Міністерство освіти і науки України
Харківський національний університет імені В.Н. Каразіна
Факультет комп'ютерних наук
Спеціальність 125 «Кібербезпека»
Освітня програма «Безпека інформаційних та комунікаційних систем»

«Допущено до захисту»
В.о. зав. кафедрою БІСТ
Ольга МЕЛКОЗЬОРОВА
_____
« » 2023 р.

Пояснювальна записка

до кваліфікаційної роботи магістра

на тему: «Тестування систем біометричної автентифікації по голосу»

оцінка « »
Голова ЕК
Олександр ЛЕМЕШКО _____

Керівник Мелкозьорова О.М.
Рецензент Краснобаєв В.А.
Виконавець : студент групи КБ-61
Загайнов Михайло Сергійович

Харків – 2023

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Тестування систем біометричної автентифікації по голосу»: 67 с., 23 рис., 2 табл., 11 стор. додатків, 32 літературних джерел.

Робота містить вступ, три розділи, загальні висновки, список використаних джерел та один додаток.

Мета роботи: вивчення, аналіз та тестування систем біометричної автентифікації з використанням розпізнавання голосу на прикладі програмного забезпечення VoiceSens.

В ході роботи були використані наступні методи дослідження:

1) Перший метод полягав у літературному аналізі, який передбачав вивчення теоретичної бази з питань біометричної автентифікації та розпізнавання голосу. Це дозволило отримати глибше розуміння принципів роботи та контексту розглядуваної теми.

2) Другий метод включав експериментальні тести, під час яких проводилися практичні випробування з використанням програми VoiceSens для оцінки її ефективності в розпізнаванні голосу. Ці тести були спрямовані на збір даних та визначення точності та швидкості роботи програми.

Результати роботи: під час виконання дипломної роботи було проведено детальний аналіз біометричної автентифікації, зокрема на основі розпізнавання голосу. Проведено літературний пошук та вивчено основні концепції та принципи роботи біометричних систем. Далі, було визначено основні етапи та методи розпізнавання голосу. Ключовою частиною досліджень стало експериментальне тестування програми VoiceSens, включаючи збір голосових даних та аналіз їх результатів.

Результати дослідження вказують на високий рівень ефективності програм голосової аутентифікації на прикладі програмного забезпечення

VoiceSens. Основною новизною є виявлення високої точності та швидкості розпізнавання голосу за допомогою цієї програми.

Рекомендації щодо використання результатів роботи: Результати роботи можуть бути використані для подальшого вдосконалення систем біометричної автентифікації на основі голосу, а також для впровадження цієї технології у сфері інформаційної безпеки та автентифікації користувачів.

Значущість роботи та висновки: Дипломна робота висвітлює важливий аспект сучасних інформаційних технологій - біометричну автентифікацію на основі голосу. Результати дослідження підтверджують високий потенціал цієї технології у питаннях ідентифікації користувачів.

Можливими напрямками розвитку є подальше вдосконалення алгоритмів розпізнавання голосу, розширення сфери застосування біометричної автентифікації по голосу, а також розробка нових програмних рішень у цій галузі.

Ключові слова: БІОМЕТРИЧНА АВТЕНТИФІКАЦІЯ, ТЕСТУВАННЯ, РОЗПІЗНАВАННЯ ГОЛОСУ, ІДЕНТИФІКАЦІЯ КОРИСТУВАЧІВ, БІОМЕТРИЧНІ ПАРАМЕТРИ, ІНФОРМАЦІЙНА БЕЗПЕКА.

ABSTRACT

Explanatory note to the qualification work "Testing of biometric authentication systems by voice": 67 p., 23 fig., 2 table, 11 p. applications, 32 literary sources.

The work contains an introduction, three chapters, general conclusions, a list of used sources and one appendix.

The purpose: study, analysis and testing of biometric authentication systems using voice recognition on the example of the VoiceSens software.

The following research methods were used during the work:

1) The first method consisted in a literary analysis, which involved the study of the theoretical base on the issues of biometric authentication and voice recognition. This made it possible to gain a deeper understanding of the principles of work and the context of the topic under consideration.

2) The second method included experimental tests, during which practical tests were carried out using the VoiceSens program to evaluate its effectiveness in voice recognition. These tests were aimed at collecting data and determining the accuracy and speed of the program.

Work results: during the thesis, a detailed analysis of biometric authentication, in particular based on voice recognition, was carried out. A literature search was conducted and the basic concepts and principles of biometric systems were studied. Next, the main stages and methods of voice recognition were determined. A key part of the research was the experimental testing of the VoiceSens program, including the collection of voice data and analysis of their results.

The results of the study indicate a high level of effectiveness of voice authentication programs using the VoiceSens software as an example. The main novelty is the detection of high accuracy and speed of voice recognition with the help of this program.

Recommendations for using the results of the work: The results of the work can be used for further improvement of voice-based biometric authentication systems, as well as for the implementation of this technology in the field of information security and user authentication.

Significance of the work and conclusions: The thesis highlights an important aspect of modern information technologies - voice-based biometric authentication. The results of the study confirm the high potential of this technology in matters of user identification.

Possible areas of development are the further improvement of voice recognition algorithms, the expansion of the scope of application of voice biometric authentication, as well as the development of new software solutions in this field.

Keywords: BIOMETRIC AUTHENTICATION, TESTING, VOICE RECOGNITION, USER IDENTIFICATION, BIOMETRIC PARAMETERS, INFORMATION SECURITY.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

БА — Біометрична аутентифікація

ГШ — Голосові шаблони

ПЗ — Програмне забезпечення

МА — Методи аутентифікації

ІБ — Інформаційна безпека

СА — Системи аутентифікації

FAR — False Acceptance Rate

FRR — False Rejection Rate

ВСТУП

Актуальність. Сучасний світ насичений інформаційними технологіями, інтернет-сервісами та електронними системами, що вимагають забезпечення безпеки даних та доступу до них. У зв'язку з цим, питання ідентифікації та аутентифікації користувачів стає надзвичайно важливим. Традиційні методи аутентифікації, такі як паролі або PIN-коди, стають уразливими перед сучасними загрозами, такими як фішинг, витік даних та хакерські атаки.

У цьому контексті біометрична аутентифікація набуває особливого значення. Біометричні технології базуються на унікальних фізіологічних та поведінкових характеристиках особи, таких як відбитки пальців, розпізнавання обличчя, сканування голосу тощо. Один з цих методів — розпізнавання голосу, стає все популярнішим завдяки своїй надійності та природній спрощеній процедурі аутентифікації.

Проте для успішного впровадження систем біометричної аутентифікації, включаючи розпізнавання голосу, необхідно провести детальне вивчення та аналіз таких систем, а також визначити їх ефективність та недоліки. Дана дипломна робота має на меті вивчення, аналіз та тестування системи біометричної автентифікації по голосу на прикладі програмного забезпечення VoiceSens, що сприятиме дослідженню можливостей цієї технології та надасть рекомендації для подальшого використання в сферах інформаційної безпеки, банківського сектору, медицини та багатьох інших галузях.

Отже, можна зазначити, що актуальність даної дипломної роботи полягає у необхідності дослідження та вдосконалення методів аутентифікації в епоху зростаючої кіберзагрози та цифрової трансформації суспільства.

Об’єкт дослідження: системи біометричної автентифікації, зокрема системи, які використовують розпізнавання голосу для ідентифікації користувачів.

Предмет дослідження: технології, методи, та системи біометричної автентифікації по голосу, зокрема програма VoiceSens. Дослідження включає вивчення основних понять біометричної автентифікації, аналіз технологій розпізнавання голосу та їх застосування в інформаційній безпеці, а також тестування та опис роботи програми VoiceSens.

Мета роботи: вивчення, аналіз та тестування систем біометричної автентифікації з використанням розпізнавання голосу на прикладі програмного забезпечення VoiceSens.

Для досягнення поставленої мети необхідно виконати наступні завдання:

- Провести огляд основних концепцій та понять біометричної автентифікації з використанням розпізнавання голосу;
- Дослідити принципи роботи систем біометричної автентифікації по голосу, зокрема, розібратися у процесі збору та обробки голосової інформації;
- Вивчити та проаналізувати різні методи обробки та порівняння голосових шаблонів для забезпечення точності розпізнавання голосу;
- Вивчити можливості впровадження голосової біометрії в інформаційну безпеку та системи автентифікації користувачів, оцінити переваги цього методу для забезпечення безпеки даних та об'єктів;
- Провести аналіз системи біометричної автентифікації по голосу VoiceSens, визначити основні характеристики та компоненти програми;
- Вивчити функції та алгоритми реєстрації та аутентифікації користувачів за допомогою біометричної автентифікації по голосу в VoiceSens;

- Провести тестування системи VoiceSens з метою оцінки її продуктивності, точності та надійності;
- Описати результати тестування та зробити висновки щодо ефективності та можливого використання системи біометричної автентифікації в майбутньому;

Результати даної дипломної роботи мають практичне застосування в сферах інформаційної безпеки, банківського сектору та наукових досліджень. Зокрема, вони можуть бути використані для підвищення рівня безпеки в інформаційних системах, безпечної аутентифікації клієнтів у банківських системах та подальшого наукового дослідження в галузі біометричної аутентифікації. Ці результати також взаємодіють з існуючими дослідженнями та розширюють базу знань в галузі розпізнавання голосу та біометричної аутентифікації.

1 ОГЛЯД ОСНОВНИХ ПОНЯТЬ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ

1.1 Визначення та види біометричних параметрів

Біометричні параметри — це вимірювальні фізичні характеристики або особистісні поведінкові риси, які використовуються для ідентифікації (впізнання) особи або верифікації наданої ідентифікаційної інформації про особу (ст. 3 Закону ЄДДР).[20]

Біометрія — це сукупність автоматизованих методів і засобів ідентифікації людини, заснованих на її фізіологічній або поведінковій характеристиці.

За сучасних умов розвитку суспільства проблема безпеки постає у новому аспекті – значна кількість об’єктів, яким потрібно забезпечити безпеку, надана у вигляді інформації, яка зберігається в електронних комп’ютерних системах та передається через мережі зв’язку. Тобто, виник новий аспект безпеки — захист інформації. Причому в даному випадку необхідно забезпечити декілька рівнів захисту — обмежити фізичний доступ до електронних комп’ютерних систем (серверів), де зберігається інформація, забезпечити доступ до роботи з інформацією тільки акредитованим особам, забезпечити контроль фізичного доступу до приміщень, де знаходяться сервери і т. ін.

Існує цілий комплекс заходів із забезпечення захисту інформації, проте вони не є на сто відсотків ефективними. Для підвищення ефективності систем захисту останнім часом пропонується використовувати так звані біометричні системи ідентифікації. Біометричні системи ідентифікації встановлюють особу за індивідуальними біометричними параметрами людини. [30] (Рис. 1.1)

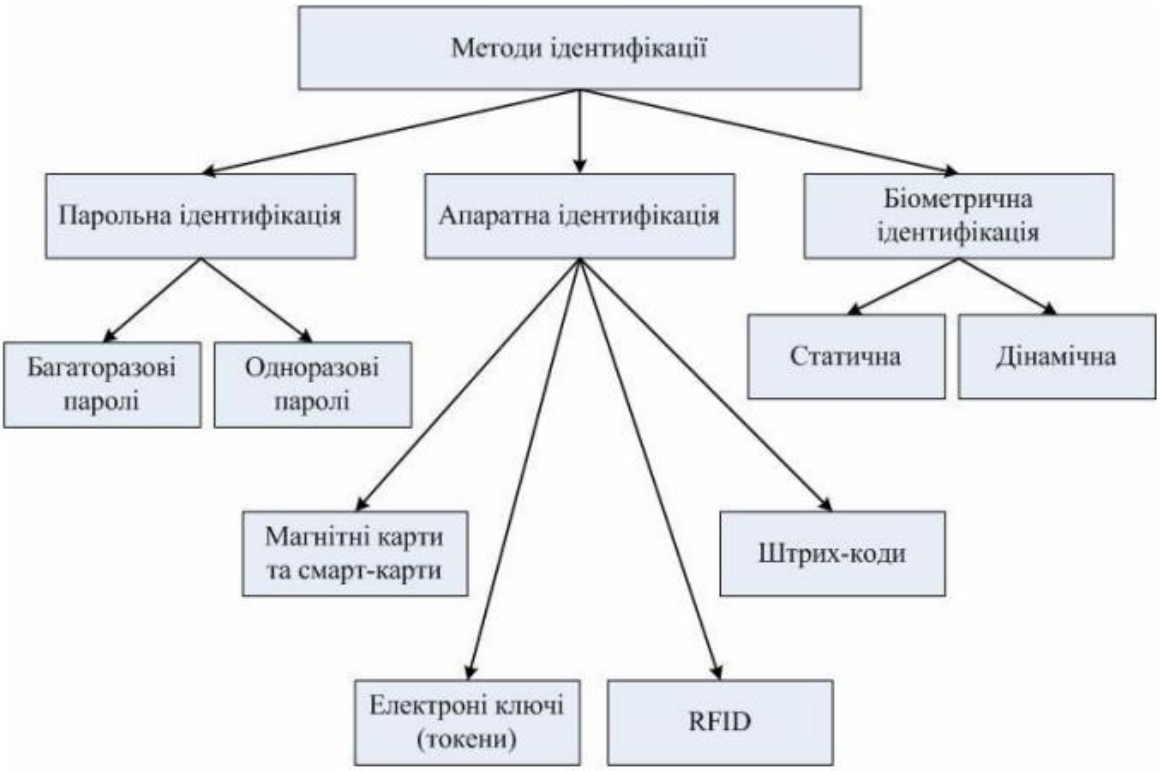

Рис. 1.1 — Класифікація методів ідентифікації

Сьогодні завдяки розвитку технологій крім відбитків пальців, голосу та підпису можна використовувати ще декілька біометричних ознак. До фізіологічних методів ідентифікації відносяться[4]:

1) Ідентифікація за відбитками пальців.

2) Ідентифікація за формою долоні.

3) Ідентифікація за сітчаткою ока.

4) Ідентифікація за геометрією обличчя.

5) Ідентифікація за розташуванням вен на лицьовій стороні долоні.

6) Ідентифікація за термограмою обличчя (розташування артерій під шкірою обличчя).

7) Ідентифікація за райдужною оболонкою ока.

8) Ідентифікація за геометрією вуха.

9) Ідентифікація за допомогою ДНК.

Психологічних методів значно менше і до них відносяться:

1) Ідентифікація за голосом.

2) Ідентифікація за підписом (або почерком).

3) Ідентифікація за клавіатурним почерком.

Загальна класифікації методів аутентифікації за біометричними параметрами показана на рис. 1.2

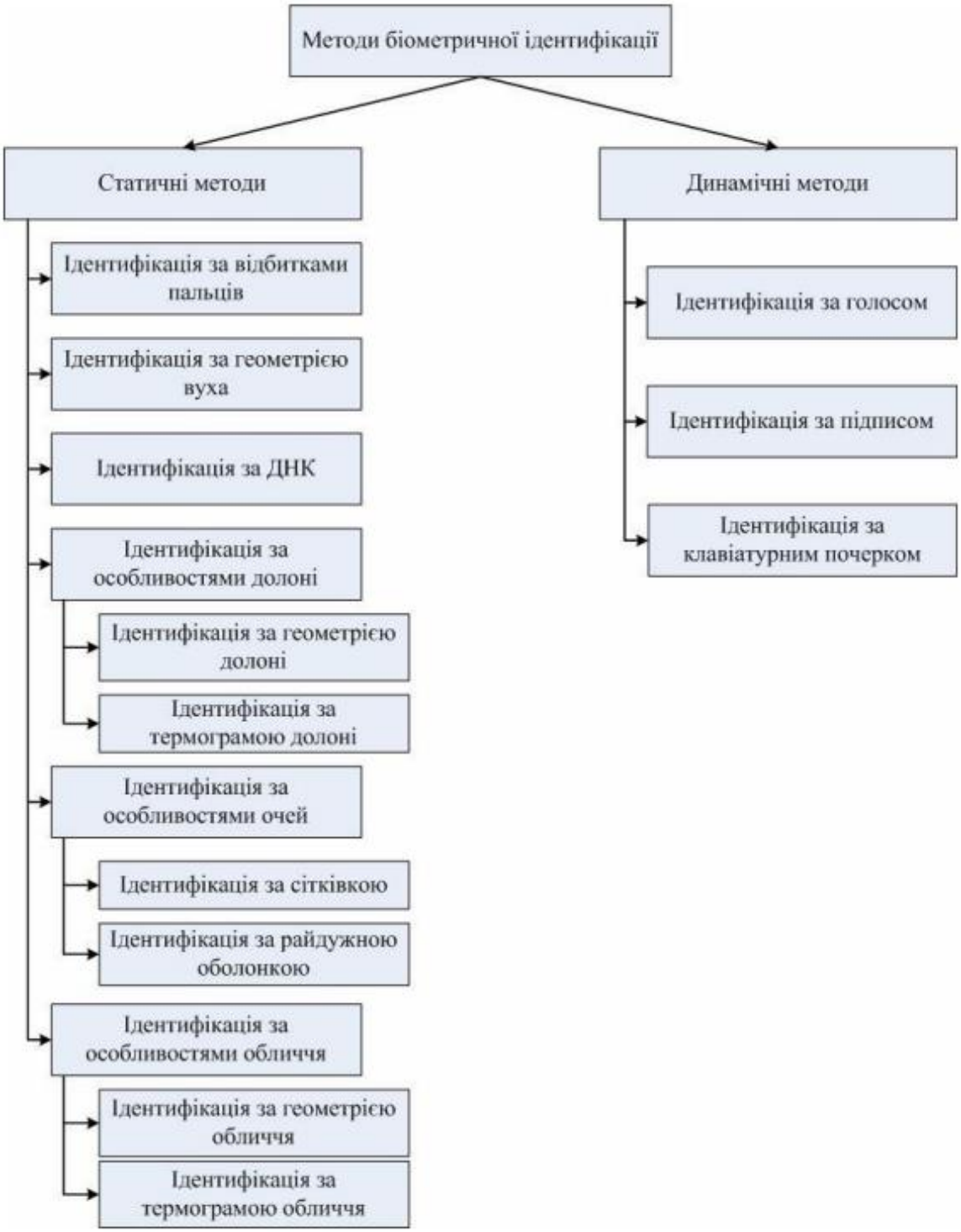

Рис. 1.2 — Класифікація методів біометричної ідентифікації

На сьогодні існує близько 20-ти біометричних ідентифікаторів, які можна використовувати, проте історично так склалось, що до найбільш розповсюджених методів біометричної ідентифікації відносяться способи, засновані на використанні наступних біометричних ідентифікаторів[19]:

– відбитки пальців;

– райдужна оболонка ока;

– сітківка ока;

– геометрія обличчя;

– геометрія долоні;

– почерк (або підпис);

– ідентифікація за голосом.

1.2 Принципи роботи систем біометричної аутентифікації

Аутентифікація — це засіб захисту, що встановлює справжність особи, що отримує доступ до автоматизованої системи, шляхом зіставлення повідомленого ним ідентифікатора та пред’явленого підтверджуючого фактора.

Для аутентифікації користувача використовуються такі фактори:

- деяка секретна інформація, Наприклад логін та пароль. Введені дані порівнюються зі відомостями, що зберігаються у спеціальній базі даних, і у разі збігу користувач пропускається до системи. Це найпопулярніший, найпростіший і найменш захищений спосіб перевірки його справжності. Найбільш поширені методи отримання шахраями таких даних аутентифікації називаються фішингом та фармінгом;
- унікальний предмет або технічний пристрій (смарт-карта, USB-токен (eToken) та ін.). Забезпечує серйозніший захист, ніж парольна автентифікація, але також має ряд недоліків. Наприклад, такий предмет може бути викрадений;
- біометрія. Заснована на унікальності ряду характеристик людини – відбитків пальців або долоні, голосу, візерунку райдужної оболонки ока та структури його сітківки тощо.[18]

Під час автентифікації облікові дані, надані користувачем, порівнюються з даними у файлі в базі даних користувача авторизованих користувачів або в локальній операційній системі, або через сервер аутентифікації. Якщо облікові дані збігаються, і автентифікований суб'єкт має право використовувати ресурс, процес завершується, і користувачеві надається доступ. Надані дозволи та папки визначають як середовище, яке бачить користувач, так і спосіб взаємодії з нею, включаючи годинник доступу та інші права, такі як обсяг простору ресурсів.

Традиційно автентифікація здійснювалася системами чи ресурсами, яких здійснюється доступ; наприклад, сервер аутентифікації користувачів,

використовуючи свою власну систему паролів, реалізовану локально, використовуючи ідентифікатори входу (імена користувачів) та паролі.

Передбачається, що знання облікових даних для входу гарантує дійсність користувача. Кожен користувач спочатку реєструється (або зареєстрований кимось іншим, наприклад, системним адміністратором), використовуючи призначений або самостійно оголошений пароль. При кожному наступному використанні користувач повинен знати та використовувати раніше оголошений пароль.[25]

Загальний алгоритм біометричної аутентифікації включає такі основні етапи:

1) Захоплення біометричних даних. Перший крок полягає в зборі біометричних даних від користувача. Це може бути відбиток пальця, зразок голосу, фотографія обличчя, скан сітківки ока або інші унікальні біологічні параметри.

2) Екстракція характеристик. Отримані біометричні дані перетворюються на числовий формат, що можна обробити. Це включає в себе виділення основних характеристик або шаблонів, які будуть використовуватися для подальшого порівняння та аутентифікації.

3) Збереження характеристик. Характеристики, отримані на попередньому етапі, зберігаються в базі даних або в безпечному місці. Важливо забезпечити конфіденційність і цілісність цих даних.

4) Подальша аутентифікація або ідентифікація. Користувач надає свої біометричні дані для аутентифікації. Отримані дані порівнюються зі збереженими характеристиками. Якщо це аутентифікація, то система визначає, чи належать ці дані визначеному користувачеві. Якщо це ідентифікація, то система визначає, до якого користувача належать ці дані.

5) Порівняння характеристик. Система виконує порівняння отриманих біометричних характеристик зі збереженими у базі даних. Це може

включати в себе різні методи порівняння, такі як порівняння відстані, порівняння шаблонів тощо.

6) Прийняття рішення. На основі результатів порівняння система приймає рішення про успішну аутентифікацію чи ідентифікацію користувача. Якщо біометричні дані користувача відповідають збереженим даним, то аутентифікація вважається успішною.

7) Видача доступу або відмова. У разі успішної аутентифікації користувачеві надається доступ до системи, або йому дозволяється виконувати певні дії. У випадку невдачі користувачеві може бути відмовлено в доступі.[29]

Загальну спрощену схему біометричної аутентифікації зображено на рис. 1.3

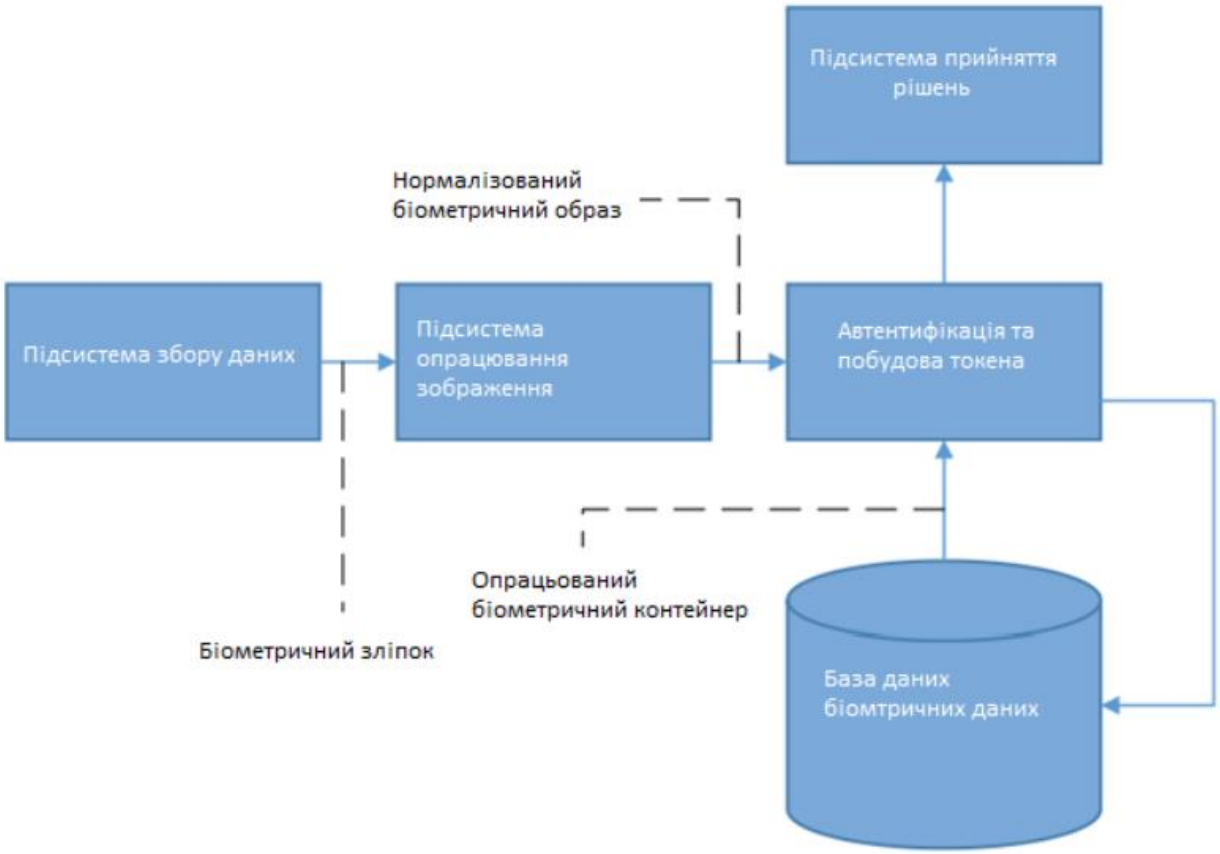

Рис. 1.3 — Спрощена схема біометричної аутентифікації

1.3. Сфери застосування біометричної аутентифікації

Біометрична аутентифікація широко використовується в різних сферах і галузях через свою надійність і зручність. Далі розглянемо основні сфери застосування біометричної аутентифікації.

1) Управління доступом.

Цей варіант використовується для отримання доступу до комп'ютерної мережі, як на території підприємства чи корпорації, так і через безпечний віддалений зв'язок з віддаленої локації.

Зазвичай для забезпечення безпеки використовуються традиційні ім'я користувача та пароль. Однак ця комбінація, можливо, ефективно працювала у минулому, але зараз вона виявляє важкі ознаки вразливості, оскільки стала основною метою для кібератак.

Імена користувача та паролі можуть легко піддаватися компрометації та перехопленню за допомогою атак типу "Відмова в обслуговуванні" або словникового атак.

Через часту появу таких атак багато організацій зараз вимагають від своїх співробітників створювати довгі та складні паролі, які містять комбінацію великих і малих літер, розділових знаків, пробілів, цифр та інших спеціальних символів.

Через складність запам'ятовування таких паролів працівники буквально записують їх на стікерах Post-It і прикріплюють до монітора свого робочого місця. Цей явище стало відоме як "синдром Post-It." Для боротьби з цими та іншими вразливостями безпеки використовується технологія біометричної ідентифікації для їх повного заміщення.

У цьому контексті найчастіше використовуються два методи: розпізнавання за відбитками пальців (рис. 1.4) та розпізнавання за радужками. За одним рухом пальця або одним скануванням радужки працівник може увійти в свою робочу станцію всього за одну секунду.

Рис. 1.4 — Управління доступом за відбитком пальця

Через таку можливість, ці методи також називають "Один Вхід" або "Один Вхід для Всіх" рішеннями. Ці пристрої можна підключити до робочої станції через USB або вбудовувати безпосередньо в комп'ютер чи бездротовий пристрій.[12]

2) Фізичний доступ.

Фізичний доступ відноситься до надання співробітнику підприємства чи корпорації доступу до безпечної будівлі, навіть до безпечного офісу всередині неї. Традиційно використовуються ключі та бейджі. Однак основна проблема полягає в тому, що ці інструменти можуть бути дуже легко вкрадені, втрачені, скопійовані або навіть передані іншим співробітникам, які не повинні мати доступ до цих безпечних зон.

Смарт-карти використовуються для подолання цих вразливостей безпеки, але вони також мають свій набір обмежень. У цій області найчастіше використовуються Розпізнавання за відбитками пальців (рис. 1.5), розпізнавання за геометрією руки, а також Розпізнавання за венозними малюнками. У цих випадках одну з цих біометричних систем підключають до електромагнітного замка.

Рис. 1.5 —Фізичний доступ за відбитком пальця

Як тільки особу ідентифіковано за відбитками пальців або формою їхньої руки, замок відчиняється за кілька секунд. Основні переваги використання біометрії наступні:

- Більше не втрачаються, не викрадаються і не використовуються шахраянський ключі і бейджі.
- Доступ до будь-яких безпечних зон, до яких потрібен доступ, мають лише законні співробітники, чий ідентифікацію було підтверджено на 100%.

У сценаріях фізичного доступу біометричний пристрій для розпізнавання відбитків пальців або сканер геометрії руки можуть працювати як у самостійному режимі, так і в клієнт-серверному режимі.

3) Документи що посвідчують особу

Електронний паспорт містить мікрочіп, який зберігає ту саму біометричну інформацію, що й звичайний паспорт. Чіп зберігає цифрове зображення фотографії власника паспорта, яке пов’язане з його іменем та іншою інформацією, яка його ідентифікує. Електронний паспорт видається в електронному вигляді органом країни видачі, який перевіряє особу заявника за відбитками пальців або іншою біометричною інформацією та підтверджує дані в чіпі інформацією, наданою заявником перед видачею паспорта.(рис. 1.6)

Рис. 1.6 — Закордонний паспорт з відбитками пальців

4) Правоохоронна сфера. Правоохоронні органи використовують різні види біометричних даних для ідентифікації. Державні та федеральні органи використовують відбитки пальців, риси обличчя, малюнки райдужної оболонки ока, зразки голосу та ДНК. Це робить їм швидшим і легшим доступ до конфіденційної інформації. Зазвичай правоохоронні органи використовують навченого експерта, щоб порівняти зображення відбитка пальця з відбитками у файлі. Сьогодні AFIS (Автоматизована система ідентифікації відбитків пальців) може зіставити відбиток пальця з базою даних мільйонів відбитків за лічені хвилини.[16]

5) Облікові записи. Біометрична автентифікація стає все більш популярною як додатковий рівень безпеки для облікових записів в Інтернеті. Ця технологія використовує фізичні характеристики, такі як відбитки пальців (рис. 1.7) або розпізнавання обличчя, для перевірки особистості користувача. Завдяки впровадженню біометричної автентифікації у свої протоколи безпеки онлайн-сервіси можуть посилити захист даних користувачів і зменшити ризик кібератак. [29]

Рис. 1.7 — Доступ до облікового запису за відбитком пальця

Біометрична автентифікація усуває потребу в традиційних паролях та іменах користувачів, які можна легко вкрасти або вгадати. Натомість біометрія базується на унікальних ідентифікаторах, таких як відбитки пальців, які неможливо відтворити. Це ускладнює доступ хакерів до облікових записів користувачів, оскільки кожен окремий обліковий запис має бути підтверджено унікальним біометричним ідентифікатором.

Крім того, біометрична автентифікація безпечніша за традиційні паролі. Це запобігає доступу неавторизованих користувачів до облікових записів користувачів, оскільки біометрична автентифікація вимагає відповідного

біометричного сканування від користувача. Крім того, біометрична автентифікація додає додатковий рівень безпеки, оскільки вимагає від користувачів фізичного пред’явлення свого біометричного ідентифікатора, щоб отримати доступ до своїх облікових записів. Цей додатковий захист допомагає гарантувати безпеку даних користувача.

Окрім покращення захисту даних користувачів, біометрична автентифікація також надає користувачам більш зручний спосіб доступу до своїх облікових записів. Ця технологія позбавляє користувачів від необхідності запам’ятовувати складні паролі, оскільки вони можуть просто використовувати свій біометричний ідентифікатор для входу. Це також допомагає зменшити час, витрачений на процеси входу, оскільки користувачі можуть швидко та легко отримати доступ до своїх облікових записів за допомогою одного сканування.

Загалом біометрична автентифікація є ефективним способом підвищення безпеки в Інтернеті та захисту даних користувачів. Впроваджуючи цю технологію в свої протоколи безпеки, онлайн-сервіси можуть гарантувати, що дані користувачів залишаються в безпеці.[27]

2 АНАЛІЗ ТЕХНОЛОГІЇ ТА МЕТОДИ РОЗПІЗНАВАННЯ ГОЛОСУ

2.1 Основні етапи та компоненти систем біометричної аутентифікації по голосу

Системи аутентифікації особи за голосом працюють у режимах реєстрації (ідентифікації) та аутентифікації. Основними етапами роботи системи аутентифікації в режимі реєстрації є:

1) відбір голосових даних з пристрою введення (мікрофону);
2) дискретизація вхідних даних.
3) попередня фільтрація отриманого сигналу;
4) мінімізація діагностичних характеристик шляхом розкладу в «ряди» (отримання коефіцієнтів розкладу)
5) формування біометричного еталону на основі кількаразового повтору особою ключової фрази (голосового паролю).

На етапі 5 система повинна визначити стабільність еталону: якщо коридор допустимих значень (який може визначатись на основі дисперсії) буде надто великим, то процедура реєстрація має бути проведена повторно.

До основних етапів роботи системи аутентифікації за голосом людини належать:

1) відбір голосових даних з пристрою введення (мікрофону);
2) дискретизація
3) попередня фільтрація отриманого сигналу;
4) мінімізація діагностичних характеристик шляхом розкладу в «ряди» (отримання коефіцієнтів розкладу)
5) порівняння набору отриманих коефіцієнтів з еталонними коефіцієнтами в рамках допустимого коридору значень зареєстрованої особи — процес аутентифікації.[26]

Біометрична система, по суті, є системою розпізнавання образів, яка розпізнає користувача шляхом визначення автентичності конкретної анатомічної чи поведінкової характеристики, якою володіє користувач. При розробці практичної біометричної системи необхідно враховувати кілька важливих питань. По-перше, користувач має бути зареєстрований у системі, щоб можна було отримати його біометричний шаблон або посилання. Цей шаблон надійно зберігається в центральній базі даних або на смарт-картці, виданій користувачеві. Шаблон використовується для зіставлення, коли потрібно ідентифікувати особу. Залежно від контексту біометрична система може працювати або в режимі перевірки (автентифікації), або в режимі ідентифікації.

Розпізнати особу можна двома способами: верифікація та ідентифікація. Верифікація (чи я є тим, за кого себе видаю?) передбачає підтвердження або спростування заявленої особи особи. З іншого боку, під час ідентифікації система має розпізнати особу (Хто я?) зі списку з N користувачів у базі даних шаблонів. Ідентифікація є складнішою проблемою, оскільки вона передбачає зіставлення 1:N порівняно зі збігом 1:1 для перевірки.[5]

Схематично процес аутентифікації по голому проілюстровано нижче. (Рис. 2.1)

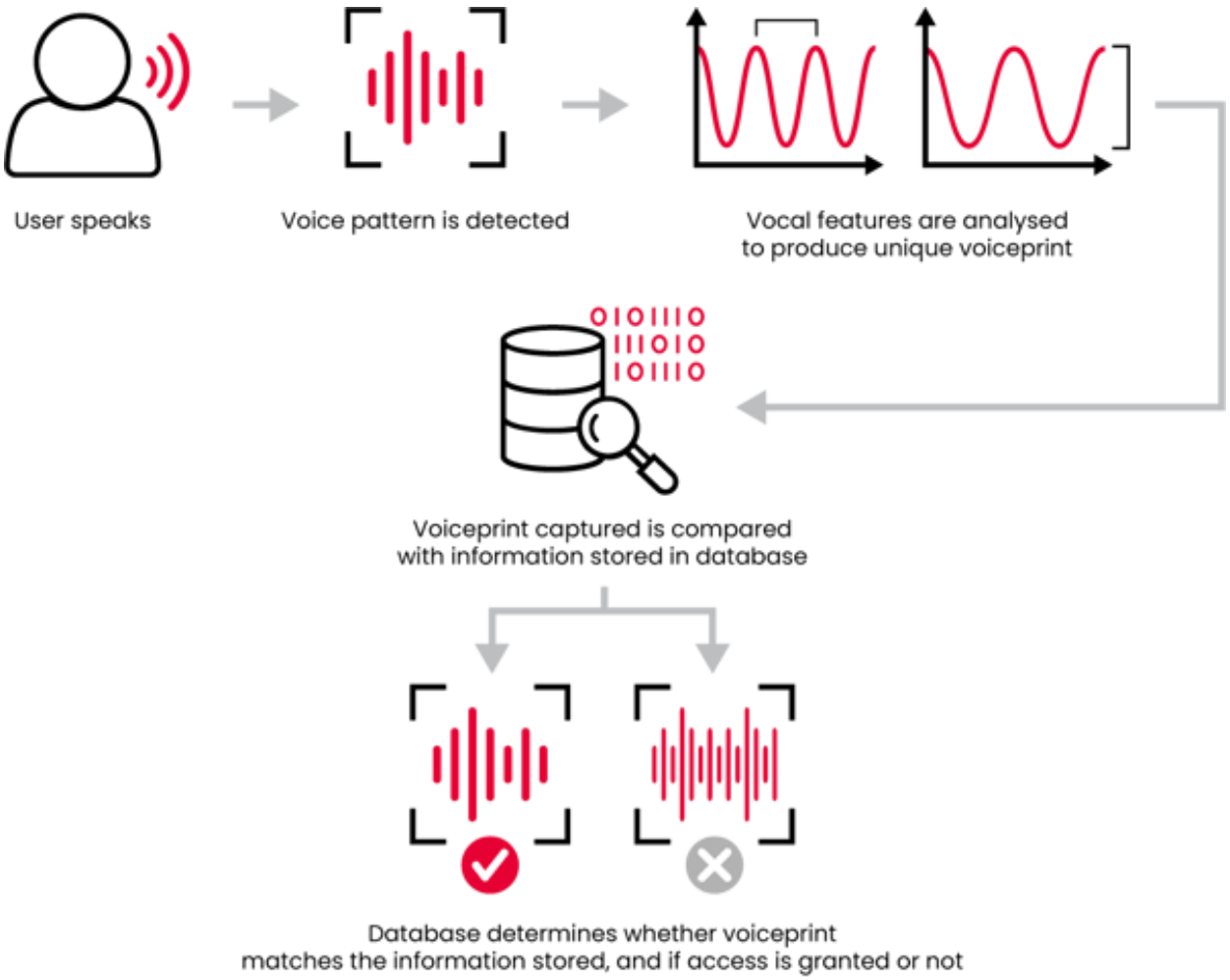

Рис. 2.1 — Схема аутентифікації по голому

Нижче наведено детальний опис цього процесу:

1) Реєстрація голосового шаблону. Перший крок полягає в реєстрації голосового шаблону користувача. Під час цього процесу, користувачу пропонується вимовити певні фрази або числа, які система записує. Голосовий зразок користувача обробляється і зберігається як голосовий шаблон. Цей голосовий шаблон включає в себе унікальні вокальні особливості користувача.

2) Аналіз вокальних особливостей. Система аналізує вокальні особливості голосового зразка, включаючи частоту основного тону, мел-кепстральні коефіцієнти, інтонацію та інші характеристики голосу.

3) Створення унікального голосового відбитку. На основі аналізу вокальних особливостей створюється унікальний голосовий "відбиток"

користувача. Цей відбиток представляє собою компактне представлення вокальних характеристик користувача.

4) Користувач говорить. Під час подальших спроб аутентифікації, користувач надає голосовий зразок, просто вимовляючи певні фрази або числа.

5) Порівняння голосових відбитків. Система порівнює голосовий зразок, наданий користувачем, з голосовим відбитком, який зберігається в базі даних. Це порівняння використовує різні метрики схожості для оцінки ступеня відповідності між двома відбитками.

6) Визначення доступу. База даних визначає, чи голосовий відбиток, наданий користувачем, відповідає збереженій інформації. Якщо ступінь подібності перевищує певний поріг, то аутентифікація вважається успішною, і користувач має доступ до системи або облікового запису.

7) Результат аутентифікації. В залежності від результату аутентифікації, система приймає рішення про надання або відмову в доступі до облікового запису або системи.[14]

Хоча голосова біометрія пропонує безпечний спосіб автентифікації користувачів, вона не захищена від загроз. Прогрес у машинному навчанні, технологіях запису та синтетичного мовлення дає змогу підмінювати високоякісний голос або «глибокі підробки» голосу, які здатні змусити людей і голосові біометричні системи подумати, що вони чують справжню особу. Ці атаки можуть бути використані для отримання несанкціонованого доступу до облікових записів.

Для боротьби з підробкою голосу потрібна технологія виявлення живості, здатна розрізняти живий голос від записаної, синтетичної або згенерованої комп’ютером версії голосу.[17]

2.2 Методи обробки та порівняння голосових шаблонів

Результати ідентифікації особи за голосом повністю залежить від вхідних даних, математичних алгоритмів та обчислювальної потужності. Під вхідними даними розуміють зразок голосу особи, отриманий за допомогою запису з мікрофона.

Якість такого зразка залежить від типу пристрою введення (наприклад, професійний мікрофон або мобільний телефон) і навколишнього середовища (гучна вулиця або тихе приміщення). Математичні алгоритми використовуються для того, щоб порівняти отриманий голосовий зразок із зразками в базі даних. Під обчислювальною потужністю розуміють швидкість і якість обробки біометричних ознак користувача, що залежить від апаратних особливостей системи.

Системи ідентифікації особи за голосом поділяються на два основних види: текстозалежні і текстонезалежні. У текстозалежних методах особа повинна сказати одну і ту ж парольну фразу під час навчання системи і під час розпізнавання голосу. Текстонезалежні системи можуть ідентифікувати особу незалежно від того, що вона сказала.[23]

Алгоритм трансформації звуку для обробки мовного сигналу може бути поділений на кілька етапів, включаючи наступні кроки (рис.):

1) Мовний сигнал (амплітуда). Початковий звуковий сигнал, отриманий від мікрофона або завантажений з аудіофайлу, представляє собою амплітуду звуку відносно часу. Цей сигнал може бути аналізований та оброблений для вилучення корисної інформації.[24]

2) Каркаси та вікна. Мовний сигнал поділяється на короткі фрагменти, відомі як каркаси. Для зменшення впливу спектральних переходів, кожен каркас зазвичай згладжується за допомогою функції вікна, такої як функція Хеммінга. Це створює перекриваючіся віконні фрагменти, які дозволяють аналізувати спектральні характеристики в різні моменти часу.

3) Короткі фрагменти мовлення. Кожен короткий фрагмент мовного сигналу представляється як амплітуда звуку відносно часу. Ці фрагменти служать основою для подальшого аналізу.

4) Обчислення Дискретного Перетворення Фур'є (ДПФ). Для кожного короткого фрагмента обчислюється ДПФ, що перетворює сигнал із часового домену в частотний домен. Результатом є спектральна інформація, яка показує, які частоти присутні у фрагменті.[30]

5) Спектральна мова. Спектральна мова представляється у вигляді часової послідовності спектрів, де кожен спектр відображає частотні компоненти на певний момент часу. Вона дозволяє аналізувати зміни у спектральних характеристиках звуку.[24]

6) Обчислення спектральної потужності. Абсолютне значення амплітуди в кожному спектрі може бути піднесено до квадрата, щоб отримати спектральну потужність. Ця інформація вказує на силу різних частот у кожному фрагменті мовлення.

7) Фільтрбанк та журнал Filterbank. Зазвичай застосовують фільтрбанк Мела для створення мел-шкали фільтрів. Ці фільтри використовуються для отримання вагованих спектральних характеристик, які відображають спектральні компоненти у більш "мовному" форматі. Може також бути виконано логарифмування для отримання журналу спектральної потужності.

8) MFCC (Мел-кепстральні коефіцієнти). Остаточні характеристики, які використовуються для аналізу мови, можуть бути обчислені на основі мел-шкали фільтрів та спектральної потужності. MFCC - це набір коефіцієнтів, які добре підходять для аналізу та розпізнавання мови.

Схематично алгоритм трансформації звуку для обробки мовного сигналу наведено на рис. 2.2

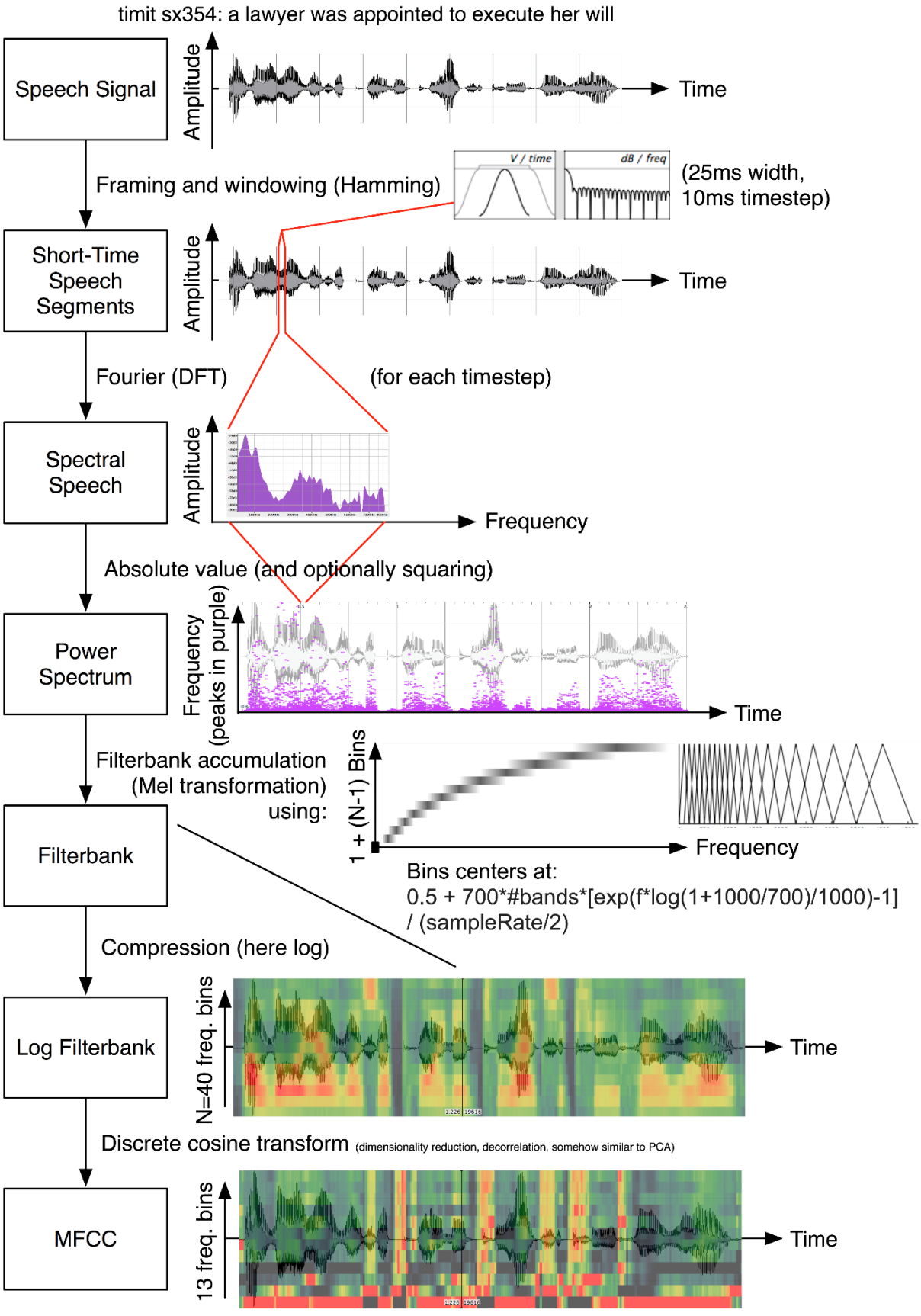

Рис. 2.2 — Алгоритм трансформації звуку

Два популярні набори ознак, часто використовувані в аналізі мовленнєвого сигналу, — це коефіцієнти Мел-частотного кепстрового перетворення (MFCC) та коефіцієнти лінійного передбачення (LPCC). Найпоширеніші моделі розпізнавання — це векторна квантизація (VQ), динамічне віддалення часу (DTW) і штучна нейронна мережа.

Коефіцієнти Мел-частотного кепстрового перетворення (MFCC) — це набір числових значень, що використовуються для опису спектральних особливостей аудіосигналу, зокрема для аналізу мовлення та виконання завдань розпізнавання голосу.[13] Цей набір коефіцієнтів представляє собою акустичні характеристики аудіосигналу і використовується для створення акустичних моделей та розрізнювання різних звуків, фонем або мовних фраз. (рис. 2.3)

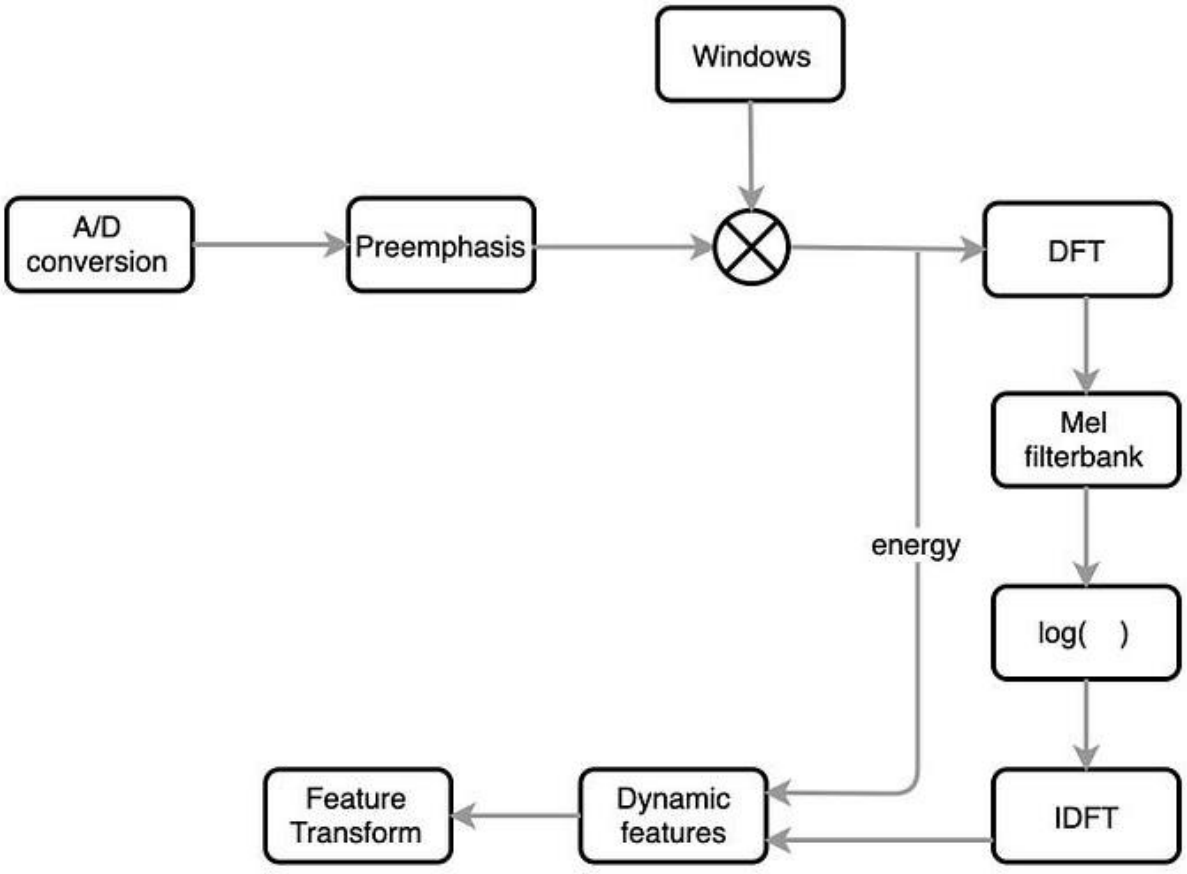

Рис. 2.3 — Схема розрахунку коефіцієнта MFCC

Далі наведено детальний опис кожного етапу отримання коефіцієнта MFCC:

1) A/D перетворення (Аналого-цифрове перетворення). Цей етап включає в себе збір аналогового аудіосигналу (зазвичай записаного мікрофоном) та його перетворення в цифровий формат. Цифровий сигнал представляє собою послідовність дискретних значень амплітуд з часом.

Спочатку аудіосигнал записується у вигляді послідовності амплітудних значень: x[n],

де n – часовий індекс.

2) Переднаголос. Зазвичай, в мовленні існує певна частина перед головною акцентованою частиною слова або фрази, яку називають переднаголосом. Ця частина має важливі акустичні ознаки і може бути визначена на цьому етапі.

Визначається переднаголос, наприклад, N_0, відоме як кількість відлунь.

3) Вікна. Аудіо сигнал поділяється на короткі часові фрейми або кадри, кожен з яких має фіксовану тривалість, наприклад, 20-30 мілісекунд. Кадри можуть перекриватися частково для збереження контексту мовлення.

Сигнал x[n] поділяється на короткі часові кадри, і для кожного кадру використовується віконна функція w[n], наприклад віконна функція Гаммінга:

$$x_w[n] = x[n] * w[n],$$

де x_w[n] – віконний сигнал

4) ДПФ (Дискретне перетворення Фур'є). Для кожного кадру виконується ДПФ, яке перетворює сигнал із часової області в частотну область. Отримуємо спектр сигналу, який показує, які частоти присутні в кожному кадрі.

Обчислюється ДПФ для кожного віконного сигналу $x_w[n]$, отримуючи спектральний сигнал X[k]:

$$X[k] = \sum_{n=0}^{N-1} x_w[n] * e^{-j\frac{2\pi}{N}kn},$$

де N – розмір віконного кадру.

5) Банк фільтрів Mel. Спектр сигналу (X[k]) подається через банк фільтрів Mel. Цей банк фільтрів розбиває спектр на декілька піддіапазонів згідно зі шкалою Мел, яка відображає спосіб, яким люди сприймають звукові частоти. Кожен фільтр важливий для виділення певних частотних складових мовлення.

6) Обчислення енергії: Для кожного піддіапазону обчислюється енергія, яка представляє собою суму квадратів амплітуд спектральних компонент в кожному піддіапазоні.

7) Логарифмування: Логарифмується енергія кожного піддіапазону. Це допомагає стиснути динаміку сигналу і зменшити вплив великих значень.

$$M_i = \log(E_i),$$

де M_i – логарифмований коефіцієнт для і-го піддіапазону, E_i – енергія у і-му діапазоні.

8) Трансформація функцій: Логарифмовані енергії стають коефіцієнтами Мел-частотного кепстрового перетворення (MFCC).

$$C_i = \sum_{i-1}^{N} M_i * \cos(\frac{(2i-1)\pi}{2N}),$$

де C_i – і-й коефіцієнт MFCC, M_i – логарифмована енергія у і-му піддіапазоні, N – кількість піддіапазонів.

9) Динамічні особливості. До отриманих MFCC можуть додаватися динамічні особливості, такі як ΔMFCC (перша похідна MFCC) та ΔΔMFCC

(друга похідна MFCC), для врахування змін в часі та отримання більш докладної інформації про рух звуку.

10) IDFT (зворотне дискретне перетворення Фур'є). Остаточний крок включає в себе обернене ДПФ, яке перетворює кепстральні коефіцієнти MFCC назад в часову область. Отримані результати представляють собою набір акустичних ознак, які можна використовувати для подальшого аналізу мовлення, такого як розпізнавання голосу чи інші завдання обробки аудіосигналів.

Коефіцієнти лінійного передбачення (LPCC) — це характеристики, які використовуються для опису акустичних особливостей мовлення у звуковому сигналі. LPCC використовується в обробці мовлення та розпізнаванні голосу.[6] Ці коефіцієнти отримуються внаслідок аналізу спектра голосу та описують, як звукові хвилі перетворюються в акустичні особливості мовлення, такі як форманти та характеристики голосу (рис. 2.4).

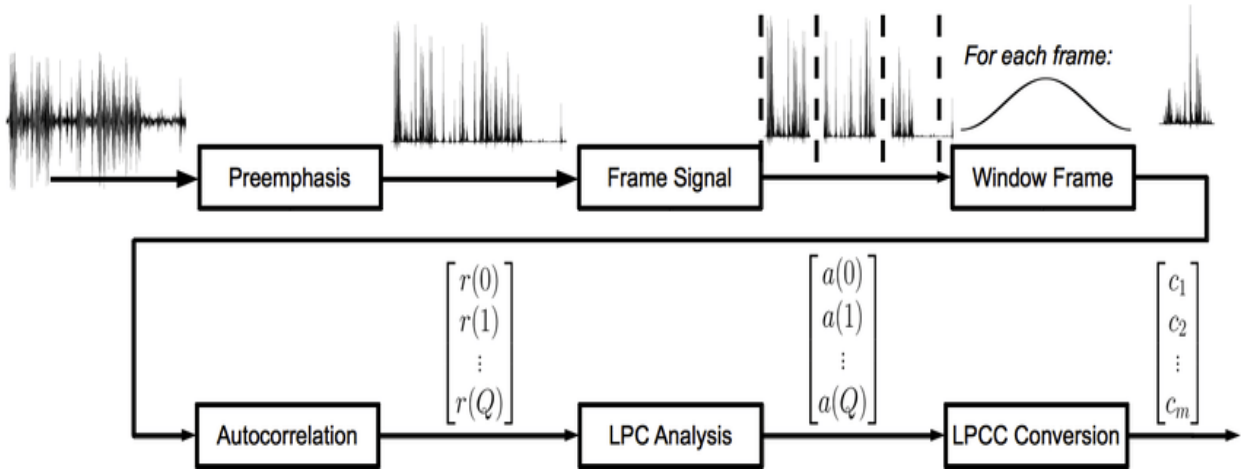

Рис. 2.4 — Схема розрахунку коефіцієнта LPCC

Схема отримання коефіцієнтів лінійного передбачення (LPCC) включає наступні кроки:

1) Переднаголос. Визначається переднаголос аудіосигналу, що може містити важливі акустичні особливості перед головною акцентованою частиною слова або фрази.

2) Кадровий сигнал. Аудіосигнал розбивається на короткі часові кадри, наприклад, кожні 20-30 мілісекунд. Ці кадри обрамляються віконною функцією, такою як функція Гаммінга, для зменшення артефактів на краях кадру та підготовки сигналу для обчислень.

3) Автокореляція: Для кожного кадру обчислюється автокореляція. Автокореляція — це міра схожості сигналу зі собою при різних зсувів часу. Вона дозволяє визначити часові залежності в сигналі.

Формула автокореляції для k-го коефіцієнта виглядає наступним чином:

$$R[k] = \sum_{n=k+1}^{N} s[n] * s[n-k],$$

де s[n] – вхідний аудіосигнал, N – довжина кадру.

4) LPC аналіз (Linear Predictive Coding). На основі автокореляції проводиться LPC аналіз, який полягає в моделюванні аудіосигналу як лінійну комбінацію попередніх відлунь. В результаті аналізу отримується набір параметрів, що описують акустичні характеристики сигналу.

Коефіцієнти a_i LPCC обчислюються шляхом розв'язання системи лінійних рівнянь методои автокореляції. Ця система може бути записана так:

$$R[1] * a_1 + R[2] * a_2 + \ldots + R[p] * a_p - R[0],$$

де p – порядок LPCC аналізу.

5) Перетворення LPCC (Linear Predictive Cepstral Coefficients). Отримані параметри LPC піддаються перетворенню у кепстральний простір, аналогічно Мел-частотному кепстровому перетворенню (MFCC). Цей крок включає в себе обчислення коефіцієнтів LPCC, які можуть бути використані для подальшого аналізу мовлення, включаючи розпізнавання голосу та інші обчислювальні завдання.

Після отримання коефіцієнтів a_i, їх можна перетворити у кепстральні коефіцієнти c_i за допомогою формули, аналогічно до Мел-частотного кепстрового перетворення:

$$c_i = a_i + \sum_{m=1}^{p} \frac{m}{p} * a_m * a_{i-m},$$

де p – рядок LPCC аналізу, a_i – коефіцієнти, c_i – кепстральні коефіцієнти.

2.4 Впровадження голосової біометрії в інформаційну безпеку та системи автентифікації користувачів

Біометричне розпізнавання голосу має широкий спектр використання, розглянемо основні сфери її застосування:

- Контакт-центр. Це найпоширеніший приклад застосування голосової біометрії. При взаємодії з клієнтською службою використання голосу для автентифікації дозволяє економити час і зусилля як для споживача, так і надавача послуг.
- Виявлення шахрайства. Голосова біометрія є потужним інструментом виявлення шахрайства, адже пропонує безпечний механізм автентифікації, стійкий до підробки. Таким чином, цей інструмент використовується для запобігання несанкціонованому доступу до даних клієнта або його фінансів.
- Фінансові послуги. За останні роки світовий ринок фінансових послуг пережив значні зміни. Життя клієнтів стало легшим завдяки мобільному банкінгу та іншим фінансовим технологіям. Фінансові установи використовують голосову біометрію для зручнішої, швидшої та безпечнішої взаємодії з клієнтами.
- Цифрові підписи. Голосові біометричні дані можна використовувати для встановлення голосових підписів, які використовуються для підписання документів, таких як договори страхування життя. Фінансові операції також можна авторизувати за допомогою голосових підписів.
- Управління персоналом. Використання голосової біометрії в застосунках для управління персоналом вже є звичним явищем. Ця технологія є безпечною альтернативою системам бейджингу для організацій з великим штатом.[22]

Голосова аутентифікація стає все більш поширеною інноваційною технологією, яка дозволяє користувачам підтверджувати свою ідентичність за допомогою унікальних характеристик їх голосу. Ця технологія просувається

завдяки розвитку штучного інтелекту і машинного навчання, і вона знайшла застосування в різних галузях, включаючи фінансовий сектор. Завдяки голосовій аутентифікації можна покращити безпеку та зручність фінансових транзакцій, зменшити ризик шахрайства та забезпечити доступ лише для авторизованих осіб.[3]

У сучасному світі технології стрімко розвиваються, і голосова біометрична ідентифікація стає все більш затребуваною в галузі захисту цифрової ідентичності. Її інтеграція в повсякденні пристрої перетворила голосову аутентифікацію з наукової фантастики в реальність для тисяч людей по всьому світу. Глобальний ринок голосового визнавання прогнозується на зростання, вказуючи на великий попит на цю технологію.

Далі розглянемо найвідоміші приклади застосування біометричної аутентифікації за голосом:

- Amazon. Віртуальний помічник Amazon, Alexa, використовує розпізнавання голосу для автентифікації користувача та персоналізованого досвіду. Пристрої Amazon Echo (рис. 2.5) дозволяють користувачам виконувати завдання та отримувати доступ до інформації за допомогою голосових команд.

Рис. 2.5 — Пристрої Amazon Echo

- Apple. Голосовий помічник Siri від Apple (рис. 2.6) використовує розпізнавання голосу для взаємодії з користувачем, і компанія запровадила голосову автентифікацію для розблокування пристроїв і авторизації транзакцій за допомогою функції «Hey Siri».[9]

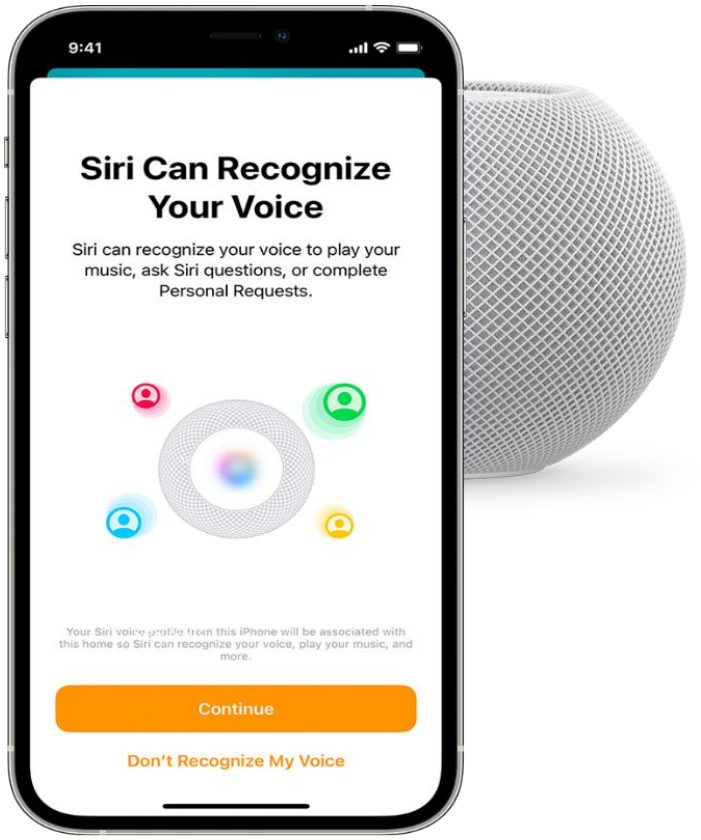

Рис. 2.6 — Голосовий помічник Siri від Apple

- Google. Технологія Google Voice Match (рис.2.7) забезпечує голосову автентифікацію для доступу до пристроїв і персоналізованих служб. Google Assistant також використовує розпізнавання голосу для взаємодії з користувачем за допомогою фрази «Hey, Google».

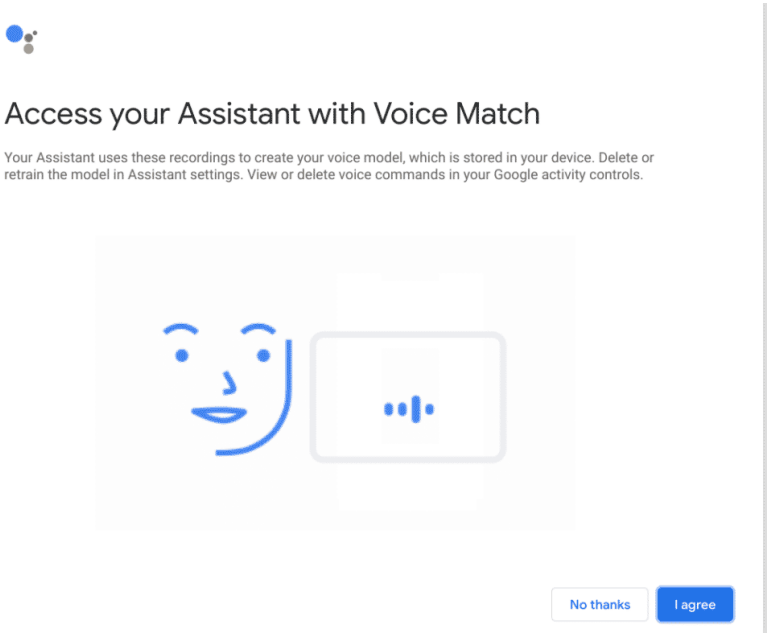

Рис. 2.7 — Технологія Google Voice Match

- Microsoft. Віртуальний помічник Cortana від Microsoft (рис. 2.8) використовує розпізнавання голосу для взаємодії з користувачем та автентифікації. Крім того, Microsoft Azure пропонує інструменти голосової автентифікації для компаній.

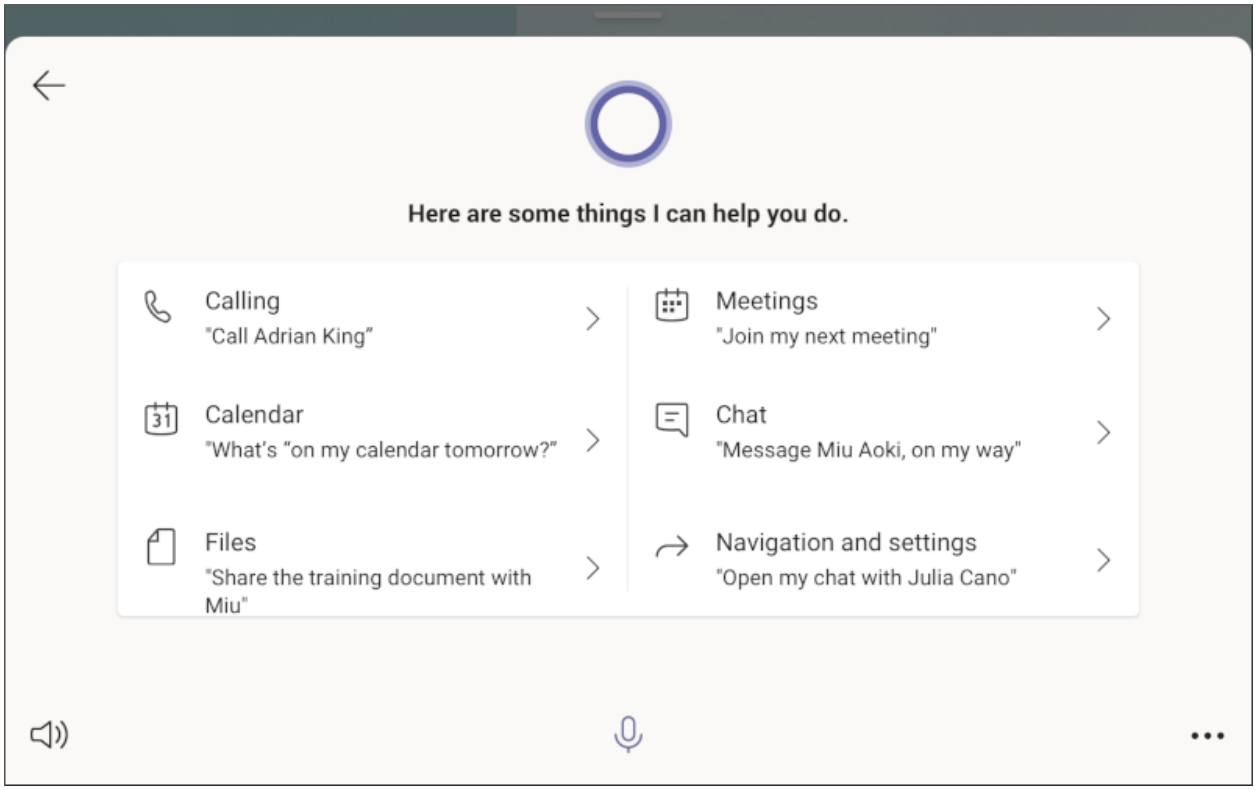

Рисунок 2.8 — Віртуальний помічник Cortana від Microsoft

- Samsung: пристрої Samsung, включаючи смартфони, смарт-телевізори та інноваційні продукти для дому, використовують розпізнавання голосу для автентифікації користувачів і керування пристроями.
- Wells Fargo. Велика фінансова установа Wells Fargo запровадила голосову автентифікацію для мобільного банкінгу. Клієнти можуть безпечно отримувати доступ до своїх рахунків і виконувати транзакції за допомогою голосових відбитків.
- Barclays. Barclays, міжнародний банк, запровадив розпізнавання голосу для автентифікації клієнтів у своєму мобільному банківському додатку. Клієнти можуть використовувати свій голос для входу в облікові записи. Приголомшливі 93% клієнтів Barclays повідомили про підвищення задоволеності системою розпізнавання голосу, оскільки вона значно скоротила час транзакції.[3]

Важливо також відмітити яким чином голосова ідентифікація впроваджується в компанії і установи нашої країни. Голосова біометрія в ПриватБанку є інноваційною технологією, яка була впроваджена найбільшим банком України на початку 2022 року і отримала широке визнання серед клієнтів(рис. 2.9.). Ця технологія дозволяє клієнтам банку авторизувати себе за допомогою голосу під час звернення до клієнтської підтримки.

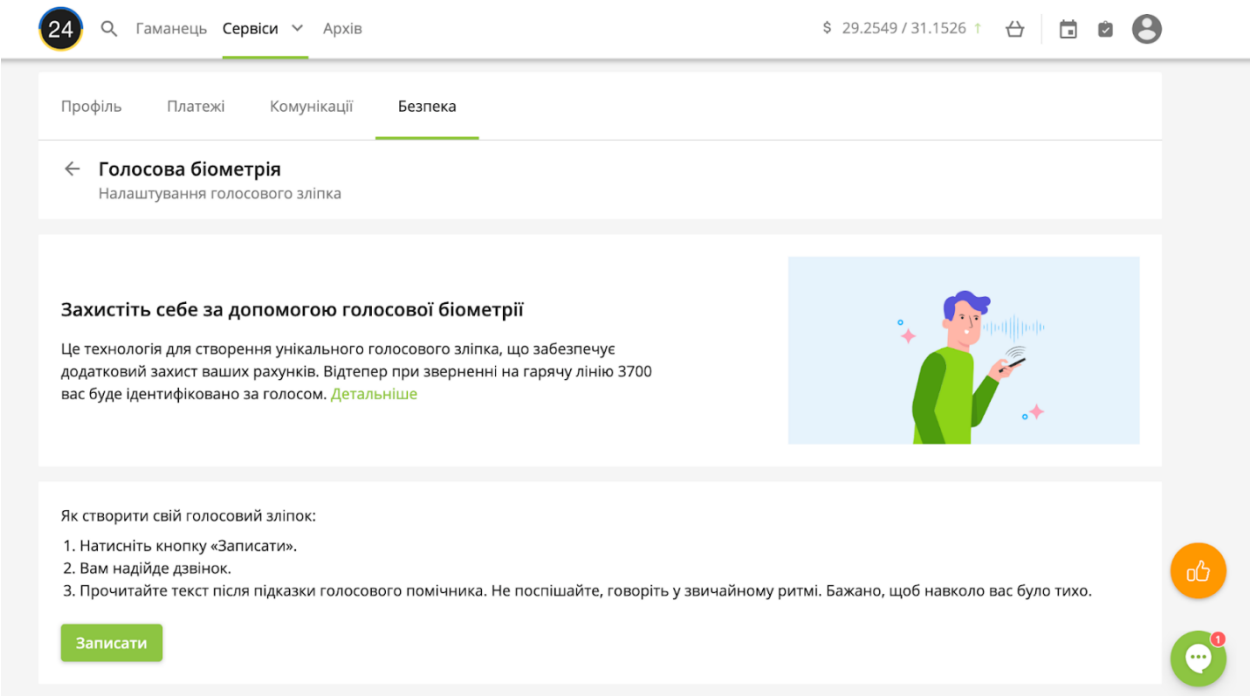

Рис. 2.9 — Голосова біометрія в ПриватБанку

Процес роботи голосової біометрії в ПриватБанку дуже простий. Клієнт просто здійснює дзвінок до клієнтської підтримки і розпочинає розмову з віртуальним асистентом або оператором. Протягом кількох секунд система розпізнає клієнта за його голосом, навіть під час того, як він пояснює причину свого дзвінка. Це спрощує процедуру і значно прискорює обслуговування, оскільки оператору не потрібно задавати додаткових питань для ідентифікації клієнта.

Головні переваги голосової біометрії для клієнтів ПриватБанку включають в себе зручність (необов'язковість запам'ятовування особистих даних), швидкість (скорочення часу розмови з оператором) і високий рівень безпеки (неможливість здійснення операції імітуючи голос клієнта, оскільки банк зберігає відбиток голосу та порівнює дані під час кожного дзвінка на клієнтську підтримку). Така технологія стала істотним покращенням обслуговування клієнтів та забезпечує їхню ідентифікацію. [21]

3 ТЕСТУВАННЯ СИСТЕМИ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ ПО ГОЛОСУ VOICESENS

3.1 Основні характеристики та компоненти "VoiceSens"

Тестування систем біометричної аутентифікації в сучасному цифровому світі має надзвичайну важливість, оскільки ці системи використовуються для захисту особистої інформації та доступу до найбільш цінних ресурсів. Впевненість у безпекових і функціональних аспектах таких систем вимагає докладного тестування, яке може виявити потенційні проблеми та недоліки. У даному контексті, в ході дипломної роботи, було проведено тестування системи "VoiceSens".

"VoiceSens" — це текстово-незалежне рішення для голосової біометрії, призначене для подолання обмежень традиційних методів аутентифікації, таких як паролі та PIN-коди, а також існуючих рішень для голосової біометрії. Воно розроблено за допомогою мови програмування Python та використовує сервіс Watson Speech to Text для розпізнавання мови.[28]

Далі детально розглянемо основні компоненти даного програмного забезпечення:

- IBM Watson Speech to Text. Цей компонент відповідає за розпізнавання мови з аудіо-запису. Він використовує сервіс IBM Watson, який здатний конвертувати голосовий сигнал у текстовий формат. Це є важливим кроком для збору вхідних даних з голосових зразків користувачів та подальшої обробки цих даних.[2]

IBM Watson Speech to Text є технологією швидкого та точного перетворення мовлення на текст у різних мовах для різноманітних сценаріїв застосування. Ця технологія використовується для вдосконалення обслуговування клієнтів, надання допомоги операторам і аналізу мовлення.

IBM Watson Speech to Text має високошвидкісні моделі машинного навчання, що можуть бути адаптовані до конкретних вимог розроблюваних програм.

Ця технологія доступна для використання на будь-якому хмарному сервісі, включаючи публічний, приватний, гібридний, багатохмарковий або власний хмарний сервіс. Основні функції Watson Speech to Text включають автоматичне розпізнавання мовлення, навчання моделей, підтримку галузі обслуговування клієнтів та багато іншого. Відфільтровування слов, виявлення мовців у багатомовному спілкуванні та інші функції роблять цю технологію досить різноманітною та високофункціональною для великої кількості сценаріїв використання, включаючи обслуговування клієнтів, аналітику тощо.[2]

- SciPy — це бібліотека для мови програмування Python, яка спеціалізується на наукових обчисленнях та інженерних застосунках. Вона містить багато корисних функцій для обробки даних, математичних обчислень та оптимізації, що можуть бути корисні в голосовій біометрії для аналізу та обробки голосових характеристик. [8]

Бібліотека SciPy є потужним інструментом для наукових обчислень та аналізу даних, що надає широкий спектр алгоритмів для розв'язання різних математичних та обчислювальних задач. Серед них оптимізація, інтегрування, інтерполяція, розв'язання власних значень, алгебраїчні рівняння, диференціальні рівняння, статистика та багато інших класів проблем.

SciPy розширює можливості бібліотеки NumPy, надаючи додаткові інструменти для обробки масивів та спеціалізовані структури даних, такі як розріджені матриці та дерева з k-вимірними даними. Вона використовує високооптимізовані реалізації на мовах низького рівня, таких як Fortran, C та C++, що надає високу швидкість обчислень.

- Speech Recognition. Ця бібліотека розроблена для розпізнавання мови в аудіо-записах. Вона надає можливість використовувати різні двигуни та API для виконання розпізнавання, як в онлайн, так і офлайн режимах. Це

дозволяє VoiceSens працювати з різними типами аудіо-джерел та вибирати найкращий двигун для конкретного завдання.[11]

Бібліотека SpeechRecognition представляє собою інтерфейс Web Speech API, який контролює розпізнавання мовлення та обробку голосу. Вона служить контролером для служби розпізнавання мовлення та обробки голосу та обробляє події SpeechRecognitionEvent, які надсилаються службою розпізнавання.

SpeechRecognition дозволяє створювати об'єкти для розпізнавання мови та управляти різними параметрами розпізнавання, такими як мова, граматика, кількість альтернативних результатів та багато інших. Вона також дозволяє реалізувати різні події, пов'язані з процесом розпізнавання, такі як початок та завершення запису аудіо, помилки розпізнавання, результати розпізнавання та інші.

Ця бібліотека використовується для роботи з розпізнаванням мовлення в браузері та може надсилати аудіодані на веб-сервіс для обробки розпізнавання, тому вона не працює в офлайн-режимі. SpeechRecognition дозволяє створювати веб-додатки, які взаємодіють з користувачами за допомогою їх голосу та можуть розпізнавати команди та інструкції, вимовлені голосом, перетворюючи їх на текстовий формат для подальшого використання.[11]

- Python Speech Features. Дана бібліотека надає різні загальні функції для обробки голосу. Однією з найважливіших функцій є обчислення коефіцієнтів Мел-частоти цепстральних (MFCC), які є важливими для аналізу аудіосигналу та визначення його характеристик.

Бібліотека python_speech_features надає засоби для роботи з характеристиками мови, такими як коефіцієнти MFCC та енергія фільтрбанку, що використовуються в автоматичному розпізнаванні мови (ASR). За допомогою цієї бібліотеки можна обчислювати різні акустичні ознаки з аудіосигналу, що допомагає у вирішенні завдань ASR та обробки мовлення.

До підтримуваних функцій входять обчислення MFCC, енергії фільтрбанку, логарифму фільтрбанку та центроїдів спектральних піддіапазонів. Бібліотека також надає інші функції для перетворення між частотами Герца та Mels, а також для роботи з фреймами аудіосигналу.

Для використання бібліотеки, вам потрібно мати встановлені бібліотеки numpy та scipy. Ця бібліотека дозволяє обчислювати різні характеристики аудіосигналу, такі як коефіцієнти MFCC, енергія фільтрбанку тощо, з аудіо сигналу та використовувати їх для подальшого аналізу або класифікації мовлення. Бібліотека може бути корисною для вирішення завдань обробки мовлення, включаючи автоматичне розпізнавання мови та аналіз акустичних характеристик аудіосигналу.[15]

- Fuzzy Wuzzy. Ця бібліотека використовується для нечіткого порівняння рядків. Вона базується на відстані Левенштейна, яка вимірює відмінності між послідовностями символів. У контексті голосової біометрії, це може використовуватися для порівняння голосових слідів та визначення їхньої схожості.[1]
- Random Words. Цей пакет дозволяє генерувати випадкові англійські слова. Його можна використовувати для створення текстових рядків, які користувач повинен вимовити під час реєстрації голосового зразка.[7]
- Scikit-learn Gaussian Mixture Models. Бібліотека забезпечує можливість навчати моделі змішаного розподілу Гаусса (GMM). У голосовій біометрії GMM може використовуватися для моделювання і порівняння голосових слідів користувачів для подальшої автентифікації.

Бібліотека sklearn.mixture.GaussianMixture надає засоби для роботи з моделями суміші гауссівських розподілів. Ця бібліотека дозволяє оцінювати параметри суміші гауссівських розподілів з вхідних даних. Головною метою використання цієї бібліотеки є моделювання складних розподілів даних, де кожен розподіл визначається як сума кількох гауссівських компонент.

Основні параметри класу GaussianMixture включають кількість компонент суміші гауссівських розподілів, тип коваріації для кожної компоненти (загальна, об'єднана, діагональна або сферична), поріг збіжності для алгоритму очікування-максимізації (EM), кількість ітерацій EM та інші.

Клас GaussianMixture надає методи для оцінки параметрів моделі за допомогою алгоритму EM, передбачення міток для вхідних даних, обчислення логарифмічної ймовірності для даних та багато інших корисних функцій. Ця бібліотека широко використовується для кластеризації та аналізу даних, коли припускається, що дані мають складну структуру, яку можна розкласти на гауссівські компоненти.[10]

3.2 Функції та алгоритми реєстрації та аутентифікацієї користувачів за допомогою біометричної автентифікації по голосу

Програма "VoiceSens" складається з низки компонентів та файлів, які забезпечують її функціональність. Основні складові програми включають наступні файли:

1) JavaScript файли:

- auth.js: Реалізація автентифікації.
- enroll.js: Реалізація реєстрації користувачів.
- main.js: Основний файл програми.
- voice.js: Опрацювання голосових даних.

2) Бібліотеки:

- p5.dom.min.js: Бібліотека для роботи з DOM-елементами.
- p5.min.js: Основна бібліотека p5.js.
- p5.sound.min.js: Бібліотека для роботи з звуком.
- wavesurfer.microphone.min.js: Бібліотека для роботи з аудіоданими.

3) Інші компоненти:

- stylesheets: Стилі для веб-інтерфейсу.
- templates: HTML-шаблони сторінок.

Важливо детально розглянути функцію, що знаходиться в файлі voice.js (Додаток А). Цей код виконує ряд дій, пов'язаних з аутентифікацією користувача за допомогою біометричної аутентифікації по голосу та запису звукових даних для подальшого аналізу. Нижче наведено основні частини коду та їх функціональність:

1) Ініціалізація WaveSurfer та мікрофону.

Створюється об'єкт wavesurfer, який використовується для візуалізації аудіоданих на сторінці. Ініціалізується мікрофон для запису аудіо за допомогою WaveSurfer:

```
var wavesurfer = WaveSurfer.create({
  container: '#waveform',
  waveColor: '#01BAB6',
  interact: false,
  cursorWidth: 0,
  barGap: 2,
  barHeight: 2,
  barWidth: 0,
  fillParent: true,
  forceDecode: true,
  plugins: [
    WaveSurfer.microphone.create()
  ]
});
```

2) Робота з мікрофоном:

Після ініціалізації мікрофону та WaveSurfer, визначаються обробники подій для готовності мікрофону (wavesurfer.microphone.on('deviceReady')) та помилки мікрофону (wavesurfer.microphone.on('deviceError')). Запуск мікрофону відбувається за допомогою wavesurfer.microphone.start():

```
wavesurfer.microphone.on('deviceReady', function (stream) {
  console.log('Device ready!', stream);
});
wavesurfer.microphone.on('deviceError', function (code) {
  console.warn('Device error: ' + code);
});
```

3) Запис звуку. Створюється об'єкт mic, який представляє доступ до мікрофону. Далі створюється об'єкт recorder, який використовується для запису звуку з мікрофону. При кліку на кнопку з id "startRecButton", відбувається запис звуку (recorder.record(soundFile)). При кліку на кнопку з id "stopRecButton", запис звуку припиняється, і звуковий файл відтворюється (recorder.stop() та soundFile.play()). Записаний звуковий файл відправляється на сервер для подальшого аналізу:

```
wavesurfer.microphone.start();
mic = new p5.AudioIn();
mic.start();
recorder = new p5.SoundRecorder();
recorder.setInput(mic);
if (document.referrer == "http://localhost:8080/enroll") {
  var number_of_attempts = 3;
  console.log("number of attempts : ", number_of_attempts);
}
else {
  var number_of_attempts = 1;
  console.log("number of attempts : ", number_of_attempts);
}

document.querySelector('#startRecButton').addEventListener('click',
function () {

  if (document.querySelector('#passphraseMessage').style.display == 'none') {
    showElement('#environmentMessage');

    console.log("You have started recording passphrase...");
```

```
  recorder.record(soundFile);
 } else {
  document.querySelector('#passphraseMessage').classList.add('green');;

  console.log("You have started recording the background...");
  recorder.record(soundFile);
 }
```

4) Відправлення записаного голосу на сервер для аналізу:

Записаний голосовий файл конвертується у формат "Blob" і відправляється на сервер для аналізу:

```
console.log("Saving the SoundFile to a blob file ...");
  var soundBlob = soundFile.getBlob();
  var xhr = new XMLHttpRequest();
```

Результат аналізу (який може бути "fail", "pass" або інший) обробляється у функції stopRecording(). Результати відображаються на сторінці, і зменшується кількість залишишихся спроб:

3.3. Тестування та опис роботи програми VoiceSens

Програма "VoiceSens" розроблена на мові програмування Python і використовує службу Watson Speech to Text для розпізнавання мови.

Далі детально розглянемо інтерфейс та функціонал програми для користувачів:

Перше, що ви бачите при відкритті веб-сторінки на головній сторінці - це дві опції: зареєструвати нового користувача та аутентифікувати існуючого користувача.(рис. 3.1)

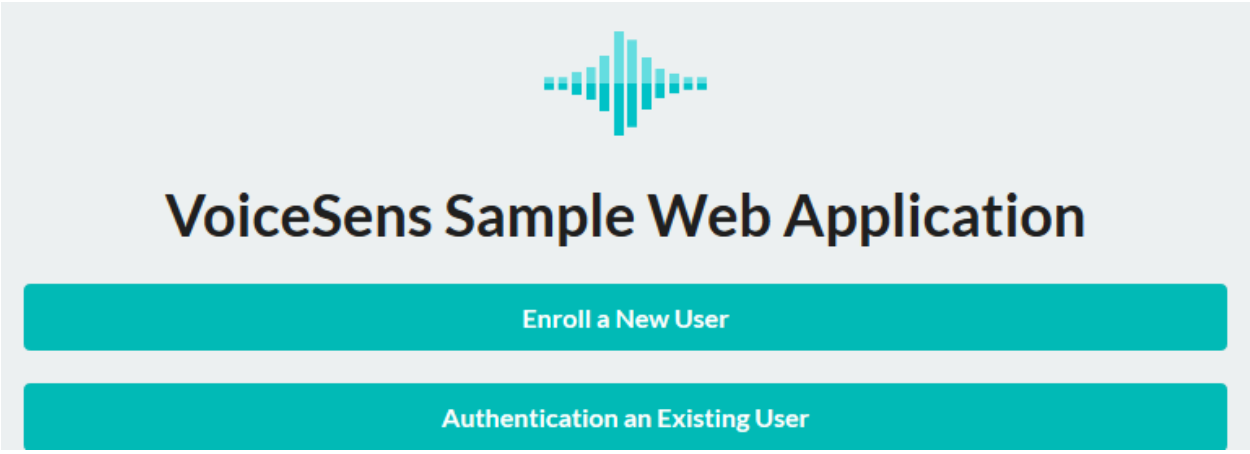

Рис. 3.1 — Головний екран програми "VoiceSens"

Аутентифікація існуючого облікового запису зображена на рис. 3.2.

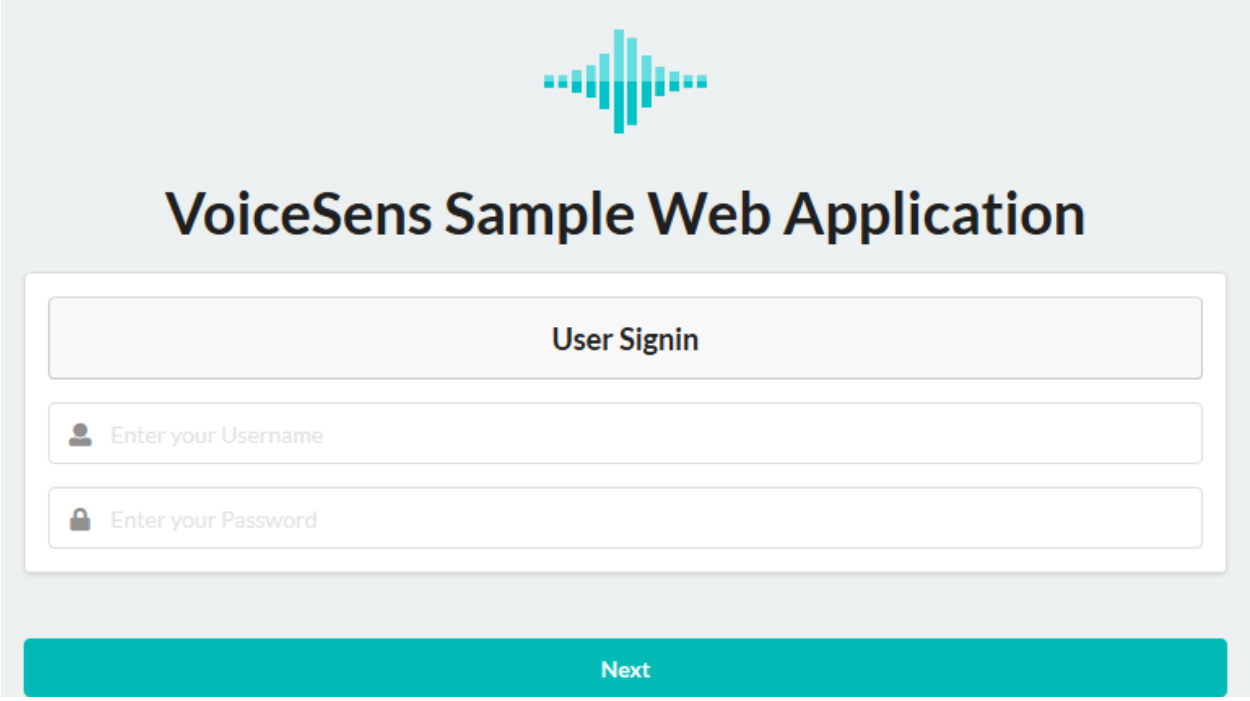

Рис. 3.2 — Аутентифікація існуючого облікового запису в програмі

Якщо у вас ще немає голосового зразка (облікового запису), його варто створити обліковий запис та зареєструвати свої голосові зразки. (рис. 3.3) Модель генерує голосовий відбиток на основі наданих голосових зразків.

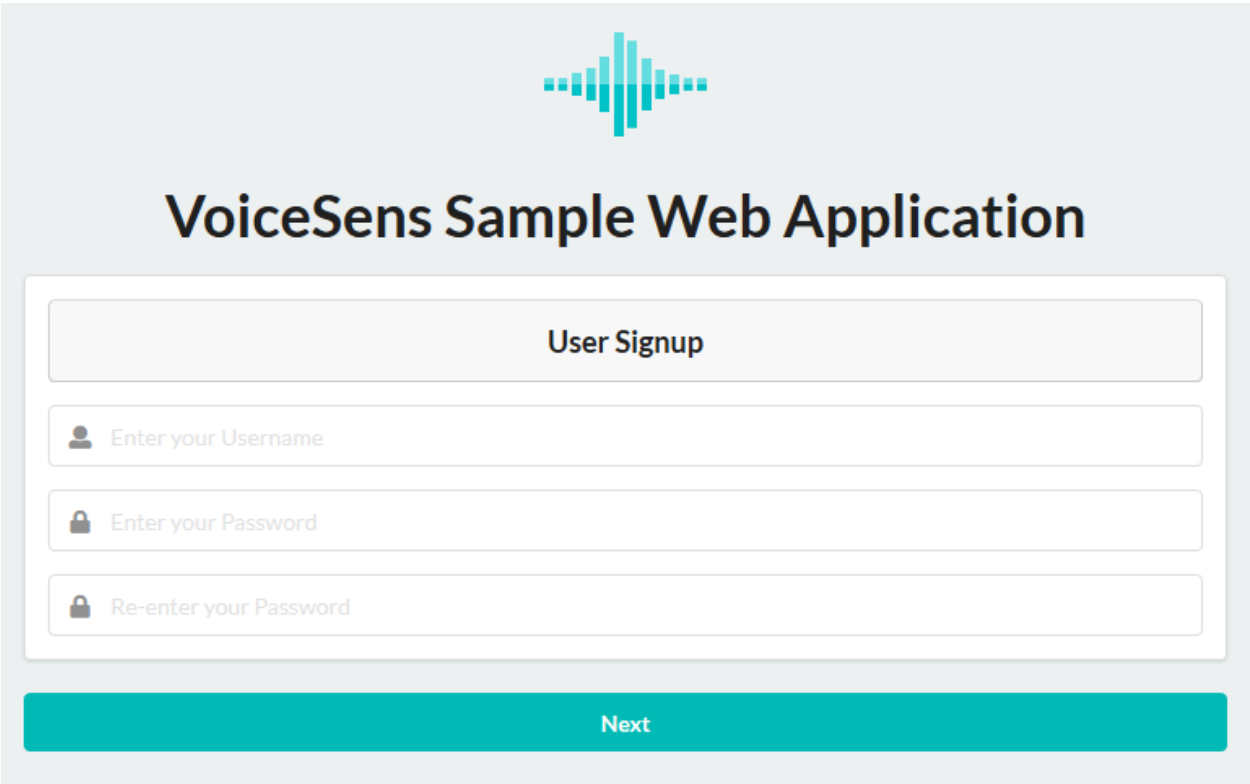

Рис. 3.3 — Процес створення голосового зразка

Після створення облікового запису ви можете аутентифікувати себе, записуючи голосовий зразок, генеруючи голосовий відбиток і порівнюючи його з голосовими відбитками в базі даних.

Під час запису голосового зразка спочатку вас просять записати оточуючий звук для встановлення базового рівня шуму. Потім ви можете перейти до вимовляння випадково генерованих слів.(рис. 3.4)

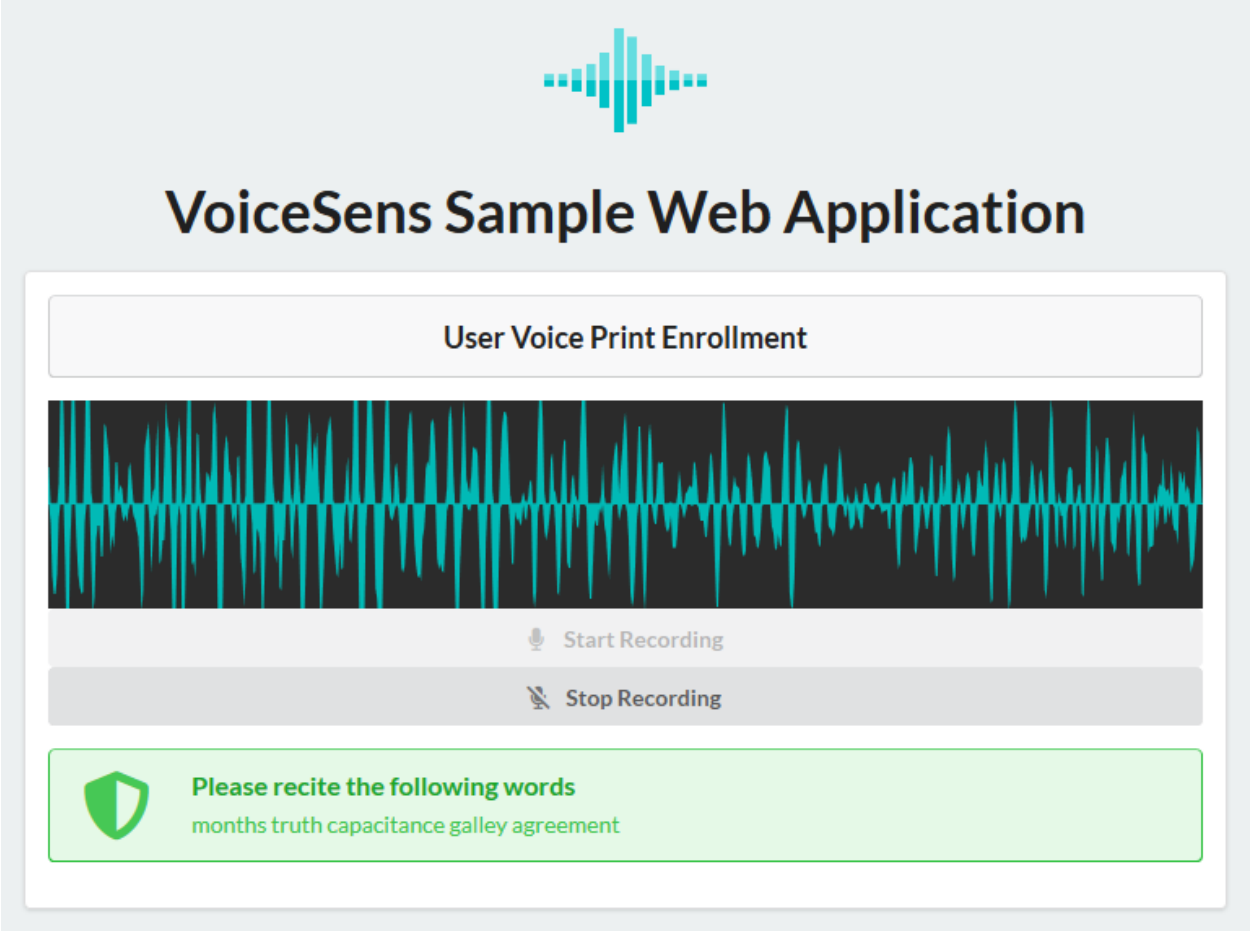

Рис. 3.4 — Процес запису голосового зразка

Далі відбувається процес аналізування введеного голосового зразка. (рис. 3.5)

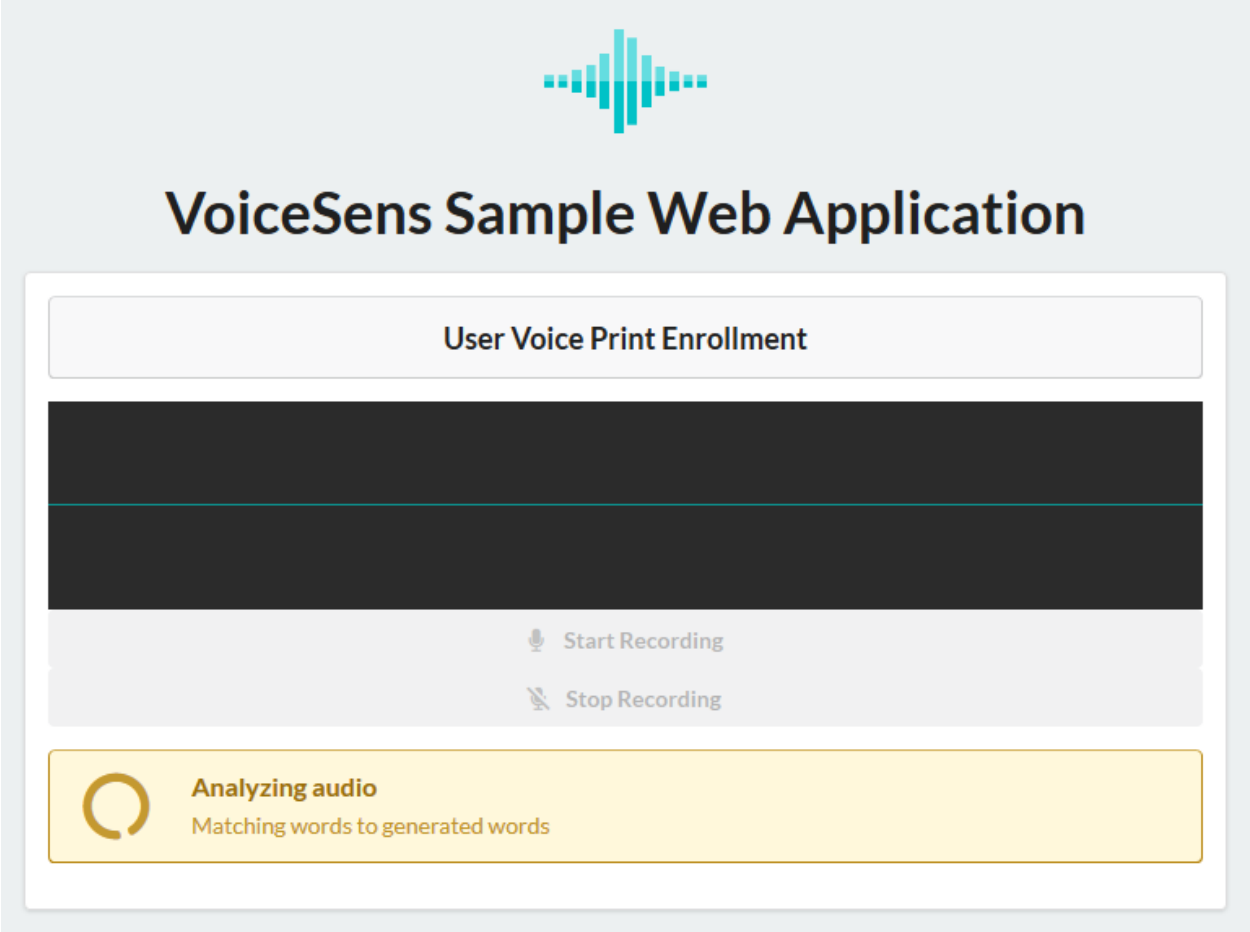

Рис. 3.5 — Аналізування введеного голосового зразка програмою "VoiceSens"

Якщо розміркований відсоток відповідності між згенерованими словами та визнаними словами менший за 65, то записаний голосовий фразу не буде прийнято, і вас попросять записати голосовий зразок знову.

Скріншот негативної ідентифікації голосового зразка зображено на рис. 3.6.

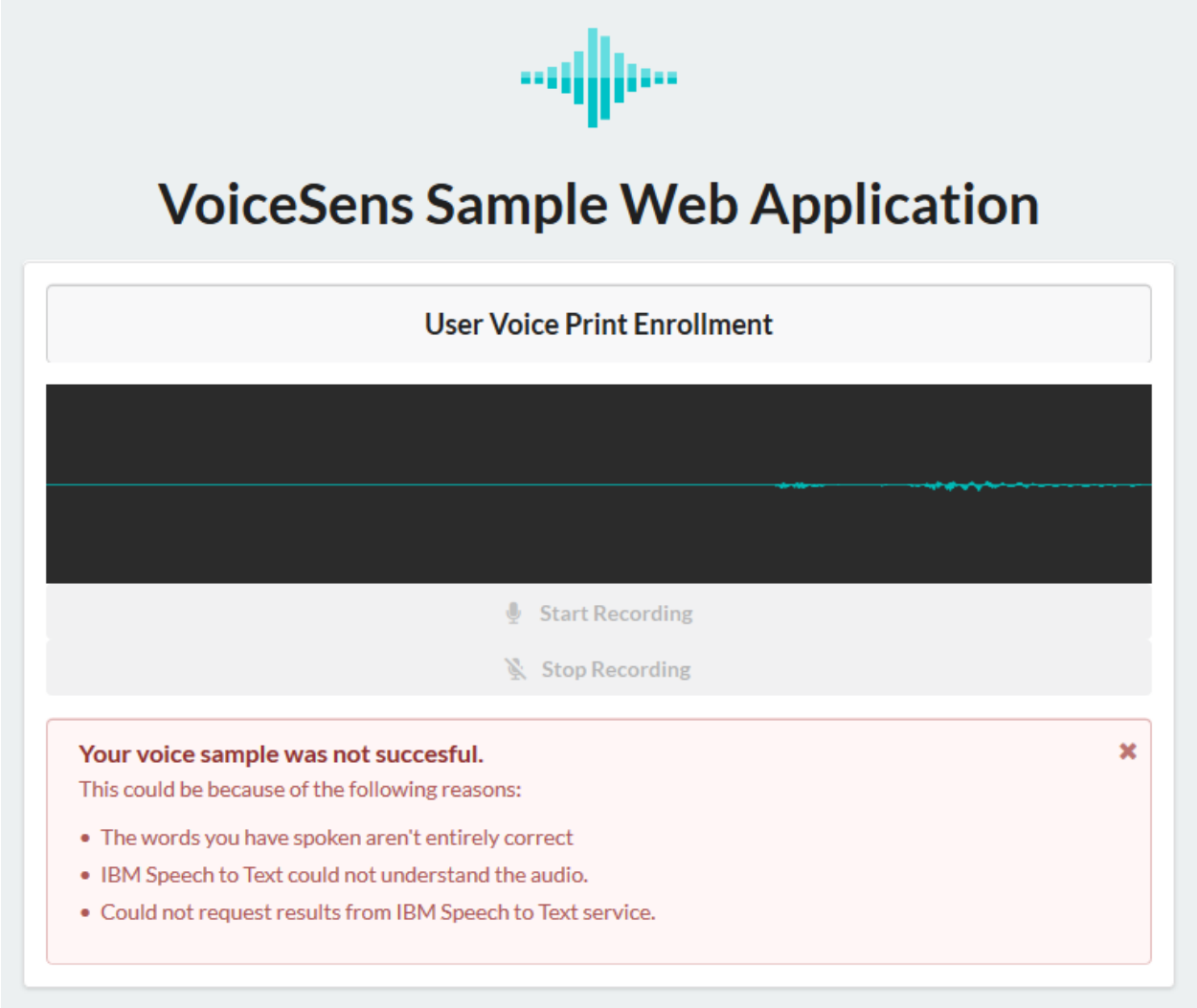

Рис. 3.6 — Відповідь програми що голосовий зразок не ідентифіковано

Приклад успішного розпізнавання голосового зразка зображено на рис. 3.7.

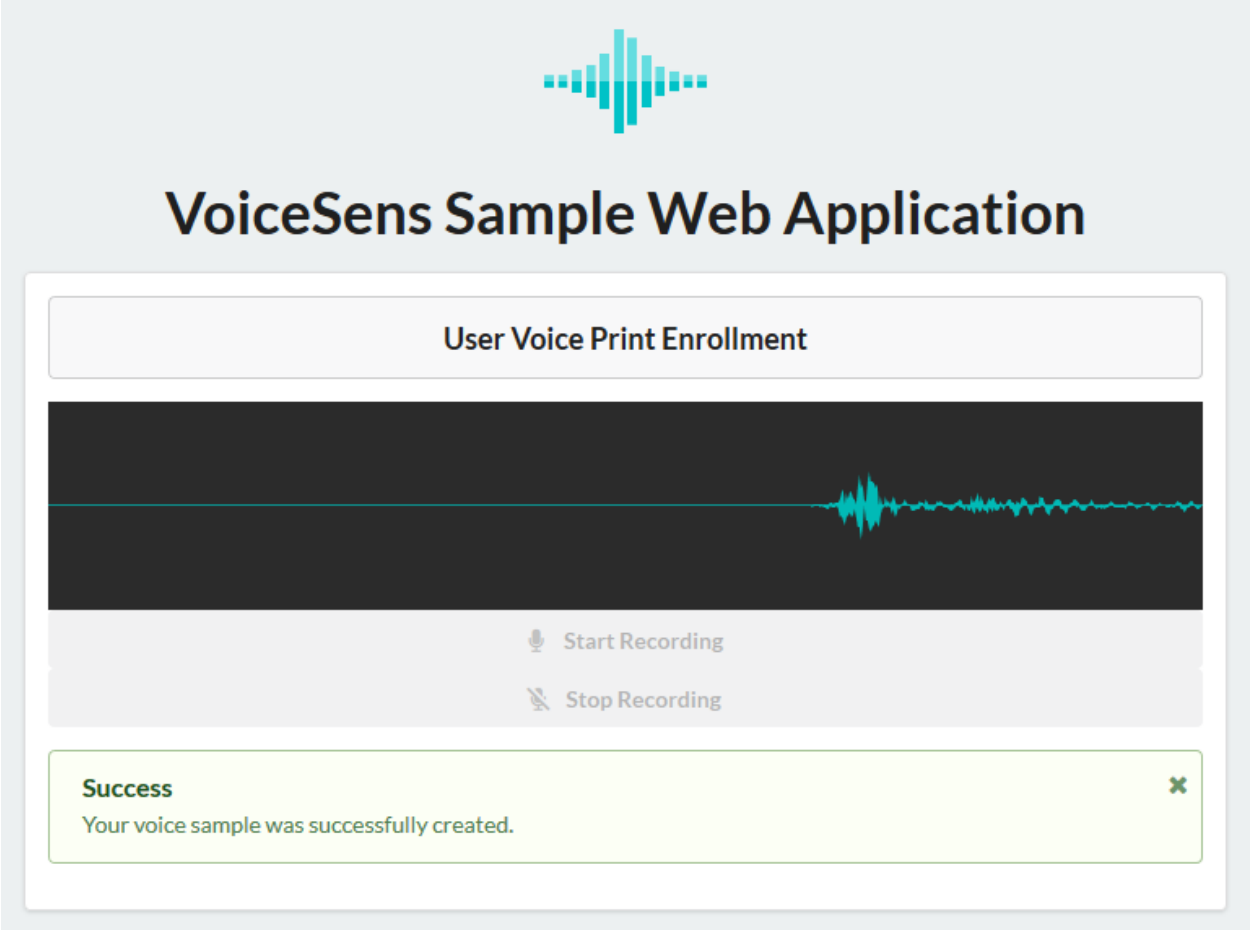

Рис. 3.7 — Відповідь програми, що голосовий зразок успішно аутентифіковано

В ході дипломної роботи було проведено тестування цієї програми для оцінки її функціональності, точності та надійності.

Першочергово було проведено комплексне функціональне тестування системи біометричної аутентифікації "VoiceSens". Воно включає коректність реєстрації користувачів, аутентифікацію, точність розпізнавання голосу, продуктивність та безпеку збереження даних користувачів. Такий підхід дає повну картину про роботу системи і гарантує її надійність і ефективність. Всі дані цього тестування наведено в таб. 4.1.

Таблиця 4.1 — Результати комплексного функціонального тестування системи біометричної аутентифікації "VoiceSens"

Тип тестування	Опис дій	Робота програми
Реєстрація нового користувача	Створення облікового запису та надання голосових зразків для реєстрації.	Успішно зберігає голосові дані користувачів.
Аутентифікація існуючого користувача	Запис голосового зразка та спроба аутентифікації.	Успішно визнає голос користувача.
Точність	Спроба аутентифікації голосу іншої особи.	Правильна відмова в доступі.
Операції на голосовому вводі	Запис голосових зразків з різними рівнями шуму та акцентами.	Добре справляється з різними умовами.
Тестування продуктивності	Вимірювання часу реєстрації та аутентифікації.	Швидко та ефективно працює.
Використання різних голосових виразів	Запис голосових зразків з різними фразами та словами.	Надійно розпізнає різні голосові вирази.
Використання на різних платформах та пристроях	Тестування на різних веб-браузерах та пристроях.	Працює коректно на різних платформах.
Спроби взлому	Спроби використовувати інший голос для аутентифікації.	Надійний біометричний захист.

Наведена таблиця, що надає детальний опис кожного типу тестування, описує дії, які були проведені, та вказує на роботу програми в кожному конкретному випадку. Всі тести пройшли успішно, і програма виявилася надійною та ефективною у всіх аспектах голосової біометрії.

Наступним важливим тестуванням є точності на надійності системи. Для цього необхідно визначити показники FAR та FRR програмного забезпечення VoiceSens.

False Acceptance Rate (FAR) — це показник, що визначає частоту помилкового прийняття. FAR вказує на ймовірність того, що система біометричної автентифікації надасть доступ недійсній особі, яка не має права на доступ. Іншими словами, це ймовірність помилкової ідентифікації. Чим нижче значення FAR, тим краще.[32]

False Rejection Rate (FRR) — показник, що визначає частоту помилкового відхилення. FRR вказує на ймовірність того, що система біометричної автентифікації відхилить легітимну особу і не надасть їй доступ. Іншими словами, це ймовірність помилкового відхилення. Чим нижче значення FRR, тим надійніша програма.[32]

У ході тестування програми VoiceSens було проведено оцінку її точності і безпеки за допомогою вимірювання FAR (False Acceptance Rate) і FRR (False Rejection Rate). У цьому тесті було використано 14 спроб, включаючи 7 спроб користувача (легітимних) і 7 спроб зловмисника (атаки).

Результати тестування наведені в таблиці 4.2.

Таблиця 4.2 — Результати тестування системи біометричної аутентифікації даних на надійність та безпечність.

№ спроби	Тип спроби	Результат
1	Користувач	Прийнято
2	Користувач	Прийнято
3	Користувач	Прийнято

Продовження таблиці 4.2 — Результати тестування системи біометричної аутентифікації даних на надійність та безпечність.

4	Користувач	Прийнято
5	Користувач	Прийнято
6	Користувач	Прийнято
7	Користувач	Прийнято
8	Зловмисник	Відхилено
9	Зловмисник	Відхилено
10	Зловмисник	Відхилено
8	Зловмисник	Відхилено
9	Зловмисник	Відхилено
10	Зловмисник	Відхилено
10	Зловмисник	Відхилено

Розглянемо результати тестування спроби входу користувачів (легітимні). Всі 7 легітимних спроб були правильно визнані і прийняті програмою "VoiceSens".

Спроби атаки зловмисників. Усі 7 спроб атаки зловмисників були відхилені і не прийняті програмою "VoiceSens".

Розрахуємо коефіцієнти FAR і FRR:

1) FAR = (Кількість помилково прийнятих атакуючих спроб) / (Загальна кількість атакуючих спроб) = 0 / 7 = 0%

2) FRR = (Кількість помилкових відмов від доступу до легітимного користувача) / (Загальна кількість легітимних спроб) = 1 / 7 ≈ 14.29%

Отримані результати свідчать про високу точність і надійність програми "VoiceSens" в розпізнаванні голосових даних користувачів. FAR дорівнює 0%, що свідчить про відсутність помилкових в прийнятті спроб атак зловмисника. FRR становив приблизно 14.29%, що вказує на одну помилкову відмову від

доступу до легітимного користувача, що може бути виправлено в подальших розробках програми. У цілому, програма "VoiceSens" виявилася ефективною в уникненні ложних прийнять і надійною в захисті від спроб атаки.

ВИСНОВОК

У ході дипломної роботи було проведено вивчення, аналіз і тестування систем біометричної автентифікації на прикладі програми "VoiceSens", яка базується на розпізнаванні голосу. У першому розділі роботи був проведений огляд основних понять біометричної аутентифікації, включаючи визначення та види біометричних параметрів, принципи роботи систем біометричної аутентифікації і сфери їх застосування.

У другому розділі був проведений аналіз технології та методів розпізнавання голосу. Розглянуто основні етапи та компоненти систем біометричної аутентифікації за голосом, методи обробки та порівняння голосових шаблонів і впровадження голосової біометрії в інформаційну безпеку та системи автентифікації користувачів.

В останньому розділі описано процес використання та тестування системи біометричної автентифікації по голосу "VoiceSens". Розглянуті основні характеристики та компоненти цієї програми, функції та алгоритми реєстрації та аутентифікації користувачів за допомогою біометричної автентифікації по голосу, а також надано опис роботи програми "VoiceSens".

У результаті дослідження виявлено, що система "VoiceSens" показала високу точність розпізнавання голосу та може бути успішно використана для біометричної аутентифікації користувачів. Також можливі напрямки розвитку і подальші дослідження в галузі біометричної аутентифікації за голосом.

Висновки даної дипломної роботи підтверджують актуальність біометричної автентифікації за голосом та перспективи її використання в різних галузях, зокрема в інформаційній безпеці та системах автентифікації користувачів. В результаті аналізу технології та методів розпізнавання голосу, а також тестування програми "VoiceSens", було встановлено, що біометрична

аутентифікація за голосом може бути вдосконалена та застосована з високою точністю.

З урахуванням світових тенденцій в галузі біометричної безпеки та широкого застосування біометричних технологій, отримані результати мають велике значення для національної та глобальної інформаційної безпеки. Рекомендації щодо подальших досліджень включають у себе поглиблення аналізу новітніх методів розпізнавання голосу, покращення алгоритмів біометричної аутентифікації, а також розширення сфер застосування цих технологій.

Отже, дана робота має важливу наукову, науково-технічну і соціальну значущість і може служити основою для подальших досліджень і розробок в області біометричної автентифікації за голосом, сприяючи підвищенню рівня інформаційної безпеки та зручності користувачів у процесі аутентифікації.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Fuzzywuzzy. PyPI. URL: https://pypi.org/project/fuzzywuzzy/ (дата звернення: 29.09.2023).
2. IBM Watson Speech to Text. IBM in Deutschland, Österreich und der Schweiz | IBM. URL: https://www.ibm.com/products/speech-to-text (дата звернення: 29.09.2023).
3. Is Voice Authentication Secure Enough to be Your New Password? – Softjourn. URL: https://softjourn.com/insights/security-considerations-in-voice-authentication (дата звернення: 29.09.2023).
4. J.P. Campbell, J.P. Jr. Speaker Recognition: A Tutorial/ J.P. Campbell, Jr. //Proceedings of the IEEE. – 1997. – Vol. 85, № 9. – P. 1437–1462.
5. Mobile Voice Biometrcis, Infrastructure Security Management| Rapidsoft Systems. URL: http://www.rapidsoftsystems.com/mobile-voice-biometrics-platform.html (date of access: 29.09.2023).
6. Pooja Yadav, Vinay Kumar Jain / MFCC AND LPCC ANALYSIS OF SPEECH SIGNAL FOR DIFFERENT LANGUAGES // Faculty of Engineering and Technology, SSTC-SSGI, Bhilai, Chhattisgarh, India, 2017, C. 1052-1057.
7. Random-Word. PyPI. URL: https://pypi.org/project/Random-Word/ (дата звернення: 30.09.2023).
8. SciPy. FUNDAMENTAL ALGORITHMS. URL: https://scipy.org/ (дата звернення: 30.09.2023).
9. Set up voice recognition and Personal Requests. Apple Support. URL: https://support.apple.com/uk-ua/guide/homepod/apd1841a8f81/homepod (дата звернення: 30.09.2023).

10. Sklearn.Mixture.Gaussianmixture. Documentation. URL: https://scikit-learn.org/stable/modules/generated/sklearn.mixture.GaussianMixture.html (дата звернення: 30.09.2023).
11. SpeechRecognition - Web APIs | MDN. URL: https://developer.mozilla.org/en-US/docs/Web/API/SpeechRecognition (дата звернення: 1.10.2023).
12. The application of biometric technologies. Infosec Resources - IT Security Training & Resources by Infosec. URL: https://resources.infosecinstitute.com/topics/general-security/the-application-of-biometric-technologies/ (дата звернення: 1.10.2023).
13. Uday Kiran / MFCC Technique for Speech Recognition // 2023 URL: https://www.analyticsvidhya.com/blog/2021/06/mfcc-technique-for-speech-recognition/#
14. Voice Verification System for Contact Centres. Automated Intelligent Conversations | Convai URL: https://www.convai.com.au/feature/voice-verification (date of access: 1.10.2023).
15. Welcome to python_speech_features's documentation! — python_speech_features 0.1.0 documentation. URL: https://python-speech-features.readthedocs.io/en/latest/ (дата звернення: 5.10.2023).
16. What is Biometric Authentication and How Does It Work? LoginTC. URL: https://www.logintc.com/types-of-authentication/biometric-authentication/ (дата звернення: 5.10.2023).
17. What is Voice Biometrics and why should you use it? Voice Biometrics & Verification URL: https://www.idrnd.ai/voice-biometrics/ (дата звернення: 12.10.2023).
18. Аутентифікація – LivingFo. URL: https://livingfo.com/autentyfikatsiia/ (дата звернення: 12.10.2023).
19. Билинский, И. И., М. И. Юкиш, и А. А. Павлюк. «ДАКТИЛОСКОПИЧЕСКИЕ СКАНЕРЫ». Научные труды

Винницкого национального технического университета, вып. 3, ноябрь 2011 г., https://trudy.vntu.edu.ua/index.php/trudy/article/view/223.

20. Біометричні дані: збір і захист у Європі, США та Україні - Юридична Газета. Юридична газета – онлайн версія. URL: https://yur-gazeta.com/publications/practice/inshe/biometrichni-dani-zbir-i-zahist-u-evropi-ssha-ta-ukrayini.html (дата звернення: 12.10.2023).
21. Голосова біометрія (аутентифікація) | Як увімкнути, Як працює | ПриватБанк. URL: https://privatbank.ua/voice-biometrics (дата звернення: 12.10.2023).
22. Голосова біометрія: що це, як працює та навіщо вона банкам? - Fintech Insider. URL: https://fintechinsider.com.ua/golosova-biometriya-shho-cze-yak-praczyuye-ta-navishho-vona-bankam/ (дата звернення: 13.10.2023).
23. Горбійчук М. І., Соловій Р. Р. / Комп‘ютерна система контролю доступу з використанням авторизації за голосом // Івано-Франківський національний технічний університет нафти і газу, вул. Карпатська, 15, м. Івано-Франківськ, 2017, С. 98-105.
24. Коваль Д.І. Методи голосової ідентифікації в комп'ютерних системах. Харківський національний університет радіоелектроніки. Харків, 2021.
25. Кузик В.М., та ін. Біометрична система аутентифікації з використанням голосових даних. Збірник матеріалів науково-практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та компютерно-інтегровані технології»(КБКІТ-2020), Тернопіль, 2020.
26. Луцків А.М. доц., к.т.н., Пасіка Д.Р. АНАЛІЗ АЛГОРИТМІВ ТА МЕТОДІВ СИСТЕМ АУТЕНТИФІКАЦІЇ ОСОБИ ЗА ГОЛОСОМ. Тернопільський національний технічний університет імені Івана Пулюя. Матеріали Міжнародної науково-технічної конференції

«Фундаментальні та прикладні проблеми сучасних технологій», Тернопіль, 2018

27. Переваги біометричної автентифікації для безпеки та конфіденційності. TS2 SPACE. URL: https://ts2.space/uk/%D0%BF%D0%B5%D1%80%D0%B5%D0%B2%D0%B0%D0%B3%D0%B8-%D0%B1%D1%96%D0%BE%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%BD%D0%BE%D1%97-%D0%B0%D0%B2%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%86%D1%96/ (дата звернення: 29.09.2023).
28. Програмне забезпечення VoiceSens. Github.Com. URL: https://github.com/bedangSen/VoiceSens (date of access: 15.10.2023).
29. Продан Т.І., Івасьєв С.В., Сучасні методи біометричної ідентифікації. Збірник матеріалів проблемно-наукової міжгалузевої конференції «Автоматизація та комп'ютерно – інтегровані технології» (АКІТ - 2022), Тернопіль, 2022.
30. Показники FAR та FRR. Recogtech.com. URL: https://www.recogtech.com/en/knowledge-base/security-level-versus-user-convenience (дата звернення: 15.10.2023).
31. Я. І. Дасюк, та ін; Функції комплексної змінної. Перетворення Фур'є та Лапласа : Навч. посіб. для студ. техн. спец. вищ. закл. освіти / Ін-т змісту і методів навчання. — Л., 1999. — 271 с. — (Математика для інженерів). — Бібліогр.: 20 назв.
32. Царьов Р.Ю. Біометричні технології: навч. посіб. [для вищих навчальних Ц18 закладів] / Р.Ю. Царьов, Т. М. Лемеха. – Одеса: ОНАЗ ім. О.С. Попова, 2016. – 140 с.

ДОДАТОК А

Код файлу voice.js

```
// hideElement('#progress');
hideElement('#environmentMessage');
hideElement('#vadMessage');
hideElement('#passphraseMessage');
hideElement('#acceptMessage');
hideElement('#rejectMessage');
hideElement('#authenticationComplete');
hideElement('#authenticationInComplete');
hideElement('#enrollmentComplete');

document.querySelector('#stopRecButton').classList.add('disabled');

var x = document.referrer;
console.log("The refferer of this page is : ", x);

var wavesurfer = WaveSurfer.create({
  container: '#waveform',
  waveColor: '#01BAB6',
  interact: false,
  cursorWidth: 0,
  barGap: 2,
  barHeight: 2,
  barWidth: 0,
  fillParent: true,
```

```
  forceDecode: true,
  plugins: [
    WaveSurfer.microphone.create()
  ]
});

wavesurfer.microphone.on('deviceReady', function (stream) {
  console.log('Device ready!', stream);
});
wavesurfer.microphone.on('deviceError', function (code) {
  console.warn('Device error: ' + code);
});

// start the microphone
wavesurfer.microphone.start();

// pause rendering
//wavesurfer.microphone.pause();

// resume rendering
//wavesurfer.microphone.play();

// stop visualization and disconnect microphone
//wavesurfer.microphone.stopDevice();

// same as stopDevice() but also clears the wavesurfer canvas
//wavesurfer.microphone.stop();

// destroy the plugin
```

```
//wavesurfer.microphone.destroy();

// create an audio in
mic = new p5.AudioIn();

// users must manually enable their browser microphone for recording to work properly!
mic.start();

// create a sound recorder
recorder = new p5.SoundRecorder();

// connect the mic to the recorder
recorder.setInput(mic);

// create an empty sound file that we will use to playback the recording
soundFile = new p5.SoundFile();

if (document.referrer == "http://localhost:8080/enroll") {
  // number of attempts for enrollment.
  var number_of_attempts = 3;
  console.log("number of attempts : ", number_of_attempts);
}
else {
  // number of attempts for enrollment.
  var number_of_attempts = 1;
  console.log("number of attempts : ", number_of_attempts);
}
```

```
// One-liner to resume playback when user interacted with the page.
document.querySelector('#startRecButton').addEventListener('click', function () {

  // For the background sound
  if (document.querySelector('#passphraseMessage').style.display == 'none') {
    showElement('#environmentMessage');

    console.log("You have started recording passphrase...");
    recorder.record(soundFile);
  } else {
    document.querySelector('#passphraseMessage').classList.add('green');;

    console.log("You have started recording the background...");
    recorder.record(soundFile);
  }

  document.querySelector('#startRecButton').classList.add('disabled');
  document.querySelector('#stopRecButton').classList.remove('disabled');
});

document.querySelector('#stopRecButton').addEventListener('click', function () {

  if (document.querySelector('#passphraseMessage').style.display == '') {

  document.querySelector('#stopRecButton').classList.add('disabled');
  document.querySelector('#passphraseMessage').classList.remove('green');

    hideElement("#passphraseMessage");
```

```
    showElement("#vadMessage");

    stopRecording();
  }
  // For the background sound
  else {
    document.querySelector('#startRecButton').classList.remove('disabled');
  document.querySelector('#stopRecButton').classList.add('disabled');

    hideElement("#environmentMessage");
    showElement("#vadMessage");

    stopBackgroundRecording();
  }

});

function stopRecording() {
  console.log("You have stopped recording...");
  recorder.stop(); // stop recorder, and send the result to soundFile

  console.log("Playing the audioifle now...");
  soundFile.play();

  // console.log("Saving the audio file now...");
  // p5.prototype.saveSound(soundFile, file_name); // save file

  console.log("Saving the SoundFile to a blob file ...");
  var soundBlob = soundFile.getBlob();
```

```
// Now we can send the blob to a server...
var xhr = new XMLHttpRequest();

xhr.onreadystatechange = function () {
  if (xhr.readyState == XMLHttpRequest.DONE && xhr.status == 200) {
    console.log("xhr.resposne : ", xhr.response);

    if (xhr.response == "fail") {
      hideElement('#vadMessage');
      showElement('#rejectMessage');


    } else if (xhr.response == "pass") {
      hideElement('#vadMessage');
      showElement('#acceptMessage');

      number_of_attempts--;
      console.log("number of attempts : ", number_of_attempts);
    } else {
      showElement('#passphraseMessage');
      hideElement('#vadMessage');

      document.getElementById('randomPassphrase').innerHTML = xhr.response;
    }
  }
}

xhr.open("POST", "/voice", true);
```

```
  xhr.send(soundBlob);

  console.log("Your http message has been sent.");
}

function stopBackgroundRecording() {
  console.log("You have stopped recording...");
  recorder.stop(); // stop recorder, and send the result to soundFile

  console.log("Playing the audioifle now...");
  soundFile.play();

  // console.log("Saving the audio file now...");
  // p5.prototype.saveSound(soundFile, file_name); // save file

  console.log("Saving the SoundFile to a blob file ...");
  var soundBlob = soundFile.getBlob();

  // Now we can send the blob to a server...
  var xhr = new XMLHttpRequest();

  xhr.onreadystatechange = function () {
    if (xhr.readyState == XMLHttpRequest.DONE && xhr.status == 200) {
      showElement('#passphraseMessage');
      hideElement('#vadMessage');
      document.getElementById('randomPassphrase').innerHTML = xhr.response;
      console.log("xjr.resposne : ", xhr.response);
    }
  }
```

```
  xhr.open("POST", "/vad", true);
  xhr.send(soundBlob);

  number_of_attempts--;
  console.log("Your http message has been sent.");
  console.log("number of attempts : ", number_of_attempts);
}

document.querySelector('#close_button_accept').addEventListener('click', function
() {
  if (number_of_attempts < 0) {
    if (document.referrer == "http://localhost:8080/auth") {
      hideElement('#acceptMessage');
      showElement('#vadMessage');
      hideElement('#passphraseMessage');

      var analysis_text = 'Identifying user based on voice print';
      document.getElementById('recordBody').innerHTML = analysis_text;

      document.querySelector('#vadMessage').classList.add('green');
      document.querySelector('#vadMessage').classList.remove('yellow');

      var xhr = new XMLHttpRequest();

      xhr.onreadystatechange = function () {
        if (xhr.readyState == XMLHttpRequest.DONE && xhr.status == 200) {
          // showElement('#passphraseMessage');
          // hideElement('#vadMessage');
```

```
        // document.getElementById('randomPassphrase').innerHTML =
xhr.response;
        console.log("xjr.resposne : ", xhr.response);

        if (xhr.response == "success") {
          showElement('#authenticationComplete');
        } else {
          showElement('#authenticationIncomplete');
        }
       }
     }

     xhr.open("GET", "/verify", true);
     xhr.send();
   }
   else {
     hideElement('#acceptMessage');
     showElement('#vadMessage');
     hideElement('#passphraseMessage');

     var analysis_text = 'Building Voice Print';
     document.getElementById('recordBody').innerHTML = analysis_text;

     document.querySelector('#vadMessage').classList.add('green');
     document.querySelector('#vadMessage').classList.remove('yellow');

     var xhr = new XMLHttpRequest();

     xhr.onreadystatechange = function () {
```

```
      if (xhr.readyState == XMLHttpRequest.DONE && xhr.status == 200) {
        // showElement('#passphraseMessage');
        hideElement('#vadMessage');
        // document.getElementById('randomPassphrase').innerHTML =
xhr.response;
        console.log("xjr.resposne : ", xhr.response);

        showElement("#enrollmentComplete");
      }
     }

     xhr.open("GET", "/biometrics", true);
     xhr.send();
   }
  }
  else {
   document.querySelector('#startRecButton').classList.remove('disabled');

   hideElement('#acceptMessage');
   showElement('#vadMessage');
   hideElement('#passphraseMessage');

   var xhr = new XMLHttpRequest();

   xhr.onreadystatechange = function () {
    if (xhr.readyState == XMLHttpRequest.DONE && xhr.status == 200) {
      showElement('#passphraseMessage');
      hideElement('#vadMessage');
      document.getElementById('randomPassphrase').innerHTML = xhr.response;
```

```
      console.log("xjr.resposne : ", xhr.response);
    }
  }

  xhr.open("GET", "/vad", true);
  xhr.send();
 }
});

document.querySelector('#close_button_reject').addEventListener('click', function
() {
 document.querySelector('#startRecButton').classList.remove('disabled');

 showElement('#vadMessage');
 hideElement('#rejectMessage');
 hideElement('#passphraseMessage');

 var xhr = new XMLHttpRequest();

 xhr.onreadystatechange = function () {
  if (xhr.readyState == XMLHttpRequest.DONE && xhr.status == 200) {
   showElement('#passphraseMessage');
   hideElement('#vadMessage');
   document.getElementById('randomPassphrase').innerHTML = xhr.response;
   console.log("xjr.resposne : ", xhr.response);
  }
 }

 xhr.open("GET", "/vad", true);
```

```
  xhr.send();
});

function hideElement(elSelector) {
  document.querySelector(elSelector).style.display = 'none';
}

function showElement(elSelector) {
  document.querySelector(elSelector).style.display = '';
}
```