On the Discrimination Power of Dynamic Features for Online Signature

Sandipan Pal[1], Hisham Al-Assam[2] and Harin Sellahewa[3]
Department of Applied Computing, University of Buckingham, Buckingham, United Kingdom
Email: [1]sandipan.pal@buckingham.ac.uk, [2]hisham.al-assam@buckingham.ac.uk, [3]harin.sellahewa@buckingham.ac.uk

***Abstract*—The mobile market has taken huge leap in the last two decades, re-defining the rules of communication, networking, socializing and transactions among individuals and organizations. Authentication based on verification of signature on mobile devices, is slowly gaining popularity. Most online signature verification algorithms focus on computing the global Equal Error Rate across all users for a dataset. In this work, contrary to such a representation, it is shown that there are user-specific differences on the combined features and user-specific differences on each feature of the Equal Error Rate(EER) values. The experiments to test the hypothesis is carried out on the two publicly available dataset using the dynamic time warping algorithm. From the experiments, it is observed that for the MCYT-100 dataset, which yields an overall EER of 0.08, the range of user-specific EER is between 0 and 0.27.**

I. Introduction

With the rapid development of touch screen capabilities on mobile devices, virtual transactions and the need to have secure biometric authentication services have also increased. Along with facial recognition, voice recognition, one of the biometric modality that is gaining popularity recently is online signature verification. Signatures have been used to authenticate individuals for over centuries and is a legally accepted biometric trait for authenticating an individual. The fundamental advantage of the signature modality over other biometric modalities (like face, fingerprints etc.) is that it gives the user the control to change their signature in an event of a predicted impending security attack. Signatures are personalized gesture patterns within a finite space. There are two traditional approaches to signature verification: online and offline systems. In an offline system, the image attributes are matched for authenticating an individual [1] while in an online system, dynamic features like the x or y coordinates, pressure, azimuth etc. are used for verification purposes.

In this work, it is shown through experiments that different dynamic attributes of a signature contributes differently for every user. The rest of paper is arranged as follows: Section II details the background of online signature verification and the dynamic time warping (DTW) algorithm, Section III methodology of the experiments, Section IV discusses the results of the experiments and Section V consist the conclusions.

II. Background

DTW-based online signature verification algorithms have proved to be effective based on effective In this section, different approaches of online signature verification systems is discussed followed by the DTW-based approaches.

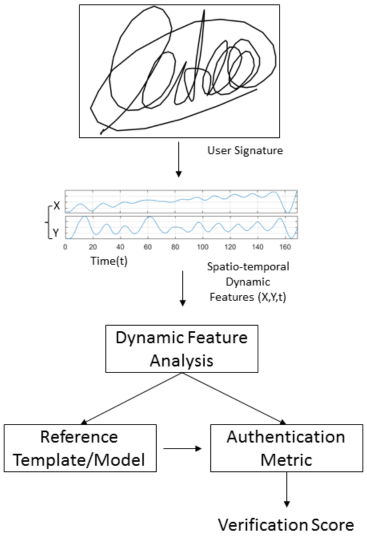

Fig. 1. A generic signature Verification algorithm

A. Online Signature Recognition

In an online signature verification system, the dynamic features of a test signature is compared against one or a set of genuine enrolled signatures to obtain a verification score and decide whether the test signature is genuine or forged as shown in Fig. 1. The dynamic features of a signature includes the positional information (i.e. the x and y coordinates) and the pressure information as temporal functions of the signing process. Often additional features like the pen-up/pen-down points, the azimuth or the inclination angle of signing are also captured depending on the hardware used. A signature is often represented as a stroke or a collection of strokes where each stroke starts with a pen-down signal and ends with a pen-up signal. One of the main challenges of any biometric based verification system is that the recogntion process depends heavily on the quality of the enrolment samples [2]. Quality of enrolment is often measured through the 'character' and 'fidelity' of a signature [3]. The character refers to the general characteristics of a signature represented by average speed, average acceleration, length of the signature etc. The fidelity of a signature represents the consistency with which an individual can replicate own signature.

Online signature verification can be broadly divided into two broad approaches, function-based and feature-based. Feature-

TABLE I
EER VALUES OF DIFFERENT DTW-BASED APPROACHED ON THE MCYT-100 DATASET

Method	EER	Reference
Kholmatov *et al.*	0.09	[9]
Faundez-Zanuy	0.05	[10]
Muramatsu *et al.*	0.10	[11]
Maiorana *et al.*	0.05	[12]
Barkoula *et al.*	0.06	[13]
Sharma *et al.*	0.02	[14]

based approaches include converting the dynamic features into a fixed length feature vector and then comparing them using using histograms [4] or distance-based functions. Though feature-based models are computationally inexpensive, the function-based approaches like dynamic time warping and hidden markov models [5] yield better accuracy as it gives a better representation of the distribution of the original data. Generative classifiers like Gaussian-mixture models as well as discriminative classifiers like Support Vector Machines [6] and multilayer neural networks [7] are used for classification in these model-based approaches.

B. DTW based online signature verification

The DTW algorithm finds its earliest application in the speech recognition algorithms where two varying lengths of speech signals are matched against one another to get a similarity score [8]. DTW has been used widely to solve the signature verification problem for nearly a decade [9] [13]. TABLE I lists the performance of the different variations of the DTW algorithm on the MCYT-100 dataset.

In [12], the authors propose a template protection scheme using a transformation function and the DTW algorithm to secure the privacy of the enrolled signatures. A local-based feature approach is adopted in [15] to distinguish between a genuine and forged signature within an authentication system. A sparse implementation of the DTW algorithm was introduced where the distance is computed on a select number of extreme points of the signature trace in [16]. The sparse implementation was improved in [17] using a string edit distance function. Another variant of the DTW implementation is introduced in [10], where the algorithm is amalgamated with a vector quantizer and classified using neural networks. Using the similar DTW-VQ strategy, authors in [14] propose an enhanced mechanism to vote a binary cost matrix along the warping path to account for the distortions between the two compared signals.

III. METHODOLOGY

The proposed hypothesis is validated through a number of experiments on 2 widely used datasets for online signature verification.

A. The Hypothesis

As mentioned in II, there are number of proposed online signature verification algorithms. As shown in TABLE I, all the algorithms report a global EER value for the whole dataset. EER values for online verification system forms the basis for choosing a threshold based on the intersection point of the false acceptance rate and the true acceptance rate for the system. Having a common global threshold for a range of users affects the performance of the verification system in real life scenarios.

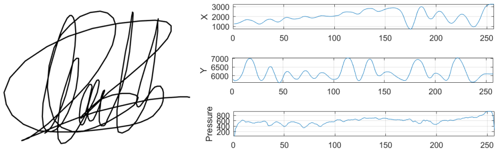

Fig. 2. A genuine signature of user number 50 of the MCYT-100 dataset

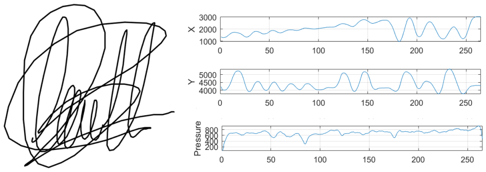

Fig. 3. A genuine signature of user number 50 of the MCYT-100 dataset

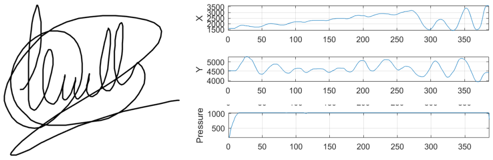

Fig. 4. A skilled forged signature of user number 50 of the MCYT-100 dataset

The hypothesis behind this work is that there are user-specific differences on the combined features and user-specific differences on each feature of the EER values. Experiments show that different features in a signature contributes different amount of information for different users. To test out hypothesis, the normalized DTW score between every pair of genuine signatures and also every pair of genuine and skilled forgery signatures is computed for each user. The EER values are computed for the whole feature matrix as one signal as well as taking individual features as individual signals to demonstrate the user-based variation within a dataset.

B. Feature Extraction

Each sample point of an individual signature(S) in the dataset is represented by a set of positional (x, y) and pressure p features. From these raw feature, a set of basic derived features are obtained at each sample point. These include the differences of x co-ordinate, y co-ordinate and the pressure between consecutive points, as well as other derived features angle, speed, velocity, acceleration *etc*.

For sample points $i = 1, 2, 3, ..., n$, where n is the total number sample points, the basic derived feature are obtained by:

$$\delta x(i) = x(i + 1) - x(i), \quad (1)$$

$$\delta y(i) = y(i+1) - y(i), \tag{2}$$

$$\delta p(i) = p(i+1) - p(i). \tag{3}$$

Hence, each sample point of a signature is represented by a three dimensional feature vector $f_i = \delta x, \delta y, \delta p$ and each signature S is represented by a feature matrix ($F_S = f_1, f_2, ..., f_{n-1}$). Each feature matrix F_S is further scaled to have a zero mean and unit variance.

C. Dynamic Time Warping

Dynamic Time Warping is an algorithm to find the similarity score and the path of alignment between a pair of time series signal of varying lengths. For two feature matrices F_A and F_B of lengths u and v respectively, a cost matrix C of dimension uxv is obtained. The (uxv)th position of the cost matrix is populated with the dissimilarity scores between the feature matrices F_A and F_B by computing the Euclidean distance between the uth sample point of F_A and the vth sample point of F_B denoted by $d(u, v)$.

One of the main aims of the DTW algorithm is to find an optimal warping path [$\mathcal{W} = (a_1, b_1), (a_2, b_2), ..., (a_{\mathcal{W}_l}, b_{\mathcal{W}_l})$], so that the distance along the warping path is minimized subjected to the boundary conditions of monotonicity and continuity with an anchored beginning [$(a_1, b_1) = (1, 1)$] and anchored ending [$(a_{\mathcal{W}_l}, b_{\mathcal{W}_l}) = (u, v)$] of the cost matrix C. The optimal minimization along the warping path is obtained by the following recursion:

$$\gamma(u, v) = d(u, v) + min \begin{cases} \gamma(u, v-1) \\ \gamma(u-1, v-1) \\ \gamma(u, v-1), \end{cases} \tag{4}$$

where γ(u,v) is the cumulative distance upto the current element. Since the length of the two feature matrices are different, the cumulative distance score of the optimal warping path is normalized over the length of the path ($\mathcal{W}_l$).

D. Dataset for testing the Hypothesis

The two popularly available datasets that are used to test the hypothesis are MCYT-100 [18] and SUSIG [19]. The MCYT-100 dataset consists of 100 individuals with 50 signatures per individual. For every user, there are 25 genuine samples and 25 skilled forgery samples. In the SUSIG dataset, there are 94 individuals with 20 genuine samples from two different sessions and 10 skilled forgery samples. Both the dataset contain the positional information (x and y coordinates) and the pressure information of each user signature trace. The temporal information in the SUSIG dataset has been ignored for this work.

IV. DISUCSSIONS

For this work, only the positional and pressure features are used for both the datasets. Fig. 2 and Fig. 3 shows 2 genuine signatures of an user within the MCYT-100 dataset. It is clearly evident that variations between the positional features and pressure features for a genuine signature are minimal. Since the warping path of the cost matrix is selected based on the minimal cost, the resultant score obtained is extremely low. If the positional features of the genuine signature is compared to the positional features of the forged signature, it can be seen here also the variations are minimal as the forged signature is done by a skilled forger. It must also be noted that between the x and y coordinate values, the y values offer more discriminative information for this user than the x values. This is mainly due to the orientation of the signature. However, when the pressure attribute is compared, it can be seen that there are minor variations between the 2 genuine signatures but the variation is major between a genuine and a forged signature. This highlights the importance of the pressure attribute for any online signature verification method. Even though the forged signature looks similar to the genuine signature and the positional features bear minor variations, it is the pressure attribute has the highest discrimination power to distinguish between the genuine and forged signature.

TABLE II
AVERAGE EER VALUES OF INDIVIDUAL DYNAMIC FEATURES OF THE MCYT-100 DATASET AND THE SUSIG DATASET

Dataset	**X**	**Y**	**P**	**Overall**
MCYT-100	0.10	0.09	0.31	0.08
SUSIG	0.21	0.18	0.38	0.47

A. User-based differences on the whole feature matrix

The overall EER for the DTW algorithm using only three dynamic features is 0.08. Though is this lower than state-of-art algorithms, in this work, it is highlighted that such a global EER value is not enough to determine the threshold of the verification system. As shown in Fig. 5, the user specific EER values, and it can be observed the for certain users, the EER is as low as 0 while the highest value is around 0.27. This signifies that the quality and robustness of the signatures of certain users are extremely high as compared to others. Even in the SUSIG dataset as shown in Fig. 6, the variations among the users are even larger with a range of 0 to 0.70 whereas the overall EER for the whole dataset is only 0.47. Though EER is only an indicative representation, computing the global EER across all users is an incorrect representation of the performance and should not be used as a basis for setting the threshold for a verification system.

B. User-based differences on individual features

On further investigation, at a feature-level, it is observed that the different features have different levels of discrimination power for different users. Table II shows the average EER across all users for individual features for both the datasets.

Table III shows the extreme variations of a few selected users of the MCYT-100 dataset. It can be observed that for users like userID 19, an EER of 0 can be achieved only with the x and y coordinate values whereas for users like userID 33, the additional pressure information is needed to achieve maximum accuracy. Again for users like userID 27 and 28, there is contribution of each of the dynamic features.

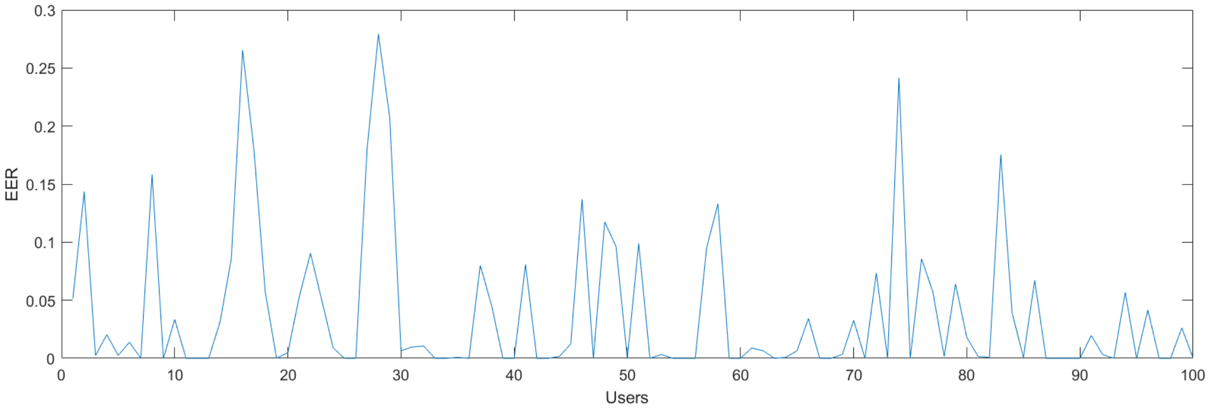

Fig. 5. EER distribution of individual users of the MCYT-100 dataset

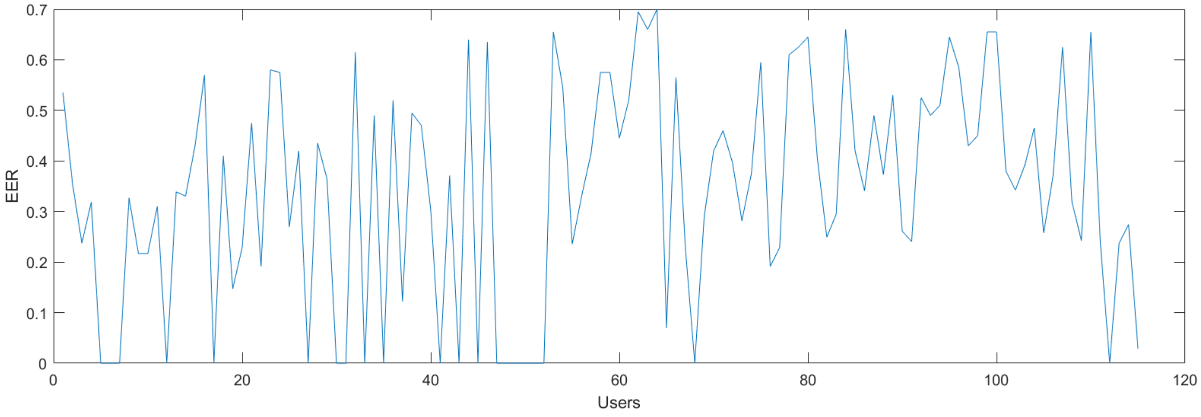

Fig. 6. EER distribution of individual users of the SUSIG dataset

Hence, it can be concluded that the dynamic features of a signature contribute different varying amount of information for different users.

User-specific threshold are being proposed in recent times [20], to have a robust solution, along with the threshold, the contribution of each feature should be user-specific and adaptive. The discriminative power of each feature varies from user to user and contributes to the biometric trait of an individual. Hence for a plausible real life solution, an adaptive weighting of features is required as opposed to having an equal weighting for each of features as advocated by all the proposed algorithms.

V. Conclusions

The hypothesis proposed that different dynamic features contribute differently for each user is tested using the DTW algorithm on two publicly available datasets. Though variations of the DTW algorithm seem to achieve good results on datasets, for real-life implementation of an authentication engine, these results are hard to replicate as a global EER value irrespective of users is not indicative of the performance of the algorithm. Experiments reveal that there are user-specific differences in the EER values at a global level as well as at feature level. Having equal contribution of dynamic features in the feature matrix does not work for all users. In future, the authors would like to investigate the use of a weighted contribution of the dynamic features for online signature verification so that an adaptive user-specific threshold could be formulated based on the quality of the enrolled genuine signatures.

TABLE III
EER VALUES OF INDIVIDUAL FEATURES OF SELECTED USERS OF THE MCYT-100 DATASET

UserID	X	Y	P	Overall
19	0	0	0.10	0
33	0.04	0.03	0.14	0
67	0.003	0	0.12	0
51	0.25	0.31	0.47	0.09
27	0.24	0.31	0.45	0.18
28	0.45	0.30	0.41	0.28

Acknowledgment

The authors would like to thank Innovate UK and Deepnet Security (www.deepnetsecurity.com) for funding this work through a Knowledge Transfer Partnership research grant.

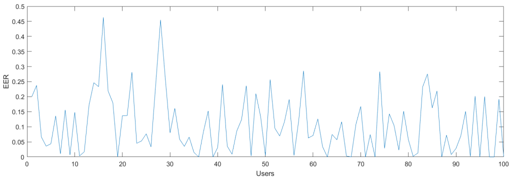

Fig. 7. EER distribution of individual users using only the x-attribute of the MCYT-100 dataset

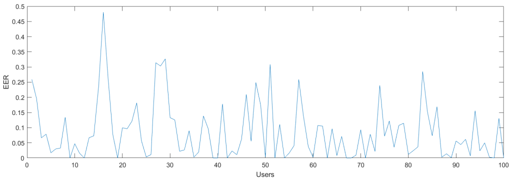

Fig. 8. EER distribution of individual users using only the y-attribute of the MCYT-100 dataset

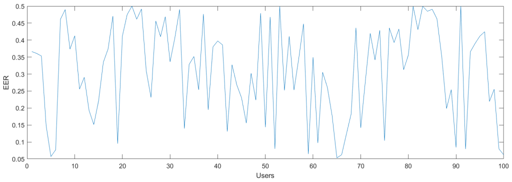

Fig. 9. EER distribution of individual users using only the pressure attribute of the MCYT-100 dataset

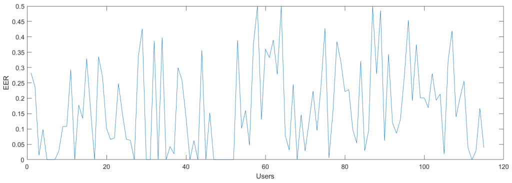

Fig. 10. EER distribution of individual users using only the x-attribute of the SUSIG dataset

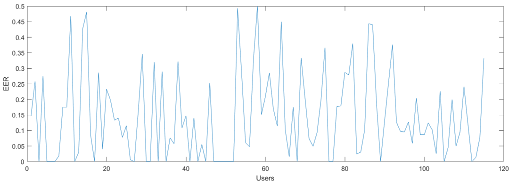

Fig. 11. EER distribution of individual users using only the y-attribute of the SUSIG dataset

References

[1] S. Y. Ooi, A. B. J. Teoh, Y. H. Pang, and B. Y. Hiew, "Image-based handwritten signature verification using hybrid methods of discrete radon transform, principal component analysis and probabilistic neural network," *Applied Soft Computing*, vol. 40, pp. 274–282, 2016.

[2] M. Liwicki, "Evaluation of novel features and different models for online signature verification in a real-world scenario," in *Proceedings of 14th Conference of the International Graphonomics Society*, 2009, pp. 22–25.

[3] S. Müller and O. Henniger, "Evaluating the biometric sample quality of handwritten signatures," in *International Conference on Biometrics*. Springer, 2007, pp. 407–414.

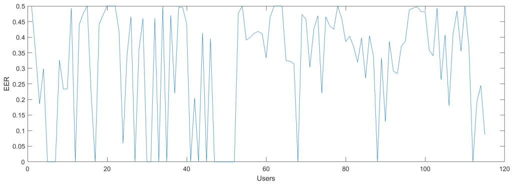

Fig. 12. EER distribution of individual users using only the pressure attribute of the SUSIG dataset

[4] N. Sae-Bae and N. Memon, "Online signature verification on mobile devices," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 6, pp. 933–947, 2014.

[5] J. Fierrez, J. Ortega-Garcia, D. Ramos, and J. Gonzalez-Rodriguez, "Hmm-based on-line signature verification: Feature extraction and signature modeling," *Pattern Recognition Letters*, vol. 28, no. 16, pp. 2325–2334, 2007.

[6] C. Gruber, T. Gruber, S. Krinninger, and B. Sick, "Online signature verification with support vector machines based on lcss kernel functions," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 40, no. 4, pp. 1088–1100, 2010.

[7] H. Baltzakis and N. Papamarkos, "A new signature verification technique based on a two-stage neural network classifier," *Engineering applications of Artificial Intelligence*, vol. 14, no. 1, pp. 95–103, 2001.

[8] L. R. Rabiner and B.-H. Juang, "Fundamentals of speech recognition," *NJ: PTR Prentice Hall*, 1993.

[9] A. Kholmatov and B. Yanikoglu, "Identity authentication using improved online signature verification method," *Pattern Recognition Letters*, vol. 26, no. 15, pp. 2400–2408, 2005.

[10] M. Faundez-Zanuy, "On-line signature recognition based on vq-dtw," *Pattern Recognition*, vol. 40, no. 3, pp. 981–992, 2007.

[11] D. Muramatsu and T. Matsumoto, *Effectiveness of Pen Pressure, Azimuth, and Altitude Features for Online Signature Verification*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 503–512.

[12] E. Maiorana, P. Campisi, and A. Neri, "Template protection for dynamic time warping based biometric signature authentication," in *Proceedings of 16th International Conference on Digital Signal Processing*. IEEE, 2009, pp. 1–6.

[13] K. Barkoula, G. Economou, and S. Fotopoulos, "Online signature verification based on signatures turning angle representation using longest common subsequence matching," *International Journal on Document Analysis and Recognition (IJDAR)*, vol. 16, no. 3, pp. 261–272, 2013.

[14] A. Sharma and S. Sundaram, "An enhanced contextual dtw based system for online signature verification using vector quantization," *Pattern Recognition Letters*, vol. 84, pp. 22–28, 2016.

[15] A. K. Jain, F. D. Griess, and S. D. Connell, "On-line signature verification," *Pattern Recognition*, vol. 35, no. 12, pp. 2963–2972, 2002.

[16] H. Feng and C. C. Wah, "Online signature verification using a new extreme points warping technique," *Pattern Recognition Letters*, vol. 24, no. 16, pp. 2943–2951, 2003.

[17] G. Gupta and R. Joyce, "Using position extrema points to capture shape in on-line handwritten signature verification," *Pattern Recognition*, vol. 40, no. 10, pp. 2811–2817, 2007.

[18] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez-Zanuy, V. Espinosa, A. Satue, I. Hernaez, J.-J. Igarza, C. Vivaracho *et al.*, "Mcyt baseline corpus: a bimodal biometric database," *IEE Proceedings-Vision, Image and Signal Processing*, vol. 150, no. 6, pp. 395–401, 2003.

[19] A. Kholmatov and B. Yanikoglu, "Susig: an on-line signature database, associated protocols and benchmark results," *Pattern Analysis and Applications*, vol. 12, no. 3, pp. 227–236, 2009.

[20] A. Sharma and S. Sundaram, "A novel online signature verification system based on gmm features in a dtw framework," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 3, pp. 705–718, 2017.