \tag{5}$$

Note that the a priori probability of event A (i.e. P(A)) does not affect FRR_{total}.

Now let s determine the probability of a false access of the system FAR_{total}. This is the probability of occurrence of the event F, provided that any of the events B or C occurred. Therefore, it is influented by the following events:

–The image contains the photo of a legitimate user, the face is recognized as a user, recognized as a living person (BF);

–The image contains the face of an impostor, the face is recognized as a user, recognized as a living person (CF).

Then FAR_{total} is calculated by

$$FAR_{total} = \frac{(P(F|B) * P(B) + P(F|C) * P(C))}{(P(B) + P(C))}, \tag{6}$$

where

$$P(F|B) = (1 - FRR(t_1)) * FAR_2(t_2), \tag{7}$$

$$P(F|C) = FAR(t_1) * (1 - FRR_2(t_2)), \tag{8}$$

$P(B)$, $P(C)$ are the a priori probabilities of occurrence of the events B and C, respectively.

We didn't find any examples in which the system would be wrong at recognition of the presence or the absence of a person. Therefore, FAR_0 and FRR_0 were taken as 0.1%. With this in mind, we walked through all the values of t_1 and t_2 and achieved the optimal values of $FAR_{total} = 1.02\%$ and $FRR_{total} = 1.06\%$ at $t_1 = 0.63$ and $t_2 = 0.1$.

3.5. Performance Testing

Performance testing was conducted on a PC with 8 GB of RAM and an Intel Core i5-3570K 3.40 GHz processor with 4 cores. The load was distributed to one core. There was a video with 11 minutes duration at different resolutions.

Let s consider the change in the average duration of the recognition procedure at different resolutions of the video. The time increases almost linearly, from half a second at 240 pixels, to 0.66 seconds at 360 pixels and to 1.28 seconds at 720 pixels. Consequently, a larger resolution adversely affects the duration.

Testing the average CPU usage and the effect of different resolutions was conducted. This indicator also demonstrates a practically linear increase at resolution change: from 22.7% at 240 pixels to 71.6% at 720 pixels.

Testing the RAM usage showed that different resolutions have little effect on this indicator. The system uses at least 230 MB at startup. Subsequently, the usage grows on average to 285 MB (290 MB limit) when processing video with 720 pixels.

Figure 7 shows the relative change in all three indicators. Their value with 360 pixels was taken as 100%.

When analyzing the results of testing the RAM and CPU usage, it should be taken into account that only the usage with time interval on which a recognition procedure occurs is considered. The time interval between them is not considered.

Performance and recognition time using both photo classification methods are approximately the same. The execution time of the first method is approximately 0.3 seconds, the execution time of the second method is approximately 0.5 seconds.

The results of performance testing showed that the use of the system on smartphones is unreasonable because of the high load on the processor, and as consequence, large energy losses. The most suitable types of mobile devices are laptops and tablets.

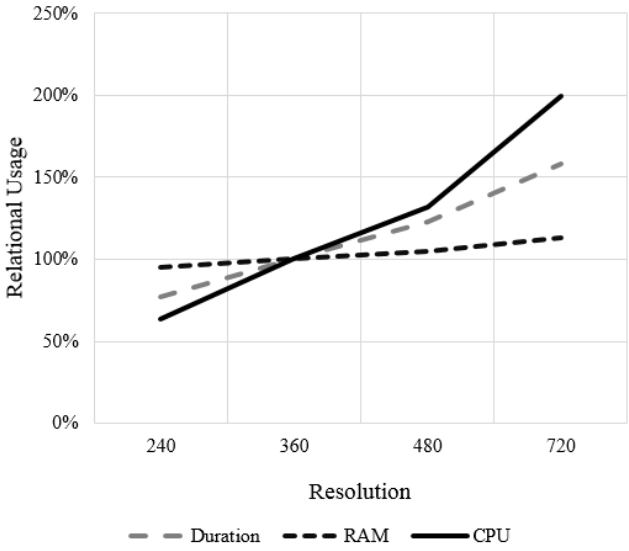

Fig. 7. The relative change in CPU usage, RAM usage and average duration of the recognition procedure at different video resolution.

4. Conclusions and Future Work

We developed a system of continuous authentication through two-dimensional recognition of face geometry using a standard webcam. This system was tested on video from different bloggers. It was found that different video resolution affects an accuracy, duration of a recognition procedure, RAM and CPU usage. The best accuracy expressed through the Equal Error Rate is equal to 0.86% and it is achieved for video with a resolution of 360p, with an increase in the user's templates brightness by 25%.

The ability of the system to distinguish a user's real face from his photo by two different methods was developed and tested. EER of the first method is equal to 3.5%. EER of the second method is up to 1.4%.

In future, we plan to optimize the system as a whole to reduce its resource requirements for widespread use on mobile devices.

The research was supported by Act 211 of the Government of the Russian Federation, contract 02.A03.21.0011.

References

1. Rajkumar J., Kumar S., Zhang S., Sim T. Using Continuous Face Verification to Improve Desktop Security. *Seventh IEEE Workshops on "Applications of Computer Vision" (WACV/MOTION'05), Vol. 1*, IEEE, 2005, pp. 501–507. DOI: 10.1109/ACVMOT.2005.120

2. Feng T., Zhao X., Carbunar B. Continuous Mobile Authentication Using Virtual Key Typing Biometrics. *12th IEEE International Conference on "Trust, Security and Privacy in Computing and Communications" (TrustCom)*, IEEE, 2013, pp. 1547–1552. DOI: 10.1109/TrustCom.2013.272

3. Feng T., Liu Z., Kwon K. A., Shi W., Carbunar B., Jiang Y., Nguyen N.

Continuous Mobile Authentication Using Touchscreen Gestures. *IEEE Conference on Technologies for "Homeland Security" (HST)*, IEEE, 2012, pp. 451–456. DOI: 10.1109/THS.2012.6459891

4. Mondal S., Bours P. Continuous Authentication Using Mouse Dynamics. *International Conference for the "Biometrics Special Interest Group" (BIOSIG)*, IEEE, 2013, pp. 1–12.
5. Donida L. R., Sassi R., Scotti F. ECG Biometric Recognition: Permanence Analysis of QRS Signals for 24 Hours Continuous Authentication. *IEEE International Workshop on "Information Forensics and Security" (WIFS)*, IEEE, 2013, pp. 31–36. DOI: 10.1109/WIFS.2013.6707790
6. Lin F., Song C., Zhuang Y., Xu W., Li C., Ren K. Cardiac Scan: a Non-Contact and Continuous Heart-Based User Authentication System. *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*, 2017, ACM, pp. 315–328.
7. Mahbub U., Patel V. M., Chandra D., Barbello B., Chellappa R. Partial Face Detection for Continuous Authentication. *IEEE International Conference on "Image Processing" (ICIP)*, IEEE, 2016 , pp. 2991–2995. DOI: 10.1109/ICIP.2016.7532908
8. Pamplona Segundo M., Sarkar S., Goldgof D., Silva L., Bellon O. Continuous 3D Face Authentication Using RGB-D Cameras. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, 2013, pp. 64–69. DOI: 10.1109/CVPRW.2013.17
9. Kazemi V., Sullivan J. One Millisecond Face Alignment with an Ensemble of Regression Trees. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2014, pp. 1867–1874. DOI: 10.13140/2.1.1212.2243
10. Gupta S., Markey M. K., Bovik A.C. Advances and Challenges in 3D and 2D+ 3D Human Face Recognition. *Pattern Recognition in Biology*, 2007, pp. 63–103.
11. Mills E., Borg N. Trends in Recommended Illuminance Levels: an International Comparison. *Journal of the Illuminating Engineering Society*, 1999, vol. 28, no. 1, pp. 155–163. DOI: 10.1080/00994480.1999.10748262
12. Kaiming H., Xiangyu Zh., Shaoqing R., Sun J. Deep Residual Learning for Image Recognition. *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2016, pp. 770–778. DOI: 10.1109/CVPR.2016.90

Anton A. Kudinov, Bachelor, Department of Applied Mathematics and Programming, South Ural State University (Chelyabinsk, Russian Federation), neverdark74@gmail.com

Sergey M. Elsakov, PhD (Math), Department of Applied Mathematics and Programming, South Ural State University (Chelyabinsk, Russian Federation), elsakovsm@susu.ru

Received March 3, 2019

УДК 004.93'1 DOI: 10.14529/jcem190103

УЛУЧШЕННАЯ СИСТЕМА НЕПРЕРЫВНОЙ АУТЕНТИФИКАЦИИ С ПОМОЩЬЮ ЗАЩИТЫ ОТ ПОДДЕЛОК

А. А. Кудинов, С. М. Елсаков

В статье рассматривается возможность повышения безопасности рабочих мест пользователей, оснащенных веб-камерами. Это достигается за счет реализации непрерывной аутентификации пользователя с помощью распознавания лица. Этот метод значительно повышает уровень защищенности системы от угрозы завладения доступом, пока пользователь покинул рабочее место. Кроме того, были разработаны различные методы защиты системы от имитации образа подлинного пользователя. Выполнено тестирование различных подходов к решению задачи, и получены оценки надежности соответствующей системы.

Ключевые слова: аутентификация; распознование лиц; веб-камера; распознование фотографий; библиотека Dlib.

Литература

1. Radjkumar, J. Using Continuous Face Verification to Improve Desktop Security / J. Radjkumar, S. Kumar, S. Zhang, T. Sim // Seventh IEEE Workshops on "Applications of Computer Vision" (WACV/MOTION'05), vol. 1. – 2005. – P. 501–507.

2. Feng, T. Continuous Mobile Authentication Using Virtual Key Typing Biometrics / T. Feng, X. Zhao, B. Carbunar // 12th IEEE International Conference on "Trust, Security and Srivacy in Computing and Communications" (TrustCom). – 2013. – P. 1547–1552.

3. Feng, T. Continuous Mobile Authentication Using Touchscreen Gestures / T. Feng, Z. Liu, K. A. Kwon, B. Carbunar, Y. Jiang, N. Nguyen // IEEE Conference on Technologies for "Homeland Security" (HST). – 2012. – P. 451–456.

4. Mondal, S. Continuous Authentication Using Mouse Dynamics / S. Mondal, P. Bours // International Conference for the "Biometrics Special Interest Group" (BIOSIG). – 2013. – P. 1–12.

5. Donida, L. R. ECG Biometric Recognition: Permanence Analysis of QRS Signals for 24 Hours Continuous Authentication / L. R. Donida, R. Sassi, F. Scotti // IEEE International Workshop on "Information Forensics and Security" (WIFS). – 2013. – P. 31–36.

6. Lin, F. Cardiac Scan: a Non-Contact and Continuous Heart-Based User Authentication System / F. Lin, C. Song, Y. Zhuang, W. Xu, C. Li, K. Ren // Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking. – 2017. – P. 315–328.

7. Mahbub, U. Partial Face Detection for Continuous Authentication / U. Mahbub, V. M. Patel, D. Chandra, B. Barbello, R. Chellappa // IEEE International Conference on "Image Processing" (ICIP). – 2016. – P. 2991–2995.

8. Pamplona Segundo, M. Continuous 3D Face Authentication Using RGB-D Cameras / M. Pamplona Segundo, S. Sarkar, D. Goldgof, L. Silva, O. Bellon // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops. – 2013. – P. 64–69.

9. Kazemi, V. One Millisecond Face Alignment with an Ensemble of Regression Trees / V. Kazemi, J. Sullivan // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. – 2014. – P. 1867–1874.

10. Gupta, S. Advances and Challenges in 3D and 2D+ 3D Human Face Recognition / S. Gupta, M. K. Markey, A. C. Bovik // Pattern Recognition in Biology. – 2007. – P. 63–103.

11. Mills, E. Trends in Recommended Illuminance Levels: an International Comparison / E. Mills, N. Borg // Journal of the Illuminating Engineering Society. – 1999. – V. 1, № 28. – P. 155–163.

12. Kaiming, H. Deep Residual Learning for Image Recognition / H. Kalming, Zh. Xiangyu, R. Shaiging, J. Sun // The IEEE Conference on Computer Vision and Pattern Recognition (CVPR). – 2016. – P. 770–778.

Кудинов Антон Александрович, бакалавр, кафедра прикладной математики и программирования, Южно-Уральский государственный университет (Челябинск, Российская Федерация), neverdark74@gmail.com.

Елсаков Сергей Михайлович, кандидат физико-математических наук, доцент, кафедра прикладной математики и программирования, Южно-Уральский государственный университет (Челябинск, Российская Федерация), elsakovsm@susu.ru.

Received 3 марта 2019 г.