МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

на тему:

« Інтелектуальна система графічної аутентифікації »

Завідувач кафедрою : **Довбиш А.С.**

Керівник роботи : **Шелехов І.В.**

Студент гр. КБ61\1 : **Марченко В.О.**

СУМИ 2020

ЗМІСТ

ВСТУП

В наш час з розвитком інформаційних технологій і появою глобальних комп'ютерних мереж доступ до інформації став значно простішим. У зв'язку з цим постає проблема про продуктивності та надійності інформаційних систем, загроз порушення безпеки даних при відсутності їх захисту, а саме проблема захисту інформації від несанкціонованого доступу. Для того щоб забезпечити безпеку інформаційних ресурсів, усунути можливість несанкціонованого доступу, посилити контроль за санкціонованим доступом до конфіденційної або до підлягає засекречування інформації, впроваджуються різні системи розпізнавання, встановлення автентичності суб'єкта (об'єкта) і розмежування доступу. Також в інформаційних системах зберігається, обробляється, циркулює різна інформація, втрата або спотворення якої може завдати істотної шкоди. Для уникнення таких ситуацій, важливо захистити дані від будь-яких загроз технічного характеру. Для цього необхідно вибрати найбільш ефективний спосіб захистити інформацію .Однією з таких систем є графічна аутентифікація .Одна з найуспішніших і застосовуваних технологій, в якій можуть застосовуватися для аутентифікації .

Люди живуть і взаємодіють в середовищі, де сприйняття зором переважає для більшості видів діяльності, тому наш мозок здатний обробляти і зберігати великі обсяги графічної інформації з легкістю. Хоча нам, можливо, буде дуже важко згадати рядок з п'ятдесяти символів, ми можемо легко згадати обличчя людей, місць, які ми відвідали, і речі, які ми бачили. Загалом графічні дані представляють собою багато байтів інформації . І тому пароль може бути абсолютно унікальним . Таким чином графічні паролі будуть більш зрозумілими для людей та будуть краще запам’ятовуватися і тим самим підвищіться система безпеки . В останній час для користувачів комп'ютерних і комунікаційних систем найбільш ефективним методом аутентифікації

виявляється саме графічний . Ці паролі складаються з певних дій , які користувач виконує на зображенні . Звичайно такі паролі є простими до запам’ятовування , але вони є більш уразливими .

1 ГРАФІЧНА АУТЕНТИФІКАЦІЯ

За класичними експериментами когнітивної науки людина володіє величезною пам'яттю для фотографій (Standing, Conezio and Haber, 1970). Таким чином, частіше використовують графічні методи аутентифікації , тоді рідше виникають проблеми із запам'ятовуванням, аніж методів які використовують на основі тексту. Запам’ятовування складних паролів, а також декількох паролів для різних систем складне завдання , тому що люди знаходять зображення навіть через певний проміжок часу набагато простіше .

1.1 Основні поняття і принципи

Аутентифікація - це процес перевірки особистості людини або пристрою. Поширеним прикладом є введення імені користувача і пароля при вході на веб-сайт . Введення правильних реєстраційних даних дозволяє веб-сайту дізнатися хто ви і що це насправді ви відвідуєте веб-сайт.

Хоча поєднання імені користувача і пароля є звичайним способом аутентифікації вашої особистості , існує багато інших типів аутентифікації. Наприклад, для розблокування телефону можна використовувати чотирьох або шестизначний код доступу. Для входу на ваш ноутбук або робочий комп'ютер може знадобитися один пароль. Кожен раз, коли ви перевіряєте чи відправляєте електронну пошту, поштовий сервер перевіряє вашу особистість, зіставляючи вашу адресу електронної пошти з правильним паролем. Ця інформація часто зберігається у вашому браузері або поштовою програмою, тому вам не потрібно буде вводити її кожен раз.

В сучасному світі існує безліч різних систем аутентифікації

Суть аутентифікації в тому, що користувачу представляється кілька колекцій зображених, які, в свою чергу , розбиваються по темам. Користувач повинен вибрати конкретний набір зображень, при цьому ввівши додатковий текстовий пароль (багаторазовий). Така аутентифікація стійка до перехвату:

програма - шпигун не відшукає введення пароля з клавіатури, так як існує ще графічний й пароль, окрім, текстового. Графічну аутентифікацію користувачів іноді просто називають графічним паролем .

Графічний пароль - це система аутентифікації, яка працює за допомогою вибору користувача із зображень у певному порядку, поданих у графічному інтерфейсі користувача (GUI).

В наш час інформаційні технології змінюються настільки швидко, що статичні механізми безпеки вже не забезпечують повної захищеності системи [1, с. 152]. В інформаційних системах зберігається, обробляється, циркулює різна інформація, втрата або спотворення якої може завдати істотної шкоди підприємству [2, с.54]. Тому важливо захистити нашу організацію, від будь-яких загроз технічного характеру. У зв'язку з цим необхідно вибрати найбільш ефективний спосіб захистити інформацію за допомогою графічних парольних систем. Графічні паролі будуються з будь-яких дій, які користувач виконує на зображенні. Коли користувач робить спробу увійти за допомогою графічного пароля в систему, та оцінює намальовані їм графічні знаки або дії з ними і порівнює їх з графічними знаками і діями, які використовувалися при виборі графічного пароля. Далі система оцінює різницю між кожним графічним знаком і приймає рішення про те, авторизувати користувача чи ні, на підставі кількості помилок в комплексі. Якщо графічний знак помилковий або використаний не в тому порядку, то авторизація не пройде. Якщо типи ліній, точок, їх порядок і положення правильні, то система буде оцінювати, наскільки графічний знак відрізняється від того, який вона бачила раніше, і прийме рішення, чи є він досить схожим, щоб авторизувати відвідувача. З цієї причини, аутентифікацію на основі графічного пароля іноді називають графічної аутентификацией користувачів [3]. Графічні паролі є найбільш надійним методом у використанні аутентифікації користувача в комп'ютерних та комунікаційних системах. Вони складаються з будь-яких дій, які користувач виконує на зображенні. Такі паролі

простіше запам'ятати, але вони уразливі до підглядання. Тому далі будуть розглянуті схеми графічних паролів, при використанні яких користувач може не побоюватися за те, що стоїть позаду людина ,може побачити його пароль або що пароль буде знятий на відеокамеру.

1.2 Класифікація графічних паролів

Графічні паролі поділяються на :

- На основі розпізнавання
- Згадування пароля на основі механічної пам’яті
    - Чиста методика обирання
    - На основі методу нагадування
- Гібридна техніка

1.2.1 Техніка на основі розпізнавання

У техніці розпізнавання деякі зображення показуються користувачеві під час реєстрації. Користувач повинен вибрати декілька зображень, значків або символів із колекції зображень. Під час процедури аутентифікації користувачі вимагають ідентифікувати свої зображення, символи чи піктограми, які вибираються на етапі реєстрації між групою зображень. У цій техніці користувачі можуть запам'ятати свої паролі навіть через 45 днів.

1.2.2 Техніка на основі механічної пам'яті

У техніці бази виклику користувач повинен згадати те, що було створено або призначено під час реєстрації. Користувач може відтворити свій пароль без жодних підказів. Цей прийом дуже розслаблений, тобто легкий і зручний. Він більш захищений, ніж техніка, заснована на розпізнаванні. Нагадаємо, заснована техніка має дві підкатегорії:

1.2.3 Чиста методика на основі нагадування:

У техніці, заснованій на чистому відкликанні, користувачеві не надається підказки для згадування свого пароля.

1.2.4 Техніка на основі нагадування

У техніці, що базується на згадуванні, користувачеві надається пропозиція згадати свої паролі. Ця методика проста, ніж техніка, заснована на чистому відкликанні.

1.2.5 Гібридна техніка

У гібридній техніці аутентифікація може бути групуванням двох або більше методик для більших переваг, ніж окремі методи. Це покращує аналіз даних. Обговорюється багато одиничних систем як на основі розпізнавання, так і на основі відкликання, і деякі з цих схем приєднуються для розробки гібридної техніки, тобто схем. У цій техніці паролі краще запам'ятовуються , ніж текстові паролі.

1.3 Приклади реалізації

1.3.1 Проста схема графічного пароля

Користувачеві пропонується вибрати будь-якої графічний файл (це може бути фотографія, будь-яка картинка або скріншот) і тричі провести по довільним областям на ньому курсором миші. Ці області користувач вибрав, коли створював пароль. Вибір трьох областей довільний, щоб споживач міг легко запам'ятати ці місця. Можна збільшити кількість обраних областей для надійного графічного пароля. Найбільший недолік для даного пароля - проблема підглядання стоїть позаду людини. Через цю уразливість до підглядання графічні паролі ніколи не можуть бути використані в середовищах, де екран бачить не тільки людина, що входить в систему.

1.3.2 Схема трикутника

Система випадковим чином розсіює N зображень на екрані. На практиці, число N може бути кілька сотень або кілька тисяч, і об'єкти повинні бути різними настільки, що користувач може розрізняти їх. Крім того, є підмножина K парольних зображень (наприклад, $K = 3$), які попередньо вибрав і запам'ятав

користувач. При вході система буде випадковим чином вибирати розміщення N зображень. Однак, система спочатку випадковим чином вибирає ділянку, яка покриває половину екрану, і випадково розміщує . До вибраних зображень на цій ділянці. При створенні пароля користувачеві пропонується вибрати і запам'ятати три іконки приблизно з 200-400 можливих. При необхідності введення пароля система видає на екран відразу величезну кількість іконок, перемішаних випадковим чином. Серед них обов'язково будуть три «ваші». Їх слід подумки з'єднати лініями (вийде трикутник) і клацнути мишкою в будь-якій точці всередині цієї фігури. Тут же іконки перебудовуються, перемішуються. Одні при цьому зникають, інші - додаються. І знову серед усього цього хаосу ви бачите і будь-які свої значки з тієї самої трійки (не обов'язково ті, що були на екрані тільки що). Знову ви подумки з'єднуєте їх в геометричну фігуру і клацаєте в будь-якому місці, але знову-таки в її межах. І так відбувається 10 разів. Взагалі система передбачає при створенні пароля вибір налаштувань: числа іконок, швидкість їх переміщення, числа кліків по фігурам і деяких інших параметрів. Лише після 10 таких проходів машина однозначно ідентифікує іконки, які ви подумки тримали в голові, вибираючи місце для клацання. Але будь-який, хто буде за вами спостерігати, ні за що не вгадає ваш пароль.

Головна ідея - дозволити користувачеві довести знання їм пароля, не показуючи сам пароль в процесі його набору. Питання змінюється кожен раз і відповідь - так само. Але секретне знання залишається тим же самим. При цьому рівень секретності забезпечується високий. Якщо ви маєте достатньо багато чого зображень, і якщо ви повинні пройти тест досить багато раз, можливі комбінації іконок обчислюються мільярдами. Недолік у цієї системи, мабуть, один: для входу в систему потрібно значно більше часу, ніж на традиційний набір п'яти-шести букв у віконці пароля.

1.3.3 Схема перетину діагоналей чотирикутника

При запуску сервісу, замість введення пароля буде з'являтися вікно введення графічного пароля, що містить 154 зображень.

Для аутентифікації користувач повинен виконати наступне:

1. Знайти 4 свої парольні картинки.
2. Подумки утворити з них чотирикутник.
3. Клацнути на зображення, яке знаходиться на перетині діагоналей чотирикутника. Точно так, як показано на малюнку.
4. Після виконання цієї операції, відбудеться вхід в систему. При цьому рівень секретності буде максимальний.

Якщо користувач забуде пароль, адміністратор системи зможе йому допомогти, натиснувши спеціальну кнопку. Було розглянуто три види графічних систем: «Проста схема графічного пароля», «Схема трикутника» і «Схема перетину діагоналей чотирикутника». У кожного способу є свої особливості для захисту інформації від різних технічних загроз, а також свої недоліки .

1.4 Постановка задачі

Аналіз існуючих підходів до реалізації систем графічної аутентифікації доводить можливість застосування інтелектуальних технологій для реалізації процесів збереження і перевірки графічних паролів. Метою роботи є розробка системи графічної аутентифікації з використанням штучних нейронних мереж, що здатні автоматизувати обидва вказаних процеси. Для досягнення поставленої мети необхідно виконати ряд завдань:

1) Сформувати вхідний математичний опис інтелектуальної системи графічної аутентифікації;
2) Обрати тип нейромережі та визначити структуру і функціональні параметри її елементів;

3) Обрати критерій якості навчання нейромережі.
4) Розробити та програмно реалізувати алгоритм навчанн нейромержі.
5) Перевірити працездатність розробленої системи на задачі збереження та перевірки п’яти графічних паролів.

2 БІОМЕТРИЧНІ ТЕХНОЛОГІЇ АУТЕНТИФІКАЦІЇ ОСОБИ

2.1 Основні визначення, класифікація, порівняльний аналіз

Графічна аутентифікація відноситься до біометричних технологій, що знайшли своє застосування в галузі кібербезпеки.

Зазвичай при класифікації біометричних технологій виділяють дві групи біометричних систем по типу використовуваних біометричних ознак.

Перша група систем використовує статичні біометричні ознаки, отримані людиною з народження і практично не змінні в часі. До таких ознак належать:

- відбитки пальців;
- райдужна оболонка ока;
- зображення особи;
- геометрія кисті руки;
- рисунок пальців руки;
- ДНК тощо

Друга група систем використовує для ідентифікації динамічні біометричні ознаки, що здатні змінюватися з часом і відображають такі індивідуальні особливості кожної людини, як:

- рукописний почерк (підпис);
- голос;
- манера працювати на клавіатурі тощо

Кожна з цих ознак має свої переваги і недоліки. Перевагою використання статичних біометричних ознак є їх відносна незалежність від психофізичного стану особи, не значні витрати на реалізацію алгоритмів розпізнавання і, як наслідок, можливість організації біометричної ідентифікації великих потоків людей. Не випадково, найбільшого поширення на практиці отримали біометричні методи, що відносяться саме до цієї (першої) групи і засновані на використанні перших трьох зі згаданих вище ознак (розпізнавання за

відбитками пальців, райдужною оболонкою ока і особливостями геометрії особи). Недоліком статичної біометрії є статичність (фіксованість) біометричних ознак, внаслідок чого з'являється спокуса їх підробки (підміни), визначення якої виконується додаткових спеціальних методик та пристроїв.

На відміну від методів першої групи, методи динамічної біометрії забезпечують більшу варіантність (так, підпис або парольну фразу завжди легко змінити); вони легко реалізуються програмним шляхом, з використанням стандартних периферійних пристроїв комп'ютера. Дані обставини роблять динамічну біометрії більш ефективною для аутентифікації / ідентифікації особистості при віддаленому доступі користувача. Основний недолік динамічних методів - вплив на роботу біометричної системи психофізичного стану особистості (втома, переляк, вплив лікарських препаратів).

В основі функціонування будь-якої біометричної системи лежить ланцюжок наступних дій (рис. 2.1):

1) запис - зчитуються за допомогою сканера біометричні дані особи;

2) екстракція - з представлених біометричних даних витягується унікальна інформація (у вигляді вектору інформативних ознак або короткого ідентифікаційного коду, довжиною до 1000 біт), яка і буде представляти собою біометричний «образ» конкретної людини;

3) порівняння - проводиться порівняння представленого біометричного способу з одним або більшим числом еталонів (шаблонів), що зберігаються в базі даних системи;

4) прийняття рішення - система вирішує, збігаються чи ні біометричні образи, і виносить судження про закінчення процедури ідентифікації, її повторенні або зміну умов її проведення.

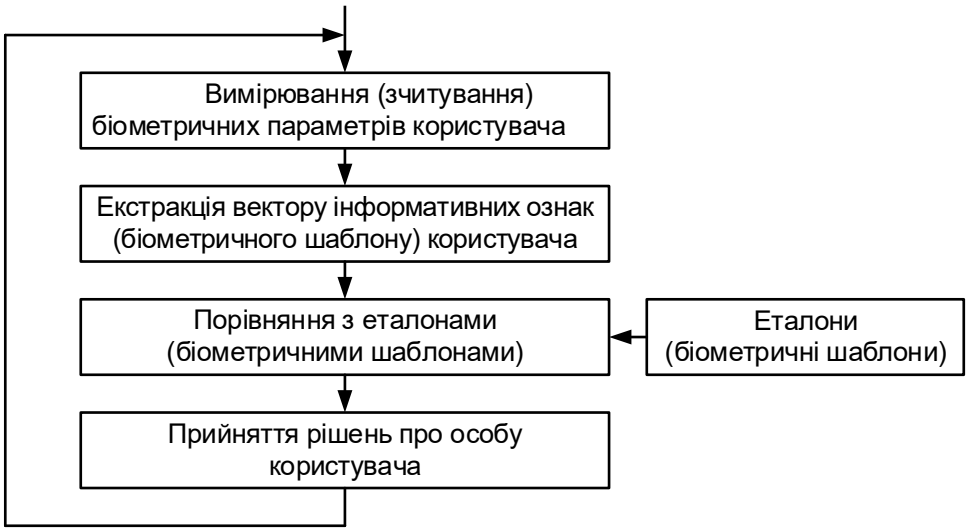

Рисунок 2.1 – Процедура біометричної ідентифікації

На етапі екстракції (виділення) і порівняння біометричних даних використовуються біометричні шаблони (Biometric Templates), тобто набори даних в закритому, двійковому форматі, що містять в закодованому (стислому) вигляді інформацію про відповідні біометричні образи. Міжнародний стандарт CBEFF (Common Biometric Exchange File Format) встановлює єдиний формат подання біометричних даних і пропонується для заміни біометричних форматів, що використовуються сьогодні на біометричний ринку різними виробниками обладнання та програмного забезпечення.

Розрізняють два можливих режими роботи біометричної системи - верифікація («порівняння одного з одним») і ідентифікація («порівняння одного з багатьма»).

В режимі верифікації користувач пред'являє системі свої біометричні дані («біометрику»), оголошуючи тим самим їй, «хто він такий». Завдання системи в даному випадку - перевірити «правдивість» отриманої інформації, тобто звірити відповідність отриманих біометричних даних з записаним раніше шаблоном (еталоном) вказаної особи.

В режимі ідентифікації користувач також пред'являє системі свою біометрику, проте завдання системи змінюється - необхідно прийняти рішення,

чи належить користувач до числа відомих їй осіб, і якщо належить, то - хто він? В цьому випадку виміряні біометричні дані порівнюються з базою даних раніше записаних шаблонів всіх «відомих» системі осіб.

Очевидно, що в реальних умовах застосування біометричні системи стикаються з рядом проблем, одна з яких полягає в необхідності забезпечення високої надійності розпізнавання особи. Складність вирішення цієї проблеми полягає в тому, що:

а) сама процедура біометричної ідентифікації / верифікації має імовірнісний характер, оскільки самі вимірювані біометричні дані схильні до впливу великої кількості факторів невизначеності, тобто зберігається певна ймовірність «не визнати свого» і «визнати свого чужим»;

б) біометрична система повинна бути захищена від свідомого обману, тобто можливості підміни об'єкта біометричного сканування;

в) набуває особливої важливості питання про збереження зібраної біометричної інформації (мова йде не тільки про можливості її злому, але і про те, що будь-який біокод, наприклад, стан райдужної оболонки ока або вен руки, несе в собі багато інформації про стан здоров'я конкретної людини, що може бути використано в протиправних цілях).

Для порівняльної оцінки ефективності різних біометричних технологій розглянемо табл. 2.1. У стовпцях цієї таблиці вказані основні критерії, яким повинна відповідати в тій чи іншій мірі будь-яка біометрична технологія, а також якісні значення цих критеріїв для різних технологій (розглядаються тільки технології розпізнавання особи за зображенням - двомірна (2D) і тривимірна (3D) фотографія, за відбитками пальців і за райдужною оболонкою ока).

Таблиця 2.1 – Характеристики біометричних технологій

	Технологія			
	за зображенням обличчя		за відбитками пальців	за райдужною оболонкою ока
Критерій	2D	3D		
Вимірювальність	B	C	C	C
Стійкість до зовнішніх впливів	B	B	A	B
Стійкість до підроблення	C	C	C	B
Точність розпізнавання	C	B	C	B

1. Вимірність. Біометрична ознака (параметр) повинена легко вимірюватися. Вимірність можна кількісно оцінити величиною 1 - FER, де FER (Failure to Enroll) - частка індивідуумів, які не змогли пройти реєстрацію (система не змогла побудувати біометричний шаблон), і середнім часом розпізнавання (Recognition Time). Під часом розпізнавання мається на увазі або час верифікації, або час ідентифікації - в залежності від режиму, в якому працює система. FER включає в себе випадки, коли у індивідуумів потрібні біометричні дані відсутні, але головним чином випадки, коли з тих чи інших причин вимір цих даних для даної людини на даному сканері утруднено.

Так, наприклад, для розпізнавання за райдужною оболонкою ока потрібно зображення з високою роздільною здатністю, що призводить до певних ускладнень, пов'язаних з необхідністю точного позиціонування ока по відношенню до скануючого пристрою.

Розпізнавання багатьох груп людей за відбитками пальців також ускладнене, особливо це стосується працівників фізичної праці, людей зі слабо

вираженими папілярним візерунками і дефектами шкіри, літніх людей із сухою шкірою. Методи розпізнавання по зображенню особи - безконтактні і тому мають високу вимірювальність біометричного ознаки.

2. Стійкість до зовнішніх впливів. Біометрична технологія повинна бути стійка до зміни навколишнього середовища. Експлуатаційні характеристики різних технологій в значній мірі залежать від оточуючих умов і можуть втрачати стабільність при зміні цих умов. Наприклад, сканери відбитків пальців швидко забруднюються, а при розпізнаванні осіб за двомірною фотографією велике значення має розподіл зовнішньої освітленості.

3. Стійкість до підроблення. Біометрична система повинна бути стійкою до різного роду підробок (несанкціонованого доступу). Систему розпізнавання за двовимірним зображенням особи здатна прийняти неправильне рішення, коли їй пред'являють фотографію «правильної» особи з числа «знайомих» системі. Вкрасти зображення чужої оболонки ока, звичайно, складніше, ніж фотографію особи, але якщо це зроблено, то систему також можна обдурити фотографічним зображенням «потрібного» ока, роздрукованим з високою роздільною здатністю або нанесеним на контактну лінзу.

Для отримання несанкціонованого доступу за відбитком пальця, в принципі, можна зняти відбитки пальців «потрібної» особи, що були залишені на будь-якій поверхні, оцифрувати їх і обробити отримане зображення на комп'ютері, після чого виготовити «фальшивий» палець або накладку на нього (класичний приклад, часто цитований в літературі, - японський криптограф Цутому Мацумото з групою своїх студентів з університету Йокогами показав, як легко в лабораторних умовах виготовити фальшиві відбитки пальців, за допомогою яких можна обдурити практично будь-яку сучасну систему біометричної аутентифікації).

Найбільш стійкою до підробки є технологія розпізнавання по тривимірному зображенню особи. Для того щоб обдурити таку систему,

потрібно виготовити точну твердотільну маску особи, яка повторює в усіх деталях її геометрію, що на практиці є досить складним завданням.

4. Точність розпізнавання. Для оцінки точності роботи біометричної системи зазвичай використовуються такі показники:

- FAR (False Acceptance Rate) - ймовірність помилкового розпізнавання, коли система надає доступ незареєстрованим користувачам;
- FRR (False Rejection Rate) - ймовірність помилкового відмови в доступі, коли система не розпізнає «знайомого» їй суб'єкта і відповідно визнає його за «чужого».

У теорії статистичних рішень значення FRR і FAR прийнято називати відповідно помилками 1-го і 2-го роду.

На практиці будь-яку біометричну систему можна налаштувати на різну ступінь «пильності», тобто на різне значення ймовірності помилкового розпізнавання FAR. Але зменшення FAR завжди призводить до зменшення чутливості системи і збільшення ймовірності помилкового відмови (не-розпізнавання) FRR. Таким чином, чим «більш пильною» налаштована система на непропускання «чужих», тим вона менш чутлива, а значить, гірше пропускає «своїх». У сучасних системах значення FAR становлять частки відсотка, значення FRR - кілька відсотків (2 ... 5%).

Як показують дослідження, конкретні показники точності системи сильно варіюються в залежності від виробника і методики тестування, проте важливо, що три із зазначених в табл. 2.1 технологій розпізнавання - за тривимірним зображенням особи, за відбитком пальця і за райдужною оболонкою ока - мають точність одного порядку.

При цьому розпізнавання за двовимірним зображенню особи істотно поступається в точності іншим технологіям, так само як і біометричним технологіям, що не подані в табл. 3.1, (розпізнавання за геометрією руки, за

голосом тощо). З другої сторони слід зазначити, що двомірне зображення обличчя найзручніше для візуального порівняння оператором.

Зауважимо також, що при використанні біометричної системи в режимі ідентифікації («порівняння одного з багатьма») точність розпізнавання багаторазово погіршується в порівнянні з режимом верифікації («порівняння одного з одним»). Так, наприклад, якщо при FRR, рівному 1,3%, кращий пальцевий сканер в режимі верифікації забезпечує FAR, рівний 0,001% (один шанс зі ста тисяч), то в режимі ідентифікації при тому ж FRR і базі даних в 100 чоловік FAR вже залишає 0,1%, а при базі даних в 1000 чоловік - 1% (тобто один шанс зі ста), що вже неприпустимо для більшості додатків.

Для підвищення точності розпізнавання в режимі ідентифікації доцільно використання одночасно декількох біометричних технологій. Цей перспективний напрямок в біометрії базується на концепції побудови багатофакторних біометричних (мультибіометричних) систем ідентифікації (AMIS, Automated Multimodal Biometric Identification Systems). Зазвичай це багатофакторні біометричні системи, що інтегрують такі технології розпізнавання:

- за відбитками пальців;
- за зображенням особи;
- за голосом;
- за почерком.

Інтеграція зазначених біометричних технологій передбачає два аспекти - технічний і алгоритмічний. Технічно інтеграція полягає в об'єднанні кількох програмно-апаратних комплексів за допомогою єдиного інтерфейсу, що в достатній мірі вирішується шляхом стандартизації. При цьому як базові модулі біометричного програмного забезпечення до складу системи включені:

- бібліотека Biolink SDK порівняння і експертної обробки відбитків пальців;

- бібліотека Neirotechnologia VeriLook 2.0 SDK ідентифікації особи;
- бібліотека IIT FaceDetection SDK виявлення і міжкадрового відстеження осіб в відеопотоці;
- бібліотека Trawl SDK ідентифікації абонента в телефонному каналі.

З алгоритмічної точки зору, інтеграція біометричних технологій є досить складною прикладною математичною задачею прийняття рішення про ідентичність наборів біометричних образів, для вирішення якої використовуються методи статистичної теорії прийняття рішень.

При створенні багатофакторної біометричної системи враховується, що біометрична ідентифікація сама по собі є витратною обчислювальної процедурою, внаслідок чого до складу програмно-апаратного комплексу включають високопродуктивний сервер зі спеціально обладнаним АРМ біометриста, тобто біометрична система розробляється як клієнт-сервер додаток.

В цілому, впровадження такої багатофакторної біометричної системи дозволяє значно підвищити якість процесів розпізнавання особи, забезпечуючи:

- зменшення вірогідності помилок 1-го і 2-го роду;
- зниження вимог до кваліфікації операторів (експертів);
- охоплення більшої частини населення, у порівнянні з будь-якою однофакторною системою;
- можливість ведення єдиного сховища (бази) біометричних даних за рахунок інтеграції різних біометричних банків.

Повернемося ще раз до базових функцій, що лежать в основі будь-якої біометричної системи (Рис. 2.1). При цьому навмисно не будемо зупинятимемося на функціях вимірювання біометричних параметрів користувача та побудови його ідентифікатора (біометричного шаблону), вважаючи, що ці функції дуже специфічні і прив'язані до конкретних біометричних ознак людини (зображення особи, відбиток пальця тощо).

Інваріантну частину біометричної системи займають модулі, відповідальні за функції розпізнавання і прийняття рішень. Будемо вважати, що біометричний образ користувача подається вектором $x = (x_1, x_2, \dots, x_m)^T$ інформативних ознак, які використовуються для ідентифікації. Тоді задача розпізнавання особи зводиться до віднесення такого вектору до одного з класів, що «відомі» системі. У разі успішної класифікації, система «впізнає» користувача і виробляє зумовлену адміністратором дію: надати йому доступ до інформаційних ресурсів, відкрити двері в приміщення, що охороняється тощо.

Початковим етапом побудови системи розпізнавання особи є етап навчання. На цьому етапі здійснюється:

- формування алфавіту класів - для системи ідентифікації особи класами є її користувачі. При цьому система формує (оновлює) свій алфавіт класів в той час, коли користувач проходить реєстрацію і створює його унікальний ідентифікаційний номер (ID) або мітку класу;
- виконання навчальних спостережень - оновивши словник класів, система вже «знає» про існування нового користувача (класу), але «не знає» його параметрів. Для отримання такої інформації система кілька разів (від одного до R) вимірює відповідні параметри. Наприклад, в разі розпізнавання людини за кистю руки, користувач кілька разів сканує руку для «навчання» системи. При цьому формується (оновлюється) так звана матриця даних, або навчальна вибірка. Рядками цієї матриці є вектори ознак, а першим стовпцем - мітка класу. Сукупність матриць для всіх класів, відомих системі розпізнавання, становить її загальну базу даних. Саме ця інформація використовується для оптимізації простору ознак; саме з цього моменту система здатна «впізнати» користувача;
- побудова еталонів класів - для формування еталонних описів класів, що зберігаються в архіві системи, використовуються різні методи: статистичні, структурні, логічні, нейромережеві тощо. Найпростішим прикладом еталонного

опису класу є вектор ознак, кожен компонент якого це середнє значення відповідної ознаки.

В основі більшості алгоритмів, що використовуються на етапі розпізнавання біометричних образів, закладені наступні підходи: порівняння з еталоном, дискримінантний і синтаксичний (або лінгвістичний) підходи.

1. Метод порівняння з еталоном. Розпізнавання в даному випадку зводиться до прямого порівняння біометричного образу, що поданий у вигляді вектору ознак x, з еталонами класів $X_j, (j = 1, 2, \dots, M)$. Рішення про належність образу до певного класу приймається шляхом обчислення значення міри близькості (або подібності) μ_j між x і кожним X_j. Рішення про належність образу x до k-того класу приймається, якщо виконуються дві умови (2.1-2.2): міра близькості між x і X_k перевищує міру близькості між x і іншими класами та перевищує деякий заданий поріг r, тобто

$$\mu_k = \max_{j=1,\dots,M} \mu_j \tag{2.1}$$

$$\mu_k > r \tag{2.2}$$

При цьому, якщо виконується лише умова (2.1), тобто міра близькості не перевищує число r, то приймається рішення, що в базі даних системи розпізнавання не існує клас, до якого належить біометричний образ. Зміна значення r дозволяє регулювати «суворість» системи ідентифікації. У теорії систем розпізнавання це число називають порогом прийняття рішення.

Як міра близькості використовуються:

- коефіцієнт парної кореляції;
- імовірнісні оцінки на основі методу Байєса;
- міра близькості Хеммінга;
- евклідова відстань тощо.

Обчислюючи міри близькості між біометричним образом і всіма відомими класами і визначаючи екстремум, отримаємо систему ідентифікації, а обчислюючи міру близькості між невідомим системі вектором ознак і еталонним вектором класу, який визначено введеним паролем (ID), отримуємо систему верифікації.

2. Дискримінантний підхід, що розроблено в рамках теорії статистичних рішень, є універсальним і включає в себе метод порівняння з еталоном як окремий випадок.

Згідно цього підходу вважається, що кожному вектору $x = (x_1, x_2, \dots, x_m)^T$ відповідає певна точка в m-мірному просторі ознак. Якщо алфавіт класів розпізнавання складається M класів, то кожному класу буде відповідати певна область (як правило, компактна, оскільки значення біометричних ознак однієї особи відрізняються лише незначним відхиленням). Таким чином, простір ознак по числу класів розбивається на M областей. Якщо вдасться побудувати такі роздільні (дискримінантні) функції $f_i(x)$, $(i = 1, 2, \dots, N)$, які відповідали границям для зазначених областей, то за величиною або за знаком цих функцій можна було б судити про належність вектору x тій чи іншій області (а отже, біометричного образу - того чи іншого класу). Правило, яке дозволяє на основі наявної (в тому числі апріорної) інформації про компоненти вектору ознак x і обчислених значеннях функції $f_i(x), (i = 1, 2, \dots, N)$ прийняти рішення про належність образу, що розпізнається, конкретного класу з числа відомих («свій») або його відсутність («чужий»), називається вирішальним правилом. Загальна схема процесу розпізнавання на основі дискримінантного підходу наведена на рис. 2.2.

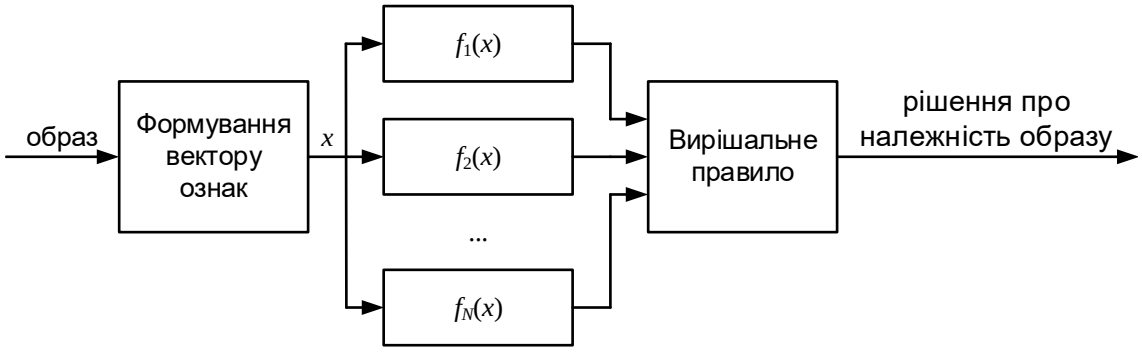

Рисунок 3.2 – Схема процесу розпізнавання на основі дискримінантного підходу

Зрозуміло, що побудова «точних» роздільних функцій є досить складною задачею, а часто такою, що немає розв'язку. На практиці обмежуються побудовою наближених (апроксимуючих) виразів для роздільних функцій. При цьому можливі такі ситуації:

а) класи розпізнавання лінійно роздільні, тобто роздільні функції мають лінійний вигляд:

$$f_i(x) = \sum_{j=1}^{m} w_{ij}\, x_j + w_{i0} \qquad (2.3)$$

де w_{ij} і w_{i0} - деякі постійні коефіцієнти, а розбиття простору ознак на області здійснюється за допомогою підібраних відповідним чином N гіперплоскостей.

У найпростішому випадку (для $m = 2$) завдання формування вирішального правила зводиться до проведення на площині прямих, що найкращим чином розділяють класи розпізнаваних об'єктів «Свій 1», «Свій 2», «Чужий» (рис. 2.3, а);

б) класи розпізнавання роздільні з використанням нелінійних, наприклад, поліноміальних функції:

$$f_i(x) = \sum_{j=1}^{m} \left(w_{ij}^{(1)} x_j + w_{ij}^{(2)} x_j^2 + \cdots + w_{ij}^{(p)} x_j^p \right) + w_{i0} \qquad (2.4)$$

де $w_{ij}^{(1)}$, $w_{ij}^{(2)}$, …, $w_{ij}^{(p)}$ і w_{i0} - постійні коефіцієнти, що підбираються таким чином, щоб забезпечити розбиття просторі ознак за допомогою нелінійних гіперповерхонь (приклад для m = 2 наведено на рис. 3.3, б);

в) класи розпізнавання нероздільні «точно», тобто перетинаються (рис. 3.3, в). У цьому найскладнішому (проте найбільш характерному для практики) випадку, при будь-якому виборі виду роздільних функцій і вирішального правила існує ймовірність того, що особа не буде «впізнана» системою FRR (помилка 1-го роду) і ймовірність «неправильного розпізнавання» FAR (помилка 2-го роду). На помилки розпізнавання впливає також пов'язане з перешкодами (шумами вимірювань) і спотворення інформації, що міститься в самому векторі ознак x.

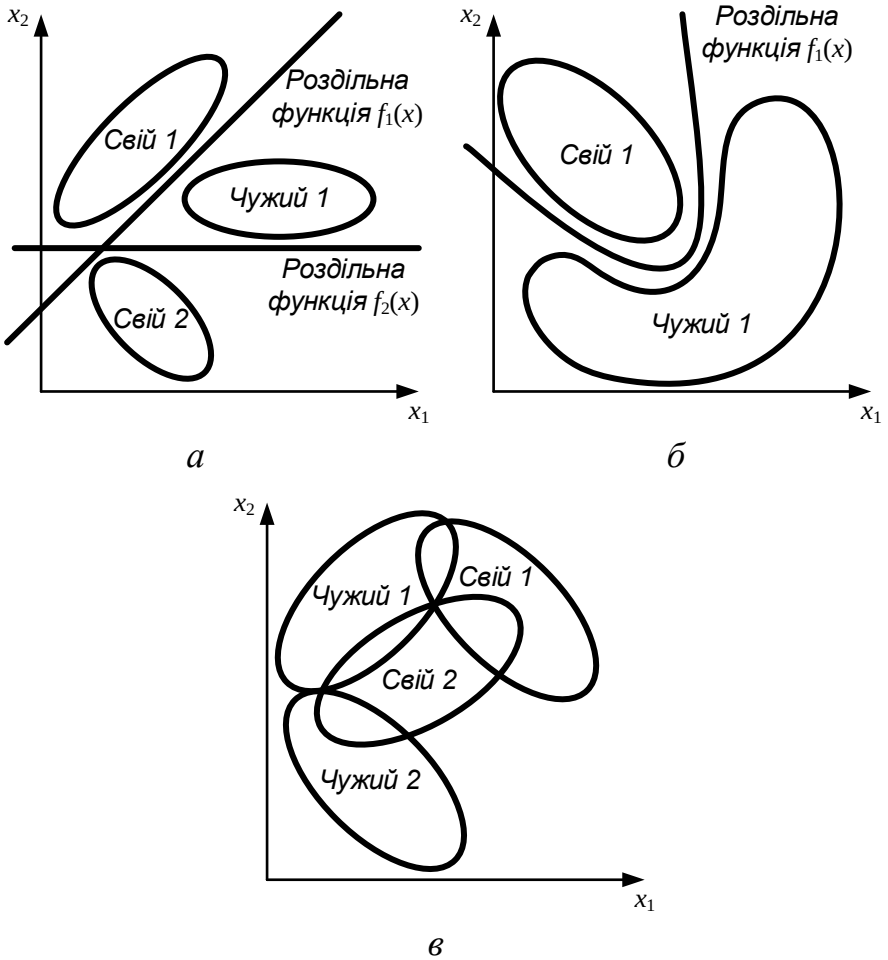

Рисунок 2.3 – Розбиття площини ознак на класи

Виходом в даній ситуації є врахування стохастичною природи вектору x, що можна розглядати як значення m -мірної випадкової величини y, розподіл якої описує статистичну мінливість біометричних параметрів користувача і характеризується щільністю $p(x)$. Відповідно розподіл векторів біометричних ознак «своїх» (X_j) і «чужих» $(\overline{X_k})$ користувачів буде характеризуватися щільністю $p(x/X_j)$ і $p(x/\overline{X_k})$. При цьому завдання полягає в побудові на основі статистичного матеріалу, отриманого в процесі навчання, роздільних функцій

$$f_i(x) = p(X_j/x), (j = 1, 2, \dots, M) \quad (2.5)$$

де $p(X_j/x)$ - умовна ймовірність того, що невідомий об'єкт (користувач) відноситься до класу X_j, якщо йому відповідає вектор x.

Якщо щільності розподілу вектору $p(x/X_j)$, $(j = 1, 2, \dots, M)$ заздалегідь невідомі, то роздільні функції $f_i(x)$ можуть бути задані в явному вигляді з використанням M параметрів-ваг:

$$f_i(x) = f_i(x, w_1, w_2, \dots, w_M) \quad (2.6)$$

а побудова вирішального правила зводиться до вибору виду функцій $f_i(x)$ і підбору таких значень параметрів-ваг, що гіперповерхні $f_i(x)$ з прийнятною точністю могли видділити в m-мірному просторі біометричних ознак M класів «своїх» користувачів, виключаючи «чужих ».

У разі, якщо параметри розподілу $p(x/X_j)$ відомі, доцільно використовувати параметричні методи, коли гіперповерхні $f_i(x)$ будуються на основі даних навчальної вибірки. При цьому як вирішальні правила можуть використовуватися різні критерії, пов'язані з ризиком прийняття рішення:

- критерій Байеса - правило, згідно з яким стратегія прийняття рішення вибирається таким чином, щоб забезпечити мінімум середнього ризику;
- мінімаксний критерій - такий, який мінімізує максимально можливе значення середнього ризику;

- критерій Неймана-Пірсона, заснований на мінімізації помилок розпізнавання.

Зауважимо, що якість вирішального правила значною мірою залежить від ступеня відповідності реальних і використаних в $f_i(x)$ параметрів розподілу. При відсутності (або малому обсязі) статистичних даних, завдання оцінки параметрів розподілу і прийняття рішення можна вирішувати з використанням так званих «суб'єктивних ймовірностей», що визначаються експертами, і залученням апарату теорії нечітких множин і лінгвістичних змінних.

Загальні недоліки існуючих біометричних методів ідентифікації особистості:

- якість розпізнавання (прийняття рішень) в значній мірі залежить від якості вимірюваних біометричних даних;
- має місце значний розкид показників якості системи, оскільки існуючі біометричні системи орієнтовані, як правило, на абстрактного середньостатистичного користувача;
- високий відсоток помилок в умовах впливу факторів невизначеності, залежність показників точності розпізнавання від числа користувачів системи;
- значне ускладнення алгоритмів розпізнавання (прийняття рішень) при використанні багатофакторної біометричної ідентифікації;
- не до кінця вирішені питання атестації (оцінки відповідності) і сертифікації засобів біометричної ідентифікації користувачів.

2.2 Нейромережеві алгоритми біометричної ідентифікації

Зазначені недоліки в значній мірі нівелюються в нейромережевих біометричних системах ідентифікації, що використовують механізми налаштування (адаптації) до конкретного користувача шляхом навчання (або самонавчання) мережі на множині отриманих біометричних даних в реальних умовах експлуатації.

Нейронні мережі (НМ) займають важливе місце при вирішенні завдань забезпечення інформаційної безпеки, оскільки мають ряд переваг:

- можливість відтворення з заданою точністю складних нелінійних залежностей (за що їх часто називають «універсальними апроксиматорами»);
- здатність до навчання і самонавчання (налаштування НМ на вирішення певної задачі проводиться на серії «прикладів» з навчальної вибірки, причому на навчальну вибірку не накладаються обмеження);
- здатність до узагальнення (тобто досвід, отриманий мережею в процесі навчання на кінцевому числі образів, можна успішно поширити на інші, в тому числі невідомі їй образи);
- потенційно висока завадо- і відмовостійкість (так, в разі поступового виходу з ладу до 50% елементів, з яких складається НМ, зберігається прийнятна її працездатність);
- в силу паралельної природи НМ, її архітектура природним чином реалізується на паралельних обчислювальних засобах.

Система розпізнавання образів, побудована на основі НМ, в загальному випадку складається з двох частин (рис. 2.4): підсистеми екстракції інформативних (інваріантних) ознак і нейромережевого класифікатора, що виконує функцію вирішального правила.

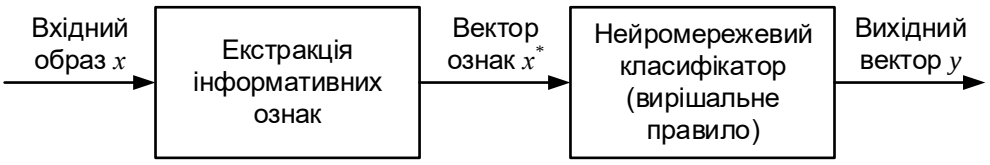

Рисунок 2.4 – Блок-схема розпізнавання образів на основі нейромережі

На першому етапі проводиться перетворення координат вхідного вектору (образа) x з метою екстракції з нього інформативних ознак, які зберігають найбільш важливу інформацію, що міститься в наборі вхідних даних (спостережень), і при цьому є інваріантними до трансформацій вхідного

сигналу, пов'язаних зі зміною положення розпізнається об'єкта (зрушення, обертання, зміни масштабу, ракурсу тощо). Це перетворення переводить вхідний образ - точку x в m-мірному просторі вхідних даних - в точку x^* в m^*-мірному просторі ознак. Оскільки $m^* < m$, то таке перетворення можна розглядати як операцію зниження розмірності (тобто стиснення даних), яка спрощує завдання класифікації. Сама класифікація являє собою перетворення, яке відображає точку (вектор) x^* в один з класів M-мірного простору рішень (де M - кількість виділених класів). Розмірність вихідного вектору y при цьому можна прийняти рівною M, якщо припустити, що j-я компонента вектору y приймає значення 1 тільки в тому випадку, якщо вектор ознак x^* належить «відомому» k-тому класу; інші компоненти вектору y при цьому приймають нульові значення.

Узагальнена блок-схема нейромережевої системи біометричної - ідентифікації особи, наведена на рис. 2.5.

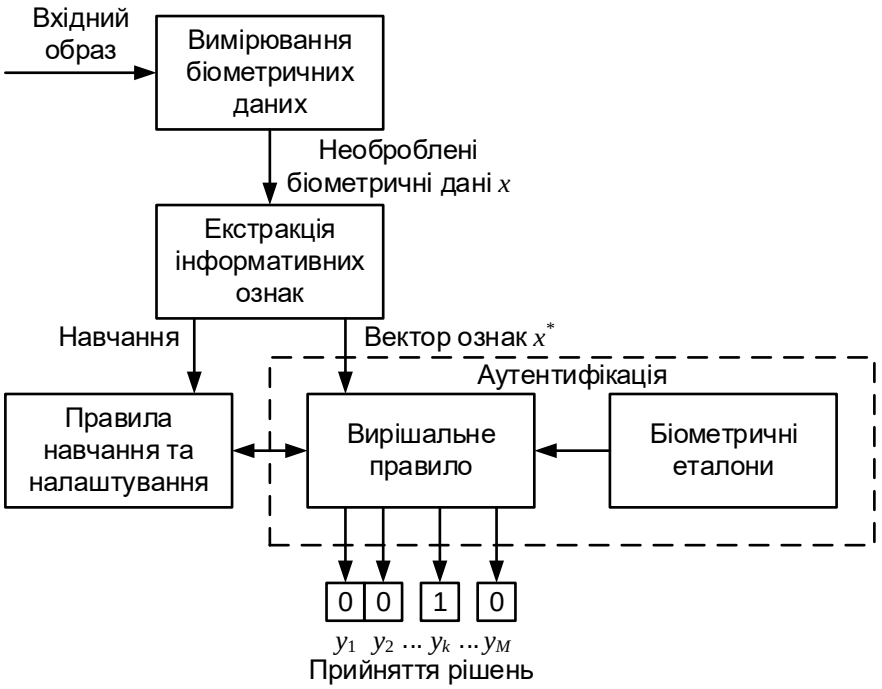

Рисунок 2.5 – Узагальнена блок-схема нейромережевої системи біометричної ідентифікації

Вона відображає основні етапи обробки інформації НМ:

- вимір біометричних даних користувача за допомогою сенсорів (вхідних перетворювачів);
- екстракція інформативних (інваріантних) біометричних ознак;
- побудова нейромережевого біометричного еталону користувача;
- реалізація вирішального правила на основі НМ.

Слід зазначити, що перші два блоки обробки інформації працюють за одними і тими ж алгоритмами, незалежно від режиму роботи самої біометричної системи. Режим роботи системи (навчання або ідентифікація/ аутентифікація) визначає сукупність операцій, що виконуються з векторами інформативних біометричних ознак $x_t^* = \left(x_{1,t}^*, x_{2,t}^*, \dots, x_{m^*,t}^*\right)^T, (t = 1,2, \dots, T)$

У режимі навчання вектори ознак $x_t^*, (t = 1,2, \dots, T)$ надходять в блок правил навчання та налаштування, який формує біометричні еталони користувачів (класів). Оскільки біометричні образи одного користувача повністю неідентичні один до одного, то для формування біометричних еталонів потрібно кілька прикладів таких образів для кожного з користувачів.

В режимі ідентифікації (аутентифікації) вектор ознак x^* порівнюється вирішальним правилом з біометричним еталоном. Якщо вектор x^* виявляється близький до біометричного еталону, приймається позитивне аутентифікаційне рішення. При значних відмінностях вектору x^* і його біометричного еталону приймається рішення про відмову користувачеві в аутентифікації. У ряді випадків користувачеві може бути надана спроба повторної аутентифікації.

Зупинимося докладніше на процедурі побудови і навчання НМ, яку використовують як вирішальне правило і біометричного еталону особи.

На рис. 2.6 наведено приклад найбільш поширеною схеми НМ - багатошарового персептрона.

Дана мережа містить три прошарки нейронів:

- вхідний прошарок, на який подаються компоненти вектору ознак x^* і який передає їх на нейрони наступного прошарку, не виконуючи жодних перетворень;
- прихований прошарок, що здійснює нелінійне перетворення координат $(x_1^*, x_2^*, \dots, x_{m^*}^*)$ до деяких величини $(z_1, z_2, \dots, z_n)$ - виходи нейронів прихованого прошарку;
- вихідний прошарок - формує вектор вихідних реакцій $(y_1, y_2, \dots, y_M)$, що складається з M нейронів (по числу класів розпізнавання).

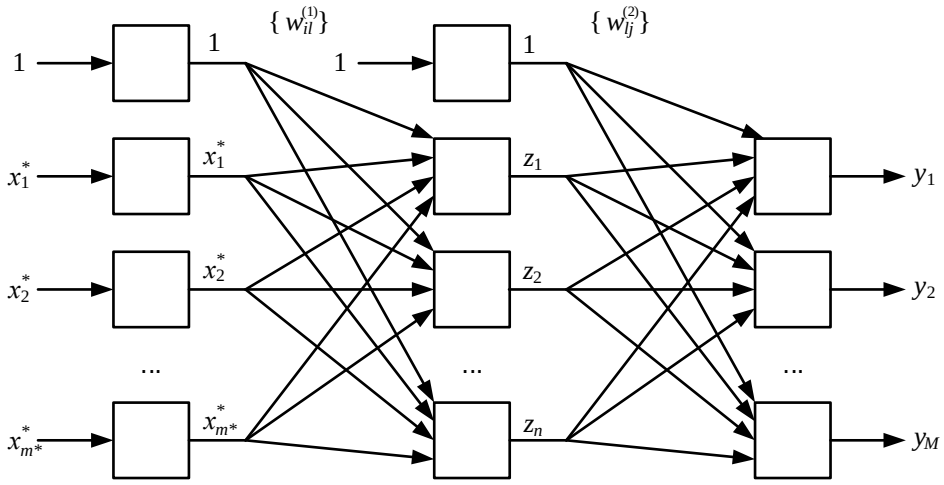

Рисунок 2.6 – Структурна схема тришарового персептрону

Вихідні значення нейронів прихованого та вихідного прошарків обчислюються за такими рівняннями:

$$z_l = f\left(\sum_{i=1}^{m^*} w_{il}^{(1)} x_i^* + w_{0l}^{(1)}\right), l = 1, 2, \dots, n \tag{2.7}$$

$$y_j = f\left(\sum_{l=1}^{n} w_{lj}^{(2)} z_l + w_{0j}^{(2)}\right), j = 1, 2, \dots, M \tag{2.8}$$

де $f(s)$ нелінійна передатна функція нейрона; $\left\{w_{il}^{(1)}\right\}$ і $\left\{w_{lj}^{(2)}\right\}$ - матриці ваг синаптичних зв'язків; $\left\{w_{0l}^{(1)}\right\}$ і $\left\{w_{0j}^{(2)}\right\}$ - зміщення. Варіанти завдання передатної

функцій $f(s)$ у вигляді порогової (логічної) (рис. 2.7 а,в), сігмоідной функції (рис. 2.7 б) або функції у вигляді гіперболічного тангенсу (рис. 2.7 г).

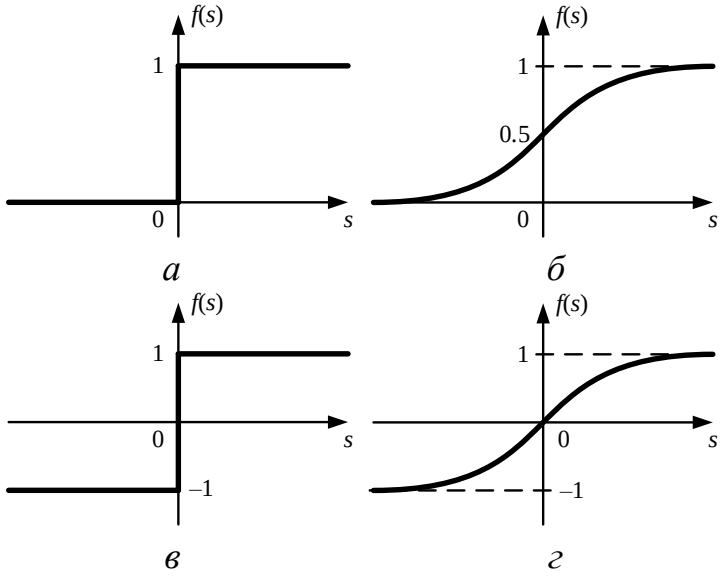

Рисунок 2.7 – Передатні функції: а) порогова (логічна), б) сігмоїдна, в) порогова; г) у вигляді гіперболічного тангенсу

Нехай, що є деяка навчальна вибірка

$$\left\{\begin{array}{c}\left(\left(x^*_{1,1}, x^*_{2,1}, \dots, x^*_{m^*,1}\right)^T; \left(d_{1,1}, d_{2,1}, \dots, d_{M,1}\right)^T\right); \\ \left(\left(x^*_{1,2}, x^*_{2,2}, \dots, x^*_{m^*,2}\right)^T; \left(d_{1,2}, d_{2,2}, \dots, d_{M,2}\right)^T\right); \\ \dots; \\ \left(\left(x^*_{1,T}, x^*_{2,T}, \dots, x^*_{m^*,T}\right)^T; \left(d_{1,T}, d_{2,T}, \dots, d_{M,T}\right)^T\right)\end{array}\right\}$$

складена з пар векторів де $x^*_t = \left(x^*_{1,t}, x^*_{2,t}, \dots, x^*_{m^*,t}\right)^T$ і $d_t = \left(d_{1,t}, d_{2,t}, \dots, d_{M,t}\right)^T$ - відповідно вхідний вектор і вектор бажаних вихідних реакцій мережі в t-му навчальному прикладі; T - число таких прикладів в навчальній вибірці. Зауважимо, що число навчальних прикладів має бути не менше числа класів розпізнавання ($T > M$), тобто в навчальну вибірку має входити принаймні по одному представнику (вектору ознак) кожного з класів розпізнавання.

Мета навчання НМ полягає в тому, щоб при поданні на входи мережі вектору ознак x^*_t, що належить k-му класу, вихідний сигнал НМ (тобто вектор

y_t) вказував би (у прийнятій кодуванні) номер цього класу. Процес навчання зводиться до вибору таких значень ваг $\left\{w_{il}^{(1)}\right\}$ і $\left\{w_{lj}^{(2)}\right\}$, де $i = 0,1,\dots,m^*$, $l = 0,1,\dots,n$, $j = 1,\dots,M$ які мінімізують сумарну квадратичну помилку мережі.

$$E = \sum_{t=1}^{T}\left(\sum_{j=1}^{M}\left(d_{j,t} - y_{j,t}\right)^2\right) \tag{2.9}$$

де $y_{j,t}$ і $d_{j,t}$- фактичне і бажане значення j-го виходу мережі для t-го прикладу з навчальної вибірки. Найбільш простим (але не найкращим) є градієнтний алгоритм навчання НМ, відповідно до якого настройка ваг мережі здійснюється за правилом

$$\begin{aligned} w_{il}^{(1)}(k+1) &= w_{il}^{(1)}(k) - \eta\frac{\partial E(k)}{\partial w_{il}^{(1)}(k)} \\ w_{lj}^{(2)}(k+1) &= w_{lj}^{(2)}(k) - \eta\frac{\partial E(k)}{\partial w_{lj}^{(2)}(k)} \end{aligned} \tag{2.10}$$

де $\frac{\partial E(k)}{\partial w_{il}^{(1)}(k)}$ та $\frac{\partial E(k)}{\partial w_{lj}^{(2)}(k)}$ частинна похідні помилки навчання E по вагам $w_{il}^{(1)}$ та $w_{lj}^{(2)}$, $k = 0,1,2,\dots$ – дискретний час (крок навчання). Якість навчання вважається прийнятною, якщо помилка навчання приймає досить малі значення ($E = 10^{-3}\dots 10^{-4}$). Зауважимо, що оскільки в процесі навчання НМ «запам'ятала» біометричні образи всіх поданих в начальній вибірці представників M класів користувачів, то навчена НМ одночасно з вирішальним правилом виконує функцію зберігання відповідних біометричних еталонів (рис. 3.5).

Доведено, що персептрон з одним прихованим шаром (рис. 3.6) і пороговою передатною функцією нейронів (рис. 3.7, а) здатен за кінцеве число кроків вирішити задачу формування вирішального правила для M довільних класів за допомогою M роздільних гіперплощин в m-вимірному просторі ознак в тому випадку, якщо ці класи представлені опуклими обмеженими областями.

Безпомилкове вирішальне правило можливо, якщо такі класи не перетинаються (рис. 3.3, а). В загальному випадку, помилка вирішального правила залежить тільки від ступеня перетину класів. Наприклад, при використанні сігмоїдної передатної функції (рис. 3.7, б) і двох прихованих шарів, за допомогою персептрона можливе формування із заданою похибкою будь-яких опуклих областей в просторі ознак, а додаванні третього прихованого шару - областей будь-якої складності, в тому числі і неопуклого форми.

Основні труднощі, що виникають при навчанні НМ:

- наявність локальних мінімумів цільової функції E - призводить до «зависання» процесу пошуку в «пастках» («лакунах»);
- шум у вхідних даних - призводить до зміни напрямку пошуку, і в кінцевому підсумку, до суттєвого його уповільнення;
- помилки класифікації - виникають внаслідок близькості (перетину) образів сусідніх класів розпізнавання;
- «прокляття розмірності» - при збільшенні числа ваг, що налаштовуються, обчислювальні витрати на пошук їх оптимальних значень ростуть експоненційно.

На сьогодні відомо більше сотні різних алгоритмів навчання НМ, що ставлять собі за мету в тій чи іншій мірі уникнути вказаних труднощів. Одним із способів скорочення часу навчання НМ є застосування «швидких» алгоритмів навчання, заснованих на процедурі обчислення ваг мережі з попередньої декореляції (ортогоналізації) її вхідних даних.

Крім багатошарових персептронов, в даний час ведуться активні дослідження щодо застосування ряду інших архітектур НМ для вирішення завдань біометричної ідентифікації:

- модулярні НМ (Modular neural networks);
- машини опорних векторів (Vector Support Machines);
- згорткові НМ (Convolutional networks);

- вейвлет-мережі (Wavelet networks);
- асоціативні НМ (Associative networks);
- карти Кохонена, що самоорганізуються (Self-organizing maps, SOM);
- радіально-базисні мережі (Radial-Basis Function networks, RBFN);
- сигма-пі НМ (Σ-П neural networks) тощо.

3 ІНФОРМАЦІЙНЕ І ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ГРАФІЧНОЇ АУТЕНТИФІКАЦІЇ

3.1 Формування вхідних даних

Оптимізацію параметрів навчання системи графічної аутентифікації будемо проводити загального випадку, коли алфавіт класів складається з трьох і більше класів. Кожна реалізація в навчальній матриці представляє собою геометричний опис траєкторії, за якою переміщується перо при формуванні графічних паролів (рис. 3.1). Таким чином, в навчальній матриці фіксуються послідовність координат точок такої траєкторії.

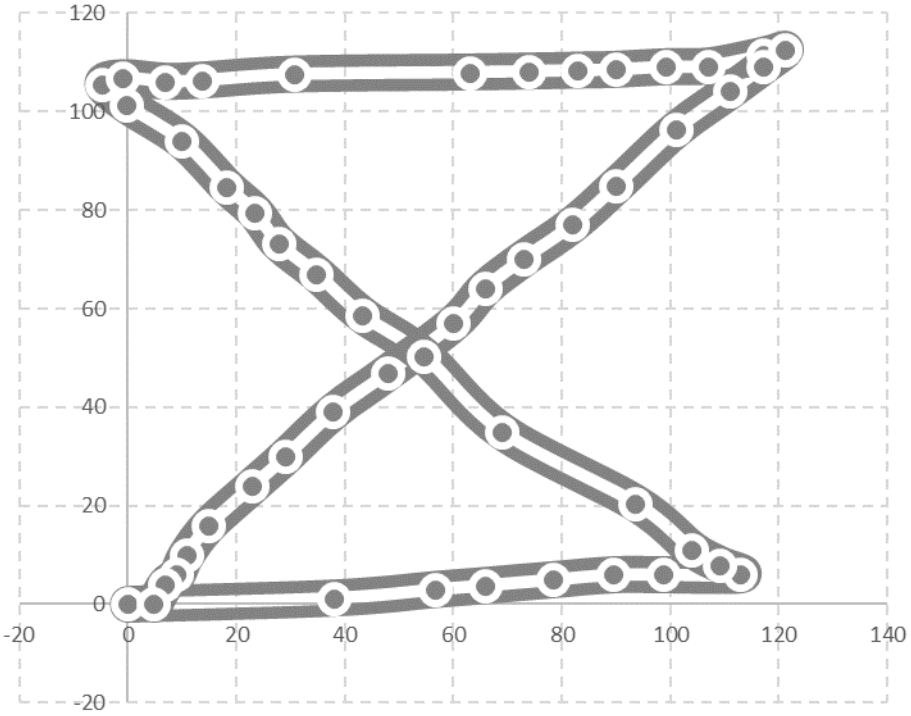

Рисунок 3.1 – Формування реалізації навчальної матриці за динамікою відтворення графічного паролю

На рис. 3.1. темна суцільна лінія відображає підпис, а круги – точки, координати яких увійдуть до навчальної матиці. При цьому координати першої

точки графічного паролю будемо вважати (0; 0). Навчальні матриці в графічних паролів різних користувачів повинні містити однакову кількість ознак розпізнавання для віх класів, то кількість точок, координати яких будуть відображатися в начальній матриці буде однакова. В роботі використовується 50 таких точок. При цьому навчальну матрицю умовно можна розділити на дві частини: таку, що зберігає перші координати точок, та таку, що зберігає другі координати. Таким чином, кількість ознак розпізнавання в навчальній матриці складає 100. Іншим параметром навчальної вибірки є кількість реалізації, тобто прикладів графічного паролю одного користувача. В роботі формувалися 40 таких реалізацій. Для прискорення процесу формування навчальної матриці кожний графічний пароль вводиться в одному екземплярі. Інші реалізації формуються автоматично шляхом часткової незначної зміни координат точок, сформованих за першою реалізацією. Приклад реалізації сформованої автоматично наведено на рис. 3.2.

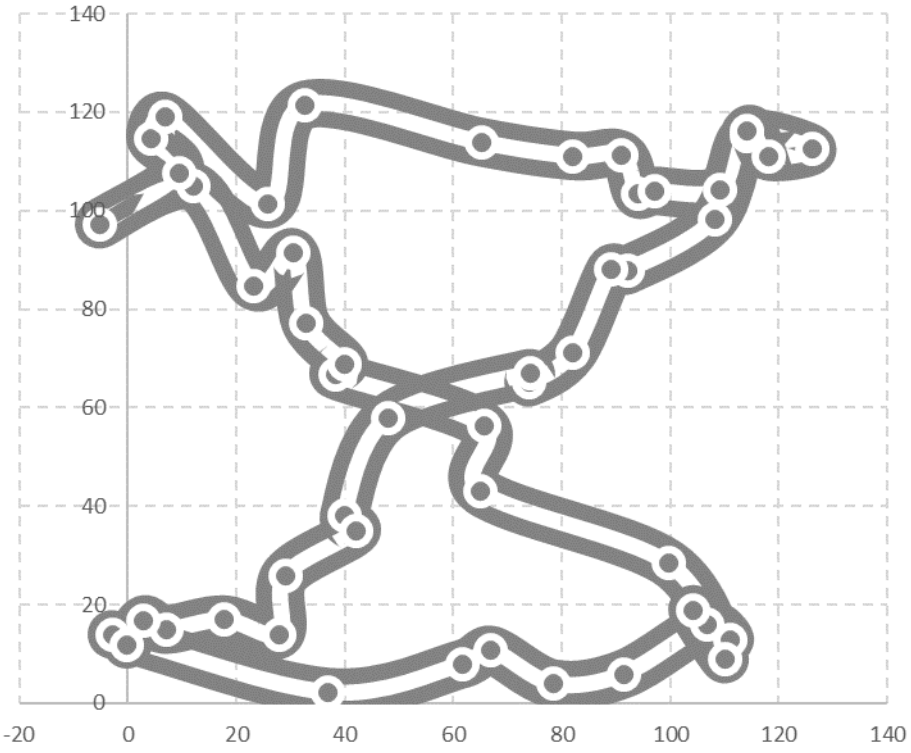

Рисунок 3.2 – Реалізація навчальної матриці, сформована автоматично за зображенням графічного паролю на рис. 3.1

3.2 Програмна реалізація

Найбільш зручним та доступним інструментом створення нейронних мереж являється набір програмних рішень MATLAB. Система MATLAB (матрична лабораторія) була створена спеціалістами фірми Math Works, Inc. як мову програмування високого рівня для технічних обчислень. Найважливішою перевагою системи MATLAB є можливість її розширення нових науково-технічних завдань. Однак якщо в самій системі MATLAB вже опубліковано ряд відомих книг, то книг по пакетах розширення все ще дуже мало. Завдання зі створення та навчанню нейромереж в MATLAB покладені на пакет розширення NNTool (NeuralNetworkToolbox). Пакет фірми "TheMathWorks" MATLAB надає користувачам можливість роботи з нейронними мережами. Входить в стандартну поставку MATLAB тулбокс надає широкі можливості для роботи з нейронними мережами усіх типів. Використання "NeuralNetworkToolbox" спільно з іншими засобами MATLAB відкриває широкий простір для ефективного комплексного використання сучасних математичних методів для вирішення найрізноманітніших завдань прикладного та наукового характеру. В даний час доступна версія 4.0 "NeuralNetworkToolbox", що поставляється в складі MATLAB 6.0.При розробці NeuralNetworkToolbox використано принципи об'єктно-орієнтованого програмування. Основний об'єкт - нейронна мережа. Властивості нейромережі визначають масиви осередків структур, які визначають кожен з входів мережі, шари, виходи, еталони, зміщення і ваги:

• Входи - містить структури властивостей для кожного з входів мережі. net.inputs - матриця Ni x1 осередків вхідних структур, де Ni-число входів мережі (net.numInputs). Структура, що визначає властивості і-го мережевого входу, визначена в: net.inputs {i}.

• Шари - layers - містить структури властивостей для кожного з шарів мережі. net.layers - масив Ni x1 осередків вхідних структур, де Ni-число шарів

мережі (net.numLayers). Структура, що визначає властивості і-го шару визначена в: net.layers {i}.

• Виходи - outputs - містить структури властивостей для кожного з виходів мережі. net.outputs - масив 1xNi осередків вхідних структур, де Ni-число шарів мережі (net.numLayers). Структура, що визначає властивості і-го виходу, визначена в: net.outputs {i} якщо відповідне вихідна сполука net.outputConnect (i) - 1 (або 0):

• Еталони - targets - містить структури властивостей для кожного з еталонів мережі. net.targets - масив 1xNi осередків вхідних структур, де Ni-число шарів мережі (net.numLayers). Структура, що визначає властивості еталона пов'язаного з і-им шаром (або нульова матриця) визначена в: net.targets {i} якщо відповідне вихідна сполука net.targetConnect (i) - 1 (або 0).

• Зміщення - biases - містить структури властивостей для кожного з зміщень мережі. net.biases - масив Nix1 осередків, де Ni-число шарів мережі (net.numLayers). Структура, що визначає властивості зміщень і-го шару (або нульова матриця) розташована в: net.biases {i} якщо відповідне з'єднання для зміщення net.biasConnect (i) - 1 (або 0).

• Вхідні ваги - inputWeights - містить структури властивостей для кожного з вхідних ваг. net.inputWeights - масив NlxNi осередків, де Nl-число шарів мережі (net.numLayers), а Ni - число входів мережі (net.numInputs). Структура, що визначає властивості ваг до і-му шару від j го шару (або нульова матриця) визначена в: net.inputWeights {i, j}, якщо відповідне з'єднання входу net.inputConnect (i, j) - 1 (або 0).

• Веса шарів - layerWeights - містить структури властивостей для кожного з ваг шару мережі. net.layerWeights - масив NlxNl осередків, де Nl-число шарів мережі (net.numLayers). Структура, що визначає властивості зв'язків і-го шару з j м шаром (або нульова матриця) визначена в: net.layerWeights {i, j}, якщо відповідна зв'язок шару net.layerConnect (i, j) - 1 (або 0).Для зміни властивостей

даний підструктур в MATLAB реалізовано більше 150 функцій, які утворюють своєрідну макромову програмування, дозволяючи створювати, навчати і використовувати різноманітні нейромережі.Розглянемо m-сценарій, в якому використовуються функції, пов'язані із застосуванням мереж зустрічного поширення для вирішення задачі класифікації функціональних станів технологічного процесу.Попередньо необхідно сформувати навчальну матрицю і задати вектор рядок приналежності кожного вектора-реалізації до певного класу.

Спочатку потрібно сформувати навчальну матрицю і задати вектор рядок належності кожного вектора-реалізації до певного класу. Навчальні матриці були завантажені з файлів 1.txt, 2.txt, 3.txt, 4.txt, 5.txt та 6.txt, що містили 40 рядків з 100 значень ознак реалізацій кожного графічного паролю відповідно.

```
n=100;
N=40;
m=5;
P=[];
for k=1:6
fid = fopen(strcat(int2str(k),'.txt'));
a= fscanf(fid, '%g');
x=reshape(a,N,n)';
P=[P x];
T(1+N*(k-1):N*k)=k;
fclose(fid);
end;
```

Для зчитування з файлу використовується функція `fscanf()`, до параметрів якої належать ідентифікатор файлу з даними, шаблон рядку даних, розмірність вихідного масиву.

Крім того застосовувалася функція `reshape()`, за допомогою якої виконувалось перетворення одномірних масивів на двовимірні.

Після зчитування виконуємо формування навчальної матриці та вихідного вектору за допомогою стандартних матричних операцій і MATLAB.

```
P=[P x];
T(1+N*(k-1):N*k)=k;
```

В роботі проводилося перетворення вектору бажаних вихідних сигналів T на матрицю, кожен стовпчик якої містив п’ять нулів і одну одиницю, що відповідала номеру графічного пароля *k*.

Створення штучної нейромережіnet виконується за допомогою команди:

```
net = newnnn (P1,P2,…PL),
```

де newnnn – тип штучної нейромережі; P1,…,PL – параметри штучної нейромережі.

В даній роботі використовується штучної нейромережі типа багатошаровий перцептрон, який створюється за допомогою команди команди:

```
net = newff (R, [A1 A2 … AL], {F1 F2 … FL}, BTF, PF),
```

де `R` - масив мінімальних і максимальних значень входних нейронів (ознак);

`Ai` - число нейронів і-го шару, починаючи з першого прихованого прошарку, $i = 1,\ldots,L$;

`Fi` - функція активації нейронів і-го прошарку, за замовчанням ‘tansig’;

`BTF` - функція навчання мережі, за замовчанням ‘trainlm’;

PF - критерій зупину, за замовчанням ‘mse’ (мінімум середньо квадратичного відхілення).

В роботі формування нейромережі виконувалося створюється за допомогою даної команди з такими параметрами.

```
net=newff(minmax(P),[hid_neuton m],{'logsig' 'logsig' });
```

Додаткові параметри, що задаються при створенні мережі:

net.performFcn=’msereg’ - навчання штучної нейромережі виконується за методом регуляризації;

net.performParam.ratio=0.1 - значення параметру регуляризації;

net.trainParam.show=1- число епох, після виконання яких виводяться параметри навчання;

net.trainParam.epochs=100 - максимальне число епох при навчанні мережі;

net.trainParam.goal=0.02 - значення цільової функції, при досягненні якого процес навчання зупиняється.

Процес навчання штучної нейромережі виконується командою:

```
net = train (net, P, t)
```

Для розв’язання задач класифыкацыйного прогнозування рекомендується використовувати тришарову штучну нейромережу (один прихований прошарок) з числом нейронів:

N= 100 - у вхідному прошарку;

A1=6 - у прихованому прошарку;

A2=6 - у вихідному прошарку.

Робота штучної нейромережі, тобто формування вихідного сигналу Y при вхідному X[N,1] виконується командою:

```
y = sim (net, P).
```

Для випадку, коли вихідний сигнал приймає цілочисельні значення, рекомендується використовувати округлення

```
y = round (sim (net, P)).
```

На рис. 3.2 представлена архітектура нейромережі зворотного розподілу, яка була сформована в роботі.

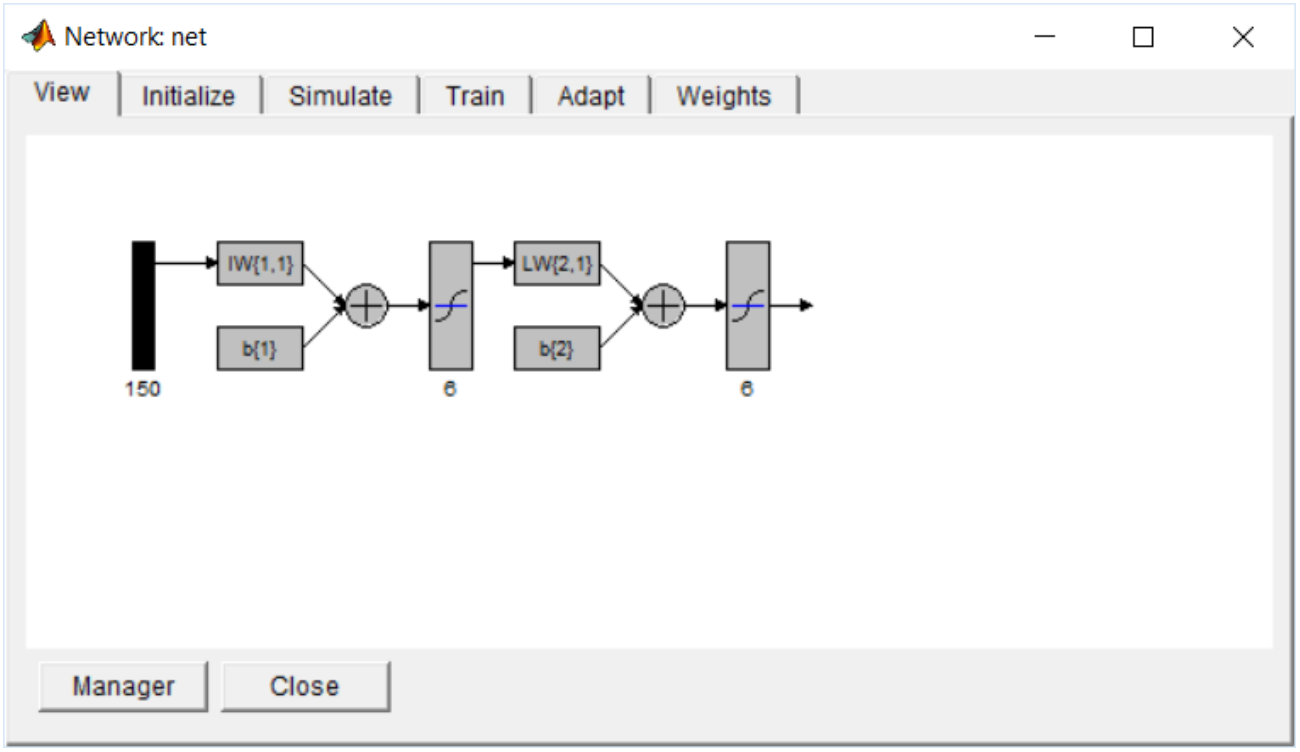

Рисунок 3.2 – Архітектура нейромережі зворотного розподілу

Достовірність одержаних результатів перевіряємо шляхом порівняння вихідних сигналів нейромережі `y` з вектором бажаних сигналів `t`

```
num1=find(T==1);
num0=find(T==0);
tx(1,:)=[mean(y(num1)==T(num1)) mean(y(num0)==T(num0))];
```

Повний код програми наведено в додатку.

3.3 Аналіз результатів

Спочатку виконаємо навчання нейронмережі зворотного розповсюдження помилки з використанням параметрів, що задаються в середовищі MATLAB для такого типу нейромереж за замовчуванням.
На рис. 3.3 наведено графік динаміки зміни значення середньоквадратичної помилки в процесі навчання нейромережі з такими параметрами та передатною функцією нейронів прихованого та вихідного прошарку у вигляді гіперболічного тангенса:

$$f(s) = tansig(s) = \frac{2}{(1 - e^{-2s})} - 1$$

де s – результат роботи суматора штучного нейрону.

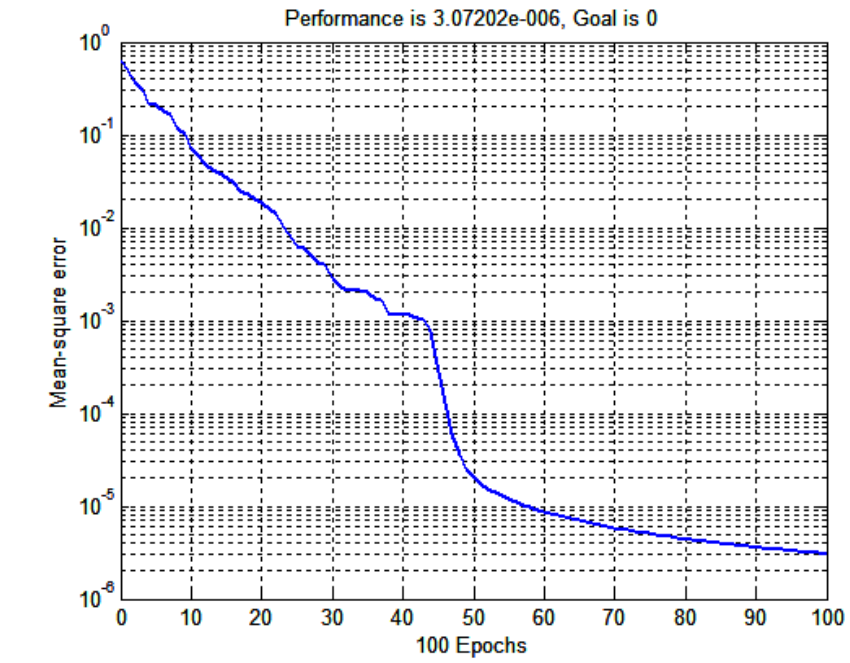

Рисунок 3.3 – Динаміка зміни значення середньоквадратичної помилки при навчанні штучної нейромержі з передатною функцією у вигляді гіперболічного тангенсу

Аналіз рис. 3.3 показує, що значення середньоквадратичної помилки складає E=0,000003. При цьому точність розпізнавання складає 100%

ВИСНОВКИ

В ході виконання роботи було розроблено системи графічної аутентифікації з використанням штучних нейронних мереж, що здатні автоматизувати обидва вказаних процеси збереження і перевірки графічних паролів. При цьому виконано такі завдання:

1) Сформовано вхідний математичний опис інтелектуальної системи графічної аутентифікації;
2) Обрано тип нейромережі та визначено структуру і функціональні параметри її елементів;
3) Обрано критерій якості навчання нейромережі.
4) Розроблено та програмно реалізовано алгоритм навчання нейромержі.
5) Перевірнгл працездатність розробленої системи на задачі збереження та перевірки п’яти графічних паролів.

СПИСОК ЛІТЕРАТУРИ

[1] Holger Reibold. Android Forensik kompakt: Der praxisorientierte Einstieg in die Welt der digitalen Forensik von Android-Geräten Янв.. 2016;

[2] Scott Augenbaum. The Secret to Cybersecurity: A Simple Plan to Protect Your Family and Business from Cybercrime Forefront Books 29 Jan 2019

[3] Alan T. Norman. Computer Hacking Beginners Guide - How to Hack Wireless Network, Basic Security and Penetration Testing, Kali Linux, Your First Hack [1 ed.] Independently published 24.Februar 2015

[4] Jennifer Golbeck.The Great Courses. Taking Control of Your Personal Data [1138]. The Teaching Company 2020 year

[5] Graeme Edwards. Cybercrime Investigators Handbook, John Wiley & Sons 2020

[6] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano. ―The quest to replace passwords: a framework comparative evaluation of web authentication schemes. In IEEE Symposium on Security and Privacy, 2012

[7] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," Communications of the ACM, vol. 33, pp. 168-176, 2000.

[8] R. N. Shepard, "Recognition memory for words, sentences, and pictures," Journal of Verbal Learning and Verbal Behavior, vol. 6, pp. 156-163, 2018

[9] S. Saeed and M. S. Umar. ―A hybrid graphical user authentication scheme.‖ In Communication, Control and Intelligent Systems (CCIS), (pp. 411-415). IEEE. November, 2015.

[10] P. Dunphy, A. P Heiner, and N Asokan. "A closer look at recognition based graphical passwords on mobile devices". In Proceedings of the Sixth Symposium on Usable Privacy and Security (p. 3). ACM, July, 2010.

[11] C. Singh and L. Singh "Investigating the Combination of Text and Graphical Passwords for a more secure and usable experience". International Journal of Network Security & Its Applications (IJNSA), 3(2), March 2011.
[12] S. Chowdhury, R. Poet and L. Mackenzie. "A study of mnemonic image passwords." In Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on, pp. 207-214. IEEE, 2014.
[13] E. Hayashi, R Dhamija, N. Christin, and A. Perrig. "Use your illusion: secure authentication usable anywhere". In Proceedings of the 4th Symposium on Usable Privacy and Security (pp. 35-45). ACM, July, 2018.
[14] B. Coskun and C. Herley ―Can "Something You Know" Be Saved?‖ In ISC (Vol. 8, pp. 421-440). September, 2008.

ДОДАТОК

```
clear;
n=150;
N=40;
% Nt=round(N*0.8);
Nt=N;
% Ne=N-Nt;
Ne=N;
m=6;
P=[];
Ex=[];
tf=cells(1,11);
tf{1}='tansig';
tf{2}='logsig';
tf{3}='purelin';
for k=1:m
fid = fopen(strcat(int2str(k),'.txt'));
a= fscanf(fid, '%g');
x=reshape(a,N,n)';
%P=[P x(1:100,1:Nt)];
P=[P x(:,1:Nt)];
%Ex=[Ex x(1:100,Nt+1:end)];
Ex=[Ex x(:,1:Ne)];
t(1+Nt*(k-1):Nt*k)=k;
tEx(1+Ne*(k-1):Ne*k)=k;
fclose(fid);
end;
T=ind2vec(t);
% a=min(P')';
% b=max(P')';
% for i=1:m*n
%     P(:,i)=(P(:,i)-a)./(b-a);
% end;

for i=1:1
    for j=1:1
net=newff(minmax(P),[6 k],{tf{i} tf{j}});

  net.trainParam.epochs=100;
  net.trainParam.show=1;
  net=train(net,P,T);
    Y=(sim(net,P));
    e_new=mse(Y-T);
    Y=(sim(net,Ex));
for kk=1:m*Ne
```

```
  tmp=find(Y(:,kk)==max(Y(:,kk)));
  y(kk)=tmp(1);
end;

     e(i,j)=e_new;
     e2(i,j)=mean(y==tEx);
     for k=1:m
         num1=find(tEx==k);
         num0=find(tEx~=k);
     tx(i,j,k,:)=[mean(y(num1)==k) mean(y(num0)==k)]
 end;
end;
end;
rez=[];
for k=1:m
rez=[rez; tx(1,1,k,1) tx(1,1,k,2)];
end;
rez
```