УДК 004.58 DOI: 10.31673/2412-4338.2023.039699

Бондарчук А.П.
Державний університет інформаційно-комунікаційних технологій
Онисько А.І., Отрох С.І., Шевчук Д.О.
Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

СИСТЕМА ДВОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧА ЗА ДОПОМОГОЮ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ

Анотація: *У сучасному світі інформаційних технологій безпека даних стає ключовим питанням. Однією з найефективніших методик захисту є двофакторна аутентифікація. Ця стаття присвячена розгляду новітнього методу двофакторної аутентифікації, який базується на комбінації нейромереж та розпізнавання обличчя. Глибоке навчання, яке використовується в нейромережах, дозволяє системі адаптуватися до невеликих змін у зовнішності користувача, таких як нова зачіска, відсутність або наявність макіяжу, носіння окулярів тощо. Це робить систему гнучкою і здатною розпізнавати користувача навіть при незначних змінах у його вигляді. Основна ідея методу полягає в аналізі унікальних особливостей обличчя користувача. Нейромережа "вивчає" особливості кожного користувача, створюючи його унікальний "портрет". Цей "портрет" потім використовується для верифікації особи при спробі входу в систему. Додатково до розпізнавання обличчя, система може вимагати введення пароля або іншого виду аутентифікації, що робить процес входу ще більш безпечним. Комбінація цих двох методів забезпечує високий рівень захисту від несанкціонованого доступу. Важливою перевагою такої системи є її зручність для користувача. Обличчя користувача стає "ключем" до системи, що робить процес входу швидким і непомітним. Також хочеться зазначити, що розвиток технологій розпізнавання обличчя відкриває нові горизонти для забезпечення безпеки даних. Використання нейромереж у комбінації з двофакторною аутентифікацією може стати стандартом у найближчому майбутньому.*

Ключові слова: *двофакторна аутентифікація (2FA), розпізнавання обличчя, біометрика, безпека, аутентифікація, ідентифікація, обліковий запис, токен, біометричні дані, приватність, помилка розпізнавання, система безпеки, технологія, камера, алгоритм, нейрона мережа.*

Bondarchuk A.P.
State University of Information and Communication Technologies
Onysko A.I., Otrokh S.I., Shevchuk D.O.
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

TWO-FACTOR USER AUTHENTICATION SYSTEM USING FACIAL RECOGNITION

Abstract: *In today's world of information technology, data security is becoming a paramount concern. One of the most effective protection methodologies is two-factor authentication. This article delves into a cutting-edge method of two-factor authentication based on the combination of neural networks and facial recognition. Deep learning, employed in neural networks, allows the system to adapt to minor changes in a user's appearance, such as a new hairstyle, the presence or*

© Бондарчук А.П., Онисько А.І., Отрох С.І., Шевчук Д.О. 2023

absence of makeup, wearing glasses, and so on. This makes the system flexible and capable of recognizing the user even with slight alterations in their look. The core idea of the method is to analyze the unique features of the user's face. The neural network "learns" the characteristics of each user, creating their unique "portrait". This "portrait" is then used for identity verification upon attempting to access the system. In addition to facial recognition, the system may require password input or another form of authentication, making the login process even more secure. The combination of these two methods ensures a high level of protection against unauthorized access. A significant advantage of such a system is its convenience for the user. The user's face becomes the "key" to the system, making the login process quick and seamless. It's also worth noting that the advancement of facial recognition technology opens new horizons for data security. Using neural networks in conjunction with two-factor authentication may become the standard in the near future.

Keywords: *Two-Factor Authentication (2FA), facial recognition, biometrics, security, authentication, identification, account, token, biometric data, privacy, recognition error, security system, technology, camera, algorithm, neural network.*

Постановка проблеми. У сучасному цифровому світі безпека даних стає все більш актуальною темою. З ростом кількості онлайн-сервісів та платформ, користувачам потрібно забезпечити надійний захист своїх особистих даних. Однією з ключових технологій, яка допомагає в цьому, є двофакторна аутентифікація. Цей метод передбачає використання двох різних компонентів для підтвердження особи користувача, замість традиційного введення лише логіну та паролю [1].

Останнім часом особливу увагу привертає двофакторна аутентифікація за допомогою розпізнавання обличчя. Ця технологія використовує нейронні мережі для аналізу особливостей обличчя користувача і порівняння їх з збереженими даними. Такий підхід забезпечує високий рівень безпеки, адже кожна особа має унікальні риси обличчя, які важко симулювати або підробити.

Також варто відзначити, що розпізнавання обличчя стає все більш популярним завдяки його зручності для користувача. Немає потреби запам'ятовувати складні паролі або використовувати додаткові пристрої для генерації кодів. Просто подивіться на камеру свого пристрою, і система вас впізнає.

В умовах постійної еволюції кіберзагроз, методи двофакторної аутентифікації, зокрема з використанням розпізнавання обличчя та нейронних мереж, відіграють ключову роль у забезпеченні конфіденційності та інтеграції даних користувачів.

Аналіз останніх досліджень і публікацій. В останні роки технологія розпізнавання обличчя стає все більш популярною. Однією з найновіших розробок в цій області є підхід GWOECN-FR, який використовує оптимізацію сірого вовка (Grey Wolf Optimizer, GWO) з покращеною капсульною мережею на основі глибокого переносу навчання для розпізнавання обличчя в реальному часі [5]. Цей метод показав вражаючі результати, зокрема час відгуку в 0,03 секунди, що є набагато швидше, ніж більшість сучасних методів.

Також варто звернути увагу на дослідження, яке розглядає використання глибоких нейромереж для розпізнавання обличчя в умовах низької роздільної здатності хї. Це дослідження показало, що за допомогою спеціальної архітектури нейромережі можна досягти високої точності розпізнавання навіть на зображеннях низької якості.

Інший цікавий підхід, представлений в дослідженнях, - це використання нейромереж для розпізнавання обличчя на основі теплових зображень [4]. Цей метод може бути особливо корисним у випадках, коли звичайні камери не можуть виявити обличчя через погане освітлення або інші перешкоди.

Сучасні технології розпізнавання обличчя, зокрема на основі нейромереж [10], відкривають нові можливості для систем безпеки та аутентифікації. Завдяки постійним

дослідженням та розробкам ми можемо очікувати ще більшого прогресу в цій галузі в найближчому майбутньому.

Мета і задачі дослідження. Метою даної роботи є проектування, розробка та впровадження високоефективної системи двофакторної аутентифікації користувача в інформаційних системах за допомогою передової технології розпізнавання обличчя[9]. Ця система комбінує традиційні методи авторизації, такі як введення пароля, з біометричним розпізнаванням особи користувача, що забезпечує додатковий рівень захисту від несанкціонованого доступу.

Результати дослідження. Нейронні мережі стали ключовим інструментом в області розпізнавання обличчя завдяки їхній здатності автоматично вивчати та визначати важливі особливості з великих наборів даних. Нейронна мережа для розпізнавання обличчя зазвичай складається з наступних шарів:

- Вхідний шар (Input Layer): Приймає вхідні дані у вигляді зображення обличчя. Зображення обличчя перетворюється на масив пікселів, де кожен піксель має значення яскравості (для чорно-білих зображень) або трійку значень RGB (для кольорових зображень).
- Згорткові шари (Convolutional Layers): Виявлення основних особливостей на зображенні, таких як краї, текстури, форми тощо. Використовують невеликі "фільтри" або "ядра", які "згортають" зображення, виявляючи особливості на різних рівнях деталізації.
- Шари пулінгу (Pooling Layers): Зменшення розмірності даних, зберігаючи при цьому найважливіші особливості Часто використовується максимальний пулінг (max pooling), де з підмножини пікселів вибирається найбільше значення.
- Повнозв'язні шари (Fully Connected Layers): Інтерпретація особливостей, виявлених згортковими шарами, для класифікації зображення. Кожен нейрон у цьому шарі з'єднується з усіма нейронами попереднього шару.
- Функції активації: Визначення виходу кожного нейрона на основі його входу. Найпопулярніші функції активації включають ReLU (Rectified Linear Unit), сигмоїду та гіперболічний тангенс.
  Функції активації (ReLU) має наступний вигляд:

$$f(x) = max(0, x), \tag{1}$$

Сигмоїдна функція:

$$\sigma(x) = \frac{1}{1 + e^{-1}}, \tag{2}$$

Гіперболічний тангенс:

$$tanh(x) = \frac{e^{x} - e^{-x}}{e^{x} + e^{-x}} \tag{3}$$

де x є вхідним значенням для даної функції активації.

- Вихідний шар (Output Layer): Подання кінцевого результату класифікації. Зазвичай використовується функція активації softmax для багатокласової класифікації, яка визначає ймовірності належності зображення до кожного класу.

- Зворотне поширення (Backpropagation): Оптимізація ваг і зміщень у мережі на основі різниці між передбаченим виходом та дійсним міткою. Як правило, використовується алгоритм градієнтного спуску або його варіації для мінімізації функції втрат.

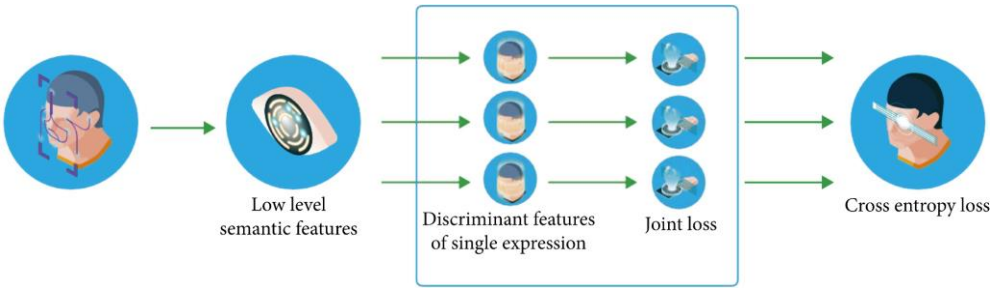

Рис.1 Алгоритм роботи нейромережі з розпізнавання обличчя [2]

Ось приклад коду, який може бути використаний для створення та навчання нейронної мережі для розпізнавання обличчя за допомогою бібліотеки TensorFlow:

backend > validators > model.py > ...

```python
import tensorflow as tf
from tensorflow.keras import layers, models

# Створення моделі
model = models.Sequential()
model.add(layers.Conv2D(32, (3, 3), activation='relu', input_shape=(150, 150, 3)))
model.add(layers.MaxPooling2D((2, 2)))
model.add(layers.Conv2D(64, (3, 3), activation='relu'))
model.add(layers.MaxPooling2D((2, 2)))
model.add(layers.Conv2D(128, (3, 3), activation='relu'))
model.add(layers.MaxPooling2D((2, 2)))
model.add(layers.Flatten())
model.add(layers.Dense(512, activation='relu'))
model.add(layers.Dense(1, activation='sigmoid'))

# Компіляція моделі
model.compile(loss='binary_crossentropy',
              optimizer='adam',
              metrics=['accuracy'])

# Навчання моделі (припустимо, що train_data та train_labels - це ваші дані)
# model.fit(train_data, train_labels, epochs=10, batch_size=32)
```

Рис.2 Фрагмент коду створення нейромережі

Цей код є лише прикладом того, як можна створити нейронну мережу для розпізнавання обличчя. У реальних застосуваннях використовуються більш складні архітектури та додаткові оптимізації.

Висновки і перспективи подальших досліджень. У сучасному світі, де технології швидко розвиваються та інтегруються в повсякденне життя людей, питання інформаційної безпеки набуває особливої актуальності. Система двофакторної аутентифікації за допомогою розпізнавання обличчя, яку ми розглядали в цій статті, представляє собою перспективний крок у напрямку забезпечення конфіденційності даних користувачів.

За допомогою сучасних алгоритмів та технологій машинного навчання, система розпізнавання обличчя може визначати унікальні особливості особи з високою точністю. Це, у поєднанні з традиційними методами авторизації, такими як паролі або QR-коди, створює надійний бар'єр для потенційних зловмисників.

Однак слід зазначити, що, як і будь-яка інша технологія, система розпізнавання обличчя має свої слабкі місця. Питання освітленості, кута зйомки, зміни в зовнішності особи

(наприклад, внаслідок операції або старіння) можуть впливати на ефективність системи. Тому важливо постійно вдосконалювати алгоритми та проводити додаткові дослідження в цій області.

В майбутньому, з розвитком технологій, можна очікувати ще більшої інтеграції біометричних систем аутентифікації в різноманітні сфери життя, від корпоративних мереж до побутової електроніки. Тому робота над вдосконаленням цих систем є не тільки актуальною, але й дуже перспективною.

Завершуючи, хочеться підкреслити, що інноваційні рішення в області інформаційної безпеки є ключем до створення надійного, безпечного та зручного цифрового середовища для всіх користувачів.

Список використаної літератури

1. Alzubaidi L., Zhang J., Humaidi A.J., Al-Dujaili A., Duan Y. Development of a Secure Access Control System Based on Two-Factor Authentication Using Face Recognition and OTP SMS-Token [Електронний ресурс] // URL: https://dx.doi.org/10.1109/ICIMCIS51567.2020.9354328
2. Zhang B., Wang Y., Wang J. Convolutional Neural Network Face Recognition Method Using Fisher's Criterion [Електронний ресурс] // URL: https://www.hindawi.com/journals/misy/2022/1101282/
3. Nelson D. Image Recognition and Classification in Python with TensorFlow and Keras [Електронний ресурс] // URL: https://stackabuse.com/image-recognition-in-python-with-tensorflow-and-keras/
4. Naoyuki K. Applying Artificial Neural Networks for Face Recognition [Електронний ресурс] // URL: https://www.hindawi.com/journals/aans/2011/673016/
5. Zhang B., Wang Y. Capsule Network-Based Deep Transfer Learning Model for Face Recognition [Електронний ресурс] // URL: https://www.hindawi.com/journals/wcmc/2022/2086613/
6. Banumalar K., Manikandan B.V., Vanaja N. Face Recognition using Deep Learning [Електронний ресурс] // URL: https://www.e3s-conferences.org/articles/e3sconf/pdf/2023/24/e3sconf_icseret2023_05001.pdf
7. Wenting L., Zhou L., Chen J., Face Recognition Based on Lightweight Convolutional Neural Networks [Електронний ресурс] // URL: https://www.mdpi.com/2078-2489/12/5/191
8. Wei-Meng L. Implementing Face Recognition Using Deep Learning and Support Vector Machines [Електронний ресурс] // URL: https://www.codemag.com/Article/2205081/Implementing-Face-Recognition-Using-Deep-Learning-and-Support-Vector-Machines
9. Manisha M. K., Bhattacharyya D., Tai-hoon K., Face Recognition Using Neural Network: A Review [Електронний ресурс] // URL: http://article.nadiapub.com/IJSIA/vol10_no3/8.pdf
10. Noor T., Facial Recognition Using Deep Learning [Електронний ресурс] // URL: https://towardsdatascience.com/facial-recognition-using-deep-learning-a74e9059a150
11. Zhebka V., Gertsiuk M., Sokolov V., Malinov V.Sablina M. Optimization of Machine Learning Method to Improve the Management Efficiency of Heterogeneous Telecommunication Network // CEUR Workshop Proceedings, 2022, 3288, p. 149–155

References

1. Alzubaidi L., Zhang J., Humaidi A.J., Al-Dujaili A., Duan Y. Development of a Secure Access Control System Based on Two-Factor Authentication Using Face Recognition and OTP SMS-Token. [Electronic resource] // URL: https://dx.doi.org/10.1109/ICIMCIS51567.2020.9354328.

2.Zhang B., Wang Y., Wang J. Convolutional Neural Network Face Recognition Method Using Fisher's Criterion. [Electronic resource] // URL: https://www.hindawi.com/journals/misy/2022/1101282/.
3.Nelson D. Image Recognition and Classification in Python with TensorFlow and Keras. [Electronic resource] // URL: https://stackabuse.com/image-recognition-in-python-with-tensorflow-and-keras/.
4.Naoyuki K. Applying Artificial Neural Networks for Face Recognition. [Electronic resource] // URL: https://www.hindawi.com/journals/aans/2011/673016/.
5.Zhang B., Wang Y. Capsule Network-Based Deep Transfer Learning Model for Face Recognition. [Electronic resource] // URL: https://www.hindawi.com/journals/wcmc/2022/2086613/.
6.Banumalar K., Manikandan B.V., Vanaja N. Face Recognition using Deep Learning. [Electronic resource] // URL: https://www.e3s-conferences.org/articles/e3sconf/pdf/2023/24/e3sconf_icseret2023_05001.pdf.
7.Wenting L., Zhou L., Chen J. Face Recognition Based on Lightweight Convolutional Neural Networks. [Electronic resource] // URL: https://www.mdpi.com/2078-2489/12/5/191.
8.Wei-Meng L. Implementing Face Recognition Using Deep Learning and Support Vector Machines. [Electronic resource] // URL: https://www.codemag.com/Article/2205081/Implementing-Face-Recognition-Using-Deep-Learning-and-Support-Vector-Machines.
9.Manisha M. K., Bhattacharyya D., Tai-hoon K. Face Recognition Using Neural Network: A Review. [Electronic resource] // URL: http://article.nadiapub.com/IJSIA/vol10_no3/8.pdf.
10. Noor T. Facial Recognition Using Deep Learning. [Electronic resource] // URL: https://towardsdatascience.com/facial-recognition-using-deep-learning-a74e9059a150.
11. Zhebka V., Gertsiuk M., Sokolov V., Malinov V.Sablina M. Optimization of Machine Learning Method to Improve the Management Efficiency of Heterogeneous Telecommunication Network // CEUR Workshop Proceedings, 2022, 3288, p. 149–155