http://doi.org/10.35784/iapgos.2718

DYNAMIC HANDWRITTEN SIGNATURE IDENTIFICATION USING SPIKING NEURAL NETWORK

Vladislav Kutsman[1,2], **Oleh Kolesnytskyj**[2]

[1]TOV "Ulf-Finans", Kyiv, Ukraine, [2] Vinnytsia National Technical University, Computer Sciences Department, Vinnytsia, Ukraine

Abstract. *The article proposes a method for dynamic signature identification based on a spiking neural network. Three dynamic signature parameters l(t), xy(t), p(t) are used, which are invariant to the signature slope angle, and after their normalization, also to the signature spatial and temporal scales. These dynamic parameters are fed to the spiking neural network for recognition simultaneously in the form of time series without preliminary transformation into a vector of static features, which, on the one hand, simplifies the method due to the absence of complex computational transformation procedures, and on the other hand, prevents the loss of useful information, and therefore increases the accuracy and reliability of signature identification and recognition (especially when recognizing forged signatures that are highly correlated with the genuine). The spiking neural network used has a simple training procedure, and not all neurons of the network are trained, but only the output ones. If it is necessary to add new signatures, it is not necessary to retrain the entire network as a whole, but it is enough to add several output neurons and learn only their connections. In the results of experimental studies of the software implementation of the proposed system, it's EER = 3.9% was found when identifying skilled forgeries and EER = 0.17% when identifying random forgeries.*

Keywords: online signature identification, spiking neural network, invariant dynamic parameters, signature recognition

DYNAMICZNA IDENTYFIKACJA PODPISU ODRĘCZNEGO PRZY UŻYCIU PULSUJĄCEJ SIECI NEURONOWEJ

Streszczenie. *W artykule zaproponowano metodę dynamicznej identyfikacji podpisów opartą na pulsującej sieci neuronowej. Wykorzystywane są trzy parametry dynamiczne podpisu l(t), xy(t), p(t), które są niezmienne względem kąta nachylenia podpisu, a po ich normalizacji – także do skali przestrzennej i czasowej podpisu. Te dynamiczne parametry są podawane do sieci neuronowej w celu rozpoznania jednocześnie jako szeregi czasowe bez uprzedniej konwersji na wektor cech statycznych, co z jednej strony upraszcza metodę ze względu na brak skomplikowanych procedur konwersji obliczeniowej, a z drugiej ręka zapobiega utracie przydatnych informacji – zwiększa dokładność i wiarygodność identyfikacji i rozpoznawania podpisów (zwłaszcza w rozpoznawaniu podpisów sfałszowanych, które są silnie skorelowane z autentycznymi). Zastosowana sieć neuronowa typu spiking ma prostą procedurę treningu, przy czym nie wszystkie neurony sieci są trenowane, a jedynie te wyjściowe. Jeśli konieczne jest dodanie nowych sygnatur, nie jest konieczne trenowanie całej sieci, ale wystarczy dodać kilka neuronów wyjściowych i uczyć tylko te połączenia. W wyniku eksperymentu programowego zaproponowanego systemu otrzymano EER = 3,9% przy identyfikacji sfałszowanych podpisów i EER = 0,17% przy identyfikacji fałszerstw losowych.*

Słowa kluczowe: identyfikacja podpisu online, pulsująca sieć neuronowa, niezmienne parametry dynamiczne, rozpoznawanie podpisu

Introduction

Signature identification is a biometric authentication method and is becoming increasingly popular for a wide range of practical applications, from fraud prevention in financial transactions to access control to closed areas. Handwritten signature analysis is one of the most common methods of identifying a person, which we often encounter in our daily lives. The signature identification by a human operator has many "weaknesses". So, the operator can evaluate only the static image of the signature, as far as it corresponds to the template of the signature. At the same time, there is a danger that a well-trained attacker may very similarly forge a person's signature, i.e. the image of the signature reproduced by the attacker will be very similar to a genuine person's signature. The widespread use of computer technology and information technology for data processing allows us to apply not only the analysis of the static image of the signature, but also the dynamic characteristics of its writing.

All methods of signature identification can be divided into 2 major groups: static (Offline) signature identification and dynamic (Online) signature identification [1, 3]. Static signature identification is based on the analysis of the signature image itself and uses a variety of methods for recognizing graphic images. It is unreliable because it is easy to falsify a peep image by stroking the existing original with carbon paper, transillumination, or by scanning or photocopying. Dynamic signature identification (DSI) is more reliable, as it provides for the analysis of the author's pen oscillation parameters when reproducing the signature. In the simplest case, such parameters of the signature reproduction dynamics can be three-time functions: two functions of changing the *X(t)* coordinate and *Y(t)* coordinates of the pen oscillations in the plane of the graphics tablet and another function, changing the pen pressure on the graphics tablet *P(t).* Even if an attacker learns to reproduce a graphically similar to the original signature, it is unlikely that he will be able to accurately reproduce the dynamics of the movements of the signature author, because it is individual to each person. Therefore, the most promising is the dynamic (On-line) signature identification. In addition, it is best suited for the implementation of modern information technology and exceeds the capabilities of the human operator in this process.

Despite a large amount of research on this topic, the creation of DSI systems with the required reliability and quality of work remains problematic. The difficulties of the practical application of various DSI information technologies are caused by the shortcomings of the phenomenon of signature formation as an object of the information process. Thus, the signature of the same person due to the natural variability of human handwriting is an unstable reproducible process and has the following disadvantages [9, 13]:

- variability of geometric dimensions (spatial scale) of different signatures;
- variability of writing time (time scale) of different implementations of the signature;
- variability of the angle of inclination of the signature relative to the sides of the tablet of different signature implementations.

In addition, the signature dynamic parameters (coordinates *X(t)* and *Y(t)*, pen pressure on the graphics tablet *P(t)*, etc.) are often converted into a vector of static features, which are then used in different types of classifiers to obtain the identification result. With this conversion of dynamic parameters into static ones, useful information is often lost, which reduces the discrepancy between genuine and forged signatures and thus reduces the reliability of identification.

The purpose of the article is to present the results of the new DSI method, which is based on the use of dynamic parameters of the signature process (without converting them into static parameters) and spiking neural networks, simplifies the process and increases the reliability of signature identification.

1. The general architecture of the proposed dynamic signature identification system

The general architecture of the proposed DSI system is shown in Fig. 1. The user performs the signature writing process on a graphics tablet, which usually gives the following primary dynamic parameters of the signature: *X* and *Y* spatial coordinates, pressure, pen angular orientations (i.e., azimuth and altitude angles), and timestamps. From these primary dynamic parameters, it is often suggested to obtain secondary (derived) parameters and use them. Such secondary parameters suggest taking the speed of change of coordinates ($v_x = dX/dt, v_y = dY/dt$), the acceleration of change of coordinates ($a_x = dv_x/dt, a_y = dv_y/dt$), as well as various discrete features, such as the number of maxima, minima, convex and concave areas, etc. [1, 3, 20]. Not all dynamic parameters are taken at the same time, but certain of their optimal sets. There are even studies comparing the informativeness of different dynamic parameters and their resistance to intrapersonal variability of signatures [4, 13].

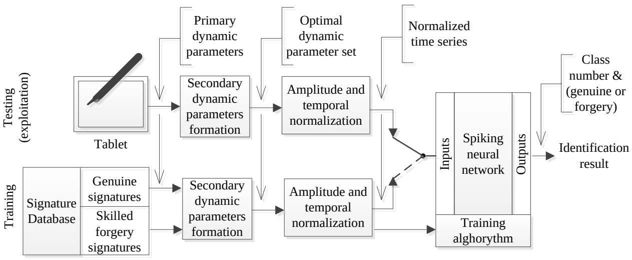
Primary dynamic parameters
Optimal dynamic parameter set
Normalized time series
Class number & (genuine or forgery)
Testing (exploitation)
Tablet
Secondary dynamic parameters formation
Amplitude and temporal normalization
Inputs
Spiking neural network
Outputs
Identification result
Training
Signature Database
Genuine signatures
Skilled forgery signatures
Secondary dynamic parameters formation
Amplitude and temporal normalization
Training alghorythm

Fig. 1. Architecture of proposed dynamic signature identification system based on Spiking Neural Networks. The Spiking Neural Networks block is enlarged in Fig. 3 for a better understanding

In this study, we used a set of 3 parameters: 1) the distance *l(t)* from the current time sample of the pen coordinates (x_i, y_i) to the next (x_{i+1}, y_{i+1}) (see Fig. 2); 2) the product of the coordinates *X(t)* and *Y(t)*; 3) pen pressure on the tablet *P(t)*. These parameters were taken because they are invariant to the slope of the signature with respect to the sides of the plate [13, 14]. And the amplitude and temporal normalization [14] indicated in Fig. 1 makes these parameters also invariant to the spatial and temporal scales of a specific signature implementation and the shift of its location on the tablet field. It should be noted that the proposed method will work with other parameters and their number, but the successful choice of parameters set has a positive effect on the overall quality of the system.

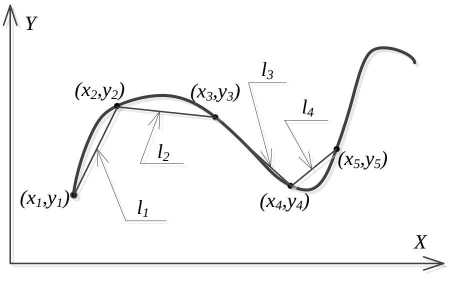

Fig. 2. Obtaining a dynamic signature parameter l(t)

After normalization, we have time series, which are sequences of digitized samples of the corresponding dynamic parameters at discrete time moments with a certain time step. These time series are fed to the input of a pre-trained spiking neural network. This is the first main difference and advantage of the proposed system, which is that the normalized dynamic parameters are fed to the spiking neural network for identification without conversion into a vector of static features, which often occurs in known systems [1, 3]. This advantage is explained by the fact that in known systems when converting dynamic parameters into static ones, a large part of useful information is lost, which reduces the reliability of identification.

The spiking neural network must be pre-trained in the task of classifying time series (dynamic parameters of the signature), so at its output, we get the result of the signature identification in the form of a class number (signatory identifier). And since the proposed spiking neural network has 2 outputs for each class (see Fig. 3), we still have information on whether the recognized signature is genuine or skilfully forged.

Genuine user signatures are used to train the spiking neural network. In principle, one genuine user signature is enough for learning, but the more genuine signatures used for learning, the more accurate the system will work. The system also provides the ability to use skilled forged signatures for training. This is optional, but also has a positive effect on the accuracy of the identification. Any database of user signatures can be used to train the system, in which the primary dynamic parameters of signatures (*X(t), Y(t)* and *P(t)*) are stored. DeepSignDB [5, 20] was used in this study.

2. The structure of the spiking neural network

In the proposed method of Online signature identification, it is necessary to use namely spiking neural networks [11, 15], because they allow recognizing dynamic signals directly, i.e. without their prior conversion into a vector of static features. They also have other benefits. All the advantages of spiking neural networks over traditional neural networks are due to their neuromorphism (similarity to networks of biological neurons) and are formulated as follows:

1) recognition of dynamic patterns (language, moving images, cardiograms, dynamic parameters of the signature, etc.) without their prior conversion into a vector of static features;
2) multitasking (information about input flows circulates in a recurrent neural network and the output can be simultaneously presented the results of different tasks using different groups of readout neurons, trained to perform a respective task);
3) predictive recognition (any dynamic process can be recognized even by incomplete information about it, i.e. even before it is finished);
4) simplicity of the learning procedure (not all neurons of the network learn, but only the output reading neurons);
5) increased productivity of information processing and noise immunity due to pulse-frequency representation of information.

The structure of the spiking neural network developed in [11] was taken as a basis for Online signature identification. The modified structure of the spiking neural network for Online signature identification and recognition is shown in Fig. 3.

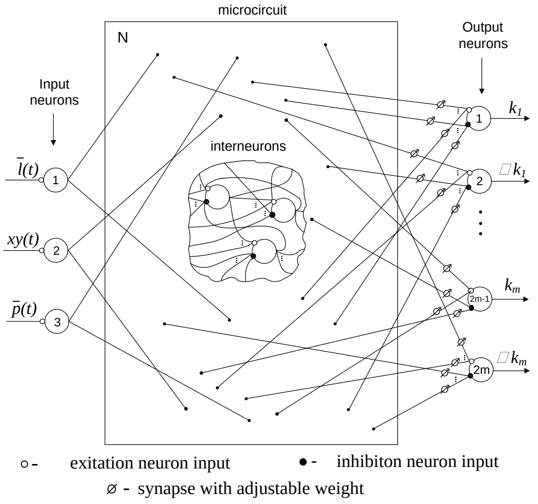

Fig. 3. The structure of the spiking neural network for online signature identification and recognition

Input spiking neurons can be constructed, for example, according to the LIF model [7]. The input neurons are fed normalized dynamic parameters of the signature *l(t), xy(t)* and *p(t)*, which are converted by the input neurons into their corresponding pulse sequences as shown in Fig. 4.

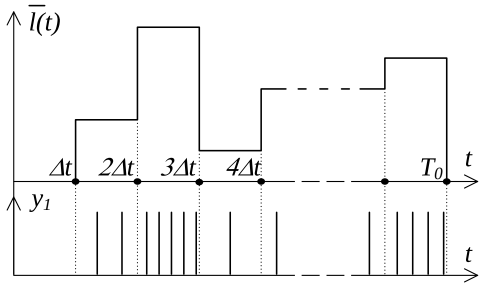

Fig. 4. Conversion of a parameter by an input spiking neuron into its output pulse signal $y_1(t)$

3. Dynamic signature identification method based on spiking neural networks

Taking into account the spiking neural network structure according to Fig. 3, as well as developed in [10] the learning rule for the spiking neural network output neurons, the principles of operation and mathematical models of spiking neurons with separate inputs [11], we can formulate a method of online signature identification and recognition using the spiking neural network.

This method is as follows:

1. Create (generate) a recurrent spiking neural network composed of interneurons in the amount of not less than $N \geq 15m$, where m is the number of classes (in this case signatures) that the network must "remember". Perform connection of neurons in the network according to neurophysiological studies [7, 15]. Choose the weights of the connections of neurons small random.
2. Generate 3 input neurons by the number of dynamic signature parameters. Connect each of them randomly with at least q neurons of the microcircuit ($n < q < N$). Choose the weights of the connections randomly.
3. Generate 2m of output neurons (2 for each template signature, first neuron to indicate a genuine signature, and second neuron to indicate a forged signature). Connect each of them randomly with at least s neurons of the microcircuit ($m < s < N$). Choose the weights of the connections randomly.
4. Apply the learning algorithm described in [10]. Only the weights of the connections of each of the 2m output neurons are adjusted. The ideal target output $k_i(t)$ can be a pulse signal with a constant (maximum) pulse frequency f_{max}, equal to the liability of the output neuron. The actual output signal *f(x(t))* will be a sequence of pulses with arbitrary time intervals between them. The input signals of the network are closer to the template signature, the higher the average for the recognition period of the pulse frequency of the output neuron, which corresponds to this template image.
5. Apply to the input of the network the investigated 3-dimensional signal (3 normalized dynamic characteristics of the signature) with duration T_0 and record which of the 2m output neurons will emit the maximum number of pulses during T_0. Namely this neuron determines the template signature, which best corresponds to the input signals of the network. The ratio of the average pulse frequency of the output neuron to f_{max} can be used as an estimate of the degree of similarity of the input signals and the template signature.

The proposed method has the following advantages:

1. The selected three dynamic parameters of the signature: *l(t), xy(t), p(t)* are invariant to the signature inclination angle, and after their normalization, even to the spatial and temporal scale of the signature;
2. Dynamic signature parameters are fed to the spiking neural network for recognition simultaneously in the form of time series without prior conversion into a vector of static features, which, on the one hand, simplifies the method due to the lack of complex computational conversion procedures, and on the other hand prevents loss of useful information. and therefore increases the accuracy and reliability of identification and recognition of signatures (especially in the recognition of forged signatures, which are strongly correlated with the genuine);
3. The result of identification and recognition can be evaluated before the end of the period of the dynamic parameters of the signature on the intense pulsing at the appropriate output (recognition with prediction), which increases the operating speed;
4. The used neural network has a light learning procedure, and not all neurons of the network are trained, but only the output ones;
5. If you need to add new signatures, you do not need to retrain the entire network completely, but just add a few output neurons and learn only their connections;
6. Noise immunity is increased due to the information coding in frequency-pulse form.

4. Experimental results

To study the performance of DSI systems, a test set is used, which includes both genuine and forged signatures, but those that were not present in the training set. Most often, the test set includes both skilled forgery and random forgery signatures, and sometimes simple forgery. Most often use one of three options. The test set includes:

1. only skilled forgery signatures,
2. only random forgery signatures,
3. both skilled forgery signatures and random forgery signatures in the proportion of 50:50.

The most interesting is, of course, the first option, because it is important to know the resistance of the system to skilled forgeries. Most DSI systems are often quite resistant to random forgeries. In this work, we used for testing 1 and 2 options.

The software implementation of the dynamic signature identification method based on the spiking neural network was carried out in the Python programming language. The TensorFlow and Keras libraries were chosen to work with neural networks in Python.

The MCYT-330 database [17], which is a part of DeepSignDB [5, 20], was chosen for the experimental study of the proposed DSI system performance. For this purpose, it would be necessary to construct a spiking neural network on Fig. 3 with the number of output neurons 660 (2 neurons for each of the 330 users of the database) and the number of interneurons not less than $330 \times 15 = 4950$ neurons. But such a network would be cumbersome to implement on a regular computer. It would take tens of hours to train it. Therefore, to accelerate the intervals of training and operation, the software of spiking neural network on Fig. 3 was implemented, which had 40 output neurons (for 20 users), 3 input neurons (for 3 dynamic signature parameters - *l(t), xy(t), p(t)*) and 400 interneurons. Simply, 12 such spiking neural networks were programmatically implemented and trained to cover 230 MCYT-330 database users selected for training. Training of one such SNN took no more than 2 hours.

The experimental protocol proposed in [5, 20] does not provide for the use of skilled forged signatures to train the DSI system. And our proposed DSI system provides such an opportunity for training. So we changed this protocol a bit. In addition, we can use more than 4 genuine signatures to train the proposed system. Therefore, changes are needed here as well.

Our protocol looks like this:

1. from the MCYT-330 database, which contains 330 users, 230 first users were selected according to the protocol [5, 20] for training and testing of our system;
2. for each user in the MCYT-330 database there are 25 genuine signatures and 25 skilled forged signatures, i.e. as a whole for selected 230 users there are 230×25 = 5750 genuine signatures and 5750 skilled forged signatures;
3. for the training of the system from every 25 genuine signatures the first 15 are chosen, and the other 10 for testing are chosen. Similarly, for training the system, out of every 25 skilled forged signatures, the first 15 were selected, and the other 10 skilled forged signatures were selected for testing;
4. thus 15×230 = 3450 genuine signatures and 3450 skilled forged signatures were selected for system training;
5. and for testing the system 10×230 = 2300 genuine signatures and 2300 skilled forged signatures were selected (testing option 1);

The results of testing the proposed DSI system based on the spiking neural network using only skilled forged signatures are given in table 1.

Table 1. Test results of the proposed DSI system based on the spiking neural network

Actual condition	Identification result	
	Signature is genuine	Signature is forged
Genuine signature (total number of genuine signatures P = 2300)	True positive – TP = 2292	False Negative – FN = 8
Skilled forged signature (total number of skilled forged signatures N = 2300)	False positive – FP = 171	True Negative – TN = 2129

We calculated the main quality indicators of the developed DSI system based on the data of table 1 when testing only on skilled forgeries – SF.

$$\text{Accuracy(SF)} = \frac{TP+TN}{TP+FP+FN+TN}\times 100\% \quad (1)$$

$$= \frac{2292+2129}{4600}\times 100\% \;= 96.1\%$$

$$\text{Precision(SF)} = \frac{TP}{TP+FP}\times 100\% \quad (2)$$

$$= \frac{2292}{2292+171}\times 100\% \;= 93.1\%$$

$$\text{Recall(SF)} = \frac{TP}{TP+FN}\times 100\% \quad (3)$$

$$= \frac{2292}{2292+8}\times 100\% \;= 99.65\%$$

The F1 Score is the weighted average of precision and recall. Therefore, this assessment takes into account both false-positive and false-negative identification results.

$$\text{F1 Score(SF)} = 2\,\frac{\text{Recall}\cdot\text{Precision}}{\text{Recall} + \text{Precision}} \quad (4)$$

$$= 2\,\frac{99.65\cdot 93.1}{99.65+93.1} \;= 96.26\%$$

We calculated 4 main quality indicators of the proposed DSI system when recognizing skilled forged signatures: accuracy 96.1%, precision 93.1%, recall 99.65%, F1 score 96.26%. To prove the achievement of the research goal, it is necessary to compare these quality indicators with the indicators of similar DSI systems [1]. This comparison is given in table 2.

Table 2 shows that the proposed system (96.1%) is better than analogs of the 1st (93.1%), 2nd (94.25%) and 5th (90.4%) rows of the table; slightly worse than the analog of the 3rd (96.5%) line. As for the 4th line, for set II (89%) our system is better, and for set I (98%) it seems worse, but in [2] it is not said how these 98% were obtained only for skilled forgeries, or only for random forgeries or both. In addition, our system and analog [2] have been studied on different databases, so the comparison may be incorrect if the complexity of signatures in the MCYT database is greater than in ATVS. Similarly, our system seems to be worse than the system in line 6 of Table 2, but again, [8] does not specify which type of forged signatures the accuracy study was performed, and the database from [8] is very small (10 + 32 people), and small signature databases usually have worse quality and complexity of signatures than large. Therefore it is necessary to compare our system with that which was investigated on the same DB and under the same (or at least similar) conditions of a choice of test signatures.

In [20], several recent developments of dynamic signature verification systems based on recurrent neural networks are considered. There are 3 approaches compared:

1. based on Dynamic Time Warping (DTW),
2. based on Recurrent Neural Networks (RNN),
3. based on Time-Aligned Recurrent Neural Networks (TA-RNN).

They are used to assess the quality of the DeepSignDB database [5, 20], where the MCYT database is included. Although these are not identification but verification systems, they can still be compared by drawing an analogy between the quality indicators of signature verification and signature identification systems.

Table 2. Comparison of quality indicators of known DSI systems with the proposed system based on the spiking neural network

	Reference	Dataset	Extracted features	Classifier	Evaluation
1	[6] 2007	SVC 2004 dataset	Basic functions, Geometric normalization, Extended functions, Time derivatives, Signal normalization	Hidden Markov Models (HMM)	6.9% (equivalent accuracy 93,1%) and 3.02% EER to skilled and random forgeries respectively
2	[19] 2011	Small dataset of 27 users	Graph theory	Graph norm	94.25% accuracy
3	[16] 2013	SVC	Wavelet transform	Neural network (NN)	3.5% EER (equivalent accuracy 96,5 %)
4	[2] 2015	Two sets of ATVS dataset are collected, dataset I contains 25 signature samples per each writer. Dataset II contains 46 signature samples per each writer	9 global features	Feed forward neural network	98% accuracy for dataset I and 89% accuracy for dataset II
5	[18] 2018	dataset consists of 10 writers with 10 genuine signatures and 10 forged signatures per each user	Extracted some features as (coordinates, pressure, altitude and azimuth) which are functions of time t	DTW algorithm was used to calculate warping distance	This system can detect fake signatures with an accuracy of 90.4%.
6	[8] 2018	Two datasets, the first dataset contains 240 signatures that were taken from ten writers and the second dataset contains 768 signatures that were taken from 32 writers	Using speed up robust features (SURF)	Support vector machine (SVM)	98.75% accuracy for the first dataset and 97.7% accuracy for the second dataset
7	Our system	DeepSignDB (MCYT-330)	*l(t), X(t)×Y(t), p(t)*	Spiking neural network	accuracy 96.1% to skilled forgeries

EER – equal error rate

Quality indicators of signature verification and identification systems are related by the formula [1]:

$$\text{Accuracy} = 100 - EER \tag{5}$$

since both EER and Accuracy take into account indicators such as FP and FN. Since for the developed system Accuracy = 96.1%, we can assume that EER = 3.9. Table 3 shows that the best value among the known systems is TARNN – 4.3%.

The quality indicators of the known systems [20] and the proposed DSI system are given in tables 3 and 4.

Table 3 shows that the developed system when testing on skilled forgeries has an EER = 3.9%, and the best known (TARNN) – has an EER = 4.3%, i.e. the developed system is better by 0.4% (absolute) accuracy than the TARNN system, and in relative units, it is (0.4/4.3)·100% = 9%. As for testing on random forgeries, Table 4 shows that the developed system has an EER = 0.17%, and the best known (TARNN) has an EER = 0.2%, i.e. the developed system has a better accuracy of 0.03% (absolute value) than the TARNN system, and in relative units, it is (0.03/0.17)·100% = 15%. In general, in relative terms, the proposed system is better than the reference system by 9% when tested on skilled forgeries and 15% when tested on random forgeries.

Table 3. Comparison of the quality (EER) of the known signature verification systems with the proposed system when tested on skilled forgeries

	Skilled Forgeries						
	1 training signature			4 training signatures			15 training signatures
	DTW	RNN	TA-RNN	DTW	RNN	TA-RNN	Proposed system
MCYT	9.1	10.5	4.4	7.2	10.1	4.3	3.9
BiosecurID	8.1	3.9	1.9	6.5	3.4	1.3	
Biosecure DS2	14.2	8.0	4.2	12.1	7.4	3.0	
eBS DS1 w1	15.3	11.4	5.4	9.3	9.0	4.3	
eBS DS1 w2	12.0	8.2	4.0	11.4	7.1	2.9	
eBS DS1 w3	14.5	14.3	5.4	12.1	11.4	4.8	
eBS DS1 w4	14.6	13.2	5.8	11.4	12.1	5.2	
eBS DS1 w5	14.9	18.9	10.6	12.9	14.0	8.0	
eBS DS2 w2	9.6	3.9	3.7	8.3	2.9	2.8	
DeepSignDB	11.2	8.5	4.2	9.3	7.9	3.3	

Table 4. Comparison of the quality (EER) of the known signature verification systems with the proposed system when tested on random forgeries

	Random Forgeries				
	1 training signature		4 training signatures		15 training signatures
	DTW	TA-RNN	DTW	TA-RNN	Proposed system
MCYT	1.2	1.1	0.6	0.2	0.17
BiosecurID	1.0	0.6	0.6	0.1	
Biosecure DS2	2.5	1.9	1.6	1.1	
eBS DS1 w1	3.2	2.5	0.7	0.1	
eBS DS1 w2	1.3	1.7	0.7	1.4	
eBS DS1 w3	0.9	1.6	0.3	0.4	
eBS DS1 w4	1.1	1.4	0.7	0.9	
eBS DS1 w5	2.7	4.1	2.1	1.4	
eBS DS2 w2	2.7	2.2	0.7	0.9	
DeepSignDB	1.8	1.5	1.1	0.6	

5. Prospects for further research

Further research can be divided into the following 2 general areas:

1. research in terms of analysis and synthesis of effective dynamic parameters of the signature and their pre-processing,
2. research in terms of finding new and improving known methods and means of classifying time series, which are the dynamic parameters of the signature.

In the course of the research, it was found that a good influence on the result of identification has a successful choice of a set of dynamic parameters of the signature, which are submitted to the classifier. It is necessary to continue the study of informativeness and variability of various dynamic parameters of the signature in the following areas:

- look for more informative dynamic parameters of the signature, having adequate metrics of informativeness,
- look for dynamic signature parameters that have low intrapersonal variability, having adequate metrics of intrapersonal variability,
- look for dynamic signature parameters that have high interpersonal variability, having adequate metrics of interpersonal variability.

The question also remains relevant: how many optimal dynamic parameters should be chosen and which ones to achieve the maximum reliability of dynamic identification of signatures at a minimum cost? On the one hand, the more parameters you take, the more accurate the system should be. But, on the other hand, processing a large number of parameters requires more computing resources and more time to make a decision. It is also not clear whether it is justified to choose a large number of parameters, as they are not all independent, as they are calculated from four primary parameters (*x(t), y(t), p(t)* and *γ(t)*).

Therefore, the task of further research is to study the degree of influence of individual dynamic parameters of the signature on the overall reliability of the process of signature identification and justification of the optimal sets of dynamic parameters of the signature.

In the course of the research, it was noticed that the dynamic parameters of the signature are more stable in some areas (time intervals) and less stable in others. Therefore, logically, the idea arises to highlight such areas in the analysis of different implementations of the user's signature and then use only them, and not the entire signature in the identification. This possibility is provided by the metric proposed in [21] for finding the similarity of time series, which is called Longest Common Sub-Sequences - LCSS.

In terms of finding new and improving known methods and means of classifying time series, you need to pay more attention to methods that do not require the conversion of dynamic parameters into static vectors or descriptors, because it loses useful information. Such methods are methods using recurrent and spiking neural networks. Therefore, in particular, it is necessary to improve the structure and learning methods of spiking neural networks.

6. Conclusions

1. The article proposes a method of dynamic (Online) signature identification based on a spiking neural network. The structure of the network is original and uses spiking neurons with separate inputs of excitation and inhibition [11]. A feature of the network structure is also the use of 2 output neurons for each signature, first, to indicate a genuine signature, and second to indicate a skilled forged signature.
2. To represent the signature, the choice of the following three dynamic parameters of the signature is substantiated: 1) *l(t)* – the distance between adjacent discrete signature points, 2) *xy(t)* – the product of the coordinates *X(t)* and *Y(t)*; 3) *p(t)* – pen pressure on the graphics tablet. These dynamic parameters are invariant to the signature writing angle, and after their normalization even to the spatial and temporal scales of the signature.
3. The selected dynamic parameters of the signature are fed to the spiking neural network for recognition without prior conversion into a vector of static features, which simplifies the method due to the lack of complex computational conversion procedures, and prevents the loss of useful information, and therefore increases the accuracy (especially when recognizing forged signatures, which are strongly correlated with the genuine).

4. The proposed spiking neural network has a simple learning procedure. In addition, if you need to add new signatures, you do not need to retrain the entire network, but just add a few output neurons and learn only their connections. This network is also the basis of modern neurocomputer architectures [12].
5. The software implementation of the proposed method was experimentally evaluated. It turned out that the developed system when testing on skilled forged signatures has EER = 3.9%, and the best known (TARNN) has EER = 4.3%. As for random forgeries testing, the developed system has an EER = 0.17%, and the best known (TARNN) has an EER = 0.2%.

References

[1] Al-Banhawy N. H., Mohsen H., Ghali N. I.: Signature identification and verification systems: a comparative study on the online and offline techniques. Future Computing and Informatics Journal 5(1), 2020, article 3 [https://digitalcommons.aaru.edu.jo/fcij/vol5/iss1/3]

[2] Babita P.: Online Signature Recognition Using Neural Network. Journal of Electrical & Electronics 4(3), 2015, 1.

[3] Diaz M., Ferrer M. A., Impedovo D., Malik M. I., Pirlo G., Plamondon R.: A Perspective Analysis of Handwritten Signature Technology. ACM Comput. Surv. 51(6), 2019, article 117.

[4] Doroshenko T. Y., Kostyuchenko E. Y: The authentication system based on dynamic handwritten signature. TUSUR 2(32), 2014, 219–223.

[5] Fierrez J., Galbally J., et al.: BiosecurID: A Multimodal Biometric Database. Pattern Analysis and Applications 13(2), 2010, 235–246.

[6] Fierrez J., Ortega-Garcia J., Ramos D., Gonzalez-Rodriguez J.: Hmm-Based On-Line Signature Verification: Feature Extraction And Signature Modeling. Pattern Recognition Letters 28(16), 2007, 2325–2334.

[7] Gerstner W., Kistler W.: Spiking Neuron Models: Single Neurons, Populations, Plasticity. Cambridge University Press, Cambridge 2002. [http://doi.org/10.1017/CBO9780511815706].

[8] Hamadly I., Khaleel A., Munim A., Hassan H. E., Mohamed H. K.: Online Signature Recognition And Verification Using (SURF) Algorithm With SVM Kernels. Journal of Al-Azhar University Engineering Sector 13(49), 2018, 1332–1344.

[9] Houmani N., Garcia-Salicetti S., Dorizzi B.: On assessing the robustness of pen coordinates, pen pressure and pen inclination to time variability with personal entropy. IEEE 3rd Int. Conf. on Biometrics: Theory, Applications, and Systems 2009, 1–6.

[10] Kolesnytskij O. K., Samra Muavija Hassan Hamo: A method for recognizing multidimensional time series using pulsed neural networks. Information technology and computer engineering 2(6), 2006, 86–93.

[11] Kolesnytskyj O. K., Bokotsey I. V., Yaremchuk S. S.: Optoelectronic Implementation of Pulsed Neurons and Neural Networks Using Bispin-Devices. Optical Memory & Neural Networks (Information Optics) 19(2), 2010, 154–165.

[12] Kolesnytskyj O. K., Kutsman V. V., Skorupski K., Arshidinova M.: Neurocomputer architecture based on spiking neural network and its optoelectronic implementation. Proc. SPIE 11176, 2019, 1117609 [http://doi.org/10.1117/12.2536607].

[13] Kutsman V. V., Kolesnytskyj O. K., Denysov I. K.: Investigation of intrapersonal and interpersonal variability of dynamic signature parameters in the process of their identification, Optoelectronic Information-Power Technologies 39(2), 2020, 5–15.

[14] Kutsman V. V., Kolesnytskyj O. K.: Signature verification and recognition as a multiparametric process based on a spiking neural network. Information technologies and computer engineering 50(1), 2021, 36–44 [http://doi.org/10.31649/1999-9941-2021-50-1-36-44].

[15] Maass W.: Networks of spiking neurons: the third generation of neural network models. Neural Networks 10, 1997, 1659–1671.

[16] Nilchiyan M. R., Yusof R. B.: Improved Wavelet-Based Online Signature Verification Scheme Considering Pen Scenario Information. IEEE 1st International Conference on Artificial Intelligence, Modelling and Simulation 2013, 8–13.

[17] Ortega-Garcia J., Fierrez J., et al.: MCYT Baseline Corpus: A Bimodal Biometric Database. IEEE Proc. Vision, Image and Signal Processing 150(6), 2003, 395–401.

[18] Patil B. V., Patil P. R.: An Efficient DTW Algorithm For Online Signature Verification. IEEE International Conference on Advances in Communication and Computing Technology (ICACCT) 2018, 1–5.

[19] Pavlidis I., Papanikolopoulos N. P., Mavuduru R.: Signature Identification Through The Use Of Deformable Structures. Signal Processing 71(2), 1998, 187–201.

[20] Tolosana R., Vera-Rodriguez R., Fierrez J., Ortega-Garcia J.: DeepSign: Deep On-Line Signature Verification. arXiv preprint arXiv: 2002.10119, 2020.

[21] Vlachos M., Kollios G., Gunopulos D.: Discovering similar multidimensional trajectories. Proceedings 18th International Conference on Data Engineering 2002, 673–684.

M.Sc. Vladislav Kutsman
e-mail: kutsmanvlad@gmail.com

Software Engineer TOV "Ulf-Finans", Kyiv, Ukraine, Ph.D. student in Vinnytsia National Technical University, Computer Sciences Dpt., Research interests: artificial intelligence, neural networks, spiking neural networks, neurocomputers.

http://orcid.org/0000-0001-5256-9651

Ph.D. Oleh Kolesnytskyj
e-mail: kolesnytskiy@vntu.edu.ua

Ph.D., associate professor, Vinnytsia National Technical University, Computer Sciences Dpt., Vinnytsia, Ukraine.
Research interests: artificial intelligence, neural networks, spiking neural networks, neurocomputers.

http://orcid.org/0000-0003-0336-4910

otrzymano/received: 24.08.2021 *przyjęto do druku/accepted: 15.09.2021*