МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра комп'ютерних наук

БОВА Костянтин Валерійович

Методи та засоби ідентифікації користувачів у системах дистанційного навчання / Methods and Tools of Users Identification in Distance Learning Systems

спеціальність: 121 - Інженерія програмного забезпечення
освітньо-професійна програма - Інженерія програмного забезпечення

Кваліфікаційна робота

Виконав студент групи ІПЗм-21
К. В. Бова

Науковий керівник:
д.т.н., доцент, А. В. Пукас

Кваліфікаційну роботу
допущено до захисту:

"___" _____ 20___ р.

Завідувач кафедри
_____ **А. В. Пукас**

ТЕРНОПІЛЬ - 2022

ВСТУП

Актуальність. Сьогодні актуальним є питання якості знань, отриманих за допомогою технологій дистанційної освіти. При очній формі навчання більшість викладачів веде облік відвідуваності студентів. З переходом на дистанційну освіту (ОД) кількість студентів збільшується в рази, і відслідковувати відвідуваність студентів важко.

Сучасні біометричні інформаційні системи та технології ідентифікують людей за їх анатомічними ознаками (відбитки пальців, риси обличчя, рисунок долоні, райдужна оболонка ока, голос) або особливостями поведінки (підпис, хода).

Оскільки ці атрибути фізично пов’язані з користувачем, біометрія надійно діє як механізм, який гарантує, що тільки ті, хто має необхідні облікові дані, можуть отримати доступ до комп’ютерної системи.

Біометричні інформаційні системи також мають унікальні переваги - вони не дозволяють відмовити в ідеальній транзакції та можуть бути визначені, коли особа використовує кілька документів (наприклад, паспортів) на різні імена. Тому при грамотній реалізації у відповідних додатках система ідентифікації людини за біометричними параметрами забезпечує високий рівень безпеки.

Робочий зв'язок з науковими програмами, планами, темами

Напрямок дослідження безпосередньо пов’язаний з науковим напрямком кафедри «Комп’ютерні науки» Тернопільського національного економічного університету.

Мета та завдання дослідження. Метою роботи є дослідження залежностей між окремими біометричними параметрами особи для її унікальної ідентифікації в системах дистанційного навчання, розробка відповідних методів, моделей та програмних засобів для підвищення безпеки інформаційних ресурсів від несанкціонованого доступу в цілому.

Основними завданнями дослідження є:

- дослідження проблеми ідентифікації користувача в системах дистанційного навчання;
- аналіз відомих методів ідентифікації користувачів у системах дистанційного навчання ;
- розробити бімодальну систему ідентифікації користувача на основі розпізнавання голосу та розпізнавання обличчя ;
- розробити алгоритми та реалізувати програмні методи створення стандартів біометричної ідентифікації користувачів у системах дистанційного навчання.
- розробити веб-додаток для реалізації ідентифікації користувачів у системах дистанційного навчання ;

Мета та зміст дослідження. Метою дослідження є процес ідентифікації користувача в системах дистанційного навчання . Це предмет дослідження методи та засоби ідентифікації користувачів у системах дистанційного навчання .

Методи дослідження . Теоретичні дослідження базуються на застосуванні системного аналізу, методології функціонального моделювання, інженерії знань, штучного інтелекту, теорії розпізнавання зображень, теорії графів, теорії нечіткого висновку, теорії алгоритмів та об'єктно-орієнтованого проектування.

Наукова новизна про отримані результати. Бімодальна архітектура розпізнавання користувачів покращена за допомогою розпізнавання голосу та обличчя, яке використовує метод посилання на обличчя шляхом поєднання методу Віоли-Джонса, півтонів і фільтра Собеля .

Практичне значення отриманих результатів полягає в наступному : запропонований підхід може бути інтегрований у відомі системи дистанційного навчання для ідентифікації користувачів , які знаходяться в процесі організації навчання .

Особистий внесок магістранта . Усі результати були отримані автором самостійно.

РОЗДІЛ 1
АСПЕКТИ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ У СИСТЕМАХ ОСВІТИ

1.1. Проблема ідентифікації користувача в системах дистанційного навчання.

Сьогодні актуальним є питання якості знань, отриманих за допомогою технологій дистанційної освіти. При очній формі навчання більшість викладачів веде облік відвідуваності студентів. З переходом на дистанційну освіту (ОД) кількість студентів збільшується в рази, і відслідковувати відвідуваність студентів важко. ДО висуває певні вимоги до психологічних особливостей учня:

- перш за все, він повинен мати високу і стійку мотивацію до здобуття освіти;

- по-друге, студент повинен чітко представити бажаний результат навчання.

- по-третє, він повинен розуміти, що несе відповідальність за інформацію, отриману за допомогою SDN. Говорити про те, що люди з такими психологічними даними сьогодні підуть на дистанційну освіту, неможливо. Більшість людей в Україні вчаться заради того, щоб отримати диплом. Для багатьох твердження про те, що дистанційна освіта дає безкоштовний графік навчання, асоціюється з вільним доступом до сервера SDN. У зв’язку з цим існує ймовірність того, що студент може сидіти за комп’ютером під час тестування, а не хтось, хто знає більше про предмет. Навчальній системі віддаленої навігації потрібно перевірити, чи насправді віддалений комп’ютер навчається, як він прикидається, ідентифікувати користувача.

Те, як ця проблема вирішується сьогодні, потребує подальших досліджень. Кожен вступник на навчання в системі дистанційної освіти отримує свій логін і пароль для доступу до сервера з навчальними матеріалами.

Коли учень отримує доступ до сервера, про нього може бути зібрана інформація, яка буде корисна вчителю:

- перелік сторінок, відвіданих користувачем під час робочого сеансу;
- час, витрачений на кожну сторінку;
- активоване гіперпосилання на цій сторінці;
- список файлів, скопійованих користувачем з освітнього сервера;
- час випробування;
- тощо

Якщо необхідно, адміністратор сервера системи дистанційного навчання може використовувати інформацію для відновлення будь-якого екземпляра будь-якого робочого сеансу студента.

Але вся інформація, зібрана таким чином, є непрямою. Тобто, якщо людина зайшла в систему під логіном і паролем свого колеги, щоб виділитися і взяти участь у тестуванні, то вона не може бути виявлена. Іншими словами, нам потрібні прямі докази того, що тренувальну сесію дійсно проводив користувач, чиє ім’я збігається з логіном і паролем.

Є два шляхи вирішення цієї проблеми. Перший спосіб заснований на використанні додаткового обладнання, він найнадійніший, але пов'язаний з додатковими витратами, яких сьогодні, мабуть, не понесе жодна система дистанційної освіти, хоча все залежить від того, наскільки студент «відповідальний». "за знання. отримує.

Додаткове обладнання дозволяє перевірити біометричні характеристики людини:

- відбиток пальця;
- ручна геометрія;
- райдужка ока;
- сітківка ока;
- людський голос;
- геометрія людини.

Питанням часу є те, чи буде один із цих біометричних параметрів використовуватися для ідентифікації в системах дистанційного навчання, але сьогодні можна виділити найбільш надійні та доступні методи ідентифікації з цієї групи.

1.2. Біометричні ідентифікаційні характеристики.

Біометричні технології ідентифікації особистості мають глибоке історичне коріння, засновані на ідентифікації людини за зовнішніми морфологічними ознаками. Люди не здатні впізнавати один одного за зовнішнім виглядом, голосом, запахом тощо. або базова біометрична ідентифікація.

В даний час технології біометричної ідентифікації поділяються на дві групи: статичні та динамічні.

Статичні технології засновані на унікальних фізіологічних особливостях людини. До них відносяться такі методи [3, 4]:

1) за відбитком пальця. Найпоширеніший біометричний метод ідентифікації, цей метод заснований на унікальності папілярних візерунків на пальцях для кожної людини. Зображення відбитка пальця, отримане спеціальним сканером, буде перетворено в цифровий код (пломбу) і порівняно з попередньо поданим шаблоном (стандартом) або набором шаблонів (у разі ідентифікації).

2) за формою долоні. Цей метод заснований на розпізнаванні геометрії руки. За допомогою спеціального приладу, який дозволяє отримати тривимірне зображення руки, отримують необхідні розміри для унікального цифрового згортку, що ідентифікує особу.

3) за місцем розташування вен на тильній стороні долоні. За допомогою інфрачервоної камери зчитується малюнок вен на тильній стороні долоні або кисті, обробляється отримане зображення і створюється цифрова згортка за схемою розташування вен.

4) за сітківкою. Швидше, це метод розпізнавання за малюнком кровоносних судин очного дна. Щоб знімок був видимим, людина повинна дивитися на віддалену точку світла, а освітлене таким чином очне дно сканується спеціальною камерою.

5) за журналом. Метод заснований на унікальності малюнка райдужної оболонки ока. Для реалізації методу необхідна спеціальна камера та відповідне програмне забезпечення, яке дозволяє витягти з отриманого зображення малюнок райдужної оболонки ока, на основі якого будується цифровий код.

6) за формою особи. При такому способі ідентифікації створюється двовимірне або тривимірне зображення обличчя людини. За допомогою камери та спеціалізованого програмного забезпечення підсвічуються контури очей, брів, носа, губ тощо. на зображенні, і обчислюється відстань між ними. На основі цих даних робиться знімок, який перетворюється в цифрову форму для порівняння.

7) за термограмою людини. В основі цього методу лежить унікальність розподілу артерій на обличчі, які кровопостачають шкіру і віддають тепло. Для отримання зображень використовуються спеціальні інфрачервоні камери.

8) інші методи. Існують і такі унікальні методи, як ідентифікація за ДНК, кутикулою, формою вуха, запахом тіла тощо.

Динамічні методи базуються на поведінкових (динамічних) особливостях людини, тобто враховують особливості, що характеризують підсвідомі рухи в процесі відтворення будь-якої дії:

- з рукописним почерком. У цьому методі використовується підпис людини (іноді написання кодового слова). Цифровий код формується відповідно до динамічних характеристик письма, тобто будується згортка, яка містить інформацію про графічні параметри, часові характеристики підпису та динаміку тиску на поверхню тощо.

- з клавіатурним почерком. Спосіб подібний до описаного вище, але замість підпису використовується кодове слово. Основною характеристикою, на якій будується згортка, є динаміка набору кодових слів.

- голосом. Існує багато способів побудови коду розпізнавання голосу, як правило, це різна комбінація частотних і статистичних характеристик голосу.

- інші методи. Для цієї групи методів виконуються лише найпоширеніші з описаних вище, є унікальні методи, такі як розпізнавання по руху губ, по динаміці повороту ключа в дверному замку і т.д.

При всьому різноманітті біометричних методів в системах дистанційного навчання в основному використовуються три: ідентифікація за відбитками пальців, по зображенню людини (двовимірному або тривимірному - 2D або 3D фото) і по райдужній оболонці ока. Однак будь-який з них заснований на порівнянні даних відомого об'єкта з біометричним стандартом. Таке порівняння неможливе без запису та збереження біометричної інформації, тобто без її документування.

1.3. Аналіз відомих методів ідентифікації користувачів у системах дистанційного навчання.

Розглянемо більш детально методи, які можна використовувати в системах дистанційного навчання для ідентифікації користувачів. Сканування відбитків пальців є найстарішою з існуючих методик, але в той же час вона вважається однією з найбільш перспективних. Кожна людина має унікальний, незмінний відбиток пальця, доведений судово-медичною експертизою та підтверджений експертною практикою. Відбитки пальців зазвичай складаються з рельєфних ліній - папілярного малюнка, структура якого визначається шарами гребінчастих виступів шкіри, розділених борозенками. Ці лінії утворюють складні образи шкіри - дуги, петлі, завитки, які в цілому мають такі властивості, як: індивідуальність, стійкість, можливість переставлення (показано на рисунку 1.1).

Рис. 1.1. Розпізнавання відбитків пальців

Біометричні системи ідентифікації особи за відбитками пальців зазвичай мають дуже низький рівень відхилення об’єктів (система не розпізнає автентичність відбитка пальця зареєстрованого користувача), і існує певна ймовірність фальшивого або підробленого доступу до об’єкта (можливість того, що система «зробить» ідентифікувати" відбиток пальця помилково. користувач, який не зареєстрований у цій системі).

Системи розпізнавання облич. Усі основні типи технологій розпізнавання облич розроблені з метою пошуку потрібного контенту в режимі «один до багатьох», тобто визначення конкретного обличчя серед тисяч облич, записаних у базі даних. Якісні характеристики такої системи залежать від технологічних

можливостей відеокамер з роздільною здатністю не менше 320x240 пікселів на дюйм при швидкості відеопотоку не менше 3-5 кадрів в секунду, підключених до мережі з персональними комп'ютерами. Вища швидкість відеопотоку та краща здатність системи розподілу призведуть до кращої якості отриманої ідентифікації.

Існує три основні методи розпізнавання обличчя. Вони включають аналіз зображення для визначення характерних рис обличчя:

- аналіз «характерних рис обличчя» - найбільш поширених і найбільш придатних для зміни виразу обличчя;

- аналіз на основі «нейронних мереж» [9] — на основі порівняння «особливих точок», які можуть ідентифікувати обличчя в складних умовах;

- метод «автоматична обробка зображення обличчя» - для визначення дистанції та дистанції зв'язку між особливими ознаками за обличчям людини.

На малюнку 1.2 показано процес розпізнавання обличчя.

Рис. 1. 2 . Розпізнавання обличчя

Спосіб ідентифікації особи за геометрією руки за технологічною структурою та рівнем достовірності схожий на метод ідентифікації людини за відбитками пальців, але поки використовується рідко. Математична модель для ідентифікації людини таким чином вимагає дуже мало інформації – лише 9 байт. Це дозволяє зберігати великий обсяг необхідної інформації про людей, яких необхідно швидко ідентифікувати та розшукати. Найбільш інноваційним є

пристрій «Handkey», який сканує не лише внутрішню, а й зовнішню сторону долоні за допомогою вбудованої відеокамери.

Подібні системи, де можна сканувати інші ручні параметри, зараз розробляються такими компаніями, як VioMetRagtners, Ralmetrics і VTG. На малюнку 1.3 показано процес ідентифікації особи вручну.

Рис. 1.3. Ідентифікація людини за кистю руки

Для біометричних систем сканування сітківки ідентифікація відбувається за допомогою інфрачервоного світла низької інтенсивності, спрямованого через зіницю до кровоносних судин на задній стінці ока. Сканери сітківки ока зареєстрованих користувачів мають найнижчий відсоток забороненого доступу до об’єктів і майже повну відсутність помилок доступу. Проте імідж журналу має бути чітким. Одним із найперших і найнадійніших методів ідентифікації людини є використання малюнка кровоносних судин ока. Судини і артерії, які кровопостачають око, добре видно при освітленні зіниці ока зовнішнім джерелом світла.

Процедура ідентифікації людини зводиться до того, що людина всюди через спеціальний окуляр бачить віддалену світлову точку. При цьому око освітлюється інфрачервоними променями, які підсвічують мережу кровоносних судин, яка потім порівнюється зі стандартом. На малюнку 1.4 показано процес

розпізнавання на сітківці. Ця біометрична система ідентифікації має низьку пропускну здатність і досить дорога у використанні, але за рівнем надійності часто перевищує інші. Він поєднує в собі найкращі особливості ідентифікації за малюнком вен і основних точок розрізу

Рис. 1.4. Розпізнавання людини за сітківкою ока

Біометрична ідентифікація за почерком. Підпис є одним із класичних методів ідентифікації, який використовується вже кілька століть у юридичній практиці, банківській справі та торгівлі. Автор придумує власноручний підпис і практикується з вправами. Бажано, щоб підпис не повторював звичайне написання букв і мав додаткові елементи (штрихи, накладення букв тощо).

Існує два незалежних способи ідентифікації підпису:

- ідентифікація за нанесенням підпису на документі;

- ідентифікація за динамікою введеного в комп'ютер підпису.

У першому способі потрібно порівняти два зображення. Можна впоратися з цим краще. У другому способі є дані про коливання пера при відтворенні підпису в тривимірному просторі (X, Y - координати і Z - тиск на планшет). З цим може впоратися лише комп’ютер.

Біометрична ідентифікація з рукописним текстом на клавіатурі. Сучасні дослідження показують, що почерк користувача на клавіатурі має певну стійкість, що дозволяє досить однозначно ідентифікувати користувача.

Як вихідні дані використовуються інтервали часу між натисканням клавіш на клавіатурі та час їх утримання. При цьому часові інтервали між натисканнями характеризують швидкість роботи, а час утримання клавіш характеризує стиль роботи з клавіатурою - різкий удар або легке натискання.

Ідентифікація користувача за допомогою рукописного введення клавіатури можлива такими способами:

- три набори ключових фраз;

- набравши довільний текст.

Основна відмінність цих двох методів полягає в тому, що в першому випадку використовується ключова фраза, яку користувач встановлює під час реєстрації в системі (пароль), а в другому випадку використовуються ключові фрази, які генеруються. системою кожного разу, коли ідентифікується користувач. Передбачено 2 режими роботи: навчання та ідентифікація. На етапі навчання користувач певну кількість разів вводить запропоновані йому тестові фрази, розраховуються і запам'ятовуються еталонні характеристики конкретного користувача.

На етапі ідентифікації розраховані бали порівнюють з еталонними, на підставі чого роблять висновок щодо збігу або розбіжності параметрів почерку клавіатури. Дуже важливим кроком для нормального функціонування системи є вибір тексту, на якому система навчається. Фрази, пропоновані користувачеві, повинні бути підібрані таким чином, щоб використовувані в них символи повністю і рівномірно покривали робочу область клавіатури. У задачі ідентифікації користувача за рукописним текстом первинна обробка даних є важливим етапом. У результаті такої обробки вхідний потік даних розбивається на ряд елементів, які характеризують певні якості ідентифікованої особистості. У подальшому ці можливості дозволяють, за умови статистичної обробки, отримати деякі довідкові характеристики користувача.

Потім виділяється інформація, пов’язана з такими характеристиками користувача:

- кількість помилок друку;
- інтервали між натисканнями клавіш;
- час зберігання ключа;
- кількість перекриттів між ключами;
- ступінь аритмічності під час набору кадрів;
- швидкість набору

Біометрична ідентифікація з голосом. Існує багато способів побудови коду розпізнавання голосу, як правило, це різні комбінації частотних і статистичних характеристик голосу.

Одним із традиційних методів ідентифікації, який використовується повсюдно, є впізнання людини за голосом. Ви можете легко ідентифікувати співрозмовника по телефону, не бачачи його. Психологічний стан також можна визначити за емоційним станом голосу.

Так само, як розпізнавання голосу є безконтактним і не вимагає особливих зусиль з боку людини, ведуться роботи зі створення голосових замків і систем обмеження доступу до інформації.

1.4. Постановка проблеми дослідження

Сьогодні біометричні системи являють собою друге покоління систем безпеки, оскільки біометрія використовує вимірювання індивідуальних параметрів людини для її ідентифікації. Актуальність розвитку біометричної ідентичності людини зумовлена збільшенням кількості об’єктів та інформаційних потоків, які необхідно захищати від несанкціонованого доступу, де особливе місце займають системи дистанційного навчання.

Метою роботи є дослідження залежностей між окремими біометричними параметрами особи для її унікальної ідентифікації в системах дистанційного

навчання, розробка відповідних методів, моделей та програмних засобів для підвищення безпеки інформаційних ресурсів від несанкціонованого доступу в цілому.

Основними завданнями дослідження є:

- дослідження проблеми ідентифікації користувача в системах дистанційного навчання;
- аналіз відомих методів ідентифікації користувачів у системах дистанційного навчання ;
- розробити бімодальну систему ідентифікації користувача на основі розпізнавання голосу та розпізнавання обличчя ;
- розробити алгоритми та реалізувати програмні методи створення стандартів біометричної ідентифікації користувачів у системах дистанційного навчання.
- розробити веб-додаток для реалізації ідентифікації користувачів у системах дистанційного навчання.

Висновки до розділу 1

Аналізуючи основні методи ідентифікації, які існують на сьогодні, можна спрогнозувати, що програмні методи почнуть використовуватися в системах дистанційного навчання найближчим часом. Ці методи не вимагають додаткових витрат на придбання спеціального обладнання, вони цікаві для педагогіки тим, що аналізують психофізичний стан учня в даний момент часу. І сьогодні однією з найактуальніших проблем вищої освіти є психологічне обґрунтування організації індивідуального навчання в телекомунікаційному комп’ютерному освітньому середовищі. Тобто проблема верифікації за

допомогою психофізичних параметрів має багато спільних точок дотику з проблемою індивідуальних технологій навчання.

РОЗДІЛ 2
МАТЕМАТИЧНА МОДЕЛЬ СИСТЕМ, ВИЗНАЧЕНИХ КОРИСТУВАЧЕМ, У СИСТЕМАХ ДИСТАНЦІЙНОЇ ОСВІТИ

2.1. Подвійна система ідентифікації користувача

На основі аналізу сучасних біометричних систем ідентифікації людини запропоновано використовувати мультимодальну (бімодальну) систему ідентифікації, яка складається з двох характеристик: обличчя та голосу.

Мультимодальна система біометричної ідентифікації – це багатофакторна ідентифікація персоналу, яка складається з двох основних статичних частин:

1) ідентифікація за зображенням особи;

2) ідентифікація за допомогою парольної фрази.

Розпізнавання обличчя відбувається в режимі реального часу, коли ви піднімаєте або наближаєтеся до пристрою з камерою. Для реєстрації та ідентифікації достатньо трьох зображень.

Голосова ідентифікація базується на використанні статичної парольної фрази. На етапі реєстрації фразу необхідно повторити кілька разів, щоб досягти максимальної достовірності та оцінити варіацію вимови.

Мультимодальне рішення є узагальненням результатів, отриманих під час розпізнавання голосу та обличчя. Результатом обробки цього модуля є математичні ймовірності схожості Голосу та Обличчя еталонної вибірки користувача, що надійшла на вхід аудіо/відеопотоку. На основі цих значень розраховується мультимодальна ймовірність ідентифікації.

Прийняття рішення про доступ користувача відбувається за логічною схемою, яка враховує результати роботи всіх модулів системи ідентифікації.

Для оцінки точності будь-якої біометричної системи прийнято використовувати характеристичні криві: ROC (Receiver Operating Characteristic) або DET (Detection error comproise), які встановлюють зв'язок між помилками

FRR і FAR. Для мультимодального рішення ми отримуємо наступну криву DET (рисунок 2.1).

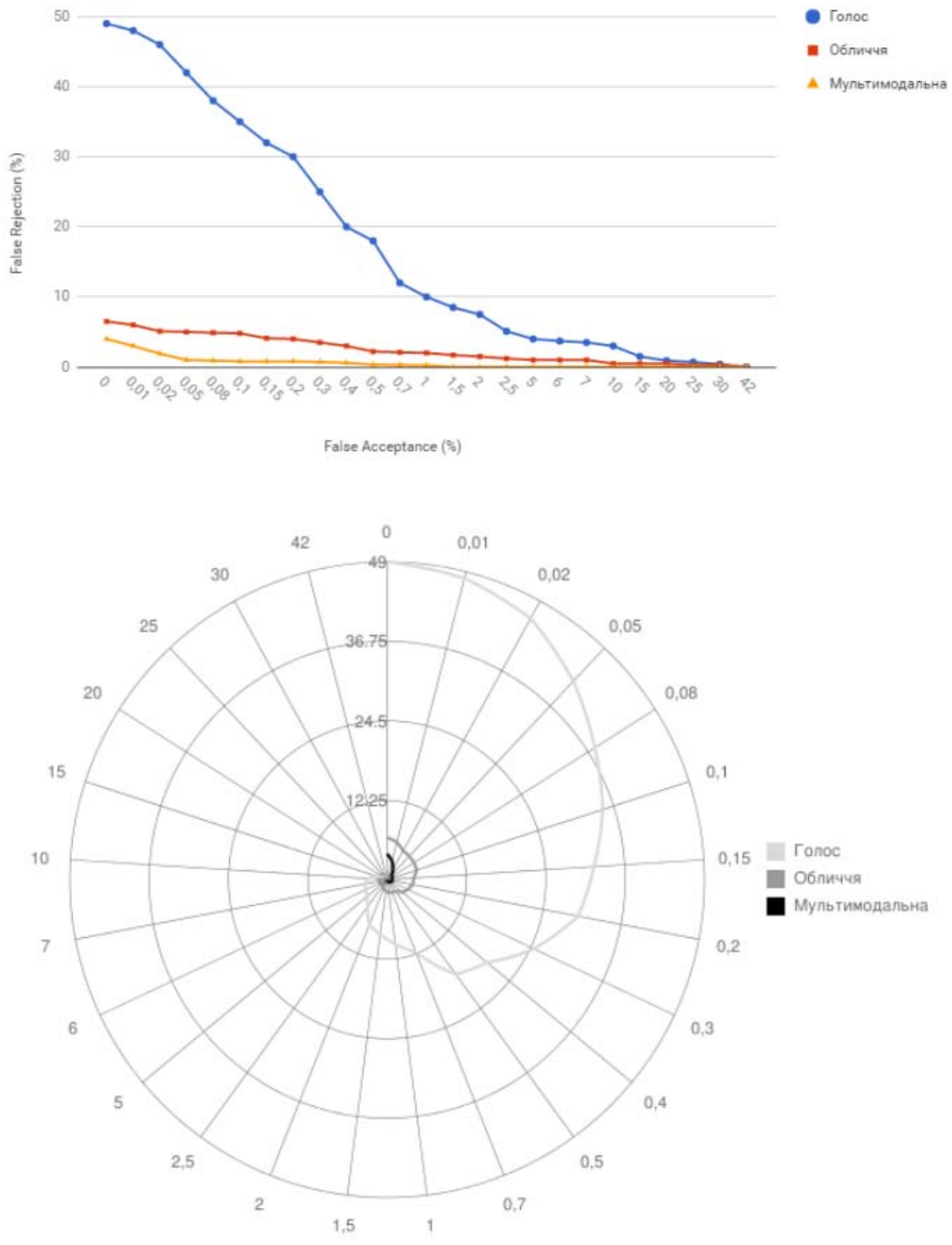

Рис. 2.1. Оцінка точності біометричної системи (криві DET)

2.2. Математична модель ідентифікації користувачів у системах дистанційного навчання .

Для підтримки інформаційної безпеки або контролю доступу необхідно забезпечити певну кількість біометричних параметрів у біометричних системах ідентифікації користувачів.

Нехай у нас є n різних людських параметрів $P_1, P_2, \ldots, P_n$ і m кількість користувачів $L_1, L_2, \ldots, L_m$. У таблиці 2.1 наведено кількість параметрів P_i, характерних для однієї людини L_j.

Таблиця 2.1 – Вхідні дані для математичної моделі

Персонал, m	Біометричні параметри людини, n				Мінімальна норма для доступу
	P_1	P_2	…	P_n	
L_1	x_{11}	x_{12}	…	x_{1n}	d_1
L_2	x_{21}	x_{22}	…	x_{2n}	d_2
…	…	…		…	…
L_m	x_{m1}	x_{m2}	…	x_{mn}	d_k
Вартість системи	c_1	c_2	…	c_r	

Завдання полягає в наступному: необхідно організувати доступ користувачів до інформації так, щоб виконувалася мінімальна норма доступу d_k, яка встановлюється для кожної особи окремо залежно від рівня безпеки та вартості c_r такої системи є мінімальним.

1. X кількість біометричних параметрів, які має людина.
2. Система обмежень:

$$\begin{cases} x_{11} + x_{12} + \ldots + x_{1n} \geq d_1 \\ x_{21} + x_{22} + \ldots + x_{2n} \geq d_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_{m1} + x_{m2} + \ldots + x_{mn} \geq d_k \end{cases}$$

$$x_{ij} \geq 0, \text{де } i, j = \overline{1, n};\ d_i \geq 0, \text{де } i = \overline{1, k};$$

3. Мінімум цільової функції

$$F(X) = c_1 x_1 + c_2 x_2 + c_r x_n \rightarrow min$$

задачу введено визначники для *невідомого X і* встановлено обмеження: $x_{ij} \geq 0, \text{де } i, j = \overline{1, n};\ d_i \geq 0, \text{де } i = \overline{1, k};$. Створено систему обмежень задачі відносно мінімальної норми доступу d_k і цільової функції z встановити екстремум: $F(X) = c_1 x_1 + c_2 x_2 + c_r x_n \rightarrow min$. Наведена вище модель застосовується до задач лінійного програмування .

Принцип мультимодального статико-динамічного біометричного розпізнавання за голосом та обличчям зводиться до тих пір, поки відповідні біометричні характеристики людини не будуть перетворені у вектор *V. біометричних параметрів* , представлених у *N* - мірній ортогональній системі координат:

$$V = \{v_1, v_2, \ldots v_j, \ldots v_N\} j = \overline{1, N};$$

На етапі додавання нової людини в систему, на основі представлених їй зразків, вона створює біометричні стандарти цієї людини у вигляді векторів *Vvoice* і *Vface* .

Наступного разу, коли людина заходить в систему, вона ідентифікується і представляє свої біометричні характеристики у вигляді вектора *V* . На основі ідентифікатора особи система викликає відповідні *стандарти Vvoice* і *V face з бази даних зареєстрованих користувачів* і на основі порівняння *представленого вектора V з доступними* стандартами Vvoice і Vface визначає процедуру автентифікації для цієї особи, які можна побудувати за допомогою різних моделей [12].

На малюнку 2.2 ми надаємо модель побудови системи для ідентифікації користувачів

. За результатом класифікації система приймає рішення, допускати чи ні певного користувача [13].

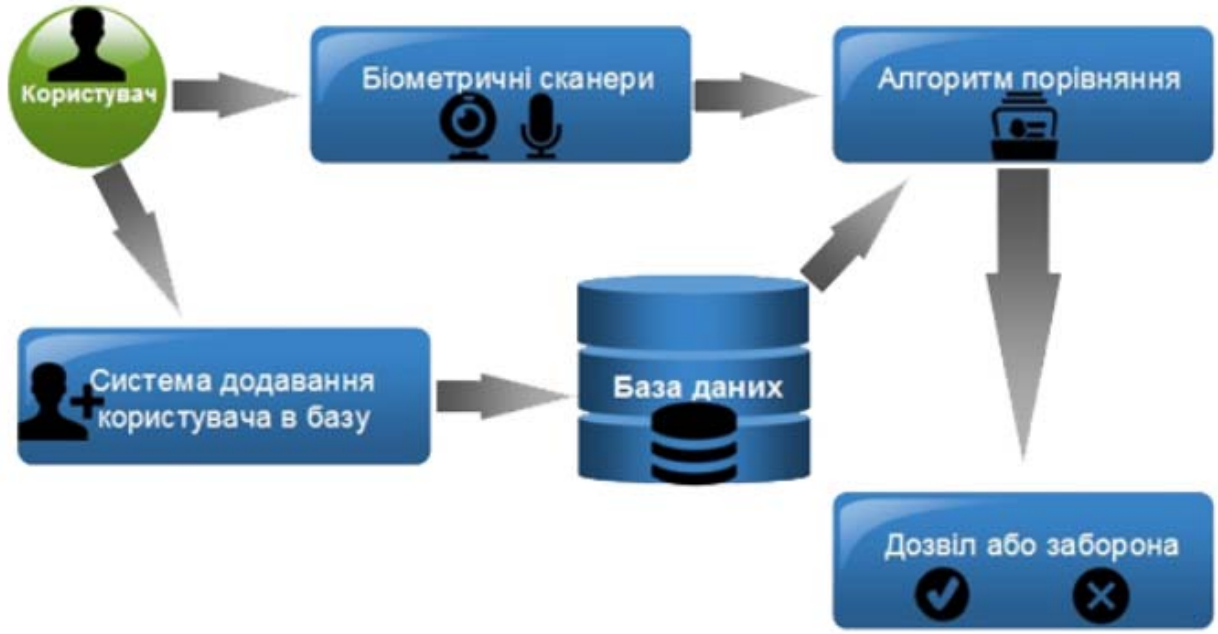

Рис. 2.2. Модель схеми ідентифікації користувача

2.3. Вибір моделі для розпізнавання голосу та обробки звукового сигналу

Проблема розпізнавання голосу залишається актуальною і сьогодні. У цьому підрозділі використовуються різні алгоритми та методи для оптимізації цього процесу для його вирішення. Представлення цих алгоритмів досить просте для розуміння та реалізації у вигляді електронного пристрою.

Розпізнавання мови в режимі реального часу за допомогою сучасних методів вимагає великих обчислювальних ресурсів, а їх кількість часто обмежена.

Той факт, що сьогодні неможливо широко використовувати багато алгоритмів,

наприклад, у мобільних пристроях, змушує дослідників шукати більш ефективні та кращі методи. Завдяки своїй простоті та малій кількості операцій на кожній ітерації розглянуті алгоритми можна рекомендувати як альтернативу існуючим підходам до розпізнавання голосу в реальному часі [5].

Кілька основних моделей використовуються в задачах розпізнавання мовлення та розпізнавання особистості.

1) Моделі з використанням прихованих марковських моделей (Hidden Markov Model - HMM), в яких процес моделювання описується за допомогою кінцевого набору станів, змінних на кожному кроці в довільному напрямку, але статистично прогнозованих (рис. 2.3) [12]. Такий підхід заснований на припущенні, що мова може бути розділена на сегменти (стани), в яких мовний сигнал може розглядатися як зупинка, і що перехід між цими станами відбувається миттєво. Також передбачається, що ймовірність символу спостереження, згенерованого моделлю, залежить лише від поточного стану моделі і не залежить від раніше згенерованих символів. Насправді жодне з цих припущень не є дійсним для мовного сигналу. Проте стандартні є основою для більшості сучасних систем розпізнавання мовлення [13].

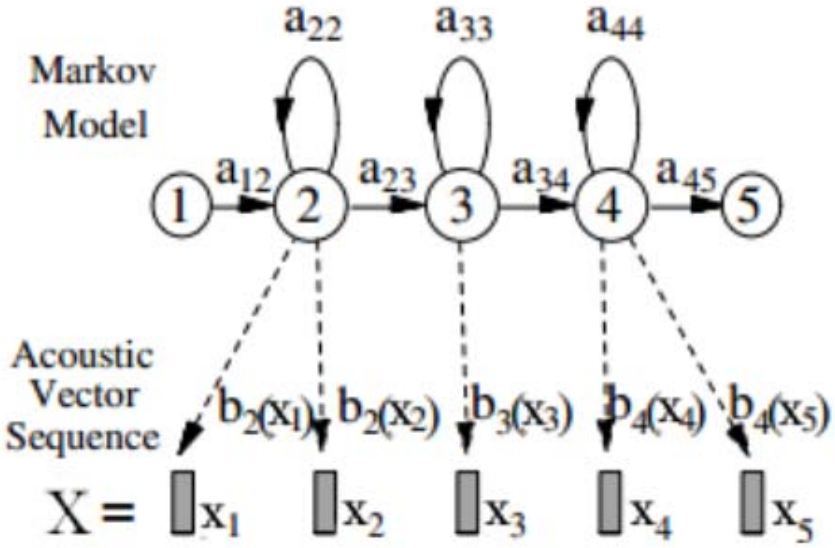

Рис. 2.3. Прихована модель Маркова

Моделі з використанням методу опорних векторів (Support Vector Machine - SVM) (Малюнок 2.4)

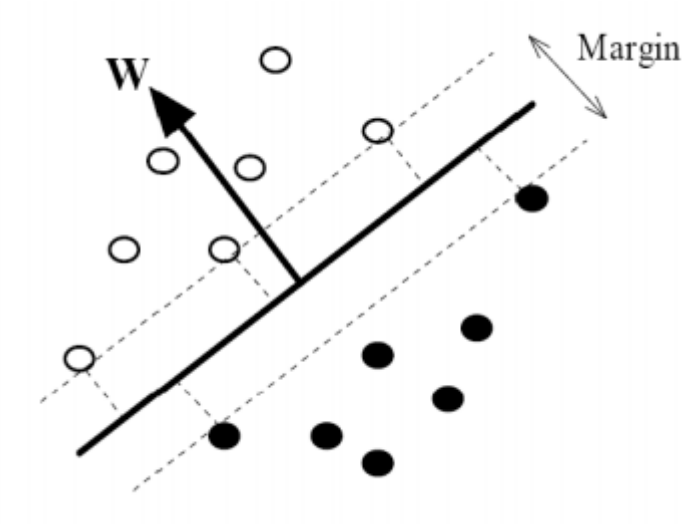

Рис. 2.4. Методи опорних векторів

Метод SVM шукає таку гіперплощину в просторі всіх можливих вхідних даних, щоб вона розділяла різні класи даних і була максимально віддалена від кожного з них. Використання методу опорного вектора дозволяє отримати функцію класифікації з мінімальною верхньою оцінкою очікуваного ризику (рівень помилки класифікації), а також використання лінійного класифікатора для роботи з нелінійним розподілом даних, поєднуючи простоту з ефективністю. .

Система забезпечує цифрову обробку звукового сигналу [10] для презентації аналоговий мовний сигнал у цифровій формі. В результаті аналого-цифр перетворення (АЦП) перетворює безперервний сигнал у ряд дискретних тимчасовий відлік, кожен з яких є числом. Схарактеризуйте це число сигнал у точці з певною точністю. Від ширини залежить точність зображення діапазону прийнятих чисел, і, отже, від розрядності АЦП. Процес виведення з Ознака числових значень називається квантифікацією. Процес поділу сигналу на Підрахунок називається дискретизацією. Кількість відліків за секунду

називається частотою розсуд. У деяких випадках для визначення використовується кількісна оцінка поняття біта (швидкості передачі) - це кількість бітів, оброблених за одну секунду. Знаючи бітрейт і частоту дискретизації, можна знайти пропускну здатність з отриманих чисел.

Процес обробки звукових хвиль схематично зображено на рисунку 2.5.

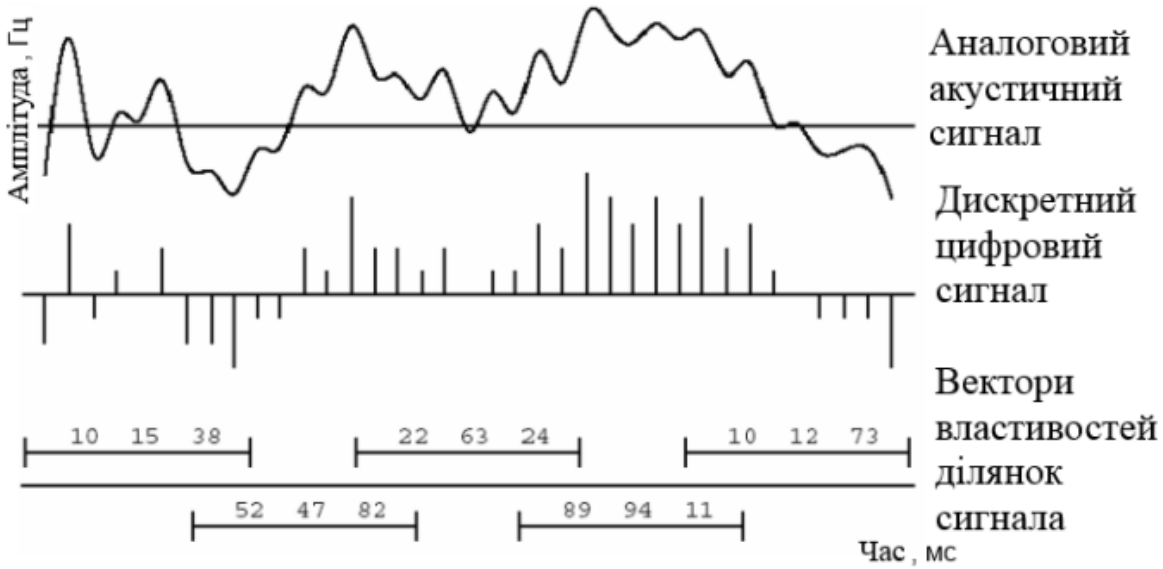

Рис. 2.5. Етапи обробки звукової хвилі

Аналоговий акустичний сигнал, що надходить від мікрофона, дискретизується та кількісно визначається за допомогою АЦП. Реалізація звуку відбувається так називається, тобто цифровий запис вимови слова (звуку) у вигляді лічильної послідовності звукового сигналу {Sk}. Реалізація слів (звуків) у процесі цифрової обробки розбивається на послідовність кадрів { *Xi* }. Порядок підрахунку аудіосигналу кадру *X* (довжина *N) називається S1, S2, ..., Sn* .

Довжина кадру фіксується в часі. Наприклад, при N=100 і частоті дискретизації 8000 Гц це відповідає тривалості 12,5 мс. Кадри часто зміщуються відносно один одного, щоб інформація не втрачалася на межі кадру. Фаза зміщення кадру - кількість звуків підраховується між початками послідовних кадрів.

крок зміщення менше ніж N (довжина кадру), що кадри розташовані один над одним.

Потім у цілому ряді завдань, таких як розпізнавання мовлення або розпізнавання особи, кожен кадр зіставляється з деякими даними, які найкраще представляють звук.

Такі дані утворюють вектор властивостей (або вектор ознак). Математично це може бути вектор із простору $R_м$, або набір функцій, або одна функція.

Завдання розпізнавання окремих слів мови полягає в ототожненні кожного слова, яке надходить на вхід системи, з попередньо визначеним класом. Існує цілий ряд різних факторів, які можуть негативно вплинути на точність системи розпізнавання - настрій і стан того, хто говорить, шум навколишнього середовища, швидкість звукових фраз і т.д.

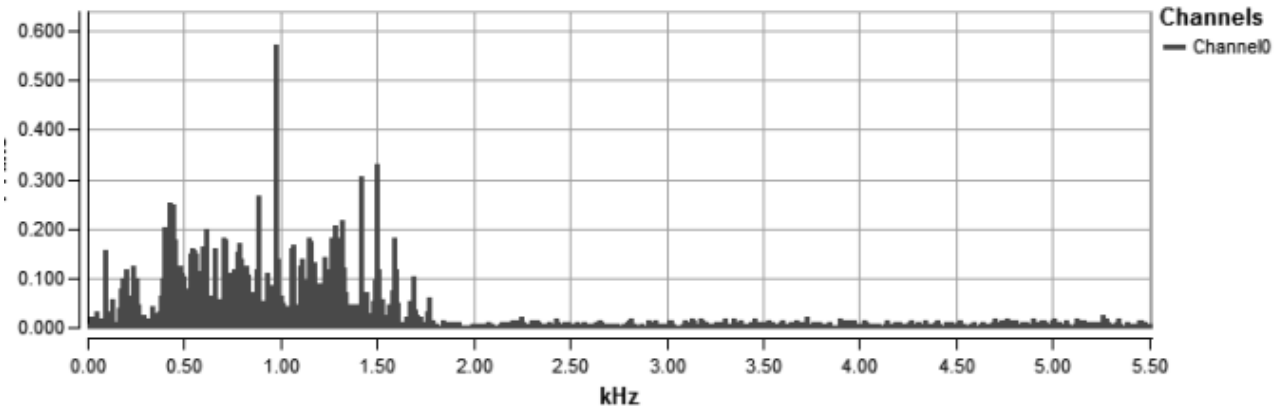

Рис. 2.6. Чистий сигнал

Записати сигнал без зовнішнього шуму дуже важко. На рисунку 2.6 і 2.6 показані амплітудно-частотні діаграми сигналу в чистому вигляді і такого ж сигналу, але з інтерференцією типу білого шуму. Білий шум - це шум, в якому звукові коливання різних частот представлені однаково, тобто середня інтенсивність звукових хвиль різних частот приблизно однакова.

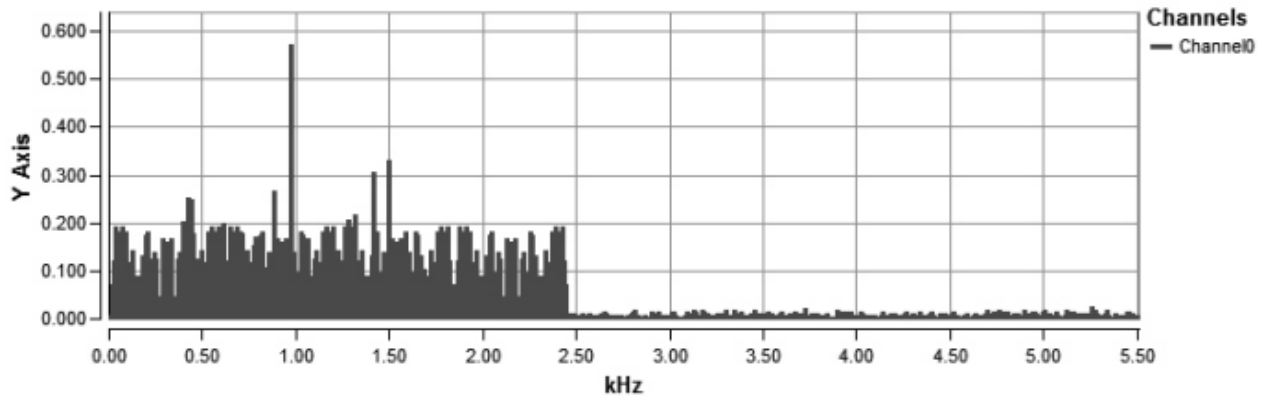

Рис. 2.7. Сигнал білого шуму

Як бачите, існує значна різниця між шумовими сигналами та чистими сигналами. Щоб позбутися від негативного впливу шуму, сигнал обробляється спеціальними частотними фільтрами. Частотний фільтр працює наступним чином: з усього набору гармонік, що складають звуковий сигнал, фільтр залишає тільки ті частоти, які потрапляють в задану смугу пропускання.

Для виконання спектрального аналізу голосу нашої задачі було обрано швидке перетворення Фур'є, оскільки час обчислення економиться завдяки зменшенню кількості множень, необхідних для аналізу кривої.

2. 4 . Алгоритм вибору грані.

Для тестування було обрано та розміщено три алгоритми виділення обличчя на основі навчання на основі методу, запропонованого П. Віолою та М. Джонсом (метод підсилення), навчальної мережі SNoW (Sparse Network of Winnows) та методу опорних векторів (SR). в силі.

Метод Віоли-Джонса був розроблений і представлений в 2001 році, і в даний час він є основою для виявлення об'єктів зображення в реальному часі. Основні принципи, на яких базується метод:

1) зображення використовуються в комплексному вигляді, що дозволяє швидко розрахувати необхідне;
2) Використовуються сигнали Хаара, які використовуються для пошуку бажаний предмет (у даному контексті обличчя);
3) посилення використовується для вибору найбільш підходящих функцій для бажаний об'єкт на цій частині зображення;
4) усі функції додаються до вхідних даних класифікатора, який дає «істинний» результат або "брехня";
5) каскади функцій використовуються для швидкого видалення вікон, коли

   обличчя не знайдено [4].

Winnows Boundary Network (SNoW) [5] можна перекласти як « розріджена мережа відсіювальних елементів». Snow — це двошарова мережа для виявлення облич [6]
, вхідний рівень якої складається з вузлів, кожен з яких відповідає деяка характеристика вхідного зображення (генерує 1 за наявності деяких функції та 0, якщо вона відсутня на зображенні), оригінал складається з усього два вузли, кожен з яких відповідає відомим класам зображень («обличчя», «не обличчя»). Прапори використовуються як атрибути зображення дорівнює певним значенням середнього значення і варіації яскравості в кожному з них прямокутні фрагменти зображення розміром 1x1, 2x2, 4x4 і 10x10 (всі зображення мають розмір 20x20 пікселів).

Це дає простір функцій розмірністю 135424. Під час класифікації інформація про присутність надається вхідним вузлам певні характеристики обробленого зображення. Вузли вихідного шару обчислити лінійну комбінацію сигналів, що генеруються на вхідних вузлах. Коефіцієнти лінійної комбінації задаються вагами зв'язків між вхідним і вихідним вузлами. При перевищенні заданого порогу приймається рішення про це наявність обличчя на зображенні.

Snow спеціально розроблений для ситуацій класифікації, коли можлива кількість ознак об’єктів, важливих для класифікації, може бути дуже великою, але наперед невідомо. Розріджена архітектура мережі дозволяє її використовувати величезна кількість властивостей зображення як вхідних даних, тому що і в процесі навчання відкидаються всі непотрібні риси, і вони не гальмують, адже продуктивність класифікатора [7].

Метод опорних векторів (RMV) використовується для зменшення розмірності простору ознак без значних втрат навчальної інформації. ряд речей. Застосуйте метод головних компонент до набору векторів лінійного простору, ви можете перейти до такої основи простору, яка є найбільшою розкид набору буде спрямований вздовж кількох перших осей основи, наз головні осі. Таким чином виходить підпростір, продовжений до головних осей це найкращий серед усіх просторів у тому сенсі, що він представляє найкраще навчальна серія. Це набір алгоритмів, подібних до алгоритмів «навчання». вчителем», який використовується для завдань класифікації та регресійного аналізу.

Цей метод належить до сімейства лінійних класифікаторів. Методи опорних векторів заснований на тому, що шукається лінійний поділ класів. Мета навчання для класифікаторів полягає в мінімізації помилки класифікації на навчальному наборі набір (званий емпіричним ризиком). На відміну від них, використовуючи метод опорних векторів, ви можете побудувати класифікатор, який мінімізує верхню оцінку очікувана помилка класифікації (в тому числі у випадку невідомого об’єкта, який не є входять до навчального набору). Застосування методу опорних векторів до задачі Ідентифікація особи — це знаходження гіперплощини в просторі ознак а клас відокремлює зображення обличчя від зображень без обличчя. Лінійна можливість навряд чи можна розділити такі складні класи, як зображення обличчя та «не обличчя».

Однак класифікація за допомогою опорних векторів дозволяє його використовувати апарат ядерних функцій для неявного проектування вектора

ознак у простір потенціалу вище (навіть вище, ніж простір зображення), що містить класи можуть бути розподілені лінійно.

Використання інтуїтивно зрозумілого дизайну Ядерні функції не призводять до складних обчислень, що забезпечує успіх використовувати лінійний класифікатор для лінійно нероздільних класів [10].

відбору користувачів можуть виникнути два типи помилки: нездатність привернути увагу вперед і помилкове виявлення (вибір об'єкта а обличчя не видно). Через наявність двох типів помилок їх два основні параметри, що характеризують ефективність алгоритмів виявлення faces: швидкість виявлення, яка показує відсоток розпізнаних облич, і коефіцієнт помилкових позитивних результатів дорівнює загальній кількості помилкових позитивних результатів виявлено на всій тестовій сукупності [5].

Одне й те саме обличчя має різний розмір, який вибирається різними алгоритмами. Тому алгоритм, заснований на повному посиленні світлих ділянок обличчя, захопленні чола, підборіддя та Щоки Алгоритми на основі SNSO і MOV, крім того, розрізняють очі, ніс і рот алгоритм на основі MOV вибирає обличчя з вужчим вікном. Ці відмінності є причиною той факт, що під час створення алгоритмів використовувалися різні навчальні набори Зображення для побудови класифікатора. Слід зазначити, що алгоритм заснований на більш адекватне підкріплення показує фактичний розмір людини .

На рисунку показано залежність рівня виділення від ймовірності імпульсного шуму 2 . 8 відповідно. Крім появи різних зашумлених пікселів на зображенні також можлива підлягає невідомості. Ступінь розмитості зображення буде характеризуватися за допомогою універсального індексу якості (UII). Чим сильніше розмиття зображення, тим менше значення цього критерію. Для вихідного зображення він приймає значення 1, а при сильному розмиття його значення наближаються до нуля.

На відміну від ситуації з додаванням шуму, легке розмиття зображення не призводить до значного зниження рівня виділення обличчя. При зміні UI від 1

до 0,7 рівень вибору тестованих алгоритмів зменшується менш ніж на 10% [12]. І крім сильного розмиття, спостерігається різке зниження рівня акцентування обличчя.

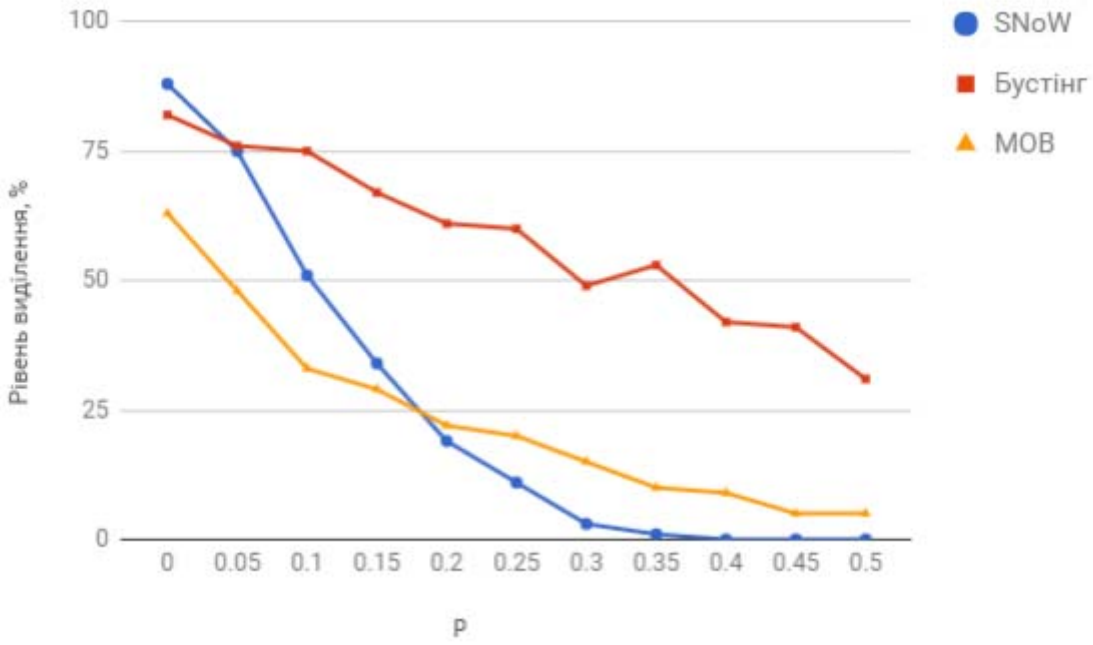

Рис. 2.8. Залежно від рівня вибирається ймовірність виникнення імпульсного шуму

Через нечіткість алгоритми на основі SNOW і MOV збільшують кількість помилкових виявлень (рис. 2.9). Плавна зміна значень пікселів за допомогою цих алгоритмів сприймається як обличчя. Лише алгоритм, заснований на посиленні, зберігає здатність відокремлювати класи обличчя та неособи. Рівень їх неправильного вибору знижується в міру збільшення ступеня неоднозначності.

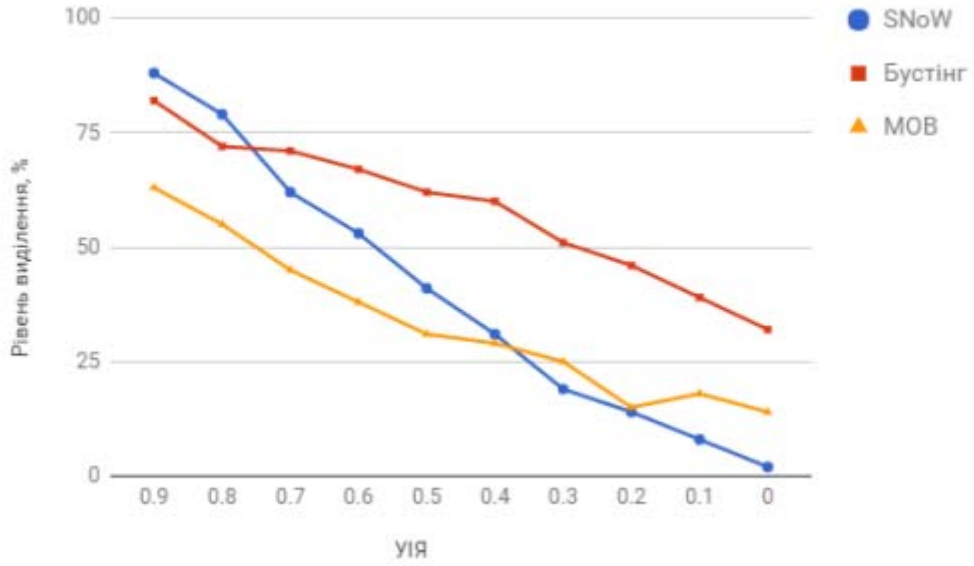

Рис. 2.9. Залежно від обраного рівня ступінь розмитості зображення

Оператор Sobel [8] використовується в обробці зображень для виділення меж. Це дискретний диференціальний оператор, який обчислює приблизне значення градієнта або норму градієнта яскравості зображення.

Оператор Sobel заснований на згортці зображення з невеликими роздільними цілочисельними фільтрами у вертикальному та горизонтальному напрямках. Однак градієнтна апроксимація досить груба, особливо у високочастотних областях зображення.

Значення функції є лише на регулярній сітці, тому похідні не можуть бути отримані, але, припускаючи неперервність функції, можна застосувати кінцеві різниці, тобто оператор Собеля для наближення часткових похідних.

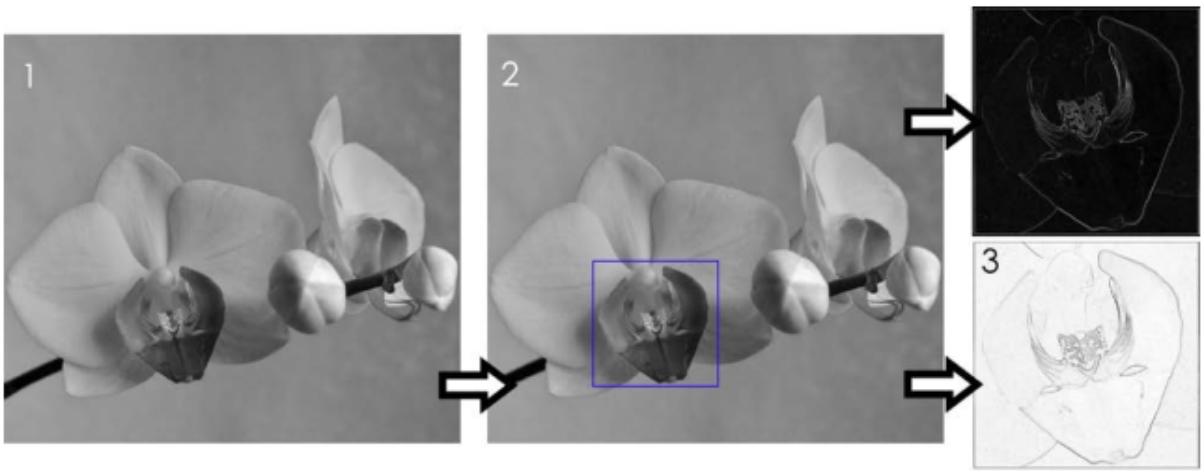

Рис. 2. 10. Процес створення стандарту для подальшого розпізнавання об'єктів

істотна різниця між результатами фільтра Собеля. Фільтр Собеля зазвичай менш чутливий до шуму зображення порівняно з фільтром Лапласа. Виявлені обмежувальні лінії не такі візуально зернисті, як лінії інших існуючих обмежувальних фільтрів. Результат застосування фільтра Собеля до попередньо підготовленого зображення представлено на рисунку 2.10 (3) у звичайному та інверсному варіантах.

На основі наведених вище рекомендацій щодо вдосконалення існуючих методів створення еталонного зображення можна реалізувати універсальний алгоритм для роботи з будь-яким об’єктом (рис. 2.11).

Рис. 2. 11. Алгоритм створення еталонного зображення

Після кожної дії виходить еталонне зображення з роздільною здатністю 500 × 500 пікселів і розміром всього 150 Кбайт, що підходить для сучасних баз даних.

2.5 _ _ Використовуйте метод шифрування для створення еталонних зразків біометричних характеристик людини

Безпека та конфіденційність є одними з найактуальніших тем сьогодення, особливо коли йдеться про біометричні характеристики людини, адже основним недоліком такої ідентифікації є наслідки витоку даних. Якщо ви забудете пароль, його можна легко змінити, але якщо зловмисник отримає доступ до бази даних із зразками біометричних зразків, змінити їх буде неможливо, і ви можете на деякий час забути про збереження даних. Це змушує використовувати метод шифрування створених еталонних зразків біометричних характеристик людини.

Використаний метод дозволить користувачам системи відбирати еталонні зразки власних біометричних характеристик і шифрувати їх на стороні клієнта за допомогою коду доступу.

Не буде потрібно ніякого серверного коду, ніякої інформації між клієнтом і сервером не буде передаватись - це підвищить довіру користувача до методу розробки в цілому. Для реалізації ми будемо використовувати API HTML5 FileReader і бібліотеку шифрування JavaScript - CryptoJS.

CryptoJS — це зростаюча колекція стандартних і надійних криптографічних алгоритмів, реалізованих у JavaScript із використанням найкращих практик і моделей. Вони швидкі, мають послідовний і простий інтерфейс. CryptoJS — це програмне забезпечення з відкритим кодом.

Щоб вирішити нашу проблему шифрування, алгоритм Advanced Encryption Standard (AES) - симетричний блочний алгоритм шифрування (розмір блоку 128 біт, ключові біти 128/192/256), конкурент у конкурсі AES був обраний і прийнятий як американський стандарт шифрування. . урядом США. Було обрано AES, і очікувалося, що алгоритм буде широко використовуватися та активно аналізуватися, як це було з його попередником, DES. Національний інститут стандартів і технологій США (NIST) опублікував попередню специфікацію AES 26 жовтня 2001 року після п'яти років підготовки. 26 травня 2002 року AES було оголошено стандартом шифрування. Станом на 2009 рік AES є одним із найпопулярніших алгоритмів симетричного шифрування [6].

HTML5 FileReader API [6] – спосіб читання вмісту файлу або об’єкта Blob (Binary Large Object) у пам’ять. Об’єкт FileReader дозволяє нам читати вміст локальних файлів за допомогою JavaScript, але лише ті файли, які були безпосередньо вибрані користувачем через діалогове вікно, яке пропонує вибір файлу. Браузери, які підтримують цю технологію, показані на малюнку 2.12.

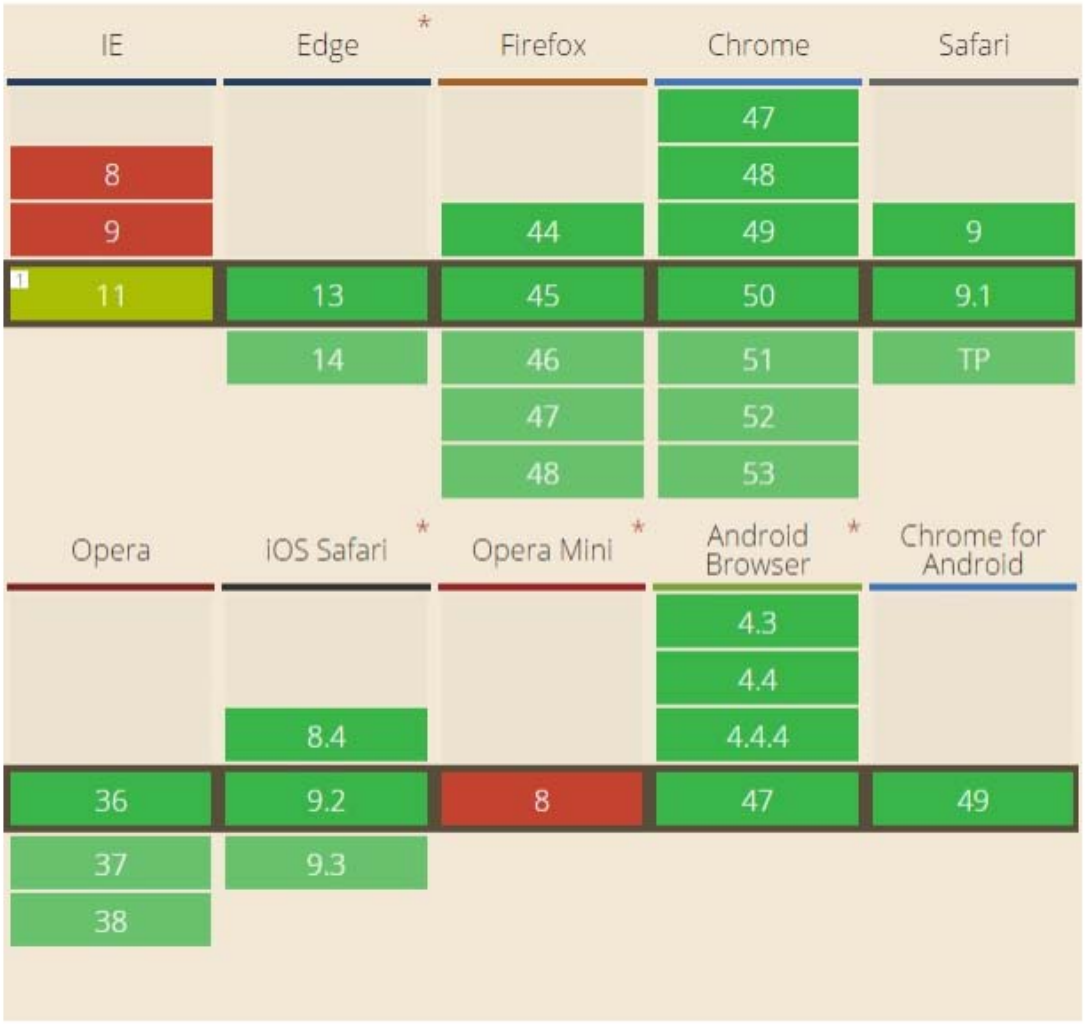

Рис. 2.12. Підтримка технології FileReader API різними браузерами

Після завантаження біометричного довідкового файлу його вміст перетворюється на рядок даних URI. Перевага полягає в тому, що стандарт зберігає свій початковий вміст безпосередньо в URI, тому ми можемо записати вміст файлу як текст і додати запропоноване вище шифрування з вибраним паролем [13]. Під час дешифрування відбувається зворотна процедура.

2. 6 . Реалізація функціональної моделі системи ідентифікації користувача в системах дистанційного навчання

Для розробки структурно-функціональної моделі використовуються різноманітні прийоми графічного зображення. Одним із них є IDEF0 – графічна нотація моделювання, яка використовується для створення функціональної моделі, яка представляє структуру та функції системи, а також інформаційні потоки та відповідні об’єкти, що зв’язують ці функції [5].

Перш за все, необхідно побудувати контекстну діаграму - це сама верхня діаграма, на якій об'єкт моделювання представлений єдиним блоком зі стрілками-краями. Ця діаграма називається А-0 (А мінус нуль).

Стрілки на цій діаграмі показують взаємозв’язок між змодельованим об’єктом і середовищем. Діаграма А-0 визначає область моделювання та її межі (рисунок 2.13).

Наступний крок - розкладання. Нотація IDEF0 підтримує послідовну декомпозицію процесу до необхідного рівня деталізації. Дочірня діаграма, створена декомпозицією, охоплює ту ж область, що й батьківський процес, але описує його більш детально.

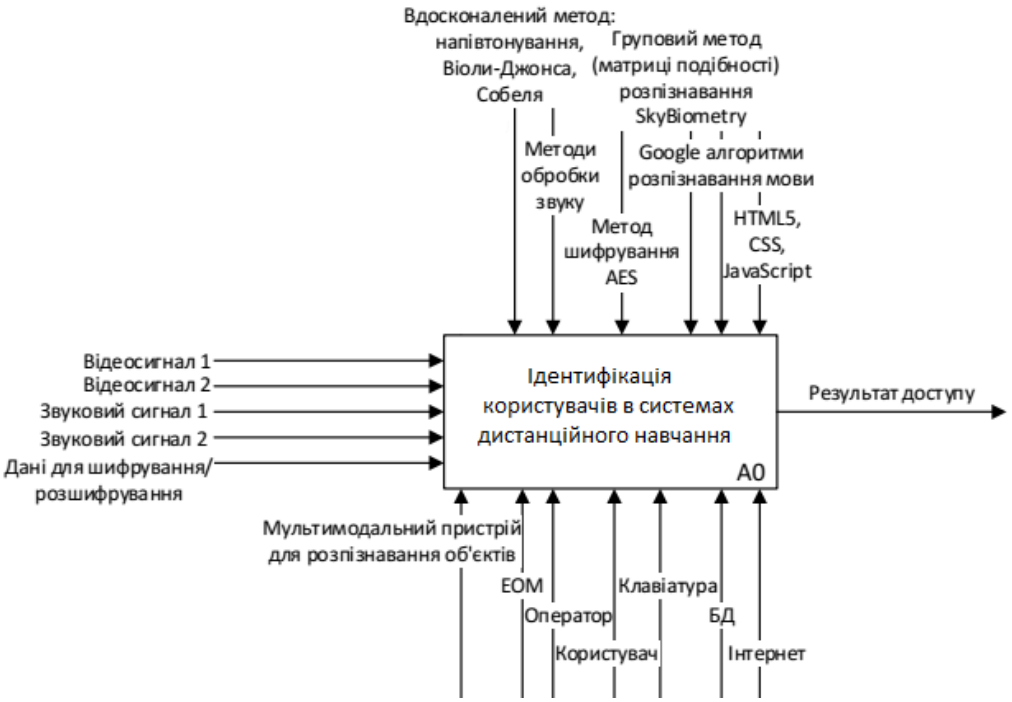

Рис. 2.13. Контекстна діаграма IDEF0 для ідентифікації користувача в системах дистанційного навчання на основі набору біометричних параметрів

Відповідно до методології IDEF0 під час декомпозиції стрілки батьківського процесу переносяться на дочірню діаграму у вигляді граничних стрілок (рис. 2.14).

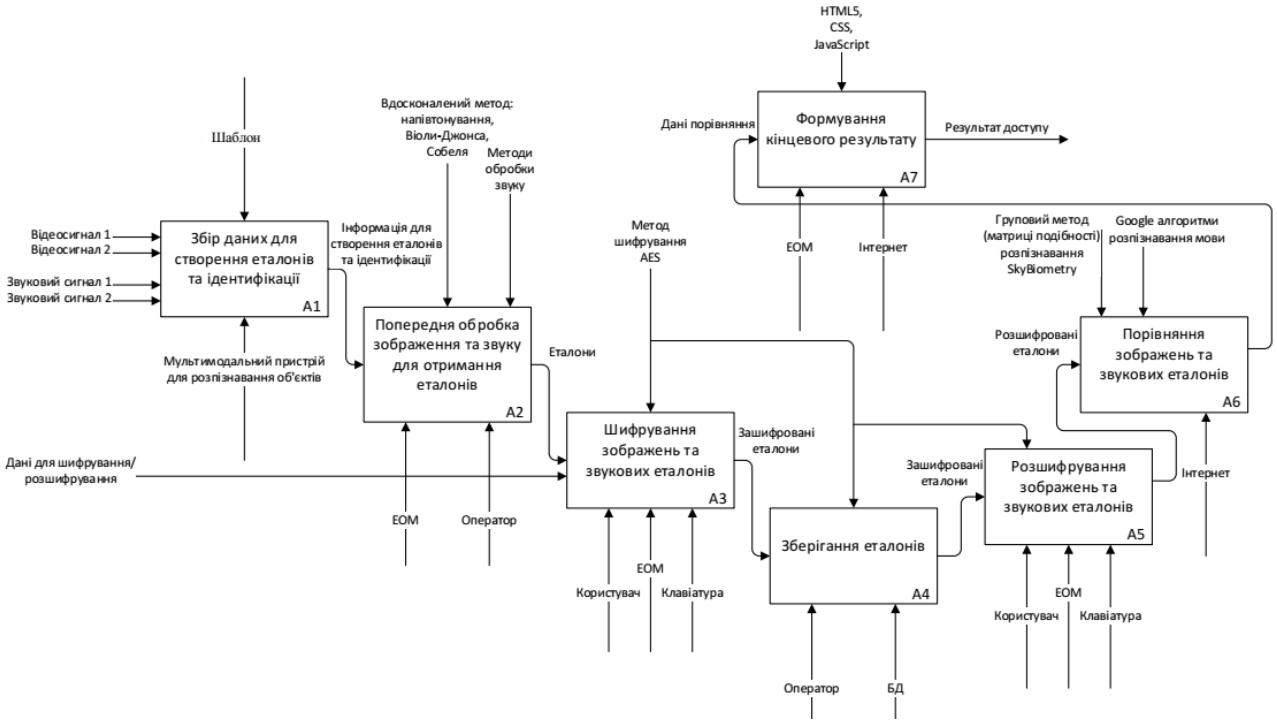

Рис. 2.14. Дочірня діаграма IDEF0 ідентифікатора користувача на основі комплекс біометричних параметрів

Блоки діаграми IDEF0 зі складною внутрішньою реалізацією потребують подальшої декомпозиції. У нашому випадку більш детальному розгляду реалізації підлягає блок А2 «Попередня обробка зображення та звуку для отримання еталонів».

Будемо вважати, що рівень декомпозиції розглянутих діаграм достатній для відображення мети моделювання, а базові функції використовуються на діаграмах нижчого рівня, з точки зору користувачів системи.

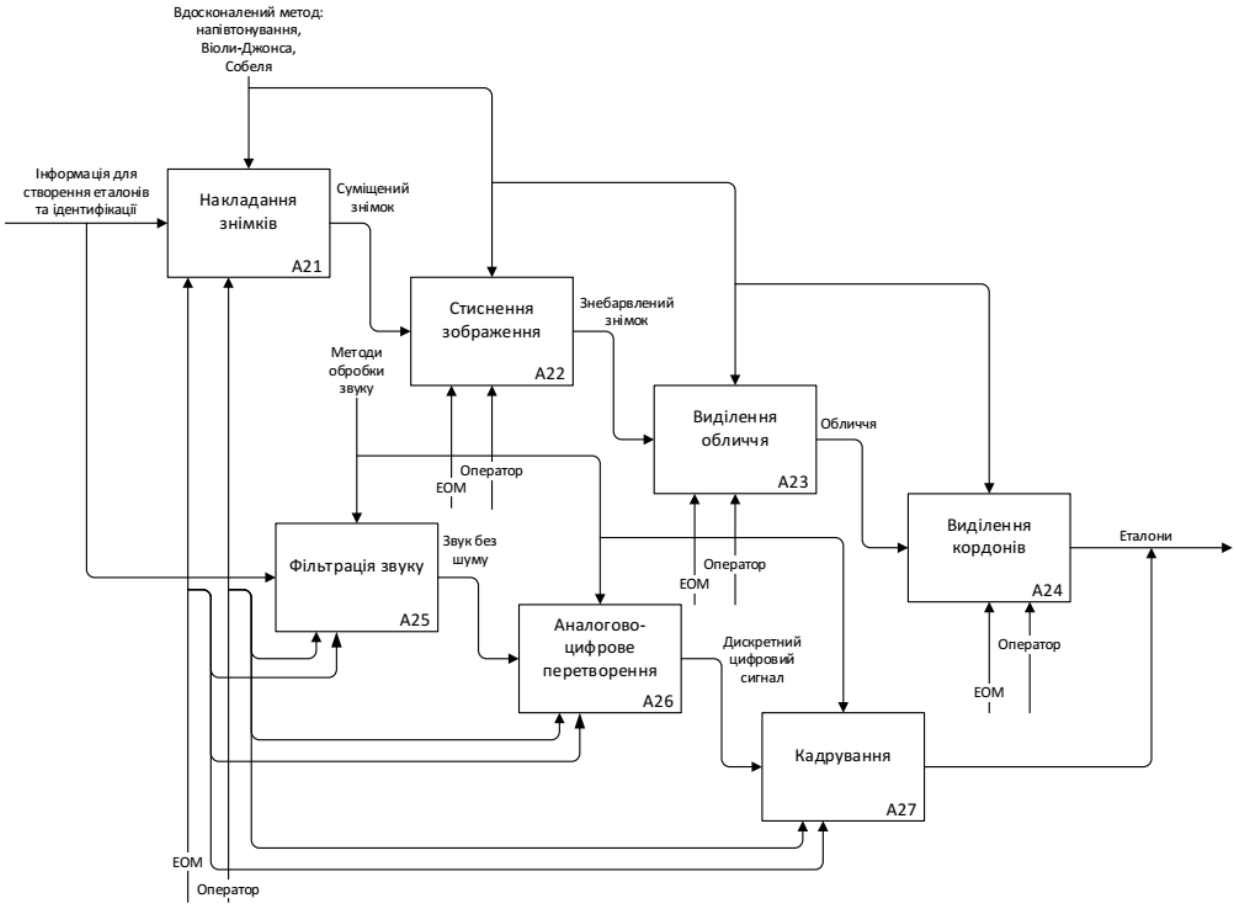

Рис. 2.15. Діаграма декомпозиції IDEF0 блоку А2 «Попередня обробка зображення та звук для отримання стандартів"

Висновки розділу 2

1. ідея бімодальної системи ідентифікації користувача в системах дистанційного навчання на основі розпізнавання голосу та розпізнавання обличчя .
2. найкращі алгоритми серед методів обробки зображень.
3. Покращено алгоритм створення еталонного зображення.

Розділ 3
ВПРОВАДЖЕННЯ СИСТЕМИ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ В ОСВІТНІХ СИСТЕМАХ

3.1. Застосування підходу до ідентифікації користувача

Мультимодальний підхід може подолати багато обмежень одномодальних систем, оскільки одні характеристики компенсують недоліки інших.

Переваги мультимодального підходу:

1) збільшити охоплення області застосування (одного атрибута немає, використовуємо інший);

2) зменшення помилок неправильної ідентифікації, розширення діапазону умов навколишнього середовища, за рахунок використання кількох модальностей;

3) зниження чутливості до шуму.

Мультимодальна система ідентифікації, розпізнавання та авторизації об'єктів, що поєднує дві біометричні характеристики: голос і обличчя.

Спочатку був розроблений алгоритм роботи модуля зі звуком (голосом): вмикання пристрою, вибір режиму (опорний або розпізнаючий запис), при виборі першого виходить звуковий стереосигнал, шумозаглушення і запис посилання. спектр; коли він обирає другий, пристрій отримує стереозвуковий сигнал у реальному часі, виконує шумозаглушення та порівнює його зі стандартним. Якщо запис не відповідає стандарту, доступ до розпізнаного об’єкта не буде здійснюватися (рис. 3.1 а).

Далі був розроблений алгоритм роботи модуля зображення: вмикає пристрій, вибирає режим (зберегти референс або ідентифікатор), коли вибирає перший, надходить 3D відеосигнал, зображення накладаються і зображення зберігається еталонним. ; коли він обирає останнє, пристрій отримує 3D-відеосигнал у режимі реального часу, накладає зображення та порівнює їх із

стандартом. Якщо зображення людини не відповідає стандарту, доступ до розпізнаного об’єкта буде недоступним (рис. 3.1 б).

Переваги цієї схеми проекту:

1) отримати два зображення: одне нормальне та одне в ІЧ-діапазоні. (При подальшій обробці фотографії зображення можна накладати, досягаючи розширеного динамічного діапазону зображення);

2) можливий стереозвук завдяки 2 мікрофонам;

3) регульоване світлодіодне підсвічування для зйомки у вечірній час або в місцях зі слабким освітленням (складається з 12 світлодіодів);

5) просте підключення за допомогою USB для зйомки та MiniJack 3,5 мм для підключення мікрофонів. Додаткові джерела живлення не потрібні;

6) низька вартість.

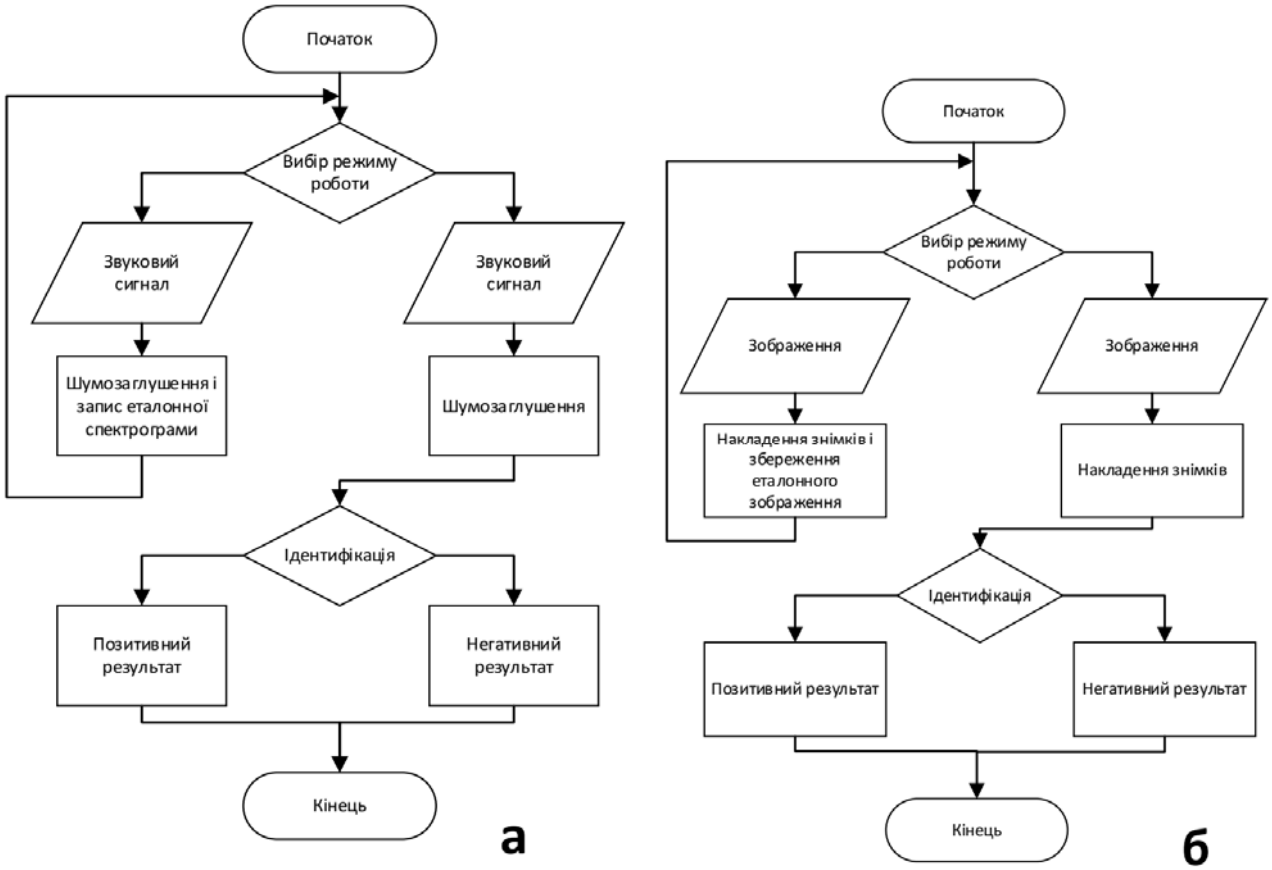

Рис. 3.1. Алгоритм аудіо та графічних модулів

Значні переваги має розпізнавання об'єктів біометричними методами. Завдяки застосуванню мультимодального підходу, який враховує відразу кілька біометричних характеристик, можна на порядок зменшити кількість людей, біометрична ідентифікація яких неможлива, а також значно підвищити захищеність інформаційних ресурсів від несанкціонованого доступу. Загалом.

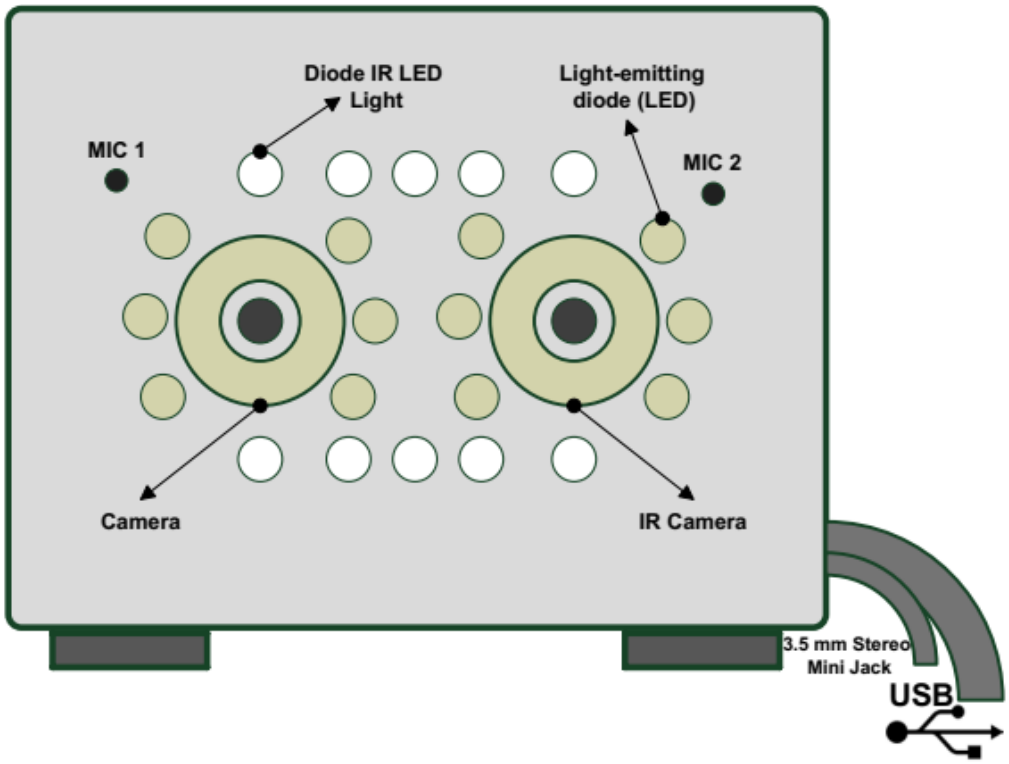

Рис. 3.2. Мультимодальний пристрій

Мультимодальний пристрій розпізнавання об’єктів долає багато обмежень унімодальних систем, оскільки деякі параметри компенсують властиві недоліки інших параметрів, він поєднує дві характеристики: розпізнавання аудіо та зображення, він робить збір цифрової інформації багатопотоковим у відеоформі. і звукового сигналу в режимі реального часу, покриття областей застосування збільшується, помилки ідентифікації та чутливість до шуму зменшуються.

3.2. Програмне забезпечення методів обробки зображень.

Окреслення — це назва кількох математичних методів, які використовуються для визначення контурів у цифровому зображенні, де яскравість зображення різко змінюється або де є інші типи неоднорідностей.

Контури, які містять різкі зміни яскравості зображення, зазвичай організовані в кілька вигнутих лінійних сегментів, які називаються межами. Виділення меж є основним інструментом обробки та розпізнавання зображень, особливо в області виявлення та виділення ознак. Тому застосування граничного фільтра виділення на зображенні може істотно зменшити обсяг оброблюваних даних, за рахунок того, що відфільтрована частина зображення вважається менш значущою, а структурні властивості зображення зберігаються найбільш важливими. Однак на реальних картинках середньої складності межі не завжди помітні.

Межі, виділені з таких зображень, часто мають такі недоліки, як фрагментарність (криві меж не пов'язані між собою), відсутність меж або наявність фальшивих, що не відповідають досліджуваному об'єкту.

Згортка — це проста математична операція, яка лежить в основі багатьох операторів обробки зображень. Згортка забезпечує можливість множення двох наборів чисел, як правило, різного розміру, але однакової розмірності, для отримання третього набору чисел тієї ж розмірності. Це можна використовувати в обробці зображень для реалізації операторів, вихідні піксельні значення яких є простими лінійними комбінаціями заданих вхідних піксельних значень. У контексті обробки зображень одним із вхідних масивів зазвичай є лише сірі кольори зображення. Другий шар зазвичай набагато менший і також двовимірний (хоча він може мати товщину лише в один піксель), і він називається ядром.

Дискретний оператор Лапласа часто використовується в обробці зображень, наприклад, у програмах виявлення меж і оцінки руху. Дискретне перетворення Лапласа визначається як сума другої похідної виразу координати

оператора Лапласа та обчислюється як сума різниць між найближчими сусідами центрального пікселя.

Для одновимірних, двовимірних і тривимірних сигналів дискретний лапласіан можна задати як згортку з наступними ядрами

$$\text{Фільтр 1D: } D_x^{\,2} = \begin{bmatrix} 1 & -2 & 1 \end{bmatrix}$$

$$\text{Фільтр 2D: } D_{xy}^{\,2} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & -4 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

Ці ядра виводяться за допомогою дискретних частинних похідних. Багато змін матриці/ядра можна застосувати з результатами від непомітних до дуже очевидних. Нижче ми розглядаємо дві реалізації матриць: 3 x 3 і 5 x 5.

Реалізація:

Матриця Лапласа 5 x 5 створює зображення результату зі значними відмінностями. Сегментація меж виражається відносно дрібними деталями, хоча матриця Лапласа, як правило, чутлива до шуму зображення.

Виділення межі зображення методом Гауса-Лапласа. Гаусса-Лапласа є загальною різновидом фільтра Лапласа. Метод Гаусса-Лапласа призначений для протидії чутливості до шуму звичайного фільтра Лапласа.

Метод Гаусса-Лапласа для видалення шуму зображення застосовує згладжування за допомогою розмиття за Гаусом. Щоб оптимізувати продуктивність, ми можемо обчислити єдину матрицю, яка представляє дані Галісіана та матрицю Лапласа.

Метод граничного вибору Собеля є іншим загальним застосуванням граничного вибору. Оператор Sobel використовується в обробці зображень для виділення меж. Це дискретний диференціальний оператор, який обчислює приблизне значення градієнта або норму градієнта яскравості зображення. Оператор Sobel заснований на згортці зображення з невеликими роздільними цілочисельними фільтрами у вертикальному та горизонтальному напрямках.

На відміну від розглянутих вище фільтрів Лапласа, результати фільтра Собеля істотно відрізняються. Фільтр Собеля зазвичай менш чутливий до шуму зображення порівняно з фільтром Лапласа.

Дослідивши та впровадивши методи виділення меж зображення, ви можете вибрати найкращий для нашого завдання розпізнавання людини. Вибираємо оператора Sobel, оскільки він не такий чутливий до шуму зображення, як межова лінія точно зернистий, як і в інших розрахункових фільтрах.

3.3. Веб- додаток

Сучасні мови веб-програмування: HTML5 і JavaScript, а також спеціальна мова CSS (каскадні таблиці стилів) були використані для реалізації розробленого алгоритму створення стандарту зображення та подальшого шифрування біометричних зразків для сторінок, написаних на мовах розмітки, для представлення даних. візуально.

На рисунку 3.3 зображено головну сторінку створеного сайту, яка має таку структуру сторінок: головна сторінка, база даних, публікації та шифрування. Структура кожної окремої сторінки складається з: верхнього колонтитула (верхня частина сторінки), навігаційного меню (меню навігації), меню (меню правого розділу), основної частини (основна частина сторінки) і нижнього колонтитула (нижня частина сторінки).

Всього на сайті використовується 14 різних стилів, які написані <style>… </style> і мають адаптивний дизайн.

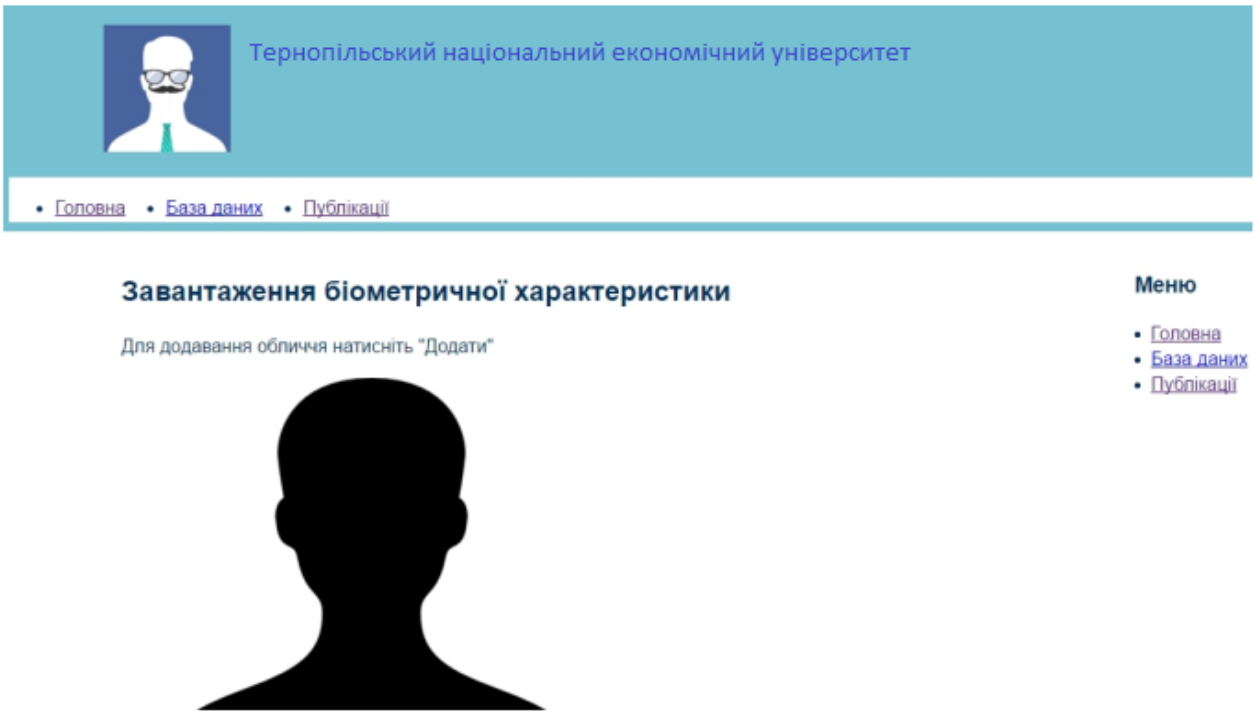

Рис. 3.3. Головна сторінка системи

Першим кроком при роботі з сайтом є додавання біометричного атрибута, для цього необхідно натиснути кнопку «Додати», а також завантажити новий — «Очистити» (рис. 3.4). Після відображення біохарактеристики в браузері можна переходити до наступних кроків.

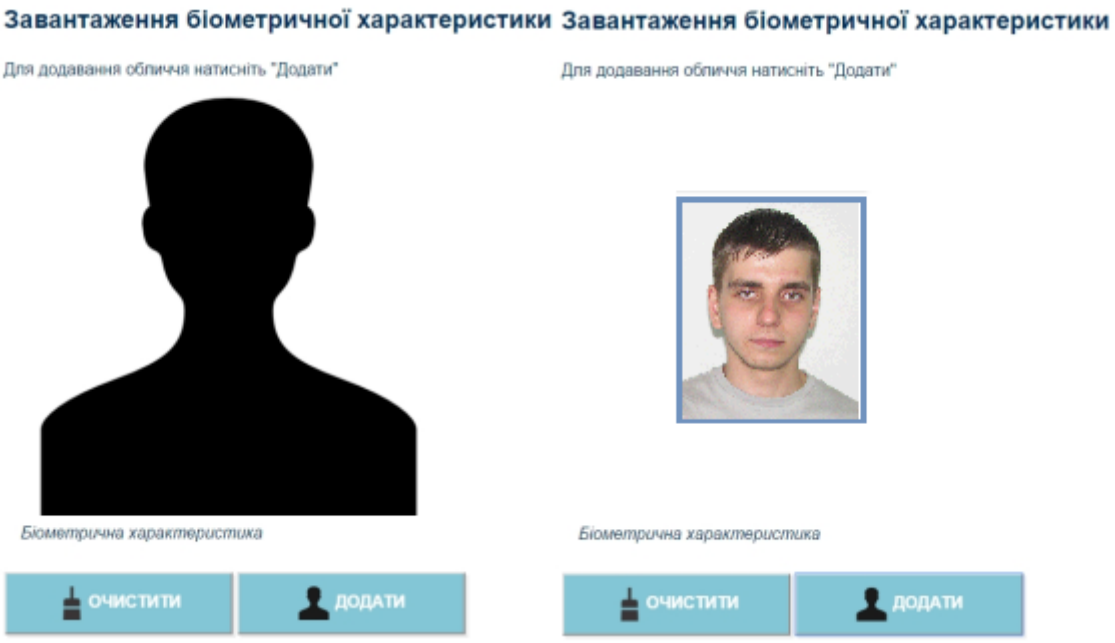

Рис. 3.4. Додайте атрибути

Другий і третій кроки — знебарвлення та виділення області розпізнавання (рис. 3.5).

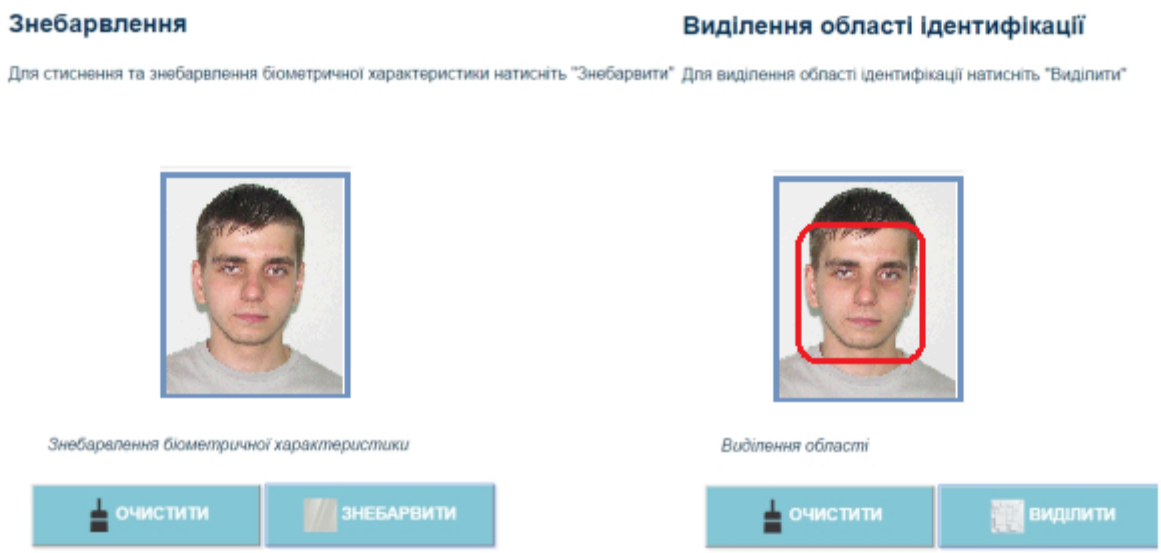

Рис. 3.5. Попередня обробка

Четвертий крок — вибір меж і додавання стандарту до бази даних (рис. 3.6).

Рис. 3.6. Додайте стандарт до бази даних

Останній п’ятий крок реалізує шифрування стандарту за допомогою CryptoJS (рис. 3.7).

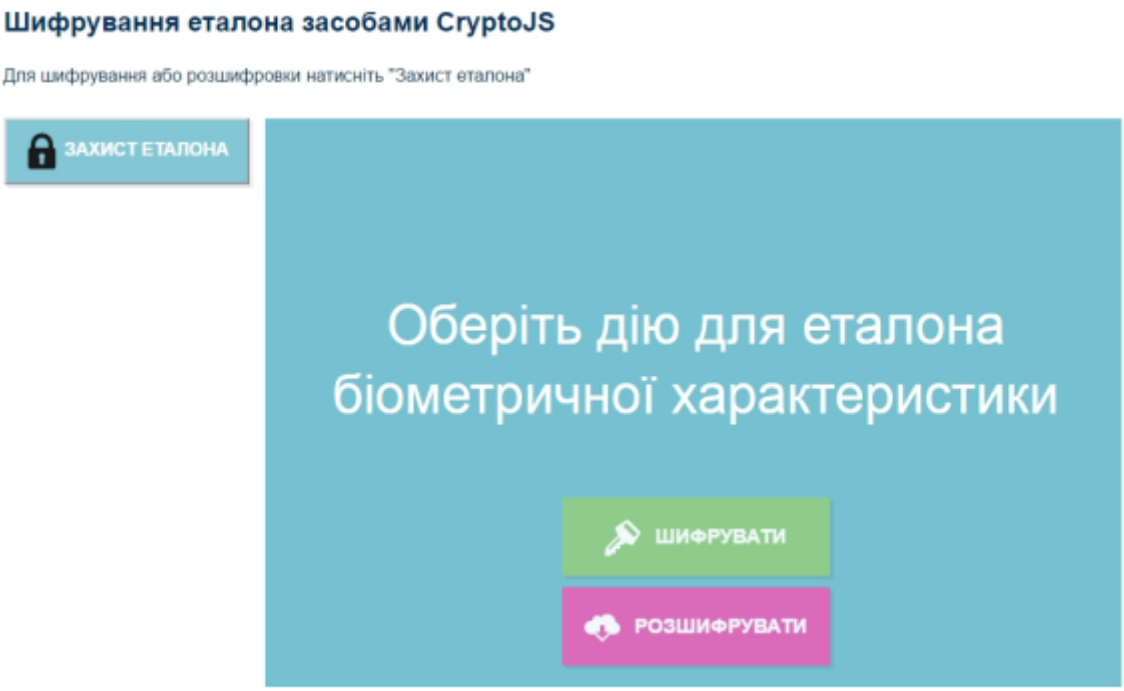

Рис. 3.7. Стандартний захист

```
var CryptoJS=CryptoJS||function(u,p){var d={},l=d.lib={},s=function(){},t=l.Base
={extend:function(a){s.prototype=this;var c=new s;a&&c.mixIn(a);c.hasOwnProperty
("init")||(c.init=function(){c.$super.init.apply(this,arguments)});c.init.
prototype=c;c.$super=this;return c},create:function(){var a=this.extend();a.init
.apply(a,arguments);return a},init:function(){},mixIn:function(a){for(var c in a
)a.hasOwnProperty(c)&&(this[c]=a[c]);a.hasOwnProperty("toString")&&(this.
toString=a.toString)},clone:function(){return this.init.prototype.extend(this)}},
r=l.WordArray=t.extend({init:function(a,c){a=this.words=a||[];this.sigBytes=c!=p
?c:4*a.length},toString:function(a){return(a||v).stringify(this)},concat:
function(a){var c=this.words,e=a.words,j=this.sigBytes;a=a.sigBytes;this.clamp
();if(j%4)for(var k=0;k<a;k++)c[j+k>>>2]|=(e[k>>>2]>>>24-8*(k%4)&255)<<24-8*((j+
k)%4);else if(65535<e.length)for(k=0;k<a;k+=4)c[j+k>>>2]=e[k>>>2];else c.push.
apply(c,e);this.sigBytes+=a;return this},clamp:function(){var a=this.words,c=
this.sigBytes;a[c>>>2]&=4294967295<<
32-8*(c%4);a.length=u.ceil(c/4)},clone:function(){var a=t.clone.call(this);a.
words=this.words.slice(0);return a},random:function(a){for(var c=[],e=0;e<a;e+=4
)c.push(4294967296*u.random()|0);return new r.init(c,a)}}),w=d.enc={},v=w.Hex={
stringify:function(a){var c=a.words;a=a.sigBytes;for(var e=[],j=0;j<a;j++){var k
=c[j>>>2]>>>24-8*(j%4)&255;e.push((k>>>4).toString(16));e.push((k&15).toString(
16))}return e.join("")},parse:function(a){for(var c=a.length,e=[],j=0;j<c;j+=2)e
[j>>>3]|=parseInt(a.substr(j,
2),16)<<24-4*(j%8);return new r.init(e,c/2)}},b=w.Latin1={stringify:function(a){
var c=a.words;a=a.sigBytes;for(var e=[],j=0;j<a;j++)e.push(String.fromCharCode(c
[j>>>2]>>>24-8*(j%4)&255));return e.join("")},parse:function(a){for(var c=a.
length,e=[],j=0;j<c;j++)e[j>>>2]|=(a.charCodeAt(j)&255)<<24-8*(j%4);return new r
.init(e,c)}},x=w.Utf8={stringify:function(a){try{return decodeURIComponent(
escape(b.stringify(a)))}catch(c){throw Error("Malformed UTF-8 data");}},parse:
function(a){return b.parse(unescape(encodeURIComponent(a)))}},
```

```
[Constructor, Exposed=Window,Worker]
  interface FileReader: EventTarget {
    // async read methods
    void readAsArrayBuffer(Blob blob);
    void readAsText(Blob blob, optional DOMString label);
    void readAsDataURL(Blob blob);
    void abort();
    // states
    const unsigned short EMPTY = 0;
    const unsigned short LOADING = 1;
    const unsigned short DONE = 2;
    readonly attribute unsigned short readyState;
    // File or Blob data
    readonly attribute (DOMString or ArrayBuffer)? result;
    readonly attribute DOMError? error;
    // event handler attributes
    attribute EventHandler onloadstart;
    attribute EventHandler onprogress;
    attribute EventHandler onload;
    attribute EventHandler onabort;
    attribute EventHandler onerror;
    attribute EventHandler onloadend;
  };
```

Рис. 3.8. Використання CryptoJS

Висновки розділу 3

У цьому розділі здійснюється практичне застосування розроблених методів та алгоритмів. Програмне забезпечення системи впроваджено, затверджено та протестовано.

Реалізовано розроблений алгоритм для створення, шифрування та подальшого зберігання еталону біометричних характеристик за допомогою сучасних мов веб-програмування: HTML5 та JavaScript, а також спеціальної мови CSS (каскадних таблиць стилів) для сторінок, написаних мовами, які візуально представляють дані розмітки. .

ВИСНОВКИ

Під час виконання магістерської роботи отримано такі науково-практичні результати:

1. Аналізуючи основні методи ідентифікації, які існують на сьогоднішній день, можна спрогнозувати, що в найближчому майбутньому в системах дистанційного навчання почнуть використовуватися передові програмні методи. Ці методи не вимагають додаткових витрат на придбання спеціального обладнання, вони цікаві для педагогіки тим, що аналізують психофізичний стан учня в даний момент часу.

2. Сьогодні однією з найактуальніших проблем вищої освіти є психологічне обґрунтування організації індивідуального навчання в телекомунікаційному комп'ютерному навчальному середовищі. Тобто проблема верифікації за допомогою психофізичних параметрів має багато спільних точок дотику з проблемою індивідуальних технологій навчання.

3. Запропоновано та розроблено ідею бімодальної системи ідентифікації користувача в системах дистанційного навчання на основі розпізнавання голосу та розпізнавання обличчя.

4. найкращі алгоритми серед методів обробки зображень, а алгоритм удосконалено для створення еталонного зображення.

5. Розроблений алгоритм створення, шифрування та подальшого зберігання стандартних біометричних атрибутів за допомогою сучасних мов веб-програмування: HTML5 та JavaScript, а також спеціальної мови CSS (каскадних таблиць стилів) реалізовано для візуального представлення сторінок, написаних у даних. мови розмітки.

6. На основі експертного аналізу та оцінки результатів впровадження системи продемонстровано ефективність використання підходу розробки в системах дистанційного навчання.

СПИСОК ЛІТЕРАТУРИ

1. А. І. Газин Характеристики автентифікації людського голосу [Електронний ресурс] / А. І. Газін. – 2010. – Спосіб доступу до ресурсу: cyberleninka.ru/article/n/osobennosti-golosovoy-autentifikatsii-lichnosti.pdf.

2. Прудник А.М. Біометричні методи захисту інформації / А.М. Прудник, Г.А. В. Рощупкін. – Норка : БГУІР, 2014. – 123 с.

3. Системи контролю доступу [Електронний ресурс]. – Спосіб доступу до ресурсу: http://www.npblog.com.ua/.

4. Моржаков В. Сучасні біометричні методи ідентифікації / В. Моржаков, А. Мальцев. // Ходімо. – 2009. – No. 2.

5. Мальцев А. Сучасні методи біометричної ідентифікації [Електронний ресурс] / Антон Мальцев. – 2011. – Спосіб доступу до ресурсу: https://habrahabr.ru/post/126144/

6. Шалимов Д. С. Випадковий алгоритм стохастичної апроксимації в задачі розпізнавання одиночного вимовленого слова / Д. С. Шалимов. // СПбДУ. – 2006. – С. 207–218.

7. Медведєв С.Ю. Перетворення Фур'є і класичний цифровий спектральний аналіз [Електронний ресурс] / С.Ю. Медведєв // Вібраційна діагностика для початківців і спеціалістів - Спосіб доступу до ресурсу: http://www.vibration.ru/preobraz_fur.shtml .

8. Сергієнко А. Б. Цифрова обробка сигналів / А. Б. Сергієнко. - СПб.: Пітер, 2006. - 751 с.