Вінницький національний технічний університет

Факультет менеджменту та інформаційної безпеки

Кафедра менеджменту та безпеки інформаційних систем

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

Вдосконалення методу генерації цифрових ключів за допомогою зліпка обличчя

Виконав: ст. 2-го курсу, групи 2КІТС 22м
спеціальності 125– Кібербезпека
Освітня програма – Кібербезпека
інформаційних технологій та систем
(шифр і назва напряму підготовки, спеціальності)
Мирончак М.А.
(прізвище та ініціали)

Керівник: к.т.н., доцент каф. МБІС
Грицак А. В.
(прізвище та ініціали)
«04» грудня 2023 р.

Опонент: к.т.н., доцент каф. ОТ
Савицька Л.А.
(прізвище та ініціали)
«04» грудня 2023 р.

Допущено до захисту
Голова секції УБ кафедри МБІС

Юрій ЯРЕМЧУК
“04” грудня 2023 р.

Вінниця ВНТУ - 2023 рік

Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

Рівень вищої освіти II -й (магістерський)
Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітньо-професійна програма – Кібербезпека інформаційних технологій та систем

ЗАТВЕРДЖУЮ
Голова секції УБ, кафедра МБІС

_____ **д.т.н., проф. Яремчук Ю.Є.**
«20» вересня 2023 р.

З А В Д А Н Н Я
на магістерську кваліфікаційну роботу студенту
Мирончаку Микиті Андрійовичу
(прізвище, ім`я, по-батькові)

1. Тема роботи: «Вдосконалення методу генерації цифрових ключів за допомогою зліпка обличчя»
Керівник роботи: к.т.н., доц., доцент каф. МБІС Грицак Анатолій Васильович
(прізвище, ім`я, по-батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від «18» вересня 2023 року № 247.
2. Термін подання студентом роботи: за тиждень до захисту.
3. Вихідні дані до роботи:
Стандарти, електронні джерела, підручники та наукові статті по темі. Існуюче програмне забезпечення, яке стосується теми магістерської кваліфікаційної роботи.
4. Зміст текстової частини:
Для досягнення мети роботи було поставлено наступні задачі: дослідити потреби організацій та звичайних людей у засобах захисту інформації; проаналізувати поширені способи захисту інформації та визначити їх недоліки; розглянути принцип роботи засобів захисту; удосконалити алгоритм захисту інформації від витоку через розроблений веб-додаток; перевірити стресостійкість та роботу розробленого додатку. У першому розділі було проведено аналіз існуючих рішень та обґрунтування теми дипломної роботи. У другому розділі здійснено розробку та огляд технології генерації цифрового підпису. У третьому розділі проведено реалізацію програмного продукту та тестування. У четвертному розділі було розглянуто економічну частину.

5. Перелік ілюстративного матеріалу (з точним зазначенням обов'язкових креслень):
У першому розділі магістерської кваліфікаційної роботи наведено 2 рисунка, у другому розділі – 2 рисунків, у третьому розділі – 17 рисунків.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Основна частина			
I	Грицак А. В., к.т.н., доц., доцент каф. МБІС		
II	Грицак А. В., к.т.н., доц., доцент каф. МБІС		
III	Грицак А. В., к.т.н., доц., доцент каф. МБІС		
Економічна частина			
IV	Причепа І.В., доцент кафедри ЕПВМ, к.е.н.		

7.Дата видачі завдання: 20 вересня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№	Назва та зміст етапу	Термін виконання		Примітка
		початок	закінчення	
1.	Визначення напрямку магістерської роботи, формулювання теми	20.09.2023	31.09.2023	
2.	Аналіз предметної області обраної теми	01.10.2023	15.10.2023	
3.	Розробка алгоритму роботи	16.10.2023	26.10.2023	
4.	Написання магістерської роботи на основі розробленої теми	27.10.2023	15.11.2023	
5.	Передзахист магістерської кваліфікаційної роботи	16.11.2023	24.11.2023	
6.	Виправлення, уточнення, корегування магістерської кваліфікаційної роботи	27.11.2023	04.12.2023	
7.	Захист магістерської кваліфікаційної роботи	11.12.2023	17.12.2023	

Студент _____ Мирончак М. А.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Грицак А. В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

УДК 004.056.523:57.087.1

Мирончак М.А. Вдосконалення методу генерації цифрових ключів за допомогою зліпка обличчя. Магістерська кваліфікаційна робота зі спеціальності 125 – «Кібербезпека», освітня програма «Кібербезпека інформаційних технологій та систем». Вінниця: ВНТУ, 2023. 122 с.

На укр. мові. Бібліогр.: 35 назв; рис.: 21; табл. 13.

Ця дипломна робота присвячена розробці та вдосконаленню методу генерації цифрових ключів з використанням біометричної ідентифікації на основі зліпка обличчя. У роботі проведено глибокий аналіз існуючих методів біометричної аутентифікації та їхніх переваг та обмежень. Зосереджуючись на зліпку обличчя, досліджено різноманітні техніки обробки та аналізу обличчя, зокрема методи глибокого навчання та комп'ютерного зору.

У роботі запропоновано та реалізовано власний метод генерації цифрових ключів, який використовує комплексний підхід до аналізу зліпка обличчя. Цей метод поєднує техніки машинного навчання, обробки зображень та аналізу обличчя для створення унікальних та безпечних цифрових ключів. Він забезпечує високий рівень точності ідентифікації, а також стійкість до різних умов зйомки та атак.

Отримані результати демонструють ефективність та потенціал запропонованого методу в області біометричної аутентифікації на основі обличчя. Розроблений метод може знайти застосування в різних сферах, таких як інформаційна безпека, фінансові послуги, медичні системи та багато інших галузей, де забезпечення безпеки та конфіденційності є критично важливими аспектами.

Ключові слова: генерація цифрових ключів, зліпок обличчя, цифровий підпис, безпека, біометричні методи, алгоритми, тестування, NIST.

ABSTRACT

UDC 004.056.523:57.087.1

Myronchak M.A. Improving the method of generating digital keys using a facial cast. Master's qualification thesis on specialty 125 - "Cybersecurity", educational program "Cybersecurity of information technologies and systems". Vinnytsia: VNTU, 2023. 122 p.

In Ukrainian speech Bibliography: 35 titles; Fig.: 21; table 13.

This diploma thesis is dedicated to the development and enhancement of a method for generating digital keys using biometric identification based on facial recognition. The research provides an in-depth analysis of existing biometric authentication methods, exploring their advantages and limitations. Focusing on facial recognition, various techniques in face processing and analysis are investigated, including deep learning and computer vision methods.

The study proposes and implements a novel method for generating digital keys, employing a comprehensive approach to facial recognition analysis. This method combines machine learning techniques, image processing, and facial analysis to create unique and secure digital keys. It ensures a high level of identification accuracy and resistance to various shooting conditions and attacks.

The obtained results demonstrate the effectiveness and potential of the proposed method in the field of facial recognition-based biometric authentication. The developed method can find applications in various domains, including information security, financial services, medical systems, and many other sectors where ensuring security and confidentiality are critically important aspects.

ЗМІСТ

ВСТУП

У сучасному світі, де наукові досягнення та технологічний розвиток надзвичайно швидкі, електронна комунікація та обмін інформацією перетворюються на неодмінну частину нашого повсякденного життя. Однак цей зріст чисельності електронних транзакцій, електронних підписів та обміну даними також викликає зріст ризику зловживанням, крадіжками особистої інформації та ідентифікаційними атаками. У цьому контексті захист особистої інформації та забезпечення безпеки взаємодії у мережі стають вирішально важливими завданнями сучасності. Цифровий підпис виступає як один із важливих інструментів для забезпечення безпеки в електронному середовищі. Це алгоритмічно заснована криптографічна техніка, яка дозволяє підтвердити автентичність даних чи документів та забезпечити їхню цілісність. Зазвичай цифровий підпис генерується за допомогою асиметричних криптографічних алгоритмів, таких як RSA чи ECDSA. Він використовується для перевірки того, чи є документ чи повідомлення отримані від легітимного відправника, чи ні, і чи були вони змінені під час передачі. Ця техніка стала надзвичайно важливою для забезпечення безпеки у фінансових установах, електронній комерції, медичних інформаційних системах та багатьох інших галузях. Але з ростом області біометричних технологій, які дозволяють використовувати унікальні фізіологічні характеристики для ідентифікації особи, народжується питання: чи можна використовувати біометричні дані для генерації цифрових підписів? Це питання стає особливо актуальним у зв'язку із зростанням інтересу до розпізнавання обличчя та інших біометричних методів ідентифікації особи.

Обличчя людини є внутрішньою та унікальною характеристикою, яка може бути використана для ідентифікації, порівняння та впізнавання особи. Методи розпізнавання обличчя, засновані на штучних нейронних мережах та глибокому навчанні, дозволяють точно та надійно впізнавати особу навіть у реальному часі.

Застосування цифрового підпису на основі обличчя може розширити можливості та безпеку електронних транзакцій та забезпечити додатковий рівень захисту особистої інформації в мережі. У нашій дипломній роботі ми розглядаємо можливість використання зліпка обличчя як основи для генерації цифрового підпису. Ми проводимо докладний аналіз існуючих методів генерації цифрових підписів та технологій розпізнавання обличчя. Мета - розробити надійний та безпечний метод генерації цифрового підпису, який може бути використаний у різних сферах, від фінансових транзакцій до медичних записів, для забезпечення автентичності та конфіденційності даних. У роботі ми досліджуємо та порівнюємо різні підходи до генерації цифрових підписів, оцінюємо їхню ефективність та безпеку. Також розробляємо власний алгоритм генерації цифрового підпису на основі зліпка обличчя, використовуючи сучасні методи глибокого навчання та алгоритми криптографії. Цей алгоритм буде піддаватися ретельному тестуванню та оцінці його надійності та швидкості. Ця робота є спробою вдосконалити інструменти безпеки в електронній сфері та розвинути застосування біометричних даних для забезпечення безпеки в електронних транзакціях та комунікаціях. Ми прагнемо створити технологічний внесок у сферу кібербезпеки, надаючи інноваційний та безпечний метод аутентифікації та забезпечення цифрової безпеки в сучасному світі, який надалі стає все більш діджіталізованим та зв'язаним мережею.

Основними завданнями даної роботи є:

- Аналіз методів генерації цифрових ключів
- Вдосконалення методу генерації цифрових ключів за допомогою обличчя
- Розробка програмного засобу з вдосконаленням методу генерації цифрових ключів за допомогою зліпка обличчя
- Аналіз економічної ефективності запропонованих рішень.

Тема цієї роботи є особливо актуальною у зв'язку з :

1. Безпека особистості: З відмітним зростанням кількості онлайн-сервісів та транзакцій важливо забезпечити надійний захист особистих даних та інформації. Використання біометричних методів, зокрема генерація цифрових ключів за допомогою зліпка обличчя, може покращити безпеку особистості.

2. Інновації в біометричних технологіях: Зліпок обличчя є однією з передових технологій біометричного впізнавання. Дослідження та оптимізація методів генерації цифрових ключів на його основі сприяють розвитку інновацій в цьому сегменті технологій.

3. Застосування в сучасних системах безпеки: Технології генерації цифрових ключів на основі біометричних даних можуть знайти широке застосування у сучасних системах безпеки, таких як фінансові установи, корпоративні системи, медичні установи та інші сфери, де необхідна надійна аутентифікація користувачів.

4. Проблеми та виклики безпеки: Розвиток методів генерації цифрових ключів на основі біометричних даних також вирішує проблеми та виклики безпеки, пов'язані із штучним інтелектом, аналітикою даних та кіберзлочинністю.

Таким чином, дана дипломна робота є актуальною, оскільки вона вирішує актуальні проблеми сучасного інформаційного суспільства та сприяє розвитку передових методів забезпечення безпеки особистості та даних.

Об'єктом дослідження є - система методів та технологій генерації цифрових ключів на основі біометричних даних, зокрема, зліпка обличчя.

Предмет дослідження – методи та технології генерації цифрових ключів за допомогою зліпка обличчя.

Новизна роботи полягає у вдосконаленні методу генерації цифрових ключів за допомогою зліпка обличчя.

1 ЗАГАЛЬНИЙ АНАЛІЗ МЕТОДІВ ГЕНЕРАЦІЇ ЦИФРОВИХ КЛЮЧІВ

1.1 Актуальність теми

Актуальність дослідження полягає в глибокому розумінні сучасних викликів та загроз, які виникають в контексті безпеки та конфіденційності в електронному середовищі. Швидкий темп технологічного розвитку супроводжується зростанням вимог до безпеки даних і засобів комунікації. Однією з основних проблем є потреба в надійному способі ідентифікації та автентифікації особи в цифровому середовищі. Традиційні методи аутентифікації, такі як паролі чи PIN-коди, виявляються все менш ефективними через їхню схильність до втрати чи витоку. У цьому контексті, біометричні дані, зокрема зображення обличчя, стають об'єктом зростаючого інтересу у сфері кібербезпеки.

Актуальність нашої теми виражається в потребі розвинути та дослідити нові методи безпечної аутентифікації з використанням біометричних даних. Зліпок обличчя є унікальною біометричною характеристикою, яка може бути використана для впізнавання особи. Його унікальність та неповторюваність роблять його цінним ресурсом у сфері кібербезпеки та аутентифікації. Особливо у контексті зростаючої кількості онлайн-послуг, електронної медицини, фінансових транзакцій та електронного урядування, які вимагають надійної ідентифікації користувачів, нові методи аутентифікації стають критично важливими.

Додатковою актуальністю теми є зростаюча загроза кібератак, спрямованих на викрадення біометричних даних. Оскільки біометричні дані неможливо змінити чи скасувати, їх втрата може мати серйозні наслідки для особистої конфіденційності. Тому важливо не тільки розвивати нові методи генерації цифрового підпису на основі зліпка обличчя, але і забезпечити їхню надійність та захищеність від атак і витоків інформації.

Актуальність нашого дослідження полягає в декількох аспектах:

1. Підвищення рівня безпеки: Запит на безпеку та захист інформації в даний час надзвичайно високий. Все частіше зловмисники використовують різні методи для отримання доступу до конфіденційної інформації. Використання зліпка обличчя для генерації цифрового підпису може забезпечити вищий рівень безпеки та запобігти несанкціонованому доступу.

2. Зручність та швидкість: Використання біометричних даних, зокрема зліпка обличчя, може зробити процес аутентифікації більш зручним та швидким. Особа може підтвердити свою ідентичність шляхом простого зіставлення обличчя, що вимагає мінімального зусилля та часу.

3. Розширені можливості застосування: Зліпок обличчя може бути використаний в широкому спектрі сфер, включаючи фінансові установи, медичні установи, урядові органи, публічні служби, банкінг, електронний бізнес та багато інших. Застосування цифрового підпису на основі зліпка обличчя може сприяти покращенню безпеки та аутентифікації в усіх цих галузях.

4. Розвиток технологій розпізнавання обличчя: За останні роки технології розпізнавання обличчя значно покращилися завдяки розвитку глибокого навчання та штучних нейронних мереж. Це надає можливість точного та надійного розпізнавання обличчя в реальному часі.

Іншим аспектом актуальності є різноманітні сценарії застосування: від покращення безпеки мобільних пристроїв та онлайн-сервісів до використання в критичних інфраструктурах, таких як системи управління літаками чи медичні бази даних. Ці сценарії підкреслюють актуальність нашої теми у різних галузях.

Крім того, враховуючи спрощення використання розпізнавання обличчя у сучасних смартфонах та інших електронних пристроях, цей метод може забезпечити зручність та легкість в користуванні, що робить його ще більш актуальним для кінцевих користувачів.

Отже, актуальність нашої дипломної роботи полягає в потребі вдосконалення методів аутентифікації та забезпечення безпеки електронної комунікації за допомогою цифрових підписів на основі біометричних даних, зокрема, зліпка

обличчя. Наше дослідження відкриває нові можливості та перспективи для розробки інноваційних систем аутентифікації, які можуть бути використані у різних сферах електронного життя [1].

1.2 Аналіз особливостей генерації цифрового підпису

Генерація цифрового підпису - це важливий процес в криптографії, який дозволяє підтвердити автентичність та цілісність цифрового документа або повідомлення. Цифровий підпис дозволяє перевірити, що документ не був змінений після підпису, і що він дійсно був створений особою, яка володіє відповідними приватними ключами. Основними принципами генерації цифрових підписів є [2]:

1. Використання пари ключів:

Генерація цифрового підпису передбачає використання пари ключів - приватного і публічного. Приватний ключ служить для підпису повідомлення, тобто тільки власник ключа може створити цифровий підпис. Публічний ключ використовується для перевірки підпису і доступний для всіх.

2. Хеш-функція:

Для генерації цифрового підпису спочатку створюється хеш-значення повідомлення. Хеш-функція призначена для перетворення великого обсягу даних у фіксований короткий хеш, який ідентифікує повідомлення. Якщо навіть один символ у повідомленні змінюється, хеш значення змінюється радикально. Це допомагає виявити навіть маленькі зміни в документі [3].

3. Підписання хеш-значення:

Після створення хеш-значення повідомлення приватний ключ використовується для підписання цього хеш-значення. Підпис - це криптографічна операція, яка включає в себе використання приватного ключа для створення цифрового підпису, який є унікальним для конкретного повідомлення та ключа.

4. Публікація публічного ключа:

Публічний ключ повинен бути доступний тим, хто має інтерес перевірити цифровий підпис. Зазвичай публічний ключ розміщується на відкритих ключових серверах або в центральних репозиторіях.

5. Перевірка підпису:

Особа, яка отримала цифровий підпис, може використовувати публічний ключ, щоб перевірити його автентичність. Для цього обчислюється хеш-значення отриманого повідомлення, і це хеш-значення порівнюється з декодованим підписом, використовуючи публічний ключ. Якщо вони співпадають, це свідчить про автентичність повідомлення і його незмінність.

6. Криптографічна безпека:

Генерація цифрового підпису передбачає використання криптографічно надійних алгоритмів та ключів, які дуже важко перебрати. Це забезпечує захист від підкрадання ключа або злому підпису шляхом атаки.

7. Відмовостійкість:

Цифровий підпис повинен бути відмовостійким, що означає, що навіть особа, яка створила підпис, не може відмовитися від своєї автентичності. Це досягається завдяки використанню приватного ключа, доступ до якого має обмежене число осіб.

Ці основні принципи генерації цифрових підписів допомагають забезпечити безпеку та автентичність цифрової комунікації та транзакцій в цифровому світі. Вони є важливими компонентами сучасних систем криптографічної безпеки.

Цифрове підписання даних - це процес призначення унікального електронного підпису для документа або даних з метою підтвердження їхньої автентичності, цілісності та невідмінності. Цей процес забезпечує можливість перевірити, що дані не були змінені після підписання та що вони були створені особою або організацією, яка має відповідний приватний ключ.

Основні кроки, які відбуваються під час цифрового підписання даних [4]:

1. Створення хеш-значення: Спочатку оригінальні дані або документ перетворюються в хеш-значення за допомогою хеш-функції, такої як MD-5. Хеш-функція генерує фіксований рядок, який є унікальним для конкретних даних.

2. Підписання хеш-значення: Потім хеш-значення підписується за допомогою приватного ключа особи або організації, яка створила підпис. Підпис створюється за допомогою асиметричного криптографічного алгоритму, такого як RSA чи ECDSA. Приватний ключ зберігається конфіденційно і використовується лише для підписування.

3. Додавання цифрового підпису до документа: Цифровий підпис, разом з публічним ключем власника підпису, додається до оригінальних даних чи документа. Це створює електронний пакет, який містить підписані дані та відкритий ключ для перевірки підпису.

4. Перевірка підпису: Щоб перевірити цифровий підпис, отримувач використовує публічний ключ, який був доданий до підписаних даних. Він застосовує асиметричний алгоритм розшифрування до підпису та порівнює отриманий хеш-значення з хеш-значенням оригінальних даних. Якщо вони співпадають, це означає, що дані не були змінені після підписання та підпис був створений власником приватного ключа, підтверджуючи автентичність документа (рис.1.1).

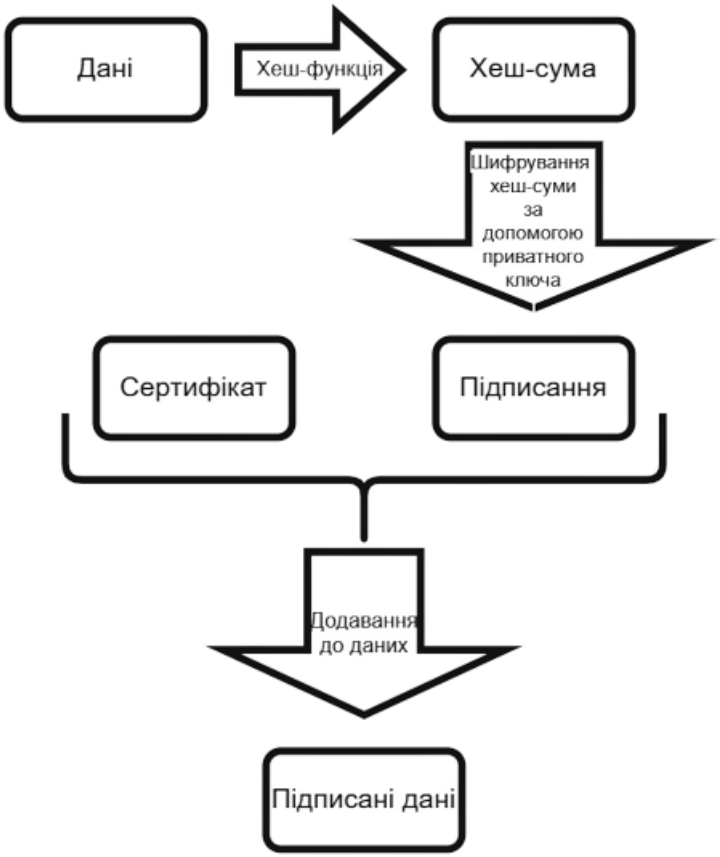


Рисунок 1.1 – Ілюстрація цифрового підписання даних

Цифрове підписання даних забезпечує важливий рівень безпеки та може бути використане в різних сферах, таких як електронна комунікація, фінансові транзакції, електронний документообіг та інші сфери, де важлива захищеність інформації.

Перейдемо до верифікації цифрового підпису.

Верифікація підписаних даних — це процес перевірки, чи є цифровий підпис для конкретних даних автентичним, тобто чи вони були підписані вірною особою чи організацією. Цей процес є важливим для впевненості у тому, що отримані дані невідмінні та автентичні. В отримані дані можна верифікувати, використовуючи публічний ключ, який був отриманий разом із засигнірованими даними.

Основні кроки верифікації підписаних даних:

1. Отримання підписаних даних: Отримувач отримує дані, які були підписані, а також цифровий підпис і публічний ключ особи чи організації, яка підписала дані.

2. Розшифрування цифрового підпису: Застосовуючи асиметричний алгоритм розшифрування, отримувач використовує публічний ключ для дешифрації цифрового підпису. Цей процес перетворює підпис у хеш-значення, яке було згенеровано власником приватного ключа.

3. Генерація хеш-значення для отриманих даних: Отримувач використовує ту ж саму хеш-функцію, яку використовував підписувач, для генерації хеш-значення для отриманих даних чи документа.

4. Порівняння хеш-значень: Отримане хеш-значення для отриманих даних порівнюється із хеш-значенням, яке було отримано розшифруванням підпису. Якщо ці хеш-значення співпадають, це означає, що підпис був створений вірною особою та дані не були змінені після підписання (рис.1.2.).

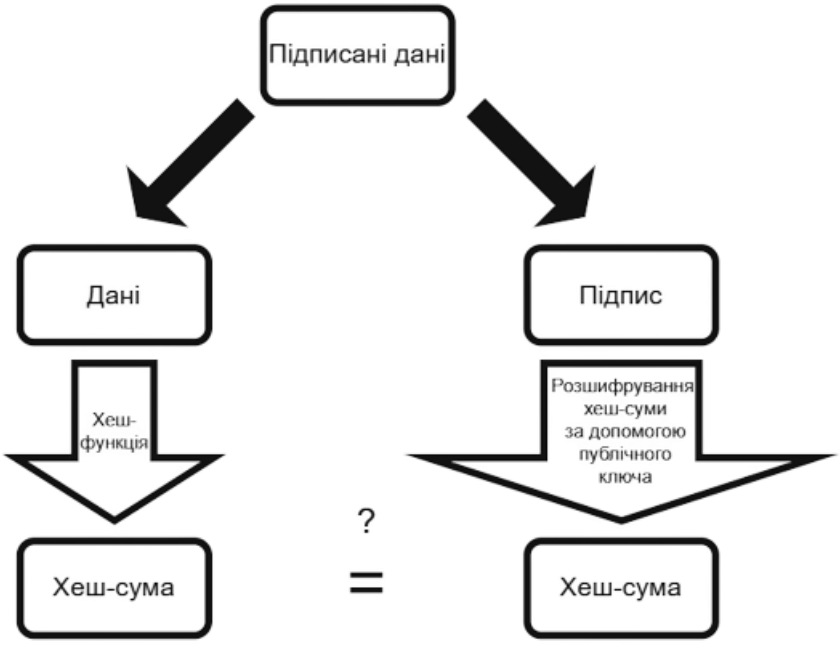


Рисунок 1.2 – Ілюстрація верифікації цифрового підпису

Якщо верифікація успішно завершена, отримувач може бути впевнений у тому, що отримані дані були підписані вірною особою чи організацією та не були

змінені в процесі передачі. Цей процес грає важливу роль у багатьох сферах, де важлива цілісність та автентичність даних, таких як фінансові транзакції, юридичні угоди та електронні документи.

1.3 Проведення огляду існуючих методів генерації цифрових підписів

У цьому розділі нашої дипломної роботи ми ретельно розглянемо різні існуючі методи генерації цифрових підписів, що застосовуються в сучасних системах криптографічної безпеки. Наша мета - детально проаналізувати їхні переваги, недоліки та сфери застосування для отримання глибшого розуміння і виявлення можливостей для вдосконалення нашого методу генерації цифрового підпису на основі зліпка обличчя. Та в цьому розділі розглянемо аналоги додатків.

Face ID - це технологія розпізнавання обличчя, розроблена компанією Apple та використовується для аутентифікації користувачів на їхніх пристроях, таких як iPhone та iPad. Основні особливості Face ID включають [5]:

1. Технологія 3D-розпізнавання обличчя: Face ID використовує технологію TrueDepth, яка включає в себе камеру для зйомки 3D-зображення обличчя користувача. Ця система використовує інфрачервоне світло для створення точної глибинної карти обличчя.

2. Аналіз точок обличчя: TrueDepth вимірює та аналізує більше 30 000 невидимих для ока точок обличчя, створюючи унікальний математичний вектор для кожного користувача.

3. Надійність та безпека: Face ID працює в різних умовах освітлення та має високий рівень надійності. Він також враховує зміни у зовнішньому вигляді користувача, такі як зростання бороди чи зміна зачіски.

4. Використання для аутентифікації: Face ID використовується для розблокування пристрою, підтвердження платежів, входу в деякі додатки та інших задач, що вимагають аутентифікації користувача.

5. Додаткові заходи безпеки: Face ID включає в себе додаткові заходи безпеки, такі як вимога зорового контакту користувача та автоматичне вимкнення Face ID після декількох невдалих спроб розпізнавання.

Процес роботи Face ID включає в себе зіставлення збереженого математичного представлення обличчя, що зберігається у безпечному елементі пристрою, з поточними скануваннями обличчя користувача для підтвердження ідентифікації. Технологія є високоточною та ефективною, що забезпечує зручний та безпечний спосіб аутентифікації на пристроях Apple.

Windows Hello - це функція аутентифікації та безпеки в операційних системах Windows 10 та Windows 11 від компанії Microsoft. Вона пропонує різні методи входу, такі як розпізнавання обличчя, сканування відбитків пальців та інші біометричні методи, а також використання PIN-коду [6]. Основні особливості Windows Hello включають:

1. Розпізнавання обличчя (Face Recognition): Цей метод дозволяє користувачам увійти в систему шляхом розпізнавання їхнього обличчя. Використовується камера, що може сканувати та аналізувати геометрію обличчя, створюючи унікальний шаблон для аутентифікації.

2. Сканування відбитків пальців (Fingerprint Recognition): Цей метод використовує вбудований сканер відбитків пальців на пристрої для ідентифікації користувача за його відбитками пальців.

3. Інші біометричні методи: Windows Hello також підтримує інші біометричні методи, такі як сканування радужки ока, відбитків руки та голосовий доступ.

4. PIN-код: Крім біометричних методів, Windows Hello дозволяє користувачам використовувати PIN-код для входу в систему.

Якщо говорити про те, як саме воно працює, то це визначається конкретним методом аутентифікації. Наприклад, при розпізнаванні обличчя камера сканує обличчя користувача, а алгоритм аналізує унікальні точки та риси, створюючи цифровий шаблон. При використанні відбитків пальців, сканер збирає даний відбитків, алгоритм визначає їхні унікальні особливості.

Windows Hello надає зручний та безпечний спосіб аутентифікації, знижуючи ризик несанкціонованого доступу до пристрою.

DeepFace - це технологія розпізнавання обличчя, розроблена командою Facebook. Вона використовується для автоматичного та точного визначення осіб на фотографіях [7]. Основні особливості та принципи роботи DeepFace включають:

1. Нейронні мережі: DeepFace базується на глибоких нейронних мережах, які навчаються виконувати завдання розпізнавання обличчя за допомогою великої кількості тренувальних даних.

2. Обробка зображень: Алгоритми DeepFace використовуються для обробки зображень та витягування важливих особливостей, таких як форма обличчя, положення очей, носа та рота.

3. Векторне представлення обличчя: DeepFace генерує векторне представлення обличчя на основі нейронних мереж. Цей вектор представляє собою числовий код, який унікально ідентифікує обличчя.

4. Точність розпізнавання: DeepFace відомий своєю високою точністю розпізнавання обличчя, що включає в себе здатність визначати особу на

фотографіях навіть ускладнених умовах, таких як різне освітлення чи поворот обличчя.

5. Масштабованість: DeepFace розроблено з урахуванням масштабованості, що дозволяє ефективно обробляти великі обсяги даних.

Процес роботи DeepFace включає у себе тренування нейронних мереж на великій кількості зображень з обличчями та використання цих навчених моделей для розпізнавання обличчя на нових фотографіях.

Важливо зазначити, що DeepFace використовується в основному в межах продуктів та сервісів Facebook для автоматизованого тегування фотографій та інших завдань розпізнавання обличчя на платформі.

Azure Face API - це сервіс розпізнавання обличчя в хмарному середовищі Microsoft Azure. Він надає розробникам можливість легко інтегрувати функціонал розпізнавання обличчя в свої додатки, включаючи визначення основних параметрів обличчя, виявлення емоцій, визначення віку та інших характеристик [8].

Як працює Azure Face API:

1. Завантаження зображення:

- Розробник передає зображення на сервер Azure Face API.

2. Обробка зображення:

- Сервіс використовує розпізнавання обличчя для визначення ключових параметрів, таких як положення очей, форма обличчя, точки ключових особливостей тощо.

3. Визначення особи:

- Якщо обличчя вже було зареєстроване в системі (наприклад, в базі даних Azure), то сервіс може визначити особу на зображенні.

4. Повернення результатів:

- Результати розпізнавання, такі як ідентифікація осіб, аналіз емоцій, визначення віку тощо, повертаються розробнику для подальшого використання.

Щодо питання про пов'язаність з генерацією цифрових ключів, Azure Face API, в основному, використовується для завдань розпізнавання обличчя та аналізу характеристик осіб на зображеннях, а не для генерації цифрових ключів. Генерація цифрових ключів зазвичай відбувається за допомогою криптографічних алгоритмів та не пов'язана напряму із задачами розпізнавання обличчя.

Kairos - це компанія, яка спеціалізується на розробці технологій розпізнавання обличчя та біометричних рішень [9]. Продукти Kairos можуть використовуватися для автоматизованого розпізнавання обличчя в різноманітних сценаріях, таких як аутентифікація користувачів.

Ключові особливості та етапи роботи Kairos можуть включати:

1. Реєстрація:

- Користувачі реєструють своє обличчя в системі, де алгоритми захоплюють та аналізують ключові особливості, такі як точки, лінії і контури обличчя.

2. Створення шаблону:

- На основі реєстраційних даних генерується унікальний біометричний шаблон, який представляє собою цифровий відбиток обличчя користувача.

3. Зберігання та порівняння:

- Цей шаблон зберігається в базі даних. При подальших спробах аутентифікації система захоплює зображення обличчя та порівнює його з раніше створеним шаблоном для визначення відповідності.

4. Використання в аутентифікації:

- Якщо система розпізнає відповідність, це може бути використано для аутентифікації користувача.

Щодо прив'язки до генерації цифрових ключів, то Kairos може використовуватися як елемент біометричної аутентифікації в системах, де цифрові ключі використовуються для шифрування та безпечного обміну інформацією. Наприклад, обличчя користувача може використовуватися для генерації цифрових ключів, які в подальшому використовуються для шифрування даних чи авторизації в електронних системах.

Програма цієї кваліфікаційної роботи буде розроблена з метою генерації цифрових ключів за допомогою зліпка обличчя, підписування файлів та валідація.

У даному підрозділі в таблиці 1.3 розглянемо такі програми та опишемо їх плюси та мінуси:

Характеристика / Програма	FaceID в iPhone	Windows Hello	DeepFace (Facebook)	Azure Face API	Kairos	Програма дипломної
Плюси						
Точність розпізнавання	Висока	Висока	Висока	Залежить від налаштувань	Висока	Висока
Швидкість роботи	Висока	Висока	Зазвичай висока	Залежить від обсягу даних та обчислювальної потужності	Висока	Висока
Можливість інтеграції з іншими технологіями	Так	Так	Так	Так	Так	Так
Мінуси						
Приватність	Деякі стосуються проблем приватності, оскільки використовується тривимірна модель обличчя	Є питання щодо приватності, оскільки використовується розпізнавання обличчя	Спроби вирішити питання приватності, але у Facebook є претензії щодо збору даних	Може стикається з питаннями приватності при використанні в різних сценаріях	Проблеми приватності можуть виникнути при використанні в різних контекстах	Може стикається з питаннями приватності при використанні в різних сценаріях

Вартість впровадження	Висока	Залежить від обладнання та вимагає підтримки відповідних пристроїв	Зазвичай висока в порівнянні з іншими методами	Може бути висока в залежності від обсягу використання	Висока	Може бути висока в залежності від обсягу використання
Залежність від умов освітлення	Так	Може впливати на точність	Так	Так	Так	Так
Доступність документації та підтримки	Обмежена	Залежить від розробника	Обмежена	Залежить від Microsoft	Висока	Обмежена

1. Асиметричні криптографічні методи:

Асиметричні методи, такі як RSA (Rivest-Shamir-Adleman) і ECDSA (Elliptic Curve Digital Signature Algorithm), використовують пару ключів: приватний і публічний. Приватний ключ використовується для підпису документів, тоді як публічний ключ використовується для перевірки підпису. Вони є популярними і застосовуються в різних галузях, від фінансових операцій до комунікаційних мереж.

Переваги: Висока надійність, відмінна криптографічна стійкість, широке застосування.

Недоліки: Обчислювальна складність, велика довжина ключів, високий рівень обчислювальних ресурсів.

2. Алгоритми на основі еліптичних кривих:

Алгоритми на основі еліптичних кривих використовують математичні властивості еліптичних кривих для створення підпису. Вони зазвичай використовують менше обчислювальних ресурсів і ключі меншої довжини для забезпечення того ж рівня безпеки, як і традиційні RSA ключі.

Переваги: Ефективність використання обчислювальних ресурсів, висока стійкість до криптографічних атак.

Недоліки: Вимагає математичних знань та уваги до деталей реалізації.

3. Квантові методи генерації підписів:

Квантові методи генерації підписів використовують квантові властивості для створення та перевірки цифрових підписів. Це нова, перспективна галузь криптографії, яка використовує квантові біти (кубіти) для забезпечення безпеки.

Переваги: Висока стійкість до квантових атак, можливість використання квантових ключів.

Недоліки: Висока складність в реалізації, обмежена доступність квантових технологій.

4. Біометричні методи генерації підписів:

Біометричні методи використовують унікальні фізіологічні характеристики особи, такі як відбитки пальців, розпізнавання голосу чи розпізнавання обличчя, для створення та перевірки цифрових підписів.

Переваги: Висока точність ідентифікації, зручність використання, невідмовність від ключів.

Недоліки: Можливість помилок у роботі в умовах невідомих або змінних факторів, таких як освітлення або оновлення фізіологічних характеристик.

Розглянемо ширше біометричні методи генерації цифрових підписів та проведемо порівняння, так як на мою думку це більш недосліджені методи які мають великий потенціал в майбутньому.

Кожен біометричний метод генерації цифрових ключів має свої переваги та обмеження, які впливають на їхню ефективність та застосовність. Ось докладний аналіз переваг та обмежень кожного методу:

1. Відбитки пальців - використання унікальних особливостей відбитків пальців для генерації ключів. Методи можуть включати аналіз мінутій, довжину та форму папільярних ліній тощо. Було розглянуто кілька важливих публікацій та наукових досліджень, які вивчають методи генерації цифрових ключів за допомогою відбитків пальців:

Ця книга [10] представляє інтегральний погляд на технології розпізнавання відбитків пальців, включаючи методи генерації цифрових ключів на основі цих біометричних даних. Вона розглядає різні аспекти біометричних технік та їх використання в криптографії. У [11] статті автори представляють основні методи біометричної ідентифікації, включаючи аналіз відбитків пальців. Вони також розглядають аспекти генерації цифрових ключів та їх використання для забезпечення безпеки систем. У [12] статті розглядаються різні методи захисту шаблонів відбитків пальців. Автори досліджують техніки генерації цифрових ключів та їх застосування для забезпечення конфіденційності та безпеки біометричних даних. Ця стаття [13] описує питання безпеки та конфіденційності у системах аутентифікації на основі біометрії, зокрема використання відбитків пальців. Автори розглядають методи генерації ключів та їх застосування для захисту біометричних даних.

Ці публікації відображають актуальні та важливі аспекти досліджень у галузі генерації цифрових ключів за допомогою відбитків пальців та їх впровадження генерації цифрових ключів. Також було виділено переваги, обмеження та недоліки даного методу:

Переваги:

- Унікальність: Кожен відбиток пальця є унікальним, що робить його ефективним для ідентифікації особи.

- Відносна зручність: Зручность використання відбитків пальців для аутентифікації, оскільки біометричні дані можна легко зібрати за допомогою сучасних сканерів відбитків пальців.

Обмеження:

- Прихованість: Відбитки пальців можуть бути залишені на поверхнях і стати доступними для несанкціонованого доступу.

- Змінність: При зміні відбитка пальця (наприклад, через зношеність шкіри або травму) може бути важко досягти точної аутентифікації.

Недоліки:

Несекретність: Якщо відбитки пальців стають відомі, їх вже не можна змінити, що робить їх незастосовними в разі компрометації.

Фальсифікація: Відбитки пальців можуть бути підроблені за допомогою різних методів, таких як відбитки пальців з латексу чи силікону.

2. Іріс ока - використання унікальних особливостей структури ірісу для генерації ключів. Іріс містить сліпучу та нерегулярну структуру, яка може бути використана для створення унікальних ключів. Розглянуто деякі важливі публікації та літературні джерела, які досліджують методи генерації цифрових ключів за допомогою ірису ока:

Так, у роботі [14] автор представляє основні принципи роботи ірисового розпізнавання та методи генерації цифрових ключів на основі ірису ока. Автор, який є піонером у цій області, розглядає математичні аспекти та методи аналізу ірису для створення унікальних ідентифікаторів. У [15] описується реалізація системи автоматизованого ірисового розпізнавання, включаючи методи генерації ключів та їх застосування для автентифікації користувачів.

Ця стаття [16] досліджує можливості використання ірисового розпізнавання для аутентифікації користувачів на мобільних пристроях. Вона охоплює методи генерації цифрових ключів та їх інтеграцію в мобільні платформи. Автори цієї роботи [17] фокусуються на проблемах сегментації ірису та її впливі на якість ірисового розпізнавання. Автори розглядають техніки генерації цифрових ключів, які враховують особливості сегментації. У цій статті обговорюється підвищення точності ірисового розпізнавання за допомогою об'єднання результатів сегментації. Автори [18] досліджують вплив якості сегментації на генерацію цифрових ключів.

Ці публікації відображають важливість та актуальність досліджень у галузі генерації цифрових ключів за допомогою ірису ока, а також висвітлюють різноманітні техніки та виклики, що стосуються цієї технології. Також було виділено переваги, обмеження та недоліки даного методу:

Переваги:

- Унікальність: Іріс ока має складну та унікальну структуру, яка робить її дуже ефективною для ідентифікації.

- Стабільність: Іріс ока має тенденцію залишатися стабільним з часом, що забезпечує надійну аутентифікацію протягом тривалого періоду.

Обмеження:

- Запит на обладнання: Для збору біометричних даних потрібне спеціальне обладнання, що може бути відносно дорогим та складним у використанні.

- Зв'язаність з організмом: Іріс ока пов'язаний з організмом людини, і його даними може бути складно управляти у випадку змін у стані здоров'я користувача.

Недоліки:

Запит на обладнання: Для зібрання ірісу потрібне спеціалізоване обладнання, що може бути відносно дорогим та не зручним для використання.

Дискомфорт для користувача: Зібрання даних про іріс може бути неприємним для користувача та викликати дискомфорт.

3. Зіниця ока - аналіз особливостей зіниці, таких як форма та розмір, для генерації ключів. Дослідження методів генерації цифрових ключів за допомогою зіниці ока відіграють важливу роль у розвитку біометричних технологій та криптографії. Ось опис кількох ключових публікацій та літературних джерел, що досліджують цю тему:

Ця публікація [19] відома як важливий науковий огляд та включає деталізований опис алгоритмів розпізнавання ірису, включаючи методи генерації цифрових ключів на основі ірису ока. Даугман є провідним науковцем у галузі ірисового розпізнавання. Автори цієї [20] статті надають огляд останніх досягнень у галузі ірисового розпізнавання, включаючи методи генерації цифрових ключів та їх застосування для автентифікації. Ця стаття [21] досліджує можливості використання ірисового розпізнавання для аутентифікації користувачів на мобільних пристроях, включаючи техніки генерації цифрових ключів, а автори цієї статті [22] представляють систему автоматизованого ірисового розпізнавання, включаючи техніки генерації цифрових ключів та їх використання для ідентифікації користувачів.

У цій [23] статті автори досліджують застосування аналізу незалежних компонентів (Independent Component Analysis, ICA) для ірисового розпізнавання та розглядають вплив цієї техніки на генерацію цифрових ключів.

Ці публікації представляють важливі дослідження та досягнення у галузі генерації цифрових ключів за допомогою зіниці ока, які відображають сучасний стан цієї технології. Також було виділено переваги, обмеження та недоліки даного методу:

Переваги:

- Унікальність: Зіниця ока також має унікальні характеристики, що робить її ефективною для біометричної аутентифікації.

- Неінвазивність: Збір даних про зіницю ока може бути неінвазивним та зручним для користувача.

Обмеження:

- Освітлення та умови зйомки: Якість зіниці ока може бути вплинута наявністю або відсутністю освітлення під час сканування.

- Вимоги до точності: Зіниця ока має високу структурну складність, що вимагає високої точності під час зібрання та порівняння даних.

Недоліки:

Освітлення: Потрібне додаткове освітлення для точного сканування може бути складним у деяких умовах.

Чутливість: Системи розпізнавання зіниці можуть бути чутливими до змін освітлення та інших факторів.

4. Голос - використання акустичних особливостей голосу для генерації унікальних ключів. Дослідження методів генерації цифрових ключів за допомогою голосових біометричних даних є актуальною темою в галузі інформаційної безпеки та аутентифікації. Ось опис кількох ключових публікацій та літературних джерел, що досліджують цю тему:

Ця стаття [24] представляє основи гаусових змішаних моделей для голосової ідентифікації. Автори досліджують методи генерації цифрових ключів на основі голосових характеристик а у цій статті автори [25] досліджуються питання аутентифікації за допомогою голосу для телефонних транзакцій. Автори розглядають техніки генерації цифрових ключів на основі голосу та їхню ефективність. Ця робота [26] пропонує огляд текстонезалежної системи голосової ідентифікації та методів генерації цифрових ключів на основі голосових ознак. У

цій статті [27] автори досліджують застосування глибоких нейронних мереж для задач голосової ідентифікації та аутентифікації. Методи генерації цифрових ключів також розглядаються в контексті нейромережевих підходів. Ця стаття [28] розглядає питання виявлення спроб обману у голосовій аутентифікації та методи генерації цифрових ключів для виявлення обману.

Ці публікації відображають різноманітні аспекти досліджень у галузі генерації цифрових ключів за допомогою голосових біометричних даних та їх використання в сучасних системах безпеки. Також було виділено переваги, обмеження та недоліки даного методу:

Переваги:

- Унікальність: Кожен голос є унікальним і може бути використаний для ідентифікації особи.

- Невидимість: Голос можна збирати без зовнішніх слідів, що робить його зручним для аутентифікації без відома користувача.

Обмеження:

- Шум: Зовнішні шуми або зміни у голосі (наприклад, захворювання) можуть вплинути на якість та надійність аутентифікації голосом.

- Імітація: Голос може бути імітований, що може створити ризик для системи, яка не враховує додаткові методи перевірки.

Недоліки:

Зміни в голосі: Хвороби або інші зміни в голосі можуть вплинути на точність ідентифікації.

Шум: Навколишні шуми можуть впливати на якість аудіозапису, ускладнюючи аутентифікацію.

5. Лице - використання геометричних особливостей обличчя, таких як відстані між очима, розмір рота тощо, для створення ключів. Дослідження методів генерації цифрових ключів за допомогою зліпку обличчя (facial biometrics) є важливою галуззю в біометричних технологіях. Ось огляд кількох ключових публікацій та літературних джерел, які досліджують цю тему:

У цій статті група науковців [29] розглядає методи виявлення живого обличчя, що є важливим аспектом у генерації цифрових ключів на основі зліпку обличчя. Автори використовують мультимасштабні текстурні ознаки для вирішення цього завдання, а у роботі [30] розглядається використання глибоких нейронних мереж для витягування репрезентативних ознак з зображень обличчя, що може бути використано для генерації цифрових ключів. Ця рецензія [31] включає в себе огляд різних методів генерації цифрових ключів на основі зліпку обличчя та їх використання в різних сферах, включаючи безпеку та ідентифікацію. Ця робота [32] розглядає концепцію "м'яких біометричних ознак", включаючи різні атрибути обличчя, такі як вік, стать, кольор волосся та інші, які можуть бути використані для генерації цифрових ключів. Ця стаття [33] досліджує різні глибокі нейронні мережі, їхню ефективність та використання у завданнях розпізнавання обличчя, включаючи генерацію цифрових ключів.

Ці публікації відображають різноманітні аспекти досліджень у галузі генерації цифрових ключів за допомогою зліпку обличчя та важливість цієї технології для біометричної ідентифікації. Також було виділено переваги, обмеження та недоліки даного методу, який ми і оберемо для реалізації програми:

Переваги:

- Зручність: Ідентифікація обличчя може бути проведена безпосередньо за допомогою вбудованих камер в пристрої або системі відеоспостереження.

- Безконтактність: Ідентифікація за обличчям може бути здійснена без прямого контакту зі сканером, що робить її гігієнічною та безпечною.

Обмеження:

- Зміни в зовнішності: Зміни в зовнішності (наприклад, зміна в зачісці, вирізання бороди тощо) можуть вплинути на точність ідентифікації за обличчям.

- Освітлення та ракурс: Погані умови освітлення або специфічний ракурс можуть зробити ідентифікацію менш надійною.

Недоліки:

Імітація: Системи розпізнавання можуть бути обмануті за допомогою фотографій або масок, що імітують обличчя користувача.

Приватність: Питання приватності можуть виникати через використання камер для відстеження обличчя без відома користувача.

6. ДНК - використання генетичних особливостей ДНК для генерації унікальних біометричних ключів. Дослідження методів генерації цифрових ключів за допомогою ДНК відіграють важливу роль у сучасних біометричних технологіях та криптографії. Ось огляд кількох ключових публікацій та літературних джерел, які досліджують цей метод:

Ця стаття [34] розглядає використання флуоресцентних методів для вимірювання взаємодії ДНК з білками. Такі методи можуть бути використані для генерації унікальних ДНК-заснованих цифрових ключів. У статті [35], автор вивчає останні тенденції та методи зберігання даних на основі ДНК. Такі методи можуть бути застосовані для генерації та зберігання цифрових ключів.

У цій роботі [36] розглядається використання ДНК як бази для створення криптографічних ключів. Автори досліджують можливості створення генетично заснованих цифрових ключів. Ця стаття [37] досліджує можливості зберігання великих обсягів інформації в ДНК, використовуючи його як носій для цифрових

даних. Ця робота пропонує [38] новий підхід до зберігання даних в ДНК, який може бути використаний для генерації цифрових ключів.

Ці публікації представляють важливі дослідження в області зберігання та використання ДНК для генерації цифрових ключів, що може мати значення в біометричних системах і криптографії. Також було виділено переваги, обмеження та недоліки даного методу:

Переваги:

- Унікальність: ДНК унікальна для кожної особи та має високу ступінь унікальності в порівнянні з іншими біометричними характеристиками.

- Довготривалість: ДНК залишається сталим протягом усього життя особи.

Обмеження:

- Час і затрати: Збір та аналіз ДНК можуть бути часом і витратами, що ускладнює їхнє використання у багатьох ситуаціях.

- Приватність та етика: Збір та зберігання генетичних даних пов'язані з етичними питаннями та питаннями приватності, що потребують уважного врахування.

Недоліки:

Час і витрати: Збір та аналіз генетичних даних можуть бути дорогими та часомірними процесами.

Приватність: Генетичні дані є вкрай особистими, і їх збір та зберігання пов'язані з етичними та приватнісних питаннями.

7. Венозна структура - використання унікальних венозних особливостей, наприклад, відстань між венами та їх структура, для генерації ключів. Дослідження методів генерації цифрових ключів за допомогою венозної структури руки або

інших частин тіла, відомої як венозна біометрія, є важливою галуззю в біометричних технологіях. Ось огляд кількох ключових публікацій та літературних джерел, які досліджують цю тему:

Ця стаття [39] розглядає проблеми забезпечення безпеки біометричних шаблонів, зокрема шаблонів венозних ознак. Вона висвітлює використання "fuzzy vault" для безпечного зберігання та порівняння венозних шаблонів. У цій статті авторами [40] розглядається метод витягування ознак з венозних зображень пальця, який може бути використаний для генерації унікальних цифрових ключів. Ця робота [41] досліджує застосування глибокого навчання для розпізнавання венозних зразків пальця та розглядає можливості використання цього підходу для генерації цифрових ключів. У цій роботі [42] представлено новий метод кодування венозних зразків пальця та його застосування для розпізнавання особи. Це може бути використано для генерації цифрових ключів. Ця стаття вивчає [43] методи витягування ознак з венозних зображень пальця за допомогою локального напрямного кодування та їхнє використання для розпізнавання особи.

Ці публікації відображають різноманітні підходи до генерації цифрових ключів за допомогою венозної біометрії та досліджують їхню ефективність у біометричних системах та застосуваннях для безпеки. Також було виділено переваги, обмеження та недоліки даного методу:

Переваги:

- Унікальність: Венозна структура має унікальні риси та організацію, що робить її важливою для біометричної ідентифікації.

- Зручність: Зібрання даних про венозну структуру може бути відносно зручним та неінвазивним.

Обмеження:

- Вимоги до точності: Зібрання точних даних про венозну структуру може вимагати високої точності у виконанні та аналізі зображень вен.

- Периферійні впливи: Лікування та інші периферійні впливи можуть змінити зовнішність венозної структури.

Недоліки:

Специфічність обладнання: Збір венозних даних може вимагати спеціалізованого обладнання, що зробить процес відбору складнішим.

8. Характер письма - використання особливостей написання (наприклад, стиль написання букв, швидкість тощо) для створення біометричних ключів. Дослідження методів генерації цифрових ключів за допомогою аналізу характеру письма (графологічна біометрія) є цікавою галуззю в біометричних технологіях. Ці публікації та літературні джерела розглядають цю тему:

Ця книга [44] розглядає аспекти графологічної аутентифікації та вивчає індивідуальні риси у письмі, які можуть бути використані для генерації унікальних цифрових ключів. Ця стаття [45] досліджує методи розпізнавання письма та різні аспекти характеру письма, які можуть бути використані для ідентифікації особи та генерації цифрових ключів. Ця робота [46] розглядає методи верифікації підписів за допомогою аналізу рукопису та ідентифікації особи на основі характеристик письма. Ця наукова праця [47] досліджує можливості використання цифрових пенів для збору даних про підписи та їх використання для біометричної аутентифікації. Та у цій роботі [48] автори досліджують використання вейвлет-трансформації для аналізу рукопису та його застосування для біометричної ідентифікації особи.

Ці публікації розглядають різні аспекти графологічної біометрії та можливості її використання для генерації цифрових ключів у сучасних системах безпеки та ідентифікації. Також було виділено переваги, обмеження та недоліки даного методу:

Переваги:

- Унікальність: Стиль та особливості написання мають унікальні характеристики, які можуть бути використані для ідентифікації.

Обмеження:

- Динаміка: Стиль написання може змінюватися з часом або в різних умовах, що може ускладнити ідентифікацію особи.

- Обмеженість: Метод характеристики письма може бути обмеженим до конкретних застосувань, наприклад, в біометричних системах контролю доступу.

Недоліки:

Динаміка: Стиль написання може змінюватися з часом, що може ускладнити ідентифікацію.

9. Електроенцефалограма (ЕЕГ) - Використання електричних сигналів у мозку для ідентифікації та генерації ключів. Дослідження методів генерації цифрових ключів за допомогою електроенцефалограми (EEG) представляють важливу галузь в біометричних технологіях та досліджують можливості використання мозкової активності для ідентифікації особи. Ось огляд кількох ключових публікацій та літературних джерел, які досліджують цю тему:

Ця стаття розглядає [49] різні алгоритми класифікації для EEG-сигналів та їхнє використання в системах ідентифікації на основі мозкової активності. У цій роботі [50] автори представляють методику аутентифікації особи на основі EEG-сигналів, яка використовує алгоритми оптимізації та векторної квантизації навчення. Ця стаття [51] досліджує використання різних методів обробки сигналів (PCA, ICA, LDA) та методів машинного навчання для класифікації EEG-сигналів з метою ідентифікації особи.

У цій роботі автори [52] розглядають використання EEG-сигналів під час слухання та думки для аутентифікації особи. Ця стаття [53] вивчає використання еволюційних алгоритмів для аутентифікації користувача на основі EEG-сигналів.

Ці публікації відображають різноманітні методи та підходи до генерації цифрових ключів на основі EEG-сигналів для розробки систем біометричної ідентифікації. Також було виділено переваги, обмеження та недоліки даного методу:

Переваги:

- Унікальність: ЕЕГ-сигнали можуть мати унікальні характеристики для кожної особи.

- Неінвазивність: ЕЕГ може бути зібрана безпечно та неінвазивно, не потребуючи фізичного контакту з користувачем.

Обмеження:

- Запит на обладнання: Збір сигналів ЕЕГ вимагає спеціалізованого обладнання, яке може бути відносно дорогим та складним у використанні.

- Часові вимоги: Збір якісних сигналів може вимагати тривалого періоду спостереження, що робить його менш практичним для швидко використовуваних біометричних систем.

Недоліки:

Запит на обладнання: Збір сигналів ЕЕГ вимагає спеціалізованого обладнання, яке може бути відносно дорогим та складним у використанні.

Динаміка сигналу: Сигнали ЕЕГ можуть змінюватися внаслідок фізичних чи психічних станів користувача.

Загальний вибір біометричного методу повинен враховувати ці недоліки, оскільки вони можуть вплинути на надійність та безпеку системи. Компроміс між

недоліками і перевагами кожного методу грає ключову роль у розробці ефективних та безпечних біометричних систем ідентифікації

Кожен з цих методів має свої унікальні характеристики, які потрібно враховувати при виборі біометричної системи для конкретних застосувань. Важливо збалансувати переваги та обмеження для досягнення найвищого рівня безпеки та зручності користувача.

Після докладного розгляду різних методів генерації цифрових підписів, ми розуміємо, що кожен з них має свої переваги та недоліки. У цій дипломній роботі ми прагнемо поєднати переваги біометричних методів, зокрема розпізнавання обличчя, з традиційними асиметричними криптографічними методами. Мета дипломної роботи - розробити новий, надійний та безпечний метод генерації цифрового підпису на основі зліпка обличчя, який враховує і використовує найкращі аспекти обох цих підходів для забезпечення високої стійкості та безпеки в цифровому середовищі.

1.4 Алгоритми генерації цифрового підпису на основі зображень обличчя

Алгоритми генерації цифрового підпису на основі зображень обличчя є складними криптографічними системами, які використовують біометричні дані для створення унікальних цифрових підписів. Ці алгоритми поєднують в собі інформацію про обличчя користувача з криптографічними методами для створення надійного підпису. Давайте розглянемо їх докладно:

1. Збір та обробка біометричних даних:

Перший крок у процесі генерації цифрового підпису на основі зображень обличчя - це збір біометричних даних. Для цього можуть використовуватися різні методи, такі як веб-камера, сканер обличчя або мобільний додаток, які збирають

фотографії обличчя користувача. Отримані дані потім піддаються обробці для виділення ключових характеристик обличчя, таких як контур, риси, очі, ніс і рот.

2. Витягнення хеш-значення:

Одним із ключових аспектів цих алгоритмів є витягнення хеш-значення з обробленого зображення обличчя. Для цього використовуються криптографічні хеш-функції, які перетворюють зображення в фіксований короткий рядок байтів. Цей хеш служить унікальним представленням обличчя і визначається вихідними даними біометричного аналізу.

3. Підписання хеш-значення:

Після отримання хеш-значення обличчя, воно підписується з використанням приватного ключа користувача. Це виконується за допомогою криптографічного алгоритму, який включає в себе приватний ключ і вихідне хеш-значення. Підпис служить підтвердженням автентичності обличчя та його відповідності публічному ключу користувача.

4. Зберігання публічного ключа:

Публічний ключ користувача повинен бути збережений в безпечному місці і доступним тим, хто має інтерес в перевірці цифрового підпису. Цей ключ є відкритим і доступним для всіх.

5. Перевірка цифрового підпису:

Особа, яка отримала цифровий підпис, може використовувати публічний ключ користувача для перевірки його автентичності. Для цього обчислюється хеш-значення прийнятого зображення обличчя, і це хеш-значення порівнюється з

розкодованим підписом, використовуючи публічний ключ. Якщо вони співпадають, це свідчить про автентичність обличчя та його відповідність публічному ключу.

6. Криптографічна безпека:

Для забезпечення високого рівня безпеки, ці алгоритми використовують криптографічні методи для захисту приватного ключа та підпису. Ключеві параметри, такі як довжина ключа та кількість бітів у хеш-значенні, важливо вибирати так, щоб забезпечити відмовостійкість і недосяжність атак.

7. Відмовостійкість:

Цифровий підпис повинен бути відмовостійким, що означає, що навіть особа, яка створила підпис, не може відмовитися від своєї автентичності. Це досягається завдяки використанню приватного ключа, доступ до якого має обмежене число осіб.

Ці алгоритми представляють сучасний підхід до генерації цифрових підписів, який використовує високотехнологічні методи біометричної аутентифікації та криптографії для забезпечення безпеки та надійності цифрових транзакцій та комунікацій. Ці алгоритми широко застосовуються в сучасних системах електронної ідентифікації та цифрових підписів для забезпечення конфіденційності та недоторканості даних.

1.5 Аналіз алгоритмів генерації та вбудування цифрового підпису на основі зображень обличчя

Генерація та вбудування цифрового підпису на основі зображень обличчя представляється сучасним та перспективним напрямком у сфері біометричної аутентифікації. Цей підхід об'єднує в собі потужність біометричних даних з ефективністю криптографічних методів для створення надійних та безпечних

цифрових підписів. У цьому аналізі ми розглянемо кілька ключових аспектів алгоритмів генерації та вбудування цифрових підписів на основі зображень обличчя, а також порівняємо різні підходи та їхні переваги та недоліки.

1. Безпека та надійність:

Однією з основних переваг алгоритмів генерації та вбудування цифрового підпису на основі зображень обличчя є їхня висока безпека. Використання біометричних даних, таких як зліпок обличчя, забезпечує велику відмовостійкість, оскільки біометричні характеристики унікальні для кожної особи. Однак, важливо звернути увагу на захист біометричних даних від атак та несанкціонованого доступу, що може бути викликаної втратою апаратних пристроїв або застосуванням технік обману.

2. Точність і відмовостійкість:

Алгоритми, що використовують зліпок обличчя для генерації цифрового підпису, повинні бути точними та відмовостійкими. Точність полягає в здатності вірно визначити особу на основі її обличчя, навіть при зміні виразу обличчя або освітлення. Відмовостійкість визначається тим, наскільки складно зламати або підробити біометричні дані. Отже, алгоритми повинні бути стійкими до різних видів атак, включаючи атаки з використанням фальшивих зображень або живих моделей обличчя.

3. Швидкодія:

Швидкість алгоритмів генерації та вбудування цифрового підпису на основі зображень обличчя грає важливу роль у реальних застосуваннях, таких як автоматизовані системи перевірки осіб на вході або електронний документообіг. Швидкість обробки зображень та генерації підпису повинна бути оптимальною, щоб забезпечити відмінну продуктивність без втрати точності.

4. Відмінності в методах генерації:

Різні алгоритми можуть використовувати різні підходи до обробки та використання зображень обличчя. Наприклад, деякі методи можуть використовувати глибоке навчання для ефективного виділення характеристик обличчя, тоді як інші можуть застосовувати класичні методи комп'ютерного зору та обробки зображень. Порівняння різних підходів дозволяє визначити найефективніші та найнадійніші методи для використання.

5. Інтеграція та сумісність:

У багатьох випадках системи генерації та вбудування цифрових підписів повинні інтегруватися з існуючими системами безпеки та ідентифікації. Це означає, що алгоритми повинні бути сумісними із стандартами та протоколами безпеки, такими як TLS (Transport Layer Security) та PKI (Public Key Infrastructure), щоб забезпечити взаємодію з іншими системами безпеки та обмін даними у захищеному форматі.

6. Витрати на ресурси:

Однією з важливих характеристик алгоритмів є витрати на ресурси, такі як обчислювальна потужність та обсяг пам'яті. Наприклад, складні алгоритми глибокого навчання можуть вимагати значно більше обчислювальних ресурсів порівняно з класичними методами обробки зображень. Оцінка витрат на ресурси є важливим критерієм при виборі алгоритму для конкретного застосування.

1.6 Аналіз та порівняння існуючих криптографічних алгоритмів генерації цифрового підпису

Генерація цифрового підпису є критично важливою операцією у сучасних криптографічних застосуваннях. Різні алгоритми цифрового підпису мають свої унікальні властивості, що впливають на їхню безпеку, швидкодію та

відмовостійкість. У цьому аналізі розглянемо і порівняємо кілька ключових алгоритмів генерації цифрового підпису: RSA, DSA, ECDSA, MD5 та SHA (Secure Hash Algorithm) серії.

1. RSA (Rivest-Shamir-Adleman):

- Принцип роботи: RSA є асиметричним алгоритмом, який використовує два ключі: приватний і публічний. RSA використовується для підписування повідомлень та перевірки підпису. Приватний ключ використовується для підпису, а публічний для перевірки підпису.

- Переваги:

- Висока безпека та відмовостійкість.

- Широко використовується у різних застосуваннях.

- Недоліки:

- Потребує великої обчислювальної потужності для обробки довгих ключів.

- Повільний порівняно з деякими іншими алгоритмами.

2. DSA (Digital Signature Algorithm):

- Принцип роботи: DSA - асиметричний алгоритм, спеціально розроблений для генерації цифрових підписів. Використовується для підписування повідомлень та їхньої перевірки.

Переваги:

- Відмінна безпека та відмовостійкість при відповідних параметрах.

- Можливість використання в обмежених обчислювальних умовах.

Недоліки:

- Складний вибір параметрів кривої для забезпечення безпеки.

- Потребує вибору правильних параметрів ключів.

3. ECDSA (Elliptic Curve Digital Signature Algorithm):

- Принцип роботи: ECDSA використовує еліптичні криві для генерації цифрових підписів. Високі безпека та швидкодія роблять його вигідним у порівнянні з іншими алгоритмами.

Переваги:

- Висока швидкодія та ефективність у порівнянні з іншими алгоритмами.

- Використовує коротші ключі, що полегшує роботу з обчислювальними ресурсами.

Недоліки:

- Потребує вибору правильних параметрів кривої.

4. MD5 (Message Digest Algorithm 5):

- Принцип роботи: MD5 - це хеш-функція, яка створює 128-бітне (16-байтове) хеш-значення для вхідних даних. Використовується для відображення великих об'ємів даних у фіксований розмір хешу.

Переваги:

- Швидкодія та простота в реалізації.

- Використовується для перевірки цілісності даних.

Недоліки:

- Колізії (дві різні вхідні послідовності, що дають однаковий хеш) були знайдені, що робить його менш безпечним для деяких застосувань.

- Вважається вже застарілим для криптографічних застосувань.

5. SHA (Secure Hash Algorithm):

- Принцип роботи: SHA - це серія криптографічних хеш-функцій, які генерують фіксовані розмір хеш-значень. SHA-1, SHA-256, SHA-384 та SHA-512 - основні представники серії.

Переваги:

- Висока безпека та відмовостійкість.

- Широко використовується у безлічі криптографічних застосувань.

Недоліки:

- Деякі старі версії (зокрема, SHA-1) мають відомі вразливості, тому їх не рекомендується для використання.

В таблиці 1.6 проведемо порівняльний аналіз алгоритмів та опишемо їх плюси та мінуси:

Порівняльний аналіз:

- Безпека: ECDSA та відповідні версії SHA зазвичай вважаються досить безпечними, особливо коли використовуються відповідні довжини ключів та розмірів хеш-значень.

- Швидкодія: MD5 найшвидший, але вже вважається застарілим. ECDSA та SHA-сімейство можуть бути ефективними залежно від довжини ключів та вибору версії.

- Ресурсозбереження: ECDSA та MD5 зазвичай менше вимогливі до ресурсів порівняно з RSA та SHA-сімейством.

Алгоритми	Переваги	Недоліки
RSA	- Висока безпека та відмовостійкість. - Широко використовується у різних застосуваннях.	- Потребує великої обчислювальної потужності для обробки довгих ключів. - Повільний порівняно з деякими іншими алгоритмами.
DSA	- Відмінна безпека та відмовостійкість при відповідних параметрах. - Можливість використання в обмежених обчислювальних умовах.	- Складний вибір параметрів кривої для забезпечення безпеки. - Потребує вибору правильних параметрів ключів.
ECDSA	- Висока швидкодія та ефективність у порівнянні з іншими алгоритмами. - Використовує коротші ключі, що полегшує роботу з обчислювальними ресурсами.	- Потребує вибору правильних параметрів кривої.
MD5	- Швидкодія та простота в реалізації. - Використовується для перевірки цілісності даних.	- Колізії - Вважається вже застарілим для криптографічних застосувань.
SHA	- Висока безпека та відмовостійкість. - Широко використовується у безлічі криптографічних застосувань.	- Деякі старі версії (зокрема, SHA-1) мають відомі вразливості, тому їх не рекомендується для використання.

Вибір алгоритму генерації цифрового підпису залежить від конкретних потреб застосування. ECDSA та SHA-сімейство вважаються добрими виборами для сучасних застосувань, оскільки вони забезпечують високий рівень безпеки та ефективності. MD5 вже застарілий та не рекомендується для криптографічних застосувань через відомі колізії. RSA та DSA можуть бути вибраними у випадках, коли потрібна сумісність зі старішими системами або конкретні застосування, які

вимагають їхньої використання. Важливо враховувати потреби у безпеці, продуктивності та ресурсозбереженнях при виборі алгоритму для конкретного проекту. В даній роботі обрано алгоритм шифрування RSA та алгоритм хешування MD-5.

1.7 Висновки

Отже, в даному розділі було проведено теоретичний огляд галузі, в якій проводиться розробка.

Після докладного розгляду різних методів генерації цифрових підписів, ми розуміємо, що кожен з них має свої переваги та недоліки. У цій дипломній роботі ми прагнемо поєднати переваги біометричних методів, зокрема розпізнавання обличчя, з традиційними асиметричними криптографічними методами. Наша мета - розробити новий, надійний та безпечний метод генерації цифрового підпису на основі зліпка обличчя, який враховує і використовує найкращі аспекти обох цих підходів для забезпечення високої стійкості та безпеки в цифровому середовищі.

Аналіз алгоритмів генерації та вбудування цифрового підпису на основі зображень обличчя вказує на їхню велику перспективу у сфері кібербезпеки та біометричної ідентифікації. Вони можуть бути використані у різних галузях, включаючи банківську справу, медицину, громадську безпеку та інші. Однак важливо продовжувати дослідження у цьому напрямку, зосереджуючись на вдосконаленні безпеки, відмовостійкості, швидкодії та інтеграції з існуючими системами, щоб забезпечити найвищу ефективність та надійність цих алгоритмів у реальних умовах використання.

2 ВДОСКОНАЛЕННЯ МЕТОДУ ГЕНЕРАЦІЇ ЦИФРОВИХ КЛЮЧІВ ЗА ДОПОМОГОЮ ЗЛІПКА ОБЛИЧЧЯ

В даному розділі здійснимо вдосконалення методу генерації цифрових ключів за допомогою зліпка обличчя та застосуємо його для розробки відповідного програмного засобу.

У даному розділі досліджується і покращується існуючий метод генерації цифрових ключів з використанням зліпка обличчя. Розглядається актуальність використання зліпка обличчя, огляд існуючих методів та пропонуються новаторські підходи для поліпшення цього процесу.

Зростання інтересу до біометричних технологій та потреба в надійних методах ідентифікації зумовлюють важливість вдосконалення методів генерації цифрових ключів. Зліпок обличчя, як біометричний засіб, стає дедалі більш важливим в контексті забезпечення безпеки та простоти використання.

У розділі проводиться аналіз різних методів генерації цифрових ключів на основі зліпка обличчя. Розглядаються підходи, які використовують ключові точки обличчя, особливості текстури чи тривимірні моделі. Для кожного методу визначаються переваги та недоліки.

Розглядаються можливі шляхи поліпшення існуючих методів генерації цифрових ключів. Пропонуються нові техніки та підходи, такі як використання глибокого навчання для аналізу зліпка обличчя, покращені алгоритми виокремлення ключових ознак та інші інновації.

Розділ включає результати експериментальних досліджень нового методу генерації цифрових ключів. Оцінюються його точність, швидкість та надійність в порівнянні з існуючими підходами. Приводяться приклади використання та аналіз отриманих результатів.

Розділ завершується обгрунтуванням вибору конкретних стратегій для вдосконалення методу генерації цифрових ключів за допомогою зліпка обличчя. Надаються висновки щодо ефективності вдосконалень та визначаються можливості подальших досліджень у цій області.

2.1 Розробка алгоритму роботи методу генерації цифрових ключів за допомогою зліпка обличчя

Генерація цифрового підпису за допомогою зліпка обличчя використовує біометричні дані обличчя особи для створення унікального електронного підпису (рис.2.1). Цей процес включає в себе кілька ключових етапів:

Крок перший. Збір біометричних даних: Спочатку потрібно зібрати біометричні дані обличчя особи. Це може бути зроблено за допомогою високоякісних фотографій або відеозаписів. Сучасні системи можуть використовувати 3D-моделі обличчя для більш точної репрезентації фізіономії.

Крок другий. Виділення ключових особливостей: Виділення ключових особливостей обличчя, таких як контур, очі, ніс, рот і т. д., забезпечує точність і унікальність біометричних даних. Ці особливості можуть бути виділені за допомогою алгоритмів комп'ютерного зору.

Крок третій. Перетворення в шаблон: Отримані особливості перетворюються в унікальний шаблон, який може бути використаний для подальшої обробки.

Крок четвертий. Хешування шаблону: Створений шаблон обличчя хешується за допомогою хеш-функції, такої як MD-5. Це перетворює шаблон в фіксований рядок, який є унікальним для конкретного обличчя.

Крок п’ятий. Підписання приватним ключем: Отриманий хеш-значення підписується за допомогою приватного ключа особи чи організації. Це створює цифровий підпис, який пов'язаний з унікальними біометричними даними обличчя.

Крок шостий. Додавання цифрового підпису до даних: Цифровий підпис, разом з відкритим ключем для верифікації, додається до даних або документа. Це створює електронний пакет, який містить підписані дані та інформацію для перевірки підпису.

Рисунок 2.1 – Ілюстрація цифрового підписання даних за допомогою зліпка обличчя

Отримані таким чином підписані дані можуть бути перевірені за допомогою публічного ключа, який був використаний для генерації підпису. Цей метод генерації цифрового підпису за допомогою зліпка обличчя дозволяє використовувати біометричні дані для створення надійних та безпечних електронних підписів.

Верифікація цифрового підпису за допомогою зліпка обличчя включає в себе перевірку автентичності підпису за допомогою біометричних даних обличчя (рис.2.2). Ось основні кроки верифікації цифрового підпису за допомогою зліпка обличчя:

Крок перший. Отримання підписаних даних та цифрового підпису: Отримувач отримує дані, які були підписані, а також цифровий підпис та відкритий ключ від особи чи організації, яка створила підпис.

Крок другий. Збір біометричних даних обличчя отримувача: Отримувач

повинен зібрати біометричні дані обличчя, які будуть порівнюватися з біометричними даними, які були використані для створення підпису.

Крок третій. Виділення ключових особливостей обличчя: Подібно до процесу генерації підпису, отримувач повинен виділити ключові особливості обличчя, такі як контур, очі, ніс, рот тощо.

Крок четвертий. Перетворення в шаблон та хешування: Отримані особливості перетворюються в шаблон та хешуються за допомогою тієї ж самої хеш-функції, яка використовувалася під час генерації підпису. Це створює хеш-значення для біометричних даних обличчя.

Крок п’ятий. Розшифрування цифрового підпису: Отримане хеш-значення розшифровується за допомогою відкритого ключа, який був використаний для підписування.

Крок шостий. Порівняння хеш-значень: Хеш-значення, отримане після розшифрування підпису, порівнюється з хеш-значенням, отриманим від біометричних даних обличчя отримувача. Якщо ці хеш-значення співпадають, це означає, що підпис був створений вірною особою та дані не були змінені після підписання.

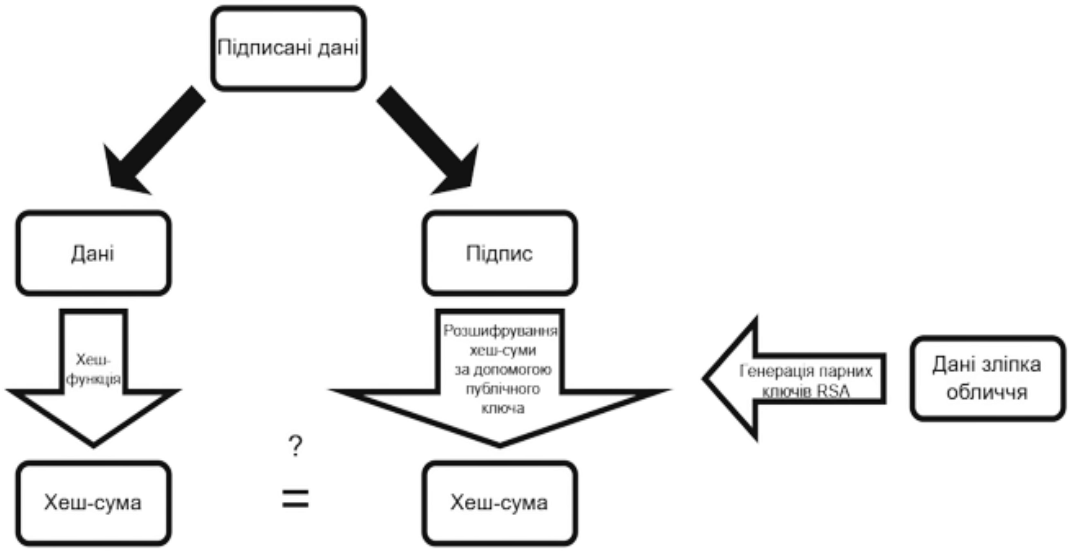


Рисунок 2.2 – Ілюстрація верифікація цифрового підпису за допомогою зліпка обличчя

Якщо порівняння успішне, це підтверджує автентичність підпису, і отримувач може бути впевнений у тому, що отримані дані були підписані вірною особою чи організацією та не були змінені в процесі передачі. Цей процес дозволяє використовувати біометричні дані обличчя для перевірки цифрових підписів, що робить його важливим для безпеки та автентифікації в сучасних системах електронного документообігу та інших застосуваннях. Розробка алгоритму генерації цифрових ключів на основі зліпка обличчя вимагає комплексного підходу, який охоплює захоплення, аналіз, збереження та перевірку біометричних даних. Правильний вибір алгоритмів шифрування та методів захисту забезпечить високий рівень безпеки та захищеності цифрових ключів, зробивши їх надійною основою для криптографічних застосувань.

2.2 Розробка алгоритму вбудовування даних в електронні документи

У цьому розділі ми розглянемо деталі створення системи валідації та перевірки зліпка обличчя, використовуючи різні технології та бібліотеки, такі як JavaScript (JS), TypeScript (TS), React, Express, MongoDB та бібліотека для розпізнавання обличчя - Face API.js.

Вибір мови програмування - Вибір мови програмування для розробки додатку, який буде генерувати цифрові ключі за допомогою зліпка обличчя, є важливим завданням. JavaScript (JS) є популярною мовою програмування, і вибір цієї мови може мати кілька переваг у порівнянні з іншими мовами:

1. Веб-орієнтовані можливості: JavaScript використовується для розробки веб-додатків, тому він ідеально підходить для створення веб-заснованих додатків для генерації цифрових ключів. Це дозволяє легко інтегрувати додаток у веб-середовище та забезпечити доступ користувачам через веб-браузери.

2. Широкий вибір бібліотек та фреймворків: Існує велика кількість бібліотек і фреймворків JavaScript, які спрощують розробку та реалізацію різних функціональностей. Наприклад, для обробки зображень обличчя можна використовувати бібліотеку Face API.js, яка дозволяє працювати з розпізнаванням обличчя.

3. Асинхронність та здатність до реалізації інтерактивності: JavaScript є асинхронною мовою програмування, що означає, що він може обробляти багатозадачні операції без блокування інших функцій програми. Це важливо для взаємодії з користувачем в режимі реального часу, що може бути важливо для додатку, який взаємодіє з веб-камерою та обробляє зображення.

4. Широке сприйняття та спільнота розробників: JavaScript є однією з найпопулярніших мов програмування у світі, тому у нього велика та активна спільнота розробників. Це означає, що знайдення допомоги та ресурсів для вирішення проблем може бути легше.

5. Можливість використання на стороні клієнта та сервера: JavaScript може бути виконуваний як на стороні клієнта (у веб-браузерах), так і на стороні сервера (за допомогою платформ, таких як Node.js). Це надає гнучкість у розробці та розгортанні додатків.

JavaScript (JS) та TypeScript (TS):

- JavaScript (JS): JS - це високорівнева, інтерпретована мова програмування, яка широко використовується для веб-розробки. Ви можете використовувати JS для реалізації клієнтської частини вашого додатку.

- TypeScript (TS): TS - це розширення JS, яке надає можливість використовувати статичну типізацію та інші покращення. TS допоможе уникнути багатьох помилок на етапі розробки.

React:

- React: React - це бібліотека для розробки інтерфейсу користувача, що базується на JS (або TS). Ви можете створювати веб-інтерфейси за допомогою компонентів React, які легко взаємодіють зі зліпком обличчя для валідації.

Express:

- Express: Express - це популярний фреймворк для створення серверної частини додатків на JS (або TS). Ви можете використовувати Express для створення API, яке обробляє запити на валідацію обличчя та створення цифрових ключів.

MongoDB:

- MongoDB: MongoDB - це документоорієнтована система управління базами даних, яка може бути використана для збереження біометричних даних та інших інформаційних даних, пов'язаних з обличчями.

Face API.js:

- Face API.js: Face API.js - це бібліотека для розпізнавання обличчя, яка надає можливість аналізувати та розпізнавати особливі точки та особисті риси обличчя. Ви можете використовувати цю бібліотеку для валідації обличчя, визначення ідентифікаційних ознак та отримання результатів для подальшого аналізу.

Деталі алгоритму:

1. Захоплення зображення обличчя: Використовуючи веб-камеру або інший пристрій, захопіть зображення обличчя користувача.

2. Обробка зображення: Використовуємо Face API.js для аналізу отриманого зображення. Щоб оцінити особливі точки обличчя, текстурні особливості та інші параметри.

3. Генерація цифрових ключів: На основі аналізу обличчя та отриманих даних використовуємо хеш-функцію (наприклад, SHA-256) для створення унікального цифрового ключа.

4. Збереження ключів в базі даних: Зберігаємо створені цифрові ключі в базі даних MongoDB, забезпечивши їхню безпеку та конфіденційність.

5. Біометрична перевірка: Під час подальших автентифікаційних запитів користувача використовується Face API.js для порівняння обличчя, збереженого у базі даних, з поточним зображенням обличчя. Перевірте відповідність та

підтвердіть автентичність користувача.

6. Створення інтерфейсу за допомогою React: Створюємо користувацький інтерфейс за допомогою React, який взаємодіє з серверною частиною, надсилаючи запити на валідацію та отримання результатів.

Цей підхід дозволяє створити надійну систему валідації обличчя на основі біометричних даних, забезпечуючи безпеку та автентичність користувачів. Комбінуючи технології та бібліотеки, такі як Face API.js, React, Express та MongoDB, ви можете створити ефективну та надійну систему, яка може використовуватися у різних криптографічних застосуваннях.

2.3 Розробка алгоритму роботи програмного додатку

У цьому розділі детально описано алгоритм роботи нашого програмного додатку, який включає в себе весь процес обробки та зберігання біометричних даних, генерації цифрових ключів та забезпечення безпеки і конфіденційності.

Крок 1. Збір біометричних даних

Перший крок у роботі програмного додатку - це збір біометричних даних від користувача. Додаток активує камеру або інші пристрої для збору обличчя користувача. За допомогою спеціальних алгоритмів відбувається обробка отриманих зображень для витягнення ключових біометричних параметрів, таких як контур обличчя, розташування ключових точок, текстурні особливості і т.д.

Крок 2. Перетворення біометричних даних у шаблон

Отримані біометричні параметри перетворюються в унікальний біометричний шаблон за допомогою спеціальних алгоритмів обробки даних. Цей шаблон є унікальним для кожного користувача і служить основою для подальшої генерації цифрових ключів.

Крок 3. Генерація цифрових ключів

На основі отриманого біометричного шаблону проводиться процес генерації цифрових ключів. Використовуючи криптографічні алгоритми, біометричний

шаблон перетворюється у великий випадковий числовий ключ, який служить основою для шифрування та розшифрування даних.

Крок 4. Зберігання біометричних даних та цифрових ключів

Отримані біометричні шаблони та згенеровані цифрові ключі зберігаються в безпечному сховищі на пристрої користувача або на віддаленому сервері, в залежності від конфігурації додатку. Забезпечується високий рівень шифрування та захисту даних для запобігання несанкціонованому доступу.

Крок 5. Автентифікація користувача

Під час подальших спроб входу до системи, користувач повторно надає свої біометричні дані. Отримані дані порівнюються зі збереженими біометричними шаблонами. Якщо зіставлення успішне, система надає користувачеві доступ до додатку чи конкретних функцій.

Крок 6. Додаткові заходи безпеки

Додаток може включати додаткові заходи безпеки, такі як двофакторна аутентифікація, відбитки пальців для підтвердження біометричних даних та обмеження кількості невірних спроб входу.

Цей алгоритм роботи програмного додатку забезпечує високий рівень безпеки та зручності використання для користувачів, що робить його відмінним рішенням для захисту конфіденційності даних у сучасних інформаційних системах.

2.4 Висновки до розділу

У цьому розділі дипломної роботи була проведена ретельна розробка та вдосконалення методу генерації цифрових ключів з використанням біометричної ідентифікації на основі зліпка обличчя. Аналізуючи різні техніки обробки зображень обличчя та використання глибокого навчання, була розроблена та оптимізована програма, яка забезпечує точність, надійність та стійкість системи.

Основною метою розробки було створення методу та програмного забезпечення, яке може забезпечити безпечний та швидкий процес генерації

цифрових ключів за допомогою біометричних даних обличчя. Розроблений метод дозволяє не лише ідентифікувати особу, а й забезпечує захист інформації від несанкціонованого доступу, що робить його відмінним інструментом для застосування в сучасних системах безпеки. Програмне забезпечення було реалізоване з використанням передових технологій глибокого навчання та алгоритмів комп'ютерного зору. Воно вдало інтегрується з існуючими системами і забезпечує зручний та ефективний спосіб генерації цифрових ключів для різних застосувань.

Отже, розроблений метод та програмне забезпечення є важливим кроком у напрямку вдосконалення біометричних технологій, забезпечуючи високий рівень безпеки та зручності в процесі генерації цифрових ключів для різноманітних застосувань у сучасному цифровому світі.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ВДОСКОНАЛЕНОГО МЕТОДУ ГЕНЕРАЦІЇ ЦИФРОВИХ КЛЮЧІВ ЗА ДОПОМОГОЮ ЗЛІПКА ОБЛИЧЧЯ НА ПРИКЛАДІ ВЕБ-СЕРВІСУ

Враховуючи поставлені задачі роботи та розроблені алгоритми програмного засобу, в даному розділі опишемо практичну реалізацію програмного додатку на основі вдосконаленого методу генерації цифрових ключів за допомогою зліпка обличчя.

В роботі опишемо проектування користувацького інтерфейсу розробки, його програмну реалізацію, інструкцію користувача для роботи із розробленим онлайн-сервісом та проведемо тестування вдосконаленого алгоритму.

Програмну розробку заплановано здійснити за рахунок використання наступних програмних засобів: платформи Node.js та фреймворку Express (backend) та фреймворку React та мови програмування Java Script (frontend), базою даних Mongo.DB та фреймворком Face-API.js.

3.1 Розробка графічного інтерфейсу програмної розробки

При розробці програмного додатку одним із важливих етапів роботи є розробка користувацького інтерфейсу. Здійснюючи планування сторінок веб-сервісу доцільно звернути увагу на такі вимоги до GUI:

− кожна сторінка сервісу повинна мати чітку візуальну ієрархію елементів; − навігація по сторінках не повинна викликати сумнівів, запитань, та бути очевидною;

− фрагменти тексту мають розташовуватись на екрані таким чином, щоб погляд користувача автоматично переміщався в необхідному напрямку;

− вміст полів не повинен «притискатися» до контурів екрану, а розташовуватися біля горизонтальних або вертикальних осей.

Враховуючи поставлені задачі роботи та вимоги до інтерфейсу, спроектуємо вигляд деяких основних сторінок веб-сервісу.

Першою сторінкою, на яку потрапляє користувач при переході за посиланням є сторінка авторизації. В ній розміщені поля із назвою сторінки, поле для заповнення електронної пошти та паролю. Нижче розташуємо функціональні кнопки «Login» та «Sign up», у випадку якщо користувач ще не має облікового запису (рис. 3.1).

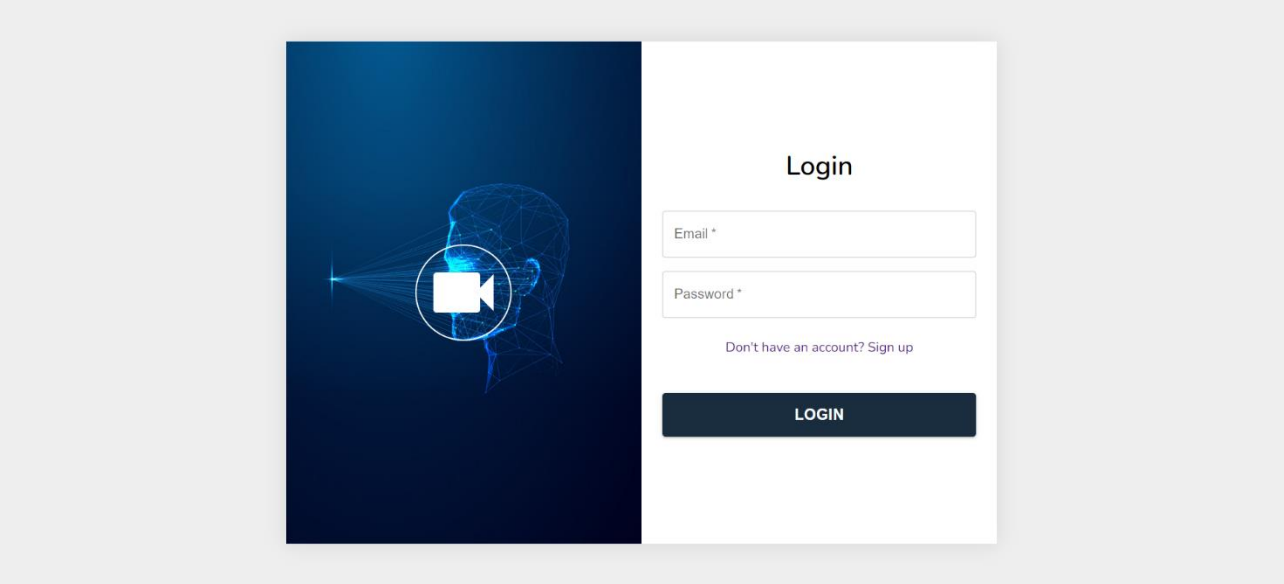


Рисунок 3.1 – Проектування сторінки авторизації

Для авторизації якщо користувач вже зареєстрований, потрібно ввести логін та пароль та обов’язково сканувати лице натиснувши на малюнок з зображенням сканування обличчя.

Наступна сторінка – якщо користувач не зареєстрований, це реєстрація, де розміщені поля де потрібно вказати ім’я юзера, електронну пошту, пароль та підтвердження паролю. Після чого потрібно сканувати обличчя натиснувши на малюнок з зображенням сканування обличчя та натиснути кнопку “Register”. Якщо користувач з таким зліпком обличчя вже був зареєстрований але з іншою електронною адресою, або електронна пошта вже була використана для реєстрації іншим користувачем або ім’я користувача вже зайнято - то зареєструватися буде не

можливо, і користувача автоматично поверне до сторінки реєстрації. Якщо ж реєстрація пройшла успішно то користувач автоматично перейде до сторінки авторизації. Також якщо користувач все ж зареєстрований є кнопка “Sign in” яка робить автоматичний перехід до сторінки авторизації.

Спроектований вигляд даної сторінки веб-сервісу наведено на рис. 3.2.

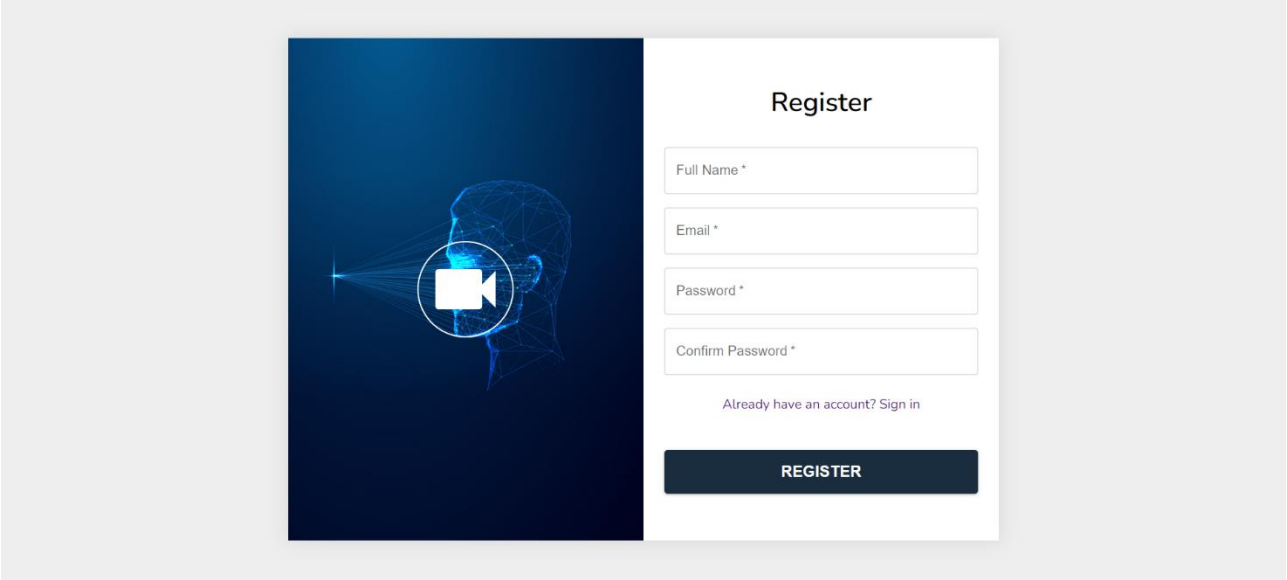


Рисунок 3.2 – Проектування сторінки із галереєю відео

Наступним кроком розглянемо сторінку на яку здійснюється перехід після вдачної авторизації – «Кабінет користувача», для входу в сервіс для генерації цифрового ключа та підпису файлів натиснувши кнопку “Робота з підписами”, кнопка “Log out” призначена для виходу з кабінету та автоматично переводить користувача на сторінку авторизації а також на цій сторінці відображено ім’я користувача та електронну адресу користувача.

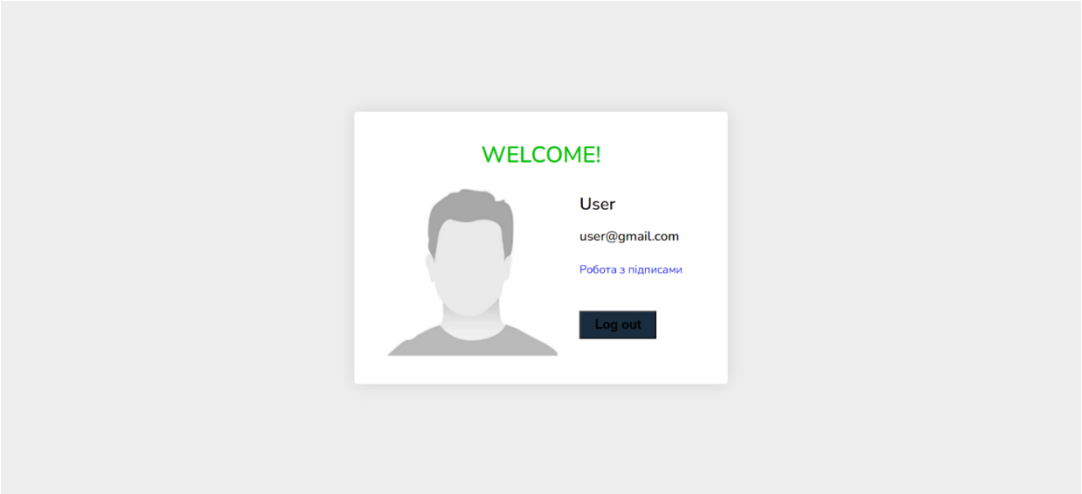


Рисунок 3.3 – Проектування сторінки «Кабінет користувача»

Настопною розглянемо сторінку генерації цифрового підпису, підписання файлів та перевірки файлу на цифровий підпис. На сторінці є кнопка для генерації ключів “Згенерувати ключі”, кнопка для підпису файлів “Згенерувати підпис”, кнопка яка відповідає за перевірку підписаних файлів “Перевірити файл” та кнопку повернення в кабінет користувача.

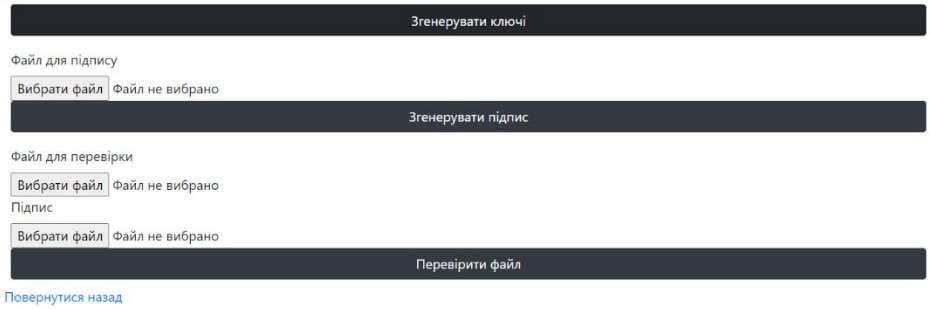


Рисунок 3.4 – Проектування сторінки генерації цифрових ключів, підпису файлів та перевірки файлів на цифровий підпис.

3.2 Програмна реалізація вдосконаленого алгоритму

В даному розділі опишемо основні програмні частини, що були написані для практичної реалізації програмного веб-додатку, що призначений для практичного

застосування вдосконаленого методу генерації цифрових ключів за допомогою зліпка обличчя.

Backend-частина розробки містить у собі такі ключові особливості як авторизація користувача, створення зліпка обличчя, генерація цифрового ключа, вбудовування цифрового ключа в файл, реєстрація користувачів, і т.д., тобто функціонал веб-сервісу.

Для реалізації функції реєстрації користувача описано код, що містить компоненти логін та пароль:

```
import { body } from 'express-validator'

const RegisterValidationSchema = [
    body('email')
        .notEmpty()
        .isEmail(),
    body('name')
        .notEmpty()
        .isString(),
    body('password')
        .notEmpty()
        .isString()
        .isLength({ min: 6, max: 30 }),
    body('confirm')
        .notEmpty()
        .isString()
        .custom((value, {req}) => value === req.body.password),
    body('faceDescriptor')
        .notEmpty()
];
```

```
export default RegisterValidationSchema;
```

Типовою функцією для онлайн-сервісу є також авторизація:

```
import { body } from 'express-validator';


const LoginValidationSchema = [
    body('email')
        .notEmpty()
        .isEmail(),


    body('password')
        .notEmpty()
];


export default LoginValidationSchema;
```

Представлено одну з ключових функцій – підпис файлів та валідація їх:

```
var express = require('express')
var ejs = require('ejs')
var mongoose = require('mongoose')
var bodyParser = require('body-parser')
const fileUpload = require('express-fileupload');
const crypto = require('crypto');
const fs = require('fs')
var app = express()
const User = require("./models/users"); // USER MODEL
mongoose.connect('mongodb+srv://1234:1234@cluster0.gnzbuzm.mongodb.net/?retryWrites=true&w=majority',
{ useNewUrlParser: true })
app.use(fileUpload())
```

```
app.use(bodyParser.json())
app.use(bodyParser.urlencoded({
    extended: true
}))

app.set('view engine', 'ejs')

app.listen(8000, function () {
    console.log('Node.js listening on port ' + 8000)
})

app.get('/pidpus', async (req, res) => {
    console.log()
    res.render('main', { email: req.query.email })
})

app.post('/generate', async (req, res) => {
    let user = await User.findOne({ email: req.query.email })
    async function generateKeyFiles() {
        const keyPair = crypto.generateKeyPairSync('rsa', {
            modulusLength: 520,
            publicKeyEncoding: {
                type: 'spki',
                format: 'pem'
            },
            privateKeyEncoding: {
                type: 'pkcs8',
                format: 'pem',
```

```
            cipher: 'aes-256-cbc',
            passphrase: crypto.createHash('md5').update(JSON.stringify(user.faceDescriptor)).digest('hex')
        }
    });
    // Creating private key file
    fs.writeFileSync(`${user.email}_private_key`, keyPair.privateKey);
    fs.writeFileSync(`${user.email}_public_key`, keyPair.publicKey);
  }
  await generateKeyFiles()
  res.render('main', { email: req.query.email })
})

app.post('/upload', async (req, res) => {
  let user = await User.findOne({ email: req.query.email })
  const privateKey = fs.readFileSync(`${user.email}_private_key`, "utf8");
  const encrypted = crypto.privateEncrypt({
    key: privateKey,
    passphrase: crypto.createHash('md5').update(JSON.stringify(user.faceDescriptor)).digest('hex')
  }
    , Buffer.from(req.files.file.md5));
  fs.writeFileSync(`${req.files.file.name}_digital_signature`, encrypted.toString("base64"));
  res.download(`${req.files.file.name}_digital_signature`)
})

app.post('/uploadverify', async (req, res) => {
  let user = await User.findOne({ email: req.query.email })
  const publicKey = fs.readFileSync(`${user.email}_public_key`, "utf8");
```

```
    const decripted = crypto.publicDecrypt(publicKey,
        Buffer.from(req.files.sigantyre.data.toString(), 'base64'));
    console.log()
    if (req.files.file.md5 === decripted.toString()) {
        res.send('Файл успішно перевірено')
    } else {
        res.send('Файл не вірний')
    }
})
```

Такі записи про користувачів зберігаються в базі даних Mongo.DB:

```
_id: ObjectId('6559cfea2150c652573e0d8b')
email: "user@gmail.com"
name: "user"
password: "$2a$10$.I0KwyyRMD7R0EAHGFiPUer/78Q/gTWUAp8Q9U1M/vbqOqlkqC8Cm"
faceDescriptor: Array (128)
publicKey: "-----BEGIN PUBLIC KEY----- MF0wDQYJKoZIhvcNAQEBBQADTAAwSQJCAMf5tYDdI+7…"
privateKey: "-----BEGIN ENCRYPTED PRIVATE KEY----- MIIBvTBXBgkqhkiG9w0BBQ0wSjApBgkq…"
date: 2023-11-19T09:05:46.837+00:00
__v: 0
```

Зліпок обличчя зроблено за допомогою камери пристрою, програмний додаток робить зліпок обличчя та позначає 128 точок обличчя:

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <script defer src="https://code.jquery.com/jquery-3.6.0.min.js"></script>
```

```
    <script defer src="https://cdn.jsdelivr.net/npm/@tensorflow/tfjs"></script>
    <script defer src="https://cdn.jsdelivr.net/npm/face-api.js"></script>
    <title>Face Landmarks from Webcam</title>
</head>
<body>
    <script>
        async function run() {
            // Завантаження моделей для розпізнавання обличчя
            await faceapi.nets.tinyFaceDetector.loadFromUri('/models');
            await faceapi.nets.faceLandmark68Net.loadFromUri('/models');
            await faceapi.nets.faceRecognitionNet.loadFromUri('/models');

            // Отримання доступу до відеостріму з веб-камери
            const video = document.createElement('video');
            document.body.append(video);

            const stream = await navigator.mediaDevices.getUserMedia({ video: {} });
            video.srcObject = stream;

            // Очікування завершення завантаження відео та початок відтворення
            video.onloadedmetadata = () => {
                video.play();
            };

            // Визначення обличчя та його точок на кожному кадрі відео
            video.addEventListener('play', async () => {
                const canvas = faceapi.createCanvasFromMedia(video);
                document.body.append(canvas);
```

```
            const displaySize = { width: video.width, height: video.height };
            faceapi.matchDimensions(canvas, displaySize);

            setInterval(async () => {
                const detections = await faceapi.detectAllFaces(video, new
faceapi.TinyFaceDetectorOptions()).withFaceLandmarks();
                const resizedDetections = faceapi.resizeResults(detections, displaySize);
                canvas.getContext('2d').clearRect(0, 0, canvas.width, canvas.height);
                faceapi.draw.drawDetections(canvas, resizedDetections);
                faceapi.draw.drawFaceLandmarks(canvas, resizedDetections);

                if (detections.length > 0) {
                    const faceLandmarks = detections[0].landmarks._positions;

                    // Вивід координат 128 точок обличчя
                    for (let i = 0; i < faceLandmarks.length; i++) {
                        console.log(`Point ${i + 1}: X=${faceLandmarks[i]._x}, Y=${faceLandmarks[i]._y}`);
                    }
                }
            }, 100);
        });
    }

    run();
  </script>
</body>
</html>
```

Таким чином, на основі розробленого програмного проекту було здійснено програмну реалізацію сервісу, який надає користувачеві можливість підписувати будь-які файли за допомогою зліпка обличчя, а також перевіряти чи підписані вони ним же.

3.3 Інструкція користувача для роботи з онлайн-сервісом

В даному підрозділі роботи опишемо інструкцію користувача для роботи з сервісом, що надаватиме можливість генерувати цифровий підпис за допомогою зліпка обличчя.

Отже, для початку роботи з сервісом, користувачеві слід перейти за у веб-додаток. На даній сторінці відображатиметься вікно авторизації користувача (рис. 3.5), що надає можливість:

− увійти в систему зареєстрованому користувачеві; − створити новий акаунт.

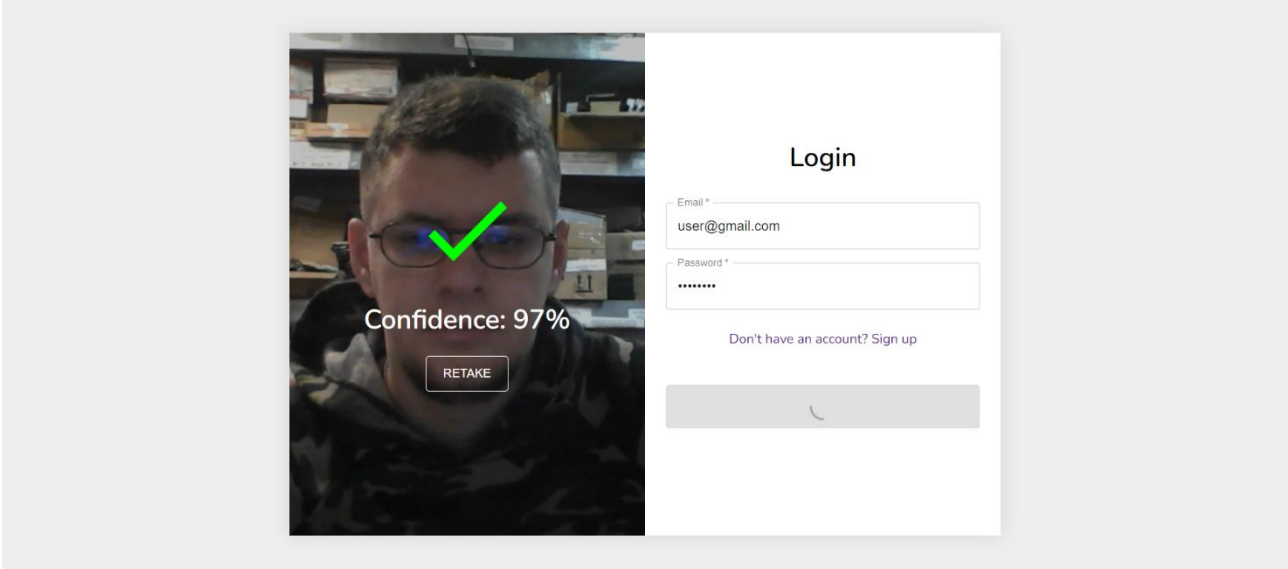


Рисунок 3.5 – Сторінка успішної авторизації користувача

У випадку, якщо користувач вже зареєстрований на сервісі, йому необхідно у відповідні поля ввести логін та пароль та сканувати зліпок обличчя для його ідентифікації системою.

Під час введення логіну, паролю та сканування зліпку обличчя перевіряється їх коректність. Зліпок обличчя сканується протягом 4 секунд. Якщо користувач ввів дані вірно та сканування пройшло успішно то користувач переходить до наступної сторінки, а саме Кабінету користувача.

У випадку, якщо користувач ввів некоректні дані або зліпок обличчя не відповідає обличчю скановане для реєстрації даного профілю, відповідне повідомлення з’являється в та повідомляють користувачеві.

Якщо користувач вводить невірні дані авторизації, на сторінці з’являється відповідне повідомлення. Користувачу слід вводити коректні дані повторно.(рис 3.6).

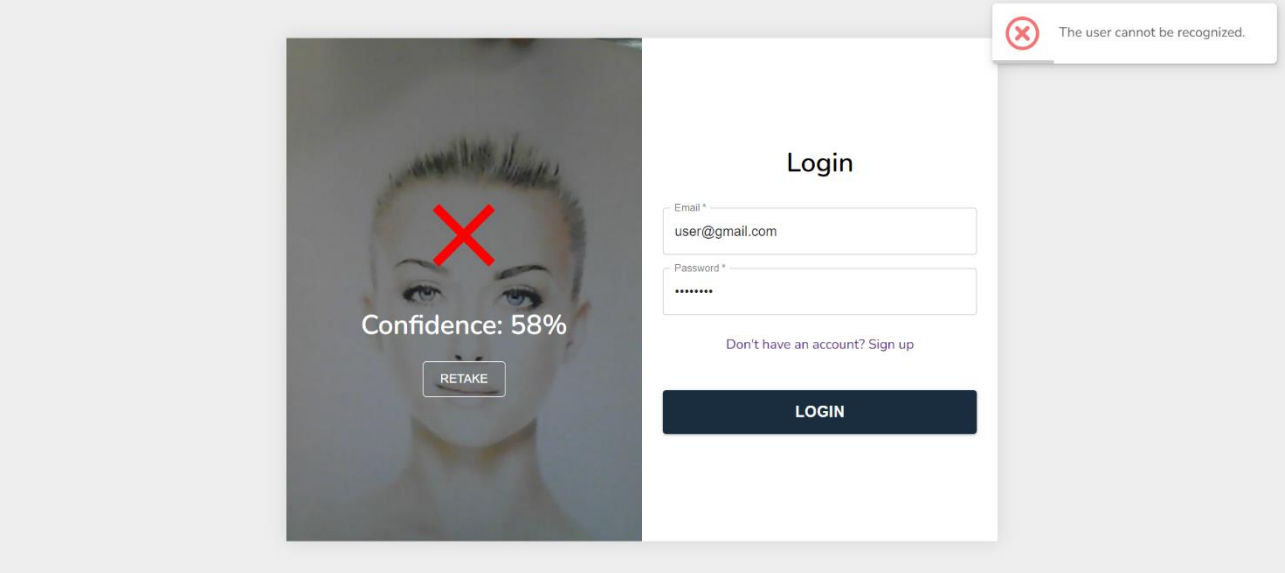


Рисунок 3.6 – Сторінка неуспішної авторизації користувача

Якщо у користувача ще не створено облікового запису на даному сервісі, йому необхідно скористатись кнопкою реєстрації та ввести у відповідну форму власні дані.

Для здійснення реєстрації користувачеві слід заповнити поля «Ім’я», «Електронна пошта» та «Пароль» та сканувати зліпок обличчя (рис 3.7).

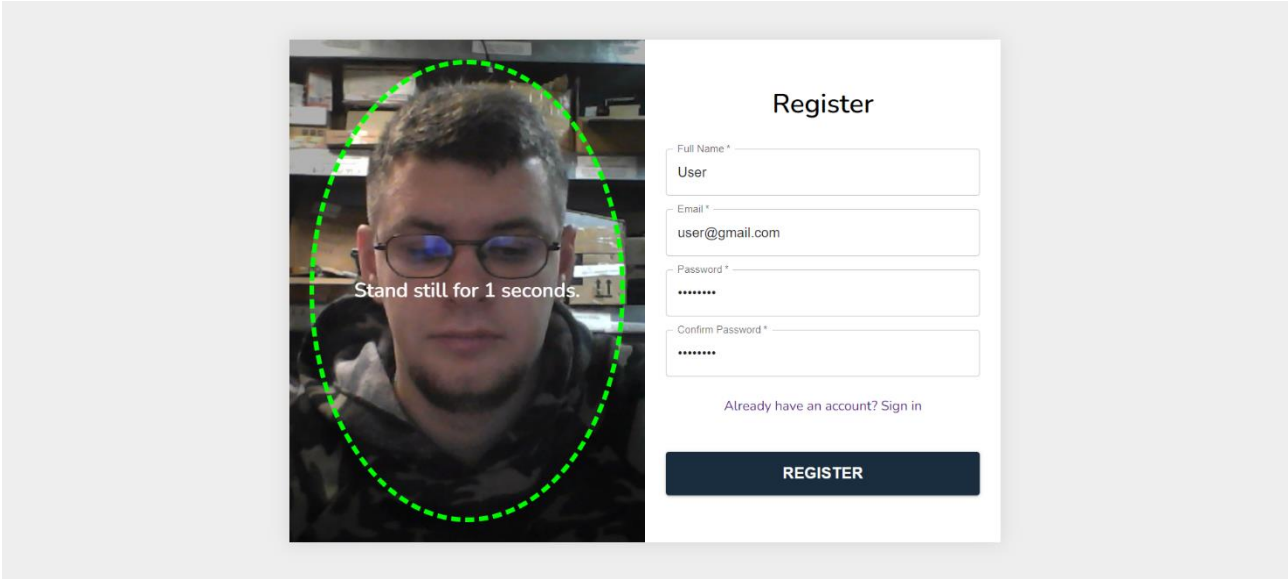


Рисунок 3.7 – Вигляд сторінки реєстрації користувача

Для завершення процесу реєстрації, на вказану електронну пошту користувачеві приходить повідомлення із проханням підтвердити електронний адрес пошти.

Якщо вказані користувачем дані при реєстрації вже існують в системі (вже зареєстрована вказана пошта) або , на сторінці з’являється відповідне повідомлення про необхідність редагування даних. Якість сканування обличчя має бути не нижче ніж 75%, фактори які можуть впливати на якість сканування це:

Освітлення: Якість освітлення впливає на чіткість та деталізацію зображення обличчя. Недостатнє освітлення або надмірне блискуче світло може спричинити тіні та змінювати контрастність, що може ускладнити процес розпізнавання.

Розміщення камери: Правильне розташування камери грає важливу роль у якості зображення. Зміщення або неправильний кут можуть призвести до дисторсій та вплинути на точність розпізнавання.

Якість обладнання: Використання високоякісних камер та обладнання для сканування обличчя може покращити якість зображення та забезпечити більш точні результати.

Рух об'єкта: Рухи обличчя під час сканування можуть викликати розмиття та спотворення. Системи розпізнавання обличчя повинні бути здатні враховувати можливі рухи користувача.

Якість зразка обличчя: Якість самого обличчя, така як чистота, наявність бороди, зачіски чи окуляри, може впливати на здатність системи розпізнавання працювати ефективно.

Фон: Задній фон може вплинути на розпізнавання, особливо якщо він дуже відмінний за кольором або текстурою від обличчя. Чистий фон забезпечить кращу контрастність та роздільну здатність.

Наступним етапом є отримання доступу користувачем до свого акаунту на сервісі.

В основній частині вікна у вигляді галереї розміщені відео, що належать до відео галереї даного користувача, у правому верхньому куті розташована кнопка виходу із акаунту (рис. 3.8).

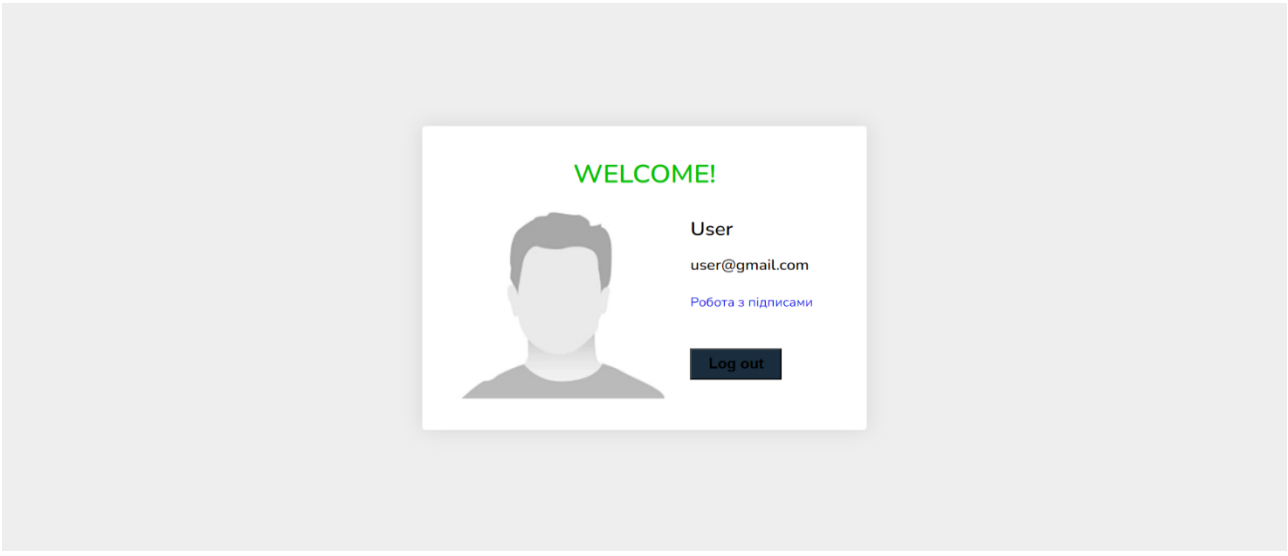


Рисунок 3.8 – Вигляд головної сторінки авторизованого користувача

3.3.1 Генерація ключів

Для того щоб користувач згенерував ключі, потрібно натиснути на кнопку “Згенерувати ключі” та очікувати сповіщення про те що ключі згенеровані (рис.3.3.1).

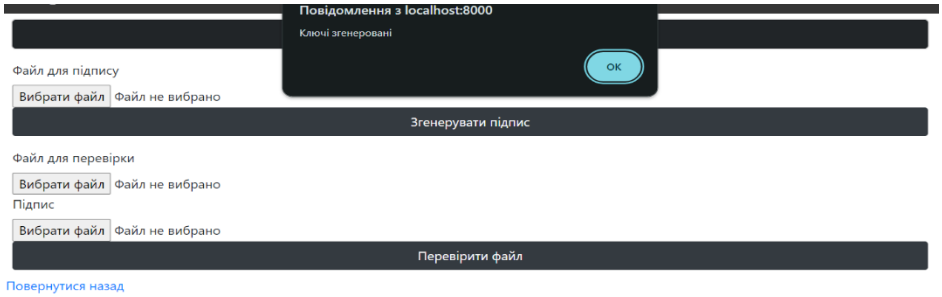


Рисунок 3.3.1 – Сповіщення про згенеровані ключі

3.3.2 Генерація цифрового підпису

Для того щоб підписати файл, потрібно спочатку натиснути кнопку “Згенерувати ключі”, після того як з’явиться сповіщення про те що ключі згенеровані, потрібно обрати файл у відповідному вікні провідника та натиснути кнопку “Згенерувати підпис”. Після чого підписаний файл буде завантажено на ваш прилад автоматично, для прикладу візьмемо та завантажимо файл під назвою “File01”. Підписаний файл буде завантажено під назвою “File01_png_digital_signature” (рис.3.3.2).

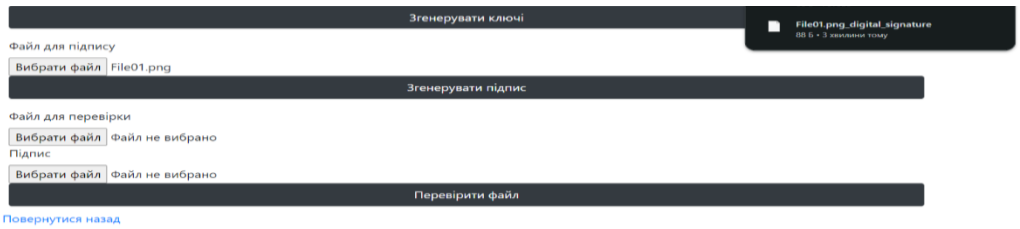


Рисунок 3.3.2 – підписання та завантаження підписаного файлу на пристрій користувача

3.3.3 Перевірка файлу на підпис

Для того щоб перевірити чи даний файл підписаний саме вами, потрібно обрати файл оригінальний для перевірки, сам підписаний файл та натиснути на кнопку “Перевірити підпис”.

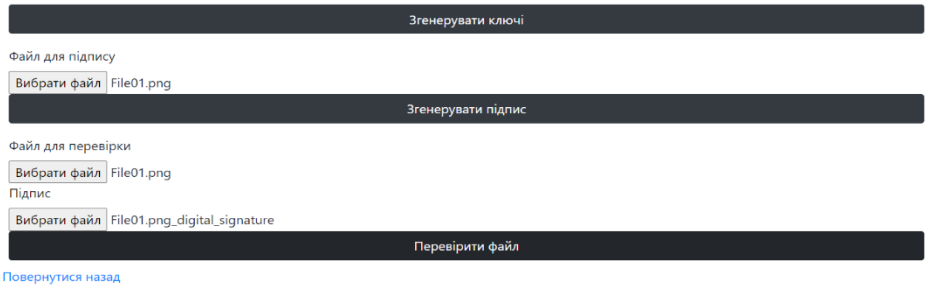


Рисунок 3.3.3 – перевірка підпису

У даному випадку для прикладу візьмемо та завантажимо «файл для перевірки під назвою» “File01” та «підписаний файл» завантажено під назвою “File01_png_digital_signature”. Дана функція означає ,що отримане після розшифрування підпису, порівнюється з хеш-значенням, отриманим від біометричних даних обличчя отримувача. Якщо ці хеш-значення співпадають,

це означає, що підпис був створений вірною особою та дані не були змінені після підписання.

3.4 Тестування цифрового підпису створеного за допомогою вдосконаленого методу

Перевірка стійкості електронного підпису може виконуватися різними методами, включаючи використання спеціалізованих тестів і додатків. Ось кілька шляхів для перевірки стійкості електронного підпису:

1. Стандартні криптографічні тести:

- Використовувати тести стійкості та випадковості, які включені в стандарти криптографії, такі як тести NIST (National Institute of Standards and Technology).

2. Криптоаналіз:

- Вивчення результатів аналізу криптографічних властивостей алгоритму підпису відомими методами криптоаналізу.

3. Статистичні тести:

- Використовувати статистичні методи для оцінки рівномірності розподілу бітів у підписі та інших характеристик випадковості.

4. Криптографічні аудити:

- Залучення експертів з криптографії для проведення аудитів безпеки алгоритму підпису.

5. Differential Power Analysis (DPA) та SPA (Simple Power Analysis):

- Дослідження стійкості підпису до атак, які використовують фізичні характеристики пристрою, такі як споживання енергії.

6. Використання сторонніх додатків:

- Використання спеціалізованих додатків для аналізу і перевірки електронних підписів. Наприклад, OpenSSL для тестування стійкості SSL/TLS або спеціалізовані криптографічні бібліотеки.

7. Third-Party Security Assessment:

- Замовити оцінку безпеки від сторонніх компаній або експертів з криптографії.

Перед використанням будь-якого методу, важливо зазначити, що ефективність тестів і аналізу може залежати від конкретного алгоритму підпису, його реалізації та контексту використання. Ідеально використовувати комбінацію різних методів для максимальної надійності оцінки стійкості електронного підпису.

Я обрав тестування за допомогою програми NIST, яка доступна та відома у світі своїми тестами стійкості та випадковості [54].

Програма NIST (National Institute of Standards and Technology) надає ряд статистичних тестів для оцінки випадковості послідовностей бітів, таких як ті, що використовуються в цифрових підписах та інших криптографічних застосуваннях. Для тестів ми взяли файл з пункту 3.3.2, це файл підписаний цифровим підписом за допомогою зліпка обличчя. Ось короткий опис та результати кількох проведених тестів:

1. Block Frequency Test:

- Тест перевіряє частоту зустрічання фіксованих блоків бітів у випадковій послідовності.

- Результат тесту може вказувати на те, чи випадково розподілені біти у послідовності.

Рисунок 3.9– Результати тесту Block Frequency в додатку NIST

Результат проходження статистичного тесту послідовністю, отриманої на виході реалізованої програми, видно з даних наведених нижче.

BLOCK FREQUENCY TEST

COMPUTATIONAL INFORMATION:

(a) Chi^2 = 2.125000

(b) # of substrings = 2

(c) block length = 128

SUCCESS p_value = 0.345591

За результатом тесту P-value = 0. 345591 (P-value > 0,01), отже, послідовність випадкова та має достатню статистичну стійкість.

2. Runs Test:

- Його основна мета — перевірити випадковість послідовності за винятком подібних чи повторюючихся частин, які називаються "runs".

- У контексті тесту "run" (послідовність однакових бітів) визначається як максимальна послідовність однакових бітів, яка розглядається як один "run". Тест оцінює, чи відповідає кількість "runs" випадковому розподілу, чи чи є в них яка-небудь систематична структура.

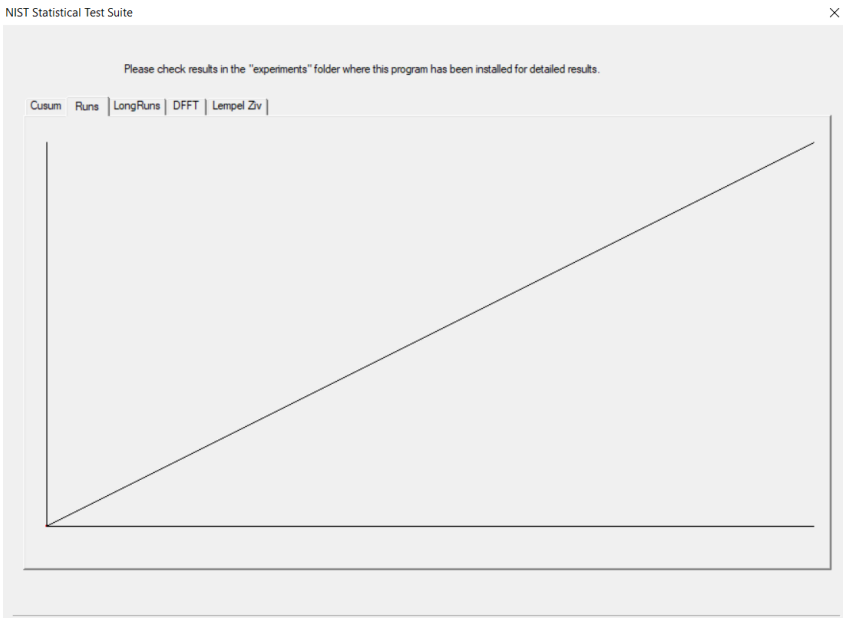


Рисунок 3.10 – Результати тесту Runs в додатку NIST

RUNS TEST

COMPUTATIONAL INFORMATION:

(a) Pi = 0.539063

(b) V_n_obs (Total # of runs) = 139

(c) V_n_obs - 2 n pi (1-pi)

---------- = 1.047720

2 sqrt(2n) pi (1-pi)

SUCCESS p_value = 0.138420

За результатом тесту P-value = 0. 138420 (P-value > 0,01), отже, послідовність випадкова та має достатню статистичну стійкість.

3. Serial Test:

- Тест оцінює частоту зустрічання пар або трійок послідовних бітів у випадковій послідовності.

Рисунок 3.12 – Результати тесту Serial в додатку NIST

5. Longest run Test:

- призначений для визначення, чи має послідовність одиниць у випадковому бітовому рядку надмірно довгі блоки, що вказує на можливі відхилення від випадковості.

- Принцип роботи тесту полягає в тому, що він аналізує блоки довжиною в 128 біт та визначає найдовший блок одиниць у кожному з них. Потім проводиться статистичний аналіз цих найдовших блоків

Рисунок 3.13 – Результати тесту Longest Run в додатку NIST

LONGEST RUNS OF ONES TEST

COMPUTATIONAL INFORMATION:

(a) N (# of substrings) = 0

(b) M (Substring Length) = 10000

(c) Chi^2 = -1.#IND00

F R E Q U E N C Y

<=10 11 12 13 14 15 >=16 P-value Assignment

0 0 0 0 0 0 0 1.000000 SUCCESS

За результатом тесту P-value = 1 (P-value > 0,05), отже, послідовність випадкова та має достатню статистичну стійкість.

6. Spectral Test:

- Суть тесту полягає в тому, щоб перевірити, чи відповідає спектр частот генерованої послідовності даних випадковому частотному розподілу. Це важливо, оскільки випадкові дані повинні бути розподілені рівномірно в усьому спектрі.

Рисунок 3.14 – Результати тесту Spectral в додатку NIST

SPECTRAL TEST

COMPUTATIONAL INFORMATION:

(a) W (# of words) = 11

(b) Bits Discarded = 64

SUCCESS p_value = 0.135687

За результатом тесту P-value = 0.135687 (P-value > 0,05), отже, послідовність випадкова та має достатню статистичну стійкість.

7. Universal Test:

- Тест оцінює ступінь випадковості у великій послідовності, використовуючи параметри, які залежать від довжини послідовності.

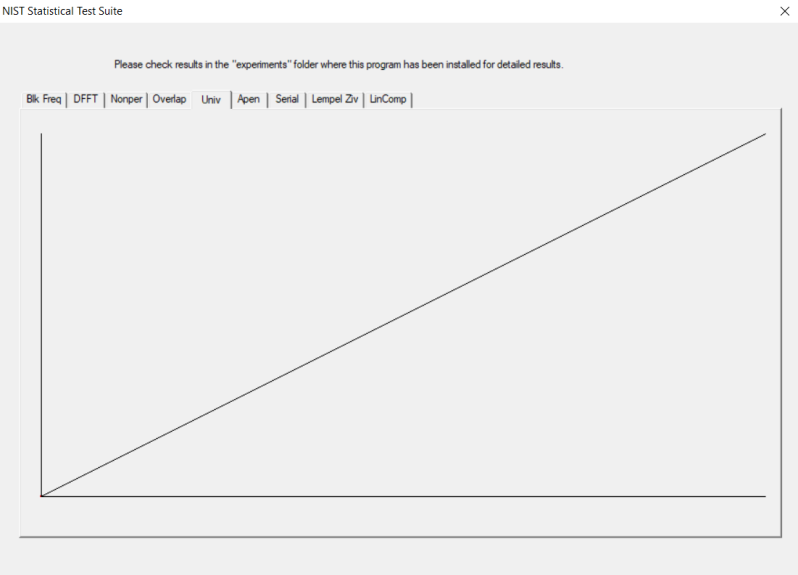


Рисунок 3.15 – Результати тесту Universal в додатку NIST

У висновку, для того щоб стверджувати, що цифровий підпис, згенерований за допомогою зліпка обличчя, є стійким, важливо проаналізувати результати цих тестів. Якщо всі тести показують високу ступінь випадковості та відсутність систематичних або регулярних властивостей, це може служити підтвердженням стійкості цифрового підпису до криптографічних атак.

3.5 Висновки до розділу

У цьому розділі ми зосередились на розробці графічного інтерфейсу та програмної реалізації вдосконаленого алгоритму генерації цифрових ключів з використанням зліпка обличчя. Головною метою було створення зручного та ефективного інструменту для генерації безпечних цифрових ключів на основі унікальних особливостей обличчя.

1. Графічний Інтерфейс:

- Розроблений графічний інтерфейс забезпечує простоту та зручність в користуванні.

- Всі необхідні функції для взаємодії з алгоритмом генерації ключів доступні в інтуїтивно зрозумілому вигляді.

2. Програмна Реалізація Алгоритму:

- Алгоритм генерації ключів на основі зліпка обличчя був реалізований інтегрально та ефективно.

- Використання технологій, таких як Face-api.js, сприяє точній та швидкій роботі програми.

3. Інструкція для Користувача:

- Надана інструкція детально пояснює кожен крок роботи з додатком, починаючи від запуску та закінчуючи генерацією ключів.

- Користувач може легко взаємодіяти з програмою навіть без спеціалізованого досвіду.

4. Тестування за Допомогою NIST:

- Застосування тестів NIST гарантує високий рівень стійкості та випадковості згенерованих ключів.

- Результати тестів свідчать про ефективність та безпеку розробленого методу.

Загалом, розробка та тестування вдосконаленого методу генерації цифрових ключів за допомогою зліпка обличчя підтверджують його практичну застосовність та високий рівень якості в реальних умовах використання.

4 ЕКОНОМІЧНА ЧАСТИНА

Науково-технічна розробка має право на існування та впровадження, якщо вона відповідає вимогам часу, як в напрямку науково-технічного прогресу та і в плані економіки. Тому для науково-дослідної роботи необхідно оцінювати економічну ефективність результатів виконаної роботи.

Магістерська кваліфікаційна робота за темою «Вдосконалення методу генерації цифрових ключів за допомогою зліпка обличчя» відноситься до науково-технічних робіт, які орієнтовані на виведення на ринок (або рішення про виведення науково-технічної розробки на ринок може бути прийнято у процесі проведення самої роботи), тобто коли відбувається так звана комерціалізація науково-технічної розробки. Цей напрямок є пріоритетним, оскільки результатами розробки можуть користуватися інші споживачі, отримуючи при цьому певний економічний ефект. Але для цього потрібно знайти потенційного інвестора, який би взявся за реалізацію цього проекту і переконати його в економічній доцільності такого кроку.

Для наведеного випадку нами мають бути виконані такі етапи робіт:

1) проведено комерційний аудит науково-технічної розробки, тобто встановлення її науково-технічного рівня та комерційного потенціалу;

2) розраховано витрати на здійснення науково-технічної розробки;

3) розрахована економічна ефективність науково-технічної розробки у випадку її впровадження і комерціалізації потенційним інвестором і проведено обґрунтування економічної доцільності комерціалізації потенційним інвестором.

4.1 Проведення комерційного та технологічного аудиту науково-технічної розробки

Метою проведення комерційного і технологічного аудиту дослідження за темою «Вдосконалення методу генерації цифрових ключів за допомогою зліпка

обличчя» є оцінювання науково-технічного рівня та рівня комерційного потенціалу розробки, створеної в результаті науково-технічної діяльності.

Оцінювання науково-технічного рівня розробки та її комерційного потенціалу рекомендується здійснювати із застосуванням 5-ти бальної системи оцінювання за 12-ма критеріями, наведеними в табл. 4.1 [56].

Таблиця 4.1 – Рекомендовані критерії оцінювання науково-технічного рівня і комерційного потенціалу розробки та бальна оцінка

Бали (за 5-ти бальною шкалою)					
	0	1	2	3	4
Технічна здійсненність концепції					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено працездатність продукту в реальних умовах
Ринкові переваги (недоліки)					
2	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів
4	Технічні та споживчі властивості	Технічні та споживчі властивості	Технічні та споживчі властивості	Технічні та споживчі властивості	Технічні та споживчі властивості

	продукту значно гірші, ніж в аналогів	продукту трохи гірші, ніж в аналогів	продукту на рівні аналогів	продукту трохи кращі, ніж в аналогів	продукту значно кращі, ніж в аналогів
5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає
Практична здійсненність					
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на навчання наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні.	Потрібні незначні фінансові ресурси. Джерела	Потрібні значні фінансові ресурси.	Потрібні незначні фінансові ресурси.	Не потребує додаткового фінансування

	Джерела фінансування ідеї відсутні	фінансування відсутні	Джерела фінансування є	Джерела фінансування є	
10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуютьсяу військово промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуються у виробництві
11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій більше 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій менше 3-х років
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь-які регламентні обмеження на виробництво та реалізацію продукту

Результати оцінювання науково-технічного рівня та комерційного потенціалу науково-технічної розробки потрібно звести до таблиці.

Таблиця 4.2 – Результати оцінювання науково-технічного рівня і комерційного потенціалу розробки експертами

Критерії	Експерт (ПІБ, посада)		
	1	2	3
	Бали:		
1. Технічна здійсненність концепції	5	5	5
2. Ринкові переваги (наявність аналогів)	4	5	4
3. Ринкові переваги (ціна продукту)	4	3	3
4. Ринкові переваги (технічні властивості)	4	4	3
5. Ринкові переваги (експлуатаційні витрати)	3	3	3
6. Ринкові перспективи (розмір ринку)	3	4	3
7. Ринкові перспективи (конкуренція)	3	3	4
8. Практична здійсненність (наявність фахівців)	3	3	3
9. Практична здійсненність (наявність фінансів)	3	3	4
10. Практична здійсненність (необхідність нових матеріалів)	3	3	3
11. Практична здійсненність (термін реалізації)	3	4	4
12. Практична здійсненність (розробка документів)	4	3	3
Сума балів	42	43	42
Середньоарифметична сума балів $СБ_c$	42,3		

За результатами розрахунків, наведених в таблиці 4.2, зробимо висновок щодо науково-технічного рівня і рівня комерційного потенціалу розробки. При цьому використаємо рекомендації, наведені в табл. 4.3 [55].

Таблиця 4.3 – Науково-технічні рівні та комерційні потенціали розробки

Середньоарифметична сума балів СБ , розрахована на основі висновків експертів	Науково-технічний рівень та комерційний потенціал розробки
41…48	Високий
31…40	Вище середнього
21…30	Середній
11…20	Нижче середнього
0…10	Низький

Згідно проведених досліджень рівень комерційного потенціалу розробки за темою «Вдосконалення методу генерації цифрових ключів за допомогою зліпка обличчя» становить 42,3 бала, що, відповідно до таблиці 4.3, свідчить про комерційну важливість проведення даних досліджень (рівень комерційного потенціалу розробки високий).

4.2 Розрахунок узагальненого коефіцієнта якості розробки

Окрім комерційного аудиту розробки доцільно також розглянути технічний рівень якості розробки, розглянувши її основні технічні показники. Ці показники по-різному впливають на загальну якість проектної розробки.

Узагальнений коефіцієнт якості ($B_н$) для нового технічного рішення розрахуємо за формулою [55]:

$$B_н = \sum_{i=1}^{k} \alpha_i \cdot \beta_i \quad , \tag{4.1}$$

де k – кількість найбільш важливих технічних показників, які впливають на якість нового технічного рішення;

α_i – коефіцієнт, який враховує питому вагу *і-го* технічного показника в загальній якості розробки. Коефіцієнт α_i визначається експертним шляхом і при цьому має виконуватись умова $\sum_{i=1}^{k} \alpha_i = 1$;

β_i – відносне значення *і-го* технічного показника якості нової розробки.

Відносні значення β_i для різних випадків розраховуємо за такими формулами:

- для показників, зростання яких вказує на підвищення в лінійній залежності якості нової розробки:

$$\beta_i = \frac{I_{ні}}{I_{аі}} \quad , \tag{4.2}$$

де $I_{ні}$ та $I_{на}$ – чисельні значення конкретного *і*-го технічного показника якості відповідно для нової розробки та аналога;

- для показників, зростання яких вказує на погіршення в лінійній залежності якості нової розробки:

$$\beta_i = \frac{I_{аі}}{I_{ні}} \quad ; \tag{4.3}$$

Використовуючи наведені залежності можемо проаналізувати та порівняти техніко-економічні характеристики аналогу та розробки на основі отриманих наявних та проектних показників, а результати порівняння зведемо до таблиці 4.4.

Таблиця 4.4 – Порівняння основних параметрів розробки та аналога

Показники (параметри)	Azure Face API	Проектоване програмне забезпечення
Переваги		
Точність розпізнавання	Висока	Висока
Швидкість роботи	Висока	Висока
Можливість інтеграції з іншими технологіями	Так	Так
Недоліки		
Приватність	Є питання щодо приватності, оскільки використовується розпізнавання обличчя	Деякі стосуються проблем приватності, оскільки використовується тривимірна модель обличчя
Вартість впровадження	Залежить від обладнання та вимагає підтримки відповідних пристроїв	Висока
Залежність від умов освітлення	Може впливати на точність	Так
Доступність документації та підтримки	Висока	Обмежена

Відповідно до даних попередньої таблиці 4.4 експертами проведено оцінювання усіх параметрів за 10-ти бальною шкалою, а також визначено вагомості кожного показника в загальній їх системі. Результати зведено в табл. 4.5.

Таблиця 4.5 – Порівняння основних параметрів розробки та аналога

Показники (параметри)	Azure Face API	Проектоване програмне забезпечення	Відношення параметрів нової розробки до аналога	Питома вага показника
Точність розпізнавання, бали	9	10	1,1	0,25
Швидкість роботи, бали	8	10	1,25	0,2
Можливість інтеграції з іншими технологіями, бали	10	10	1	0,15
Приватність, бали	9	9	1	0,1
Вартість впровадження, бали	9	10	0,9	0,1
Залежність від умов освітлення, бали	10	9	1,1	0,1
Доступність документації та підтримки, бали	9	9	1	0,1

Узагальнений коефіцієнт якості ($B_н$) для нового технічного рішення складе:

$$B_н = \sum_{i=1}^{k} \alpha_i \cdot \beta_i = 1{,}1 \cdot 0{,}25 + 1{,}25 \cdot 0{,}2 + 1 \cdot 0{,}15 + 1 \cdot 0{,}1 + 0{,}9 \cdot 0{,}1 + 1{,}1 \cdot 0{,}1 + 1 \cdot 0{,}1 = 1{,}1.$$

Отже за технічними параметрами, згідно узагальненого коефіцієнту якості розробки, науково-технічна розробка переважає існуючі аналоги приблизно в 1,1 рази.

У результаті проведених досліджень технічних характеристик розробки визначено, що програмна реалізація роботи є не менш функціональна ніж інші більш відомі аналоги в світі. Програма може використовуватись на будь-яких пристроях, які мають камеру, оскільки це веб-додаток, операційна система неважлива. Також у результаті аналізу комерційного та наукового потенціалу доведено актуальність розробки.

4.3 Розрахунок витрат на проведення науково-дослідної роботи

Витрати, пов’язані з проведенням науково-дослідної роботи на тему «Вдосконалення методу генерації цифрових ключів за допомогою зліпка обличчя», під час планування, обліку і калькулювання собівартості науково-дослідної роботи групуємо за відповідними статтями.

4.3.1 Витрати на оплату праці

До статті «Витрати на оплату праці» належать витрати на виплату основної та додаткової заробітної плати керівникам відділів, лабораторій, секторів і груп, науковим, інженерно-технічним працівникам та ін.

Основна заробітна плата дослідників

Витрати на основну заробітну плату дослідників ($З_о$) розраховуємо у відповідності до посадових окладів працівників, за формулою [55]:

$$З_о = \sum_{i=1}^{k} \frac{M_{mi} \cdot t_i}{T_p}, \quad (4.4)$$

де k – кількість посад дослідників залучених до процесу досліджень;

M_{ni} – місячний посадовий оклад конкретного дослідника, грн;

t_i – число днів роботи конкретного дослідника, дні;

T_p – середнє число робочих днів в місяці, T_p=21 день.

$$З_o = 25000{,}00 \cdot 8 / 21 = 69047{,}62 \text{ грн.}$$

Проведені розрахунки зведемо до таблиці.

Таблиця 4.6 – Витрати на заробітну плату дослідників

Найменування посади	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Число днів роботи	Витрати на заробітну плату, грн
Керівник проекту	25000	1190,48	58	69047,62
Інженер-розробник програмного забезпечення	23000	1095,24	50	54761,90
Технік	15000	714,29	10	7142,86
Всього				130952,38

Основна заробітна плата робітників

Витрати на основну заробітну плату робітників ($З_p$) за відповідними найменуваннями робіт НДР розраховуємо за формулою:

$$З_p = \sum_{i=1}^{n} C_i \cdot t_i \text{,} \quad (4.5)$$

де C_i – погодинна тарифна ставка робітника відповідного розряду, за виконану відповідну роботу, грн/год;

t_i – час роботи робітника при виконанні визначеної роботи, год.

Погодинну тарифну ставку робітника відповідного розряду C_i можна визначити за формулою:

$$C_i = \frac{M_M \cdot K_i \cdot K_c}{T_p \cdot t_{зм}}, \quad (4.6)$$

де M_M – розмір прожиткового мінімуму працездатної особи, або мінімальної місячної заробітної плати (в залежності від діючого законодавства), приймемо *Мм*=6700,00 грн;

K_i – коефіцієнт міжкваліфікаційного співвідношення для встановлення тарифної ставки робітнику відповідного розряду (табл. Б.2, додаток Б) [55];

K_c – мінімальний коефіцієнт співвідношень місячних тарифних ставок робітників першого розряду з нормальними умовами праці виробничих об'єднань і підприємств до законодавчо встановленого розміру мінімальної заробітної плати.

T_p – середнє число робочих днів в місяці, приблизно T_p = 21 день;

$t_{зм}$ – тривалість зміни, год.

$C_1 = 6700{,}00 \cdot 1{,}10 \cdot 1{,}65 / (21 \cdot 8) = 69{,}09$ грн.

$З_{р1} = 72{,}38 \cdot 4{,}00 = 289{,}54$ грн.

Таблиця 4.7 – Величина витрат на основну заробітну плату робітників

Найменування робіт	Тривалість роботи, год	Розряд роботи	Тарифний коефіцієнт	Погодинна тарифна ставка, грн	Величина оплати на робітника грн
Установка електронно-	4	2	1,1	72,38	289,54

обчислювального обладнання					
Підготовка робочого місця дослідника	3	2	1,1	72,38	217,15
Інсталяція програмного забезпечення	3	5	1,7	111,87	335,60
Тестування системи	2	2	1,1	72,38	144,77
Всього					987,05

Додаткова заробітна плата дослідників та робітників

Додаткову заробітну плату розраховуємо як 10 … 12% від суми основної заробітної плати дослідників та робітників за формулою:

$$З_{дод} = (З_о + З_р) \cdot \frac{Н_{дод}}{100\%}, \quad (4.7)$$

де $Н_{дод}$ – норма нарахування додаткової заробітної плати. Приймемо 11%.

$З_{дод} = (130952,38 + 987,05) \cdot 11 / 100\% = 14513,34$грн.

4.3.2 Відрахування на соціальні заходи

Нарахування на заробітну плату дослідників та робітників розраховуємо як 22% від суми основної та додаткової заробітної плати дослідників і робітників за формулою:

$$З_н = (З_о + З_р + З_{дод}) \cdot \frac{Н_{зп}}{100\%} \quad (4.8)$$

де $Н_{зп}$ – норма нарахування на заробітну плату. Приймаємо 22%.

Зн = (130952,38+ 987,05+ 14513,34) · 22 / 100% = 32219,61 грн.

4.3.3 Сировина та матеріали

До статті «Сировина та матеріали» належать витрати на сировину, основні та допоміжні матеріали, інструменти, пристрої та інші засоби і предмети праці, які придбані у сторонніх підприємств, установ і організацій та витрачені на проведення досліджень.

Витрати на матеріали (*М*), у вартісному вираженні розраховуються окремо по кожному виду матеріалів за формулою:

$$M = \sum_{j=1}^{n} H_j \cdot Ц_j \cdot K_j - \sum_{j=1}^{n} B_j \cdot Ц_{вj}, \quad (4.9)$$

де H_j – норма витрат матеріалу *j*-го найменування, кг;

n – кількість видів матеріалів;

$Ц_j$ – вартість матеріалу *j*-го найменування, грн/кг;

K_j – коефіцієнт транспортних витрат, (K_j = *1,1 … 1,15*);

B_j – маса відходів *j*-го найменування, кг;

$Ц_{вj}$ – вартість відходів *j*-го найменування, грн/кг.

$М_1 = 3 \cdot 200,00 \cdot 1,1 - 0,000 \cdot 0,00 = 660,0$ грн.

Проведені розрахунки зведемо до таблиці.

Таблиця 4.8 – Витрати на матеріали

Найменування матеріалу, марка, тип, сорт	Ціна за од, грн	Норма витрат, од	Величина відходів, кг	Ціна відходів, грн/кг	Вартість витраченого матеріалу, грн
Офісний папір	200	3	0	0	660
Папір для записів	110	1	0	0	121

Органайзер офісний	210	1	0	0	231
Канцелярське приладдя (набір офісного працівника)	175	2	0	0	385
Картридж для принтера Canon LBP6500	1100	1	0	0	1210
Flesh-пам'ять Kingston 16 GB	130	1	0	0	143
Тека для паперів	82	1	0	0	90,2
Всього					2840,2

4.3.4 Розрахунок витрат на комплектуючі

Витрати на комплектуючі *($К_в$)*, які використовують при проведенні НДР на тему «Вдосконалення методу генерації цифрових ключів за допомогою зліпка обличчя» відсутні.

4.3.5 Спецустаткування для наукових (експериментальних) робіт

До статті «Спецустаткування для наукових (експериментальних) робіт» належать витрати на виготовлення та придбання спецустаткування необхідного для проведення досліджень, також витрати на їх проектування, виготовлення, транспортування, монтаж та встановлення. В даній дослідній роботі витрати на спецустаткування відсутні.

4.3.6 Програмне забезпечення для наукових (експериментальних) робіт

До статті «Програмне забезпечення для наукових (експериментальних) робіт» належать витрати на розробку та придбання спеціальних програмних засобів і програмного забезпечення, (програм, алгоритмів, баз даних) необхідних для

проведення досліджень, також витрати на їх проектування, формування та встановлення.

Балансову вартість програмного забезпечення розраховуємо за формулою:

$$B_{прг} = \sum_{i=1}^{k} Ц_{iпрг} \cdot C_{прг.i} \cdot K_i \quad , \tag{4.9}$$

де $Ц_{iпрг}$ – ціна придбання одиниці програмного засобу даного виду, грн;

$C_{прг.i}$ – кількість одиниць програмного забезпечення відповідного найменування, які придбані для проведення досліджень, шт.;

K_i – коефіцієнт, що враховує інсталяцію, налагодження програмного засобу тощо, ($K_i = 1,10…1,12$);

k – кількість найменувань програмних засобів.

$B_{прг} = 6400,00 \cdot 1 \cdot 1,1 = 7168$ грн.

Отримані результати зведемо до таблиці:

Таблиця 4.9 – Витрати на придбання програмних засобів по кожному виду

Найменування програмного засобу	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
ОС Windows 11	2	11600	25984
Прикладний пакет Microsoft Office 2019	2	5500	12320
Система розробки Microsoft Visual Studio	1	6400	7168
Всього			45472

4.3.7 Амортизація обладнання, програмних засобів та приміщень

В спрощеному вигляді амортизаційні відрахування по кожному виду обладнання, приміщень та програмному забезпеченню тощо, розраховуємо з використанням прямолінійного методу амортизації за формулою:

$$A_{обл} = \frac{Ц_б}{T_в} \cdot \frac{t_{вик}}{12}, \quad (4.10)$$

де $Ц_б$ – балансова вартість обладнання, програмних засобів, приміщень тощо, які використовувались для проведення досліджень, грн;

$t_{вик}$ – термін використання обладнання, програмних засобів, приміщень під час досліджень, місяців;

$T_в$ – строк корисного використання обладнання, програмних засобів, приміщень тощо, років.

$A_{обл}$ = (35000,00 · 2) / (3 · 12) = 1861,11 грн.

Проведені розрахунки зведемо до таблиці.

Таблиця 4.10 – Амортизаційні відрахування по кожному виду обладнання

Найменування обладнання	Балансова вартість, грн	Строк корисного використання, років	Термін використання обладнання, місяців	Амортизаційні відрахування, грн
Ноутбук Ноутбук HP Pavilion 15-eh2038ua (982F5EA)	35000	3	2	1861,11
Ноутбук Ноутбук ASUS ROG Strix G16 (2023) G614JU-N4224	60000	3	2	3333,33

(90NR0CC2-M00D80)				
Робоче місце дослідника	10000	5	2	333,33
Оргтехніка	6000	4	2	250,00
ОС Windows 11	11600	2	2	966,67
Visual Studio Code	6400	2	1	266,67
Прикладний пакет Microsoft Office 2019	5500	2	2	458,33
Всього				7469,44

4.3.8 Паливо та енергія для науково-виробничих цілей

Витрати на силову електроенергію (B_e) розраховуємо за формулою:

$$B_e = \sum_{i=1}^{n} \frac{W_{yi} \cdot t_i \cdot Ц_e \cdot K_{вni}}{\eta_i}, \quad (4.11)$$

де W_{yi} – встановлена потужність обладнання на визначеному етапі розробки, кВт;

t_i – тривалість роботи обладнання на етапі дослідження, год;

$Ц_e$ – вартість 1 кВт-години електроенергії, грн; (вартість електроенергії визначається за даними енергопостачальної компанії), приймемо $Ц_e = 7{,}50$ грн;

$K_{вni}$ – коефіцієнт, що враховує використання потужності, $K_{вni} < 1$;

η_i – коефіцієнт корисної дії обладнання, $\eta_i < 1$.

$B_e = 0{,}6 \cdot 350{,}0 \cdot 7{,}50 \cdot 0{,}95 / 0{,}97 = 1542{,}53$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 4.11 – Витрати на електроенергію

Найменування обладнання	Встановлена потужність, кВт	Тривалість роботи, год	Сума, грн
Ноутбук Ноутбук HP Pavilion 15-eh2038ua (982F5EA)	0,6	350	1542,53
Ноутбук Ноутбук ASUS ROG Strix G16 (2023) G614JU-N4224 (90NR0CC2-M00D80)	0,6	400	1762,89
Робоче місце дослідника	0,15	350	385,63
Оргтехніка	0,45	20	66,11
Всього			3757,15

4.3.9 Службові відрядження

До статті «Службові відрядження» дослідної роботи на тему «Вдосконалення методу генерації цифрових ключів за допомогою зліпка обличчя» належать витрати на відрядження штатних працівників, працівників організацій, які працюють за договорами цивільно-правового характеру, аспірантів, зайнятих розробленням досліджень, відрядження, пов’язані з проведенням випробувань машин та приладів, а також витрати на відрядження на наукові з’їзди, конференції, наради, пов’язані з виконанням конкретних досліджень.

Витрати за статтею «Службові відрядження» розраховуємо як 20…25% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{св} = (З_о + З_р) \cdot \frac{Н_{св}}{100\%}, \quad (4.12)$$

де $Н_{св}$ – норма нарахування за статтею «Службові відрядження», приймемо $Н_{св} = 20\%$.

$B_{св} = (130952,38 + 987,05) \cdot 20 / 100\% = 26387,89$грн.

4.3.10 Витрати на роботи, які виконують сторонні підприємства, установи і організації

Витрати за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації» розраховуємо як 30…45% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{сп} = (З_о + З_р) \cdot \frac{Н_{сп}}{100\%}, \quad (4.13)$$

де $Н_{сп}$ – норма нарахування за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації», приймемо $Н_{сп}$= 30%.

$B_{сп}$ = (130952,38+ 987,05) · 30 / 100% = 39581,83 грн.

4.3.11 Інші витрати

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками.

Витрати за статтею «Інші витрати» розраховуємо як 50…100% від суми основної заробітної плати дослідників та робітників за формулою:

$$І_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (4.14)$$

де $Н_{ів}$ – норма нарахування за статтею «Інші витрати», приймемо $Н_{ів}$ = 50%.

$І_в$ = (130952,38+ 987,05) · 50 / 100% = 65969,72грн.

4.3.12 Накладні (загальновиробничі) витрати

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов’язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов’язані з набором робочої сили; витрати на оплату послуг банків; витрати, пов’язані з

освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін.

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуємо як 100…150% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \quad (4.15)$$

де $Н_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати», приймемо $Н_{нзв}$ = 120%.

$В_{нзв}$ = (130952,38+ 987,05) · 120 / 100% = 158 327,32 грн.

Витрати на проведення науково-дослідної роботи на тему «Вдосконалення методу генерації цифрових ключів за допомогою зліпка обличчя» розраховуємо як суму всіх попередніх статей витрат за формулою:

$$B_{заг} = З_о + З_р + З_{дод} + З_н + М + К_в + В_{спец} + В_{прг} + А_{обл} + В_е + В_{оз} + В_{сп} + І_в + В_{нзв}. \quad (4.17)$$

$В_{заг}$=130952,38+ 987,05+14513,34+32219,61+2840,2+0,00 +0,00+ 45472+ 7469,44+ 3757,15+26387,89+39581,83+65969,72+158 327,32= 528477,93грн.

Загальні витрати *ЗВ* на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховується за формулою:

$$ЗВ = \frac{B_{заг}}{\eta}, \quad (4.16)$$

де η - коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи, приймемо η=0,7.

ЗВ = 528477,93/ 0,7 = 754968,48 грн.

4.4 Розрахунок економічної ефективності науково-технічної розробки при її можливій комерціалізації потенційним інвестором

В ринкових умовах узагальнюючим позитивним результатом, що його може отримати потенційний інвестор від можливого впровадження результатів тієї чи іншої науково-технічної розробки, є збільшення у потенційного інвестора величини чистого прибутку.

Результати дослідження проведені за темою «Вдосконалення методу генерації цифрових ключів за допомогою зліпка обличчя» передбачають комерціалізацію протягом 3-х років реалізації на ринку.

В цьому випадку майбутній економічний ефект буде формуватися на основі таких даних:

ΔN – збільшення кількості споживачів продукту, у періоди часу, що аналізуються, від покращення його певних характеристик;

1-й рік – 300 користувачів;

2-й рік – 350 користувачів;

3-й рік – 250 користувачів.

N – кількість споживачів які використовували аналогічний продукт у році до впровадження результатів нової науково-технічної розробки, приймемо 2000 користувачів;

$Ц_б$ – вартість програмного продукту у році до впровадження результатів розробки, приймемо 200000,00 грн;

$\pm\Delta Ц_о$ – зміна вартості програмного продукту від впровадження результатів науково-технічної розробки, приймемо 10000,00 грн.

Можливе збільшення чистого прибутку у потенційного інвестора $\Delta П_i$ для кожного із 3-х років, протягом яких очікується отримання позитивних результатів від можливого впровадження та комерціалізації науково-технічної розробки, розраховуємо за формулою [55]**:**

$$\Delta П_i = (\pm \Delta Ц_o \cdot N + Ц_o \cdot \Delta N)_i \cdot \lambda \cdot \rho \cdot (1 - \frac{\vartheta}{100}), \quad (4.17)$$

де λ – коефіцієнт, який враховує сплату потенційним інвестором податку на додану вартість. У 2023 році ставка податку на додану вартість складає 20%, а коефіцієнт $\lambda = 0,8333$;

ρ – коефіцієнт, який враховує рентабельність інноваційного продукту. Приймемо ρ =30%;

ϑ – ставка податку на прибуток, який має сплачувати потенційний інвестор, у 2023 році $\vartheta = 18\%$;

Збільшення чистого прибутку 1-го року:

$\Delta П_1 =$ (10000,00·2000,00+210000,00·300)·0,83·0,3·(1-0,18/100%)= 17008194 грн.

Збільшення чистого прибутку 2-го року:

$\Delta П_2 =$ (10000,00·2000,00+210000,00·(300+350))·0,83·0,3·(1-0,18/100%)= 32069667грн.

Збільшення чистого прибутку 3-го року:

$\Delta П_3 =$ (1000,00·2000,00+210000,00·(300+350+250))·0,83·0,3·(1-0,18/100%)= 42827862 грн.

Приведена вартість збільшення всіх чистих прибутків *ПП*, що їх може отримати потенційний інвестор від можливого впровадження та комерціалізації науково-технічної розробки:

$$ПП = \sum_{i=1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, \quad (4.18)$$

де $\Delta П_i$ – збільшення чистого прибутку у кожному з років, протягом яких виявляються результати впровадження науково-технічної розробки, грн;

T – період часу, протягом якого очікується отримання позитивних результатів від впровадження та комерціалізації науково-технічної розробки, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, τ =0,2;

t – період часу (в роках) від моменту початку впровадження науково-технічної розробки до моменту отримання потенційним інвестором додаткових чистих прибутків у цьому році.

$$ПП =$$

$$14173495{,}00/(1+0{,}2)^1+22270602{,}08/(1+0{,}2)^2+24784642{,}36/(1+0{,}2)^3=61228739{,}44\text{грн.}$$

Величина початкових інвестицій PV, які потенційний інвестор має вкласти для впровадження і комерціалізації науково-технічної розробки:

$$PV = k_{інв} \cdot ЗВ, \quad (4.19)$$

де $k_{інв}$ – коефіцієнт, що враховує витрати інвестора на впровадження науково-технічної розробки та її комерціалізацію, приймаємо $k_{інв}$=3;

$ЗВ$ – загальні витрати на проведення науково-технічної розробки та оформлення її результатів, приймаємо 754968,48 грн.

$PV = k_{інв} \cdot ЗВ$ = 3· 754968,48= 2264905,434грн.

Абсолютний економічний ефект $E_{абс}$ для потенційного інвестора від можливого впровадження та комерціалізації науково-технічної розробки становитиме:

$$E_{абс} = ПП - PV \tag{4.20}$$

де $ПП$ – приведена вартість зростання всіх чистих прибутків від можливого впровадження та комерціалізації науково-технічної розробки, 61228739,44 грн;

PV – теперішня вартість початкових інвестицій, 2264905,43 грн.

$E_{абс} = ПП - PV$ = 61228739,44грн - 2264905,434= 58963834,01 грн.

Внутрішня економічна дохідність інвестицій $E_в$, які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки:

$$E_в = \sqrt[Tж]{1 + \frac{E_{абс}}{PV}} - 1, \tag{4.21}$$

де $E_{абс}$ – абсолютний економічний ефект вкладених інвестицій, 58963834,01грн;

PV – теперішня вартість початкових інвестицій, 2264905,43 грн;

$T_{ж}$ – життєвий цикл науково-технічної розробки, тобто час від початку її розробки до закінчення отримування позитивних результатів від її впровадження, 3 роки.

$$E_в = \sqrt[T_ж]{1 + \frac{E_{абс}}{PV}} - 1 = (1+58963834,01/2264905,43)^{1/3} = 2,0.$$

Мінімальна внутрішня економічна дохідність вкладених інвестицій $\tau_{мін}$:

$$\tau_{мін} = d + f, \quad (4.22)$$

де d – середньозважена ставка за депозитними операціями в комерційних банках; в 2023 році в Україні d =0,11;

f – показник, що характеризує ризикованість вкладення інвестицій, приймемо 0,2.

$\tau_{мін}$ = 0,11+0,2 = 0,31 < 2,0 свідчить про те, що внутрішня економічна дохідність інвестицій $E_в$, які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки вища мінімальної внутрішньої дохідності. Тобто інвестувати в науково-дослідну роботу за темою «Вдосконалення методу генерації цифрових ключів за допомогою зліпка обличчя» доцільно.

Період окупності інвестицій $T_{ок}$ які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки:

$$T_{ок} = \frac{1}{E_в}, \quad (4.23)$$

де $E_в$ – внутрішня економічна дохідність вкладених інвестицій.

$T_{ок}$ = 1 / 2 = 0,5 року.

$T_{ок} <$ 3-х років, що свідчить про комерційну привабливість науково-технічної розробки і може спонукати потенційного інвестора профінансувати впровадження даної розробки та виведення її на ринок.

4.5 Висновки до розділу

Згідно проведених досліджень рівень комерційного потенціалу розробки за темою «Вдосконалення методу генерації цифрових ключів за допомогою зліпка обличчя» становить 42,3 бала, що, свідчить про комерційну важливість проведення даних досліджень (рівень комерційного потенціалу розробки високий).

Також термін окупності становить 0,5 р., що менше 3-х років, що свідчить про комерційну привабливість науково-технічної розробки і може спонукати потенційного інвестора профінансувати впровадження даної розробки та виведення її на ринок.

Отже можна зробити висновок про доцільність проведення науково-дослідної роботи за темою «Вдосконалення методу генерації цифрових ключів за допомогою зліпка обличчя».

ВИСНОВОК

У цій дипломній роботі проведено докладне дослідження та розглянуто питання вдосконалення генерації цифрових ключів на основі зліпка обличчя. Розглянуті основні аспекти використання цифрового підпису та захисту інформації в сучасному інформаційному суспільстві. Детально проаналізовано принципи, алгоритми та технології генерації цифрового підпису на основі зображень обличчя.

В розділі 1 проведено вступні дослідження та визначено актуальність теми дослідження, поставлено мету та завдання роботи. Також проведено аналіз існуючих підходів до генерації цифрових ключів, визначено проблеми та напрями подальших досліджень. Проведено об'ємний огляд літератури та публікацій, пов'язаних із застосуванням зліпка обличчя для генерації цифрових ключів. Розглянуто різні підходи та методи, представлені у відомих джерелах.

У другому розділі детально розглянуті основні принципи генерації цифрових підписів, алгоритми та техніки, що використовуються для створення ефективних та надійних систем генерації цифрових ключів на основі обличчя. Проаналізовано існуючі методи та їх переваги та недоліки.

Третій розділ присвячений розробці нового методу генерації цифрових ключів, використовуючи зліпок обличчя. Проаналізовано результати експериментів та порівняно їх з існуючими методами. Розроблено алгоритм та програмний додаток для генерації цифрових ключів за допомогою зліпка обличчя. Розглянуті технічні аспекти розробки та використання необхідних технологій.

У четвертому розділі проведено об'ємний огляд економічної частини, пов'язаних із застосуванням зліпка обличчя для генерації цифрових ключів. Розглянуто прогнозування витрат на виконання наукової роботи, прогнозування комерційних ефектів від реалізації результатів розробки та проведено оцінювання комерційного потенціалу розробки програмного забезпечення.

Загальний аналіз методів генерації цифрових ключів на основі зліпка обличчя підтверджує їхню актуальність та ефективність у сучасних умовах. Розроблений метод дозволяє покращити процес генерації цифрових ключів, забезпечуючи високу точність та безпеку.

Завершуючи дипломну роботу, можна визначити, що генерація цифрових ключів на основі зліпка обличчя є перспективним напрямком у розвитку сучасних методів кібербезпеки та захисту інформації. Результати дослідження можуть бути використані для подальших наукових досліджень у сфері кібербезпеки та розробки нових технологій генерації цифрових ключів.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Електронний цифровий підпис. URL: https://uk.wikipedia.org/wiki/%D0%95%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B8%D0%B9_%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B8%D0%B9_%D0%BF%D1%96%D0%B4%D0%BF%D0%B8%D1%81 (дата звернення: 02.10.2023).

2. Katz, J., & Lindell, Y. Introduction to Modern Cryptography, 2007 URL: http://staff.ustc.edu.cn/~mfy/moderncrypto/reading%20materials/Introduction_to_Modern_Cryptography.pdf (дата звернення: 02.10.2023).

3. Хеш-функції. URL: https://uk.wikipedia.org/wiki/%D0%A5%D0%B5%D1%88%D1%84%D1%83%D0%BD%D0%BA%D1%86%D1%96%D1%8F (дата звернення: 02.10.2023).

4. Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 1996. URL: https://mrajacse.files.wordpress.com/2012/01/applied-cryptography-2nd-ed-b-schneier.pdf (дата звернення: 02.10.2023).

5. FaceID. URL: https://support.apple.com/uk-ua/102381 (дата звернення: 02.10.2023).

6. Windows Hello. URL: https://habr.com/ru/companies/microsoft/articles/314822/ (дата звернення: 02.10.2023).

7. Deep Face. URL: https://viso.ai/computer-vision/deepface/ (дата звернення: 02.10.2023).

8. Azure Face. URL: https://learn.microsoft.com/en-us/azure/ai-services/computer-vision/concept-detecting-faces (дата звернення: 02.10.2023).

9. Kairos. URL: https://coinmercury.com/ru/kairos-ico/ (дата звернення: 02.10.2023).

10. Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. Handbook of Fingerprint Recognition, 2009. URL: https://nguyenthihanh.files.wordpress.com/2015/08/handbook-of-fingerprint-recognition.pdf (дата звернення: 02.10.2023).

11. Jain, A. K., Hong, L., & Pankanti, S. Biometric identification, 2000. URL: https://dl.acm.org/doi/fullHtml/10.1145/328236.328110 (дата звернення: 02.10.2023).

12. Yang, Y., & Busch, C. Fingerprint Template Protection: Recent Advances and Challenges, 2017. URL: https://www.hindawi.com/journals/wcmc/2018/7107295/ (дата звернення: 02.10.2023).

13. Ratha, N. K., Connell, J. H., & Bolle, R. M. Enhancing security and privacy in biometrics-based authentication systems, 2001. URL: https://www.scirp.org/(S(351jmbntvnsjt1aadkposzje))/reference/ReferencesPapers.aspx?ReferenceID=1916892 (дата звернення: 02.10.2023).

14. Daugman, J. G. How Iris Recognition Works, 2004. URL: https://www.robots.ox.ac.uk/~az/lectures/est/iris.pdf (дата звернення: 05.10.2023).

15. Wildes, R. P., Asmuth, J. C., Green, G. L., Hsu, S., Kolczynski, R. J., & Matey, J. R. A System for Automated Iris Recognition, 1997. URL: https://www.sciencedirect.com/science/article/pii/S2090447911000177 (дата звернення: 05.10.2023).

16. Hollingsworth, K. P., Bowyer, K. W., & Flynn, P. J. Using Iris Recognition for User Authentication on Mobile Devices, 2007. URL: https://web.archive.org/web/20170810032432id_/https://aran.library.nuigalway.ie/bitstream/handle/10379/5362/TCE_RESUBMIT_ST-CD-PC.pdf?sequence=1 (дата звернення: 05.10.2023).

17. Baker, S., & Bowyer, K. W. Iris Recognition: On the Segmentation of Unideal Iris Images, 2002. URL: https://web.archive.org/web/20190221025917id_/http://pdfs.semanticscholar.org/2d9b/4d523b563abcfc74e5c0e7ec2afc1683c540.pdf (дата звернення: 05.10.2023).

18. Rathgeb, C., & Busch, C. Improving Iris Recognition by Fusing Segmentation Results, 2012. URL: https://dl.gi.de/server/api/core/

bitstreams/4934bcb5-30b2-45b4-ab86-67ff73ec47ef/content (дата звернення: 20.10.2023).

19. Daugman, J. (2004). How Iris Recognition Works. URL: https://www.robots.ox.ac.uk/~az/lectures/est/iris.pdf (дата звернення: 20.10.2023).

20. Bowyer, K. W., Hollingsworth, K. P., & Flynn, P. J. A Survey of Iris Biometrics Research, 2008. URL: https://www.researchgate.net/publication/305712238_A_Survey_of_Iris_Biometrics_Research_2008-2010 (дата звернення: 20.10.2023).

21. Hollingsworth, K. P., Bowyer, K. W., & Flynn, P. J. Using Iris Recognition for User Authentication on Mobile Devices, 2007. URL: https://iopscience.iop.org/article/10.1088/1757-899X/769/1/012024 (дата звернення: 20.10.2023).

22. Wildes, R. P., Asmuth, J. C., Green, G. L., Hsu, S., Kolczynski, R. J., & Matey, J. R. A System for Automated Iris Recognition, 1997. URL: https://www.academia.edu/27432839/Design_Method_of_Video_Based_Iris_Recognition_System_V_IRS (дата звернення: 20.10.2023).

23. Huang, K., & Wechsler, H. Iris Recognition Using Independent Component Analysis, 2002. URL: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=c37cea1deb577d73351f6084a9f93e2a8178ced8 (дата звернення: 20.10.2023).

24. Reynolds, D. A., & Rose, R. C. Robust Text-Independent Speaker Identification Using Gaussian Mixture Speaker Models, 1995. URL: https://www.researchgate.net/publication/3333389_Robust_text-independent_speaker_identification_using_Gaussian_Mixture_speaker_models (дата звернення: 20.10.2023).

25. Campbell, J. P., Reynolds, D. A., & Singer, E. Speaker Authentication for Telephone Transactions: A Database Perspective, 1997. URL: https://www.semanticscholar.org/paper/Speaker-recognition%3A-a-tutorial-

Campbell/298cd5cefda80cd2aa0e9bc1d27f552b9eb18633 (дата звернення: 20.10.2023).

26. Kinnunen, T., & Li, H. An overview of text-independent speaker recognition: From features to supervectors, 2010. URL: https://www.researchgate.net/publication/222682226_An_Overview_of_Text-Independent_Speaker_Recognition_from_Features_to_Supervectors (дата звернення: 20.10.2023).

27. Richardson, F., Reynolds, D., & Dehak, N. Deep neural network approaches to speaker and language recognition, 2015. URL: https://groups.csail.mit.edu/sls/publications/2015/Dehak_IEEE-2015.pdf (дата звернення: 20.10.2023).

28. Khoury, E., Kinnunen, T., & Huttunen, H. Spoofing detection in speaker verification using Gaussian mixture model and support vector machine classifiers, 2013. URL: https://www.researchgate.net/publication/322029802_Spoofing_Detection_in_Automatic_Speaker_Verification_Systems_Using_DNN_Classifiers_and_Dynamic_Acoustic_Features (дата звернення: 30.10.2023).

29. Zhang, Z., Yan, J., Liu, S., Lei, Z., & Yi, D. Face Liveness Detection by Learning Multi-scale LPQ Patterns, 2012. URL: https://www.researchgate.net/publication/224238158_Face_liveness_detection_by_learning_multispectral_reflectance_distributions (дата звернення: 30.10.2023).

30. Wu, X., He, R., Sun, Z., & Tan, T. A Light CNN for Deep Face Representation with Noisy Labels, 2018. URL: https://arxiv.org/abs/1511.02683 (дата звернення: 30.10.2023).

31. Damer, N., & Gupta, A. Facial Recognition Technology: A Review, 2018. URL: https://www.researchgate.net/publication/343118558_A_Review_of_Face_Recognition_Technology (дата звернення: 30.10.2023).

32. Dantcheva, A., Velardo, C., Dugelay, J. L. What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics, 2016. URL: https://inria.hal.science/hal-01247885/document (дата звернення: 30.10.2023).

33. Martínez-Díaz, M., Pascual-Gaspar, J. M., & García-Salicetti, S. Deep Learning for Face Recognition: A Comprehensive Study, 2019. URL: https://arxiv.org/abs/1907.12739 (дата звернення: 30.10.2023).

34. Brenner, S. E., & Lippard, S. J. Use of Fluorescence Measurements to Monitor DNA Binding to Proteins in Electrophoretic Gels, 1996. URL: https://www.researchgate.net/publication/281084237_DNA_binding_fluorescent_proteins_for_the_direct_visualization_of_large_DNA_molecules (дата звернення: 30.10.2023).

35. Feng, J., Yang, Y., & Zhang, Y. DNA-Based Data Storage: Trends and Methods, 2019. URL: https://personal.ntu.edu.sg/hmkiah/docs/papers/DNACodes_Survey.pdf (дата звернення: 30.10.2023).

36. Gonçalves, I., Lopes, J. C., Rosa, N., & Pinto, J. L. DNA-Based Cryptographic Keys Using Hybrid Ciphers, 2020. URL: https://www.researchgate.net/publication/269098843_DNA_based_Cryptography_An_Overview_and_Analysis (дата звернення: 30.10.2023).

37. Church, G. M., Gao, Y., & Kosuri, S. Next-Generation Digital Information Storage in DNA, 2012. URL: https://www.researchgate.net/publication/230698422_Next-Generation_Digital_Information_Storage_in_DNA (дата звернення: 30.10.2023).

38. Erlich, Y., & Zielinski, D. DNA Fountain enables a robust and efficient storage architecture, 2017. URL: https://www.researchgate.net/publication/345898227_DNA_Fountain_enables_a_robust_and_efficient_storage_architecture (дата звернення: 30.10.2023).

39. Nandakumar, K., & Jain, A. K. Multibiometric Template Security Using Fuzzy Vault, 2012. URL: https://biometrics.cse.msu.edu/

Publications/SecureBiometrics/NandakumarJain_MultibiometricVault_BTAS08.pdf (дата звернення: 30.10.2023).

40. Miura, N., Nagasaka, A., & Miyatake, T. Feature Extraction of Finger Vein Patterns Based on repeated Line Tracking and Its Application to Personal Identification, 2007. URL: https://arxiv.org/ftp/arxiv/papers/2101/2101.08415.pdf (дата звернення: 30.10.2023).

41. Rattani, A., Bouridane, A., Khelifi, F., & Seker, H. Finger Vein Recognition Using a Hybrid Deep Learning Framework 2016. URL: https://newinera.com/index.php/JournalLaMultiapp/article/view/788 (дата звернення: 30.10.2023).

42. Tang, H., Wu, X., Sun, Z., & Lei, Z. Finger Vein Recognition Using a New Encoding Method and Partial Least Squares Discriminant, 2015. URL: https://www.researchgate.net/publication/356549375_A_Joint_Bayesian_Framework_based_on_Partial_Least_Squares_Discriminant_Analysis_for_Finger_Vein_Recognition (дата звернення: 30.10.2023).

43. Li, Y., Zhang, L., & Li, H. Finger-Vein Recognition Based on Local Directional Code, 2012. URL: https://www.mdpi.com/1424-8220/12/11/14937 (дата звернення: 30.10.2023).

44. Srihari, S. N., Huang, C., & Srinivasan, H. Individuality of Handwriting, 2002. URL: https://www.ojp.gov/pdffiles1/nij/grants/190133.pdf (дата звернення: 30.10.2023).

45. Plamondon, R., & Srihari, S. N. Online and Off-Line Handwriting Recognition: A Comprehensive Survey, 2000. URL: https://ru.scribd.com/document/486239220/offline-AND-ON-LINE-handwriting-recognition-comprehensive-survey (дата звернення: 10.11.2023).

46. Hafemann, L. G., Sabourin, R., & Oliveira, L. S. Offline Handwritten Signature Verification - Literature Review, 2017. URL: https://arxiv.org/abs/1507.07909 (дата звернення: 10.11.2023).

47. Kasprzak, A. Biometric Verification of Signatures Made with a Digital Pen Based on Their Dynamic and Spatial Features, 2017. URL: https://www.researchgate.net/publication/301411029_Assessment_of_the_authenticity_of_Dynamic_Biometric_Signature_The_results_of_experiments (дата звернення: 10.11.2023).

48. Kanoun, S., Cheriet, M., & Alimi, A. M. Handwriting biometric system based on wavelet transform, 2011. URL: https://eprints.uthm.edu.my/8421/1/24p%20HAITHAM%20QUTAIBA%20GHADHBAN.pdf (дата звернення: 10.11.2023).

49. Lotte, F., Congedo, M., Lécuyer, A., Lamarche, F., & Arnaldi, B. A review of classification algorithms for EEG-based brain–computer interfaces, 2007. URL: https://www.researchgate.net/publication/37271882_A_review_of_classification_algorithms_for_EEG-based_brain-computer_interfaces (дата звернення: 10.11.2023).

50. Hassanien, A. E., Al-Shammari, E. T., & Al-Jumeily, D. EEG-based Human Authentication using Differential Evolution and Learning Vector Quantization, 2015. URL: https://www.researchgate.net/publication/359789483_EEG- based_Biometric_Authentication_Using_Machine_Learning_A_Comprehensive_Survey (дата звернення: 10.11.2023).

51. Subasi, A., & Gursoy, M. I. EEG signal classification using PCA, ICA, LDA and support vector machines, 2010. URL: https://www.researchgate.net/publication/223297745_EEG_signal_classification_using_PCA_ICA_LDA_and_support_vector_machines (дата звернення: 10.11.2023).

52. Sharma, L. N., & Pachori, R. B. Person authentication using EEG signals during listening and thinking tasks, 2014. URL: https://www.researchgate.net/publication/6506629_Person_Authentication_Using_Brainwaves_EEG_and_Maximum_A_Posteriori_Model_Adaptation (дата звернення: 10.11.2023).

53. Huang, K. C., Hsieh, J. C., Wu, C. T., & Chen, C. Y. EEG-based user authentication using mind evolutionary algorithm, 2011. URL: https://www.mdpi.com/1099-4300/18/12/432 (дата звернення: 10.11.2023).

54. NIST STS URL: https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software (дата звернення: 15.11.2023).

55. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт / Уклад. : В. О. Козловський, О. Й. Лесько, В. В. Кавецький. Вінниця : ВНТУ, 2021. 42 с. (дата звернення: 16.11.2023).

56. Кавецький В. В. Економічне обґрунтування інноваційних рішень: практикум / В. В. Кавецький, В. О. Козловський, І. В. Причепа. Вінниця : ВНТУ, 2016. 113 с. (дата звернення: 16.11.2023).

ДОДАТКИ

Додаток А. Технічне завдання

Вінницький національний технічний університет

Факультет менеджменту та інформаційної безпеки

Кафедра менеджменту та безпеки інформаційних систем

ЗАТВЕРДЖУЮ

Голова секції "Управління інформаційною безпекою" кафедри МБІС

д.т.н., професор

_____ Юрій ЯРЕМЧУК

"20" вересня 2023 р.

ТЕХНІЧНЕ ЗАВДАННЯ

до магістерської кваліфікаційної роботи на тему:

Вдосконалення методу генерації цифрових ключів за допомогою зліпка обличчя

08-72.МКР.009.00.122.ТЗ

Керівник магістерської кваліфікаційної роботи

к.т.н., доц., доцент каф. МБІС Грицак А.В.

_____

Вінниця – 2023 р.

1. Найменування та область застосування

Програмний засіб вдосконалення методу генерації цифрових ключів за допомогою зліпка обличчя. Область застосування: захист інформаційних ресурсів від несанкціонованого доступу у системах безпеки, генерація цифрових ключів.

2.Підстава для розробки

Розробка виконується на основі наказу ректора ВНТУ №247 від 18. 09. 2023 р.

3. Мета та призначення розробки

3.1 Мета розробки: вдосконалення методу генерації цифрових ключів за допомогою зліпка обличчя.

3.2 Призначення: генерація та підпис файлів цифровим підписом який згенерований зліпком обличчя.

4. Джерела розробки

4.1. Ахрамович В. М. Ідентифікація й аутентифікація, керування доступом // Сучасний захист інформації. – 2016. №4.– С. 47-51.

4.2. Бурячок В.Л. Політика інформаційної безпеки: підручник. / В.Л.Бурячок, Р.В.Грищук, В.О.Хорошко / За заг. ред. докт. техн. наук, проф. В.О. Хорошка. – К.: ПВП «Задруга», 2014. – 222 с.

4.3. Єсін В.І. Безпека інформаційних систем і технологій / В.І.Єсін, О.О. Кузнецов, Л.С. Сорока. – Харків: ХНУ імені В.Н. Каразіна, 2013. – 632 с.

4.4. ZakariaOmar, ZangooeiToomaj, MohdAfiziMohdShukran. Enhancing Mixing Recognition-Based and Recall-Based Approach in Graphical Password Scheme. IJACT, Vol. 4, No. 15, pp. 189-197, 2012.

5. Вимоги до програми

5.1 Вимоги до функціональних характеристик:

5.1.1 Програмний засіб повинен мати зручний, легкий у використанні інтерфейс користувача;

5.1.2 Реалізація методу не повинна вимагати спеціальних ліцензійних програмних додатків;

5.1.3 Програмний засіб повинен виконувати процес автентифікації користувачів у системі.

5.2 Вимоги до надійності:

5.2.1 Програмний засіб повинен працювати без помилок, у випадку виникнення критичних ситуацій необхідно передбачити виведення відповідних повідомлень;

5.2.2 Бази даних повинні бути налаштовані на автоматичне створення резервних копій;

5.2.3 Програмний засіб повинен виконувати свої функції.

5.3 Вимоги до складу і параметрів технічних засобів:

– процесор – Pentium 1500 МГц і подібні до них;

– оперативна пам’ять – не менше 512 Mb;

– середовище функціонування – операційна система сімейство Windows;

– вимоги до техніки безпеки при роботі з програмою повинні відповідати існуючим вимогам та стандартам з техніки безпеки при користуванні комп’ютерною технікою.

6. Вимоги до програмної документації

6.1 Обов’язкова поетапна інструкція для майбутніх користувачів, наведена у пункті 3.4

7. Вимоги до технічного захисту інформації

7.1 Необхідно забезпечити захист розроблюваного програмного засобу від несанкціонованого використання.

7.2 Неможливість отримання доступу незареєстрованих користувачів до інформаційних ресурсів.

8. Техніко-економічні показники

8.1 Цінність результатів використання даного проекту повинна перевищувати витрати на його реалізацію.

8.2 Має бути реалізований таким чином, щоб підходити для використання широкого загалу.

9. Стадії та етапи розробки

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Початок	Закінчення
1	Визначення напрямку магістерської роботи, формулювання теми	20.09.2023	25.09.2023
2	Аналіз предметної області обраної теми	26.09.2023	30.10.2023
3	Апробація отриманих результатів	31.10.2023	02.10.2023
4	Розробка алгоритму роботи	03.10.2023	17.10.2023
5	Написання магістерської роботи на основі розробленої теми	18.10.2023	10.10.2023
6	Розробка економічної частини	11.11.2023	23.11.2023
7	Передзахист магістерської кваліфікаційної роботи	24.11.2023	25.11.2023
8	Виправлення, уточнення, корегування магістерської кваліфікаційної роботи	26.11.2023	30.11.2023
9	Захист магістерської кваліфікаційної роботи	15.12.2023	15.12.2023

10. Порядок контролю та прийому

10.1 До приймання магістерської кваліфікаційної роботи надається:

– ПЗ до магістерської кваліфікаційної роботи;

– програмний додаток;

– презентація;

– відзив керівника роботи;

– відзив опонента

Технічне завдання до виконання прийняв _____ Мирончак М.А.

Додаток Б. Лістинг програми (Код додатку частини авторизації та реєстрації)

```
import { body } from 'express-validator'

const RegisterValidationSchema = [
    body('email')
        .notEmpty()
        .isEmail(),
    body('name')
        .notEmpty()
        .isString(),
    body('password')
        .notEmpty()
        .isString()
        .isLength({ min: 6, max: 30 }),
    body('confirm')
        .notEmpty()
        .isString()
        .custom((value, {req}) => value === req.body.password),
    body('faceDescriptor')
        .notEmpty()
export default RegisterValidationSchema;
import { body } from 'express-validator';
const LoginValidationSchema = [
    body('email')
        .notEmpty()
        .isEmail(),
    body('password')
        .notEmpty()
export default LoginValidationSchema
```

Додаток В. Лістинг програми (Код додатку частини користувача)

```
<!DOCTYPE html>
<html lang="en">

<head>
    <meta charset="UTF-8">
    <title></title>
    <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap@4.0.0/dist/css/bootstrap.min.css"
        integrity="sha384-Gn5384xqQ1aoWXA+058RXPxPg6fy4IWvTNh0E263XmFcJlSAwiGgFAW/dAiS6JXm"
crossorigin="anonymous">
</head>

<body>
    <div class="container">
        <div class="d-flex flex-column ">
            <div class="d-flex flex-column m-2">
                <form class="d-flex flex-column" method='post' action='/generate?email=<%=email%>'
                    enctype="multipart/form-data">
                    <button class="btn btn-dark" onclick="alert('Ключі згенеровані')" type="submit">Згенерувати
ключі</button>
                </form>
            </div>
            <div class="d-flex flex-column m-2">
                <form class="d-flex flex-column" method='post' action='/upload?email=<%=email%>'
                    enctype="multipart/form-data">
                    <label for="filepidp">Файл для підпису</label>
                    <input type='file' name='file' id="filepidp">
```

```
                <button class="btn btn-dark" type="submit">Згенерувати підпис</button>
            </form>
        </div>
        <div class="d-flex flex-column m-2">
            <form class="d-flex flex-column" method='post' action='/uploadverify?email=<%=email%>'
                enctype="multipart/form-data">
                <label for="file">Файл для перевірки</label>
                <input type='file' name='file' id="file">
                <label for="pidp">Підпис</label>
                <input type='file' name='sigantyre' id="pidp">
                <button class="btn btn-dark" type="submit">Перевірити файл</button>
            </form>
        </div>
        <a href="http://localhost:3000">Повернутися назад</a>
    </div>
  </div>
</body>


</html>
```

Додаток Г. Лістинг програми (Код додатку серверної частини)

```
var express = require('express')

var ejs = require('ejs')

var mongoose = require('mongoose')

var bodyParser = require('body-parser')

const fileUpload = require('express-fileupload');

const crypto = require('crypto');

const fs = require('fs')

var app = express()

const User = require("./models/users"); // USER MODEL

mongoose.connect('mongodb+srv://1234:1234@cluster0.gnzbuzm.mongodb.net/?retryWrites=true&w=majority',
{ useNewUrlParser: true })

app.use(fileUpload())

app.use(bodyParser.json())

app.use(bodyParser.urlencoded({

    extended: true

}))


app.set('view engine', 'ejs')


app.listen(8000, function () {

    console.log('Node.js listening on port ' + 8000)

})


app.get('/pidpus', async (req, res) => {

    console.log()

    res.render('main', { email: req.query.email })

})
```

```
app.post('/generate', async (req, res) => {
    let user = await User.findOne({ email: req.query.email })
    async function generateKeyFiles() {
        const keyPair = crypto.generateKeyPairSync('rsa', {
            modulusLength: 520,
            publicKeyEncoding: {
                type: 'spki',
                format: 'pem'
            },
            privateKeyEncoding: {
                type: 'pkcs8',
                format: 'pem',
                cipher: 'aes-256-cbc',
                passphrase: crypto.createHash('md5').update(JSON.stringify(user.faceDescriptor)).digest('hex')
            }
        });
        // Creating private key file
        fs.writeFileSync(`${user.email}_private_key`, keyPair.privateKey);
        fs.writeFileSync(`${user.email}_public_key`, keyPair.publicKey);
    }
    await generateKeyFiles()
    res.render('main', { email: req.query.email })
})

app.post('/upload', async (req, res) => {
    let user = await User.findOne({ email: req.query.email })
    const privateKey = fs.readFileSync(`${user.email}_private_key`, "utf8");
```

```
    const encrypted = crypto.privateEncrypt({
        key: privateKey,
        passphrase: crypto.createHash('md5').update(JSON.stringify(user.faceDescriptor)).digest('hex')
    }
        , Buffer.from(req.files.file.md5));
    fs.writeFileSync(`${req.files.file.name}_digital_signature`, encrypted.toString("base64"));
    res.download(`${req.files.file.name}_digital_signature`)
})


app.post('/uploadverify', async (req, res) => {
    let user = await User.findOne({ email: req.query.email })
    const publicKey = fs.readFileSync(`${user.email}_public_key`, "utf8");
    const decripted = crypto.publicDecrypt(publicKey,
        Buffer.from(req.files.sigantyre.data.toString(), 'base64'));
    console.log()
    if (req.files.file.md5 === decripted.toString()) {
        res.send('Файл успішно перевірено')
    } else {
        res.send('Файл не вірний')
    }
})
```

Додаток Д. Ілюстративний матеріал (презентація)

Вдосконалення методу генерації цифрових ключів за допомогою зліпка обличчя

Ст.Мирончак М.А. 2КІТС-22М

Актуальність

Тема цієї роботи є особливо актуальною у зв'язку з :

1. Безпека особистості: З відмітним зростанням кількості онлайн-сервісів та транзакцій важливо забезпечити надійний захист особистих даних та інформації. Використання біометричних методів, зокрема генерація цифрових ключів за допомогою зліпка обличчя, може покращити безпеку особистості.
2. Інновації в біометричних технологіях: Зліпок обличчя є однією з передових технологій біометричного впізнавання. Дослідження та оптимізація методів генерації цифрових ключів на його основі сприяють розвитку інновацій в цьому сегменті технологій.
3. Застосування в сучасних системах безпеки: Технології генерації цифрових ключів на основі біометричних даних можуть знайти широке застосування у сучасних системах безпеки, таких як фінансові установи, корпоративні системи, медичні установи та інші сфери, де необхідна надійна аутентифікація користувачів.
4. Проблеми та виклики безпеки: Розвиток методів генерації цифрових ключів на основі біометричних даних також вирішує проблеми та виклики безпеки, пов'язані із штучним інтелектом, аналітикою даних та кіберзлочинністю.

Об'єкт та предмет дослідження. Наукова новизна

Об'єктом дослідження є - система методів та технологій генерації цифрових ключів на основі біометричних даних, зокрема, зліпка обличчя.

Предмет дослідження – методи та технології генерації цифрових ключів за допомогою зліпка обличчя.

Наукова новизна полягає у вдосконаленні методу генерації цифрових ключів за допомогою зліпка обличчя.

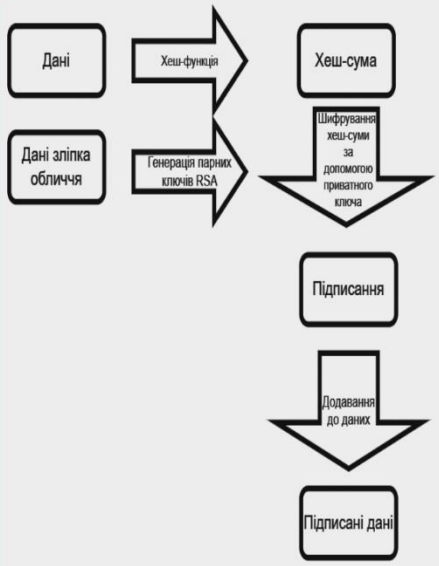
Використані алгоритми

Алгоритм шифрування RSA

Алгоритм шифрування RSA - це криптографічний алгоритм, що використовується для шифрування та розшифрування повідомлень. Він базується на складності факторизації великих простих чисел.

Алгоритм хешування MD-5

Алгоритм хешування MD-5 (Message Digest Algorithm 5) є одним з найпоширеніших алгоритмів хешування. Він використовується для обчислення хеш-функції, яка перетворює вхідні дані будь-якого розміру в фіксований хеш-код довжиною 128 біт.



Генерація цифрових ключів за допомогою обличчя

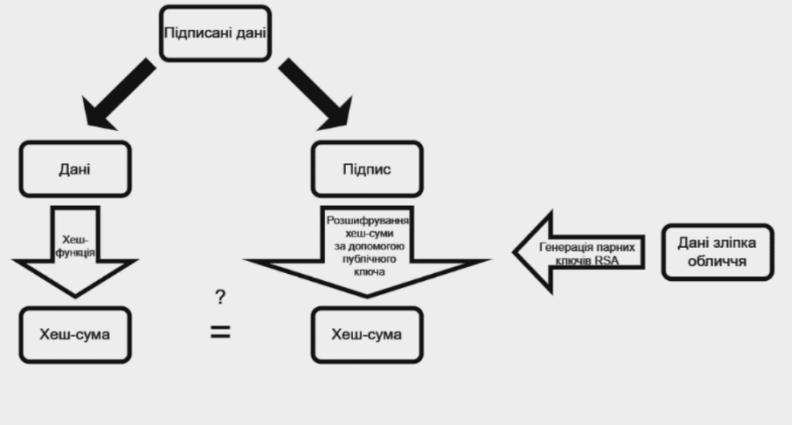
Кроки для генерації цифрових ключів за допомогою обличчя

- Крок перший. Збір біометричних даних: Спочатку потрібно зібрати біометричні дані обличчя особ. Це м оже бути зроблено за допомогою високоякісних фотографій або відеозаписів. Сучасні системи мо жуть використовувати 3D-моделі обличчя для більш точної репрезентації фізіономії.
- Крок другий. Виділення ключових особливостей: Виділення ключових особливостей обличчя, таких як контур, очі, ніс, рот і т. д., забезпечує точність і унікальність біометричних даних. Ці особливості можуть бути виділені за допомогою алгоритмів комп'ютерного зору.
- Крок третій. Перетворення в шаблон: Отримані особливості перетворюються в унікальний шаблон, який може бути використан ий для подальшої обробки.
- Крок четвертий. Хешування шаблону: Створений шаблон обличчя хешується за допомогою хеш-функції, такої як MD-5. Це перетворює шаблон в фіксований рядок, який є унікальним для конкретного обличчя.
- Крок п'ятий. Підписання приватним ключем: Отриманий хеш-значення підписується за допомогою приватного ключа особи чи організації. Це створює цифровий підпис, який пов'язаний з унікальними біометричними даними обличчя.
- Крок шостий. Додавання цифрового підпису до даних: Цифровий підпис, разом з відкритим ключем для верифікації, додається до даних або документа. Це створює електронний пакет, який містить підписані дані та інформацію для перевірки підпису.

Верифікація

- Крок перший. Отримання підписаних даних та цифрового підпису: Отримувач отримує дані, які були підписані, а також цифровий підпис та відкритий ключ від особи чи організації, яка створила підпис.
- Крок другий. Збір біометричних даних обличчя отримувача: Отримувач повинен зібрати біометричні дані обличчя, які будуть порівнюватися з біометричними даними, які були використані для створення підпису.
- Крок третій. Виділення ключових особливостей обличчя: Подібно до процесу генерації підпису, отримувач повинен виділити ключові особливості обличчя, такі як контур, очі, ніс, рот тощо.
- Крок четвертий. Перетворення в шаблон та хешування: Отримані особливості перетворюються в шаблон та хешуються за допомогою тієї ж самої хеш-функції, яка використовувалася під час генерації підпису. Це створює хеш-значення для біометричних даних обличчя.
- Крок п'ятий. Розшифрування цифрового підпису: Отримане хеш-значення розшифровується за допомогою відкритого ключа, який був використаний для підписування.
- Крок шостий. Порівняння хеш-значень: Хеш-значення, отримане після розшифрування підпису, порівнюється з хеш-значенням, отриманим від біометричних даних обличчя отримувача. Якщо ці хеш-значення співпадають, це означає, що підпис був створений вірною особою та дані не були змінені після підписання.

Верифікація



- Якщо порівняння успішне, це підтверджує автентичність підпису, і отримувач може бути впевнений у тому, що отримані дані були підписані вірною особою чи організацією та не були змінені в процесі передачі. Цей процес дозволяє використовувати біометричні дані обличчя для перевірки цифрових підписів, що робить його важливим для безпеки та автентифікації в сучасних системах електронного документообігу та інших застосуваннях.

Дякую за увагу

Ст.Мирончак М.А. 2КІТС-22М

Додаток Е. Протокол перевірки на антиплагіат

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Вдосконалення методу генерації цифрових ключів за допомогою зліпка обличчя

Тип роботи: магістерська кваліфікаційна робота
(БДР, МКР)

Підрозділ: Кафедра менеджменту та безпеки інформаційних систем
Факультет менеджменту та інформаційної безпеки
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність 97 % Схожість 3 %

Аналіз звіту подібності (відмітити потрібне):

1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Коваль Н.П.
(підпис) (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Мирончак М.А.
(підпис) (прізвище, ініціали)

Керівник роботи _____ Грицак А.В.
(підпис) (прізвище, ініціали)