user verification,
keystroke dynamics,
finger-knuckle analysis

Tomasz Emanuel WESOLOWSKI[1], Hossein SAFAVERDI[1],
Rafal DOROZ[1], Krzysztof WROBEL[1]

HYBRID VERIFICATION METHOD BASED ON FINGER-KNUCKLE ANALYSIS AND KEYSTROKE DYNAMICS

The increasing number of personal data leaks becomes one of the most important security issues hence the need to develop modern computer user verification methods. In the article, a potential of biometric methods fusion for continuous user verification was assessed. A hybrid approach for user verification based on fusion of keystroke dynamics and knuckle images analysis was presented. Verification is performed by a classification module where an ensemble classifier was used to verify the identity of a user. A proposed classifier works on a database which comprises of knuckle images and keyboard events for keystroke dynamics. The proposed approach was tested experimentally. The obtained results confirm that the proposed hybrid approach performs better than methods based on single biometric feature hence the introduced method can be used for increasing a protection level of computer resources against forgers and impostors. The paper presents results of preliminary research conducted to assess the potential of biometric methods fusion.

1. INTRODUCTION

In the world dominated by electronically stored personal data the protection of sensitive information by increasing computer systems security is a crucial task. Comparing, for example, the years 2014 and 2015 the number of individuals affected by security breaches, where sensitive medical personal information was stolen increased hundred times [19]. Because of the accessibility to digital communication and devices the number of attacks is increasing year by year and the cyber attacks themselves are becoming more and more sophisticated. Therefore the need to develop innovative counterattack strategies [14]. Aside the various kinds of digital attacks that can be performed outside of the attacked computer system a major of cyber intrusions consists of insider attacks [15]. For this reason novel security measures are highly required. Because the main goal of biometrics is the automatic recognition of individuals based on the knowledge of their characteristics, biometric methods are commonly used in computer security systems because of their high effectiveness.

Modern security measures use biometric methods to prevent not legitimate users to access computer system resources - in particular sensitive private data. These methods can be based on

[1] University of Silesia, Institute of Computer Science, ul. Bedzinska 39, 41-200 Sosnowiec, Poland,
e-mail: {tomasz.wesolowski, hossein.safaverdi, rafal.doroz, krzysztof.wrobel}@us.edu.pl

physical (eg. fingerprints) or behavioral characteristics of computer users. Behavioral biometric methods use, among other things, an analysis of the movements of various manipulators (eg. a computer mouse [16]) or the dynamics of typing on a computer keyboard (keystroke dynamics) [1]. An analysis of keystroke dynamics involves detection of a rhythm and habits of a computer user while typing on a keyboard [22]. Such an analysis results in creating user's biometric profile used than in the authorization systems. The proposed approach allows an automatic and continuous registration of user's activity connected to a keyboard. The activity registration process is performed in the background, without additionally involving a user - it is transparent to the computer user. Keystroke events are captured on the fly and saved in text files in a real-time. Based on these logs keystroke dynamics analysis is performed in order to verify an active user's access permissions. The big advantage of the proposed method is that user verification can be performed continuously on the fly. In the proposed approach a keystroke dynamics analysis constitutes only the first stage of computer user verification. To increase a protection level a hybrid computer user verification method is proposed. This hybrid solution combines two biometric methods: the keystroke dynamics analysis with finger knuckle pattern recognition. For the second stage of user verification knuckle image acquisition is performed using a dedicated device especially designed for this purpose [3].

After the biometric data acquisition an intrusion detection can be performed in various ways - for example, it can be based on a fuzzy approach [6]. However more frequently the literature sources indicate solutions based on classification methods. The intrusion detection proposed in this paper is based on classification module where ensembles of classifiers are used to classify features derived from keystroke analysis unit and a single classifier approach is used in combination with knuckle pattern analysis unit.

The main objective of the conducted research was to verify if a hybrid computer user verification method consisting of two biometric methods would perform better than the single components of the verification system. According to study assumptions the hybrid approach should allow the real-time verification. However a method of analyzing the finger knuckle on the fly has not been developed yet as it needs a lot of resources to analyze the images in a real-time. Therefore, before the decision to invest time and resources into developing such a method was made it was necessary to verify if the fusion of keystroke dynamics and finger knuckle analysis is potentially interesting. For this reason the preliminary research was conducted to assess the potential of the presented methods fusion. The paper presents the preliminary results of an intruder detection system based on the introduced novel approach.

2. PROPOSED HYBRID VERIFICATION METHOD

The innovation of the proposed solution is the fusion of finger knuckle pattern analysis and keystroke dynamics for user verification. The proposed hybrid user verification approach consists of legitimate user profiling (system preparation phase) and of active user verification. The first step of user profiling consists of recording a legitimate user's activity while working with a keyboard and of acquiring this user's finger knuckle images. Next, the acquired data is processed to designate user's profile that can be used for verification of an active user in the second phase. The introduced user verification model shown in Fig. 1 connects the two biometric methods of user verification: keystroke dynamics and knuckle analysis. For the purpose of the presented research the biometric user verification methods that perform better than other methods described in literature were chosen: for keystroke based approach [17] and for finger knuckle pattern analysis [3].

One of the objectives of the presented study is that activity of a user working at the time in a computer system should be verified continuously, in the background, while a user is performing

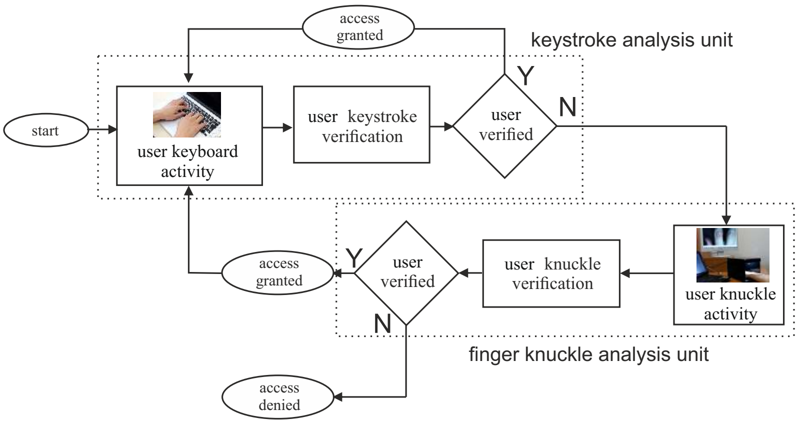

Fig. 1. The proposed hybrid biometric user verification model

his everyday tasks. To allow this, all keyboard events generated by the user are recorded and time dependencies between them are analyzed. The keystroke dynamics based verification unit uses the previously designated profiles of legitimate users and a recorded activity of an at the moment active user and establishes a decision if the activity belongs to a legitimate user. After a successful verification an access is granted and the verification procedure continues. If the verification was not successful a suspicion that an active user is an intruder occurs. Therefore an additional verification is made by the knuckle pattern verification unit after taking a picture of the user's finger knuckles. Again, after a successful verification an access is granted and the verification procedure continues with the keystroke based verification. If the verification here also has not been successful an access to resources is denied and the security breach alert is generated.

3. KEYSTROKE ANALYSIS UNIT

A computer user activity should be verified continuously so all keyboard events generated by the user are recorded in the background, while a user is performing everyday tasks. In the proposed method a profile of a user is constituted of time dependencies that occur between the key events. The profiling is performed continuously in the background, it is practically transparent for a user. This is a very important advantage of the proposed method and for this reason it can be used in Host-based Intrusion Detection Systems (HIDS) that either analyze the logs with registered user activity in the off-line mode or in a real-time mode to detect an unauthorized access. The keyboard events are captured on the fly. A set of data representing a single keyboard event can be presented in a form of a vector $\mathbf{e} = [prefix, t, id]$ that consists of a $prefix$ describing the type of an event (key up or key down), followed by the time-stamp t of this event and an identifier id of a key that generated the event. Activity data analysis is carried out separately for each user identified in the system by a user identifier uid. All vectors $\mathbf{e}$ of the user uid constitute a dataset of this user's activity. A dataset in this form does not provide directly information on how a user interacts with a computer system when using a keyboard and for this reason its interpretation is difficult. Therefore it is necessary to process the recorded data, for example, by extracting time dependencies between keyboard events. Such an extraction allows to obtain characteristics of a user in a form of a profile.

In the presented study the profiling method indicated as very efficient by the literature sources [16], [18], [17] was used. The profiling phase denotes for each user identified by uid a profile Θ^{uid} consisting of feature vectors $\Theta^{uid} = \left\{\mathbf{F}_1^{uid}, \mathbf{F}_2^{uid}, ..., \mathbf{F}_z^{uid}\right\}$ characterizing user's uid activity. The previously obtained profiles allow to perform a verification of a user currently active in a computer system based on his/her activity at the moment.

3.1. Keystroke dynamics based verification

A verification of an active user consists in assigning a user to one of two possible classes: a legitimate user or an intruder basing on the analysis of a legitimate user's profile and an activity of a user working at the moment in the computer system. A classifier Υ maps the feature vector $\mathbf{F}$ of an active at the moment user to a class label c_j, where $j \in \{1, 2\}$:

$$\Upsilon(\mathbf{F}) \rightarrow c_j \in C. \tag{1}$$

The assumption of the presented method is that a classifier Υ returns a probability $\hat{p}(c_j|\mathbf{F})$, $j \in \{1, 2\}$ that a given object - in this case vector $\mathbf{F}$ - belongs to a class c_j.

Based on the research presented in [4], [17] the keystroke verification module used in this study was built using ensembles of classifiers EC_a. Each of the ensembles EC_a consists of four single classifiers $\Upsilon^{(i)}$, where $i \in \{1..4\}$. The structure of a single ensemble of classifiers is shown in Fig. 2. The studies described in [4], [17] indicate a use of three ensembles EC_a, $a = 1, ..., 3$ in a verification module as an optimal selection for a verification system based on keystroke dynamics. The ensembles of classifiers EC_a work simultaneously and each of them is trained using a separate training set TS_a. At the input of each node Λ_a (Fig. 2) as a result of ensembles of classifiers $\Upsilon^{(i)}$ the following data matrix is introduced:

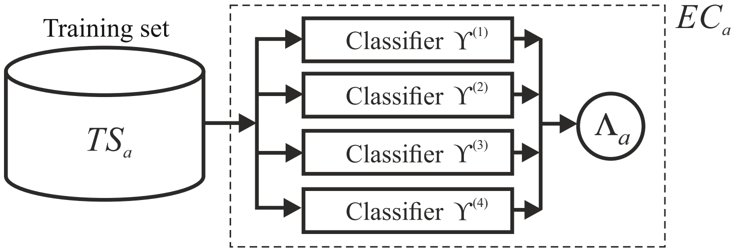
Training set
TS_a
Classifier $\Upsilon^{(1)}$
Classifier $\Upsilon^{(2)}$
Classifier $\Upsilon^{(3)}$
Classifier $\Upsilon^{(4)}$
Λ_a
EC_a

Fig. 2. The structure of a single ensemble of classifiers EC_a

$$\text{Input}\Lambda_a(\mathbf{F}) = \begin{bmatrix} \hat{p}_1(c_1|\mathbf{F}) & \hat{p}_1(c_2|\mathbf{F}) \\ \hat{p}_2(c_1|\mathbf{F}) & \hat{p}_2(c_2|\mathbf{F}) \\ \hat{p}_3(c_1|\mathbf{F}) & \hat{p}_3(c_2|\mathbf{F}) \\ \hat{p}_4(c_1|\mathbf{F}) & \hat{p}_4(c_2|\mathbf{F}) \end{bmatrix}. \tag{2}$$

Following the classification, each ensemble of classifiers EC_a, $a = 1, .., 3$ generates a local decision Λ_a according to the soft voting formula 3:

$$\Lambda_a(\mathbf{F}) = \arg\max_{c_j \in C} \sum_{i=1}^{4} \hat{p}_i(c_j|\mathbf{F}), \quad a = 1, ..., 3. \tag{3}$$

Next the class labels designated by (3) are being converted to the numerical values according to the rules (4).

$$\Gamma_a(\mathbf{F}) = \begin{cases} -1 \text{ if } \Lambda_a(\mathbf{F}) = c_1 \\ +1 \text{ if } \Lambda_a(\mathbf{F}) = c_2 \end{cases}, \quad a = 1, ..., 3. \tag{4}$$

Based on the converted local decisions $\Gamma_a(\mathbf{F})$ designated in each of the ensemble of classifiers EC_a a value of LS is determined as follows:

$$LS(\mathbf{F}) = \sum_{a=1}^{3} \Gamma_a(\mathbf{F}). \tag{5}$$

The value of $LS(\mathbf{F})$ allows to determine the decision of keystroke dynamics based verification. The value greater than a threshold ϑ indicates that an activity of a verified user is compatible with a legitimate user's profile. In this case the verified user is allowed to keep working and the process of keystroke dynamics based verification is repeated continuously. Otherwise the user must proceed to knuckle based verification phase.

4. FINGER KNUCKLE ANALYSIS UNIT

The reasons behind using finger knuckle print to recognize individuals are as follows:

- Finger knuckle biometric trait contains a discriminative texture patterns which are easily acquirable by means of only a camera.
- Finger knuckle print has a high rate of user acceptance because it is a contact less image acquisition method and the temporary states of user gesture and emotion do not effect on it.
- Finger knuckle print could be simply used in both, single-modal and multi-modal biometric systems.

After image acquisition, a process of extracting the furrows from the finger knuckle images starts. This task is done by utilizing image processing methods. The furrows obtained from the finger knuckle images are unique for each individual and could be considered as a new set of biometric features. A sample of furrows obtained from a finger knuckle is shown in Fig. 3.

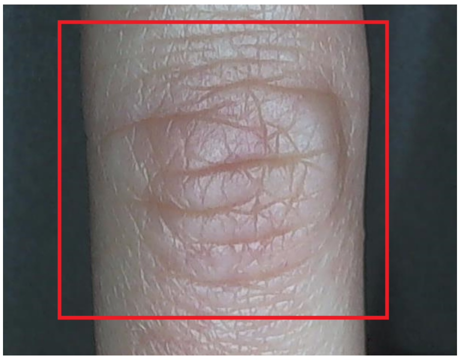

Fig. 3. Pattern of knuckle image

So far many papers covered the finger knuckle print (FKP) analysis topic and published results. Work [5] have classified the extracted features from finger knuckle images by means of Hidden Markov Models (HMM) and Support Vector Machine (SVM). In [8] authors proposed to represent finger knuckle image using a code system. The Principal Component Analysis (PCA), Radon transformation, Linear Discriminant Analysis (LDA) and Independent Component Analysis (ICA) were used to extract and classify the code system. Other studies used various techniques such as surface curvature analysis [10], Gabor filter [21], Scale-Invariant Feature Transform (SIFT) method [7] and texture analysis to recognize the individual by means of finger knuckle images. The proposed method consists of three main steps. In the first step, a special device for finger knuckle image acquisition is used. Next, the patterns from previously acquired finger knuckle images are extracted. Last step compares the knuckle images using Least Square Contour Alignment (LSCA).

4.1. FINGER KNUCKLE IMAGE ACQUISITION PROCESS

As mentioned in the previous section, for acquisition of the finger knuckle images only a digital camera is needed. We set-up a camera in a confined box and aligned the light inside it. Three LEDs are installed in different places of the box. The camera is programed to focus on the index finger and take picture of it when the finger is still and fixed in the right place. Fig. 4 shows the device in use.

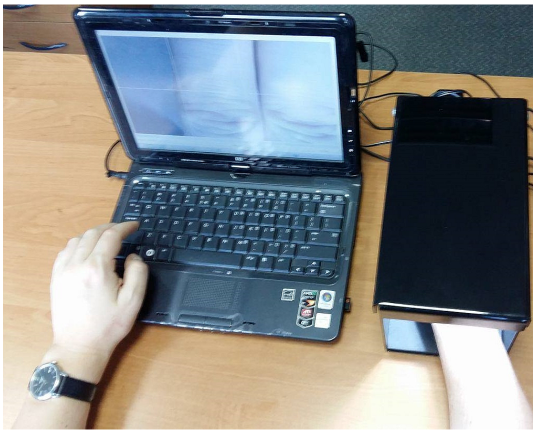

Fig. 4. Image acquisition process

4.2. PATTERN EXTRACTION

Before denoting a pattern for a finger knuckle image the furrows of a knuckle should be extracted. We accomplished this task by using Hessian filter technique [2]. This filter allows to find the edges of the knuckle images. After this step we applied the Otsu method for binarization [11]. One of the biggest advantages of this method is that it automatically finds the optimum threshold in binarization process. The following step is a line thinning process applied to reduce the thickness of the extracted lines (furrows) to one pixel. Here the Pavlidis's thinning algorithm [12] was applied to accomplish this task.

Next, furrows obtained from the thinning process are converted into chains of points. To make these chains of points we have to determine the ends and bifurcations points of the furrows on the image. To localize these points we applied a 3×3 mask on every pixel of the image. We assigned value of one for each black pixel and zero for white pixels. Then for each black pixel the *J* value was determined as follows:

$$\begin{gathered} J(x,y) = \sum_{a=-1}^{1} \sum_{b=-1}^{1} I(x+a, y+b), \\ x \in [2, ..., W-1], y \in [2, ..., H-1], \end{gathered} \tag{6}$$

where (*x*, *y*) are coordinates of an analyzed pixel, *W* and *H* are the width and height of the image *I*. According to the value *J*, labels p^T (end of the furrow) or p^B (bifurcation on the furrow) are assigned to each analyzed pixel:

$$p(x,y) = \begin{cases} p^T(x,y) & \text{if} \quad J(x,y) = 2 \\ p^B(x,y) & \text{if} \quad J(x,y) > 3 \end{cases} . \tag{7}$$

The image can contain more than one end and bifurcation points, hence we indexed them as p^{T_i} and p^{B_j}, where i and j show the number of ends and bifurcations. After finding and labeling the end and bifurcation points, we applied Algorithm 1 on each image in the database to generate a set $C = \{c_1, ...\}$ which includes all the chains found from the image being analyzed. Each i-th chain c_i consists of points (x, y) forming the i-th furrow.

Algorithm 1: Procedure of extracting the chains of points from the knuckle image.

```
Data: Thinned knuckle image. List of the image points with labels $W = \{p^{T_1}, p^{T_2}, ..., p^{B_1}, p^{B_2}, ...\}$.
Result: Set of chains of the points $C = \{c_1, ...\}$, where each chain $c_i$ has starting and ending points with any type
        label ($p^T$ or $p^B$).
$i$ = 1;
foreach labeled point $p \in W$ do
    add coordinates of the point $p \in W$ to the chain $c_i$;
    do
        move the analyzed point from the point $p$ to the neighbor black pixel $p^*$ which not belongs to any chain from
          the list $C$;
        add point $p^*$ to the chain $c_i$;
        set analyzed point $p = p^*$;
    while the analyzed point $p \notin W$;
    $i = i + 1$;
```

4.3. KNUCKLE BASED VERIFICATION

Verification process starts by determining the similarity values between two images: reference image I^a from database and test image I^b. Algorithm 1 was used, to generate two sets $C^a = \{c_i^a\}_{i=1,...,n}$ and $C^b = \{c_i^b\}_{i=1,...,m}$ describing images being compared. In our investigations comparing between two knuckle images has been done by means of Least Square Contour Alignment (LSCA) method. Before comparison, we must center the coordinates of all chains of points:

$$\underset{i=1,...,n}{\forall} c_i^a \in C^a, c_i^a = c_i^a - \frac{\sum_{j=1}^{n} c_j^a}{n}, \tag{8}$$

$$\underset{i=1,...,m}{\forall} c_i^b \in C^b, c_i^b = c_i^b - \frac{\sum_{j=1}^{m} c_j^b}{m}. \tag{9}$$

Following formula is used in LSCA to compare two chains of points c_i^a and c_j^b:

$$d(c_i^a, c_j^b) = \min_{t \in \mathbb{R}^2, \theta \in [-\pi, \pi), k > 0} \left\| c_i^a - \Omega_{t,\theta,k}(c_j^b) \right\|_F, \tag{10}$$

where:
$\Omega_{t,\theta,k}$ – is the operator of translation by the vector $t \in \mathbb{R}^2$, rotation by the angle $\theta \in [-\pi, \pi)$, and scaling by the factor $k > 0$,
$\|M\|_F$ – denotes the Frobenius norm of the matrix M.

One of the main conditions in LSCA method that needs to be satisfied is that data being compared must have the same number of elements. In our case this condition is not always delivered because of different furrow's sizes on the knuckle images. Therefore to overcome this problem we have applied a scaling method, so called Fixed Number of Points (FNP) to equalized the size of furrows being compared. This method and LSCA were described in [13] and [9]. Comparison of all furrows in two generated sets C^a and C^b is done by means of following formula:

$$d'(C^a, C^b) = \frac{1}{n}\sum_{i=1}^{n} \min\big(d(c_i^a, c_1^b), ..., d(c_i^a, c_m^b)\big), \tag{11}$$

where $C^a = \{c_1^a, c_2^a, ..., c_n^a\}$ and $C^b = \{c_1^b, c_2^b, ..., c_m^b\}$.

The coefficient in this formula (11) is not symmetrical therefore to finalize the comparison stage we applied the following formula:

$$d''(C^a, C^b) = \min(d'(C^a, C^b), d'(C^b, C^a)). \tag{12}$$

In this stage an unknown person provides a knuckle image C^v and claims for identity. To acquire his/her identity information the system goes over to all N images stored in our database for this user/person and compare them with C^v. As a consequence of comparisons we obtain a set ψ. Structure of this set is shown in below:

$$\psi = \{d''(C^v, C_1^a), d''(C^v, C_2^a), ..., d''(C^v, C_N^a)\}, \tag{13}$$

where C_i^a is the i-th knuckle image belonging to the person being verified, N is a number of all knuckle images in the database of the person being verified.

Next, C^v is compared with some randomly chosen images from another users in our database. The results of this comparison are stored in set δ:

$$\delta = \{d''(C^v, C_1^b), d''(C^v, C_2^b), ..., d''(C^v, C_N^b)\}, \tag{14}$$

where C_i^b is the i-th knuckle image which belongs to any person from the database, but not the person being verified.

After generating sets ψ, δ we calculate the mean values for each of these two sets as follows:

$$\bar{\psi} = mean\{\psi\}, \;\; \bar{\delta} = mean\{\delta\}. \tag{15}$$

The ultimate decision Dec of user verification depends on values of sets $\bar{\psi}$ and $\bar{\delta}$:

$$Dec = \begin{cases} \text{genuine knuckle} & \text{if} \quad \bar{\psi} < \bar{\delta} \\ \text{forged knuckle} & \text{otherwise} \end{cases} . \tag{16}$$

5. Fusion of the methods

Proposed system consists of fusion of two biometric methods, keystroke dynamics and finger knuckle patterns, therefore the final decision of the verification module depends on both methods. First stage in our fusion method is keystroke dynamics based verification. If the user passes this stage successfully, his/her access to the system is granted but if the user's activity is rejected in the first stage then the user has to provide an image of his/her finger knuckle prints. Then the provided image will be compared with N images of the legitimate user's knuckles stored in a database. The formula describing how the final decision of the proposed hybrid verification method is presented below:

$$Final\ decision = \begin{cases} \text{access granted} & \text{if} \quad (LS \geqslant \vartheta) \\ \text{access granted} & \text{if} \quad (LS < \vartheta) \text{ and } (\bar{\psi} < \bar{\delta}) \\ \text{access denied} & \text{otherwise} \end{cases} . \tag{17}$$

6. RESULTS

The database used in this study consists of 4000 vectors **F** representing keystroke dynamics and 150 finger knuckle images collected from 30 people. Keystroke dynamics based verification was based on three ensembles of classifiers consisting of four classifiers each: c4.5, Bayesian Network, Random Forest and Support Vector Machine. Chosen classifiers had the highest accuracy in the investigations [19]. During our experiments, different values have been assigned to the parameter ϑ. The results show that the best value for this parameter is equal to $\vartheta = 3$.

In finger knuckle analysis unit, the influence of two parameters have been tested:

- parameter N - number of knuckle images in the database taken from each person being verified, see eq. (13) and (14),
- parameter FNP - length (number of points) of the furrows being compared.

During the comparison of two furrows with different lengths those lengths are being normalized according to FNP value. The $FNP = 25$ means that after the normalization the lengths of two furrows will be equal to 25 pixels. The $shorterfurrow$ means that the length of the furrows has been normalized to the length of the shorter furrow, and accordingly for $longerfurrow$ it has been normalized to the length of the longer one.

Optimal values obtained for parameters N and FNP are as follows: $N = 2$ and $FNP = 25$ (see Table 1) [20].

Table 1. Selection of optimal parameters for knuckle analysis unit.

N	FNP				
	25	50	75	*shorter furrow*	*longer furrow*
1	91.45±0.50	91.75±0.33	90.68±0.77	89.26±0.36	89.80±0.92
2	**92.77±0.33**	91.52±0.25	91.59±0.69	89.16±0.40	89.55±0.38
3	92.37±0.14	91.71±0.19	91.65±0.38	88.95±0.58	89.38±0.14
4	91.70±0.30	91.48±0.32	91.82±0.25	88.92±0.24	89.41±0.25
5	92.23±0.07	91.94±0.13	92.04±0.19	89.25±0.08	88.76±0.49
6	91.81±0.18	91.75±0.07	91.99±0.07	89.38±0.12	89.26±0.23
7	91.72±0.15	91.95±0.06	91.99±0.20	89.41±0.17	89.15±0.11
8	92.19±0.06	91.94±0.10	91.84±0.08	89.19±0.05	88.72±0.15
9	91.98±0.19	91.87±0.10	91.99±0.04	89.30±0.08	88.99±0.21
10	91.95±0.06	91.93±0.09	91.89±0.06	89.39±0.03	89.23±0.14

In order to provide a better statistical accuracy the results obtained by the proposed verification system have been verified in the 10-fold cross-validation tests, so the average values of the evaluation metrics for all trials were calculated.

The results of the tests carried out during the research are presented in Table 2.

Table 2. Results of the experiments.

Methods	Accuracy [%]
Keystroke	97.83 ± 3.28
Knuckle	92.77 ± 0.33
Keystroke+Knuckle	98.71 ± 0.92

By analyzing Table 2, we can notice that the fusion of two methods allows to obtain better efficiency in classification than using only the knuckle analysis. In case of keystroke analysis the difference of accuracy is not significant.

7. Conclusions

The study demonstrated that a hybrid computer user verification method that consists of two biometric features gives promising results that are better than using only one feature. However, the fusion of two biometric features makes the system to work slower due to the lots of calculations and comparison between the images. The approach presented in this paper improved the system performance in comparison to previous trials and reduced the calculation time. In the future study we will focus our investigation on developing a method that will be based on a real-time finger knuckle analysis. This new method will monitor users finger knuckles while moving over a keyboard. However this task is complicated and difficult to achieve due to the constant movement of hands over the keyboard and consequently different angle and position of finger knuckle. Having the different images and different finger positions cause some problems in user identification or verification mode. Therefore, one of the main objectives of the following research will be an optimization of the method and accurate localization of finger knuckles while over a keyboard.

Bibliography

[1] Banerjee S., Woodard D. Biometric authentication and identification using keystroke dynamic: a survey. Journal of Pattern Recognition Research, 2012, Vol. 7. pp. 116–139.

[2] Choon-Ching N., Hoon Y. M., Costen N., Li B. Automatic wrinkle detection using hybrid hessian filter. Lecture Notes in Computer Science, 2015, Vol. 9005. pp. 609–622.

[3] Doroz R., et al. A new personal verification technique using finger–knuckle imaging. Lecture Notes in Computer Science, 2016, Vol. 9876. pp. 515–524.

[4] Doroz R., Porwik P., Safaverdi H. The new multilayer ensemble classifier for verifying users based on keystroke dynamics. Lecture Notes in Computer Science, 2015, Vol. 9330. pp. 598–605.

[5] Ferrer M., Travieso C., Alonso J. Using hand knuckle texture for biometric identifications. IEEE Aerospace and Electronic Systems Magazine, 2006, Vol. 21(6). pp. 23–27.

[6] Kudlacik P., Porwik P., Wesolowski T. Fuzzy approach for intrusion detection based on user's commands. Soft Computing, 2016, Vol. 20. pp. 2705–2719.

[7] Kumar A., Wang B. Recovering and matching minutiae patterns from finger knuckle images. Pattern Recognition Letters, 2015, Vol. 68. pp. 361–367.

[8] Kumar A., Zhou Y. Human identification using knuckle codes. IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems, 2009. pp. 98–109.

[9] Markovsky I., Mahmoodi S. Least-squares contour alignment. IEEE Signal Processing Letters, 2009, Vol. 16(1). pp. 41–44.

[10] Morales A., Travieso C., Ferrer M., Alonso J. Improved finger-knuckle-print authentication based on orientation enhancement. Electronics Letters, 2011, Vol. 47(6). pp. 380–382.

[11] Otsu N. A threshold selection method from gray-level histograms. IEEE Transactions on Systems, Man and Cybernetics, 1979, Vol. 9(1). pp. 62–66.

[12] Pavlidis T. A thinning algorithm for discrete binary images. Computer Graphics and Image Processing, 1980, Vol. 13(2). pp. 142–157.

[13] Porwik P., Doroz R., Wrobel K. A new signature similarity measure. Proceedings of World Congress on Nature and Biologically Inspired Computing, NABIC 2009, 2009. pp. 1022–1027.

[14] Raiyn J. A survey of cyber attack detection strategies. International Journal of Security and its Applications, 2014, Vol. 8(1). pp. 247–256.

[15] Salem M., Hershkop S., Stolfo S. A survey of insider attack detection research. Advances in Information Security, 2008, Vol. 39. pp. 69–90.

[16] Wesolowski T., Porwik P. Keystroke data classification for computer user profiling and verification. Lecture Notes in Artificial Intelligence, 2015, Vol. 9330. pp. 588–597.

[17] Wesolowski T., Porwik P., Doroz R. Electronic health record security based on ensemble classification of keystroke dynamics. Applied Artificial Intelligence, 2016, Vol. 30. pp. 521–540.

[18] Wesolowski T. E., Porwik P. Computer user profiling based on keystroke analysis. Advances in intelligent systems and computing, 2016, Vol. 395. pp. 3–13.

[19] Wesolowski T. E., Porwik P., Doroz R. Electronic health record security based on ensemble classification of keystroke dynamics. Applied Artificial Intelligence, 2016, Vol. 20. pp. 521–540.

[20] Wrobel K., Porwik P., Doroz R., Safaverdi H. Person verification based on finger knuckle images and least-squares contour alignment. International Conference on Biometrics and Kansei Engineering (ICBAKE), 2017. pp. 119–122.

[21] XIONG M., YANG W., SUN C. Finger-knuckle-print recognition using lgbp. Lecture Notes in Computer Science, 2011, Vol. 6676. pp. 270–277.

[22] ZHONG Y., DENG Y., JAIN A. Keystroke dynamics for user authentication. Computer Vision and Pattern Recognition Workshops, IEEE Computer Society Conference, 2012. pp. 117–123.