DOI 10.15276/imms.v14.no4.366
УДК 004.421.4:004.02

Informatics and Mathematical Methods in Simulation
Vol.14 (2024), No. 4, pp. 366-379

РОЗРОБКА ЗАСТОСУНКУ ДЛЯ БІОМЕТРИЧНОЇ ВЕРИФІКАЦІЇ ПІДПИСІВ

Р. І. Назаренко[1], О. А. Стопакевич[1], А. О. Стопакевич[2]

[1]Національний університет «Одеська політехніка»
1, Шевченка пр., Одеса, 65044, Україна
[2]Державний університет інтелектуальних технологій
1, Кузнечна вул., Одеса, 65000, Україна
Email: stopakevich@gmail.com

Верифікація підпису - це процес, під час якого заданий підпис порівнюється з деякими відомими зразками підписів і вирішується, чи належить підпис, що перевіряється, тому самому автору чи ні. Ця перевірка здійснюється за допомогою відповідного програмного забезпечення, створеного за результатами проведених досліджень. Таким чином, метою роботи є розробка алгоритму для ефективного розв'язку задачі верифікації підписів, створення програмного застосунку на основі розробленого алгоритму, перевірка працездатності системи шляхом дослідження функціонування розробленого застосунку з використанням достатньої бази даних автентичних та підроблених підписів різних підписантів. Проведено аналіз стану проблеми, який дозволив знайти базу з 500 автентичних та підроблених підписів, визначити 15 основних ознак підробки підпису як такого, 10 математичних методів порівняння підписів, основні характеристики та структуру алгоритму функціонування застосунку, його архітектуру. Експериментальні дослідження, проведені для перевірки знайдених ознак підробки підпису як такого за числовим значенням критерію стабільності ознаки, дозволили виявити ті ознаки, які доцільно використати в застосунку для перевірки. Також, експериментальні дослідження на базі підписів, проведені для перевірки знайдених математичних методи порівняння відомого автентичного підпису та підпису, який перевіряється, дозволили виявити методи порівняння, які доцільно використати в застосунку. При функціонуванні застосунку цифрові зображення підписів, отримані за допомогою цифрової камери або сканера, обробляються й за допомогою методів розпізнавання образів, знайдених ознак та методів порівняння, здійснюється перевірка. На використаній базі результати перевірки виявилися успішними. Розроблений застосунок може бути удосконалений та послугувати основою економної системи верифікацій підписів.
Ключові слова: біометрична верифікація підписів, кібербезпека, комп'ютерний застосунок, розпізнавання образів.

Вступ. Підпис – це характерно стилізований, написаний від руки варіант чийогось імені або іншого ідентифікаційного слова чи символу, який може бути використаний для підтвердження особи відповідної особи. Підпис людини є характерно унікальний і візуально розрізнюваний. Це зробило підпис давнім розпізнавальним знаком для ідентифікації особи. Навіть сьогодні власноручний підпис є найпоширенішим засобом засвідчення автентичності будь-яких офіційних або фінансових документів. Підпис відображує певні психологічні особливості людини. Сучасні вчені називають сім основних характеристик почерку, за якими можна створити портрет людини: розмір літер, їхній нахил і форма, напрямок почерку, інтенсивність натиску, характер написання слів і загальна оцінка почерку. Верифікація підпису - це процес, під час якого заданий підпис порівнюється з деякими відомими зразками підписів і вирішується, чи належить підпис, що перевіряється, тому самому автору чи ні. Ця перевірка здійснюється за допомогою певних характерних досліджень або аналізу. При автоматичній перевірці підписів перевірка підписів здійснюється машиною з використанням деяких методів розпізнавання образів. Під час перевірки за зображенням підписів зображення підписів отримують за допомогою цифрової камери або сканера. Ці цифрові зображення підписів

обробляються далі й за допомогою методів розпізнавання образів здійснюється перевірка. Мета роботи – провести аналіз стану наукової проблеми, розробити алгоритми для ефективного розв'язку задачі верифікації підписів, упевнитись в працездатності алгоритмів шляхом розробки прототипу застосунку.

Аналіз стану наукової проблеми. Для практичного використання біологічні ознаки при ідентифікації особи повинні відповідати такими основним вимогам [1-10]: універсальність, тобто ознака має розпізнаватися у кожному підпису і не має втрачається через нещасний випадок або хворобу; відмінність, тобто або ознаки у підписів двох різних людей повинні бути достатньо відмінними, щоб надійно відрізнити одну підпис від іншої; інваріантність, тобто ознака має бути стабільною протягом тривалого періоду часу; простота вимірювання, бажано без застосування спеціального обладнання; та необхідно враховувати наступні фактори [3]: швидкість розпізнавання; зручність для користувачів; захищеність, тобто захист від подачі фальсифікованої інформації. Підпис - це стилізований, написаний від руки варіант чийогось імені або іншого ідентифікаційного слова чи символу, який може бути використаний для підтвердження особи. Він є унікальним та візуально розрізнюваним. Навіть сьогодні власноручний підпис є найпоширенішим засобом засвідчення автентичності будь-яких офіційних або фінансових документів [4]. Основними причинами популярності підпису є простота виготовлення; перевірка власноручного підпису здійснюється візуально без особливих труднощів; підпис може бути переоформлений, тобто за потреби (у випадку компрометації) можна змінити свій підпис до певної міри, що неможливо з іншими біометричними даними [10]. Сучасні вчені називають сім основних характеристик почерку: розмір літер, їхній нахил і форма, напрямок почерку, інтенсивність натиску, характер написання слів і загальна оцінка почерку [5, 7]. Графологи вважають, що людський мозок підсвідомо "водить" рукою того, хто пише. Цим пояснюється і те, що під час дорослішання і зміни характеру почерк людини змінюється. Однак зв'язок не є достатньо надійним для того, щоб робити впевнені висновки. Мета-аналіз понад 200 досліджень показав, що графологія виявилася нездатною визначити наявність будь-якої риси особистості, що виявляється за будь-якою методикою тестування. Також графологам не вдалося правдиво оцінити й трудові здібності людини. [8, 9]. Перелік основних характеристик підписів з позиції графології показано на рис. 1.

Рис.1. Класифікація ознак підписів [11,12]

Рис.2. Оригінальні підписи [13, 14]

Суттєво більшого прогресу досягнуто у вивченні почерку під час досудового розслідування кримінальних справ, яке має в основному криміналістичні завдання [5-7]. Почеркознавча експертиза визначає, ким виконано текст досліджуваного документа,

одна чи різні особи писали в різних документах, чи є справжнім підпис тощо. Процедури кримінальної почеркознавчої експертизи підписів показують, що лише за формальними ознаками, показаними на рис. ., визначати правдивість підпису не коректне.

Це пояснюється такими основними причинами: залежно від психофізичного стану людини та її соціокультурного оточення, в різний час підписи однієї й тієї ж особи можуть суттєво відрізнятися [15]; дві справжні підписи однієї особи ніколи не можуть бути геометрично ідентичними; не всі підписи можуть бути класифіковані за приведеними на рис.1. ознаками, а підписи можуть бути складними для класифікації, наприклад ті, що показані на рис. 2. Інші підписи можуть бути занадто простими. В криміналістиці орієнтуються на те, що підпис є психологічним відображенням стану людини. Тому для людини її підпис є природним, а для інших людей виконання чужого підпису вимагає додаткової роботи, сліди якої й шукаються. Признаками підробки можуть бути: порушення координації рухів, немотивовані зупинки, уповільнений темп письма, вдавлені штрихи, неприродне натиснення, надмірна механічно сформована рівномірність елементів підпису тощо. Зазвичай, дослідники розглядають класифікацію підробок підпису, приведену в табл. 1.

Таблиця 1.

Класифікація підробок підпису

№	Деталізований опис підробки підпису [16]	Звичайна назва
1	Підпис є справжнім підписом іншої особи	Випадкова
2	Підробляється, знаючи лише ім'я справжнього підписанта	Проста чи випадкова
3	Підпис візуально імітується	Проста
4	Виготовлена без знання правопису підпису	Проста
5	Виготовлена без належного тренування	Проста
6	Виготовлена професійним фальсифікатором	Кваліфікована

Верифікація підпису - це процес, під час якого заданий підпис порівнюється з деякими відомими зразками підписів і вирішується, чи належить підпис, що перевіряється, тому самому автору чи ні. При автоматичній перевірці, перевірка здійснюється машиною з використанням деяких методів розпізнавання образів. Дослідження в галузі автоматичної верифікації підписів почалися з середини 60-х років 20 ст. [4]. Спочатку верифікація підписів ґрунтувалася на статичній природі підпису та використовувалися геометричні параметри, пов'язані з формою підпису, але пізніше також почали розглядати динамічні ознаки підписів, такі як початкова точка підпису, напрямок штрихів, кількість штрихів, швидкість і прискорення пера тощо. Таким чином, сформувалися два підходи [17,18]. В першому зображення підписів отримуються за допомогою цифрової камери або сканера, обробляються далі й за допомогою розпізнавання образів здійснюється перевірка. В другому використовують спеціальні пристрої, наприклад: оцифровуючий планшет, електронне перо, персональний цифровий асистент, спеціальний стілус із встановленою на ньому камерою, які генерують сигнали відповідно до динамічного відтворення підпису. Отримані параметри не є візуальними і фальсифікатор ніколи не зможе отримати до них. Тому при перевірці з додатковим пристроєм може бути потенційно досягнуто вищий рівень розпізнавання.

Недоліком такої перевірки є: необхідність залучення людини, чий підпис перевіряється; процедура не є автоматичною, оскільки від людини вимагається зробити підпис не на папері, а на спеціальному пристрої; коректна процедура вимагає не тільки зняття підпису, а й перевірку попередніх підписів зі знятим, щоб виключити фактор впливу психологічного дискомфорту й незвичності на процедуру зняття. Метод є доцільним лише для перевірки дуже важливих підписів. В статті розглянуто задачу перевірки підпису лише за зображенням.

Процедура верифікації підпису узагальнено має наступні етапи: збір даних – за допомогою цифрової камери або сканера фіксується зображення підпису (шаблон); проводиться попередня обробка: фільтрація, проріджування, бінаризація, обрізання, зміна розміру, скелетування, корекція перекосу, корекція нахилу; виділення ознак – виконується для зменшення обсягу даних, присутніх у шаблонах, шляхом вимірювання їх [19]; вибір надійних ознак шляхом відбору найкращих ознак і видалення нерелевантних ознак з повного набору ознак [20, 21]; класифікація підписів на автентичний і підроблений; ефективність оцінюється за частотою помилкових відмов (FRR) та частотою помилкових підтверджень (FAR) [22].

Перевірка підпису за зображеннями ведеться за такими підходами: зіставлення з шаблонами; статистичний; структурний або синтаксичний; на основі спектрального аналізу; на основі нейронних мереж [22–26]. У зіставленні створюється шаблон на основі наявних навчальних зображень. Цей шаблон порівнюється з новим тестовим зразком. Якщо тестовий зразок має варіації або спотворення, швидкість розпізнавання в цьому підході знижується. Це робить зіставлення з шаблоном підходом до розпізнавання образів. Тому, якщо зображення сигнатур спотворені, неправильно орієнтовані або є великі внутрішньокласові відмінності між сигнатурами, швидкість верифікації при такому підході буде дуже низькою. Але цей підхід самий ефективний для виявлення простих підробок і не підходить для виявлення кваліфікованих підробок та є найпростішим серед усіх інших підходів. При перевірці з допомогою статистичного підходу кожен патерн (тобто зображення сигнатури) представлений d-кількістю ознак, тобто розглядається як точка в d-вимірному просторі ознак. Вибір ознак повинен бути таким, щоб вектори ознак зі схожого класу займали компактні та відокремлені (від векторів ознак інших класів) області в просторі ознак, де можна легко відокремити зразки з різних класів. Популярні статистичні підходи до розпізнавання образів – це прихована марковська модель та баєсівська модель. Структурний підхід в основному використовується з іншими методами в автономній перевірці підписів, коли зображення підпису розглядається як єдине ціле. За наявності дуже великої навчальної вибірки цей підхід дає хорошу верифікацію, але його обчислювальні витрати дуже великі. При підході з використанням спектрального аналізу підписи з урахуванням кривизни розкладаються у формат з різною роздільною здатністю. Цей метод може бути застосований до різних мов. Перевагами використання нейромережевого підходу до верифікації підписів є уніфікація вилучення ознак і класифікації та гнучкість при пошуку. Кожен підхід має свої переваги та недоліки. Підходи були подані в порядку зростання вимог до вибірки даних. Оскільки пошук в інтернеті показав, що знайти в вільному доступі великі та різноманітні бази вибірок не можливо, то доцільними до дослідження є тільки дві підходи. Ми зупинимось на статистичному, як такому, який вимагає досліджень, але для досягнення задовільного результату розпізнавання вибірка може бути малою. В роботі [27] було проаналізовано вплив роздільної здатності зображення на точність функціонування системи перевірки підпису. Експеримент показав, що для якісної роботи було достатньо роздільної здатності в 150 точок на дюйм.

Розробка комп'ютерного алгоритму для верифікації підписів. В роботі використана наступна процедура обробки.

1. Фільтрація. Скановане зображення підпису може містити шум. Шум на зображенні погіршує виділення ознак і подальші процеси розпізнавання. Тому фільтрація шуму є неминучим етапом попередньої обробки при розпізнаванні образів. Було помічено, що скановані зображення зазвичай схильні до впливу імпульсного шуму, що призводить до появи випадкових чорних та білих пікселів. Медіанний фільтр ефективно видаляє цей тип шуму, зберігаючи краї зображень.

2. Бінарізація. Спочатку кольорове RGB зображення перетворюється у відтінки сірого. Існує декілька поширених методів такого перетворення. В роботі застосовано модифікований метод врахування яскравості, який використано в відомих телевізійних

стандартах SECAM, PAL, NTSC та в пакеті MATLAB Image Processing, де $I = 0.2989 \cdot R + 0.587 \cdot G + 0.114 \cdot B$. Для перетворення відтінків сірого у бінарне зображення використовується відповідне порогове значення (значення пікселя). Якщо значення пікселя у відтінках сірого перевищує порогове значення, то новому значенню пікселя присвоюється 1 (одиниця), інакше 0 (нуль). Таким чином, нове зображення матиме лише два значення пікселів '1' (що відповідає білому кольору) та '0' (що відповідає чорному кольору).

3. Обрізання. Скановане зображення підпису містить підпис і деякі білі області, що не містять підпису. Ці надлишкові ділянки видаляються шляхом обрізання зображення до прямокутника, що обмежує частину підпису.

4. Проріджування. При проріджуванні штрихи зображення підпису стають товщиною в один піксель. Але під час проріджування може бути втрачена деяка інформація про зображення підписів, наприклад, ширина штрихів.

5. Скелетування. Зберігає зв'язність сегментів підпису, які були початково з'єднані, і видаляє з зображення вибрані пікселі переднього плану. Після скелетування зображення підпису перетворюється на комбінацію деяких тонких дуг і кривих. Одним з основних способів виконання скелетування є використання процесу морфологічного проріджування, який послідовно видаляє пікселі від межі. Цей процес триває доти, доки проріджування не стане неможливим. Приклад скелетованого зображення приведено на рис. 3.

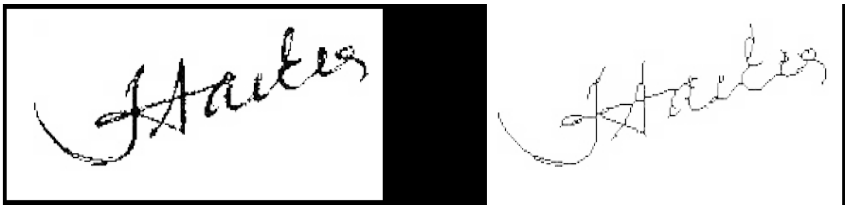

Рис.3. Приклад скелетованого зображення.

6. Корекція перекосу. Після корекції перекосу остаточне зображення робиться паралельним до горизонтальної осі. Використано метод, описаний в [28]: зображення підпису переміщають до початку координат, обчислюють мінімальне власне значення матриці, сформованої за новими координатами зображення підпису; обчислюють кут нахилу ϕ за власним вектором; після знаходження кута нахилу виконується корекція перекосу шляхом застосування перетворення обертання до кожного пікселя зображення підпису.

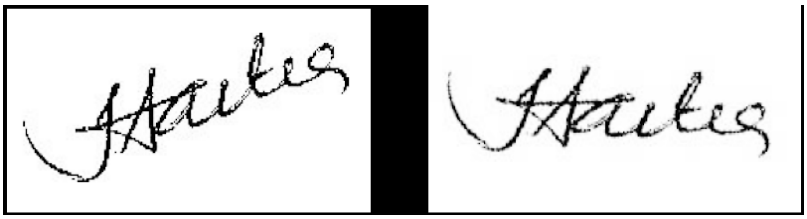

Рис.4. Приклад корекції перекосу: а-до перекосу, б-після перекосу

7. Масштабування. Довжина підпису є різною для різних підписантів. Навіть довжина підписів однієї людини також не однакова. Але коли використовується підхід перевірки підпису на основі сітки, підписи проецируються на сітку однакового розміру. Отже, всі підписи повинні бути однакового розміру. Найпростішим методом зміни розміру зображення є свого роду геометричне перетворення. Для цього є дві основні операції: просторове перетворення та інтерполяція рівня сірого. При просторовому перетворенні вибираються деякі пікселі або точки ("точки прив'язки"), положення яких на вихідному і зміненому зображенні точно відомі. На основі їхнього розташування на двох зображеннях формується рівняння просторового перетворення. Це рівняння використовується як рівняння відображення, щоб визначити положення всіх пікселів на

новому зображенні зі зміненим розміром. Інтерполяція рівня сірого використовується для присвоєння рівнів сірого новим пікселям на зміненому зображенні. Використовується метод найближчого сусіда. У цьому методі рівень сірого призначається відповідно до пікселя, який є найближчим до пікселя, що відображається [29].

Аналіз літератури показав, що в цілому для розглянутої задачі можливо визначати наступні ознаки для аналізу підпису без порівняння.

1. Нахил лінії, яка з'єднує лівий ніжній та правий верхній обрізаного зображення підпису.

2. Співвідношення сторін. Це відношення ширини підпису до висоти підпису обрізаного підпису. Видно, що співвідношення сторін підписів людини справедливо залишається постійним. Якщо висота підпису дорівнює H, а ширина підпису W, то співвідношення сторін *AR* задається формулою $AR = W / H$.

3. Чиста висота - це максимальна кількість загальних пікселів зображення (тобто чорних пікселів) серед усіх стовпців, підрахованих після обрізання зображення підпису.

4. Чиста ширина - це максимальна кількість загальних пікселів зображення (тобто чорних пікселів) серед усіх рядків, підрахованих після обрізання зображення підпису.

5. Нормалізована висота підпису - це відношення максимальної чистої висоти до максимальної чистої ширини.

6. Площа обмежувальної прямокутної рамка (реальної області підпису). Для визначення в бінарному зображення потрібно застосовувати наступний алгоритм: очищення зображення від шумових точок, що не пов'язані з основною структурою (для цього можна застосовувати Matlab функцію $im = \mathrm{bwmorph}(im_{in}, 'clean', \infty)$); визначення крайніх границь за стовпцями, а саме ліва границя $x_{\min} = \min\{i \mid \exists j : im(j,i) = 0\}$, та права границя $x_{\max} = \max\{i \mid \exists j : im(j,i) = 0\}$; пошук крайніх границь за рядками $y_{\min} = \min\{j \mid \exists i : im(j,i) = 0\}$, $y_{\max} = \max\{j \mid \exists i : im(j,i) = 0\}$; розрахунок ширини й висоти прямокутника, а саме ширина $\mathrm{w} = x_{\max} - x_{\min} + 1$, висота $\mathrm{h} = y_{\max} - y_{\min} + 1$. Таким чином, маємо координати $\mathrm{x}_{\min}, y_{\min}$ й розміри *w* і *h* прямокутника.

7. Нормалізована площа підпису (відносно обмежувальної рамки). Коли зображення підпису скелетизоване, площа підпису є мірою щільності слідів підпису. Якщо на зображенні підпису загальна кількість чорних пікселів дорівнює B, а загальна кількість пікселів у всьому зображенні дорівнює P, то нормалізована площа підпису дорівнює $NSA = B / P$. При порівнянні бінарних зображень однакових розмірів достатньо розраховувати кількість чорних пікселів.

8. Центр ваги у напряму *X*. У бінарному зображенні підпису з чорними пікселями центр ваги це координата *X* середньої точки координат усіх чорних пікселів по горизонталі

$$X = (\sum_{i=1}^{n} x_i) / N$$

де x_i - номер стовпчика чорних пікселів (Matlab функції regionprops).

9. Центр ваги у напряму *Y*. У бінарному зображенні підпису з чорними пікселями центр ваги це координата *Y* середньої точки координат усіх чорних пікселів по вертикалі

$$Y = (\sum_{i=1}^{n} y_i) / N,$$

де y_i - номер рядка чорних пікселів (Matlab функція regionprops).

10. Центр ваги X_1 лівої половини підпису у напряму *X*.

11. Центр ваги Y_1.лівої половини підпису у напряму *Y*.

12. Центр ваги X_2 правої половини підпису у напряму *X*.

13. Центр ваги Y_2. правої половини підпису у напряму *Y*.

14. Базовий зсув $Y_2 - Y_1$ (Matlab функції regionprops).

15. Нахил між центрами ваги лівої та правої половин підпису $m = (Y_2 - Y_1)/(X_2 - X_1)$.

У порядку підготовки для проведення експерименту по обґрунтуванню вибору мінімальної релевантної кількості ознак можна провести грубу класифікацію зовнішнього виду підписів на три вибірки. Дещо адаптований приклад виділення спеціальних ознак для одного типу підпису показаний на рис.5.

Рис.5. Характерні признаки підпису одного типу [30].

Таким чином, у першій вибірці підписи (300 підписів, 63% з яких є справжніми) мають нахил, діагональні та горизонтальні довгі штрихи. У другій вибірці підписи мають відірвану частину. У третьої вибірці підписи мають вертикальні довгі штрихи. Об'єми другої та третьої вибірок приблизно рівні, кількість підробок в кожній групі близько 50%. Бсього було досліджено 500 підписів. При проведенні експерименту було зроблено два істотних спрощення: варіації справжнього підпису невеликі, відмінності між справжнім та підробленим підписом візуально помітні.

Важливим є аналіз стабільності та релевантності ознак для підписів трьох різних типів. Введемо поняття індексу нестабільності, якій можна визначити за формулою

$$II = \frac{SD_G}{\mu_G} : \frac{SD_F}{\mu_F},$$

де SD_G, SD_F – стандартні відхилення ознаки автентичного та підробленого підпису, μ_G, μ_F – середні значення ознаки автентичного та підробленого підпису. Чим більше значення *II*, тим менш достовірною є ознака. Значення *II*>1 вказує на чітко нерепрезентативну ознаку, а ознаки менші за 0.5 можуть бути доцільними до розгляду.

Для кожної з трьох вибірок індекс розраховувався окремо за 15 ознаками. Автори застосували вибірку, яку отримали шляхом залучення груп людей, які робили підписи та підроблювали їх.

Результати експерименту показані на рис. 6.

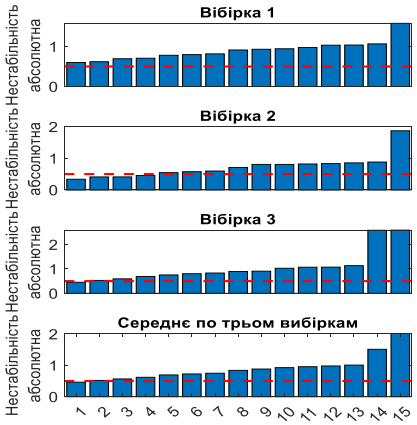

Рис. 6. Узагальнена статистика по *II* за трьома вибірками окремо та у середньому.

З рис. 6 бачимо, що у цілому майже всі ознаки мають індекс нестабільності вище за мінімально припустимий (0.5). Чим більший номер ознаки, тим більш в середньому вона не стабільна. Таким чином, виберемо ознаки з номерами 1 та 2.

Подальші експериментальні дослідження на виборці в сто підписів показали, що доцільно додати ще дві ознаки, це число Ейлера (дорівнює різниці між числом незв'язаних фрагментів підпису та числом отворів в цих фрагментах отворів в цих об'єктах, для визначення числа для бінарного зображення можна застосовувати Matlab-функцію bweuler), а також співвідношення сторін рамки підпису. Для порівняння зображення автентичних підписів необхідно спеціально підготовити, скелетузувати й привести до одного масштабу.

Далі треба визначити математичне забезпечення для порівняння різних підписів. Експериментальний аналіз ознак на вибірці в 100 підписів різних типів показав, що порівняння зображення певного реального підпису та певного підробленого підпису є задачею, яка не може бути розв'язаною з задовільною точністю.

Звичайно, можна спробувати застосувати нейромережу та машинне навчання. В прикладі [31] показано, що застосування доволі розвинутого пакета Ground DINO, який навчали визначати різні об'єкти на зображенні, не призводить до надійного результату. Час пошуку доволі тривалий (пів хвилини), а результат залежить від запиту й може бути невірним. Спеціалізоване навчання вимагає спеціальної вибірки й займе час. В той час як за допомогою визначення простих метрик задача розв'язується краще й істотно швидше.

Розглянемо задачу визначення відстаней між бінарними зображенннями *im1* та *im2*.

Індекс Жаккара $J = |im1 \cap im2| / |im1 \cup im2|$, де значення J = 1 вказує на ідентичність зображень, та його варіанти індекс Дайса $D = 2 \cdot |im1 \cap im2| / |im1| + |im2|$ та індекс Танімото

$$T = |im1 \cap im2| / \left(|im1| + |im2| - |im1 \cap im2| \right).$$

Евклідова відстань (обчислюється по пікселам) $E = \sqrt{\sum_{i,j} (im1(i,j) - im2(i,j))^2}$.

Манхеттенська відстань $M = \sum_{i,j} |im1(i,j) - im2(i,j)|$.

Хеммінгова відстань підраховує кількість відмінних пікселів між зображеннями, що відображає структурні зміни $H = \sum_{i,j} (im1(i,j) \neq im2(i,j))$.

Коефіцієнт кореляції Пірсона визначає лінійну кореляцію між зображеннями $PRS = \text{cov}(im1, im2) / \left(\sigma_{im1} \cdot \sigma_{im2} \right)$, де *PRS*=1 означає абсолютну схожість.

Логарифмічне відношення шансів $LOR = \log\left(P_1 / \left(1 - P_1\right) \right) - \log\left(P_2 / \left(1 - P_2\right) \right)$, де P_1 і P_2 - ймовірність білих пікселів для *im1* та *im2,* відображає асиметрію розподілу пікселів.

Таким чином, маємо метрики, що забезпечують різний підхід до оцінки схожості, від топологічних характеристик до геометричних і статистичних залежностей.

Виявилось що доволі позитивний результат дає порівняння нового підпису з множиною різних автентичних підписів. Для цього з автентичних підписів вибирається можливий діапазон розкиду ознак й проводиться перевірка, чи входить значення ознаки певного зображення до діапазону відхилень ознак автентичних підписів.

Для підвищення точності краще мати підписи однієї людини, що відрізняються, тобто зроблені в різний час, в різному настрої тощо. Спеціальних вимог до зображення не ставиться. Зображення має бути автоматично вичищено від фону, скелетизовано, зайві пусті частини та плями мають бути відрізані.

Порівняння зображення підпису з автентичними зображеннями підпису має проводитись в одному масштабі зі збереженням пропорцій. Збільшення кількості ознак не обов'язково призводить до гарного результату класифікації.

Насправді в більшості ситуацій це матиме негативний вплив на класифікацію. Це пов'язано з тим, що всі виділені ознаки можуть не нести суттєвої унікальності свого батьківського шаблону. Деякі з ознак несуть неоднозначну інформацію про зразок, що заплутує систему класифікатора і, як наслідок, знижує точність класифікації.

Таким чином, з усіх вилучених ознак необхідно відібрати деякі корисні ознаки для підвищення ефективності класифікації.

Якщо класифікатор наповнити нерелевантними ознаками, то можуть виникнути три проблеми: через велику кількість ознак зростають обчислювальні витрати; наявність нерелевантних ознак може призвести до помилкової класифікації і, таким чином, ефективність класифікації знижується; нерелевантні ознаки можуть спричинити надмірну підгонку.

Розроблені алгоритми, представлені на рис. 7 -11.

Рис.7. Алгоритм функціонування графічного інтерфейсу застосунку

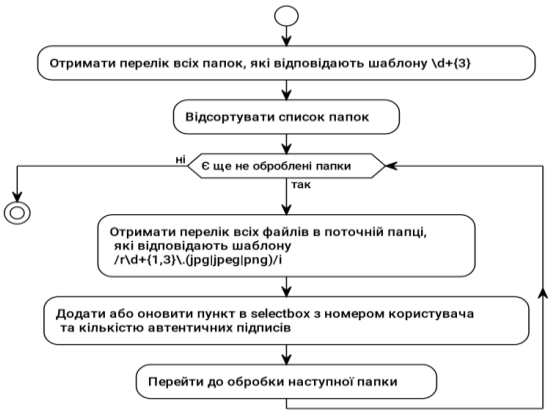

Рис. 8. Алгоритм завантаження переліку користувачів в selectbox

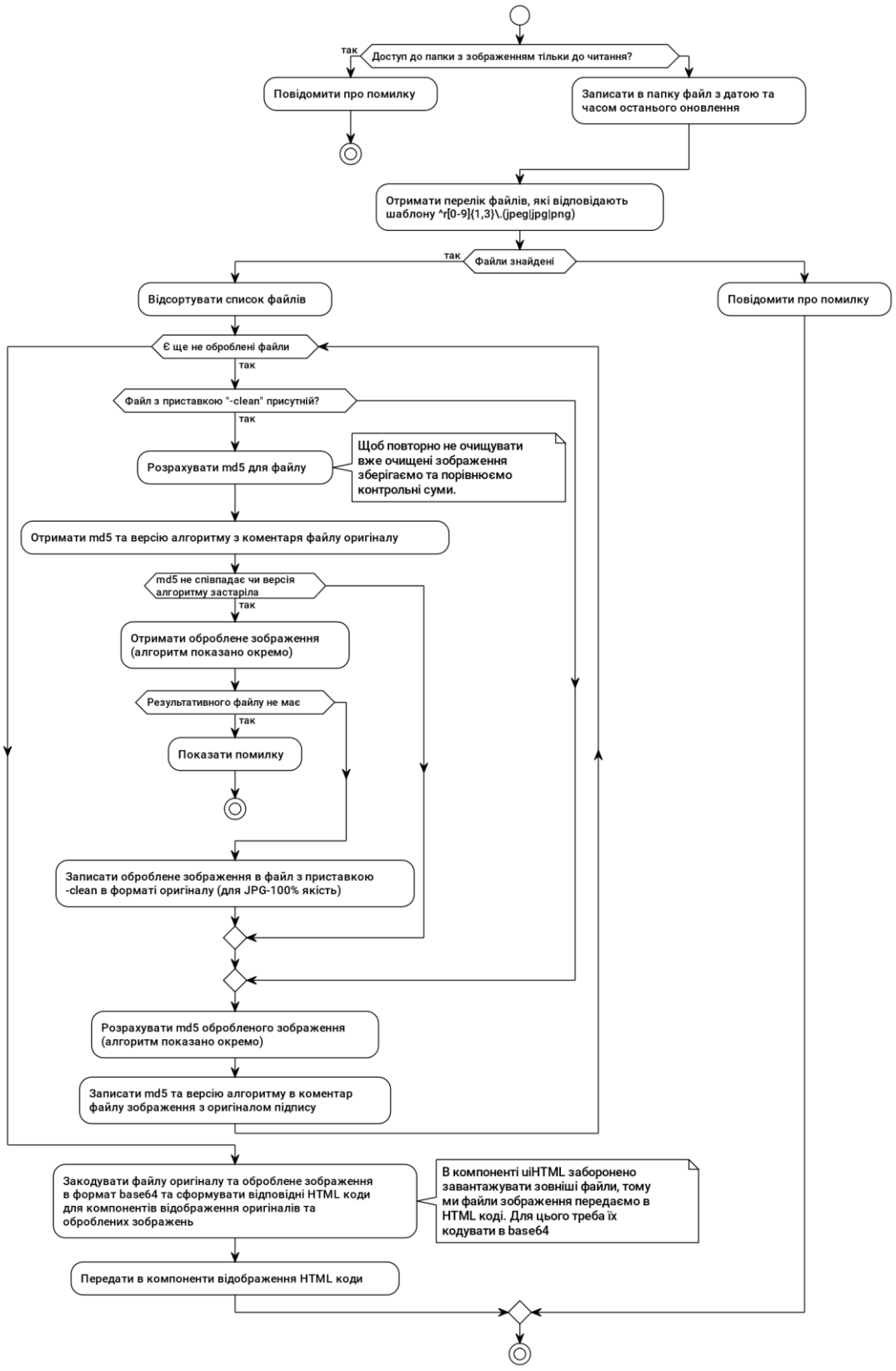

Рис.9. Алгоритм обробки зображень в папці з автентичними підписами користувача

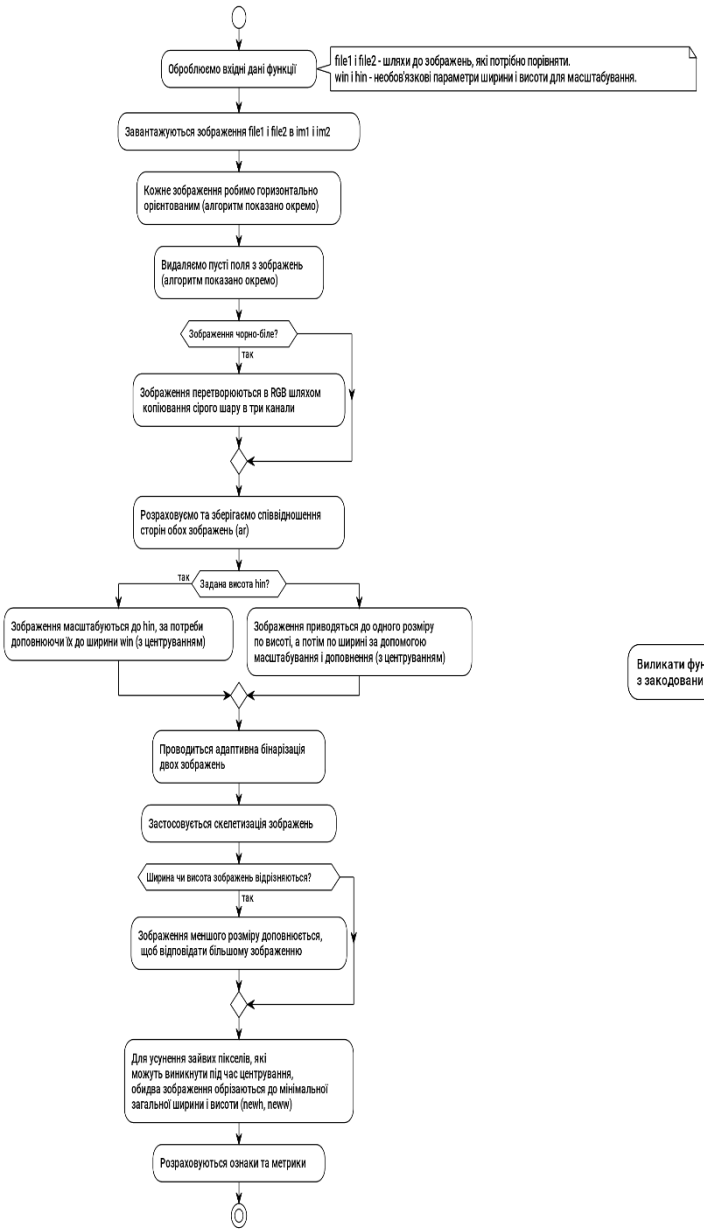

Рис.10. Алгоритм кодування зображення в форматі base64 для відображення в компоненті uiHTML

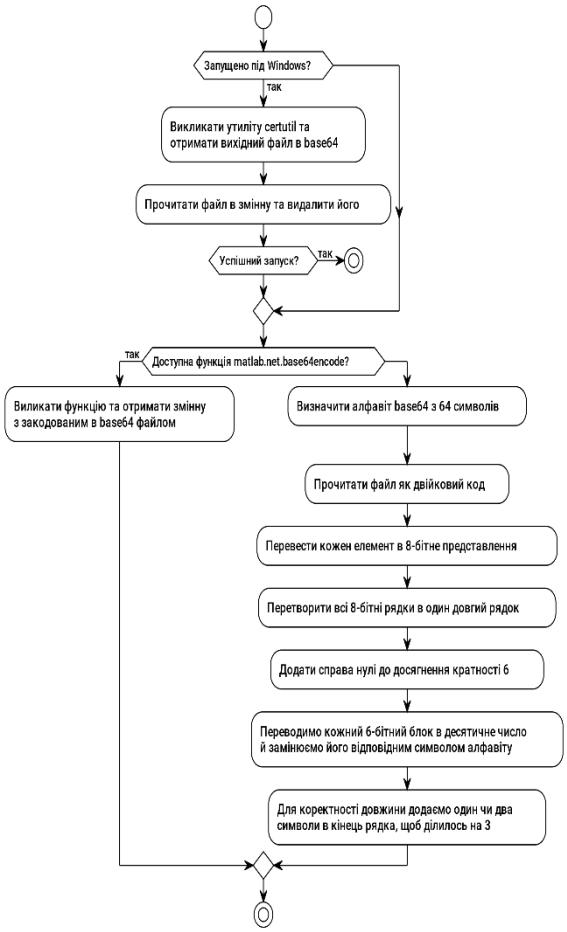

Рис.11. Алгоритм порівняння двох зображень

Розробка програмного застосунку. Розроблений макет головного вікна показаний на рис.12.

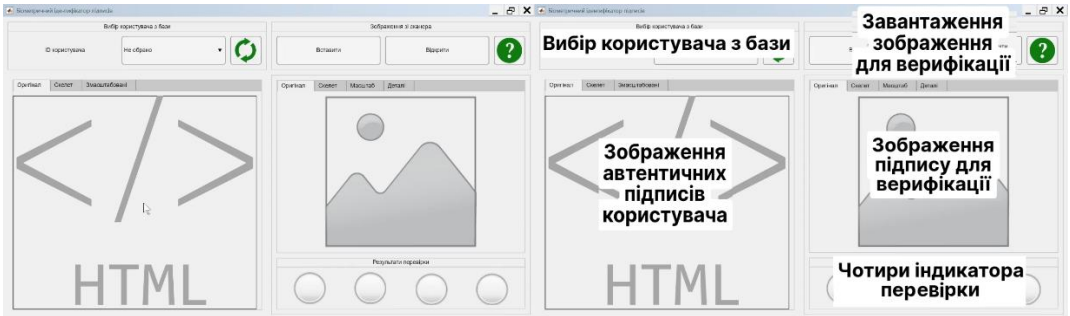

Рис.12. Макет головного вікна застосунку та поясненне його основних зон

Порядок роботи користувача застосунку з інтерфейсом наступний: з переліку клієнтів за номером обирається клієнт; візуально переглядаються реальні підписи клієнта, щоб впевнитись, що це саме той клієнт і саме той підпис (якщо підпис геть на

такий, тобто фальсифікатор не знав як виглядає реальний підпис, то перевіряти програмою не має сенсу); користувач сканує зображення для перевірки, копіює з нього область з підписом і вставляє в програму. Після перевірки її результат відображається на індикаторах. Зелений колір – індикатор пройшов перевірку, червоний – ні. Вірогідність достовірності підпису тим більша, чим більше зелених індикаторів.

Для перевірки використано набір даних під назвою "handwritten signatures - Genuine and ForgedSignature Examples" з публічного репозиторію Kaggle. Набір даних містив чотири папки зі справжніми та підробленими підписами. В результаті було сформовано 109 папок для кожного окремого користувача, в яких приблизно порівну автентичних та підроблених підписів.

Приклад результатів перевірки показаний на рис. 13.

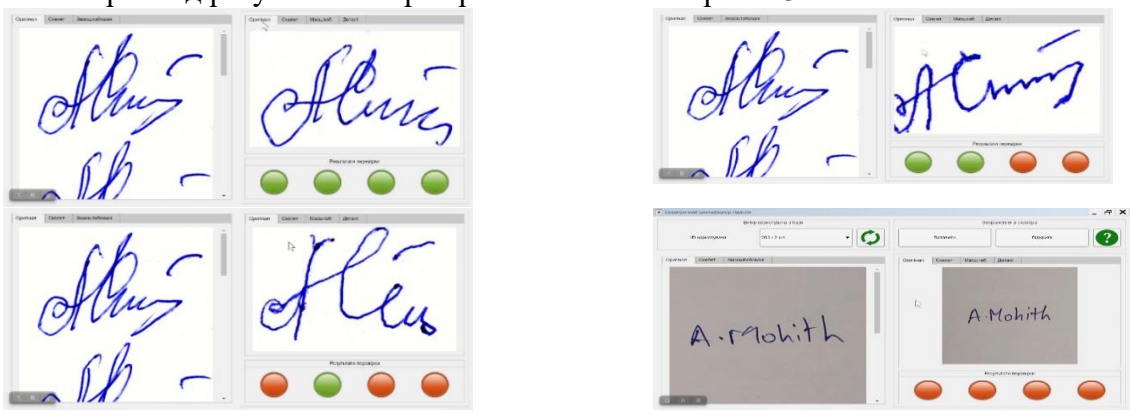

Рис.13.Приклади результатів порівняння

Отже, результат експериментальної перевірки роботи застосунку показує що робота алгоритму є задовільною.

Висновки. В роботі розв'язана задача біометричної автентифікації користувачів за підписом. Для перевірки розроблено алгоритм, який проводить аналіз скелетованих зображень, що масштабується до єдиного розміру, а також оцінюється відповідність значень признаків діапазону для автентичних підписів. Розробка застосунку здійснена на базі Matlab, оскільки ця платформа підтримує швидке прототипування й має вбудовані інструменти для обробки зображень. Програмний код застосунку реалізований у вигляді класу з графічним інтерфейсом у Matlab App Designer, що забезпечує інтуїтивно зрозумілий інтерфейс для завантаження зразків підписів, їх перегляду і порівняння. Розроблений застосунок є кросплатформовим, а інтерфейс відтворює стиль Windows для зручності користувачів. Доступна вкладка "Деталі" містить таблицю з усіма розрахованими метриками та ознаками, що підсилює можливості детального аналізу результатів. Перевірка на вибірці підписів показала високу ефективність алгоритму та підтвердила його коректність у розпізнаванні автентичних підписів та виявленні підробок.

Список літератури

1. Царьов Р.Ю., Лемеха Т.М. Біометричні технології. Одеса : ОНАЗ ім. О.С. Попова, 2016. 140 с
2. Коваль Л.Г., Злепко С.М., Новіцький Г.М., Крекотень Є.Г. Методи і технології біометричної ідентифікації за результатами літературних джерел. *Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки.* 2019. Том 30 (69). Ч. 1. № 2. С.104-112
3. Jain A.K., Ross A., Prabhakar S. An Introduction to BiometricRecognition," *IEEE Transactions on Circuits and Systems for Video Technology*. 2004. vol. 14. No.1. pp. 4-20
4. Свобода Є.Ю. Підпис як засвідчувальний знак та його значення. *Часопис Академії адвокатури України*. 2012. №16.

5. Абрамова В.М. Садченко О.О., Свобода Є.Ю. Альбом схем із судово-почеркознавчої експертизи. К.: Паливода, 2003. 120 с
6. Меленевська З.С. Свобода Є.Ю., Шаботенко А.І. Судово-почеркознавча експертиза. К.: Укр. центр духовної культури, 2007. 280 с.
7. Методика дослідження підписів. К.: ДНДЕКЦ МВС України, 2009. 21 с.
8. Dean G.A. The bottom line: effect size. Buffalo, N.Y.: Prometheus Books, 1992. p.269-341. Графологія – критичне мислення. 2023. URL: https://criticalthinkerua.wordpress.com/2023/ 07/15/graphology/
9. Pal S., Pal U., Blumenstein M. Signature-Based Biometric Authentication. In Computational Intelligence in Digital Forensics: Forensic Investigation and Applications. Springer International Publishing, 2014. P. 285-314.
10. Pinterest. URL: https://uk.pinterest.com/pin/727120302322104429/
11. Ваш підпис має значення. 2021. URL: https://vk-kp.info/novyny-ukrainy-ta-svitu/21002-vash-pidpys-maie-svoie-znachennia-i-vplyv-na-doliu-yak-zrobyty-ioho-shchaslyvym
12. Автограф як мистецтво. Незвичайні підписи знаменитостей. URL: https://www.legaltechnique.org/articles/znamenitosti/avtograf-kak-iskusstvo-neobichnie-podpisi-znamenitostej-bull-novosti-v-fotografiyah.html#google_vignette
13. Як розписуються знаменитості. URL: https://buildstuff.com.ua/yak-rozpisuyutsya-znamenitosti-pidpisi-znamenitix-lyudej-cikavi-fakti-mifi-ta-legendi/#google_vignette
14. Plamondon R. The Handwritten Signature as a Biometric Identifier:
15. Psychophysical Model and System Design. European Convention on Security and
16. Detection. 1995. P. 16-18.
17. Nguyen V., Blumenstein M., Muthukkumarasamy V., Leedham G. Off- line Signature Verification using Enhanced Modified Direction Features in Conjunction with Neural Classifiers and Support Vector Machines. *International Conference on Document Analysis and Recognition*. 2007. P. 734–738.
18. Batista L., Rivard D., Sabourin R., Granger E., Maupin P. State of the art in off-line signature verification in Pattern Recognition Technologies and Applications: Recent Advances. New York: IGI Global, 2008. P. 39-62.
19. Impedovo S., Ottaviano L., Occhinegro S. Optical character recognition – A survey. *International Journal of Pattern Recognition and Artificial Intelligence*. 1991. V. 5. No. 1/2. P. 1-24.
20. Hafemann L. G., Sabourin Ro., Oliveira L.S. Offline Handwritten Signature Verification-Literature Review. *arXiv preprint arXiv:1507.07909*. 2015. P.1-19,
21. Mauceri A.J. Feasibility studies of person identification by signature verification. Report No. SID 65 24 RADC TR 65 33. Anaheim, USA: Space and Information System Division, North American Aviation Co., 1965.
22. Wadhawan A., Kumar D. Design and Analysis of Online Punjabi Signature Verification System Using Grid Optimization. *Second International Symposium on Security in Computing and Communications, SSCC* . Delhi, India. 2014.
23. Судова експертиза: проблеми сьогодення та перспективи розвитку/ Львівський науково-дослідний інститут судових експертиз. Дрогобич : Просвіт, 2020.
24. Urmila A. Patil, J.N. Patil, N.N. Patil. A comparative study of various methods for offline signature verification. *IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), Ghaziabad*. 2014. P. 760-764.
25. Arya M. S., Inamdar V. S. A Preliminary Study on Various Off-line Hand Written Signature Verification Approaches. *International Journal of Computer Applications.* 2010. V. 1. No. 9. P. 50-56.
26. Hou W., Ye X., Wang K. A Survey of Off-Line Signature Verification. *IEEE International Conference on Intelligent Mechatronics and Automation*. *Chengdu, China*, 2004. P. 536-541.

27. Jain A. K., Duin R. P. W., Mao J. Statistical Pattern Recognition: A Review. *IEEE Transactions on Pattern Analysis and Machine Intelligence.* 2000. V. 22. No. 1. P. 4-37.
28. Theodoridis S., Koutroumbas K. Pattern Recognition. Elsevier, 2009.
29. Virajitha K., Navya B., Boggavarapu, Kumar L.N.P., Vaddi R. S. Vankayalapati H. D. Simple and Effective Techniques for Skew Correction, Slant Correction and Core-Region Detection for Cursive Word Recognition. *International Conference on Information Systems Design and Intelligent Applications. Visakhapatnam, India*. 2012. P. 353-361.
30. Gonzalez R. C.,. Woods R. E. Digital Image Processing. Prentice Hall, 2002.
31. Morales A., Morocho D., Fierrez J., Vera-Rodriguez R. Signature authentication based on human intervention: performance and complementarity with automatic systems. *IET Biometrics.* 2017. V. 6. Is. 4. P. 307–315. URL: https://doi.org/10.1049/iet-bmt.2016.0115
32. Machine learning is not all you need: a case study on signature detection. URL: https://towardsdatascience.com/machine-learning-is-not-all-you-need-a-case-study-on-signature-detection-9551f2e5d0e7

DEVELOPMENT OF AN APPLICATION FOR BIOMETRIC VERIFICATION OF SIGNATURES

R. I. Nazarenko[1], O. A. Stopakevych[1], A. O. Stopakevych[2]

[1]National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
[2]State University of Intellectual Technologies
1, Kuznechna, Odesa, 65000, Ukraine».
Email: stopakevich@gmail.com

Signature verification is a process during which a given signature is compared with some known signature samples and it is decided whether the signature being verified belongs to the same author or not. This verification is carried out using appropriate software created based on the results of the research. Thus, the purpose of the work is to develop an algorithm for an effective solution to the problem of signature verification, create a software application based on the developed algorithm, and verify the system's performance by studying the functioning of the developed application using a sufficient database of authentic and forged signatures of different signatories. The article analyzes the state of the problem, which allowed finding a database of 500 authentic and forged signatures, identifying 15 main signs of signature forgery as such, 10 mathematical methods for comparing signatures, the main characteristics and structure of the application's functioning algorithm, and its architecture. Experimental studies conducted to verify the found signs of signature forgery as such by the numerical value of the stability criterion of the sign allowed to identify those signs that are appropriate to use in the application for verification. Also, experimental studies based on signatures conducted to verify the found mathematical methods for comparing a known authentic signature and the signature being verified allowed to identify comparison methods that are appropriate to use in the application. When the application is operating, digital images of signatures obtained using a digital camera or scanner are processed and verified using pattern recognition methods, found signs and comparison methods. On the database of used signatures, the verification results were successful. The developed application can be improved and serve as the basis for an economical signatures verification system.
Keywords: biometric signature verification, cybersecurity, computer application, pattern recognition, biometric signature verification, cybersecurity, computer application, pattern recognition.