Keystroke Dynamics for User Authentication

Yu Zhong Yunbin Deng
Advanced Information and Technology
BAE Systems
6 New England Executive Park
Burlington, MA 01803

{Yu.zhong,Yunbin.deng}@baesystems.com

Anil K. Jain
Dept. Computer Science & Engineering
Michigan State University
3115 Engineering Building
E. Lasing, MI 48824

jain@cse.msu.edu

Abstract

In this paper we investigate the problem of user authentication using keystroke biometrics. A new distance metric that is effective in dealing with the challenges intrinsic to keystroke dynamics data, i.e., scale variations, feature interactions and redundancies, and outliers is proposed. Our keystroke biometrics algorithms based on this new distance metric are evaluated on the CMU keystroke dynamics benchmark dataset and are shown to be superior to algorithms using traditional distance metrics.

1. Introduction

With the ever increasing demand for more secure access control in many of today's security applications, traditional methods such as PINs, tokens, or passwords fail to keep up with the challenges presented because they can be lost or stolen, which compromises the system security. On the other hand, biometrics [9][13][14][15][21][25][31][33] based on "who" is the person or "how" the person behaves present a significant security advancement to meet these new challenges. Among them, keystroke dynamics [22][24][26] provides a natural choice for secure "password-free" computer access. Keystroke dynamics refers to the habitual patterns or rhythms an individual exhibits while typing on a keyboard input device. These rhythms and patterns of tapping are idiosyncratic [5], in the same way as handwritings or signatures, due to their similar governing neurophysiological mechanisms. As early as in the 19th century, telegraph operators could recognize each other based on one's specific tapping style [18]. This suggests that keystroke dynamics contain sufficient information to serve as a potential biometric identifier to ascertain a specific keyboard user.

Compared to other biometrics, keystroke biometrics has additional desirable properties due to its user-friendliness and non-intrusiveness. Keystroke dynamics data can be collected without a user's cooperation or even awareness. Continuous authentication is possible using keystroke dynamics just as a mere consequence of people's use of computers. Unlike many other biometrics, the temporal information of keystrokes can be collected to ascertain a user using only software and no additional hardware. In summary, keystroke dynamics biometrics enables a cost effective, user friendly, and continuous user authentication with potential for high accuracy.

Although keystroke dynamics is governed by a person's neurophysiological pathway to be highly individualistic, it can also be influenced by his or her psychological state. As a "behavioral" biometrics [35], keystroke dynamics exhibits instabilities due to transient factors such as emotions, stress, and drowsiness etc [6]. It also depends on external factors, such as the input keyboard device used, possibly due to different layout of the keys. The keying times can be noisy with outliers. As keystroke biometrics exploits the habitual rhythm in typing, it has been observed that keystrokes of frequently typed words or strings show more consistency and are better discerners [22][38].

Keystroke biometrics can use "static text", where keystroke dynamics of a specific pre-enrolled text, such as a password, is analyzed at a certain time, e.g., during the log on process. For more secure applications, "free text" should be used to continuously authenticate a user.

The rest of the paper is organized as follows. In section 2 we will review the current state of keystroke biometric techniques. We discuss the strength and limitations of two top performing distance metrics for keystroke dynamics and propose a new distance metric that combines the benefits of both these schemes in section 3. Section 4 describes our keystroke dynamics classifiers. Section 5 presents the experiments and performance study of the proposed algorithms. In section 6 we summarize our approach and outline future work.

2. Literature Review

Of late, keystroke dynamics has become an active research area due to the increasing importance of cyber security and computer or network access control. Most of

978-1-4673-1612-5/12/$31.00 ©2012 IEEE

the existing approaches focus on static verification, where a user types specific pre-enrolled string, e.g., a password during a login process, and then their keystroke features are analyzed for authentication purposes [30]. Only a few research studies address the more challenging problem of keystroke biometrics using "free text", where the users can type arbitrary text as input [22][28][37].

Keystroke dynamics features are usually extracted using the timing information of the key down/hold/up events. The hold time or dwell time of individual keys, and the latency between two keys, i.e., the time interval between the release of a key and the pressing of the next key are typically exploited. Digraphs, which are the time latencies between two successive keystrokes, are commonly used. Trigraphs, which are the time latencies between every three consecutive keys, and similarly, n-graphs, have been investigated as well. In their study on keystroke analysis using free text, Sim and Janakiraman [27] investigated the effectiveness of digraphs and more generally n-graphs for free text keystroke biometrics, and concluded that n-graphs are discriminative only when they are word-specific. As such, the digraph and n-graph features do depend on the word context they are computed in.

The use of keystroke dynamics for verification and identification purposes was first investigated back in the 1970's [7][29]. Gaines et al. [8] did a preliminary study on keystroke dynamics based authentication using the T-test on digraph features. Monrose and Rubin [22] later extracted keystroke features using the mean and variance of digraphs and trigraphs. Using the Euclidean distance metric with Bayesian-like classifiers, they reported a correct identification rate of 92% for their dataset containing 63 users.

Bergadano et al. [2] and later Gunetti and Picardi [10] proposed to use the relative order of duration times for different n-graphs to extract keystroke features that was found to be more robust to the intra-class variations than absolute timing. They demonstrated that the new relative feature, when combined with features using absolute timing, improved the authentication performance using free text.

Over the years, keystroke biometrics research has utilized many existing machine learning and classification techniques. Different distance metrics, such as the Euclidean distance [3][22], the Mahalanobis distance [3][4], and the Manhattan distance [1][16], have been explored. Both classical and advanced classifiers have been used, including K-Nearest Neighbor (KNN) classifiers [4], K-means methods [12], Bayesian classifiers [22], Fuzzy logic [11], neural networks [11][19], and support vector machines (SVMs) [36]. A large range of performance numbers has been published. However, it is not possible to make a sound comparison of various algorithms directly because of the use of different datasets and evaluation criteria across the studies. To address this issue, keystroke dynamics databases including benchmark results of popular keystroke biometrics algorithms have been published [17][19] to provide a standard experimental platform for progress assessment. Killourhy and Maxion collected and published a keystroke dynamics benchmark dataset containing 51 subjects with 400 keystroke dynamics collected for each subject [17]. Furthermore, they evaluated fourteen available keystroke dynamics algorithms on this dataset, including Neural Networks [4], K-means [12], Fuzzy Logic [11], KNNs, Outlier Elimination [11], SVMs [36], etc. Various distance metrics, including Euclidean distance [3], Manhattan distance [1][16] and Mahalanobis distance [3][4] were used. This keystroke dataset along with the evaluation methodology and state of the art performance provides a benchmark to objectively gauge the progresses of new keystroke biometric algorithms.

3. A New Distance Metric for Feature Matching

The performance study of the fourteen existing keystroke dynamics algorithms implemented by Killourhy and Maxion [17] indicated that the top performers are the classifier using scaled Manhattan distance [1], with an equal error rate (EER) of 0.096, and the nearest neighbor classifier using the Mahalanobis distance [4] with an EER of 0.10 on their keystroke dynamics benchmark dataset. In the following section we discuss the advantages of both Manhattan distance and Mahalanobis distance to understand why they succeed in matching keystroke dynamics patterns. We also point out their limitations. A new distance metric is then proposed to combine the benefits of these two distance metrics while overcoming their limitations.

3.1. Mahalanobis Distance

Euclidean distance has been the default distance metric for its simplicity and geometrical intuitiveness. However, it has two major limitations:

1. It is very sensitive to scale variations in the feature variables, and
2. It has no means to deal with the correlation between feature variables.

Mahalanobis distance, on the other hand, takes into account the covariance of data variables to correct for the heterogeneity and non-isotropy observed in most real data. The squared Mahalanobis distance between two feature vectors x and y is defined as

$$\|x-y\|^2 = (x-y)^T S^{-1}(x-y) \qquad (1)$$

where S is the covariance matrix of the data. It not only weights the distance calculation according to the statistical

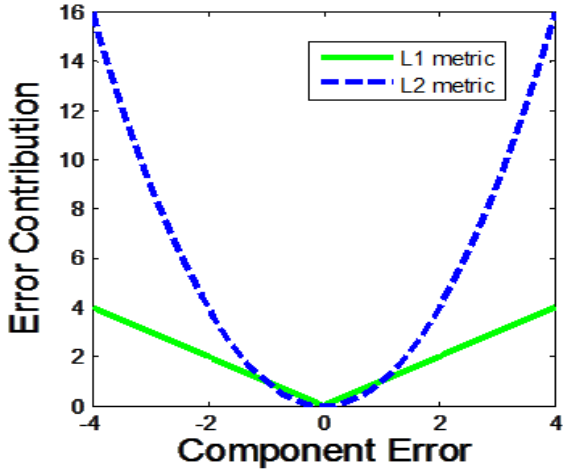

Figure 1: The error contribution of individual feature variables grows quadratically in its magnitude for L_2 metrics, including Euclidean distance and Mahalanobis distance, but it increases only linearly for L_1 metrics such as Manhattan distance.

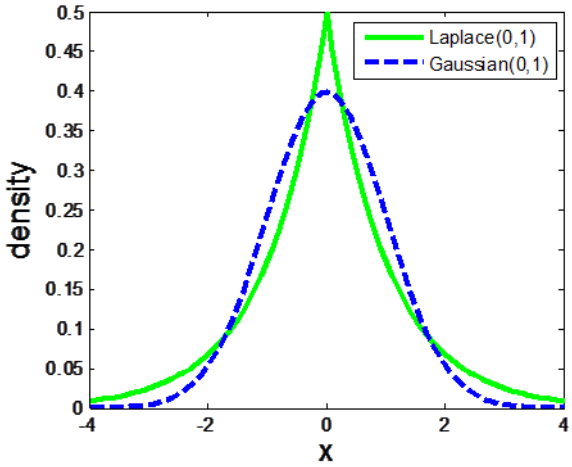

Figure 2: The probability density functions for univariate Laplace distribution and Gaussian distribution with mean 0 and variance 1. The Laplace distribution has fatter tails than the Gaussian distribution to be more tolerant to outliers.

variation of each feature component, but also decouples the interactions between features based on their covariance matrix to provide a useful distance metric for feature comparisons in pattern analysis. In statistical literature, the Mahalanobis distance is related to the log likelihood under the assumption that data follow multivariate Gaussian distribution which is a reasonable approximation for most practical data.

3.2. Manhattan Distance

The Manhattan distance metric, also called L_1 distance or city block distance, is defined as follows:

$$\|x-y\|_1 = \sum_i |x_i - y_i| \qquad (2)$$

The Manhattan distance has the advantages of simplicity in computation and easy decomposition into contributions made by each variable. Most importantly, it is more robust to the influence of outliers compared to higher order distance metrics including Euclidean distance and Mahalanobis distance. As shown in **Figure 1**, the error contribution of the individual component grows quadratically in its magnitude for L_2 metrics including Euclidean distance and Mahalanobis distance, while it increases only linearly for L_1 metrics such as Manhattan distance. As a result, Manhattan distance is more robust than Mahalanobis distance in the presence of outliers. The Manhattan distance also has a statistical interpretation as the Mahalanobis distance. It is in fact related to the log likelihood of the multivariate Laplace distribution with an identity covariance matrix. The Laplace distribution is similar to the Gaussian distribution in that both are symmetric with one mode. However, the Laplace distribution has fatter tails than the Gaussian distribution (see **Figure 2**), and therefore, it is more tolerant to outliers that significantly deviate from the mean. The Laplace distribution provides an attractive alternative to Gaussian assumption for many real world data with heavy tails. It has been observed that the Manhattan distance metric outperformed other distance metrics including Euclidean distance, the Vector Cosine Angle distance, and Histogram Intersection distance in a performance study of image retrieval on a large image database [32].

3.3. A New Distance Metric

With the above discussion, it is easy to understand why keystroke biometrics using Mahalanobis distance and Manhattan distance outperformed other algorithms including some of the more advanced machine learning techniques. The keystroke dynamics features consist of both dwell and latency timings to have large variations in individual components. The feature variables tend to interact with each other as well. These evident scale variations and feature correlations are handled well using the Mahalanobis distance metric. However, Mahalanobis distance is susceptible to the outliers that are abundant in keystroke dynamics data due to the frequent pauses during typing. On the other hand, Manhattan distance is shown to be more robust to outliers but it is not able to correct for the adverse interactions and redundancies between keystroke features. So, each of the two metrics, when used alone, has its advantages and limitations.

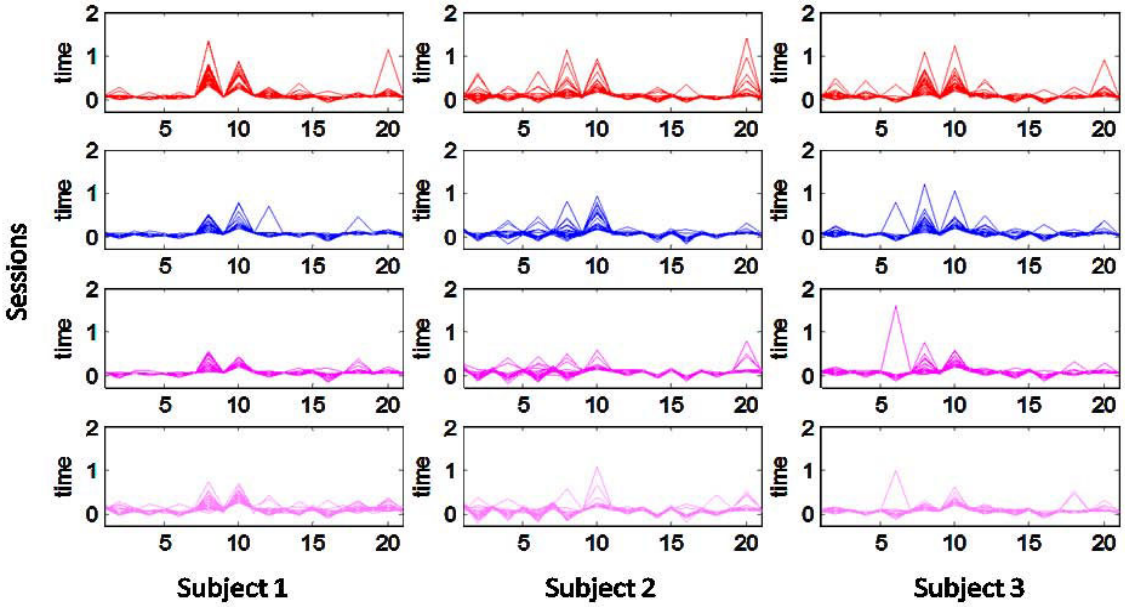

Figure 3. Keystroke dynamics features for static key string ".tie5Roanl" from the CMU keystroke dynamics benchmark dataset [17]. The dwell time and digraphs for the first four data collection sessions for three subjects are shown. Although the keystroke features provide sufficient distinguishing patterns for each subject, they are highly correlated, with large scale variations, and contain noise and outliers. Our proposed distance metric is effective in handling these challenges that are intrinsic to keystroke dynamics data.

We propose a new distance metric combining both Mahalanobis distance and Manhattan distance such that one complements the other. First, we apply the principle of Mahalanobis distance to decorrelate and normalize the keystroke dynamics feature variables so that the covariance matrix of the transformed feature vectors becomes an identity matrix. This rectifying process is accomplished by applying the following linear transform to the input keystroke dynamics data:

$$x' = \Phi x \quad (3)$$

where $\Phi = S^{-1/2}$ is the inverse of the principle square root of the covariance matrix S such that $\Phi^T * \Phi = S^{-1}$. With this transform, the data features become uncorrelated with equal variations in the feature variables. Once the data are normalized and decoupled, we then compute the Manhattan distance between two data points x' and y' in a more standardized new feature space for the original data points x and y:

$$\|x - y\|' = \| x' - y' \|_1 = \| S^{-1/2}(x - y) \|_1 . \quad (4)$$

This new distance metric ensures not only that the undesirable correlation and scale variations are accounted for, but also suppress the influence of outliers for improved performance. As a result, the proposed distance metric combines the benefits of both Mahalanobis and Manhattan distance metrics while overcoming their limitations when used individually. As it turns out, this new distance metric also has a nice statistical interpretation. It is associated with the log likelihood of the general multivariate symmetric Laplace distribution with *S* as its covariance matrix.

4. Keystroke Dynamics Classifier

We frame keystroke dynamics based authentication as a one- class classification problem which learns a model for a user, rejects anomalies to the learned model as imposters, and accept inliers as the genuine user. Although the use of negative examples in training could significantly improve the accuracy of the classifier, it is unrealistic to assume prior knowledge about the keystroke features from imposters, let alone the availability of their training data.

We used the Nearest Neighbor classifier with the new distance metric defined in to either ascertain a keystroke dynamics feature as originating from the genuine user when the distance to its nearest neighbor in the training data is below a threshold value, or reject it as an imposter, otherwise. The covariance matrix is computed using all the training keystroke feature vectors from the intended user.

The adoption of the new distance metric helps suppress the adverse effects of outliers during the classification stage. However, outliers could still corrupt the training data and deteriorate the authentication performance. We

Algorithm	Equal-error rate		Algorithm	Zero-miss false-alarm rate
Nearest Neighbor (new distance metric) + outlier removal	**0.084 (0.056)**		Nearest Neighbor (new distance metric) + outlier removal	**0.405 (0.268)**
Nearest Neighbor (new distance metric)	**0.087 (0.060)**		Nearest Neighbor (new distance metric)	**0.423 (0.269)**
Manhattan (scaled) [17]	0.096 (0.069)		Nearest Neighbor (Mahalanobis) [17]	0.468 (0.272)
Nearest Neighbor (Mahalanobis) [17]	0.100 (0.064)		Mahalanobis [17]	0.482 (0.273)

Table 1. The proposed keystroke biometric algorithms outperform existing detectors reported in [17]. Shown in bold in the table are the average equal error rate (with the standard deviation shown in brackets) and the zero-miss false-alarm rate of our two keystroke dynamics algorithms: Nearest neighbor classifier with the proposed new distance metric for keystroke dynamics features, and NN classifier using the new distance metric with additional outlier removal in training phase. We also show the performances of the top two performers for either of the error categories reported in [17]. The proposed new distance metric is shown to be advantageous in handling the challenges intrinsic to the keystroke dynamics data by reducing both errors.

employed an outlier removal process during the training phase. For the *i*th feature variable, we sort the measurements from the training data and compute the median μ_i and standard deviation σ_i using all training measurements excluding those in the upper and lower p percentiles. Only the training feature vectors with their *i*th variable falling in the interval $[\mu_i - k\sigma_i, \quad \mu_i + k\sigma_i]$ are retained and those falling outside of the interval are discarded from the training data. Once the outliers are removed from the training data, we use the Nearest Neighbor classifier with the new distance metric to classify the test keystroke feature vectors. So, we essentially have two different new metric based nearest neighbor classification algorithms: one without outlier removal and one with outlier removal.

5. Experiments

We evaluated the proposed keystroke authentication algorithms using the CMU keystroke dynamics benchmark dataset [17] because it comes with the performance numbers for a range of existing keystroke dynamics algorithms for objective comparison.

The CMU benchmark dataset contains keystroke dynamics consisting of the dwell time for each key and the latencies between two successive keys for static password string ".tie5Roanl". There are 51 subjects in the dataset. For each subject, there are eight data collection sessions with at least one day interval between two sessions. A total of 50 feature vectors were extracted in each session, resulting in a total of 400 feature vectors for each subject. We show in **Figure 3** four sessions of keystroke dynamics features collected for three subjects. The absolute value of the covariance matrix of the keystroke features for one subject is also visualized in **Figure 4**.

Although the keystroke features provide sufficient distinguishing patterns for each subject, they are highly correlated, with large scale variations, and contain noise and outliers. Our proposed distance metric is effective in handling these challenges that are intrinsic to keystroke dynamics data.

We used the exact same protocol and evaluation methodology as in [17] to ensure objective performance comparisons. For each subject, we used the first 200 feature vectors as the training data. The remaining 200 feature vectors were used as positive test data and the first 50 feature vectors from the remaining 50 subjects are used to form 250 negative feature vectors as imposters in the authentication phase for this user. The authentication accuracy is evaluated using the equal error rate (ERR), where the miss rate and false alarm rate are equal, and the zero-miss false alarm rate (ZMFAR), which is the minimum false alarm rate when the miss rate is zero. The evaluation is performed for each subject; the mean and standard deviation of error rates for the 51 subjects are reported.

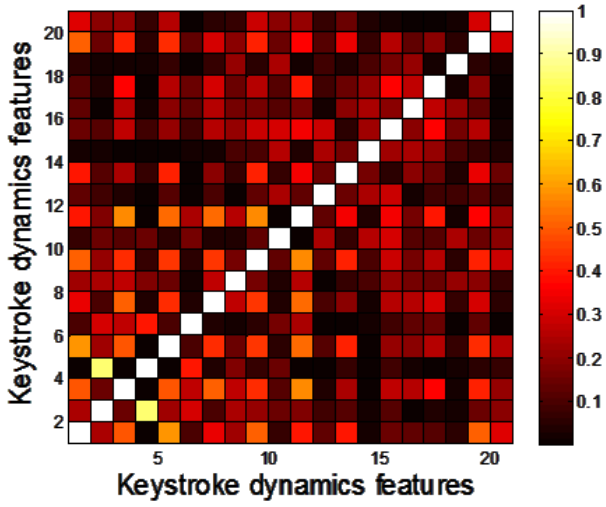

Figure 4. Keystroke dynamics features are correlated. Shown in the figure is the absolute value of the covariance matrix of the training keystroke features for one subject, normalized so that the diagonal entries are 1.

Using the nearest neighbor classifier with the proposed new distance metric, we achieved an average EER of 8.7%, and ZMFAR of 42.3% across all 51 subjects. The error rate is reduced to 8.4% for ERR and 40.5% for

ZMFAR by further removing outliers from the training dataset. We used $p = 5$ and $k = 4$ in the experiments for outlier removal. Our proposed algorithms outperform the best reported algorithms in both metrics, as shown in Table 1.

6. Conclusions and Future Work

We studied the characteristics of keystroke dynamics for computer user authentication and proposed a new distance metric which decouples correlated data, normalizes feature variations, and suppresses outliers. As outliers and data correlations are typical in keystroke dynamics data, it is not surprising that classifiers using the new distance metric outperform existing top performing keystroke dynamics classifiers which use traditional distance metrics.

Although we applied the new distance metric to the problem of matching keystroke dynamics features, it is a general distance metric that can be applied to any distance computation in feature vector spaces where the traditional Mahalanobis distance is applicable, with the additional advantage of robustness to outliers.

We have applied the proposed distance metric to improve the accuracy of keystroke dynamics using static text. In the future, we will investigate application of our new distance metric to the more challenging problem of keystroke biometrics using free text, develop richer key stroke features, and study context dependent sub-word and across-word models.

7. References

[1] L. C. F. Ara´ujo, L. H. R. Sucupira, M. G. Liz´arraga, L. L. Ling, and J. B. T. Yabu-uti. "User authentication through typing biometrics features", In Proc. 1st Int'l Conf. on Biometric Authentication (ICBA), volume 3071 of Lecture Notes in Computer Science, pp. 694–700, 2004.

[2] F. Bergadano, D. Gunetti, and C. Picardi, "User Authentication through Keystroke Dynamics", ACM Trans. Information and System Security, 5(4), pp. 367–397, 2002.

[3] S. Bleha, C. Slivinsky, and B. Hussein, "Computer-Access Security Systems using Keystroke Dynamics", IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 12, no. 12, 1990, pp. 1217–1222.

[4] S. Cho, C. Han, D. H. Han, and H. Kim. "Web-based keystroke dynamics identity verification using neural network", Journal of Organizational Computing and Electronic Commerce, 10(4):295–307, 2000.

[5] A. Dvorak, N. Merrick, W. Dealey, and G. Ford. "Typewriting Behavior. American Book Company, New York, USA, 1936.

[6] C. Epp, M. Lippold, and R. L. Mandryk, "Identifying Emotional States using Keystroke Dynamics", Proc. 2011 annual conf. on Human factors in computing systems, 2011.

[7] G. Forsen, M. Nelson, and R. Staron, Jr. "Personal attributes authentication techniques", Technical Report RADC-TR-77-333, Rome Air Development Center, October 1977.

[8] R. Gaines, W. Lisowski, S. Press, and N. Shapiro, "Authentication by keystroke timing: some preliminary results", Rand Rep. R-2560-NSF, Rand Corporation, 1980.

[9] R. Giot, B. Hemery and C. Rosenberger, "Low Cost and Usable Multimodal Biometric System Based on Keystroke Dynamics and 2D Face Recognition", Int'l Conf. on Pattern Recognition (ICPR), pp. 1128 -1131, 2010.

[10] D. Gunetti and C. Picardi. "Keystroke analysis of free text", ACM Transactions on Information and System Security, 8(3):312–347, 2005.

[11] S. Haider, A. Abbas, and A. K. Zaidi. "A multi-technique approach for user identification through keystroke dynamics", IEEE Int'l Conf. on Systems, Man and Cybernetics, pp. 1336–1341, 2000.

[12] P. Kang, S. Hwang, and S. Cho. "Continual retraining of keystroke dynamics based authenticator", In Proc. 2nd Int'l Conf. on Biometrics (ICB'07), pp. 1203–1211, 2007.

[13] A. K. Jain, R. Bolle, and S. Pankanti (editors), "Biometrics: Personal Identification in Networked Society", Kluwer Academic Publishers, 1999.

[14] A. K. Jain, S. Pankanti, S. Prabhakar, L. Hong, and A. Ross, "Biometrics: a grand challenge", Proc. Int'l Conf. on Pattern Recognition, vol. 2, pp. 935–942, August 2004.

[15] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition", IEEE Trans. on Circuits and Systems for Video Technology, vol. 14, pp. 4–20, Jan 2004.

[16] R. Joyce and G. Gupta. "Identity authentication based on keystroke latencies", *Communications of the ACM,* 33(2):168–176, 1990.

[17] K. S. Killourhy and R. A. Maxion, "Comparing Anomaly Detectors for Keystroke Dynamics", in Proc. 39th Annual Int'l Conf. on Dependable Systems and Networks (DSN-2009), pp. 125-134, 2009.

[18] J. Leggett and G. Williams, "Verifying Identity via Keystroke Characteristics", Int'l J. Man-Machine Studies, vol. 28, no. 1, pp. 67–76, 1988.

[19] Y. Li, B. Zhang, Y. Cao, S. Zhao, Y. Gao and J. Liu, "Study on the Beihang Keystroke Dynamics Database", Int'l Joint Conf. on Biometrics (IJCB), pp. 1-5, 2011.

[20] C. C. Loy, W. K. Lai and C. P. Lim, "Keystroke patterns classification using the ARTMAP-FD neural network", Proc. of the 3rd Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing, pp. 61-64, 2007.

[21] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer, NY, 2003.

[22] A. Messerman, T. Mustafic, S. Camtepe and S. Albayrak, "Continuous and non-intrusive identity verification in real-time environments based on free-text keystroke dynamics", Int'l Joint Conf. on Biometrics (IJCB), 2011.

[23] F. Monrose and A.D. Rubin, "Keystroke Dynamics as a Biometric for Authentication", Future Generation Computing Systems, vol. 16, no. 4, pp. 351–359, 2000.

[24] A. Peacock, X. Ke, and M. Wilkerson. "Typing patterns: A key to user identification", *IEEE Security and Privacy,* 2(5):40–47, 2004.

[25] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric Recognition: Security and Privacy Concerns", IEEE Security and Privacy Magazine, Vol. 1, No. 2, pp. 33-42, 2003.

[26] J.A. Robinson et al., "Computer User Verification Using Login String Keystroke Dynamics", IEEE Trans. Systems,

Man and Cybernetics, Part A, vol. 28, pp. 236–241, Mar. 1998.
[27] T. Sim and R. Janakiraman, "Are digraphs good for free-text keystroke dynamics? ", IEEE CVPR, pp. 17-22, 2007.
[28] E. Al Solami, C. Boyd, A. Clark, and A. K. Islam, "Continuous Biometric Authentication: Can It Be More Practical?", IEEE Int'l Conf. on High Performance Computing and Communications (HPCC), pp. 647–652, 2010.
[29] R. Spillane, "Keyboard Apparatus for Personal Identification", IBM Technical Disclosure Bulletin, vol. 17, no. 3346, 1975.
[30] D. Umphress and G. Williams, "Identity Verification through Keyboard Characteristics", Int'l J. Man-Machine Studies, Vol. 23, No. 3, pp. 263–273, 1985.
[31] U. Uludag, S. Pankanti, S. Prabhakar, and A. K.Jain, "Biometric Cryptosystems: Issues and Challenges", Proceedings of the IEEE, Special Issue on Enabling Security Technologies for Digital Rights Management, Vol. 92, No. 6, June 2004.
[32] A. Vadivel, A.K. Majumdar, and S. Sural, "Performance comparison of distance metrics in content-based image retrieval applications", Proc. of Int'l. Conf. on Information Technology, Bhubaneswar, India, pp. 159–164, 2003.
[33] J. D. Woodward, N. M. Orlans, and P. T. Higgins. "Biometrics: Identity Assurance in the Information Age", McGraw-Hill, New York, USA, 2003.
[34] R. Germain, A N. Yager and T. Dunstone. "The Biometric Menagerie", IEEE PAMI, Vol. 32, No. 2, 2010.
[35] R. V. Yampolskiy, V. Govindaraju, "Behavioral Biometrics: A Survey and Classification", Int'l J. Biometrics, Vol. 1, No. 1, 2008.
[36] E. Yu and S. Cho. "GA-SVM wrapper approach for feature subset selection in keystroke dynamics identity verification", In Proc. Int'l Joint Conf. on Neural Networks (IJCNN), pp. 2253–2257, 2003.
[37] R. Zack, C. Tappert, and S. Cha, "Performance of a long-text-input keystroke biometric authentication system using an improved k-nearest-neighbor classification method", IEEE Int'l Conf. on Biometrics: Theory Applications and Systems (BTAS), pp. 1-6, 2010.
[38] Benjamin Ngugi, Beverly K. Kahn, and Marilyn Tremaine, "Typing Biometrics: Impact of Human Learning on Performance Quality", J. *Data and Information Quality*, Vol. 2, No. 2, p. 11, 2011.