НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

ФАКУЛЬТЕТ ПРИКЛАДНОЇ МАТЕМАТИКИ

КАФЕДРА СИСТЕМНОГО ПРОГРАМУВАННЯ І
СПЕЦІАЛІЗОВАНИХ КОМП'ЮТЕРНИХ СИСТЕМ

«На правах рукопису»
УДК 004.8

«До захисту допущено»

Завідувач кафедри СПСКС

_____ В.П.Тарасенко_
(підпис) (ініціали, прізвище)

"___" _____2018р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 123 Комп'ютерна інженерія
Системне програмування

на тему: Методи та алгоритми розпізнавання підписів користувачів

Виконав: студент II курсу, групи _КВ-72_мп_____
(шифр групи)

Онопрієнко Маріанна Ігорівна _____ _____
(прізвище, ім'я, по батькові) (підпис)

Науковий керівник.д.т.н._проф. Терейковський І.А. _____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент д. т. н., проф. Симоненко В. П. _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018 року

Національний технічний університет України
“Київський політехнічний інститут
імені Ігоря Сікорського”

Факультет прикладної математики

Кафедра системного програмування і
спеціалізованих комп‘ютерних систем

Рівень вищої освіти – другий (магістерський)

Спеціальність 123 “Комп’ютерна інженерія”
Системне програмування

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____
В.П.Тарасенко
“___” _____
2018 р.

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ ДИСЕРТАЦІЮ СТУДЕНТУ
Онопрієнко Маріанні Ігорівні

1. Тема дисертації: _Моделі та методи розпізнавання підписів користувачів___,
науковий керівник дисертації: Терейковський І.А.,
затверджені наказом по університету від “30” жовтня 2018 року № 4030.

2. Термін подання студентом дисертації: “7” грудня 2018 р.

3. Об’єкт дослідження: методи та алгоритми розпізнавання підпису користувача.

4. Предмет дослідження: є створення системи розпізнавання підписів користувачів, які вже є в базі за допомогою нейронних мереж.

5. Перелік задач, які потрібно вирішити:

- Дослідження та аналіз існуючих методів та алгоритмів на предмет ефективного розпізнавання рукописного тексту та підпису;
- Розробка моделі процесу верифікації підписів;
- Дослідження застосування нейронних мереж;
- Розробка алгоритмів попередньої обробки та розпізнавання;
- Програмна реалізація алгоритмів;
- Тестування системи.

6. Перелік ілюстративного матеріалу:

– Презентація.

7. Перелік публікацій:

- XI конференція молодих вчених «Прикладна математика та комп’ютинг» ПМК-2018-2;
- IV міжнародна науково-практична конференція «Теоретичні та практичні аспекти розвитку ».

8. Дата видачі завдання: “3” вересня 2017 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	і
1.	Вибір теми дипломного проекту.	03.09.2017	
2.	Вивчення та аналіз існуючих матеріалів	03.11.2017	
3.	Проходження практики	03.09.2018	
4.	Написання першого розділу	03.07.2018	
5.	Написання другого розділу	03.08.2018	
6.	Написання третього розділу	03.09.2018	
7.	Написання четвертого розділу	03.10.2018	
8.	Попередній розгляд магістерської дисертації на засіданні кафедри	26.11.2018	

Студент _____ Онопрієнко М. І.
(підпис)

Науковий керівник дисертації _____ Терейковський І. А.
(підпис)

РЕФЕРАТ

Актуальність теми. Контроль доступу, облік та управління системами залишаються актуальними задачами на сьогодні, Верифікація користувача за допомогою біометричних характеристик більш надійна ніж використання звичайного паролю. Широким досліджуваним питанням є розпізнавання рукописного тексту. Може здатися, що в підробці підпису немає нічого проблематичного, проте, практично неможливо повторити унікальність швидкості написання та виробленого при цьому тиску. Тому, системи розпізнавання підпису,які використовують самі передові технології, стають ідеальною заміною для паролів в операціях, наприклад, з банківськими рахунками. Однак, як і в інших методах ідентифікації, верифікація з допомогою розпізнавання підпису має свої недоліки. На даний момент досягнута точність нижче, ніж для рукописного "друкованого" тексту. Оскільки на відміну від друкованого тексту підписант намагається зробити свій підпис унікальним і крім символів використовує додаткові графічні елементи. Тому наявність труднощів в системах розпізнавання рукописних підписів все одно не перекреслює актуальність цієї технології і робить тему даної магістерської дисертації актуальною.

Об’єктом дослідження є система розпізнавання підписів користувачів.

Предметом дослідження - є створення системи розпізнавання підписів користувачів, які вже є в базі за допомогою нейронних мереж.

Мета роботи є розробка системи розпізнавання підписів користувачів, які наявні в базі. Для цього визначено завдання, які вирішуються в роботі:

1. Дослідження та аналіз існуючих методів та алгоритмів на предмет ефективного розпізнавання рукописного тексту та підпису;
2. Розробка моделі процесу верифікації підписів;
3. Дослідження застосування нейронних мереж;
4. Розробка алгоритмів попередньої обробки та розпізнавання;
5. Програмна реалізація алгоритмів;
6. Тестування системи.

Методи дослідження. Одним з найважливіших методів дослідження у роботі є аналіз та власне розробка, оскільки магістерська дисертація присвячена вивченню великих об'ємів накопичених знань у питаннях розпізнавання рукописного підпису користувача. Також, було використано метод нейронних мереж, що дозволяє досягти потрібної точності.

Наукова новизна роботи полягає в тому, що розглянуті основні проблеми та методи їх рішення, а також розроблена програма має вищий рівень точності

Практична цінність отриманих в роботі результатів полягає в тому, що запропонована система реалізована для використання реальними програмними продуктами, що можуть бути впроваджені для реальних комп'ютерних систем.

Апробація роботи. Результати роботи пройшли апробацію або знаходяться на стадії публікації на конференціях:

- XI конференція молодих вчених «Прикладна математика та комп'ютинг» ПМК-2018-2;

– IV міжнародна науково-практична конференція «Теоретичні та практичні аспекти розвитку ».

Структура та обсяг роботи. *Магістерська дисертація складається з вступу, чотирьох розділів, висновків та додатків.*

У вступі надано загальну характеристику роботи, виконано оцінку сучасного стану проблеми, обґрунтовано актуальність напрямку досліджень, сформульовано мету і задачі дослідження та розробки.

У першому розділі описується теоретичний обсяг біометричних технологій, що базується на розпізнаванні геометричних характеристик. Розглянуто основні проблеми та існуючі методи їх вирішення.

У другому розділі представлено вирішення наукової задачі формалізації процесів біометричної аутентифікації, розроблено концептуальну модель забезпечення ефективної нейромережевої оцінки інформативності вхідних даних формалізація процесів біометричної аутентифікації.

У третьому розділі надана розробка методологічних основ оцінки інформативності образів підпису на базі нейромережевої системи діагностики. Отриманий подальший розвиток нейромережева модель оцінки інформативності образів підписів, а за рахунок теоретично обгрунтованого вибору виду нейронної мережі, забезпечує можливість ефективної оцінки інформативності, яка визначається на підставі точності розпізнавання.

Четвертий розділ представляє собою саме опис розробленої системи, проведених експериментів та тестування кінцевого продукту.

У висновках представлено отримані результати роботи.

У додатках наведено фрагменти реалізації програмної бібліотеки та копії графічних матеріалів.

Магістерська дисертація виконана на 90 аркушах, містить__ додатків та посилання на список використаних літературних джерел з __ найменувань. У роботі наведено __ рисунків та __ таблиць.

Ключові слова: розпізнавання зображення, оборобка рукописного тексту, згорткова нейронна мережа.

ЗМІСТ

РОЗДІЛ 1. АНАЛІЗ ТЕХНОЛОГІЙ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ, ЩО БАЗУЄТЬСЯ НА АНАЛІЗІ ГЕОМЕТРИЧНИХ ХАРАКТЕРИСТИК

1.1 Аналіз біометричних образів, що застосовуються в засобах аутентифікаціях

Згідно із відміченим у праці [1] на сьогоднішній день один із найбільших представних класів сучасних систем біометричної аутентифікації зводиться до фундаментального базування в якому береться за на основу процес реалізації відповідного розпізнавання користувача за набором геометричних характеристик. Вище зазначений підхід враховує наступні геометричні характеристики :

- папілярні лінії шкірного покриву подушечок пальців і долонь;
- дерево кровоносних судин пальця і долоні;
- контурні лінії долоні;
- малюнком райдужних оболонок очей і кровоносних судин очного дна:
- контурні лінії особи;
- контурні лінії вушних раковин;
- особливості відображення рукописних символів.

Далі розглянемо більш детально специфічні особливості технології аналізу вище зазначених образів в засобах біометричної аутентифікації.

В теоретичному бачені при реалізації процесу розпізнавання особистості по папілярних лініях, вважається, що шкіра людини відповідно складається з двох шарів, при цьому нижній шар утворює безліч виступів - сосочків (по латині сосочок - papillae), в вершині яких є отвори вихідних проток потових залоз.

На основній частині шкіри сосочки - papillae (потові залози) розташовуються хаотично і за ними важко вести спостереження.

При цьому на окремих ділянках шкіри кінцівок папілляров строго впорядковані в лінії (гребені), що утворюють унікальні папілярні візерунки.

Відповідно система розпізнавання знімає папіллярний візерунок з одного з пальців заявника прав доступу і порівнюють його з еталонним малюнком [2].

В даному разі варто зазначити, що у відповідності до [3] обсяг інформації, що зберігається еталонної інформації може бути суттєво зменшений. В результаті, якщо здійснити класифікацію на характерні типи папілярних малюнків і виділити на відбитку характерні мікроособливості, що представляють собою початку (закінчення) папілярних ліній або їх злиття (розгалуження). Виділяють три типи папілярних малюнків (дугові, завитки, кругові) і два типи макроособливостей (дельти і центри). Особливості папілярного візерунка проілюстровані на рис. 1.1.

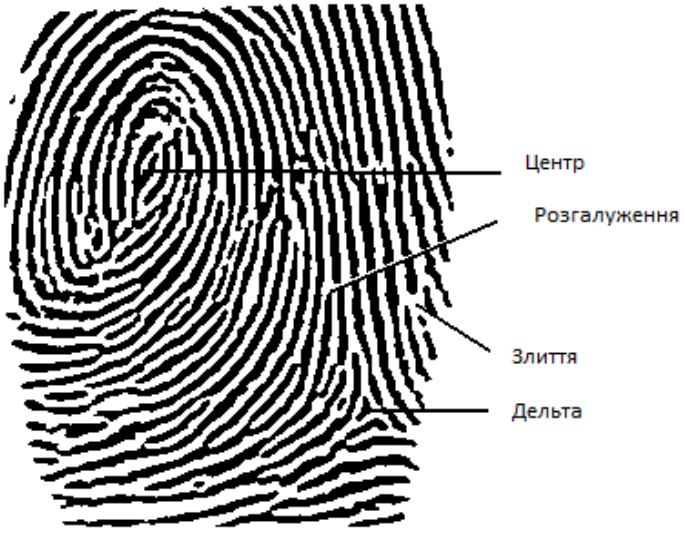

Рисунок 1.1 - Особливості папілярного візерунка

Відповідно за результатами незалежного тестування помилки першого роду для систем цього класу становлять від 10% до 20%, якщо зважати на несприятливі випадки сухої шкіри, а також включати до складу групи тестування осіб з погано вираженими папілярними малюнками (як правило, це жінки і особи азіатського походження) .

Натомість виробники папілярних біометричних систем ідентифікації в рекламі своїх продуктів оцінюють помилки першого роду на рівні 2%, а помилки другого роду на рівні 0,0001%. Остання цифра, мабуть, може бути віднесена тільки до випадків «невмілого» злому систем без використання муляжу.

Зокрема сама вартість біометричних систем цього класу швидко падає і очікується подальше істотне зниження вартості подібних біометричних систем через відмову від оптики і кремнієвих світлочутливих елементів (телевізійних ПЗС матриць).

На сьогоднішній день в основному випускаються контактні зчитувачі електричного поля пальця, здатні знімати дактилоскопічний візерунок.

Також варто зазначити, що сама вартість контактної системи виявляється істотно нижче її оптичного аналога, розрахованого на попереднє оптичне перетворення зображення.

Крім того очікується, що при падінні вартості нові чутливі елементи так само зменшать вплив рівня вологості та забрудненості руки на результат дактилоскопічної ідентифікації.

Зчитування інформації відбувається шляхом вимірювання ємності мікроконденсаторів мікросхеми, які перебувають безпосередньо по пальцем. Загальна схема вимірювань наведена на рис. 1.2.

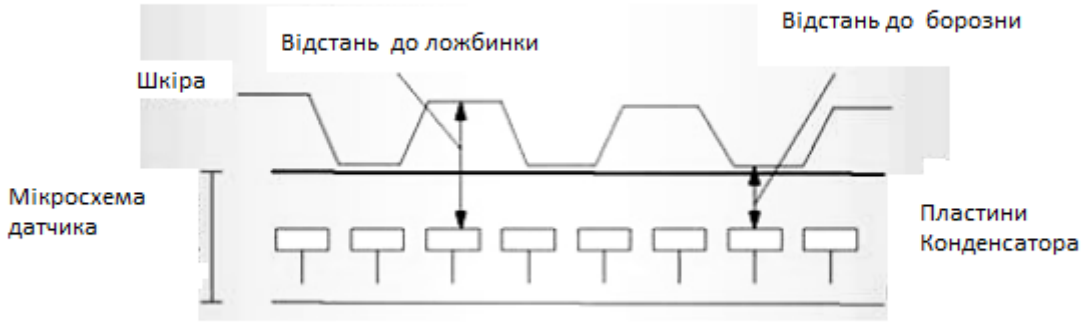

Рисунок 1.2 - Пряме зчитування інформації через контроль ємності конденсаторів

Виготовлення муляжу пальця руки з потрібним малюнком при підготовці професійної атаки оцінюється експертами як цілком реальна загроза. Цей тип систем слабо захищений від обману муляжем.

Відповідно аналіз дерева кровоносних судин пальця і долоні виконується за методикою викладеною в [4].

Зі свого боку варто зазначити, що практика використання сканерів малюнків відбитків пальців показала, що приблизно для 8% людей ця технологія виявляється малоефективною [5].

Зокрема у частині людей папілярний малюнок шкіри пальців погано виражений. Як правило, це жінки, діти та особи азіатського походження.

У зв'язку із вище відміченим в даний час японські фірми орієнтуються на технологію аналізу малюнка кровоносних судин руки або пальця.

Безпосередньо в Японії вже кілька років працюють мережі банкоматів, побудовані на аналізі розподілу кровоносних судин під шкірою пальця на руці або кровоносних судин всієї долоні. Корпорація «Хітачі» («Hitachi») спеціалізується на сканерах малюнка кровоносних судин під шкірою пальця, корпорація «Футджіцу» («Fujitsu») виробляє сканери та системи, що аналізують малюнок кровоносних судин всієї долоні (рисунок

1.3).

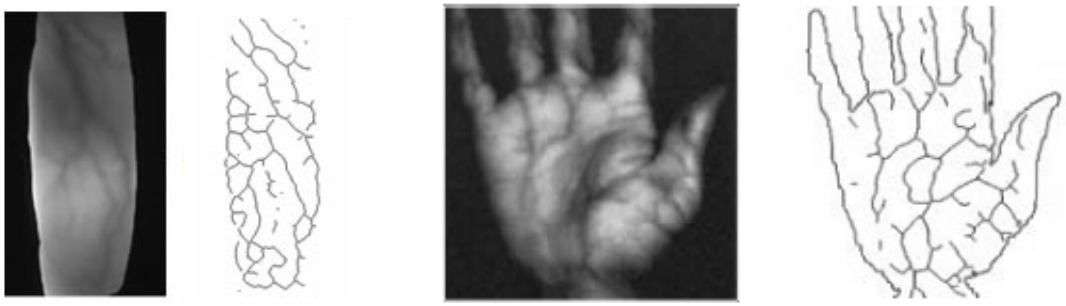

Рисунок 1.3 - Приклади малюнків кровоносних судин пальця і руки

Ймовірності помилок другого роду обох типів засобів біометричної авторизації знаходиться в інтервалі від 10-4 до 10-6. Так, як малюнок кровоносних судин змінити не можливо, оператор надання послуг платіжної системи повинен забезпечити зберігання його біометричних параметрів в конфіденційної формі.

Натомість в даному разі можуть бути використані захищені біометричні контейнери або біометричні хеш-функції. Крім того, бази цих персональних біометричних даних повинні бути знеособлені. Якщо використовуються звичайні біометричні шаблони, то захист бази біометричних шаблонів повинна бути виконаний у відповідності до класової характеристики

Дана біометрична технологія може бути використана в банкоматах і офісних терміналах операторів платіжних послуг, використовуваних для управління особистим рахунком.

Аналіз геометрії долоні виконується у відповідності до методології викладеної в [6].

В даному разі варто зазначити, що поряд з аналізом кровоносних судин руки, банкомати Японії додатково аналізують всі інші геометричні параметри кісті руки.

Зокрема у кожного з нас різна довжина і ширина пальців, крім того, шкіра на руці має явно виражені складки і зморшки. На рис. 1.4 приведена фотографія тильної сторони руки.

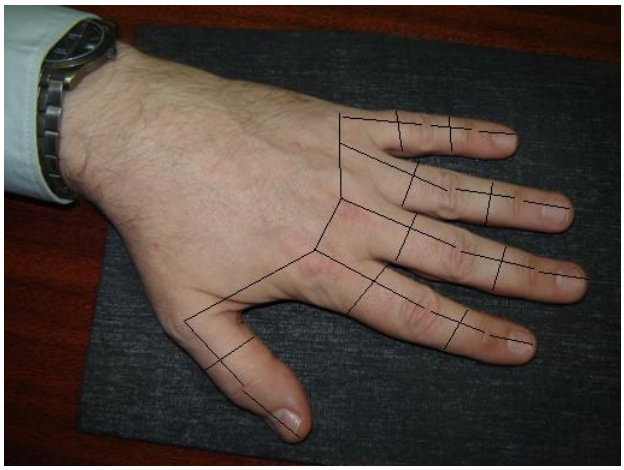

Рисунок 1.4 - Фотографія тильного боку кисті руки, за якою можна оцінити її відносні геометричні параметри

Нині існують два типи біометричних систем, побудованих на аналізі геометрію кисті руки.

Безпосередньо системи першого типу побудовані на аналізі зображень кісті руки або долоні руки, отриманих при звичайному освілнні.

Системи другого типу будуються на виділенні розташування розгалужень дерева кровоносних судин на тильній стороні кісті руки.

Натомість кров, яка надходить до кісті руки, за звичай тепліше самої руки і для виділення малюнка судин крові необхідно використовувати оптичні елементи, чутливі до інфрачервоної частини спектра.

Вельми інформативними є параметри долоні руки, отримані шляхом виділення на ній характерних складок шкіри (так званих «ліній життя»). Геометрія розташування складок шкіри на тильній стороні кісті руки і на долоні є вельми і вельми інформативними біометричними параметрами, які

поки, що не використовуються належним чином сучасними технічними засобами біометричного контролю.

Процедура аналізу райдужної оболонки ока і судин очного дна здійснюється у відповідності до методики викладеної в [7].

В даному разі варто зазначити, що у кожного з людей параметри геометрії його тіла унікальні, в тому числі унікальними є параметри очей.

Зокрема на даний момент існують два типи біометричних систем, побудованих на вимірі параметрів очі.

Відповідно до першого типу відносяться системи, побудовані на аналізі малюнка райдужної оболонки ока.

При цьому по Даугмену [8] малюнки райдужних оболонок ока не залежать від генетики людини і розрізняються навіть у однояйцевих близнюків.

До другого типу відносяться системи, побудовані на аналізі малюнка кровоносних судин очного дна (сітківки). Природно, що оптичні характеристики у перших і других систем виявляються принципово різними. Приклади малюнків сітківки ока різних людей і одного малюнка кровоносних судин очного дна наведені на рис. 1.5.

Аналіз дерева кровоносних судин здійснюється на тих же принципах, і аналіз дерева кровоносних судин кісті руки або інших ділянок тіла людини. При формуванні шаблону знаходяться корені, стовбури, гілки, далі вони класифікуються за їх довжиною, взаємного розташування і діаметру.

У правій нижній частині рис. 1.5. добре видно, що всі кровоносні судини мають яскраво виражений загальний корінь. Цей корінь повинен розглядатися, як центр, щодо якого ведуться біометричні вимірювання геометрії стовбурів і гілок різного рівня.

При аналізі малюнка райдужної оболонки ока здійснюють її сканування по паралельних концентричних кіл, розташованим навколо

зіниці. При цьому враховується, що зіницю ока людини може змінювати її розміри, адаптуючись до освітленості розглянутого предмета.

У зв'язку з цим формування біометричного шаблону райдужної оболонки ока і ідентифікацію людини по його малюнку доцільно виконувати при однаковій освітленості. У цьому випадку співвідношення діаметра зіниці і зовнішнього діаметра райдужної оболонки виявляється практично постійним і не потребує перерахунку.

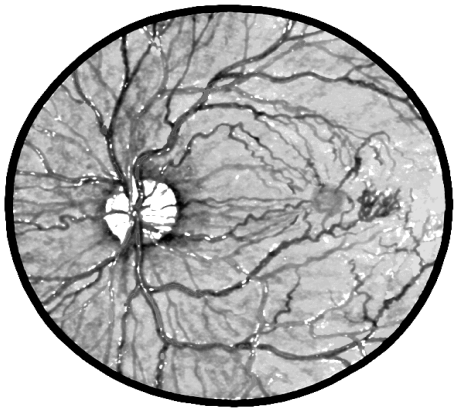

Рисунок 1.5 - Приклади малюнків райдужної оболонки ока різних людей і приклад одного малюнка взаємного розташування кровоносних судин очного дна

При скануванні райдужної оболонки оцінюють значення середнього рівня яскравості зображення уздовж заздалегідь заданій концентричного кола. Далі концентрована окружність ділиться на задане число секторів, наприклад 128 секторів, і обчислюється середня яскравість кожного сектора. Висока яскравість і низька яскравість в секторі по відношенню до середньої яскравості дають стан «1» і «0» коду сканування.

Зокрема, якщо використовувати 8 концентричних кіл сканування, то, відповідно, кінцевий код сканування матиме довжину коду 128 х 8 = 1024 біта. Приклад подібного коду наведено на рис. 1.6.

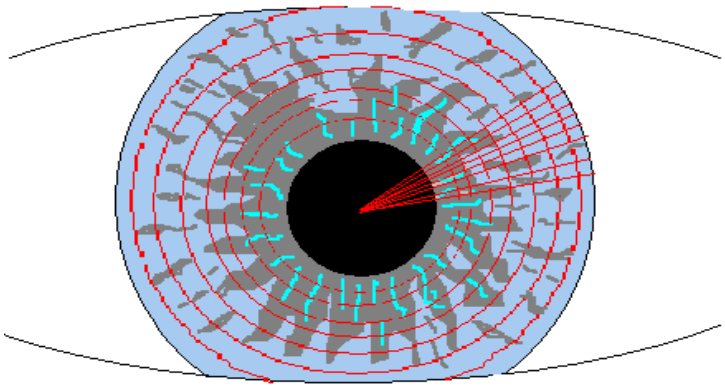

Рисунок. 1.6 - Використання кілька концентричних кіл при скануванні перепадів яскравості райдужної оболонки ока

Також варто зазначити, що підсумкова кодова комбінація перепадів яскравості райдужної оболонки матиме сильно корельовані (сильно залежні) сусідні відліки.

Проте, значна кореляція характерна для багатьох біометричних параметрів і потрібне спеціальне декорреляційне перетворення, яке дозволить зробити вимірювані дані досить незалежними.

Сучасні офтальмологічні біометричні системи можуть будуватися не тільки на аналізі малюнка райдужної оболочки ока і аналізі малюнка кровоносних судин очного дна. При хорошому дозволі використовуваної оптики на фотографіях очі добре помітні кровоносні судини, що забезпечують очне яблуко кров'ю. Їх малюнок унікальний і цілком може бути використаний для ідентифікації і аутентифікації людини. Однак на сьогодні подібних систем на біометричний ринку поки немає.

Процедури обробки офтальмологічних біометричних даних райдужної оболонки описані в стандарті ДСТУ ISO \ МЕК 19794-6 «Автоматична ідентифікація. Ідентифікація біометрична. Формати обміну біометричними даними. Дані зображення райдужної оболонки ока ».

В свою чергу варто зазначити, що нині найбільш прийнятною

технологією для аналізу райдужної оболонки ока є для авторизації користувачів банкоматами.

Зокрема для банкоматів бажано використовувати безконтактний спосіб сканування біометричних даних людини. На даний момент існують технічні засоби відео- спостереження, мають досить високий дозвіл при скануванні малюнка райдужної оболочки ока на відстані від 30 до 50 сантиметрів.

Лідерами створення біометричних засобів аналізу райдужної оболонки ока є англійці. Ця технологія захищена патентами, термін яких найближчим часом закінчується. Дія патентів, що захищають ці біометричні технології, на територію України, Росії, Білорусії і Казахстану не поширюється.

За даними джерел [20] ймовірність помилок другого роду при аналізі малюнка райдужної оболочки ока становить від 10-5 до 10-11.

Ці цифри явно завищені, так як помилки оцінювалися в рамках гіпотези незалежності розрядів коду, що породжується малюнками райдужної оболочки ока. Для забезпечення якості незалежності відкидалися розряди коду, що мають кореляцію більш 0.3. Так як малюнок райдужної оболонки ока людини є статичним біометричним чином, його еталонні параметри повинні зберігатися в захищеній формі. У вигляді звичайної хеш-функції коду або у вигляді біометричної хеш-функції, налаштованої враховувати параметри малюнка райдужної оболонки ока конкретної людини [9]. Бази еталонних даних малюнків райдужної оболонки ока повинні бути знеособлені

Безпосередній аналіз геометрії особи людини основується на засадах методології викладеної в [6]. Зазвичай люди пізнають один одного по особливостям рис обличчя. Посвідчення особи, паспорта, водійських прав, як правило, мають фотографію їх власника.

Спроби автоматизувати процедуру розпізнавання людини за особливостями рис обличчя привели до появи двох класів засобів біометричної ідентифікації.

Перший клас подібних засобів аналізує плоскі зображення обличчя людини (2D-портрети). Робота цих пристроїв ілюструється на рис. 1.7.

Двомірні аналізатори плоских зображень знаходять на портреті людини «анфас» характерні точки (рис. 1.7) і відстані:

- між центрами очей;
- між лінією очей і кінчиком носа;
- відповідного найбільшій ширині носа;
- між дугами брів і нижньою точкою підборіддя;
- між нижніми точками мочок вух;
- між кінчиком носа і нижньою точкою губ.

Рисунок 1.7 - Виділення особливих точок на плоских фотографіях людини з подальшим обчисленням відстаней між ними

При аналізі двомірних зображень портрета людини в профіль використовуються аналогічні добре виділяються точки, при цьому добре виділяються точки на контурі особи можуть бути доповнені відстанями до добре виділяються точок на вушній раковині людини.

Двомірні аналізатори взаємного розташування рис обличчя

дозволяють отримати досить мізерну біометричну інформацію, забезпечуючи ймовірності помилок другого роду (пропуск «Чужого») на рівні 0.05. Перехід до більш складного тривимірному аналізу геометрії особи дозволяє значно збільшити обсяг одержуваної біометричної інформації. Для отримання тривимірних зображень можуть бути використані дві камери [10] або одна фотокамера зі спеціальною підсвіткою.

Наприклад, це може бути підсвічування системою поздовжніх і поперечних смуг світла, що утворюють рівномірну сітку при висвітленні площині. При такому підсвічуванні на обличчі ідентифікованого людини виходить сітка, осередки, якої деформовані пропорційно відстані від підсвічування точок до фотокамери.

Аналіз геометрії вушних раковин виконується у відповідності до методології викладеної в [6].

Створюючи першу систему біометричної ідентифікації людини, Альфонс Бартільон велику увагу приділяв визначенню типу і форми вушних раковин людини.

Причина такої великої уваги в тому, що варіація положення і розмірів вушних раковин у людей суттєво вище, ніж варіації розмірів інших частин тіла. Крім того, вушні раковини значно відрізняються за формою у різних людей.

На рис. 1.8 приведені фотографії вушних раковин п'ятьох випадково обраних чоловіків в масштабі, що відтворює реальні співвідношення розмірів вушних раковин.

Незважаючи на те, що форма і розміри вушних раковин істотно варіюються, поки немає ефективних біометричних систем, що використовують геометрію вушних раковин.

Мабуть, це пов'язано з проблемами тривимірного технічного зору. Поки засоби штучного зору двовимірних, вони не можуть створювати і

запам'ятовувати складну тривимірну форму вушних раковин. Витягти ж з двомірних образів вушних раковин досить великий обсяг біометричної інформації не вдається.

Рисунок 1.8 - Різні форми вушних раковин п'ятьох випадково обраних чоловіків, наведені в одному масштабі

Робляться спроби використання оконтуривания зображення вушних раковин, однак, все програми оконтуривания виявляються дуже чутливими до бічної підсвічуванні і добре працюють тільки на нерухомих об'єктах.

Імовірно інтелектуальні можливості біометричних систем будуть поступово посилюватися і, відповідно, спостереження складної геометрії вушних раковин стане доступним для практичного застосування, якщо перейти до аналізу 3D-геометрії складної форми вушних раковин.

Зробити геометрію вушних раковин дійсно ефективної для захисту особистої інформації можна тільки забезпечивши її конфіденційність через розміщення в нейромережевих контейнерах і забезпечивши додатково

анонімність (знеособленість) власника біометрії під час виконання процедур аутентифікації.

Аналіз рукописного почерку. Принцип ідентифікації людини по рукописного підпису, в тому числі без використання електронних засобів її обробки, застосовується не одне сторіччя. Цей спосіб ідентифікації особистості побудований на тому, що автор придумує собі факсиміле, бажано, воно мало істотні відмінності за формою від класичного написання букв у вигляді додаткових елементів (розчерків, повернень, накладення букв).

При розгляді даного типу ідентифікації необхідно звернути увагу на наступні незалежні підходи:

– ідентифікацію автора по статичній підписи вже присутньої на підприємстві, що перевіряється документі;

– ідентифікація автора по динамічному образу, воспроизводимому автором підпису, що вводиться їм в комп'ютер в момент своєї ідентифікації при можливості спостереження індивідуальних особливостей звичних для автора підсвідомих рухів.

У першій постановці завдання мова йде про порівняння зображень, відтворених раніше в невідомої послідовності. У другій постановці завдання є дані про параметри коливання пера автора при відтворенні їм підписи в тривимірному просторі. Якщо користуватися тривимірною системою координат (X, Y, Z), то дані про динаміку відтворення підпису отримують у вигляді двох функцій часу коливань пера в площині графічного планшета X (t), Y (t) і ще однієї функції - зміна тиску пера на графічний планшет Z (t).

Необхідно враховувати, що рішення першого підходу є важко реалізованим для рівня розвитку сучасних інформаційних технологій і, як правило, автоматичні банківські системи ідентифікації автографів працюють істотно гірше досвідченого касира. Як правило, ці системи

тільки напівавтоматичні, вони полегшують роботу перевіряючого, даючи йому, відповідні чисельні характеристики близькості фрагментів підписи до оригіналу, але остаточне рішення приймає людина. На сьогодні, відомі технічні рішення першого варіанту постановки задачі по імовірнісним характеристикам істотно гірше, ніж статистика роботи досвідчених людей (експертів). Саме з цієї причини фірми виробники не дають статистичних даних про помилки першого і другого роду для ідентифікації автора по статичному образу його підпису.

Другий підхід навпаки дозволяє забезпечити набагато більшу точність розпізнавання при використанні автоматизованих систем, що здійснюють витяг чисельними параметроми відповідності. Дану особливість слід враховувати при розгляді можливих варіантів атак на систему, в тому числі, ситуації обвода, чужі підписи і зупинок для прийняття свідомого рішення під час підробки. Експерт не має подібної динамічної інформації і відповідно зростає ймовірність прийняття даного підпису, як дійснго. За наявностю факту візуальної відповідності еталонного підпису.

Практично всі сучасні комерційні систем ідентифікації користувача по рукописному образу слід розділити на одну, двох і трьох координатнстьі, відмінність полягає в тому, що аналіз динаміки охоплює одну криву, пару кривих або повну множину кривих X (t), Y (t), Z (t). Однокоординатні системи можуть бути побудовані шляхом обліку будь-який з цих тимчасових функцій, забезпечуючи ймовірності помилок першого і другого роду на рівні 0,1. Двох координатні системи використовують будь-яку пару функцій часу з трійки X (t), Y (t), Z (t), і на сьогоднішній день, дозволяють досягти рівня ймовірності помилок близько 0,01. Найбільш складні системи використовують повну трійку функцій, забезпечуючи рівень вірогідності помилок першого / другого роду порядку 0,003.

Слід зазначити, що деякі з систем біометричної ідентифікації за підписом використовують не самі проекції функцій X (t), Y (t), Z (t) на осі координат, а їх першу або другу похідну, дана особливість обумовлена тільки типом використовуваного датчика, чутливого до похідної, і практично не впливає на якість і обсяг вихідної інформації з нього одержуваної. Штучне нарощування числа аналізованих функцій за рахунок вимірювання їх самих і їх же похідних недоцільне, так як всі лінійні перетворення первісних дають сильно корельовані дані. Зокрема, кореляція біометричних даних, отриманих з первісної X (t), і біометричних даних отриманих з її похідною dX (t) / dt, близька до одиниці.

Необхідно пояснити, що помилка першого роду або помилковий відмова справжньому користувачеві системи з ймовірністю 0,01 - це цілком прийнятна характеристика для більшості областей застосування даного виду систем ідентифікації. Інше працювати з помилками другого роду або хибним пропуском зловмисника. Для ряду практичних застосувань ймовірність помилок другого роду 0.01 є неприйнятно великою величиною. Для зниження цієї помилки в 104 ... 106 разів вик особистості по динаміці відтворення біометричного пароля. Як біометричного за зазвичай використовується якась пов'язана літерна послідовність, наприклад слово зі словника, або група слів. Автором зберігається в секреті як, саме слово - пароль, так і його індивідуальні особливості написання. В цьому випадку для слова - пароля, що містить від 5 до 10 букв,

Більшого зниження помилки другого роду можна домогтися, використовуючи в якості біометричного пароля слова, які не мають сенсу, але цей шлях пов'язаний з додатковими труднощами запам'ятовування слів з випадкового поєднання букв.

У свою чергу тягне виникнення уразливості записи користувачем складного пароля на будь-який небезпечний носій, наприклад аркуш

паперу, що безумовно знижує ефективність даного виду захисту лише до рівня забезпечуваного індивідуальністю динаміки підпису.

За звичай враховуються при ідентифікації динамічні параметри отримані шляхом обчислення деяких лінійних функціоналів по повній реалізації підписів або по її фрагментами.

Далі будемо називати глобальними динамічні параметри, обчислені по повній реалізації кривих Y (t), X (t), Z (t). Локальними динамічними параметрами будемо називати аналогічні параметри, але обчислені за деякими відрізкам повних кривих Y (t), X (t), Z (t), наприклад, що відповідають різним буквах парольного слова.

При обчисленні лінійних функціоналів зручно використовувати ортогональні функціонали Фур'є, Уолша, Хаара. Вибір ортогональних перетворень обумовлений тим, що вони дають дані з меншою внутрішньою кореляцією в порівнянні з іншими НЕ ортогональними функціоналами.

Для визначеності задамося функціоналами Фур'є, тоді глобальні динамічні параметри будуть мати сенс коефіцієнтів ряду Фур'є при синусах і косинусах, що обчислюються наступним чином:

$$a_{yk} = \frac{1}{T}\int_0^{Y(t)} \cos\left(k\frac{2\pi}{T}t\right)dt, \quad (1.1)$$

$$b_{yk} = \frac{1}{T}\int_0^{Y(t)} \sin\left(k\frac{2\pi}{T}t\right)dt, \quad (1.2)$$

$$a_{xk} = \frac{1}{T}\int_0^{X(t)} \cos\left(k\frac{2\pi}{T}t\right)dt, \quad (1.3)$$

$$b_{xk} = \frac{1}{T}\int_0^{X(t)} \sin\left(k\frac{2\pi}{T}t\right)dt, \quad (1.4)$$

$$a_{zk} = \frac{1}{T}\int_0^{Z(t)} \cos\left(k\frac{2\pi}{T}t\right)dt, \quad (1.5)$$

$$b_{zk} = \frac{1}{T}\int_0^{Z(t)} \sin\left(k\frac{2\pi}{T}t\right)dt. \quad (1.6)$$

, де T - повний час введення підпису.

За звичай враховується кінцеве число коефіцієнтів ряду Фур'є.

Лінійність використовуваних ортогональних функціоналів дозволяє вкрай просто здійснювати операцію масштабування сигналів по осях X, Y, Z. Для визначення невідомих масштабів тільки що введеної підписи досить вирішити 3 наступних незалежних лінійних рівняння:

$$\mu_y \cdot \sqrt[2]{\sum_{k=1}^{16}(a_{yk}^2 + b_{yk}^2)} = C_y, \quad (1.7)$$

$$\mu_x \cdot \sqrt[2]{\sum_{k=1}^{16}(a_{xk}^2 + b_{xk}^2)} = C_x, \quad (1.8)$$

$$\mu_z \cdot \sqrt[2]{\sum_{k=1}^{16}(a_{zk}^2 + b_{zk}^2)} = C_z. \quad (1.9)$$

де C_x, C_y, C_z - це значення квадратних коренів в цих же рівняннях, що відповідають першому введеної підпису.

Для приведення даних до масштабу першої введеної підписи досить помножити значення обчислених лінійних функціоналів на отримані з рівнянь масштабні коефіцієнти. Слід мати на увазі, що проблема приведення до єдиного масштабу даних досить важлива і має коректне рішення тільки в класі лінійних функціональних перетворень. При використанні нелінійних функціоналів ця проблема може не мати коректного рішення.

Локальні динамічні параметри обчислюються так само, як і глобальні, з тією лише різницею, що період інтегрування береться рівним деякому добре спостерігаєму локальному відрізку часу.

Зокрема локальні динамічні параметри можуть бути обчислені на 7 інтервалах торкання пера графічного планшета, між 8 відривом пера (8 синхронними зверненнями в нуль функцій Y (t), X (t)).

Крім відривів пера від планшета для дроблення підписи на фрагменти можуть використовуватися перетину фрагментів траєкторії

підписи, точки зміни напрямку руху, кутові точки букв, що мають розрив похідної.

За звичай число виділених локальних ділянок підпису в першому наближенні виявляється пропорційно числу букв в рукописному викна, що відтворюється слові (коефіцієнт пропорційності знаходиться в межах від 1 до 2,4 в залежності від використаних алгоритмів фрагмета я).

На кожному з локальних ділянок обчислюється порівняно невелике число параметрів (від 2 до 6).

Слід підкреслити, що співвідношення між глобальними і локальними динамічними параметрами має бути розумно збалансовано. Глобальні динамічні параметри описують схожість підписи на зразок в цілому, а локальні динамічні параметри дозволяють оцінювати схожість відтворення на еталон кожної з букв, кожного фрагмента підпису.

При несвідомому підсвідомому відтворенні слова з певною частотою з'являються нові додаткові фрагменти підпису, при цьому так само можуть зникати (зливатися) раніше розділені сусідні фрагменти.

В результаті дроблення підписи на фрагменти виявляється неоднозначним, при навчанні фіксується кілька варіантів підписи присутніх у автора.

З ситуації неоднозначною розмітки підпису можливо два виходи. Перший вихід пов'язаний з формуванням декількох незалежних еталонів, при цьому для формування кожного еталона потрібно кілька підписів, що ускладнює процес навчання системи. Другий шлях пов'язаний з приведенням всіх варіантів до деякого усередненого варіанту.

Біометричний еталон для цього класу систем формується на етапі навчання і повинен відображати як стабільну, так і нестабільну складові біометричних даних ідентифікованої особистості.

Біометричний зразок підписи (слова-пароля) може формуватися кількома способами залежно від прийнятого в системі вирішального

правила. Зокрема, якщо рішення в системі приймається нейронною мережею, то роль біометричного зразка гратимуть структура штучної нейронної мережі, вид і параметри функцій збудження. У разі, коли рішенняприймаєтьсяймається детермінованим вирішальним правилом, роль біометричного зразка можуть грати вектор значень математичних очікувань вимірюваних динамічних параметрів і вектор значень дисперсій цих Реальні показники можуть відрізнятися.

Однією з основних проблем систем ідентифікації цього класу є те, що їх параметри істотно залежать від психологічного стану людей і стабільності їх почерку.

Для людей зі стабільним рукописним почерком ці системи працюють значно краще, ніж для середнього людини, але, в той же час, системи цього класу можуть бути дискредитовані людьми з нестабільним почерком.

Крім того, введення біометричної авторизації та ідентифікації, сильно обмежують свободу дій користувачів в корпоративних мережах, перший час можуть спостерігатися спроби навмисного дискредитації біометричних систем через штучну симуляцію нестабільного почерку.

1.2. Особливості аналізу біометричних образів у системах аутентифікації

Для того щоб скористатися біометричним захистом, необхідно вміти перетворювати багатовимірний континуум біометричних даних образу «Свій» в код криптографічного ключа доступу. Для цього потрібно відсканувати заявлений біометричний образ і обчислити контрольовані біометричні параметри [6]. Далі слід пред'явити біометричні параметри на вхід перетворювача біометрія-код, як це показано на рис. 1.9.

Сам перетворювач біометрії в код може бути виконаний різними технологіями, наприклад, можуть бути використані так звані «нечіткі

екстрактори» і [11]. Шляхом створення «нечітких екстракторів» йдуть в основному англомовні дослідники.

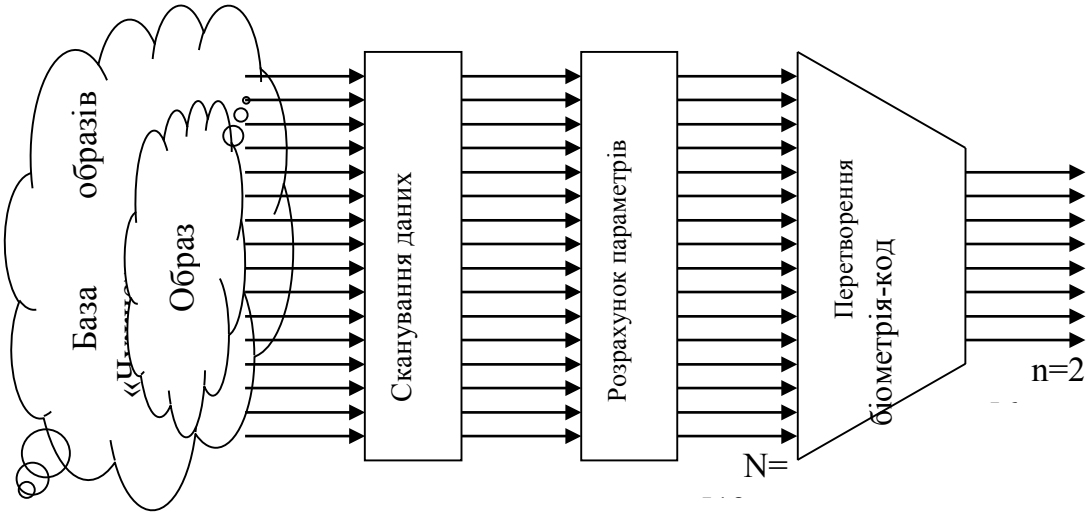

Рисунок 1.9 - Перетворення біометричних параметрів в код ключа

В Україні, Росії і Казахстані перетворювачі біометрія-код будуються з використанням штучних нейронних мереж [12].

Необхідно заздалегідь вибрати структуру зв'язків штучних нейронів мережі, а потім навчити її [13] так, щоб приклади біометричного образу «Свій» давали на виході перетворювача код особистого криптографічного ключа громадянина України, Росії або Казахстану, а для прикладів образів «Чужий» на виході перетворювача виходила випадкова кодова комбінація.

Незалежно від того, яка технологія використовується, перетворювач біометрія-код завжди має більше вхідних біометричних даних, ніж число його виходів (ніж довжина вихідного криптографічного ключа). Так, на рис. 1.10. перетворювач має N = 512 вхідних біометричних параметрів і тільки n = 256 вихідних розрядів криптографічного ключа. Умова N=n завжди виконується через низьку інформативність біометричних даних. Одного біометричного параметра, як правило, не вистачає для отримання одного біта криптографічного ключа. Обов'язково необхідно використовувати надлишкове число біометричних параметрів для того, щоб виправляти

помилки кодування в «нечітких екстракторах» або «збагачувати» вхідні біометричні дані нейронною мережею перетворювача.

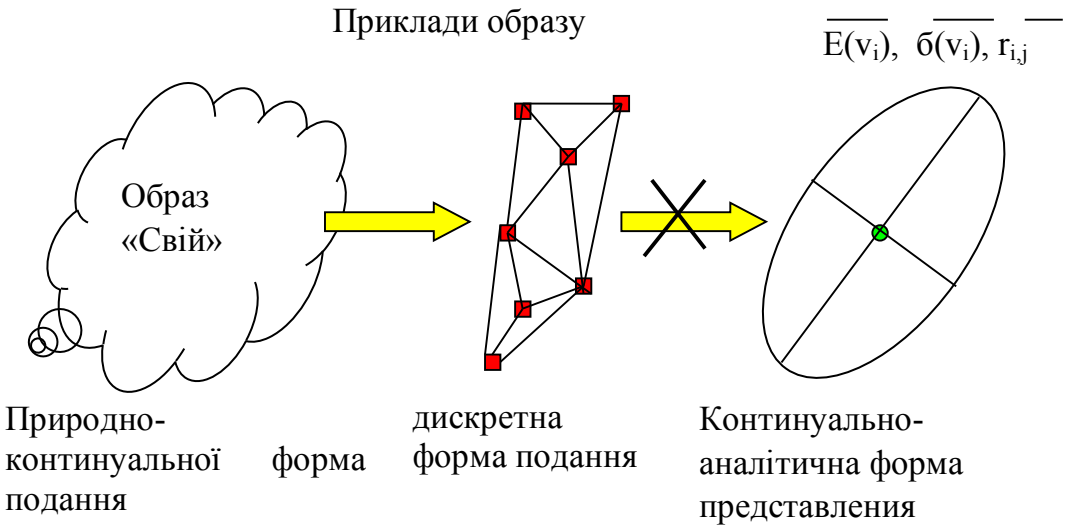

Рисунок 1.10 - Подання багатовимірного образу «Свій» малим числом прикладів (7 прикладів)

Ще однією важливою причиною труднощі біометричної аутентифікації є висока розмірність завдання (доводиться враховувати 512 і більше «поганих» біометричних параметрів). Саме з цієї причини не вдається скористатися апаратом класичної лінійної алгебри та багатовимірної статистики. Положення ускладнюється тим, що перетворювачі біометрія-код доводиться навчати (налаштовувати) на малому числі прикладів в навчальній вибірці.

Так, при навчанні біометричних засобів аутентифікації користувачі готові пред'явити від 10 до 20 прикладів біометричного образу «Свій». Однак, якщо їх попросити пред'явити 100 або 200 прикладів, то ця робота сприймається користувачами негативно. На сьогодні користувачі не готові докладати значних зусиль для навчання своєї біометричної програмної роботи (перетворювача біометрія-код). Останнє означає, що 512-мірні розподілу континуумов параметрів образу «Свій» ми змушені

представляти всього 20 прикладами по кожному з параметрів. Ми можемо спробувати уявити 512-мірний об'єм природно-континуальної форми подання даного способу «Свій» через внутрішній обсяг графа 20 прикладів «Свій», однак це буде дуже і дуже слабким наближенням. Ця ситуація відображена на рис 1.2.

Користуючись всього 20 прикладами, неможливе точне обчислення математичного сподівання біометричних параметрів E (vi), їх середньоквадратичне відхилення і коефіцієнти кореляції між параметрами ri, j. На навчальній вибірці з 20 прикладів відносна помилка в оцінці математичного очікування може бути від 0 до±25%, відносна помилка середнє відхилення може становити від 0 до ±50%, відносна помилка оцінки коефіцієнтів кореляції може бути від 0 до ±100%. При настільки неточних даних неможливо побудувати багатовимірну аналітичну модель розподілу даних образу «Свій».

РОЗДІЛ 2. ФОРМАЛІЗАЦІЯ ПРОЦЕСУ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ НА ОСНОВІ АНАЛІЗУ ГЕОМЕТРИЧНИХ ХАРАКТЕРИСТИК

2.1 Модель високонадійної біометричної аутентифікації

Як вже було зазначено в розділі 1, нині існує 7 основних технологій біометричної аутентифікації, що базуються на геометричних параметрах особистості:

- малюнок папілярних ліній;
- дерево кровоносних судин пальця і долоні;
- геометрія долоні;
- райдужна оболонка ока і судин очного дна;
- геометрія особи;
- геометрія вушних раковин;
- геометрія рукописного почерку .

Кожна із вище зазначених технологій має різний рівень стійкості, яка в свою чергу залежить від сукупності інформативності як самого статичного образу, так і динамічних характеристик користувача. З перерахованих вище семи типів найбільш надійною є технологія аутентифікації особистості щодо особливостей рукописного почерку. Дана тенденція є наслідком того, що зберегти в таємниці рукописно-відтворюєме слово-пароль (парольну фразу) багато простіше, ніж зберегти в таємниці параметри інших перерахованих біометричних образів.

У свою чергу, дані системи мають низьку вартість обладнання. Також вони можуть використовувати стандартні засоби введення рукописної графіки.

В даному разі також потрібно враховувати, що на сьогодні значна кількість кишенькових комп'ютерів мають здатність рукописного введення у вигляді сенсорного екрану.

Для настільних комп'ютерів можуть бути використані графічні планшети. Вартість графічного планшета EasyPainer становить в Україні близько 120 дол., що і стало основною причиною орієнтації на них вітчизняних виробників пристроїв біометричної аутентифікації.

Разом з тим найбільш поширеними є технології біометричної аутентифікації базуються на аналізі відбитків пальців і геометрії особи. Саме такі технології використовуються в сучасних біометричних паспортах і системах видореєстрації. Високонадійні біометричні засоби аутентифікації мають типову структуру показаної на рис. 2.1.

Рисунок 2.1 - Типовий алгоритм біометричної-криптографічної аутентифікації

Таким чином типовий алгоритм біометричної-криптографічної аутентифікації включає в себе етапи:

пред'явлення біометричного способу системі;

перетворення фізичного біометричного образу людини в електронний біометричний образ через первинні перетворювачі фізичних величин в електронні цифрові дані;

здійснює нормування електронних образів і обчислення вектора біометричних параметрів, наприклад, у вигляді коефіцієнтів Фур'є в засобах аутентифікації по динаміці відтворення рукописного пароля;

перетворення вектора біометричних параметрів у код ключа (пароля) для подальшої криптографічного аутентифікації;

криптографічний аутентифікацію користувача за її ключем або паролем.

Базуючись на аналізі цього алгоритму і результатах визначено, що порушник може здійснювати атаки на будь-які з етапів здійснення високонадійної біометричної ідентифікації. Існує три основних типи атак:

атаки засновані на знанні способу тобто з використанням так званих муляжів, які в свою чергу можуть мати фізичну структуру та бути еквівалентом способу висунутого користувачем, наприклад зліпок відбитка пальця або бути електронним еквівалентом, і являти собою матрицю відповідної висунутої легітимним користувачем і застосовується в основному для систем заснованих на динамічних параметрах образу;

атаки засновані на частковому знанні способу, наприклад, при наявність зразків підпису легітимного користувача, але не є образом (що не містять пароль) для входу в дану систему;

атаки без знання способу, тобто стала на генерації випадкових послідовностей параметрів.

2.2 Моделювання процесу оцінювання інформативності біометричних образів

Оцінка інформативності за допомогою реалізації атаки підбору корельованим шумом. Даний вид атаки заснований на прагненні зловмисника здійснити підбір та подальшу установку параметрів системи або пред'явлення образу, який прийме система, грунтуючись на деяких даних отриманих з образу легітимного користувача. Вразливі процедури високонадійної системи для реалізації атаки на корелювання сигналів представлені на рис. 2.2.

Необхідно відзначити, що унікальність відкритих рукописних образів не велика в порівнянні з відбитками пальців або райдужної оболонкою ока. Так, якщо зловмисникові відомий рукописний пароль з 5 букв і його накреслення, то він входить в систему з ймовірність 0.01. Для підбору динаміки відтворення рукописного способу досить близько 100 спроб. Однак кожне нове слово, яке відрізняється хоча б одним знаком ми повинні розглядати, як абсолютно нове слово. Динаміка рукописного написання букв істотно змінюється в залежності від попередніх знаків.

Біометричні системи, зокрема засновані на написаному Вами паролі розпізнають користувача шляхом контролю будь-яких параметрів. Зокрема для контролю можуть бути використані синусні і косинусні коефіцієнти Фур'є. Практика показала, що щільності розподілу значень, контрольованих коефіцієнтів Фур'є близькі до нормальних.

Можна умовно виділити безліч значень, що підкоряються нормальному закону розподілу n-го косинусного коефіцієнта Фур'є для «Чужих», який знає пароль і «Свій» знає парольну фразу.

На якість контрольованих даних впливає співвідношення дисперсій і відстань між центрами поділюваних множин. Чим менше значення дисперсій і чим більше відстань між центрами поділюваних множин, тим краща якість даних. Чисельно якість контрольованих параметрів може бути обчислено наступним чином:

$$r = \sqrt{\frac{(m_c - m_ч)^2}{\sigma_c^2 + \sigma_ч^2}} \qquad (2.1)$$

де mc - математичне очікування значень контрольованого параметра безлічі «Свій»,

mч - математичне очікування значень контрольованого параметра безлічі «Чужі»,

σc - дисперсія значень контрольованого параметра безлічі «Свій»,

σч- дисперсія значень контрольованого параметра безлічі «Чужі».

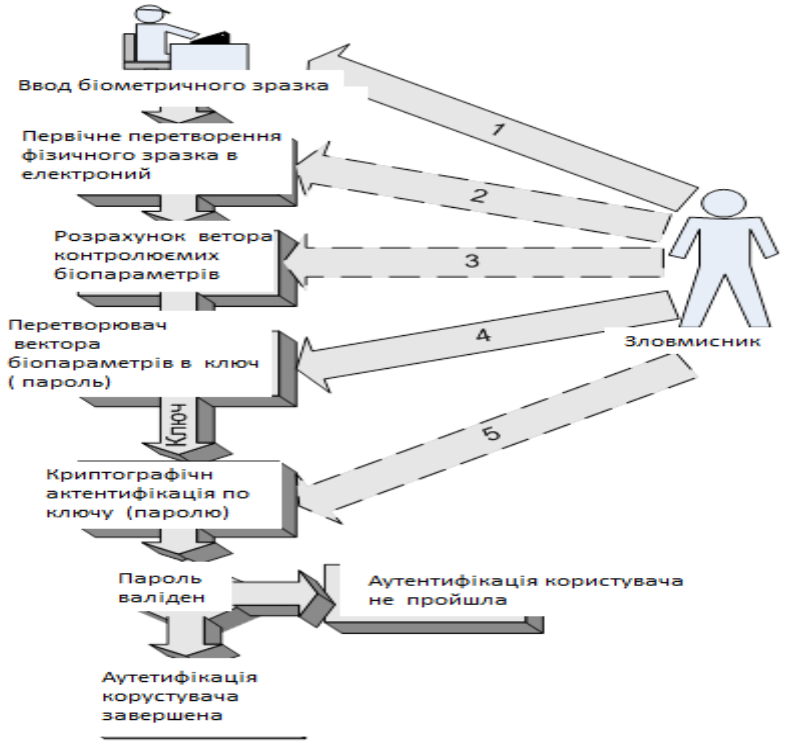

Рисунок 2.2 - Вразливі процедури високонадійної системи для реалізації атаки на корелювані сигнали

При такому розрахунку показники якості для кожного контрольованого параметра виявляються різними. Для одних параметрів показники якості високі, а для інших параметрів низькі. Очевидно, що біометрична система широкого застосування буде вивчена зловмисниками,

перед атакою і, відповідно, вони будуть знати найбільш імовірні значення параметрів. Починати атаку на біометричну систему шляхом перебору можливих значень контрольованих параметрів вигідно саме з їх найбільш імовірних значень. Як наслідок стійкість біометричного пароля буде тим вище, більший пароль буде давати параметри високої якості з малою дисперсією і з центром далеко від центру розподілу «Чужі», яким не відомий пароль.

Основними ділянками системи високонадійній біометричної аутентифікації в яких може бути здійснена атака даного типу є процедури:

1. Первинного перетворення фізичного образу в електронний.
2. Обчислення вектора контрольованих біопараметров.
3. Перетворювач вектора біопараметрів в ключ (пароль).

Реалізація першої процедури полягає в пред'явленні системи аутентифікації образу створеного на основі кореляції образу легітимного користувача, або довільних образів, якщо інші недоступні. Наприклад, для систем на основі рукописного введення пароля можливо два основні варіанти перетворення вихідних образів:

а) здійснюючи нарізку рукописного тексту довільним чином на рівні шматки, не обов'язково відповідають положенню букв в парольний фразі;

б) здійснюючи нарізку рукописного тексту з використанням механізму визначення меж букв в пральній фразі.

Після чого отримані фрагменти перемішуються довільним чином або за розробленим алгоритмом і об'єднуються, шляхом «склеювання» з використанням згладжування меж. Обидва варіанти мають як свої плюси так і мінуси, до позитивних аспектів першого підходу можна віднести

простоту реалізації і задовільні параметри нормалізації за умови розміру фрагментів порівнянних з розміром літер, другий підхід хоча і забезпечує більше наближення і більш просте рішення задачі об'єднання фрагментів, але в той час виникає проблема розробки ефективного механізму здійснення виділення окремих букв з рукописного тексту, яка до цих пір не має однозначного вирішення.

Для систем аутентифікації засновані на аналізі способу папілярного малюнка пальця, подібні атаки не є ефективними через трудомісткість пред'явлення динамічно переконфігурування носія образу через його фізичної сутності.

Атака на процедуру обчислення вектора контрольованих біопараметров вимагає втручання у функціонування системи аутентифікації тобто в електронні схеми і \ або програмні виходи. Подібні атаки вважаються найбільш небезпечними для систем побудованих на пред'явленні ідентифікатора у вигляді папілярного малюнка пальця. Наприклад, можна виділити два основних способи:

b) атака заснована на моделюванні папілярного малюнка у зовнішній системі \ програмі і подальшому виділенням контрольних точок тобто точок, розташованих на зображенні відбитка пальця в місцях закінчення відбитків гребенів або в місцях біфуркації гребенів. Опис зображення відбитка пальця в термінах розташування і орієнтації контрольних точок закінчення і біфуркацій гребенів дозволяє гарантовано визначити, чи є два зображення відбитками одного і того ж пальця.

б) атака заснована на крадіжки ідентифікатора містить біометричний образ відбитку. Нападаючий може отримати зразки відбитків пальців кінцевого користувача, витягти з нього біометричні дані і представити ці дані по вкраденій карті відповідної людини. Щоб уникнути подібних несанкціонованих нападів, а також розкрадань біометричних даних, які

використовуються в процесі верифікації, потрібен надійний канал зв'язку між ідентифікаційною картою і сервісної системою.

Для систем високонадійної біометричної аутентифікації заснованих на написаному Вами паролю так само можлива реалізація атак на даному рівні, але вони не будуть доцільними, з причини того, що якщо можливо безпосередньо втручання у функціонування системи аутентифікації, то необхідно використовувати найменш трудомісткі і ефективні шляхи реалізації атак, що і визначає перевагу атак на блок перетворення біометричного способу в ключ, наприклад на нейросеть (Росія і Казахстан) або мережу на нечітких стракторах (США);

Атака на перетворювач вектора біопараметрів в ключ (пароль) як правило є відправною точкою для початку атак для всіх типів систем аутентифікації на основі біометричних образів. Початок атаки на даній стадії дозволяє скоротити час на її реалізації, як через можливості розрахунку кореляційних матриць, що подаються на входи нейромережі із залученням необмежених зовнішніх ресурсів, так і через можливої наявності в системі високонадійній біометричної аутентифікації механізмів штучно уповільнюють зчитування і розкладання на вектори вихідного біометричного образу. З цієї причини загальну стійкість системи доцільно визначати саме на цьому етапі. Так при високій якості біопараметров тобто їх високої стабільності, стійкість біометричного пароля до підбору складе близько тисяча двадцять дві спроби при контролі системою 64 параметрів.

При зниженні стабільності, стійкість до злому біометричного способу складе приблизно 1010 спроб. Для злому біометричної системи захисту зі слабким біометричним паролем потрібно перебирати набагато менше число варіантів (число варіантів скоротилося на 12 порядків). Це означає, що дійсно надійні біометричні системи повинні вміти

контролювати очікувану стійкість використовуваного її користувачем біометричного пароля.

Сучасні біометричні системи захисту повинні вміти обчислювати якість всіх контрольованих біометричних параметрів і вміти прогнозувати свою стійкість до злому простим перебором можливих поєднань біометричних параметрів. Сьогодні виробниками декларуються тільки середньостатистичні показники стійкості біометричної системи, що явно недостатньо. Реальні характеристики біометричних систем при роботі з конкретними користувачами можуть відрізнятися від середньостатистичних на десятки порядків. Тому виникає необхідність відійти від абстрактного поняття середньостатистичний користувач і перейти до оцінки стійкості, а відповідно інформативного способу конкретного користувача системи.

Наприклад, статистичні дослідження системи «Нейрокріптон» (ФГУП ПНІЕІ) показали, що з точки зору особливостей почерку всіх людей можна розділити на 7 класів. Кожен клас має різну стабільність почерку, яка тільки залежить від парольного слова тобто користувач при його зміні може перейти на один клас нижче або вище, проте перехід до 2 класу вгору і вниз можливий, але затруднений. Стійкість системи до атак підбору істотно залежить від класу, до якого система віднесла користувача.

На рис. 2.3 наведені процентні співвідношення людей в кожному класі і стійкість класів по відношенню до атак підбору за умов відомого рукописного слова і невідомого рукописного слова.

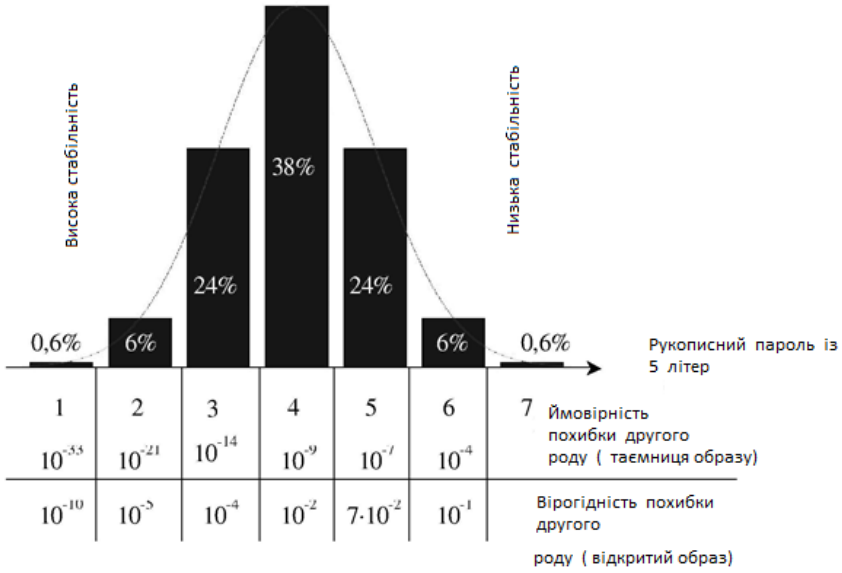

Рисунок 2.3 - Стійкість класів стабільності рукописного введення по відношенню до атак підбору

Найбільш стабільний клас користувачів при збереженні в таємниці біометричного способу має ймовірність помилки другого роду на рівні 10-33. Найстабільніший сьомий клас користувачів взагалі не може бути однозначно пізнаний системою. Середньостатистичний користувач має можливість помилки другого роду на рівні 10-9. У підсумку можна зробити висновок про те, що люди з унікальним і стабільним почерком мають ймовірність помилки другого роду на 24 порядки менше, ніж середньостатистичний користувач. Таким чином, стійкість системи багато в чому визначається індивідуальними характеристиками самого користувача.

Помилка у визначенні класу може привести до завищення або заниження стійкості системи на кілька порядків.

Необхідно використовувати спеціальні нейромережеві механізми для коректного і достовірного визначення класу користувача по його реальним біометричними параметрами. Для систем заснованих на пред'явленні відбитків пальців групи користувачів по стабільності не виділяються на

увазі статичності образу. Атаки на етапах введення образу і процедури криптографічний аутентифікація по ключу (паролю) не розглядаються, так як успішність першої не може бути описана математично, а друга ставитися до області криптографії та еквівалентної атаки на систему з дуже довгим ключем.

Оцінка інформативності за допомогою реалізації атаки підбору білим шумом. Даний вид атаки заснований на прагненні зловмисника здійснити повний перебір і подальшу установку параметрів системи, які прийме система, визнавши його легітимним користувачем. Вразливі процедури високонадійної системи для реалізації атаки на некорреліровані сигнали представлені на рис. 2.4.

Атаки даного типу на перший погляд повинні бути менш бажаними ніж, засновані на кореляційному принципі, так істотно зростає потужність безлічі можливих комбінацій параметрів, адже вони вибираються не згідно з яким-небудь законом розподілу, а на підставі рішення генератора псевдовипадкових чисел.

Практичні дослідження показали, що дані атаки представляють найбільшу загрозу для систем високонадійній біометричної аутентифікації, так як, не вимагають знання про особливості користувачів системи, математичного обґрунтування вибору кореляційних матриць. Даний тип атак доцільно застосовувати лише на етапі перетворення вектора біопараметров в ключ, в тому числі не тільки подачею на вхід нейромережі, а й на окремі її ділянки.

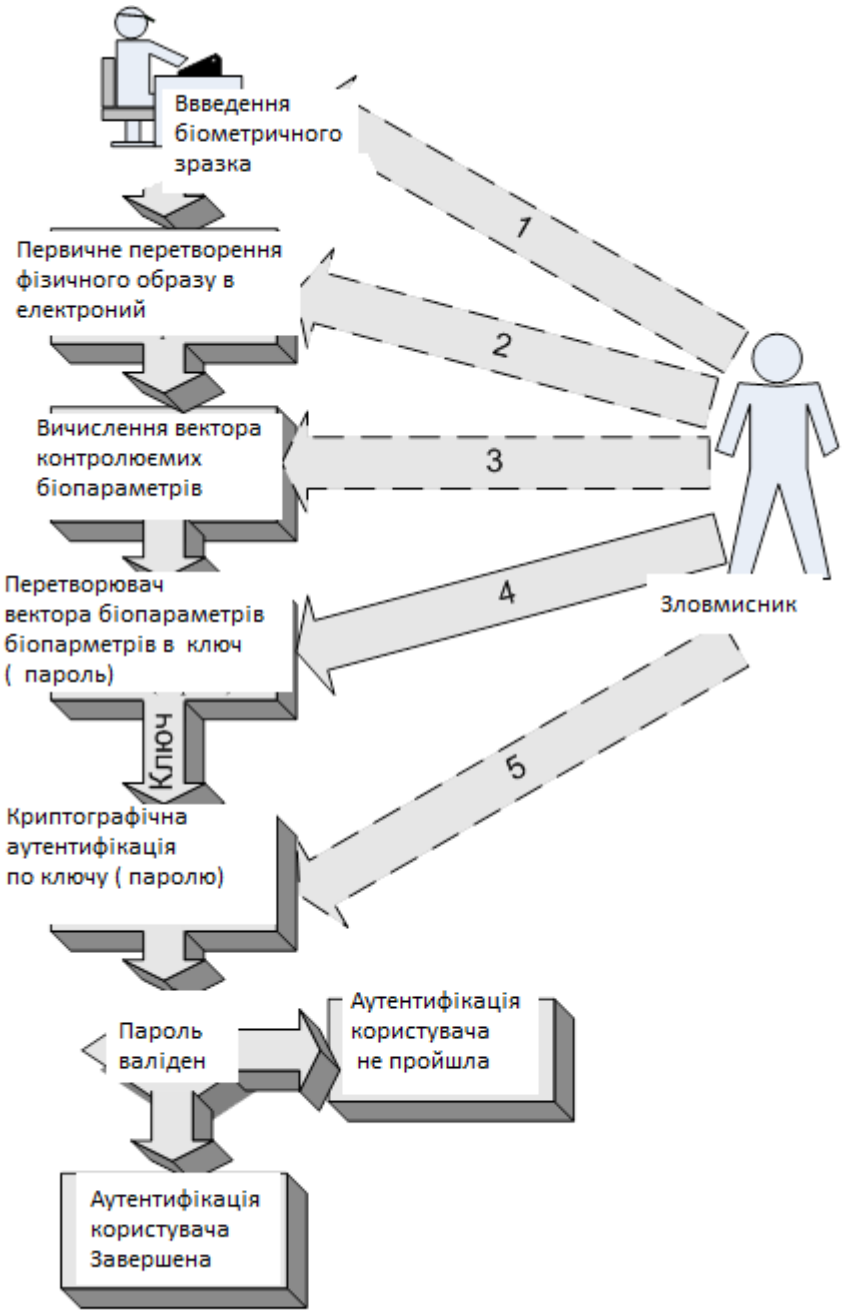

Рисунок 2.4 - Вразливі процедури високонадійної біометричної аутентифікації при атаці на некорелювані шуми

Стійкість класів стабільності рукописного введення по відношенню до атак підбору випадковим сигналом представлено на рис. 2.5. До переваг даного підходу можна віднести незалежність від використовуваного біометричного способу лише від конфігурації нейромережі.

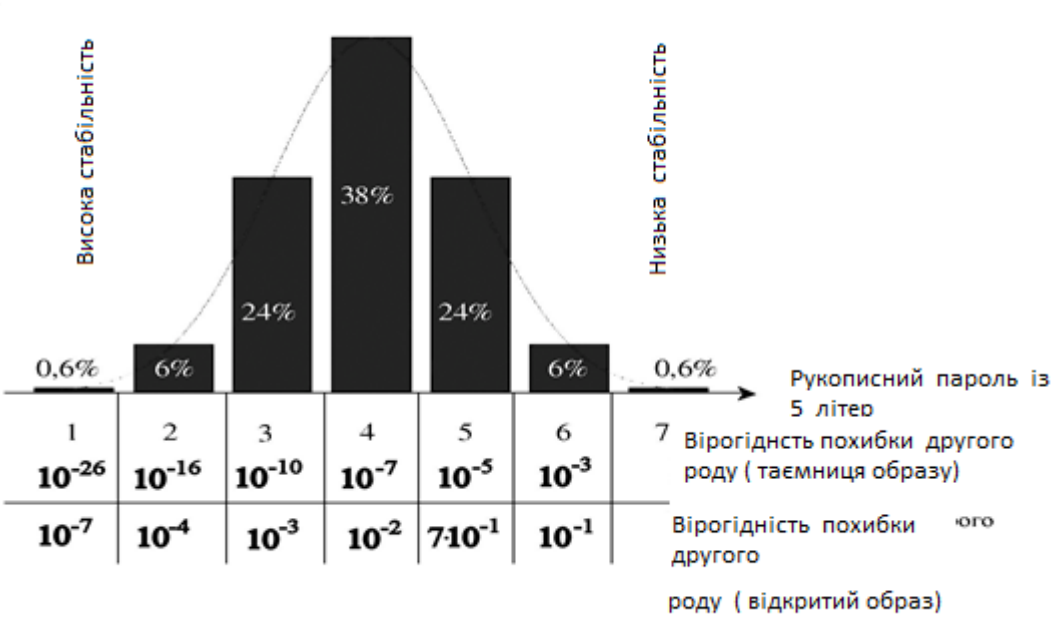

Рисунок 2.51 - Стійкість класів стабільності рукописного введення по відношенню до атак підбору випадковим сигналом

У підсумку можна сформулювати висновок про те, що оцінити інформативність біометричних образів можливо на підставі показників стійкості нейромережевої системи аутентифікації до однієї з таких атак.

2.3. Концептуальна модель забезпечення ефективної нейромережевої оцінки інформативності біометричних образів

Результати проведених досліджень даної роботи, вказують на перспективність застосування нейронних мереж для оцінки інформативності образів в системах біометричної аутентифікації. Для цього необхідно вирішити наукове завдання нейромережевого розпізнавання біометричних образів на підставі аналізу відповідних їм геометричних параметрів. Особливістю сформульованого завдання є необхідність теоретичного обґрунтування характеристик нейромережевих моделей і методів, адаптованих до умов впровадження в сучасних системах біометричної аутентифікації. До вказаних умов відносяться допустимий

термін розробки, можливість залучення трудових ресурсів, наявність доступу до баз даних біометричних образів, необхідних для навчання НСМ, особливості системи контролю біометричних параметрів і допустимий обсяг обчислювальних ресурсів. Рішення даного наукового завдання дозволить вирішити практичну задачу оцінки інформативності біометричних образів на підставі точності нейромережевого розпізнавання особистості користувача. При цьому завдання реєстрації, попередньої обробки біометричних параметрів і їх криптографічних перетворень вважаються вирішеними і в даній роботі не розглядаються [14].

Відповідно до рекомендацій [15], Для вирішення сформульованого завдання розроблено концептуальну модель забезпечення ефективної нейромережевої оцінки інформативності біометричних образів. У зв'язку з тим, що очікуваний практичний результат роботи передбачає створення програмно-апаратного комплексу, то для визначення ефективності використовувати термінологію в області захисту інформації, комп'ютерної та програмної інженерії. Також визначено, що в контексті завдання даного дослідження концептуальна модель, перш за все, призначена для формалізації причинно-наслідкових зв'язків, які властиві процесу біометричної аутентифікації, визначених необхідністю підвищення рівня захищеності сучасних інформаційних систем. Крім цього,

– Умови функціонування систем біометричної аутентифікації.

– Необхідність реалізації ефективного використання нейромережевих засобів для розпізнавання біометричних образів і основні напрямки поліпшення їх функціонування.

– Можливість управління нейромережевими засобами і визначення параметрів, що змінних.

Будь-яка біометричний захист будується на тому, що він здатен добре розпізнавати образ «Свій» і надійно виділяти безліч образів «Чужі» («Все

Чужі»). Очевидно, що засіб біометричного захисту (біометричної аутентифікації) може помилятися. Основним завданням (завданням № 1) для біометрії є забезпечення доступу донору біометричного образу «Свій». Помилка при виконанні цього завдання розглядається, як помилка першого роду. Основною характеристикою ефективності роботи засоби біометричної аутентифікації є імовірність появи помилок першого роду P_1. Другим завданням кошти біометричної аутентифікації є перешкоджати доступу донору образу «Чужий». Другою найважливішою характеристикою біометричних засобів є імовірність появи помилок другого роду P_2 через можливі колізії образів «Свій» і «Чужий» на розглянутому безлічі ознак (біометричних параметрів). Очевидно, що імовірність помилок другого роду P_2 буде тим менше, чим більше біометричних параметрів приймає до уваги той чи інший засіб біометричної аутентифікації. Високонадійними можна вважати тільки ті біометричні засоби, які аналізують сотні або навіть тисячі біометричних параметрів. При цьому атакуючий не повинен знати, що підбирається біометричного способу, тільки в цьому випадку біометрія може розглядатися, як високонадійна.

На сьогоднішній день кращі засоби високонадійної біометричної аутентифікації забезпечують вірогідність помилок другого роду на рівні однієї мільярдної і менше, тобто зловмисник, який намагається подолати біометричний захист, повинен пред'явити мільярд різних біометричних образів (наприклад, відтворити своєю рукою мільярд рукописних паролів). Якщо на відтворення одного рукописного пароля йде 10 секунд, то зловмиснику потрібно 10 млрд секунд, що складе 321 рік безперервних зусиль. Це багато більше часу життя однієї людини. Поодинці простою підстановкою реальних біометричних образів не можна подолати високонадійний захист таємним біометричним чином.

Разом з тим високонадійна біометрична аутентифікація користувачів можлива тільки тоді, коли біометричні механізми надійно пов'язані з криптографічними механізмами аутентифікації. При спільному описі біометричних і криптографічних механізмів, виникає проблема стикування їх термінів. На даний момент терміни біометрії і терміни захисту інформації не зістиковано і навіть при повній мовній тотожності мають різне змістове наповнення.

Одним із шляхів вирішення цього завдання є об'єднання термінів «біометрії» і «захисту інформації», а так само введення відсутніх термінів в ці дві предметні області, через використання більш загального термінологічного апарату «теорії інформації». «Теорія інформації» активно розвивалася в 50-тих, 60-тих, роках минулого століття силами таких вчених як: Шеннон, Колмогоров, Фішер і Кульбак. «Теорія інформації» розвивалася, в основному, для додатків кодування дискретних даних каналів зв'язку, вимірювальної техніки, автоматичного управління і контролю. У 90-роках і на початку цього століття настало певне зниження активності публікацій з «теорії інформації», однак її потенціал як і раніше потребуючий. Покажемо можливості «теорії інформації» на прикладі об'єднання і доповнення термінів і понять «біометрії» і «захисту інформації».

В даний час йде активна робота по створенню системи міжнародних біометричних стандартів. Для цієї мети в ISO / IEC утворений спеціальний підкомітет JTC1 SC37, що відповідає тільки за створення нових міжнародних біометричних стандартів. Найближчим часом ISO / IEC JTC1 SC37 передбачає підготувати і прийняти близько 20 міжнародних біометричних стандартів. В країнах СНГ аналогом ISO / IEC JTC1 SC37 є ГОСТ ТК355 (Автоматична ідентифікація) в особі 7-го підкомітету (Біометрична ідентифікація). Одним із основних понять теорії захисту інформації є рівень захищеність, що забезпечується тим чи іншим

механізмом захисту. Для прикладу, розглянемо криптографічний механізм захисту інформації, побудований на алгоритмі симетричного шифрування з довжиною ключа 256 біт. Для вимірювання рівня захищеності по теорії інформації слід побудувати деякий функціонал імовірності подолання цього захисту. Визначимо цей функціонал наступним чином:

$$J_2 = -\log_2(P_2) \tag{2.2}$$

де J_2 - рівень захищеності, вимірюваний в бітах (довжина еквівалентного симетричного довічного ключа або логарифмічна міра числа можливих станів еквівалентного ключового поля),

P_2 - імовірність подолання захисту з першої спроби або імовірність удачі атаки випадкового підбору ключа з першої спроби.

Криптографічні механізми захисту інформації, побудовані на базі симетричного шифрування, слід розглядати, як еталонні. Для них довжина ключа і рівень захищеності практично збігаються. Тобто для симетричного алгоритму шифрування по ГОСТ 28147-89 рівень захищеності буде спостерігатися тільки в системах, де допускається використання не тільки сильних, але і всіх слабких ключів. Функціонал (2.2) можна побудувати для абсолютно різних криптографічних механізмів захисту інформації. У табл.0.1 приведені логарифмічні показники рівня захищеності для парольної аутентифікації і ряду іноземних криптографічних механізмів за даними [12].

Таблиця 2.1 Показники рівня захищеності

Найменування механізму криптографічного захисту та його характеристики	Значення логарифмічного показника рівня захищеності
Парольна аутентифікація, класичний восьмі символьний пароль, який обирано особисто користувачем	22,7 біт
Алгоритм DESc 56 бітовим ключем (ANSIX9.9 і інші DES механізми, аутентифікації, шифрування, і т.д.	54 біта
Аутентифікаційні механізм з 512 - бітовим відкритим ключем для цифрових підписів	63 біта

Криптографічний механізм з 768 бітовим ключем - мінімальний розмір RSA - ключа відповідно до рекомендації RSASecurity, 1999 г.	76 біт
Механізми аутентифікації з 1024 - бітовими відкритими ключами	86 біт
Механізми аутентифікації з 2048 - бітовими відкритими ключами з високою захищеністю	116 біт
Криптографічний механізм з алгоритмом ASE з 128-бітовим ключем	127 біт

Таблиця 0.1 наочно показує, що довжина криптографічного ключа і рівень захищеності, відповідного криптографічного механізму далеко не завжди збігаються. Більш того, при точних оцінках рівня захищеності в загальному випадку повинні виходити дробові (не цілі) довжини еквівалентного ключа, що є наслідком безперервності (не дискретності) функціоналу (2.1).

Одним з головних достоїнств, наведеного вище інформаційного підходу є те, що знімаються протиріччя, що виникають при порівнянні рівня захищеності біометричних і криптографічних механізмів захисту інформації. Зокрема для кожної з існуючих на сьогодні біометричних технологій може бути побудована своя таблиця довжин еквівалентних ключів або показників рівня захищеності. Зразкові значення інформативності для різних технологій наведені в табл. 2.2.

Таблиця 2.2 Рівні захищеності різних біометричних механізмів

Назва технології біометричних механізмів захисту	Стійкість до атак підбору	Мінімальний рівень захищеності	Максимальний рівень захищеності
Аналіз кровоносних судин очного дна	Від 108 до 1012	27 біт	40 біт
Аналіз райдужної оболонки ока	Від 106 до 109	20 біт	30 біт
Аналіз геометричних особливостей особи	Від 102 до 104	7 біт	14 біт
Аналіз особливостей геометрії вушних раковин	Від 102 до 103	7 біт	10 біт
Аналіз особливостей папілярного малюнка одного пальця	Від 104 до 1013	12 біт	39 біт

Аналіз геометрії долоні, включаючи рисунки складок шкіри долоні і папілярні малюнки різних фрагментів шкіри долоні	Від 102 до 105	7 біт	17 біт
Аналіз малюнка кровоносних судин, складок шкіри тильної сторони долоні	Від 102 до 103	7 біт	10 біт
Аналіз рукописного почерку	Від 102 до ∞	7 біт	Немає обмежень
Аналіз геометричних співвідношень частин тіла	Від 103 до 106	10 біт	20 біт

Очевидно, що за своєю суттєвостю функціонал (2.2) є деяким визначенням поняття «захисної інформації» йде на захист іншої «інформації» вже в класичному розумінні цього терміна [11]. У цьому контексті можна визначити похідне поняття інформативності біометричного способу (технології, механізму). Чим більше «захисної інформації» містить біометричний образ, тим більш ефективними можуть виявитися, відповідні, біометричні механізми захисту.

На даний момент оціночні довжини еквівалентних ключів для цих технологій в залежності від довжини пароля наведені в табл.2.3, складеної на основі даних ФГУП «ПНІЕІ».

Таблиця 2.3 Довжини еквівалентних ключів для середньостатистичного користувача

Число букв (цифр) в паролі, що утворює біометричний образ без врахування пробілів між словами	Довжина ключа (пароля) одержуваного з рукописного пароля (Біт)	Довжина ключа (пароля) отриманого з звучання ключового слова (Біт)	Довжина ключа (пароля) отриманого з динамічних параметрів клавіатурного почерку (Біт)
4	24	----	-------
5	30	----	------
6	36	----	------
7	42	----	------
8	48	----	------
9	56	---	------
10	62	7	------
12	76	9	------
14	90	11	-----

16	104	13	7
18	128	15	8
20	142	17	10
24	160	21	11
26	188	25	14
32	216	29	17
36	234	33	20
40	262	37	23

На наступному етапі побудови концептуальної моделі з урахуванням загальноприйнятої технології використання НСМ визначено, що процес нейромережевої оцінки інформативності біометричних образів повинен передбачати формування параметрів навчальних прикладів, формування навчальної вибірки, визначення виду і параметрів НСМ і використання НСМ для оцінки інформативності.

Використання даного твердження дозволило побудувати показану на рис. 2.6 діаграму декомпозиції нейромережевої оцінки інформативності біометричних образів в системах біометричної аутентифікації.

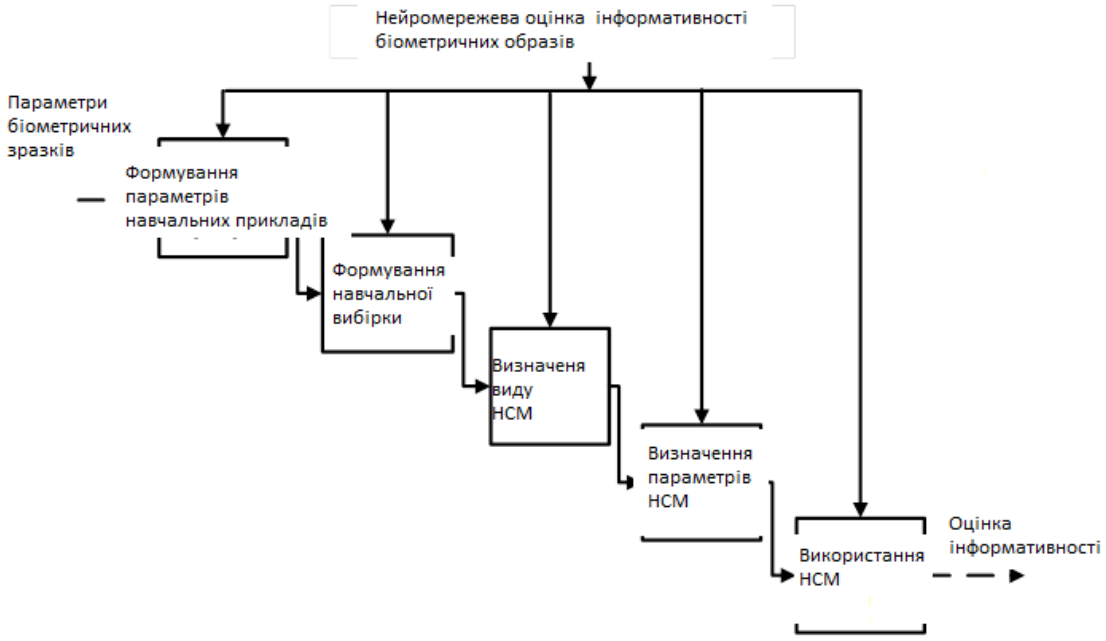

Рисунок 2.6 - Діаграма декомпозиції нейромережевої оцінки інформативності біометричних образів

Призначення складових даної діаграми складається в наступному:

– Формування параметрів навчальних прикладів - визначення для кожного виду біометричних образів безлічі вхідних і вихідних параметрів і способу їх кодування.

– Формування навчальної вибірки - визначення такого безлічі навчальних прикладів, яке відповідає стандартам біометричних образів. Кількість, якість і номенклатура прикладів повинні бути достатніми для навчання НСМ.

– Визначення виду і параметрів НСМ - визначення для використання такого виду НСМ, з такими параметрами, які найбільш повно відповідають умовам завдання оцінки інформативності біометричних образів заданого виду.

– Використання НСМ - оцінювання інформативності біометричних образів на підставі величини помилки розпізнавання розпізнавання кібератак на мережеві РІС.

Наступним етапом створення концептуальної моделі стала розробка показаної на рис. 2.7 схеми компонентів НСС оцінювання інформативності біометричних образів. У схемі враховані особливості реалізації НСС, призначені для оцінювання інформативності біометричних образів на підставі помилки розпізнавання, і результатів розділу 1, які стосуються особливостей нейромережевих технологій біометричної аутентифікації.

Таким чином, в процесі розробки враховано:

– Недосконалість методів формування параметрів НСМ, призначених для оцінювання інформативності біометричних образів.

– Тривалий період формування навчальної вибірки для НСМ в разі обмеженого доступу до баз даних біометричних образів.

– Залежність характеристик навчальної вибірки від характеристик баз даних біометричних образів і параметрів навчальних прикладів.

– Залежність параметрів НСМ від характеристик навчальної

вибірки.

Тому в схемі передбачена можливість формування параметрів НСМ і навчальної вибірки за допомогою експертних даних.

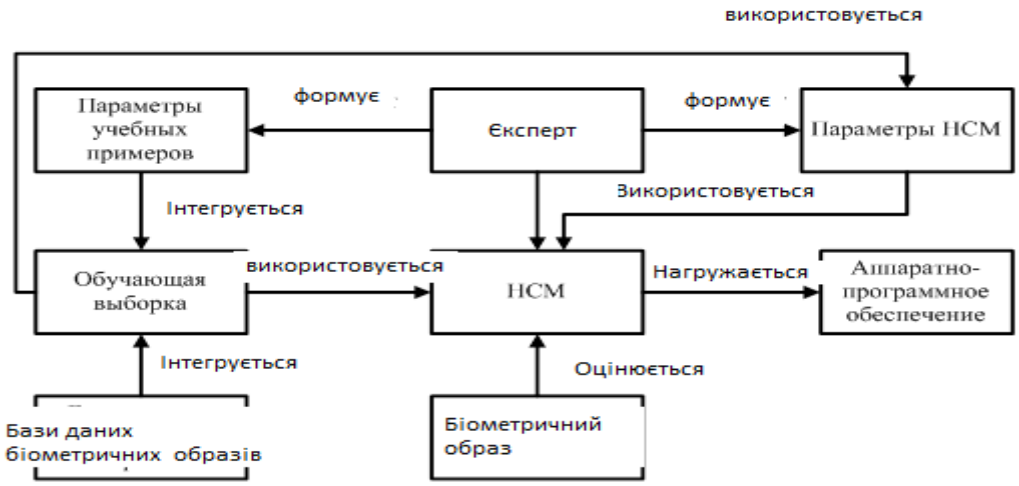

Рисунок 2.7 - Схема взаємодії компонентів НСС оцінювання інформативності біометричних образів

Аналіз даних, показаних на рис. 2.6 і рис. 2.7, дозволяє стверджувати, що на ефективність нейромережевого оцінювання інформативності біометричних образів впливає ряд факторів, показаних на рис. 2.8.

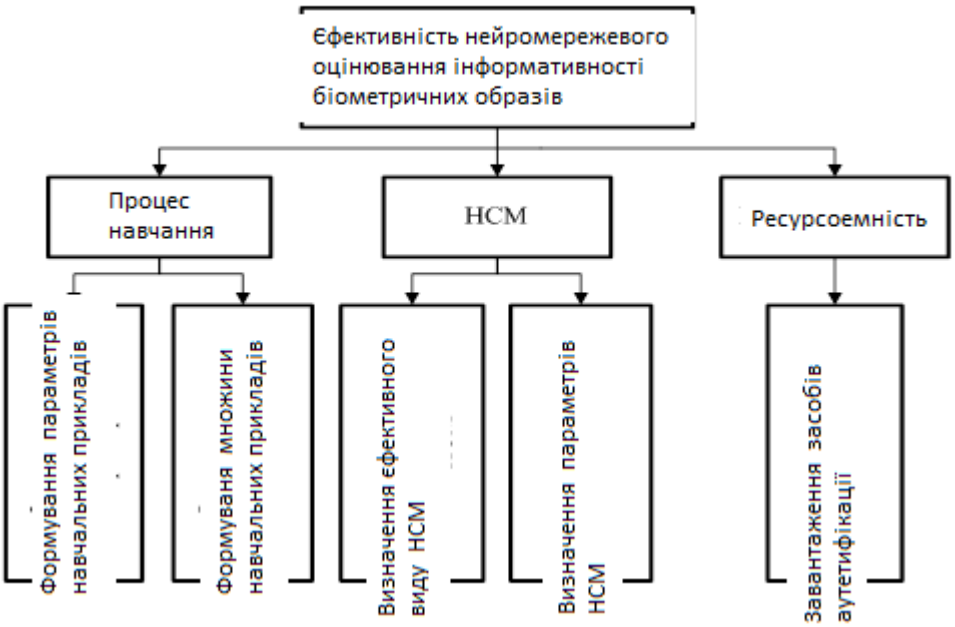

Рисунок 2.8 - Фактори, що впливають на ефективність оцінювання

Крім цього, можна стверджувати, що ефективністрь нейромережевого оцінювання інформативності доцільно характеризувати, як з точки зору ефективності процесу використання НСР, так і з точки зору ефективності процесу навчання НСМ. При цьому показники ефективності повинні відображати тривалість, ресурсомісткість і точність названих процесів. Таким чином, обгрунтовані показання на рис. 2.4 показників оцінки ефективності нейромережевого оцінювання інформативності. В результаті визначено, що в загальному вигляді концептуальну модель забезпечення ефективності процесу нейромережевого оцінювання інформативності біометричних образів можна відобразити за допомогою виразів:

$$E_{\Sigma} = f\left(E_{НСР}, E_{ОВ}\right) \tag{2.3}$$

$$E_{НСР} = f\left(e_1, e_2, e_3\right) \tag{2.4}$$

$$E_{ОВ} = f\left(e_4, e_5\right) \tag{2.5}$$

де E_{Σ} - інтегральна ефективність процесу,

$E_{НСР}$ - ефективність створення і використання НСР,

$E_{ОВ}$ - ефективність створення навчальної вибірки,

e_1 - визначення ефективних видів НСМ,

e_2 - визначення параметрів НСМ,

e_3 - ресурсомісткість використання НСР,

e_4 - визначення параметрів навчальних прикладів,

e_5 - формування навчальної вибірки.

Відзначимо, що використання нейромережевих засобів в системах

біометричної аутентифікації, що базуються на аналізі геометричних параметрах, має такі особливості:

- Наявність загальнодоступних і досить повних баз даних біометричних образів.

- Використання потужної обчислювальної бази.

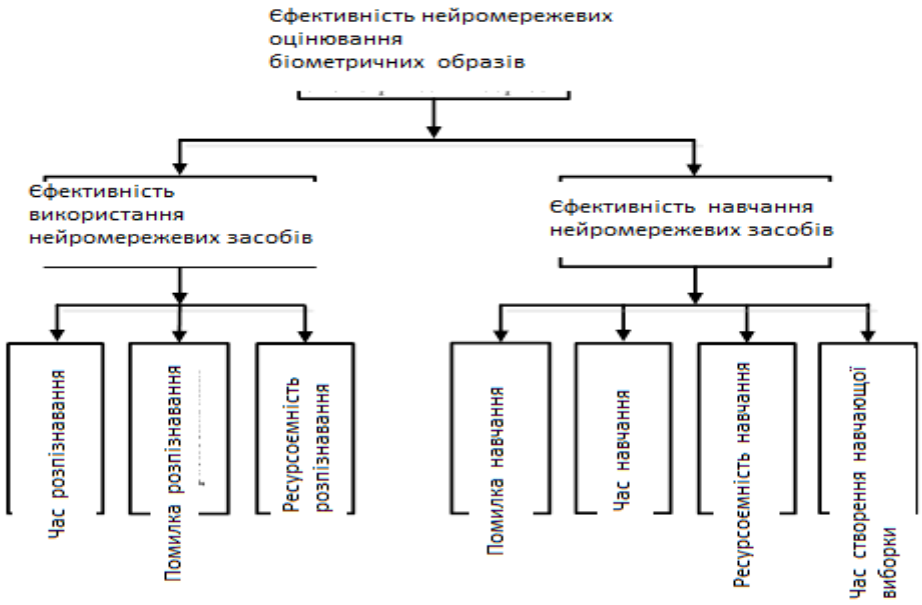

Рисунок 2.9 - Показники оцінки ефективності нейромережевого розпізнавання

Тому можна вважати, що ефективність сучасних нейромережевих засобів оцінювання інформативності біометричних образів в основному залежить від процесів їх створення і використання. Таким чином, концептуальну модель забезпечення ефективності процесу нейромережевого оцінювання інформативності можна істотно спростити і в аналітичному вигляді записати за допомогою формули:

$$E_{\Sigma} = f(e_1, e_2). \qquad (2.6)$$

Підсумок проведених досліджень дозволяє стверджувати, що для ефективного нейромережевого оцінювання біометричних образів необхідно доповнити методологічну базу поруч принципів і моделей процесів використання НСР. Надалі необхідно застосувати отримані елементи методологічної бази для розробки нейромережевих методів оцінювання інформативності біометричних образів.

Також необхідно визначити критерій, який буде використаний для нейромережевої оцінки інформативності біометричних образів.

Висновки

Другий розділ присвячено вирішенню наукової задачі формалізації процесів біометричної аутентифікації, що базуються на геометричних параметрах особистості.

Також визначено, що оцінити інформативність біометричних образів можливо на підставі показників стійкості,які в основному визначаються похибкою засобів аутентифікації.

Розроблено концептуальну модель забезпечення ефективної нейромережевої оцінки інформативності біометричних образів дозволяє врахувати:

– Умови функціонування систем біометричної аутентифікації.

– Необхідність реалізації ефективного використання нейромережевих засобів для розпізнавання біометричних образів і основні напрямки поліпшення їх функціонування.

– Можливість управління нейромережевими засобами і визначення параметрів, що змінних.

Використання отриманих моделей забезпечило можливість чіткого визначення напрямків досліджень, пов'язаних з розробкою ефективних нейромережевих моделей і засобів для ефективної оцінки інформативності біометричних образів, а саме рукописних підписів користувачів.

РОЗДІЛ 3. РОЗРОБКА МОДЕЛЕЙ ТА МЕТОДУ НЕЙРОМЕРЕЖЕВОЇ ОЦІНКИ ІНФОРМАТИВНОСТІ ПІДПИСІВ

3.1. Нейромережева модель оцінки інформативності образу підпису

Найбільш природний і давно використовуваний метод перевірки особистості - це перевірка рукописного підпису. Метод верифікації рукописного підпису більш поширений і менш нав'язливий, ніж інші методи біометричної аутентифікації. Той факт, що рукописний підпис широко використовується як засіб особистої перевірки, підкреслює необхідність автоматичної системи перевірки.

Автономні системи ідентифікації працюють з відсканованим зображенням підпису, а значить його можна розпізнати, використовуючи комп'ютерне зір. Нейронні мережі є фундаментальною частиною комп'ютеризованих задач розпізнавання образів вже понад півстоліття, і продовжують використовуватися в дуже широкому діапазоні проблемних областей [16]. Підхід до вирішення завдання за допомогою нейронних мереж пропонує кілька переваг, таких як уніфіковані підходи до вилучення і класифікації ознак і гнучкі процедури пошуку хороших, помірно нелінійних рішень. Коли даний підхід використовується в динамічній або автономної перевірки підпису, він також показує розумну продуктивність.

Розпізнавання підписів можна розглядати як задачу класифікації зображень [17]. Класифікація в такому випадку є введення вхідного зображення і виведення класу або ймовірності класів, які найкраще описують зображення. Найбільш відповідною основою для розробки автоматичної системи класифікації зображень є згорнута нейронна мережа [18].

Безпосередньо формуючи постановку задачі «розробити алгоритм автоматичної перевірки рукописного підпису за допомогою згорнутої нейронної мережі, виходячи з даних, отриманих від осіб, чиї підписи

повинні бути автентифіковано системою», варто зазначити, що алгоритм повинен по набору вхідних даних визначити, чи є власноручний підпис справжньої або підробленої, коли фізична особа вимагає підтвердження особи. Підхід до автоматичної перевірки підпису повинен здійснюватися на основі інтелектуальних алгоритмів, а саме штучних нейронних мереж.

Архітектура згорнутої нейронної мережі

Для розпізнавання рукописних підписів ми використовували архітектуру згорнутої нейронної мережі, представленої на рис 3.1.

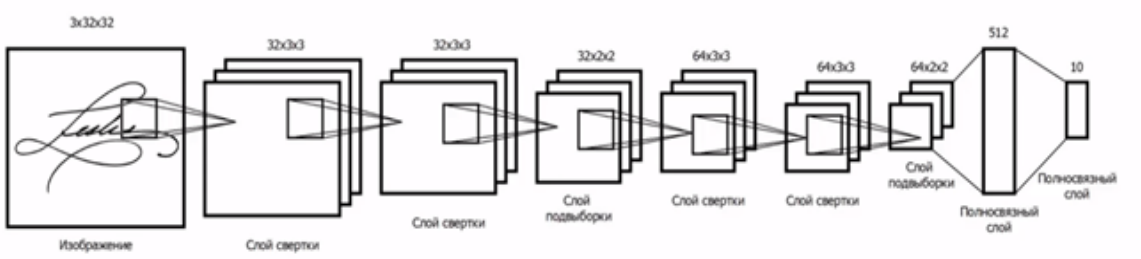

Рисунок 3.1 - Архітектура згорнутої нейронної мережі

Дана мережа складається з двох повторюваних ділянок, які містять по два шари згорнуті і по одному шару підвибірки. Дані ділянки призначені для виділення основних ознак рукописного підпису. В кінці мережі розташований класифікатор, який складається з одного повно зв'язаного шару, який містить 512 нейронів, і вихідного шару, який містить 10 нейронів.

На вхід мережі надходять зображення розміром 32 на 32 пікселів в трьох каналах: червоний, зелений і синій. На першому шарі згортки використовується 32 карти ознак розміру 3 на 3. Тобто кожен нейрон згорнутого шару підключений до квадратному ділянці зображення розміром 3 на 3.

Наступний згорнутий шар має таку ж архітектуру: 32 карти ознак с ядром згорнуті 3 на 3. Після цього йде шар підвибірки, на якому виконується зменшення розмірності зображення.

Зміна розмірності виконується для кожної карти ознак окремо, тому тут використовується також 32 карти ознак.

Розмір поля підвибірки 2 на 2. Після шару підвибірки починається новий каскад згорнутих шарів.

На третьому і на четвертому шарі згортки використовується 64 карти ознак розміром 3 на 3, а на другому шарі підвибірки, яка йде після цих згорнутих шарів, також відбувається зменшення розмірності в квадраті 2 на 2. Після цього дані перетворюються з двовимірного формату в одновимірний і передаються на повно зв'язаний шар, на якому вже виконується класифікація.

Постановка завдання «навчання і тестування згорнутої нейронної мережі» зводиться до того, що у згорнутих мережах використовується підхід навчання з учителем[19]. Тобто нам необхідно мати розмічений набір даних. Для свого завдання ми використовували рукописні підписи десяти чоловік. Кожна людина розписався ручкою на листку вісім разів. Після цього, рукописні підписи були переведені в зображення розміром 32 на 32 пікселів. Зображення мали растровий формат png. Приклади зображень підписів наведені на рис. 3.2.

Рисунок 3.2 - Приклади рукописних підписів

Перед навчанням зображення рукописних підписів розподілили по двом наборам: набір для навчання (зображення і мітки класів) і набір для тестування (зображення і мітки класів). Набір для навчання складався з 200 зображень, а набір для тестування складався з 40 зображень. Мітки класів містили правильні відповіді, чия рукописний підпис представлена на зображенні.

Відповідно до сучасної методології застосування нейронних мереж в області захисту інформації побудова ефективної нейромережевої моделі оцінки інформативності образу підпису розділяється на два основні блоки:

1. Визначення найбільш ефективного виду моделі.

2. Адаптація параметрів моделі ефективного виду до умов поставленого завдання.

Результати [20] свідчать про те, що завдання визначення найбільш ефективного виду НСМ можливо вирішити на підставі підходу - найбільш ефективним є той вид НСМ, характеристики якого більш повно відповідають значущим умовами завдання визначення інформативності біометричних образів.

Також встановлено, що безліч значимих умов ділиться на категорії, що характеризують навчальні дані, обмеження процесу навчання, обчислювальні потужності, вихідну інформацію, технічну реалізацію і сферу застосування НСР.

Показано, що відповідність виду НСМ k-му умові можна визначити за допомогою k-го параметра ефективності - цей параметр дорівнює -1:

- якщо умова не виконується, дорівнює 1;
- якщо умова виконується і дорівнює 0;
- якщо умова виконується частково.

Значимість k-го умови пропонується враховувати за допомогою вагового коефіцієнта. Математичної інтерпретацією такого підходу є вираз:

$$E_{\sum}(a_i) \rightarrow \max \; a_i \in \boldsymbol{A}, i = 1..I \qquad (3.1)$$

де $E_{\sum}(a_i)$ – інтегральний критерій ефективності і-го виду НСМ;

a_i – i-й вид НСМ;

A – безліч допустимих видів НСМ;

I – кількість допустимих видів НСМ;

У свою чергу розрахунок інтегрального критерію ефективності для і-го виду НСМ можливо реалізувати так:

$$E_{\sum}(a_i) = \sum_{k=1}^{K} \left(r_k E_k(a_i) \right),\ a_i \in \boldsymbol{A},\ i = 1..I \qquad (3.2)$$

$E_k(a_i)$ – значення k-го параметра ефективності і-го виду НСМ;

K – кількість параметрів ефективності;

r_k – ваговий коефіцієнт k-го параметра ефективності.

В результаті аналізу даних [6] з урахуванням [21],отриманий показаний в табл. 3.1 перелік основних параметрів, що характеризують умови задачі визначення інформативності образу підпису, який характеризуються геометричними параметрами. При цьому не використані параметри, що характеризують умови не істотні для поставленої задачі. До вказаних умов відносяться:

- можливість використання навчальних прикладів з необмеженою кількістю вхідних параметрів.
- можливість використання безперервних вхідних параметрів.
- інтерпретована виходу в графічному вигляді.
- можливість вербалізації.
- апробовані сфери застосування, пов'язані з аналізом тексту, управлінням параметрами захисту, моделюванням часових рядів, аналізом звуку, розвідувальним аналізом даних.

У той же час перелік доповнений кількома параметрами, які деталізують сферу застосування, пов'язану з аналізом зображень.

Таблиця 3.1 Параметри ефективності

№	Категорія	Пояснення параметра
1	2	3

E_1	навчальні дані	Обмеженість навчальної вибірки
2		Допустимість шуму
3		Допустимість кореляції
4		Необхідність відображення всіх аспектів процесу
5		Необхідність пропорційного представлення прикладів
6		Можливість використання дискретних вхідних параметрів

Продовження таблиці 3.1.

	Категорія	Пояснення параметра
	2	3
7		Можливість використання навчальної вибірки, обсяг якої буде меншою за кількість вхідних параметрів
8	Процес навчання	Короткий термін навчання
9		Необхідність подання очікуваного виходу
10		Автоматизація навчання
11		можливість донавчання
12		Якість навчання
13		Можливість навчання на експертних даних
14		Незмінність результатів
15		Можливість паралелізації навчання
16	Процес навчання	Можливість гібридного навчання на маркованих і немаркованих даних
17	Обчислювальна потужність	Обсяг пам'яті

18		Екстраполяції результатів навчання
19	Вихідна інформація	Інтерпретируємость виходу у вигляді ймовірності
20	Технічна реалізація	Швидкість прийняття рішення
21		Обсяг програмно-апаратної реалізації
22		Складність реалізації
23	Апробованість в області геометричного аналізу	папілярних ліній
29		Відображення рукописних символів

Згідно з результатами, отриманими в [11], в сучасних апробованих системах біометричної аутентифікації застосовуються НСМ з прямим розповсюдженням сигналу, архітектура яких подібна до класичного МСП. На підставі даних [22] І власного практичного досвіду в першому наближенні компоненти А можливо визначити так:

$$\mathrm{A} = \{МСП, ДСП, ГНС_A, ГНС_P, СНС\} \tag{3.3}$$

де МСП - багатошаровий персептрон,

ДСП - двошаровий персептрон,

$ГНС_A$ - глибока нейронна мережа з предобученіем,

$ГНС_P$ - глибока нейронна мережа в прихованих нейронах якої використовується функція активації типу ReLU,

СНС - згорнута нейронна мережа.

Відзначимо, що функція ReLU (випрямлена лінійна функція) визначається так:

$$f(X_\Sigma) = \max(0, X_\Sigma) \tag{3.4}$$

де $f(X_\Sigma)$ – вихідний сигнал прихованого нейрона;

X_Σ – сумарний вхідний сигнал прихованого нейрона, який визначається виразом (3.5);

max – функція визначення максимуму від переданих їй аргументів.

$$X_\Sigma = \sum_{i=0}^{I} (w_i x_i) \qquad (3.5)$$

де I – кількість вхідних сигналів нейрона прихованого шару,

x_i – i-ій вхідний сигнал ($x_0 = 1$),

w_i – ваговий коефіцієнт i-го вхідного сигналу.

Величини параметрів ефективності для апробованих видів НСМ представлені в табл.3.2. Слід зазначити, що величини параметрів визначені в базовому випадку експертним шляхом, з урахуванням необхідності порівняльного аналізу НСМ між собою. Надалі величини параметрів можуть бути скореліровани.

Таблиця 3.2 Величини параметрів ефективності для апробованих видів нейромережевих моделей

№	Вид нейромережевої моделі				
	ДСП	СНС	$\text{ГНС}_\text{А}$	$\text{ГНС}_\text{Р}$	МСП
1	2	3	4	5	6
E_1	-1	-1	0	0	-1
E_2	0	0	0	0	0
E_3	0	0	0	0	0
E_4	1	1	1	1	1
E_5	0	0	1	0	0

Продовження таблиці 3.2.

№	Вид нейромережевої моделі				
	ДСП	СНС	$\text{ГНС}_\text{А}$	$\text{ГНС}_\text{Р}$	МСП
E_6	1	1	1	1	1
E_7	-1	0	-1	-1	-1
E_8	-1	-1	0	0	-1
E_9	-1	-1	-1	-1	-1
E_{10}	1	1	1	1	1
E_{11}	-1	0	0	0	-1

E_{12}	1	1	1	0	1
E_{13}	-1	-1	-1	-1	-1
E_{14}	1	1	1	1	1
E_{15}	0	1	1	1	0
E_{16}	-1	-1	1	-1	-1
E_{17}	-1	1	1	1	0
E_{18}	1	1	1	1	1
E_{19}	0	1	1	1	0
E_{20}	1	1	1	1	1
E_{21}	0	0	0	0	0
E_{22}	1	0	0	0	1
E_{23}	1	1	1	1	1
E_{24}	0	1	0	0	0
E_{25}	0	1	0	0	0
E_{26}	0	1	0	0	0
E_{27}	0	1	0	0	0
E_{28}	0	1	0	0	0
E_{29}	0	1	0	0	0

Також в базовому випадку прийнято, що величини вагових коефіцієнтів для всіх параметрів однакові і рівні 1.

Це дозволило на підставі даних табл. 3.2 за допомогою виразу (3.2) розрахувати значення інтегрального критерію ефективності для всіх видів НСМ, які входять до складу безлічі А.

Отримані величини представлені в табл. 3.3.

Підставивши дані табл. 3.3 в вираз (3.1) визначено, що найбільш ефективним видом НСМ є СНС.

Типова структура згорнутої нейронної мережі, призначена для розпізнавання зображень, показана на рис. 3.1 [13]. Вхідні параметри такої нейросетевой моделі відповідають окремим пікселям. Тому кількість вхідних параметрів дорівнює розміру зображення. Кількість вихідних нейронів дорівнює кількості розпізнаваних образів, а кількість прихованих нейронів підбирається експериментальним шляхом з позицій максимальної точності розпізнавання.

Таблиця 3.3 Величини інтегрального критерію ефективності для апробованих видів нейромережевих моделей

Величина інтегрального критерію	**Вид нейромережової моделі**				
	ДСП	**СНС**	**ГНС$_А$**	**ГНС$_Р$**	**МСП**
E_Σ	1	13	10	6	2

По суті згорткові мережі являють собою варіацію багатошарового персептрона, що складається з згортальних шарів, шарів підвибірки (Субдіскретізація) і повнозв'язних шарів. На згортальних шарах виконується операція згортки вхідних карти ознак з ядром згортки, яке визначають вагові коефіцієнти нейрона.

Сумарний вхідний сигнал деякого нейрона першого згорнутого шару розраховується так:

$$x_1^{(i,j)} = b_1 + \sum_{s=1}^{S}\sum_{t=1}^{S} w_{1,s,t} x^{((i-1)+s,(j+t))} \tag{3.6}$$

де $x_1^{(i,j)}$ - вхідний сигнал (i,j)-го нейрона першої карти ознак,

b_1 - зміщення нейронів першої карти ознак,

S - розмір рецептивної області нейрона (розмір ядра згортки),

$w_{1,s,t}$ - ваговий коефіцієнт (s,t)-ой синаптичного зв'язку нейрона першої карти ознак,x - вихід нейрона попереднього шару.

Сумарний вхідний сигнал довільної нейрона наступних згортальних шарів розраховується так:

$$x_k^{(i,j)} = f\left(b_k + \sum_{s=1}^{K}\sum_{t=1}^{K} w_{k,s,t} x^{((i-1)+s,(j+t))}\right) \tag{3.7}$$

де $x_k^{(i,j)}$ - вхідний сигнал (*i,j*)-го нейрона *k*-ой карти признаків,

b_k - зміщення нейронів *k*-ой карти признаків,

$w_{k,s,t}$ - ваговий коефіцієнт (*s,t*)-ой синаптичного зв'язку нейрона k-ой карти ознак,*x* - вихід нейрона попереднього шару.

f – функція активації.

Вихідний сигнал нейрона карти ознак розраховується шляхом підстановки сигналу, що визначається (3.6, 3.7) в функцію активації:

$$y = f(x) \tag{3.8}$$

Досить часто в якості функції активації використовується гіперболічний тангенс. В цьому випадку вираз (3.8) змінюється так:

$$y = d\frac{e^{a\times x} - e^{-a\times x}}{e^{a\times x} + e^{-a\times x}} \tag{3.9}$$

де d, a - задані коефіцієнти.

Рекомендовані значення зазначених коефіцієнтів d = 1,7159 і a = 2/3. Зазначені значення обумовлені тим, що гіперболічний тангенс (3.9) має наступні корисні властивості [14]:

- Максимум другої похідної при *d*=1;
- $f(1) = 1, f(-1) = -1$;
- На початку координат тангенс кута нахилу близький до одиниці;
- Очікуваний відгук мережі зміщений від кордону області значень функції активації в сторону її внутрішньої частини. В цьому випадку відбувається шляхом зміни вільних параметрів мережі в процесі навчання вдається уникнути різкого зростання їх значень, що дозволяє прискорити процес навчання.

Також відомо використання в якості функції активації експоненціального сигмоїда виду

$$y = \frac{1}{1 + e^{-\alpha x}} \tag{3.10}$$

де α - заданий коефіцієнт (швидкість навчання).

Величину швидкості навчання можна розраховувати відповідно до рекомендацій [22].

Шари Субдіскретізація, такі після згортальних, зменшують розмірність карти ознак та забезпечують інваріантність до масштабу. Вони мають один настроюється параметр - коефіцієнт Субдіскретізація, який визначає, у скільки разів буде зменшено зображення, відповідне попередній карті ознак. Вихідний сигнал нейрона шару Субдіскретізація визначається виразом:

$$y_k^{(i,j)} = b_k + \frac{1}{4} w_{k,s,t} \sum_{s=1}^{2} \sum_{t=1}^{2} x^{((i-1)+s,(j+t))} \tag{3.11}$$

Сумарний вхідний сигнал нейронів повнозв'язну шару розраховується за допомогою формули (3.5), а вихідний сигнал в залежності від використовуваної функції активації - за допомогою виразів (3.4, 3.9, 3.10).

В нейронах вихідного шару СНС, як правило, використовується функція активації типу SOFTMAX, що дозволяє інтерпретувати вихідний сигнал мережі у вигляді ймовірності. У цьому випадку вихідний сигнал нейронної розраховується так:

$$y = \frac{e^{X_\Sigma}}{\sum_{q=1}^{Q} e_q^{X_\Sigma}} \tag{3.12}$$

де Q – кількість нейронів в повнозв'язну шарі. X_Σ – сумарний вхідний сигнал вхідний сигнал нейронів вихідного шару, який визначається за допомогою виразу (3.5),

Також варто відзначити, що після всіх операцій згортки і Субдіскретізація матриця, що описує вихідне зображення, вироджується в

вектор, відповідний нейронам останнього прихованого шару.

Відома кілька спрощена згорнутої нейронна мережа, структура якої показана на рис. 3.3 [24]. На відміну від типової СНС в цій мережі немає шарів підвибірки. При цьому почергове стиснення карт ознак з метою виділення ознак більш високого рівня ієрархії забезпечено за рахунок зміщення ядра згортки з кроком 2.

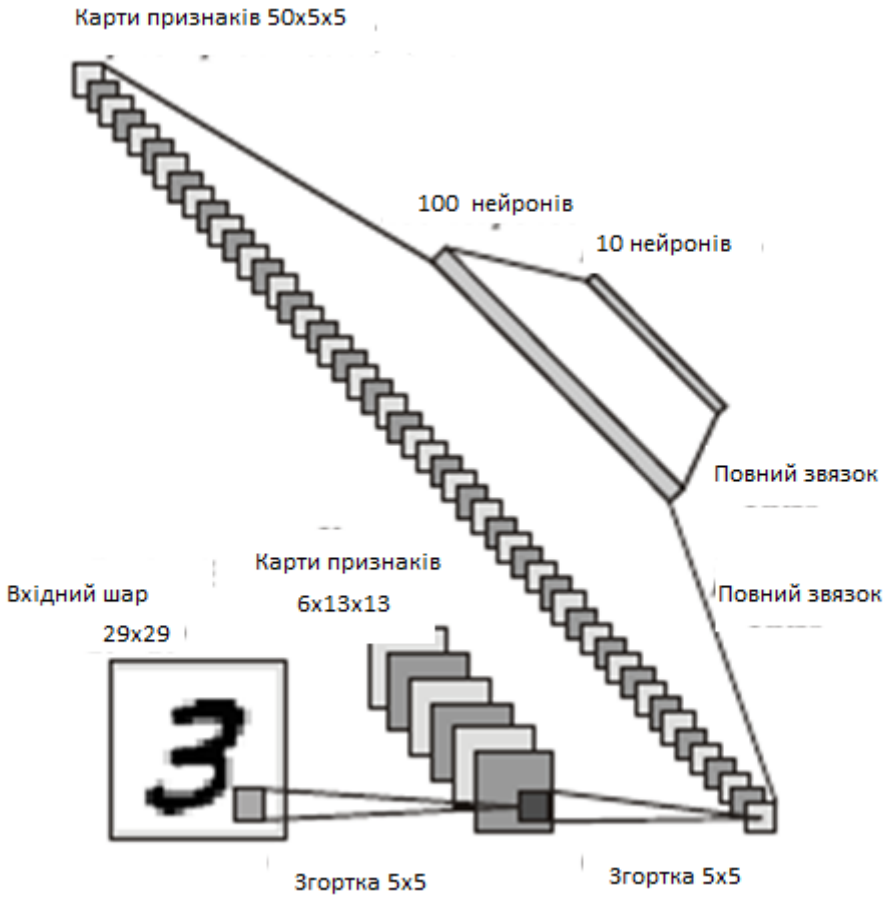

Рисунок 3.3 - Структура спрощеної свёрточной нейронної мережі

Для навчання СНС використовується стратегія навчання «з учителем», в основі якої лежить добре апробований алгоритм зворотного поширення помилки, реалізація якого спрямована на мінімізацію функції помилки виду:

$$E(\boldsymbol{W}) = \frac{1}{2}\sum_{p=1}^{P}\sum_{m=1}^{M}\left(y_m^p - d_m^p\right)^2 \qquad (3.13)$$

де P – розмір (кількість прикладів) навчальної вибірки,

p - номер навчального прикладу,

M - кількість вихідних нейронів,

m - номер вихідного нейрона,

y_m^p – реальне значення вихідного сигналу m-го вихідного нейрона для p-го навчального прикладу,

d_m^p – очікуване значення вихідного сигналу m-го вихідного нейрона для p-го навчального прикладу.

$\boldsymbol{W}$ – матриця вагових коефіцієнтів.

Для пошуку мінімуму функції (3.13) використовується градієнтний алгоритм найшвидшого спуску.

3.2. Адаптація структурних параметрів згорнутої нейронної мережі до умов завдання оцінки інформативності підпису

У загальному випадку методологія адаптації НСМ до умов поставленого завдання класифікації передбачає синтез алгоритмів настройки безлічі керованих параметрів. Структура цієї методології представлена на рис. 3.4.

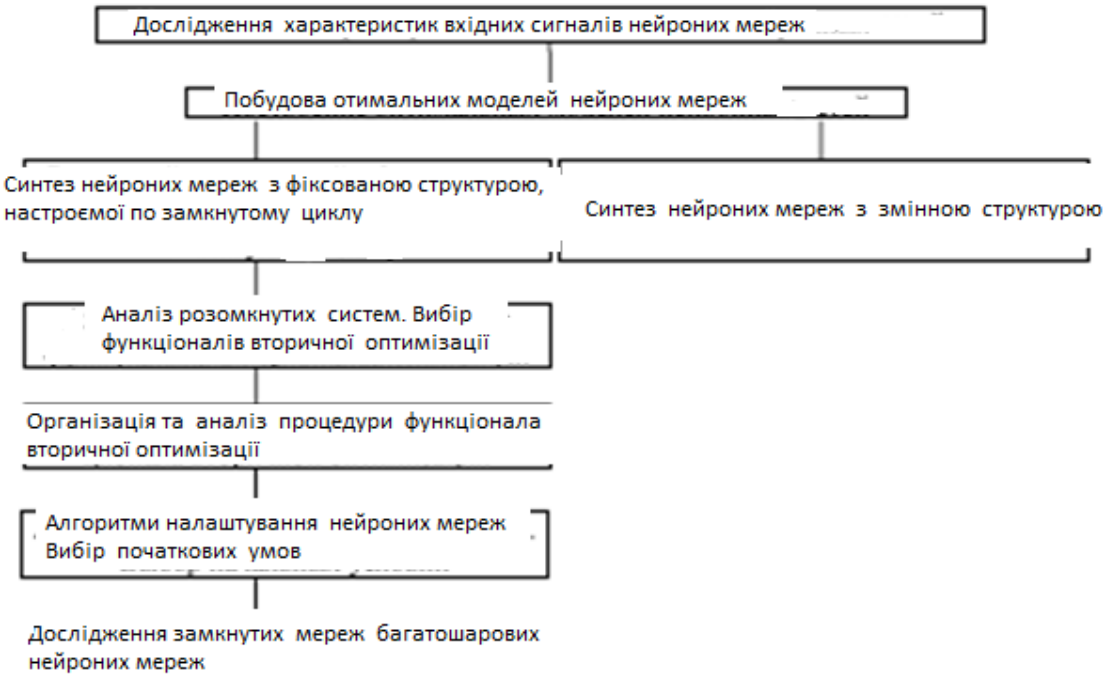

Рисунок 3.4 - Структура адаптації нейромережевої моделі до умов завдання

Специфічні вимоги прикладних задач визначали деякі особливості структур НСМ, є об'єктом управління з допомогою специфічних алгоритмів настройки, представлених в [13]:

- Континуум числа класів, коли вказівка вчителя системи формується в вигляді не перериваного значення функції в деякому діапазоні зміни;

- Континуум рішень багатошарової нейронної мережі, що формується вибором континуальної функції активації нейрона останнього шару;

- Континуум числа ознак, що формується переходом в просторі ознак від уявлення вихідного сигналу у вигляді N-мірного вектора дійсних чисел до речової функції в деякому діапазоні зміни аргументу. Континуум числа ознак, як наслідок, вимагає специфічної програмної і апаратної реалізації нейронної мережі.

- Континуум числа нейронів в шарі. Реалізація багатошарових нейронних мереж з континуумом класів і рішень проводиться вибором

відповідних видів функцій активації нейронів останнього шару. Варіант континууму ознак вхідного простору був реалізований в задачі розпізнавання періодичних сигналів без перетворення їх з допомогою аналого-цифрового перетворювача на вході системи, і реалізацією аналого-цифровий багатошарової нейронної мережі [25].

При цьому основою зазначеної методології є особливості НСМ як логічного базису алгоритмів розв'язання складних задач. До таких особливостей відносяться:

- інваріантність методів синтезу нейронних мереж від розмірності простору ознак;

- можливість вибору структури нейронних мереж в значному діапазоні параметрів в залежності від складності та специфіки розв'язуваної задачі з метою досягнення необхідної якості рішення;

- адекватність поточним і перспективним технологіям мікроелектроніки;

- відмовостійкість в сенсі його неточного, але не катастрофічного зміни якості виконання завдання в залежності від числа що вийшли з ладу елементів.

Відзначимо, що останні дві особливості НСМ актуальні тільки в разі апаратної реалізації нейромережевої системи розпізнавання.

Імовірнісна модель світу, взята за основу при побудові алгоритмів адаптації в багатошарових нейронних мережах, дозволила формувати критерій первинної оптимізації в розглянутих системах у вигляді вимог мінімуму середньої функції ризику і його модифікацій [5]:

- максимум апостеріорної ймовірності;

- мінімум середньої функції ризику;

- мінімум середньої функції ризику за умови рівності умовних функцій ризику для різних класів;

- мінімум середньої функції ризику за умови заданого значення

умовної функції ризику для одного з класів;

- інші критерії первинної оптимізації, що випливають з вимог конкретної практичної задачі.

У роботах [13] були представлені модифікації алгоритмів настройки багатошарових нейронних мереж для зазначених вище критеріїв первинної оптимізації. Відзначимо, що в переважній більшості робіт в області теорії нейронних мереж і в алгоритмах зворотного поширення розглядається найпростіший критерій - мінімуму середньоквадратичної помилки без яких би то не було обмежень на умовні функції ризику.

У режимі самонавчання (кластеризації) передумовою формування критерію та функціоналу первинної оптимізації нейронних мереж є подання функції розподілу вхідного сигналу у вигляді многомодальним функції в багатовимірному просторі ознак, де кожної моді з певною ймовірністю відповідає клас.

В якості критеріїв первинної оптимізації в режимі самонавчання (кластеризації) використовувалися модифікації середньої функції ризику. У роботах [13] представлені вище модифікації критеріїв первинної оптимізації були узагальнені на випадки:

- континууму класів і рішень,

- континууму ознак вхідного простору,

- континууму числа нейронів в шарі, при довільній кваліфікації вчителя.

Важливим розділом формування критерію та функціоналу первинної оптимізації в багатошарових нейронних мережах при ймовірнісної моделі світу є вибір матриці втрат, яка в теорії статистичних рішень визначає коефіцієнт втрат l_{12} при помилковому віднесення образів 1-го класу до 2-го, і коефіцієнт втрат l_{21} при віднесенні образів 2-го класу до 1-му.

Як правило, за замовчуванням матриця L цих коефіцієнтів при синтезі алгоритмів настройки багатошарових нейронних мереж, в тому

числі і при застосуванні методу зворотного поширення, приймається симетричною, тобто $l_{12} = l_{21}$. На практиці це не відповідає дійсності. Характерним прикладом є система аутентифікації користувача на підставі відбитків пальців. У цьому випадку втрати при помилковому віднесення вхідного образу до класу нелегітимних користувачів рівнозначно деякої невеликої втрати часу при вході в систему. У той же час втрати, пов'язані з помилковим віднесенням нелегітимного користувача до легітимним пов'язані з реалізацією вторгнення в захищається систему і можуть привести до значних втрат.

Розглянемо процес визначення критерію оптимізації параметрів СНС, призначеної для оцінки інформативності біометричних образів, які характеризуються геометричними параметрами.

У загальному випадку вирішальним критерієм інформативності в задачі розпізнавання образів є величина втрат від помилок R. Однак суттєвою перешкодою для використання R є той факт, що навіть у разі відомої функції розподілу генеральної сукупності, обчислення втрат пов'язано з дуже великими обчислювальними витратами.

У зв'язку з цим доцільно визначити критерії, більш просто обчислювані і разом з тим жорстко, якщо не однозначно, корельовані з оцінкою втрат R. Якщо розподіл реалізацій кожного образу підпорядковується нормальному закону з діагональними матрицями ковариаций (при цьому поверхні рівної щільності є сфери однакового радіуса), то мірою труднощі розпізнавання D, обернено пропорційній очікуваним втрат, може служити середнє значення евклидова відстані між математичними очікуваннями всіх пар образів:

$$D = \frac{1}{C_k^2} \sum_{i,j}^{k} \rho(i, j) \qquad (3.14)$$

де $\rho(i, j)$ - евклідова відстань між математичними очікуваннями і-го і j-го образів.

У термінах теорії інформації мірою труднощі розпізнавання служить ентропія H розподілів щільності ймовірності образів.

Нехай розподілу k образів спроектовані на одну вісь x, що вимірюється за точністю до t градацій. Ймовірність влучення реалізацій і-го образу в j-ую градацію дорівнює. Ілюстрацією зазначеної залежності є рис. 3.4.

Підсумувавши для j -ої градації ймовірності всіх k образів, отримаємо:

$$P_j = \sum_{i=1}^{k} P(j/i) \tag{3.15}$$

Вклад і-го образа в эту сумму равен

$$r_i = P(j/i)P_j \tag{3.16}$$

Тому ентропія j-ой градації виражається наступним значенням:

$$H_j = -(r_1 \lg r_1 + r_2 \lg r_2 + \ldots + r_i \lg r_i + \ldots + r_k \lg r_k) \tag{3.17}$$

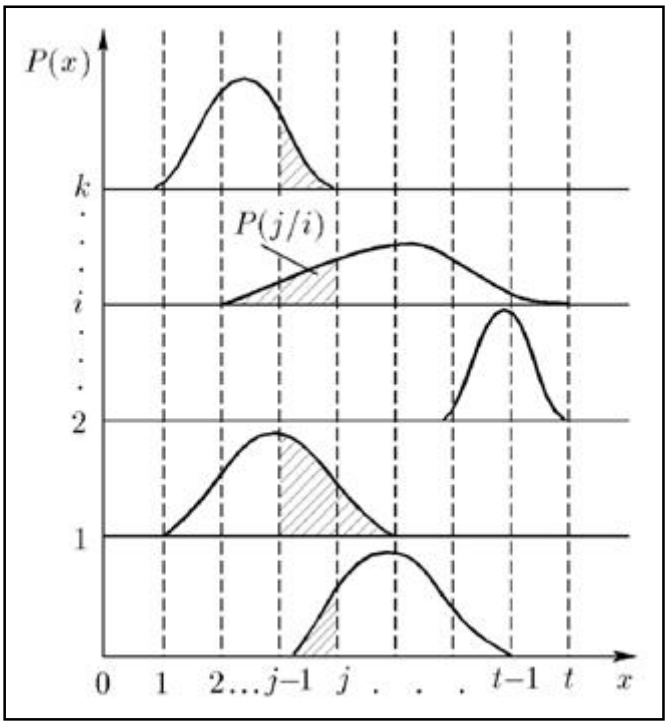

Рисунок 3.4 - Графік залежності ймовірності класифікації образів від точності вимірювання

З принципу адитивності ентропії випливає, що загальна невизначеність при розпізнаванні образів за ознакою x має вигляд:

$$H_x = \sum_{j=1}^{t} H_j P_j \qquad (3.18).$$

Якщо вихідна невизначеність ситуації дорівнювала $\lg k$, то відповідно до (3.18) кількість інформації l_x, одержуваної в результаті вимірювання ознаки x, так само $H_0 - H_x$.

Слід зауважити, що в реальних задачах закони розподілів реалізацій образів не відомі, обсяг навчальної вибірки часто буває невеликим. Тому проводити оцінку параметрів моделей розподілів, а по ним оцінку інформативності, практично неможливо. Практичний досвід і результати [6] вказують на те, що в цих умовах в якості критерію інформативності доцільно використовувати помилку розпізнавання НСМ навчальних

прикладів з тестової вибірки. Це дозволяє використовувати зазначену помилку розпізнавання в якості базису для формування критерію адаптації параметрів НСМ до умов завдання оцінки інформативності біометричних образів

Отриманий загальний перелік адаптуються параметрів НСМ і обгрунтований критерій адаптації дозволив перейти до наступного етапу розробки підходу до адаптації СНС.

Базуючись на показаних на рис. 3.1, 3.2 типових структурах СНС, з урахуванням результатів п. 3.1 та даних теоретичних робіт [12, 15], визначено, що основними структурними параметрами даного типу НСМ є:

- Кількість вхідних нейронів - L_{in}.

- Кількість вихідних нейронів - L_{out}.

- Кількість нейронів в повнозв'язну шарі - L_f.

- Кількість згортальних шарів - K_{ls}.

- Кількість карт ознак в кожному згорнутої шарі - $K_{h,k}, k \in \lfloor 1, K_{ls} \rfloor$.

- Кількість шарів підвибірки (Субдіскретізація) - K_{ld}.

- Коефіцієнт масштабування для кожного шару підвибірки (Субдіскретізація) - $m_k, k \in \lfloor 1, K_{ld} \rfloor$.

- Розмір ядра згортки для кожного k-го згорнутого шару $(b \times b)_k, k \in \lfloor 1, K_{ls} \rfloor$.

- Зсув рецептивного поля при виконанні кожної k-ой процедури згортки $d_k, k \in \lfloor 1, K_{ls} \rfloor$. Принято, що $d_k = d = 1$.

- Розмір карти ознак для кожного k-го згорнутого шару - $(a \times a)_k, k \in \lfloor 1, K_{ls} \rfloor$. При цьому:

$$a_k = a_{k-1} - b_k + 1 \tag{3.19}$$

Структура зв'язків між сусідніми шарами згортки. Цю структуру можна представити у вигляді матриці:

$$\boldsymbol{Q_{i,i+1}} = \begin{Vmatrix} q_{(i,1),(i+1,1)} & \cdots & q_{(i,1),(i+1,j)} \\ \cdots & \cdots & \cdots \\ q_{(i,G),(i+1,1)} & \cdots & q_{(i,G),(i+1,J)} \end{Vmatrix} \quad (3.20)$$

де $Q_{i,i+1}$- матриця, компоненти якої визначають наявність зв'язків між і-им і (i + 1) -им прихованими шарами, $q_{(i,g),(i+1,j)}$- компонент, який вказує на наявність / відсутність зв'язку між g-ой картою і-го шару і j-ой картою (i + 1) -го шару,G - кількість карт в і-му шарі,

J - кількість карт в (i + 1) -му шарі.При цьому $q_{(i,g),(i+1,j)} = 1$, якщо зв'язок між g-ой картою і-го шару і j-ой картою (i + 1) -го шару є, $q_{(i,g),(i+1,j)} = 0$, якщо зв'язку між g-ой картою і-го шару і j-ой картою (i + 1) -го шару немає.

Відповідно до загальноприйнятої концепцією ієрархічного розпізнавання образів згорнутої нейронною мережею багаторазове використання згортальних шарів відповідає ієрархічним розпізнаванню значущих ознак, а використання шарів підвибірки адаптує процес розпізнавання до можливої зміни масштабу зазначених ознак.

З урахуванням необхідності мінімізації помилки розпізнавання модель оптимізації структурних параметрів СНС можна записати за допомогою виразу:

$$\Delta\left(L_{in}, L_{out}, L_f, K_{ls}, K_{h,k}, K_{ld}, m_{ld}, b_k, \boldsymbol{Q}_{K_{ls}}\right) \rightarrow \min \quad (3.21)$$

де Δ - помилка розпізнавання,

$\boldsymbol{Q}_{K_{ls}}$ – вектор, що складається з матриць $\boldsymbol{Q_{i,i+1}}$, які визначають зв'язки між сусідніми прихованими шарами нейронів.

Відсутність у формулі (3.21) інших структурних параметрів згорнутої нейронної мережі пояснюється тим, що вони є похідними від

використовуваних компонентів цього виразу.

В основу адаптації перерахованих структурних параметрів покладено підхід - в системах біометричної аутентифікації процес розпізнавання СНС двомірного зображення біометричного способу користувача повинен бути максимально наближений до свого біологічного прототипу. Під біологічним прототипом мається на увазі процес розпізнавання середньостатистичним користувачем геометричних параметрів даного біометричного способу, відображається на моніторі комп'ютера, який має середні характеристики.

Синтез сформульованого підходу до загальноприйнятої концепцією функціонування СНС і особливостями системи біометричної аутентифікації користувачів на підставі аналізу двомірної геометрії їх біометричних образів дозволив сформулювати наступну групу принципів, що визначають напрямки оптимізації:

Принцип 1. Кількість згортальних шарів має дорівнювати кількості рівнів розпізнавання двомірного зображення біометричного способу среднестатітіческім користувачем.

Принцип 2. Кількість карт ознак у n-му згорнутої шарі має дорівнювати кількості ознак на n-му рівні розпізнавання.

Принцип 3. Карта ознак в n-го шару, відповідна j-му ознакою розпізнавання (j-ой, яка розпізнається геометричної фігури) зв'язується тільки з тими картами ознак попереднього шару, які використовуються для побудови зазначеної фігури.

Принцип 4. Розмір ядра згортки для n-го згорнутого шару повинен бути дорівнює розміру розпізнаються ознак на n-му ієрархічному рівні.

Відзначимо, що четвертий принцип передбачає принципову можливість зміни розміру ядер згортки, що дещо не відповідає відомим структурам СНС [13]. У цих мережах розмір ядра згортки для карт ознак постійний для всіх верств. При цьому ієрархія вилучення ознак

реалізується двома різними способами. Суть першого методу полягає в тому, що наступний рівень ознак витягується після застосування операції Субдіскретізація [23].

Другий спосіб передбачає використання такого кроку ядра згортки, який зменшує попередню карту ознак в 2 рази. Таким чином, запропонований принцип не суперечить відомій методології побудови структури згорнутої нейронної мережі, а дозволяє збільшити її гнучкість.

Разом з тим, рекомендації [12] дозволяють прийняти такі обмеження на процес введення і попередньої обробки двомірного зображення (біометричного способу) в системі біометричної аутентифікації:

1. У системі аутентифікації використовується відеокамера з роздільною здатністю 1920x1080 пікселів. В даний час відеокамери з такими характеристиками мають досить велике поширення в сучасних універсальних комп'ютерних системах.

2. Зображення, що розпізнається має чорно-білий формат. Це обмеження прийнято з позицій спрощення процесу попередньої обробки графічної інформації перед її подачею в систему розпізнавання. Тому геометрія біометричного способу має бінарне представлення.

3. Максимальний розмір розпізнається зображення дорівнює вирішенню відеокамери, а мінімальний 30x30 пікселів.

4. Перед подачею в СНС мережу зображення піддається попередній обробці, яка полягає в їх масштабування, центрування і обрізку.

Вибір зазначених параметрів реалізований, виходячи з позицій ергономіки. Відзначимо, що параметри даного обмеження мають приблизний характер і обрані в результаті аналізу [11] і власного практичного досвіду. Згодом вони можуть бути змінені шляхом врахування особливостей системи аутентифікації.

3.3. Метод адаптації структурних параметрів згорнутої нейронної мережі до умов завдання оцінки інформативності образів підпису

Інтеграція загальнозастосованої методології побудови нейромережевих систем розпізнавання підпису [12], сформованих принципів оптимізації з певними обмеженнями на процес введення і попередньої обробки зображень в системі біометричної аутентифікації дозволила запропонувати метод оптимізації параметрів СНС. Реалізація запропонованого методу передбачає виконання 7 етапів.

Укрупнення блок-схема алгоритму розробленого методу представлена на рис. 3.5.

Рисунок 3.5 - Укрупнення блок-схема алгоритму адаптації структурних параметрів згорнутої нейронної мережі

Етап 1. Визначити безліч вихідних параметрів мережі. Для цього необхідно встановити відповідність між безліччю розпізнаються користувачів і вихідними нейронами мережі. Таким чином, кількість вихідних нейронів відповідає потужності безлічі розпізнаються користувачів.

Етап 2. Визначити безліч вхідних параметрів мережі. Для цього слід розрахувати розміри зображень, що подаються для розпізнавання, а також

встановити відповідність між окремими елементами зображень і вхідними нейронами. Також необхідно врахувати розмір зображень, відповідних біометричних образів користувачів в доступних базах даних, які застосовуються для навчання мережі. Якщо розмір зображень доступних навчальних вибірок відрізняється від розпізнаються, то їх слід масштабувати.

Етап 3. Базуючись на першому і другому принципах, використовуючи геометричні характеристики еталонів розпізнаються зображень, методом експертного оцінювання визначити кількість згортальних шарів і кількість карт ознак в кожному згорнутої шарі.

Етап 4. Базуючись на третьому принципі методом експертного оцінювання визначити структуру зв'язків між сусідніми картами ознак.

Етап 5. Виходячи з вимог точності і ресурсоємності розпізнавання методом експертного оцінювання визначити наявність і параметри шарів Субдіскретізація.

Етап 6. Базуючись на четвертому принципі, з урахуванням необхідності згортки зображення до вектору ознак визначити розмір ядра і кроку переміщення згортки для кожного рівня розпізнавання. Також на цьому етапі розраховуються розміри карт ознак для кожного згорнутого шару.

Етап 7. Базуючись на методі визначення кількості прихованих нейронів в багатошаровому персептрона [26], визначити кількість нейронів в повнозв'язну шарі.

У загальному випадку з урахуванням (3.21) перетворення інформації, що реалізовується запропонованим методом, можна припустити за допомогою таких висловів:

$$\begin{aligned}&\left\langle \boldsymbol{U}, K_U, \boldsymbol{T}, \boldsymbol{S}_{db}^{\boldsymbol{T}}, \boldsymbol{E}, \boldsymbol{R}, \Delta_r, \boldsymbol{DB}, t \right\rangle \rightarrow \\ &\left\langle \overline{L}_{in}, \overline{L}_{out}, \overline{L}_f, \overline{K}_{ls}, \overline{K}_{h,k}, \overline{K}_{ld}, \overline{m}_{ld}, \overline{b}_k, \overline{\boldsymbol{Q}}_{K_{ls}} \right\rangle,\end{aligned} \tag{3.22}$$

$$\mathbf{T} = \{T_1, T_{27}\}, \tag{3.23}$$

$$\boldsymbol{DB} = \{DB(T_1), DB(T_2), DB(T_3), DB(T_4), DB(T_5), DB(T_6), DB(T_7)\}. \tag{3.24}$$

де $\boldsymbol{U}$ - безліч зображень, що характеризують легітимних користувачів; K_U - кількість розпізнаваних користувачів; $\boldsymbol{T}$ - безліч типів біометричних образів, які характеризуються геометричними параметрами;

$\boldsymbol{S}_{db}^{T} = (a \times b)_{db}^{T}$ - розмір зображення біометричних образів, в доступних базах даних; $\boldsymbol{E}$ - безліч експертних даних, що використовуються для визначення параметрів СНС;

$\boldsymbol{R}$ - безліч доступних обчислювальних ресурсів; Δ_r - требуемая точность распознавания;

T_1 - біометричний образ, відповідний папілярних ліній;

T_2 - біометричний образ, відповідний рукописному почерку;

t – тип розпізнається біометричного способу ($t \in \boldsymbol{T}$);

$\boldsymbol{DB}$ - безліч доступних баз даних, які можливо використовувати для формування навчальної вибірки;

$DB(T_t)$ - доступна база даних, яку можливо використовувати для формування навчальної вибірки для t-го типу образів підпису; $\left\langle \overline{L}_{in}, \overline{L}_{out}, \overline{L}_f, \overline{K}_{ls}, \overline{K}_{h,k}, \overline{K}_{ld}, \overline{m}_{ld}, \overline{b}_k, \overline{\boldsymbol{Q}}_{K_{ls}} \right\rangle$ - кортеж адаптованих параметрів СНС.

З урахуванням виразів (3.22, 3.23) етапи запропонованого методу деталізовані наступним чином:

Етап 1 - визначення вихідних параметрів мережі. Вхідними даними етапу є - $\boldsymbol{U}$ та K_U. Відповідно до [23] кількість вихідних нейронів СНС приймаємо на одиницю більше ніж K_U. При цьому для вихідних нейронів

з номерами від 1 до K_U, номер нейрона дорівнює номеру легітимного користувача. Вихідний нейрон з номером $(K_U + 1)$ відповідає нелегітимність користувачеві. Таким чином вихід даного етапу визначається виразом:

$$\overline{L}_{out} = K_U + 1 \tag{3.25}$$

Етап 2 - визначення вхідних параметрів мережі. Вхідними даними етапу є - $S_r, \boldsymbol{S}_{db}^{\boldsymbol{T}}, \boldsymbol{DB}, t$, Виходом етапу є. Етап розділений на 2 етапи:

Крок 1 - підбір бази даних, яку доцільно використовувати для формування навчальної вибірки при розпізнаванні t-го виду біометричного способу:

$$DB_t = \boldsymbol{DB}(t = T_t) \tag{3.26}$$

Крок 2 - визначення кількості вхідних нейронів. Для цього використовується вираз

$$\overline{L}_{in} = (a \times b)_{db}^{t} \tag{3.27}$$

Етап 3 - визначення параметрів згортальних шарів. Вхідні дані етапу - $\boldsymbol{E}, \boldsymbol{DB}, t$. Вихід етапу - $\overline{K}_{ls}, \overline{K}_{h,k}$. Етап розділений на 3 етапи:

Крок 1 - визначення еталонних зображень, які призначені для експертного аналізу:

$$\boldsymbol{DB}(t = T_t) \rightarrow \{e_t\} \tag{3.28}$$

де $\{e_t\}$- безліч еталонів зображень t-го виду способу підпису.

Крок 2 - визначення кількості згортальних шарів, яке відповідно до принципу 1 реалізується за допомогою експертного оцінювання кількості рівнів розпізнавання:

$$F(\boldsymbol{E}, \{e_t\}) = K_{rl} \tag{3.29}$$

де F - процедура експертного оцінювання, описана в [27],

K_{rl} - кількість рівнів розпізнавання $\overline{K}_{ls} = K_{rl}$.

Крок 3 - визначення кількості карт ознак, яке відповідно до принципу 2 реалізується за допомогою експертного оцінювання кількості ознак на кожному рівні розпізнавання:

$$\boldsymbol{K}_a = F\left(\boldsymbol{E}, \{e_t\}, \overline{K}_{ls}\right) \tag{3.30}$$

де $\boldsymbol{K}_a = \left\{K_{a,k}\right\}_{\overline{K}_{ls}}$ - вектор, елементи якого дорівнюють кількості ознак на кожному рівні розпізнавання. $K_{a,k}$ - кількість ознак на k-му рівні розпізнавання підпису $\overline{K}_{h,k} = K_{a,k}$.

Етап 4 - визначення зв'язків. Вхідні дані етапу - $\boldsymbol{E}, \{e_t\}, \overline{K}_{ls}, \overline{K}_{h,k}$. Вихід етапу - $\overline{\boldsymbol{Q}}_{K_{ls}}$. Реалізація етапу полягає в експертному оцінюванні номенклатури ознак (i-1) -го рівня, які застосовуються для розпізнавання ознак і-го рівня. В аналітичному вигляді перетворення інформації на даному етапі записується так:

$$\boldsymbol{Q}_{K_{ls}} = F\left(\boldsymbol{E}, \{e_t\}, \overline{K}_{ls}, \overline{K}_{h,k}\right) \tag{3.31}$$

Етап 5 - визначення параметрів шарів Субдіскретізація. Вхідні дані етапу - $\boldsymbol{E}, \overline{K}_{ls}, \overline{K}_{h,k}, \boldsymbol{R}, \Delta_r$, а вихід - $\overline{K}_{ld}, \overline{m}_{ld}$. За аналогією з третім і четвертим етапом використовується процедура експертного оцінювання:

$$\left\{\overline{K}_{ld}, \overline{m}_{ld}\right\} = F\left(\boldsymbol{E}, \overline{K}_{ls}, \overline{K}_{h,k}, \boldsymbol{R}, \Delta_r\right) \tag{3.32}$$

Етап 6 - визначення параметрів ядер згортки. Вхідні дані етапу - $(a \times b)^{t}_{db}, \overline{K}_{ls}, \overline{K}_{ld}, \overline{m}_{ld}$, а вихід - $\overline{b}_k$. При відсутності шарів Субдіскретізація

($\overline{K}_{ld} = 0$)і за умови виконання загальноприйнятого умови $(a \times b)^{t}_{db} = (a \times a)^{t}_{db}$ для визначення $\overline{b}_k$ необхідно вирішити рекурентне співвідношення виду (3.33) з урахуванням обмежень (3.34, 3.35):

$$b_k = a_{k-1} + 1 - a_k,\ k = 1...\overline{K}_{ls}, \tag{3.33}$$

$$a_1 = (a \times a)^{t}_{db}, \tag{3.34}$$

$$a_{\overline{K}_{ls}} = 1. \tag{3.35}$$

При $\overline{K}_{ld} \neq 0$ на процес визначення $\overline{b}_k$ накладається додаткове обмеження, кожен прихований шар з парним номером зменшується щодо попереднього прихованого шару в $\overline{m}_{ld}$ раз.

Етап 7 - визначення кількості нейронів в повнозв'язну шарі. Вхідні дані етапу - $\overline{L}_{in}, \overline{L}_{out}, \overline{K}_{ls}, \overline{K}_{h,k}, \overline{K}_{ld}, \overline{m}_{ld}, \overline{b}_k$, а виход - $\overline{L}_f$. Відповідно до [20] діапазон значень $\overline{L}_f$ визначається виразом:

$$\left(2\overline{L}_{in} + \overline{L}_{out}\right) \le \overline{L}_f \le K_p \tag{3.36}$$

де $\left(2\overline{L}_{in} + \overline{L}_{out}\right)$ - мінімальна кількість прихованих нейронів, яке визначається з теореми Хехт-Нільсена [28]. $K_p = f\left(\overline{L}_{in}, \overline{L}_{out}, \overline{K}_{ls}, \overline{K}_{h,k}, \overline{K}_{ld}, \overline{m}_{ld}, \overline{b}_k\right)$- кількість параметрів вагових коефіцієнтів в СНС. Відзначимо, що при реалізації третього, четвертого і п'ятого етапів запропонованого методу використовується процедура експертного ранжирування альтернатив. Виконання зазначеної процедури передбачає, що М експертів ранжирують N можливих альтернатив.

Мається на увазі, що кожен з експертів виставляє ранги для кожної з альтернатив

$$\begin{array}{ccccc} x_{1,1}, & \dots & x_{n,1} & \dots & x_{N,1} \\ \dots & \dots & \dots & \dots & \dots \\ x_{1,m} & \dots & x_{n,m} & \dots & x_{N,m}, \\ \dots & \dots & \dots & \dots & \dots \\ x_{1,M} & \dots & x_{n,M} & \dots & x_{N,M} \end{array} \qquad (3.37)$$

де $x_{n,m}$ – ранг n-ї ознаки, виставлений m-им експертом.

Надалі ця інформація підлягає наступній обробці. Спочатку визначається колективна оцінка n-го ознаки:

$$y_n = \sum_{m=1}^{M} x_{n,m} \qquad (3.38)$$

де $x_{n,m}$ – ранг n-ї ознаки, виставлений m-им експертом, n = 1 ... N.

Далі отриманий ряд даних сортується в порядку зростання. Ознака, якому відповідав би мінімальне значення (3.38) вважається найбільш значущим, а ознака з максимальним значенням - найменш значущим.

Для перевірки узгодженості думок експертів і оцінювання статистичної значущості ранжування застосовуються вирази:

$$K_0 = \frac{12L}{m^2\left(n^3 - n\right)}, \qquad (3.39)$$

$$if\ K_0 > 0{,}5 \Rightarrow погляди\ експертів\ узгоджені, \qquad (3.40)$$

$$L = \sum_{n=1}^{N} (y_n - y_{cp})^2, \qquad (3.41)$$

$$y_{cp} = 0{,}5m(n+1), \qquad (3.42)$$

$$X_r = m(n-1)K_0. \qquad (3.43)$$

Відомо, що величина має χ^2 розподіл с $(n-1)$ ступенем свободи [6]. З таблиць розподілу χ^2 , за значеннями і знаходимо $X_{кр}$.

Ранжировка вважається статистично значущою, якщо виконується умова:

$$X_r \geq X_{кр} \qquad (3.44)$$

Якщо думки експертів не узгоджені, то процедуру ранжирування необхідно повторити, помінявши експертів або надавши їм додаткову інформацію про ранжируваних альтернативи.

Висновки по третьому розділу

В даному розділі вирішувалася наукова задача розробки нейромережевих моделей і методів оцінки інформативності образів підписи, які характеризуються геометричними параметрами. Основні результати розділу наступні:

Отримала подальший розвиток нейромережева модель оцінки інформативності образів підпису, яка за рахунок теоретично обгрунтованого вибору виду нейронної мережі, забезпечує можливість ефективної оцінки інформативності, яка визначається на підставі точності розпізнавання.

Вперше запропоновано принципи адаптації структурних параметрів згорнутої нейронної мережі до умов завдання оцінки інформативності біометричних образів, що забезпечують можливість розробки ефективного методу оцінки інформативності. На відміну від відомих зазначені принципи реалізують підхід - в системах біометричної аутентифікації процес нейромережевого розпізнавання двомірного зображення

біометричного способу користувача повинен бути максимально наближений до свого біологічного прототипу.

Вперше розроблено метод адаптації структурних параметрів згорнутої нейронної мережі до умов завдання оцінки інформативності образів підпису, який за рахунок використання розробленої нейросетевой моделі, запропонованих принципів адаптації і розробленого критерію оцінки інформативності, дозволяє реалізувати ефективну оцінку інформативності.

РОЗДІЛ 4. РОЗРОБКА НЕЙРОМЕРЕЖЕВОЇ СИСТЕМИ РОЗПІЗНАВАННЯ ПІДПИСІВ КОРИСТУВАЧІ

4.1. Архітектура нейромережової системи

Архітектура запропонованої НСС СРК розроблена з позицій інтеграції рішень розробленого методу адаптації структурних параметрів згорткової нейронної мережі до умов завдання оцінки інформативності біометричних образів з рішеннями, застосовуваними в відомих нейромережевих системах біометричної аутентифікації. Запропонована структура системи оцінки інформативності образів підпису складається з 5 основних підсистем.

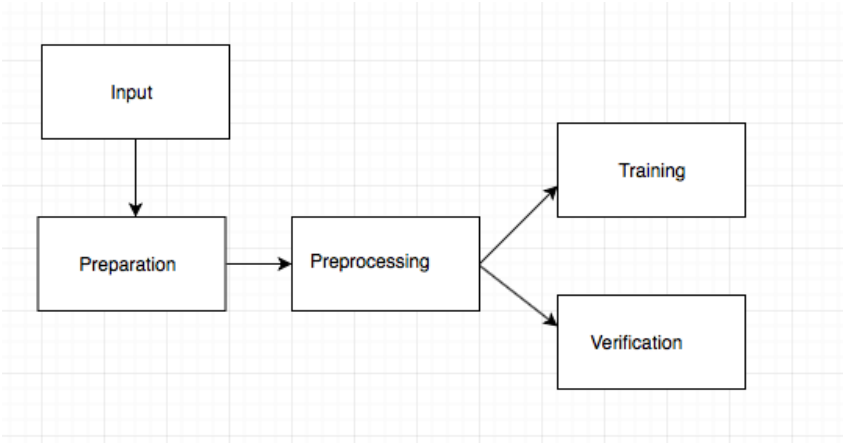

Рисунок 4.1 – Архітектура розробленої системи

Призначення підсистем:

– Input – підсистема, яка подає на вхід зображення підпису;

– Preparation - підсистема первинної обробки зображення;

– Preprocessing – підготовка зображення;

– Verification - підсистема розпізнавання підпису;

– Training - підсистема додавання нового підпису в базу та тренування моделі.

Підсистеми “Preparation” та “Preprocessing” включають в себе первинну обробку зображень, яка поділяється на декілька етапів. Метою цих етапів є підготовка підписів до вилучення об'єктів.

Обов’язковим кроком є бінаризація зображення. Вона дозволяє виявити фон та передній план зображення, а також прийти до двох кольорів та розмітити пікселі. Для вирішення даної проблеми використовувала пакет, мови програмування R, *imager*. Він дозволяє задати пороговість бінаризації числовими значеннями, або квантилями. Приклад обробки зображений на наступному рис. 4.2.

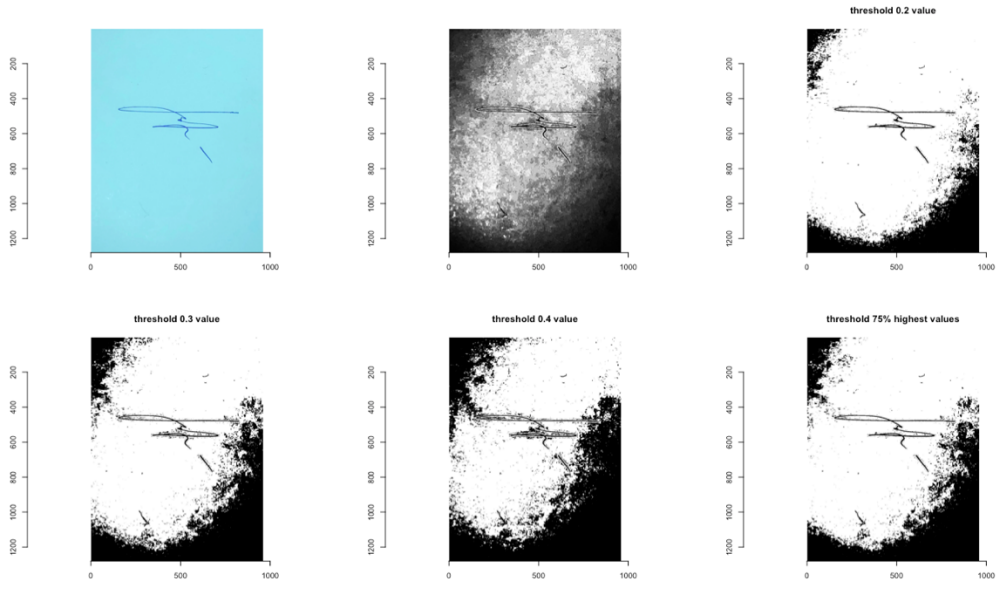

Рисунок 4.2 – Бінаризація зображеня

Наступним кроком є скелитизація зображення, а саме аналіз площі інформативних точок, що дозволяє також позбутися шумів. Існує декілька

методів:

- Шаблона скелетизація;

- Хвильовий метод;

- Алгоритм Зонга-Суня;

- Алгоритм Щепіна.

В роботі використовували перший метод, шаблонної скелетизації. Він базується на отримані шаблонів для подальшого видалення зайвих пікселів. Завжди центральний чорного кольору. Процедура ітерується до тих пір, поки не залишиться пікселів для видалення. На рис. 4.3 представлений вигляд шаблонів.

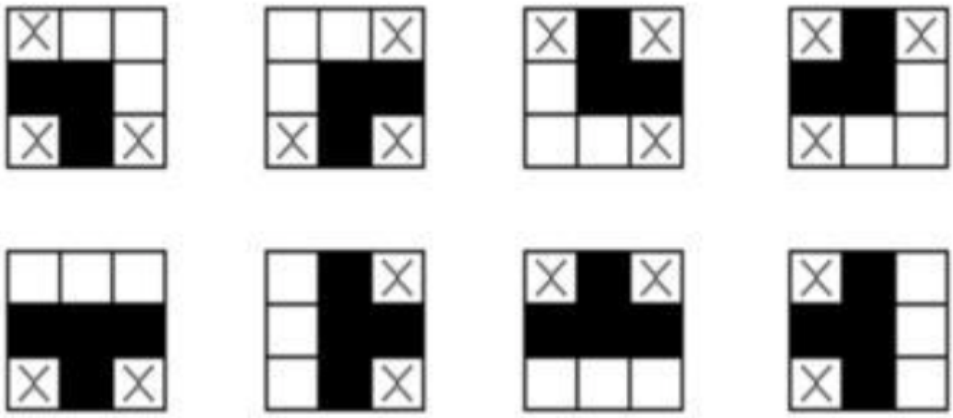

Рисунок 4.3 – Шаблони скелетизації

На рис. 4.3 клітинки з крестиками позначені неважливі пікселі.

Основні етапи скелетизації:

1. Для зберігання координат створюємо пустий стек.

2. Зберігаємо будь-яку точку скелета.

3. До тих пір поки стек не навповнений, виконуємо наступні кроки.

4. Обираємо точку зі стека.

5. Генерується ребра з обраної точкизображення до тих пір, поки не відбудеться відгалуження або кінець.

6. У випадку досягнення кінцевої точки або нового ребра, заносимо пройденний шлях.

7. У випадку розгалуження заносимо послідовність ребер. Та повертаємося до пункту 3.

Для вирішення даної задачі використовували пакет мови програмування Python, skimage.morfology. Також використовується зміна медіальної осі для обчислення ширини об'єктів на першому плані. Метод medial_axis віддає віддалене перетворення, крім медиальної осі. Тому можливо обчислити відстань до фону для всіх точок медиальної осі з цією функцією. Це дає оцінку локальної ширини об'єктів.

Медіальна вісь об'єкта - це сукупність усіх точок, що мають більше ніж одну найближчу точку на межі об'єкта. Його часто називають топологічним скелетом, тому що це 1-піксельний широкий скелет об'єкта, з тим же сполученням, що й вихідний об'єкт. Діла використовуємо функцію thin. Морфологічне розщеплення, що реалізується у даній функції, працює за тим же принципом, що і скелетінгу: видаляють пікселі з кордонів на кожній ітерації, доки жодна з них не може бути вилучена, не змінюючи зв'язність. Різні правила видалення можуть прискорити скелетонізацію і привести до різних кінцевих скелетів.

Функція thin також приймає аргумент ключового слова max_iter, щоб обмежити інтенсивність, таким чином, створювати відносно товстий скелет.

Підсистема “Preprocessing” включає в себе вторинну обробку зображень, зміна роміру вхідних зображень.

Особливості вилучення є ключем до розробки системи. Ми використовуємо набір із п'яти глобальних функцій, на які не може впливати тимчасовий зсув.

Ці особливості мають геометричні характеристики на основі форми та розмірів зображення підпису. Різні особливості форми, які ми використовуємо, є: кількість пікселів, горизонтальні та вертикальні центроїди підпису, співвідношення відстані між краями еліпса та

довжиною основної осі, міра плоскості розподілу, а також міра асиметрії розподілу. Під час процесу навчання вихід нейронної мережі порівнюється з цільовим значенням, а корекція ваги мережі через алгоритм навчання виконується таким чином, щоб мінімізувати функцію помилки між двома значеннями.

В даній роботі використали помилку MSE, яка намагається мінімізувати середню похибку між виходом мережі та цільовим значенням. Система перевірена на точність та ефективність в базі даних близько 100 підписів від 3 користувачів, що містять як справжніх, так і кваліфікованих підроблених аналогів зразків підписів. Наша база даних складається з підписів, виконаних з різними ручками з різними кольорами.

Всі зразки нашої бази даних були попередньо оброблені, а глобальні функції були вилучені.

Після вилучення функцій, тестування виконується, і результат відображається, а порогові значення було зроблено на 90% у дослідженні, яке нижче відсотка на 90%, підпис вважається підробленим.

Наступна підсистема “Training”. Включає в себе саме побудову навчання та тестування нейронної мережі. Розмір ядра конвекторальної нейронної мережі визначає кількість ознак, які будуть об'єднані для отримання нової ознаки на виході. В роботі задали 5 * 5 = 25 ознак на вході і 3 * 3 = 9 ознак на виході. Для стандартного шару ми мали б масову матрицю 25 * 9 = 225 параметрів, а кожна вихідна ознака була б сумою суми всіх ознак на вході. Кожна ознака на виході отримується аналізом не кожної ознаки на вході, а лише одного вхідного, що знаходиться в "приблизно в тому ж місці".

4.2. Тестування системи

Експеримент проводився таким чином:

1. Вводились підписи, збережені в папці train, яка містить копії зображень с аутентичними підписами (9 зображення).

2. Виконання обробки зображень та виділення ознак підписів.

3. Виконали навчання з навчальним зображенням за допомогою нейронної мережі.

4. Верифікація тестового підпису нейронною мережею.

Нейронна мережа в цьому експерименті мала два прихованих шари: в першому прихованим шаром було в цілому понад 800 нейронів, у другому - 200 прихованих нейронів. Останній шар, що називається «SoftMax», виконує власне класифікацію векторів ознак. Далі опис екранових форм програми.

В режимі попереднього навчання (тренування) відкривається вікно в якому відображається структура мережі Автоэнкодера з кодеромі Декодер, а також кількість нейронів в першому шарі (Кодер). Фінально, після всіх попередніх обробок, зображення test1, test2 і test3 стали розміром 80x80 з відображуваними лініями на білому та чорному фоні.

Після цього виконали перевірку підпису test1, test2 та test3 по даним попередньої обробки. Перевірка цих підписів виконується після вибору папки з даними. В результаті показується відповідність тестових підписей test1, test2 та test3, на яких навчалася нейронна мережа. В цьому експерименті отримали наступні результати: для тесту 1 - 52,84% зіставлення в порівнянні з підписами, які подавался на навчання нейронної мережі, для test2 - 68,22%, а для test3 - 55,47%. Відповідно до результатів, отриманих в експерименті для тесту 1,

тесту 2 і тесту 3, нейронна мережа успішно класифікувала тестові підписи, так як значення параметра схожості при ідентифікації справжніх

підписів у більшості перевищили значення 50%, а для підроблених підписів вони були значно нижче цього 50%.

Також було проведено додаткове поповнення бази для покращення розпізнавання для трьох тестових зображень підписів (test1, test2, test3), але з великим числом нейронів прихованих шарів 1600 і 900. В результаті отримали наступні точності розпізнавання: тест 1- 77,10%, тест 2- 69,48%, тест 3 - 66,07%. Це дослідження показало, що, збільшуючи кількість нейронів мережі, можна отримати збільшення відсотка подібного поточного підпису та шаблону, отриманого при навчанні системи.

Після тестування правильного підпису кожного автора, де були отримані хороші відсотки подібності з відповідним автором шаблону. Проведено ще одне тестування з підробленими підписами, які дало наступні результати: test1 - 23,66%, тест2 - 15,56%, тест3 - 22,48%. Тут порог розпізнавання в 50% не був досягнутий, тому система відповіла, що введені підписи не розпізнаються.

ВИСНОВКИ

Розпізнавання підписів можна здійснити при використанні різних математичних методів: застосування методів нечіткої логіки, методу потенційних функцій, класифікації на основі порівняння з еталонами, а також з допомогою нейронних мереж. Показано також, що використання методу розпізнавання за допомогою нейронних мереж відрізняється більш високою ефективністю і продуктивність, але для нього потрібна або велика кількість прикладів при проведенні навчання,

або створення спеціальних структур нейронних мереж, які враховують специфіку даних задач.

Висока продуктивність методів з використанням нейронної мережі в задачах обробки та аналізу рукописних підписів дає можливість використовувати його в вирішенні проблем розпізнавання та верифікації рукописних підписеів. Можливість постійного навчання та узагальнення яка володіє методом нейронних мереж, дає можливість ефективно вирішити проблему різноманіття та мінливості рукописного підпису.

Після проведення першого навчання нейронної мережі прийняття рішення про справжність підписів, поданих на вхід в систему, відбувається з великою швидкістю, що виявляється важливим фактором для систем, які мають велику базу даних підписів.

Розроблений метод також дозволяє поповнювати базу новими підписами та доповнювати вже вже існуючі підписи в базі. Також використання згорткових нейронних мереж дозволило підвищити швидкодію та точність розпізнавання підписів користувачів. Саме цей алгоритм був використаний в даній роботі. У відповідності до цілі магістерської дисертації розроблена система розпізнавання підписів. При розробці цієї системи були вирішені наступні завдання:

- Обрано алгоритм розпізнавання підписів користувачів;
- Розроблена модель попередньої обробки зображення;
- Програмна реалізація методу розпізнавання підписів користувачів;
- Тестування системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Сойфер,В.А. Компьютерная обработка изображений –Соросовский образовательный журнал.1996. № 3.

2. Дорошенко Т.Ю., Костюченко Е.Ю. (2014). «Система аутентификации на основе динамики рукописной подписи». Доклады ТУСУРа, № 2 (32).

3. Faundez-Zanuy, Marcos (2007). «On-line signature recognition based on VQ-DTW». Pattern recognition 40 (3): 856-897.

4.Image Processing Techniques For Machine Vision [online]. Available: http://www.eng.fiu.edu/me/robotics/elib/am_st_fiu_ppr_2000.pdf

5. M. M. Lange, S.N. Ganebnykh (2005). «Classification of 2D Grayscale Objects in a Space of the Multiresolution Representation».

6.Казаков П.В. Распознавания графического образа личной подписи на основе искусственных нейронных сетей ,2012 год. – 36 с.

7.Сойфер,В.А. Компьютерная обработка изображений –Соросовский образовательный журнал.1996. № 3.

8. Э.С.Анисимова(2014).«[http://crm.ics.org.ru/uploads/crmissues/crm_2014_3/14302.pdf Идентификация онлайн-подписи с помощью оконного преобразования Фурье и радиального базиса]». КОМПЬЮТЕРНЫЕ ИССЛЕДОВАНИЯ И МОДЕЛИРОВАНИЕ Т. 6 № 3 С. 145–278.

9. NALWA,S.V(1997).«Automatic On-Line Signature Verification». PROCEEDINGS OF THE IEEE, VOL. 85, NO. 2.

10. Александр Прохоров (2000). «Мой дом - моя крепость, мое лицо - мой пропуск». КомпьютерПресс 7.

11. Алгоритмы оффлайн-распознавания рукописных цифр – выпускная квалификационная работа/К.В Дмитриевич –2013-89 с.

12. Колядин Д.В., Петров И.Б. (2005). «Алгоритм выделения экстремальных точек применительно к задаче биометрической верификации рукописной подписи». Электронный журнал «ИССЛЕДОВАНО В РОССИИ».

13.Семинары по выбору моделей, Евгений Соколов, http://www.machinelearning.ru/wiki/images/1/1c/Sem06_metrics.

14. (2008) «Алгоритм разбиения подписи на фрагменты применительно к задаче повышения надежности распознавания личности по динамике написания паролей». Материалы 62-й научно-технической конференции СибАДИ. -Омск, т.Кн. 1.: 124-128. 11.Backpropagation algorithm,Mihai Vărzaru [online]. Available: https://mihaiv.wordpress.com/2010/02/08/backpropagation-algorithm/

15. Абраменко А. Принципи розпізнавання / А. Абраменко – К:.Компьютер–пресс, 1997 – 123 с.

16.Казаков П.В. Распознавания графического образа личной подписи на основе искусственных нейронных сетей ,2012 год. – 67 с.

17.Сойфер,В.А. Компьютерная обработка изображений –Соросовский образовательный журнал.1996. № 3.

18. M. M. Lange, S.N. Ganebnykh (2005). «Classification of 2D Grayscale Objects in a Space of the Multiresolution Representation».

19.Image Processing Techniques For Machine Vision [online]. Available: http://www.eng.fiu.edu/me/robotics/elib/am_st_fiu_ppr_2000.pdf

20.ТРУДЫ МФТИ. 2016. Том 8, № 3 Ле Мань Ха, Свёрточная нейронная сеть для решения задачи классификации.

21.Implementation of Deep Learning Techniques, Bryan García Navarro

22.Горошкин А Н. Применение векторного подхода к распознаванию рукописныхсимволов//удк,2006,http://cyberleninka.ru/article/n/primenenie -vektornogo-podhoda-k-raspoznavaniyu-rukopisnyh-simvolov.

23. Britz D. Implementing a CNN for Text Classification in TensorFlow, 2015.

24. Hinton G.E., Salakhutdinov R.R. Reducing the dimensionality of data with neural networks // Science. 2006.

25. Lee H., Grosse R., Ranganath R., Ng A.Y. Convolutional Deep Belief Networks for Scalable Unsupervised Learning of Hierarchical Representations. Proceedings of the 26th Annual International Conference on Machine Learning. 2009.

26. Thorsten B., Franz A. Web 1T 5-gram Version 1 LDC2006T13. DVD. Philadelphia: Linguistic Data Consortium, 2006.
27. LeCun Y. LeNet-5, convolutional neural networks. Retrieved 16 November 2013.