

DOI: <https://doi.org/10.36910/6775-2524-0560-2024-54-02>

УДК 004.932.75'1, 004.622, 004.514

Ковівчак Ярослав Васильович, к.т.н., доцент

<https://orcid.org/0000-0003-3562-4924>

Дубук Василь Іванович, к.т.н., доцент

<https://orcid.org/0000-0002-6339-1032>

Бучковський Мар'ян Володимирович, магістрант

Національний університет «Львівська політехніка», м. Львів, Україна

РОЗРОБКА АВТОМАТИЗОВАНОЇ СИСТЕМИ ІДЕНТИФІКАЦІЇ ПІДПISУ ОСОБИ

Ковівчак Я.В., Дубук В.І., Бучковський М.В. Розробка автоматизованої системи ідентифікації підпису особи.

У статті приведено розробку автоматизованої системи ідентифікації підпису особи. Обґрунтовано актуальність розробки. Здійснено аналіз існуючих подібних систем, розглянуто їх переваги та недоліки. Побудовано концептуальну модель системи ідентифікації підпису особи. Побудовано діаграму використання для користувачів системи. Розроблено блок-схему алгоритму роботи системи. Приведено функціональну модель системи. Розроблено діаграму класів автоматизованої системи ідентифікації підпису особи. Реалізовано базу даних. Приведено діаграму компонентів системи. Здійснено реалізацію компонентів системи, бази даних та інтерфейсу користувача. Запропонована автоматизована система ідентифікації підпису людини може знайти успішне використання у різних областях людської діяльності, а саме, у банківській справі, юридичній сфері, медицині, в діловодстві. Застосування розробленої системи на практиці допоможе забезпечити автоматизацію процесу визначення автентичності підпису особи. Це пришвидшить процеси ідентифікації підписів та зменшить ризики шахрайства при ідентифікації особи, підвищить рівень захисту документів.

Ключові слова: автоматизована система, ідентифікація особи, обробка зображень, нейронна мережа, машинне навчання.

Kovivchak Ya., Dubuk V., Buchkovsky M. Development of an automated system for identification of a person's signature. The article describes the development of an automated system for identification of a person's signature. The relevance of the development is substantiated. An analysis of existing similar systems was carried out, their advantages and disadvantages were considered. A conceptual model of a person's signature identification system was built. A usage diagram for system users was built. A block diagram of the system's operation algorithm has been developed. A functional model of the system is given. A class diagram of the automated system of identification of a person's signature has been developed. A database was developed. A diagram of the system components is given. The system components, database and user interface were implemented. The proposed automated human signature identification system can find successful use in various areas of human activity, namely, in banking, legal field, medicine, and document flow. The practical use of the developed system will ensure the automation of the process of determining the authenticity of a person's signature. This will speed up signature identification processes and reduce the risks of identity fraud, and increase the level of document protection.

Keywords: automated system, person identification, image processing, neural network, machine learning.

Постановка задачі. Ідентифікація особи у різних сферах людської діяльності є необхідною потребою при роботі з різними об'єктами з обмеженим доступом. Це зумовлює стрімкий розвиток різних напрямків досліджень в області біометричної ідентифікації. Біометрична ідентифікація дає змогу виявити фізичні або поведінкові унікальні характеристики окремих людей з метою розпізнавання та підтвердження їх особи.

На сьогодні фізичний підпис людини є юридично визнаним та суспільно розповсюдженим біометричним способом ідентифікації та підтвердження особи. Наявність фізичного підпису людини на документі має перевагу перед іншими біометричними способами підтвердження особи, оскільки не вимагає додаткового спеціального та дорогого обладнання для ідентифікації особи підписанта. Крім того, фізичний підпис під документом людина робить тоді, коли вона це розуміє та усвідомлює. Інші існуючі способи ідентифікації, що ґрунтуються на технологіях сканування відбитків пальців чи сітківки ока, можуть бути застосовані поза її волею, розумінням та свідомістю.

Однак, головною проблемою ідентифікації користувачів за їх підписом є низька ймовірність того, що два підписи, зроблені однією і тією ж особою, будуть ідентичними. Це пов'язано з тим, що при різних зовнішніх умовах та різному психофізичному стані для більшості людей складно повторити ті самі рухи з однаковою швидкістю та тиском на документ, щоб відтворити один і той самий підпис. Тому завдання виявлення підроблених підписів на документах є складною задачею.

Одним із найбільш ефективних автоматизованих способів ідентифікації підпису лю-

дини є застосування методів штучного інтелекту. Такі способи широко використовуються у банківській та страховій сферах, при здійсненні фінансових операцій та у юридичній області при укладанні угод, контрактів та інших документів. Основними перевагами застосування автоматизованої системи ідентифікації підпису особи є автоматизація процесу ідентифікації особи підписанта, а також підвищення швидкості та точності результатів ідентифікації.

Отже розробка автоматизованої системи ідентифікації підпису особи є актуальною задачею сьогодення.

Аналіз останніх досліджень і публікацій. Робота системи верифікації підпису особи базується на розв'язанні задач розпізнавання образів, теоретичні основи розв'язання яких ґрунтовно описані у класичній праці відомих вчених [1]. Важливі науково-практичні дослідження з вказаної проблеми виконані та опубліковані авторами з Угорщини [2, 3], міжнародним колективом вчених з різних країн [4], вченими з Індії [5, 6].

В результаті досліджень було проведено аналіз існуючих доступних для огляду систем верифікації підпису людини, серед них - "Signature Verification" та "Techsign".

Система "Signature Verification" була розроблена на факультеті автоматизації та прикладної інформатики Будапештського університету технології та економіки [7]. При її розробці були використані результати ґрунтовних науково-практичних досліджень, викладених авторами [2, 3, 4]. Дана система призначена для індивідуального використання з метою ідентифікації підпису людини. Система дає змогу користувачам вибирати тип конфігурації, кількість референтних зображень підписів, проглянути детальний звіт верифікації. На рис. 1 приведено інтерфейс користувача системи [7].

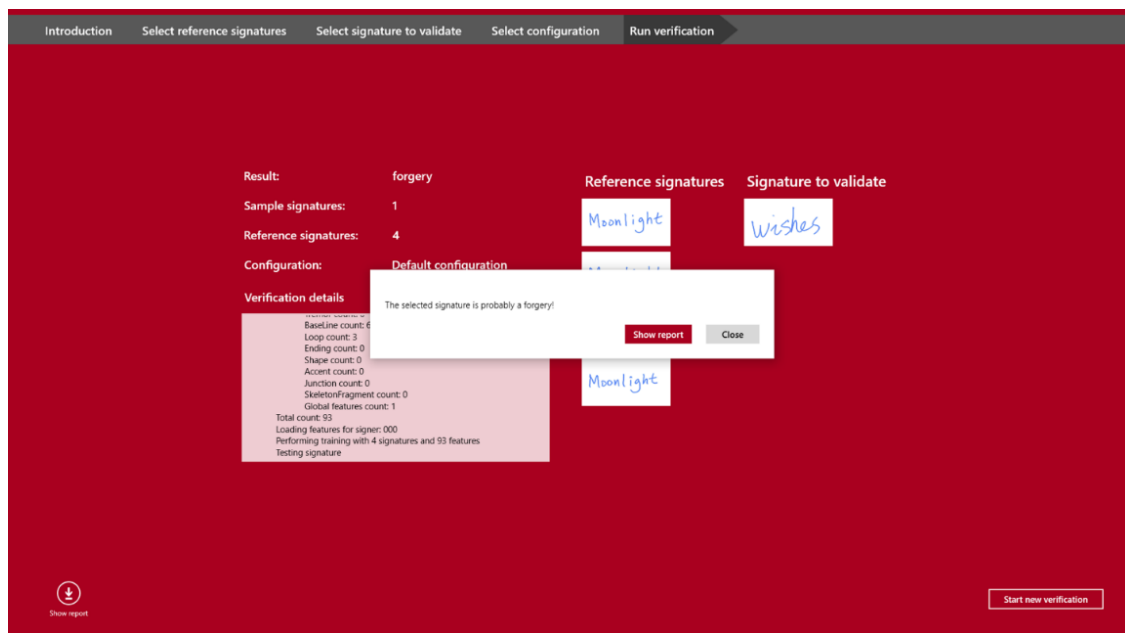


Рис. 1 – Інтерфейс системи "Signature Verification"

Завдяки можливості змінювати конфігурацію системи під час її використання, користувачі мають змогу здійснювати вибір різних методів на різних етапах верифікації підпису особи. Також користувачі можуть створити, зберегти та використовувати свою власну, найбільш оптимальну для них, конфігурацію системи.

До переваг системи можна віднести: зручний інтерфейс користувача; простота роботи з системою; можливість зміни конфігурації системи на різних етапах верифікації підпису; формування детального звіту проведеної верифікації. Недоліки: незахищеність системи від доступу інших користувачів; необхідність використання декількох референтних

зображеннях для верифікації окремого підпису; відсутність інформації про власників підписів; лише англomовний інтерфейс.

У 2022 році компанія Techsign Biometric signature & forensic tool з Туреччини розробила систему верифікації підпису людини "Techsign" для комерційного застосування [8].

Для роботи з системою передбачено використання планшету з метою отримання реального фізичного підпису особи. У результаті роботи системи формується детальний звіт, у якому вказується ймовірність співпадіння підпису, швидкість написання, кут та натиск при здійсненні підпису. На рис. 2 приведено інтерфейс системи "Techsign" [8].

Для верифікації підпису системою "Techsign", користувачі повинні надати декілька зрізців власних підписів. Отримання підписів користувача відбувається на спеціальному обладнанні, яке здійснює ідентифікацію основних характеристик окремого підпису особи. Лише після цього система може застосовуватись для ідентифікації підписів відповідних користувачів.

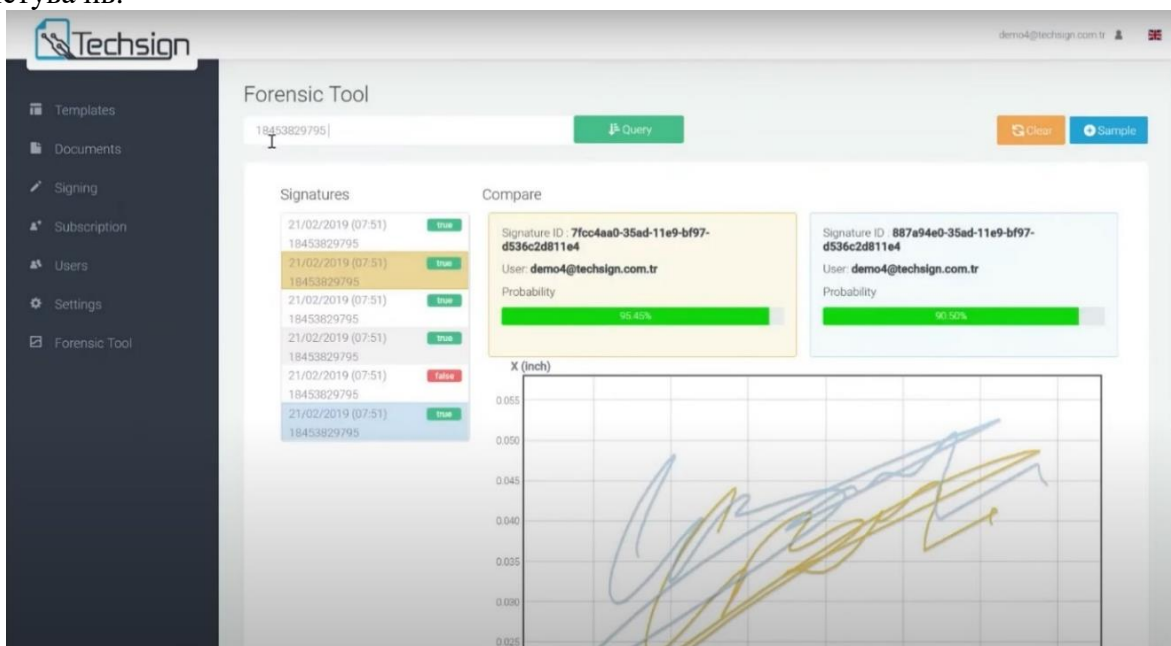


Рис. 2 – Інтерфейс системи "Techsign"

До переваг розглянутої системи можна віднести: високу точність розпізнавання підпису особи (90 – 95 %); простий інтерфейс; простоту використання системи; формування детального звіту результату верифікації підпису користувачів. Недоліки: необхідність застосування спеціального обладнання для верифікації підпису; необхідність застосування декількох зразків підписів користувача для проведення ідентифікації підпису особи; відсутність інформації про власника підпису.

Метою дослідження було розроблення автоматизованої системи ідентифікації та верифікації підпису людини на основі алгоритмів машинного навчання.

Основна частина. На першому етапі роботи було побудовано концептуальну модель системи на основі підходів, викладених автором [9] (рис. 3).



Рис. 3 – Концептуальна модель системи ідентифікації підпису особи

Оскільки система призначена для індивідуального використання, на концептуальній моделі зображено лише дві зовнішні сутності – користувача системи та базу даних з підписами осіб. Користувач має можливість завантажити підпис клієнта, здійснити його ідентифікацію, переглянути результати ідентифікації, а також зберегти підпис клієнта в базі даних. База даних містить інформацію про підписи клієнтів, яка необхідна для їх ідентифікації.

У відповідності до концептуальної моделі, приведеної на рис. 3, розроблено діаграму варіантів використання для користувачів системи. Особливості створення діаграм варіантів використання ґрунтовно пояснені у [10]. Така діаграма відображає основні функції системи, які може виконати користувач та послідовність їх виконання. Діаграма варіантів використання для системи ідентифікації підпису особи приведена на рис. 4.

Також було розроблено алгоритм роботи системи для ідентифікації підпису особи на основі використання штучних нейронних мереж на основі підходів, описаних автором [11]. Алгоритм передбачає виконання наступних основних кроків:

1. Налаштування параметрів нейронної мережі.
 2. Опрацювання навчальних даних.
 3. Навчання нейронної мережі.
 4. Визначення похибки навчання (якщо похибка велика, то навчання продовжується, якщо похибка допустима – нейронна мережа може використовуватися для ідентифікації підпису).
 5. Завантаження зображення з підписом.
 6. Попереднє опрацювання зображення.
 7. Розпізнавання підпису.
 8. Виведення результату.
- Блок-схема алгоритму наведена на рис. 5.

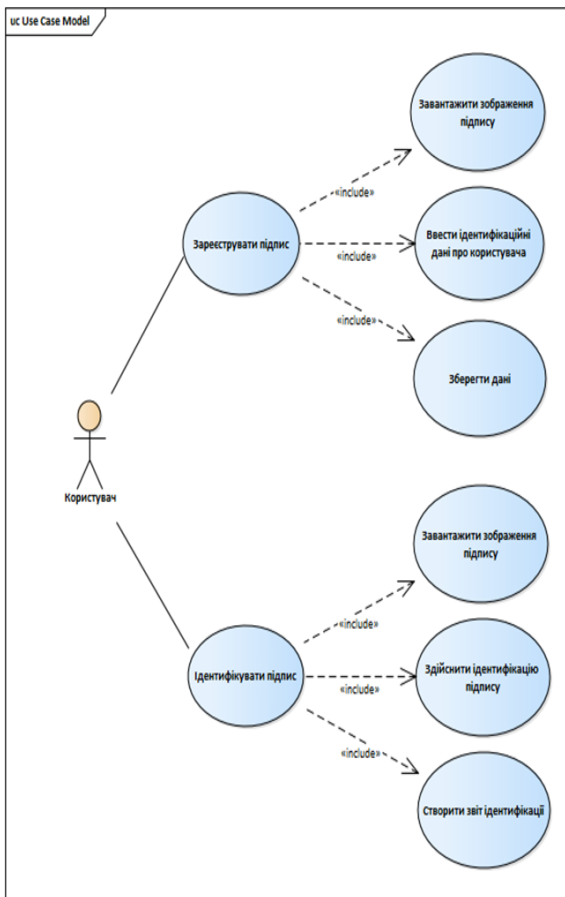


Рис. 4 – Діаграма варіантів використання

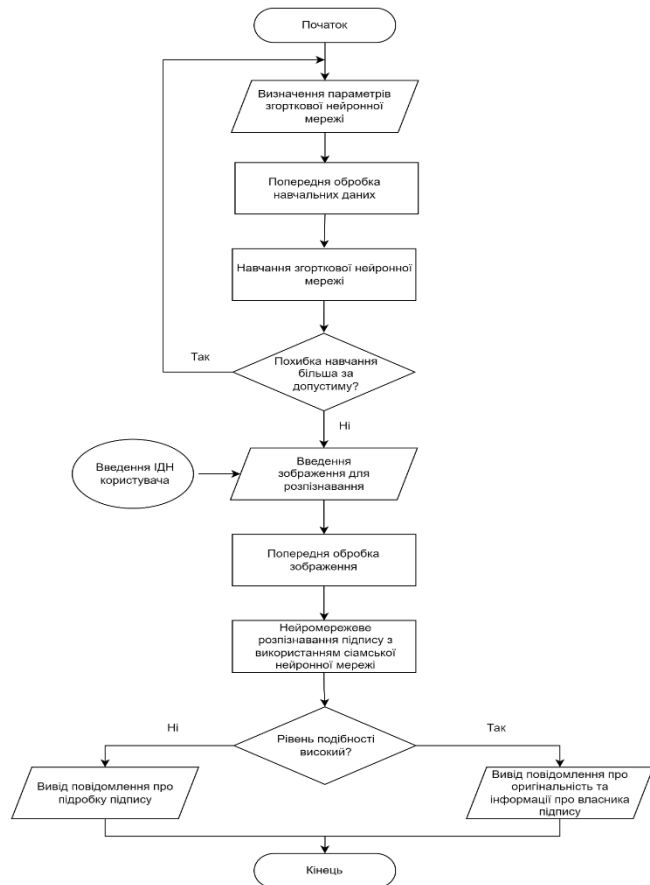


Рис. 5 – Блок-схема роботи алгоритму роботи системи ідентифікації підпису особи

Для того, щоб змоделювати та описати основні процеси в системі ідентифікації підпису особи, здійснено побудову функціональної моделі системи з використанням IDEF0 діаграм. На початку, під час проектування системи було розроблено контекстну діаграму та проведено її деталізацію на діаграмах нижчого рівня (побудову діаграм було здійснено за допомогою інструментального програмного засобу Ramus Educational [12]).

Діаграма декомпозиції першого рівня контекстної діаграми функціональної моделі системи приведена на рис. 6. У відповідності до завдань у функціональній моделі системи було передбачено виконання наступних процесів: навчання нейронної мережі, ідентифікація підпису особи та онлайн допомога.

Після проходження авторизації користувач може здійснювати процес ідентифікації підпису особи на основі використання нейронної мережі [13]. Для навчання нейронної мережі застосовуються набори підписів осіб, які зберігаються у базі даних. Нейронна мережа може використовуватись для ідентифікації підпису лише після успішного її навчання [14, 15, 16]. Всі дані з підписами користувачів та результати навчання нейронної мережі захищені у відповідності до правил захисту персональних даних та прав споживачів.

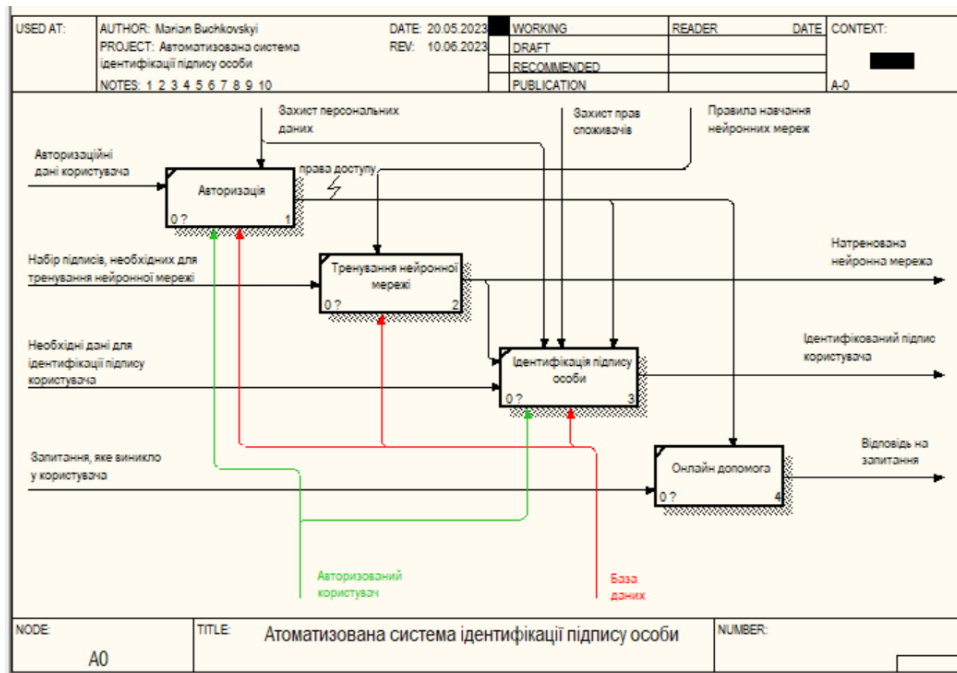


Рис. 6 – Діаграма декомпозиції першого рівня системи

Під час реалізації системи ідентифікації підпису особи розроблено структуру бази даних. База даних побудована на основі реляційної моделі. Структуру бази даних системи приведено на рис. 7.

В базі даних реалізовано наступні сутності: користувач; підпис; клієнт та запитання. Також визначено зв'язки між сутностями. Для розробки бази даних застосовано SQLite [17]. З метою організації доступу до даних використано шар Data Access (доступ до даних здійснюється за допомогою модуля sqlite3).

Архітектура системи реалізована на основі стандартного підходу "Модель-Вигляд-Контролер" (Model-View-Controller) [18]. Компонент Model забезпечує реалізацію алгоритму роботи з даними, а компонент Controller забезпечує алгоритм роботи системи. Компонент View призначений для роботи з інтерфейсом користувача.

У процесі розробки системи побудовано діаграму класів. Діаграма класів приведена на рис. 8. На даній діаграмі приведено всі класи, що формують систему, а саме: User, Signature, Question, Operator та зв'язки між ними.

Загальна структура системи відображена на діаграмі компонентів, яка приведена на рис. 9.

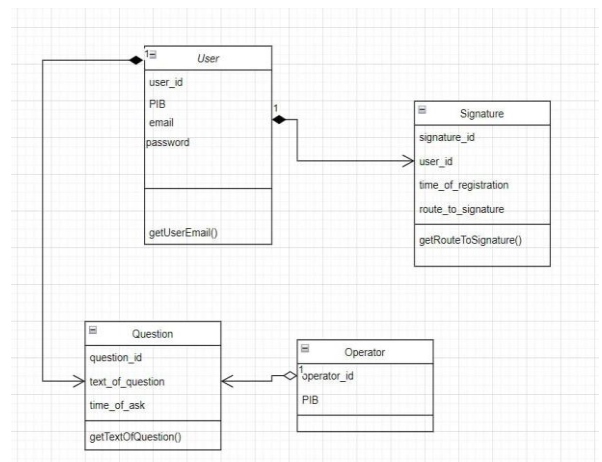
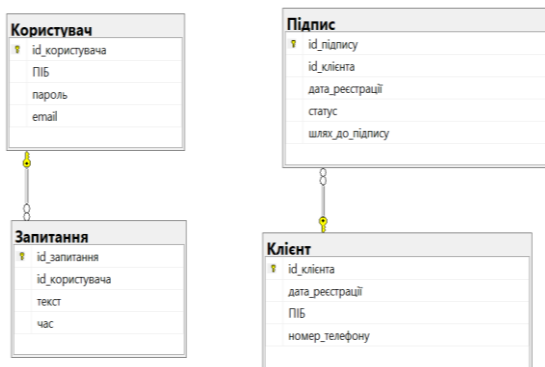


Рис. 7 – Структура бази даних системи ідентифікації підпису особи

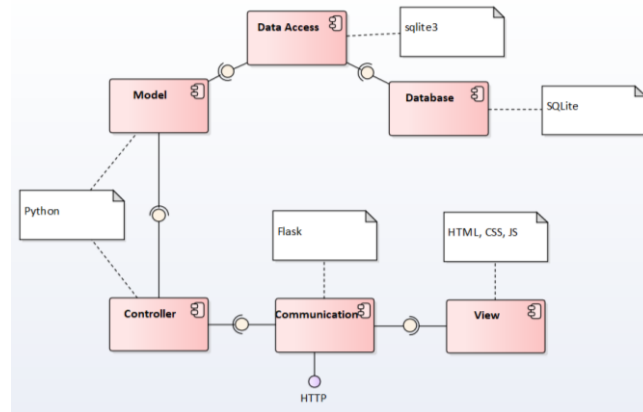


Рис. 8 – Діаграма класів

Рис. 9 – Діаграма компонентів системи ідентифікації підпису особи

Також було здійснено розробку необхідних модулів та інтерфейсу користувача системи ідентифікації підпису особи. Крім цього, проведено тестування роботи окремих компонентів та системи загалом. Основні вікна інтерфейсу користувача зображено на рис. 10 і рис. 11.

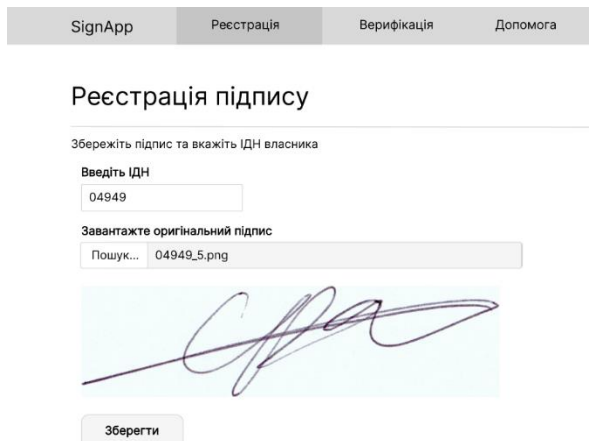


Рис. 10 – Інтерфейс користувача для реєстрації підпису особи

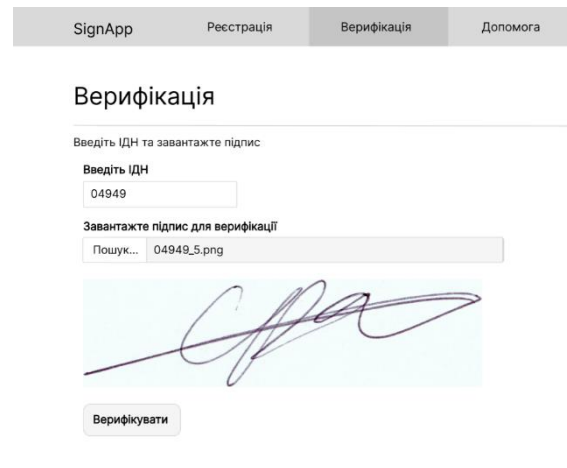


Рис. 11 – Інтерфейс користувача для ідентифікації підпису особи

Після успішної авторизації в системі перед користувачем відкривається вікно "Реєстрація підпису". Це дає змогу користувачу здійснювати внесення підписів нових клієнтів у базу даних. Для здійснення ідентифікації підпису особи необхідно ввести в систему ідентифікаційний номер власника підпису та зображення підпису, яке потрібно верифікувати. Після завершення опрацювання підпису особи, система виведе користувачу повідомлення про статус вибраного підпису (підроблений чи справжній), а також інформацію про власника підпису (якщо верифікація була успішною).

Висновки. У результаті виконання роботи було розроблено автоматизовану систему ідентифікації підпису особи. Наведено обґрунтування актуальності розробки системи. Проведено аналіз систем аналогічного призначення, а також розглянуто їх переваги та недоліки. Здійснено побудову необхідних компонентів системи, бази даних та інтерфейсу користувача. Проведено їх тестування.

Запропонована автоматизована система ідентифікації підпису особи може знайти своє успішне використання у різних областях людської діяльності, а саме: у банківській та страховій діяльності, юридичній сфері, медицині, в діловодстві. Застосування розробленої системи на практиці автоматизує процес визначення автентичності підпису особи, пришвидшить його та зменшує ризики шахрайства при ідентифікації клієнтів, а також підвищить рівень захисту підписаних документів.

Список бібліографічного опису

1. Theodoridis S., Koutroumbas K. Pattern Recognition. New York: Academic Press, 2009. 961 p. URL: <https://books.google.com/books?id=QgD-3Tcj8DkC> (date of access: 10.02.2024).
2. Kovari B., Charaf H. A study on the consistency and significance of local features in off-line signature verification. Pattern Recognition Letters. 2013. Vol. 34, Issue 3. PP. 247-255. URL: <https://doi.org/10.1016/j.patrec.2012.10.011> (date of access: 10.02.2024).
3. Saleem M., Kovari B. Online signature verification using signature down-sampling and signer-dependent sampling frequency. Neural Computing & Applications. 2021. URL: <https://doi.org/10.1007/s00521-021-06536-z> (date of access: 10.02.2024).
4. Tolosana R., Vera-Rodriguez R., Gonzalez-Garcia C., Fierrez J., Morales A., Ortega-Garcia J., Ruiz-Garcia J.C., Romero-Tapiador S., Rengifo S., Caruana M., Jiang J., Lai S., Jin L., Zhu Y., Galbally J., Diaz M., Ferrer M. A., Gomez-Barrero M., Hodashinsky I., Sarin K., Slezkin A., Bardamova M., Svetlakov M., Saleem M., Szucs C.L., Kovari B., Pulsmeier F., Wehbi M., Zanca D., Ahmad S., Mishra S., Jabin S. SVC-onGoing: Signature verification competition. Pattern Recognition. 2022. Vol. 127, 108609, URL: <https://doi.org/10.1016/j.patcog.2022.108609> (date of access: 10.02.2024).
5. Krishna Prasad P. R., Reddy K.R., Sai M.H., Gopi L.Th., Vedakshari K. A Siamese Network based Writer Independent Offline Signature Verification. IJFANS International Journal of Food and Nutritional Sciences. 2022. Vol. 11. Issue 12. URL: <https://doi.org/10.48047/ijfans/v11/i12/204> (date of access: 10.02.2024).
6. Chauhan D., Verma D., Aggarwal A. Hand-Written Characters Recognition using Siamese Network Design. 2022. 1st International Conference on Informatics (ICI), Noida, India, 2022. PP. 66-70. URL: <https://doi.org/10.1109/ICI53355.2022.9786908> (date of access: 10.02.2024).
7. Signature verification research. BME Department of Automation and Applied Informatics. Budapest University of Technology and Economics. Faculty of Electrical Engineering and Informatics. URL: <https://www.aut.bme.hu/en/Pages/Research/Signature/Introduction> (date of access: 10.02.2024).
8. Close Deals At The Speed Of Life. All eSignatures In One. Techsign Doc. Techsign. 2024. URL: <https://www.techsigndoc.com/en/features.html> (date of access: 12.02.2024).
9. Olivé A. Conceptual Modeling of Information Systems. Heidelberg: Springer-Verlag Berlin, 2007. 455 p. URL: <https://doi.org/10.1007/978-3-540-39390-0> (date of access: 12.02.2024).
10. Use Case Diagram Tutorial. Visual Paradigm. 2024. URL: <https://online.visual-paradigm.com/diagrams/tutorials/use-case-diagram-tutorial/> (date of access: 12.02.2024).
11. Weng L. Contrastive Representation Learning. Lil'Log. 2021. URL: <https://lilianweng.github.io/posts/2021-05-31-contrastive/> (date of access: 12.02.2024).
12. RAMUS Java-based IDEF0 & DFD Modeler. Ramus. URL: <https://ramussoftware.com/> (date of access: 12.02.2024).
13. Бельковець В.Ю. Дослідження та порівняння нейронних мереж на прикладі реалізації задачі розпізнавання рукописних цифр. Текстова частина до курсової роботи за спеціальністю 122 «Комп'ютерні науки». Національний університет «Києво-Могилянська академія». 2021. URL: <https://ekmair.ukma.edu.ua/server/api/core/bitstreams/7ec56f11-b512-4f38-80a2-0d4237234075/content> (дата звернення: 12.02.2024).
14. Танасюк Д.О. Дослідження методів комп'ютерного зору для вирішення задач навчання ознак для реідентифікації об'єктів. Атестаційна робота. Рівень вищої освіти – другий (магістерський). Пояснювальна записка. Харківський національний університет радіоелектроніки. 2020. URL: <https://openarchive.nure.ua/server/api/core/bitstreams/650acd74-8a10-4600-9bdc-0477298dcf91/content> (дата звернення: 12.02.2024).
15. Xiao W., Ding Y. A Two-Stage Siamese Network Model for Offline Handwritten Signature Verification. Symmetry. 2022. Vol. 14 No. 6: 1216. URL: <https://doi.org/10.3390/sym14061216> (date of access: 13.02.2024).
16. Sharma N., Gupta S., Mohamed H.G., Anand D., Mazón J.L.V., Gupta D., Goyal N. Siamese Convolutional Neural Network-Based Twin Structure Model for Independent Offline Signature Verification. Sustainability. 2022. Vol.14. No.18: 11484. URL: <https://doi.org/10.3390/su141811484> (date of access: 13.02.2024).
17. SQLite Small. Fast. Reliable. Choose any three. The SQLite Consortium. 2024. URL: <https://www.sqlite.org/index.html> (date of access: 13.02.2024).
18. Sheldon R. Model-View-Controller (MVC). TechTarget. 2024. URL: <https://www.techtarget.com/whatis/definition/model-view-controller-MVC> (date of access: 13.02.2024).

References

1. Theodoridis, S. & Koutroumbas, K. (2009). Pattern Recognition. New York: Academic Press, 961. URL: <https://books.google.com/books?id=QgD-3Tcj8DkC>
2. Kovari, B. & Charaf, H. (2013). A study on the consistency and significance of local features in off-line signature verification. Pattern Recognition Letters, 34 (3), 247-255. <https://doi.org/10.1016/j.patrec.2012.10.011>
3. Saleem, M. & Kovari, B. (2021). Online signature verification using signature down-sampling and signer-dependent sampling frequency. Neural Computing & Applications. <https://doi.org/10.1007/s00521-021-06536-z>
4. Tolosana, R., Vera-Rodriguez, R., Gonzalez-Garcia, C., Fierrez, J., Morales, A., Ortega-Garcia, J., Ruiz-Garcia, J.C., Romero-Tapiador, S., Rengifo, S., Caruana, M., Jiang, J., Lai, S., Jin, L., Zhu, Y., Galbally, J., Diaz, M., Ferrer, M. A., Gomez-Barrero, M.,

- Hodashinsky, I., Sarin, K., Slezkin, A., Bardamova, M., Svetlakov, M., Saleem, M., Szucs, C.L., Kovari, B., Pulsmeier, F., Wehbi, M., Zanca, D., Ahmad, S., Mishra, S. & Jabin, S. (2022). SVC-onGoing: Signature verification competition. *Pattern Recognition*, 127, 108609. <https://doi.org/10.1016/j.patcog.2022.108609>
5. Krishna Prasad, P. R., Reddy, K.R., Sai, M.H., Gopi, L.Th. & Vedakshari, K. (2022). A Siamese Network based Writer Independent Offline Signature Verification. *IJFANS International Journal of Food and Nutritional Sciences*, 11 (12). <https://doi.org/10.48047/ijfans/v11/i12/204>
6. Chauhan, D., Verma, D. & Aggarwal, A. (2022). Hand-Written Characters Recognition using Siamese Network Design. 1st International Conference on Informatics (ICI), Noida, India, 66-70. <https://doi.org/10.1109/ICI53355.2022.9786908>
7. Budapest University of Technology and Economics. Faculty of Electrical Engineering and Informatics. BME Department of Automation and Applied Informatics. (2024). Signature verification research. <https://www.aut.bme.hu/en/Pages/Research/Signature/Introduction>
8. Techsign. (2024). Close Deals At The Speed Of Life. All eSignatures In One. Techsign Doc. <https://www.techsigndoc.com/en/features.html>
9. Olivé, A. (2007). *Conceptual Modeling of Information Systems*. Heidelberg: Springer-Verlag Berlin, 455. URL: <https://doi.org/10.1007/978-3-540-39390-0>
10. Visual Paradigm. (2024). Use Case Diagram Tutorial. <https://online.visual-paradigm.com/diagrams/tutorials/use-case-diagram-tutorial/>
11. Weng, L. (2021). Contrastive Representation Learning. *Lil'Log*. <https://lilianweng.github.io/posts/2021-05-31-contrastive/>
12. Ramus. (2024). RAMUS Java-based IDEF0 & DFD Modeler. <https://ramussoftware.com/>
13. Belkovets, V.Yu. (2021). Research and comparison of neural networks on the example of recognition of handwritten numbers problem solving. Text part of course work by specialty 122 «Computer Science». National University «Kyiv-Mohyla Academy». <https://ekmair.ukma.edu.ua/server/api/core/bitstreams/7ec56f11-b512-4f38-80a2-0d4237234075/content>
14. Tanasiuk, D.O. (2020). Research of computer vision methods to solve the learning problems of signs for reidentification of objects. Certification thesis. The level of higher education is the second (Master's). Explanatory note. Kharkiv National University of Radioelectronics <https://openarchive.nure.ua/server/api/core/bitstreams/650acd74-8a10-4600-9bdc-0477298dcf91/content>
15. Xiao, W. & Ding, Y. (2022). A Two-Stage Siamese Network Model for Offline Handwritten Signature Verification. *Symmetry*, 14(6): 1216. <https://doi.org/10.3390/sym14061216>
16. Sharma, N., Gupta, S., Mohamed, H.G., Anand, D., Mazón, J.L.V., Gupta, D. & Goyal, N. (2022). Siamese Convolutional Neural Network-Based Twin Structure Model for Independent Offline Signature Verification. *Sustainability*, 14 (18): 11484. <https://doi.org/10.3390/su141811484>
17. The SQLite Consortium. (2024). SQLite Small. Fast. Reliable. Choose any three. <https://www.sqlite.org/index.html>
18. Sheldon, R. (2024). Model-View-Controller (MVC). TechTarget. <https://www.techtarget.com/whatis/definition/model-view-controller-MVC>