УДК 004.056.5
DOI https://doi.org/10.32838/2663-5941/2019.6-1/30

Терейковська Л.О.
Київський національний університет будівництва і архітектури

МЕТОД ВИЗНАЧЕННЯ ВИДУ ЗГОРТКОВОЇ НЕЙРОННОЇ МЕРЕЖІ ДЛЯ АНАЛІЗУ ПАРАМЕТРІВ КЛАВІАТУРНОГО ПОЧЕРКУ

Статтю присвячено проблемі створення засобів прихованого моніторингу особи та емоційного стану користувачів інформаційних систем. Визначено перспективність засобів моніторингу на основі аналізу клавіатурного почерку, побудованих із використанням згорткових нейронних мереж. Також показана недостатня адаптація наявних нейромережевих засобів до значних умов поставленого завдання аналізу клавіатурного почерку. Запропоновано виправити вказаний недолік за рахунок розроблення методу визначення найбільш ефективного виду згорткової нейронної мережі. У результаті проведених досліджень обґрунтована можливість розгляду завдання розроблення зазначеного методу як багатокритеріальної оптимізації нейромережевих засобів захисту інформації. Розроблено метод визначення найбільш ефективного виду згорткової нейронної мережі, призначеної для аналізу клавіатурного почерку. Етапи методу співвідносяться з визначенням вагових коефіцієнтів критеріїв ефективності, розрахунком значення функції ефективності для кожного допустимого виду нейромережевої моделі, визначенням виду моделі з максимальним значенням функції ефективності та верифікацією отриманих результатів. За допомогою запропонованого методу визначено, що в умовах обмеженого доступу до баз даних параметрів клавіатурного почерку, наявності доступного і апробованого інструментарію для реалізації нейромережевих засобів, прийнятної ресурсоємності програмно-апаратної реалізації, прийнятних термінів навчання і розпізнавання, а також достатньої точності розпізнавання найбільш ефективним видом згорткової нейронної мережі є SqueezeNet. У результаті комп'ютерних експериментів розраховано, що точність розпізнавання особи за допомогою SqueezeNet приблизно на 10-11% перевищує точність розпізнавання за допомогою інших видів згорткових нейронних мереж, що підтверджує ефективність розробленого методу. Запропоновано співвіднести шляхи подальших досліджень з адаптацією параметрів SqueezeNet до умов завдання аналізу клавіатурного почерку.

Ключові слова: *клавіатурний почерк, ідентифікація особи, розпізнавання емоцій, згорткова нейронна мережа, засоби розпізнавання.*

Постановка проблеми. У сучасних умовах одним із найбільш актуальних завдань в області розроблення інформаційних систем як загального, так і спеціального призначення є створення високоефективних засобів прихованого моніторингу особистості та емоційного стану користувача [1; 4]. Такі засоби необхідні, наприклад, у системах дистанційного навчання для оптимізації подачі навчального матеріалу та ідентифікації слухачів під час тестування або в банківських інформаційних системах для попередження шахрайських дій під час отримання позик (фродскоринг). При цьому до основних переваг засобів моніторингу на основі аналізу клавіатурного почерку (КП) відносять: складність підроблення, невідчужуваність від особи користувача, можливість реєстрації параметрів із використанням тільки стандартного периферійного обладнання, а також широке застосування в інформаційних системах парольних і технологічних даних у вигляді набору символів [8; 9]. Хоча розробленню таких систем присвячено досить велику кількість науково-практичних робіт, проте дані [2; 6] свідчать про необхідність подальшого підвищення їх ефективності, що і зумовлює актуальність досліджень у даному напрямку.

Аналіз останніх досліджень і публікацій. Під поняттям КП зазвичай розуміють індивідуальну біометричну поведінкову характеристику особи, що визначає особливості набору тексту із клавіатури [2; 3]. Основними часовими параметрами КП є термін утримання клавіші (ТУК), термін між послідовним натисканням двох клавіш (ТМК) та відношення цих параметрів (ВТ). Крім того, можуть розраховуватись значення динаміки ТУК та ТМК. Розрахунок цих параметрів реалізується за допомогою виразів:

$$\tau_r(i) = t_u(i) - t_d(i), \quad (1)$$

$$\tau_b(i, i-1) = t_u(i) - t_d(i-1), \quad (2)$$

$$q_{br}(i, i-1) = \frac{\tau_b(i, i-1)}{\tau_r(i)}, \quad (3)$$

$$v_r(i, i-1) = \frac{\tau_r(i) - \tau_r(i-1)}{\tau_r(i)}, \quad (4)$$

$$v_b(i, i-1) = \frac{\tau_b(i) - \tau_b(i-1)}{\tau_b(i)}, \quad (5)$$

де τ_r – ТУК; t_d, t_u – час натиснення та відпускання клавіші; τ_b – ТМК; i – номер натиснення клавіші; q_{br} – ВТ; v_r, v_b – динаміка ТУК та ТМК.

У [1; 9] визначена доцільність аналізу параметрів КП за допомогою нейронних мереж, яка пояснюється доведеною ефективністю таких моделей для оперативного аналізу великого обсягу багатовимірних даних, що є характерною особливістю означеної задачі. Також результати [6; 8; 9] свідчать про перспективність застосування згорткових нейронних мереж (ЗНМ) для розпізнавання емоційного стану особи за КП. Так, у [8] розроблена ЗНМ типу LeNet, призначена для розпізнавання емоційного стану особи за КП. Крім того, в [3; 8] розроблені процедури представлення параметрів КП у вигляді квадратного кольорового або чорно-білого зображення, що нівелює труднощі, пов'язані з кодуванням вказаних параметрів. Хоча результати наведених досліджень і свідчать про ефективність розроблених ЗНМ, однак у цих же дослідженнях обґрунтована необхідність вдосконалення архітектури ЗНМ для підвищення точності розпізнавання та адаптації до значущих умов поставленої задачі аналізу КП. Разом із тим результати [1–3; 6; 8] вказують на відсутність методу розроблення архітектури ЗНМ, призначеної для аналізу параметрів клавіатурного почерку, що зумовлює необхідність проведення складних та ресурсоємних досліджень, спрямованих на визначення параметрів вказаної архітектури. При цьому першим етапом розроблення нейромережевої архітектури є визначення виду НММ, який є найбільш ефективним в умовах поставленої задачі.

Постановка завдання. Основною метою публікації є розроблення методу визначення виду згорткової нейронної мережі, що призначена для ідентифікації та розпізнавання емоційного стану особи на базі аналізу клавіатурного почерку.

Виклад основного матеріалу дослідження. Відповідно до поширеної методології побудови нейромережевих засобів захисту інформації [4; 5; 10] аналітичну модель методу визначення найбільш ефективного виду ЗНМ можливо записати у вигляді таких виразів:

$$\max_{V_i} = \{ V_1, V_2, .. V_I \}, \quad (6)$$

$$V_i = \sum_{k=1}^{K} \alpha_k R_k(n_i), \quad n_i \in N_d, \ i = 1, ...I. \quad (7)$$

де I – кількість допустимих видів ЗНМ; V_i – функція ефективності і-ої ЗНМ; $\alpha_k = [0..1]$ – ваговий коефіцієнт k-го критерію ефективності; n_i – і-ий вид ЗНМ; N_d – множина допустимих видів ЗНМ; K – кількість критеріїв ефективності; $R_k(n_i)$ – значення k-го критерію для і-го виду ЗНМ.

При цьому методологія передбачає, що адаптація процесу побудови нейромережевих засобів полягає у визначенні множини допустимих видів ЗНМ та у формуванні множини значимих критеріїв ефективності.

Відправною точкою вибору допустимих видів ЗНМ послужили результати досліджень в області теорії нейронних мереж [5; 7]. На підставі вказаних досліджень сформовано множину допустимих видів ЗНМ:

$$N_d = \{ n_{AN}, n_{Of}, n_{VG}, n_{Ic}, n_{Gn}, n_{MN}, n_{RN}, n_{Nn}, n_{EN}, n_{SN} \}, \quad (8)$$

де n_{AN} – AlexNet, n_{Of} – Overfeat, n_{VG} – VGG, n_{Ic} – Inception, n_{Gn} – GoogleNet, n_{MN} – MobileNet, n_{RN} – ResNet, n_{Nn} – Network-in-network, n_{EN} – ENet и n_{SN} – SqueezeNet.

Також визначено, що критерії ефективності повинні відображати пристосованість виду ЗНМ до умов поставленої задачі. Базуючись на практичному досвіді та результатах [1; 2], визначено, що основні вимоги до ЗНМ, які призначені для аналізу КП, пов'язані з формуванням навчальної вибірки, програмно-апаратною реалізацією мережі, процесом навчання та процесом розпізнавання. Також на підставі сформованих вимог до ЗНМ і [4; 10] визначено, що найбільш важливими критеріями ефективності виду ЗНМ є: R_1 – наявність доступних баз даних параметрів КП, R_2 – наявність доступного і апробованого інструментарію для реалізації ЗНМ, R_3 – прийнятна ресурсоємність програмно-апаратної реалізації, R_4 – прийнятний час навчання мережі, R_5 – прийнятний час розпізнавання, R_6 – достатня точність розпізнавання. Значення представлених в табл. 1 критеріїв ефективності для кожного допустимого виду ЗНМ визначені експертним шляхом.

Визначення множин допустимих видів ЗНМ та критеріїв ефективності дозволило запропонувати метод визначення найбільш ефективного виду ЗНМ, що складається з таких етапів:

1. Визначення вагових коефіцієнтів критеріїв ефективності. Для цього слід проаналізувати особливості умов поставленої задачі розпізнавання.

2. За допомогою виразу (7) розрахувати значення функції ефективності для кожного допустимого виду ЗНМ.

Таблиця 1

Критерії ефективності для різних видів згорткових нейронних мереж

Вид ЗНМ	Критерії ефективності					
	R_1	R_2	R_3	R_4	R_5	R_6
n_{AN}	0,5	0,7	0,5	0,7	0,9	0,7
n_{Of}	0,5	0,7	0,5	0,7	0,9	0,6
n_{VG}	0,5	0,7	0,5	0,7	0,9	0,7
n_{Ic}	0,5	0,7	0,5	0,7	0,9	0,7
n_{Gn}	0,5	0,7	0,5	0,7	0,9	0,7
n_{MN}	0,5	0,7	0,9	0,8	0,8	0,8
n_{RN}	0,5	0,7	0,8	0,7	0,9	0,7
n_{Nn}	0,5	0,7	0,8	0,7	0,9	0,7
n_{EN}	0,7	0,9	0,9	0,8	0,7	0,8
n_{SN}	0,7	0,9	0,9	0,9	0,8	0,8

Таблиця 2

Значення функції ефективності для різних видів ЗНМ

n_{AN}	n_{Of}	n_{VG}	n_{Ic}	n_{Gn}	n_{MN}	n_{RN}	n_{Nn}	n_{EN}	n_{SN}
0,6	0,59	0,6	0,6	0,6	0,73	0,69	0,69	0,8	0,82

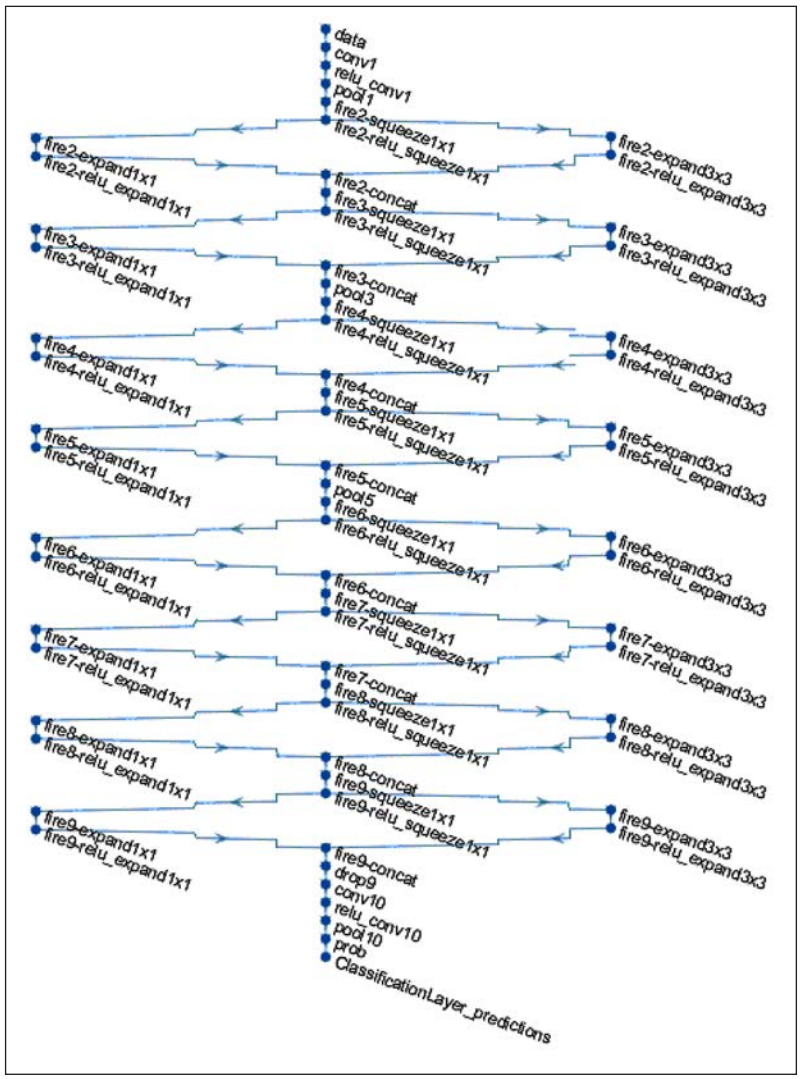

Рис. 1 Структура згорткової нейронної мережі SqueezeNet

3. Визначити найбільш ефективний вид ЗНМ. Для цього слід за допомогою виразу (6) розрахувати той вид ЗНМ, для якого значення функції ефективності є максимальним.

4. Провести верифікацію отриманих результатів.

Для перевірки доцільності використання запропонованого методу проведені експериментальні дослідження, спрямовані на визначення особи та емоційного стану користувача на основі аналізу параметрів КП. Прийняті такі умови використання ЗНМ: кількість осіб, що мають бути розпізнані, – 10; мають бути розпізнані 3 емоції (нейтральність, радість, страх); КП аналізується для текстів довжиною 12 символів; підлягають аналізу параметри ТУК, ТМК та динаміка ТУК. Найбільш суттєві обмеження поставленої задачі розпізнавання пов'язані з доступом до представницьких баз даних навчальних прикладів та обсягом обчислювальних ресурсів.

Відповідно до етапу 1 експертним шляхом визначені вагові коефіцієнти критеріїв ефективності: $\alpha_1=\alpha_3=0,3;$ $\alpha_2=\alpha_4=\alpha_5=\alpha_6=0,1$, а розраховані відповідно етапу 2 значення функції ефективності наведені в табл. 2.

Відповідно до етапу 3 визначено, що найбільш ефективним видом ЗНМ є SqueezeNet, для якого значення функції ефективності є максимальним.

Відповідно етапу 4 проведені експериментальні дослідження, спрямовані на підтвердження ефективності SqueezeNet. ЗНМ була реалізована за допомогою пакету прикладних програм MATLAB 2018. Структура мережі, візуалізована за допомогою вбудованої у програмний комплекс MATLAB R2018 функції plot, показана на рис. 1. За аналогією з [3; 6] для навчання SqueezeNet використана база даних відфільтрованих зразків КП, що відповідають трьом вказаним емоціям для 10 осіб. У результаті проведених експериментів визначено, що в середньому точність розпізнавання особи за допомогою SqueezeNet становить приблизно 92,8%, а точність розпізнавання емоцій становить приблизно 79,5%, що приблизно на 10-11% більше, ніж точність розпізнавання за допомогою

ЗНМ виду LeNet [3, 6], що і підтверджує ефективність запропонованого методу. Зазначимо, що підвищити точність розпізнавання емоцій можна за рахунок збільшення обсягу навчальної вибірки та за рахунок адаптації параметрів SqueezeNet до поставленої задачі розпізнавання, що окреслює перспективи подальших досліджень в напрямку застосування ЗНМ для аналізу КП.

Висновки. Розроблено метод визначення виду згорткової нейронної мережі, що за рахунок застосування запропонованих критеріїв ефективності дозволяє обрати вид мережі, найбільш ефективний в умовах задачі ідентифікації та розпізнавання емоційного стану особи на базі аналізу клавіатурного почерку. За допомогою запропонованого методу розроблена нейромережева модель SqueezeNet, точність якої приблизно на 10-11% вища, ніж точність інших видів згорткових нейронних мереж, що можуть бути використані за обмежених обчислювальних ресурсах та у випадку обмеженого доступу до навчальних баз даних. Показано доцільність співвіднесення подальших досліджень з адаптацію параметрів SqueezeNet до умов задачі аналізу клавіатурного почерку.

Список літератури:

1. Кошевая Н.А., Мазниченко Н.И. Подход к повышению надежности идентификации пользователей компьютерных систем по динамике написания паролей. *Системи обробки інформації*. 2014. Вип. 6(122). С. 140–146.

2. Савинов А.Н. Методы, модели и алгоритмы распознавания клавиатурного почерка в ключевых системах : автореф. дис. … канд. техн. Наук : 05.13.19 – Методы и системы защиты информации, информационная безопасность. Санкт-Петербург, 2013. 19 с.

3. Терейковська Л.О. Нейромережева модель розпізнавання емоційного стану операторів автоматизованих робочих місць за клавіатурним почерком. *Вчені записки Таврійського національного університету імені В.І. Вернадського, серія «Технічні науки»*. 2019. Т. 30(69). Ч. 1. № 4. С. 129–133.

4. Терейковский И.А., Терейковская Л.А., Корченко А.О., Ахметов Б.Б. Нейросетевое распознавание рукописных символов в системе биометрической аутентификации. *Інформаційні технології в економіці та природокористуванні*. 2017. № 2. С. 29–44.

5. Akhmetov B., Tereykovsky I., Doszhanova A., Tereykovskaya L., Adranova, A. Determination of input parameters of the neural network model, intended for phoneme recognition of a voice signal in the systems of distance learning. *International Journal of Electronics and Telecommunications*. 2018. Volume 64. P. 425–432.

6. Epp C., Lippold M., Mandryk R.: Identifying Emotional States Using Keystroke Dynamics. *In Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems*. Vancouver, BC, Canada: ACM. 2011. P. 715–724.

7. Iandola F.N., Han S., W. Moskewicz M.W. SqueezeNet: AlexNet level accuracy with 50x fewer parameters and <0.5MB model size. *arXiv:1602.07360v4.* 2016. 13:81. URL : https://arxiv.org/pdf/1602.07360.pdf.

8. Liu. M., Guan. J. User keystroke authentication based on convolutional neural network. *Communications in Computer and Information Science.* 2019. Volume 971. P. 157–168.

9. Preeti Khanna, M.Sasikumar. Recognising Emotions from Keyboard Stroke Pattern. *International Journal of Computer Applications (0975 – 8887).* 2010.Volume 11. No.9. P. 1–5.

10. Tereykovska L., Tereykovskiy I., Aytkhozhaeva E., Tynymbayev S., Imanbayev A. Encoding of neural network model exit signal, that is devoted for distinction of graphical images in biometric authenticate systems. *News of the national academy of sciences of the republic of Kazakhstan series of geology and technical sciences.* 2017. Volume 6. No. 426. P. 217–224.

Tereikovska L.A. METHOD FOR DETERMINING THE TYPE OF CONVOLUTIONAL NEURAL NETWORKS FOR ANALYSIS OF THE KEYBOARD HANDWRITING

The article is devoted to the problem of creating means for covert monitoring of the personality and emotional state of users of information systems. The prospects of monitoring tools based on the analysis of keyboard handwriting constructed using convolutional neural networks are determined. Inadequate adaptation of existing neural network tools to significant conditions of the task of analyzing keyboard handwriting is also shown. It is proposed to correct this drawback by developing a method for determining the most efficient type of convolutional neural network. As a result of the research, the possibility of considering the task of developing this method as a multi-criteria optimization of neural network information protection tools is substantiated. A method for determining the most effective type of convolutional neural network designed for the analysis of keyboard handwriting has been developed. The stages of the method are related to determining the weighting coefficients of the performance criteria, calculating the value of the efficiency function for each admissible type of neural network model, determining the type of model with the maximum value of the efficiency function,

and verifying the results obtained. Using the proposed method, it was determined that in conditions of limited access to the databases of keyboard handwriting parameters, the availability of available and tested tools for implementing neural network tools, acceptable resource consumption of hardware and software implementation, acceptable training and recognition periods, and sufficient recognition accuracy with the most effective type of convolution The neural network is SqueezeNet. As a result of computer experiments, it was calculated that the accuracy of personality recognition using SqueezeNet is approximately 10-11% higher than the accuracy of recognition using other types of convolutional neural networks, which confirms the effectiveness of the developed method. It is proposed to correlate the paths of further research with the adaptation of SqueezeNet parameters to the conditions of the task of analyzing keyboard writing.

Key words: *keyboard handwriting, personality identification, emotion recognition, convolutional neural network, recognition tools.*