Keystroke Dynamics Performance Enhancement With Soft Biometrics

Syed Zulkarnain Syed Idrus, Estelle Cherrier, Christophe Rosenberger, Soumik Mondal, Patrick Bours

Keystroke Dynamics Performance Enhancement With Soft Biometrics

Syed Zulkarnain Syed Idrus[1,2], Estelle Cherrier[2], Christophe Rosenberger[2], Soumik Mondal[3] and Patrick Bours[3]

[1]Universiti Malaysia Perlis, 01000 Kangar, Perlis, Malaysia
[2]UniCAEN / ENSICAEN / CNRS, UMR 6072 GREYC, F-14032 Caen, France
[3]NISlab, Gjøvik University College, Gjøvik, Norway

Abstract

It is accepted that the way a person types on a keyboard contains timing patterns, which can be used to classify him/her, is known as keystroke dynamics. Keystroke dynamics is a behavioural biometric modality, whose performances, however, are worse than morphological modalities such as fingerprint, iris recognition or face recognition. To cope with this, we propose to combine keystroke dynamics with soft biometrics. Soft biometrics refers to biometric characteristics that are not sufficient to authenticate a user (e.g. height, gender, skin/eye/hair colour). Concerning keystroke dynamics, three soft categories are considered: gender, age and handedness. We present different methods to combine the results of a classical keystroke dynamics system with such soft criteria. By applying simple sum and multiply rules, our experiments suggest that the combination approach performs better than the classification approach with best result of 5.41% of equal error rate. The efficiency of our approaches is illustrated on a public database.

1. Introduction

Keystroke dynamics measures the rhythms a person exhibits while typing on a keyboard. It is a behavioral biometric modality as well as signature dynamics, gait, voice [1, 2, 3]. Among its advantages in comparison to other modalities, we can mention that it is a low-cost with no extra sensor or device is required [4, 5]. The counterpart to this benefits is the worse performances compared to those morphological biometric modalities (*i.e.* fingerprint, iris recognition or face recognition) [6, 7], which can be explained by the large *intra-class* variability of the users' behaviour. One way to handle this matter is to take into account additional information in the decision process. This can be done with: (i) multibiometrics [8]; (ii) quality evaluation at the enrolment step [9]; or (iii) soft biometrics [10]. The two last aspects for keystroke dynamics are addressed in this paper.

In the soft biometrics domain, [10] had initially started the study, subsequently followed by others. The authors in [11] are able to increase the performance of their classical finger based biometric system by considering body weight and fat measurements as soft criteria. It decreases their system's error rate further by 2.4%. Thus, the authors performed their soft criteria combination based on fingerprint fusion approach. Hair colour and ethnicity were used as soft biometric information in [12]. The authors used those soft features to combine them with face recognition system. Results showed that the ethnicity is more prominent compared to hair colour, where it is able to reduce the error rate additionally by 1.5% from their classical system. They applied a group-specific algorithm as combination method. In [13], the authors are able to improve their system performance by introducing gender or ethnicity and facial marks (*i.e.* scars, moles and freckles) as soft biometrics characteristics. The authors used soft biometric information and combined it based on face matching score. A recent paper in [14] investigated the possibility to define more soft categories for keystroke dynamics, namely: hand (*i.e.* if the user types with one or two hands), gender, age and handedness categories, with an efficiency between 65% and 96%. The performances of soft biometrics categories recognition are enhanced by some fusion process. Moreover, two cases are studied: keystroke dynamics with fixed passwords and free-text. A new database is also proposed by [15], made publicly available. That database is used to illustrate our results and detailed after.

From the literature, we could evidently observe that by applying soft biometrics into various biometric recognition or authentication systems show some enhancement. Nonetheless, most articles associated with soft biometrics concentrate on either face, gender, fingerprint or gait recog-

nitions, but, very few on keystroke dynamics.

In this paper, the novelty of the work is to study to what extent soft biometrics can enhance the authentication performances by investigating several combination approaches. It is divided into to two parts: (i) the development of keystroke dynamics baseline system *i.e.* classical verification method; and (ii) defining how soft criteria can be combined with classical keystroke dynamics to obtain a better performance than the baseline system *i.e.* combination method.

This paper is organised as follows. Section 2 is devoted to the description of the data. In Section 3, we describe the proposed methods and the obtained results are detailed in Section 4. Section 5 presents the conclusions and suggestions for future research in this domain.

2. Data description and extraction

When typing on a keyboard, for every key, a user first presses the key down and then releases it. In terms of keystroke dynamics, two events have taken place and both events are stored as raw data. In both cases, three values are stored, being the value of the key, the type of event (either press or release) and the time the event took place [4]. From this, one can calculate features used in keystroke dynamics. Figure 1 illustrates a visual description of the keystroke typing features.

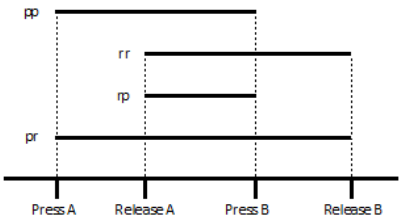

Figure 1. Keystroke typing features [15].

We exploit a publicly available dataset from [16], which provide additional soft biometric information on the participants. The used database consists of keystroke dynamics typing features of 110 users, typed 5 set of passphrases. Each user made 20 captures, 10 times with one hand and 10 times with two hands per password and hence, a total of 100 samples per user were collected. Table 1 provides an overview of information feature in the database.

For our experiment, we considered the data typed with only two hands as this represents the usual way of typing. The database contains durations and 3 kinds of latency values. These values are explicitly used in our study. A detailed description of these analyses can be found in Section 3.

We then extract the necessary data from the database.

Information	Description
Number of users	110
Gender	78 males and 32 females
Age range	Between 15 and 65 years old
Age class	$<$ 30 years old (37 males, 14 females); $\geq$ 30 years old (41 males, 18 females)
Handedness	98 right-handed (70 males, 28 females); 12 left-handed (8 males, 4 females)
Number of passwords	5
Database sample length	17 characters (“leonardo dicaprio") 18 characters (“the rolling stones") 18 characters (“michael schumacher") 22 characters (“red hot chilli peppers") 24 characters (“united states of america")

Table 1. An overview of samples contain in the database.

The extracted data features contained in the database are the timing differences between two events of these kinds (see Figure 1): press/press, release/release, press/release, release/press, and an additional vector resulting of the concatenation of the four previous ones. They are stored in the fields: *ppTime*, *rrTime*, *rpTime*, *prTime* and *vector*. Those fields provide some details pertaining to the keystroke dynamics data, which consist of information containing the timing values of keystrokes. Here, we used the fifth keystoke data that is the template vector timing value for our analysis. We also used similar features for the soft biometric information.

3. Proposed methodology

Users must type on a keyboard operating a devoted program. Every single capture is saved in a database within the program in the form of keystroke or timing features for all correct and incorrect entries. These features are composed of several timing values that are extracted, which is the *pattern vector* that is used for the analysis (see Section 2). Regarding each soft criterion, two steps are involved in recognition evaluation: (i) a training step, and (ii) a testing step, both relying on a machine learning algorithm. Here we have chosen one of the state-of-the-art techniques for classification tasks: *SVM (Support Vector Machine)* [17], by taking into consideration of its effectiveness. We compute the accuracy rate of the prediction of each soft criterion by the trained SVM, based on the testing data.

Furthermore, in this section, we illustrate several approaches on how soft biometric information can be combined into keystroke dynamics user authentication systems. Similarly to any other biometric authentication applications, the performance specifications of the system is evaluated

by measuring the number of correct and false verifications (namely: False Match Rate (FMR) and False Non-Match Rate (FNMR)), which then is reported in the form of Equal Error Rate (EER) value. For the baseline system, we perform user authentication with computations in order to obtain the verification performance scores from all 5 known passwords *i.e.* raw scores. It is considered as the foundation of our keystroke dynamics authentication system and its performance is decided by the EER values.

For the combination approaches, it is done on various aspects: first, with only a single soft biometric criterion and subsequently with all soft criteria. We make several comparison assessments in order to gain lower EER values than the values of the classical approach. The ones with lower values are considered as good performances.

We first define the performance measures. By using only raw keystroke dynamics typing features (without considering the soft criteria), we establish a performance 'baseline' by calculating the distance scores, as the basis of this experiment. We perform comparison analyses in order to obtain the EER values for users' keystroke dynamics based authentication. The computation is done by comparing the capture template with the reference one, afterwhich a score is obtained. The detailed description on how we conduct the keystroke dynamics analysis is described in Section 3.1. At this stage, we obtained only the keystroke dynamics verification scores. Subsequently, we combine those scores with three soft biometric information (either gender or age or handedness). We perform similar distance score computations as mentioned earlier to obtain the soft biometric scores.

Then, we define the combination approaches. First, we create the soft biometric templates from users' keystroke dynamics verification data. We obtain from multiple SVM recognition algorithms a set of soft biometric scores for gender, age and handedness. Once we have acquired both keystroke dynamics and soft biometric scores, we then perform the combination of those scores between them, which is described in Section 3.2. As an addition, we apply the data fusion [18], which corresponds to an enhancement approach that can increase the system's performance. For the fusion processes, we apply score fusion and majority voting, which is further explained in similar section. A graphical representation of the overall process is illustrated in Figure 2.

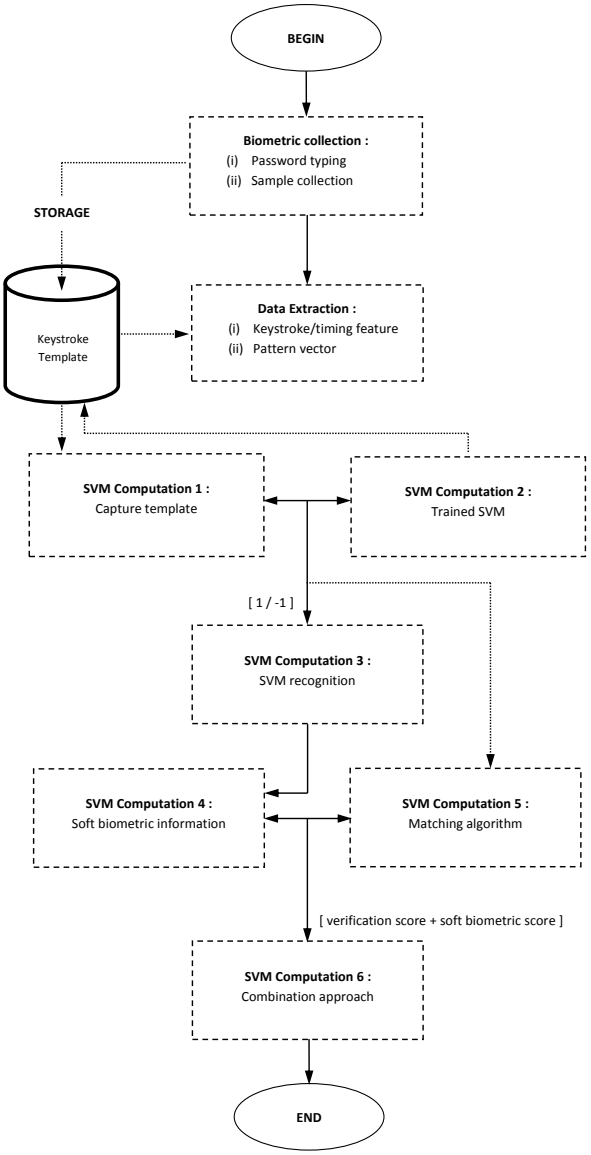

Figure 2. Principle of the proposed system.

3.1. Authentication based keystroke dynamics

The part of that dataset in [16], which is related to typing the passwords with 2 hands is used now, because this resembles the normal way that people type on the keyboard. Recall that in this dataset, each user typed 5 known passwords and each password was typed 10 times.

In general, let n_r be the number of data samples that is used for creating the template, so n_t = 10 - n_r is then the number of data samples that is used for testing. In this paper, we report the results we obtained when using n_r = n_t = 5. We have also tested on different splits, but, the results were not as good. The 5 data samples that are used to create the template are randomly selected and we used bootstrapping with 50 iterations to obtain statistically significant outcomes, and report the average result.

For the matching process, we compare a capture template with a test input to obtain a distance score. Ideally, in case template and test input are from the same person, the distance score is low compared to a distance score obtained when comparing the template and test input of two different person. Let n be the number of features in the tem-

plate and let $\mathbf{T} = ((\mu_1, \sigma_1), (\mu_2, \sigma_2), ..., (\mu_n, \sigma_n))$ denote the template, where μ_i and σ_i are the mean and standard deviation of the i^{th} feature in the template. Subsequently, let $\mathbf{t} = (t_1, t_2, \ldots, t_n)$ be a test input, where $\mathbf{t}$ corresponds to test data of each sample. The distance metric used in this paper is the so-called Scaled Manhattan Distance (SMD) [19].

$$SMD(\mathbf{T}, \mathbf{t}) = \sum_{i=1}^{n} \frac{|t_i - \mu_i|}{\sigma_i} \quad (1)$$

The distance scores are split into two: impostors scores (related to FMR) and genuine scores (related to FNMR). These two performance values depend on the threshold value. Subsequently, the performance of the system is reported for each password separately by introducing the EER value. Fusion of all 5 known passwords is also performed as follows:

- 5 separate distance values are calculated;
- Each of the 5 distance values is normalised to obtain scores in the [0,1] range *i.e.* by multiplying the class label with its associate probability values;
- The 5 normalised distance values are then averaged into a single value, and we followed a threshold.

3.2. Combination techniques

In this section, we introduce several combination approaches. We illustrate how we combine the distance score and the soft biometric score into a single value, which is used for performance analysis. In order to avoid confusion with the distance score used for normal biometric analysis, we call the new combined score "verification score". In the remainder of this section, we introduce 6 different combination rules.

First, we combine the distance score with only a single soft biometric score (either $gender$ or age or $handedness$). Let d denote the distance score and let sb_i denote the soft biometric score for the test input. While, cl denote the predicted class label value and let prb denote the probability value for the soft biometric of the template data. Finally, let v_i denote the verification score related to the fusion rules R_i that are calculated from d, sb_i, cl and prb.

In Equations (2) and (3), we define the first two rules (R_1 and R_2) for combining the distance score with the soft biometrics score. Using rule R_1, with only one soft biometric score, we get the verification score by adding the absolute difference of the predicted class label and the probability value (which derive the soft biometric score) to the distance score. With rule R_2, instead of adding, we multiply as an alternative. We further extend our analysis using similar equations and approaches. We define subsequent set of rules (R_3 and R_4) in Equations (4) and (5), respectively. But, alternatively to just one, we take all 3 soft biometric scores and combine with the distance score. Let sb_1 denote the gender score, sb_2 denote the age score, and sb_3 denote the handedness score. Finally, we obtained the verification scores, which is the results from the four combination rules mentioned. We discuss the results in Section 4.

$$v_1 = d + sb_i(|cl - prb|) \quad (2)$$

$$v_2 = d \times sb_i(|cl - prb|) \quad (3)$$

$$v_3 = d + (|sb_1 + sb_2 + sb_3|) \quad (4)$$

$$v_4 = d \times (|sb_1 + sb_2 + sb_3|) \quad (5)$$

For the final approach, we again combine the distance score with all 3 soft biometric scores. But, this time, we combine the soft biometric scores in a different manner. Let gt denote the ground truth value for the soft biometric of the template data and sbs denote the soft biometric score for the test input. Thus, sbs denote a 'factor' used in the multiplication in Equations (6) and (7). We first make a majority decision on the correctness of the soft biometric scores (sbs) when compared to the ground truth data (gt) from the template. Here, we apply the following rules to determine sbs value after comparison:

- if all 3 match, we set sbs to 1;
- if any 2 match, we set sbs to 0.5;
- if any 1 match or no match, we set sbs to 0.

In addition, we introduce two combination principles: "penalty combination" and "reward combination". These principles in regards to the distance metric are applied in order to ensure that the impostor user stay above and genuine user below a given threshold. It is done by two means: (i) take the value '2' and minus it with sbs for "penalty combination"; and (ii) take the value '1' and minus it with sbs for "reward combination". Here, a "'reward" implies to when the v_i value is lower than SMD value *i.e.* verification score obtained better result than the distance score (or baseline performance). Whereas, when the v_i value is higher than SMD value *i.e.* verification score obtained worse result than the distance score, thus is penalised with a "penalty".

Subsequently, the verification score value is the outcome of multiplying distance score value with soft biometric score value. It is defined as in Equations (6) and (7) by the last two rules (R_5 and R_6), respectively. Since, SVM

provides a score in the [0,1] range, hence, Equation (6) is defined as “penalty combination" due to the value of v_5 is force beyond the set threshold that is between 1 and 2 to penalise unlikely pattern scores. Whereas, for Equation (7), the value of v_6 stays between 0 and 1, which is within the acceptable circle of trust, thus a “reward combination" is defined.

$$v_5 = d \times (2 - sbs) \tag{6}$$

$$v_6 = d \times (1 - sbs) \tag{7}$$

4. Experimental results

In this section, we present the results obtained from the techniques presented in the previous section. Recall that we first compute the baseline performances for each of the 5 known passwords of the classical keystroke dynamics system *i.e.* without any soft criteria. Then, in Sections 4.2 and 4.3, we show the results of combining one or all soft biometric scores with the distance score according to rules (R_1 to R_4) are defined by Equations (2) to (5). Finally, the fusion results of using majority voting on the soft biometric scores is discussed given in Section 4.4 in case of rules (R_5 and $R6$) are defined by Equations (6) and (7).

4.1. Baseline system performances

Figure 3 illustrates the Detection Error Tradeoff (DET) curves, that shows the performance of the baseline biometric system. The curves are generated after computing the *intra-class* and *inter-class* scores to obtain the FMR and FNMR values for the 5 known passwords. Table 2 shows the baseline EER results based on classical keystroke dynamics: the obtained values are between 15.56% and 21.45% for equal splits of template and test data samples (where, n_r = n_t = 5). According to [20], longer passwords provide better results. Unsurprisingly, fusing information had substantially improves the performance of the proposed system, since the new EER is equal to 10.63%. This might not hold for small differences, where complexity also plays a role, but, it certainly holds when comparing a password of length 20 to a password of length 100.

4.2. Fusion process 1

Tables 3 shows the performance results of combining keystroke dynamics with soft biometric information when using the combination rule of Equation (2). The table shows the results for each combination of a password and a single soft biometric feature. Besides that, the last row shows the results of combining all 5 known passwords with each of the soft biometric features and the last column shows the performances of combining a password with all 3 soft biometrics. The results for the combination of one soft biometric score with the single password distance score are between 13.10% and 21.67% (depending on password and soft criterion). In all except 2 cases, the performance is improved. In the 2 cases where the performance does not improve (*i.e.* Password 1 in combination with the age soft biometric and Password 3 with the gender soft biometric), the EER value only slightly increases compared to the baseline performance.

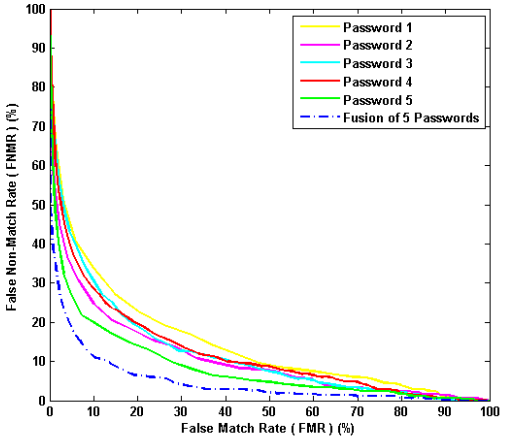

Figure 3. DET curve for 5 known passwords with fusion.

Password	EER value
Password 1	21.45%
Password 2	18.38%
Password 3	19.26%
Password 4	19.84%
Password 5	15.56%
Fusion of 5 passwords	10.63%

Table 2. Performance of the baseline keystroke dynamics system.

Next, we tested the combination of the three soft criteria with the distance score by Equation (4) and found that the results are of the same order *i.e.* between 14.88% and 19.05%. When repeating this with the combination of all 5 known passwords and either 1 or 3 soft biometric scores, the resulting EER values were found to be between 8.33% and 12.50%. In this case, we noted that combining with only one soft biometric score did not significantly improve the performance compared to the baseline performance.

4.3. Fusion process 2

We then applied the same analysis, but, only using Equations (3) and (5) to find the verification score v_i instead of Equations (2) and (4). Experimental results can be found in Table 4.

4.4. Fusion processes 3 and 4 with majority voting

In our final analysis, we choose to combine the 3 soft biometric scores using majority voting. Table 5 shows that when we apply Equation (6) with rule (R_5), the results are quite bad, since the EER values are between 29.14% and 39.07% for the single known password, and the EER value is 28.52% with the fusion of the 5 known passwords. Using rule (R_6) with Equation (7), we obtained EER values between 7.34% and 14.09%. By fusing the 5 known passwords, the performance significantly improves with a value of 5.41% for the EER.

The EER values in all cases are worse than what is found in Table 3 under the same conditions. The only exception being the fusion of the distance score related to Password 2 with the combination of all 3 soft biometric features. In that case, Equations (3) and (5) gave in fact slightly better results compared to Equations (2) and (4). But, overall did we find much worse result, *e.g.* for the combination of Password 5 with the age soft biometric, the EER using Equations (2) and (4) are less than 15%, while Equations (3) and (5) would give an EER of 40%.

Password	**Baseline**	**Penalty Eq.**(6)	**Reward Eq.**(7)
Password 1	21.45%	30.04%	10.27%
Password 2	18.38%	29.14%	7.45%
Password 3	19.26%	31.62%	9.59%
Password 4	19.84%	31.09%	7.34%
Password 5	15.56%	39.07%	14.09%
Fusion of 5 passwords	10.63%	28.52%	5.41%

Table 5. EER values of baseline performance combined with soft biometric information by using penalty and reward combinations.

Observe that, this rule acts as a “reward combination" rule (Equation (7)): the verification score is better than that of the baseline one only when the soft criteria bring interesting information. The same analysis with the rule based on Equation (6) would show that it is a “penalty combination" rule, which may explain the worse performances. Indeed, the verification score is increased only when the soft criteria are false. It means that a greater importance is given to non-corresponding soft criteria (whereas when all soft criteria are correct, the distance does not change). The reward combination provides the best result with a gain of 5.22%.

5. Conclusions and perspectives

In this paper, we proposed an improvement of user verification scores (new combined results) with keystroke dynamics by considering soft biometric information. We presented several techniques such as *majority voting* and *score fusion* with a number of combination approaches that can enhance the keystroke dynamics authentication systems.

Multiple results were obtained as illustrated in the previous section, which offers some enhancement for the baseline system performances *i.e.* initial results of the classical keystroke dynamics. For example, the results of our baseline performances for 5 known passwords show that we managed to obtain EER values between 15.56% and 21.45%, and by fusing is further reduced to 10.63%. With the correct combination approach, we are able to reduced the EER value to up to 12.50%, and 5.22% with fusion. Nonetheless, there are also some results with poor outcomes depending on the combination techniques.

In conclusion, the results presented in this paper can be used to improve user verification based on keystroke dynamics by combining soft biometric information with: (i) *‘distance score’* provided by the biometric authentication system when comparing the reference to a stored template; and (ii) fusion to further enhance the recognition systems, which may be considered as an added value for the system's performance improvement. The proposed combination approaches could be used for other biometric modalities.

References

[1] S. Impedovo and G. Pirlo, “Verification of handwritten signatures: an overview,” in *Image Analysis and Processing, 2007. ICIAP 2007. 14th International Conference on*, pp. 191–196, IEEE, 2007.

[2] K. Moustakas, D. Tzovaras, and G. Stavropoulos, “Gait recognition using geometric features and soft biometrics,” *Signal Processing Letters, IEEE*, vol. 17, no. 4, pp. 367–370, 2010.

[3] R. L. Klevans and R. D. Rodman, *Voice recognition*. Artech House, Inc., 1997.

[4] R. Giot, M. El-Abed, and C. Rosenberger, “Keystroke dynamics overview,” *Biometrics/Book*, vol. 1, pp. 157–182, 2011.

[5] P. Bours, “Continuous keystroke dynamics: A different perspective towards biometric evaluation,” *Information Security Technical Report*, vol. 17, pp. p. 36–43, February 2012.

[6] R. Wildes, “Iris recognition: an emerging biometric technology,” *Proceedings of the IEEE*, vol. 85, no. 9, pp. 1348–1363, 1997.

[7] D. Maio and A. K. Jain, *Handbook of fingerprint recognition*. springer, 2009.

[8] A. K. Jain and A. Ross, “Multibiometric systems,” *Communications of the ACM*, vol. 47, no. 1, pp. 34–40, 2004.

Password	Baseline	Gender	Age	Handedness	All soft biometrics
Password 1	21.45%	18.21%	21.67%	19.64%	19.05%
Password 2	18.38%	17.14%	17.14%	16.67%	18.45%
Password 3	19.26%	19.64%	16.19%	19.05%	19.05%
Password 4	19.84%	14.29%	19.52%	18.45%	17.86%
Password 5	15.56%	13.93%	14.76%	13.10%	14.88%
Fusion of 5 passwords	10.63%	10.36%	10.71%	12.50%	8.33%

Table 3. Results of verification approach combined with soft biometric information approach and their EER values by using Equations (2) and (4) (with additions).

Password	Baseline	Gender	Age	Handedness	All soft biometrics
Password 1	21.45%	31.43%	30.71%	29.76%	25.00%
Password 2	18.38%	30.00%	34.76%	26.19%	17.86%
Password 3	19.26%	34.29%	30.48%	30.95%	20.83%
Password 4	19.84%	27.50%	33.57%	32.14%	19.64%
Password 5	15.56%	31.07%	40.00%	28.57%	29.76%
Fusion of 5 passwords	10.63%	29.17%	32.14%	27.38%	14.29%

Table 4. Results of verification approach combined with soft biometric information approach and their EER values by using Equations (3) and (5) (with multiplications).

[9] S. Mondal, P. Bours, and S. Idrus, "Complexity measurement of a password for keystroke dynamics: preliminary study," in *Proceedings of the 6th International Conference on Security of Information and Networks*, pp. 301–305, ACM, 2013.

[10] A. K. Jain, S. C. Dass, and K. Nandakumar, "Soft biometric traits for personal recognition systems," in *Proceedings of International Conference on Biometric Authentication*, pp. p. 731–738, Springer, 2004.

[11] H. Ailisto, E. Vildjiounaite, M. Lindholm, S.-M. Mäkelä, and J. Peltola, "Soft biometrics–combining body weight and fat measurements with fingerprint biometrics," *Pattern Recognition Letters*, vol. 27, no. 5, pp. p. 325 – 334, 2006.

[12] G. L. Marcialis, F. Roli, and D. Muntoni, "Group-specific face verification using soft biometrics," *Journal of Visual Languages & Computing*, vol. 20, no. 2, pp. 101–109, 2009.

[13] U. Park and A. Jain, "Face matching and retrieval using soft biometrics," *Information Forensics and Security, IEEE Transactions on*, vol. 5, pp. 406–415, sept. 2010.

[14] S. Z. Syed Idrus, E. Cherrier, C. Rosenberger, and P. Bours, "Soft biometrics for keystroke dynamics: Profiling individuals while typing passwords," *Computers & Security*, vol. 45, no. 9, pp. 147–155, 2014.

[15] S. Z. Syed Idrus, E. Cherrier, C. Rosenberger, and P. Bours, "Soft biometrics database: a benchmark for keystroke dynamics biometric systems," in *2013 International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2013.

[16] S. Z. Syed Idrus, E. Cherrier, C. Rosenberger, and P. Bours. `http://www.epaymentbiometrics.ensicaen.fr/index.php/app/resources/91`.

[17] V. Vapnik, *Statistical learning theory*. Wiley, 1998.

[18] H. Fronthaler, K. Kollreider, J. Bigun, J. Fierrez, F. Alonso-Fernandez, J. Ortega-Garcia, and J. Gonzalez-Rodriguez, "Fingerprint image-quality estimation and its application to multialgorithm verification," *Information Forensics and Security, IEEE Transactions on*, vol. 3, no. 2, pp. 331–338, 2008.

[19] R. Niedermeier and P. Sanders, *On the Manhattan Distance Between Points on Space Filling Mesh Indexings*. Univ., Fak. für Informatik, 1996.

[20] M. Abernethy, M. Khan, and S. Rai, "User authentication using keystroke dynamics and artificial neural networks," in *Proceedings of the 5th Australian Information Warfare and Security Conference. Perth Western Australia*, 2004.