МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМ. В. ДАЛЯ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЕЛЕКТРОНІКИ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК ТА ІНЖЕНЕРІЇ

До захисту допускається
Т.в.о. завідувача кафедри
_____ Сафонова С.О.
«____»_____ 20__ р.

МАГІСТЕРСЬКА РОБОТА

НА ТЕМУ:

Метод ідентифікації людини за райдужкою ока

Освітній рівень"Магістр"
Спеціальність 123 "Комп'ютерна інженерія"

Науковий керівник роботи:	_____ (підпис)	В.М.Барбарук (ініціали, прізвище)
Консультант з охорони праці:	_____ (підпис)	Я.О.Критська (ініціали, прізвище)
Студент:	_____ (підпис)	Д.А.Любенецький (ініціали, прізвище)
Група:		КІ-18дм

Сєвєродонецьк 2020

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ

Факультет Інформаційних технологій та електроніки
Кафедра Комп'ютерних наук та інженерії
Освітній рівень магістр
Напрям підготовки _____
(шифр і назва)
Спеціальність 123 "Комп'ютерна інженерія"
(шифр і назва)

ЗАТВЕРДЖУЮ:

Т.в.о. завідувача кафедри _____
_____ С.О. Сафонова
«_____» _____20____р.

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Любенецького Дмитра Андрійовича
(прізвище, ім'я, по батькові)

1. Тема роботи Метод ідентифікації людини за райдужкою ока

керівник проекту (роботи) Барбарук Віктор Миколайович, к.т.н., доц.
(прізвище, м.'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від «11» 10 2019 р. № 135/15.15
2. Строк подання студентом роботи 10.01.2020
3. Вихідні дані до роботи Матеріали науково-дослідної практики, загальна структура обчислювальних систем, структура та функції елементів ока людини, зокрема сітківки та райдужної оболонки ока, біометричні методи ідентифікації та аутентифікація, еталонне зображення райдужки, загальна структура та принципи роботи систем біометричної ідентифікації людини, метод перетворення Ерміта, базі даних CASIA-IrisV3.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Огляд літератури і аналіз проблеми дослідження, системи біометричної ідентифікації, Ідентифікація за геометрією ока, методи аналізу зображення райдужної оболонки, охорона праці та безпека в надзвичайних ситуаціях, висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
Електронні плакати

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці та безпека в надзвичайних ситуаціях	Критська Я.О. ст. викл. кафедри КНІ		

7. Дата видачі завдання 14.10.2019

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Отримання завдання	02.09.2019-15.09.2019	
2	Аналіз технічних засобів	16.09.2019-22.09.2019	
3	Розробка методу ідентифікації	23.09.2019-25.09.2019	
4	Реалізація методу ідентифікації	26.09.2019-06.10.2019	
5	Розробка частини проекту "Охорона праці та безпеки в надзвичайних ситуаціях"	07.10.2019-25.11.2019	
6	Оформлення пояснювальної записки, автореферату та презентації	26.11.2019-9.01.2020	
7			

Студент _____ Д.А.Любенецький
(підпис) (прізвище та ініціали)

Науковий керівник _____ В.М.Барбарук
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Любенецький Д.А. Метод ідентифікації людини за райдужкою ока.

Метою роботи є розробка модифікованого методу ідентифікації людини за райдужною оболонкою ока на основі перетворення Ерміта, що використовує локальні характеристики райдужної оболонки. При побудові коду райдужної оболонки використовується аналіз знаків згорток інтенсивності зображення райдужної оболонки ока з функціями перетворення Ерміта.

Наведено аналіз вибору найбільш інформативних номерів функцій Ерміта для використання в алгоритмі й вибір критерію ідентифікації цим методом. Технологія включає також обробку зображень райдужної оболонки ока і метод визначення її областей, вільних від вій, вік і відблисків.

Ключові слова: біометрична ідентифікація, код IPIC, визначення рішень, статистичні критерії, сітківка ока, райдужна оболонка ока, перетворення Ерміта.

ABSTRACT

Lyubenetsky D.A. The method of identifying people beyond the district of the eye.

The paper proposes a modified human identification method for the iris on the basis of the Hermite transformation using the local characteristics of the iris. When constructing the code of the iris, an analysis of the symbols of the crest of the intensity of the image of the iris of the eye with the functions of the Hermite transformation is used.

The analysis of the choice of the most informative numbers of Hermite functions for use in the algorithm and the choice of the identification criterion by this method is given. The technology also includes the processing of images of the iris of the eye and the method of determining its areas, free of eyelashes, age and glare.

Keywords: biometric identification, iris code, decision making, statistical criteria, retina, iris eye, Hermite transform.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

АЧХ – амплітудно-частотна характеристика

БД – база даних

БХЛ – біометрична характеристика людини

ВЧ-фільтрація – високочастотна фільтрація

ІБ – інформаційна база

ІКТ – інформаційно комунікаційна технологія

ІС – інформаційна система

ІЧ – інфрачервоний

КІ – критична інфраструктура

КР – код райдужки

МСДБІТ – мультимодальна статично-динамічна біометрична ІТ

НЧ-фільтрація – низькочастотна фільтрація

РОО – райдужна оболонка ока

СКУД – система контролю та управління доступом

DET – Detection error tradeoff (помилка виявлення, отримана при компромісному виборі параметрів)

EER – Equal Error Rate (рівень рівної ймовірності помилок)

FAR – False Acceptance Rate (рівень помилкових дозволів)

FRR – False Rejection Rate (рівень помилкових відмов)

ISO – International Organization for Standardization (міжнародна організація зі стандартизації)

ROC – Receiver Operating Characteristic (робоча характеристика приймача)

ВСТУП

В даний час біометрична аутентифікація не тільки є невід'ємною процедурою для допуску до об'єктів підвищеної секретності, але і входить в наше повсякденне життя. Величезний інтерес до біометрії зумовлений низкою об'єктивних причин. У класичних парольних системах, а також системах на основі карт доступу підглядання або вгадування пароля, крадіжка або виготовлення дубліката картки призводить до компрометації всієї системи. Більш того, законний користувач, втративши або зіпсувавши карту, втрачає можливість доступу до системи. Системи на основі біометрії практично позбавлені цих недоліків - ідентифікатор нерозривно пов'язаний з самим користувачем, тому втрата або зміна ідентифікатора можливі тільки в надзвичайні події, а сучасні сканери біометричних даних дозволяють виявляти спроби використання муляжів.

Зараз, у зв'язку зі зростанням вимог до інформаційної безпеки стають все поширенішими методи біометричної верифікації та ідентифікації особистості. Особливої гостроти проблема ідентифікації особистості користувача набуває в розподілених системах, особливо в системах високої доступності. Зокрема, висока доступність передбачає, що будь-який користувач може отримати доступ в рамках своїх повноважень до необхідних йому ресурсів і сервісів за прийнятне для нього час.

Сучасна техніка навчилися дізнаватися користувачів по сітківці і райдужну оболонку ока, форми обличчя і рук і ряду динамічних характеристик - голосу, біологічної активності серця, рукописному і клавіатурного почерку.

Просканувати сітківку - внутрішню оболонку очного яблука, що реагує на світло, складніше: для цього до кровоносних судинах задньої стінки ока через зіницю посилають низькоінтенсивне інфрачервоні світлові промені. Подібний метод встановлення особистості вважається високоефективним і активно використовується на урядових і військових об'єктах.

Капілярний малюнок сітківки різниться навіть у близнюків, що знижує ймовірність помилки ідентифікації. Однак, в 2012 році вчені з Університету Нотр-Дам в США виявили похибки у визначенні особистостей людей, чиї дані були внесені в базу раніше 2008 року, і довели, що, на відміну від малюнка на райдужній оболонці, малюнок сітківки піддається ряду вікових змін.

З точки зору надійності, найбільш ефективними на сьогодні методами ідентифікації та аутентифікації є біометричні, які дозволяють вирішити проблеми втрати паролів та особистих ідентифікаторів [2]. Серед біометричних технологій (яких на сьогодні є досить широкий спектр) однією із найперспективніших є біометрія з використанням сітківки ока, яка має специфічну структуру і містить багато текстурної інформації.

Найбільш надійним з практично реалізованих методів вважається метод сканування сітківки ока. Тому він використовується в системах контролю доступу на особливо секретні об'єкти. Із-за низького рівня поширення таких систем малою є вірогідність реалізації спроб злому. Але недоліком є висока вартість систем із використанням цього методу. Крім того, у порівнянні з іншими біометричними об'єктами, ідентифікація по сітківці є більш стабільною і надійною [3]. Отже, обрана тема роботи є актуальною через те, що присвячений саме технологіям біометричної ідентифікації особи за райдужною оболонкою та сітківкою ока.

1 ОГЛЯД ЛІТЕРАТУРИ І АНАЛІЗ ПРОБЛЕМИ ДОСЛІДЖЕННЯ

1.1 Мотивація

Актуальність теми ідентифікації особистості людини зумовлена активною інформатизацією сучасного суспільства та збільшенням потоків конфіденційної інформації. Аналіз сучасних систем контролю доступу свідчить про очевидний рух у бік біометричних методів завдяки їх зручності, надійності та достовірності.

Система захисту критичної інфраструктури являє собою сукупність організаційних і технічних заходів для забезпечення захисту секторів критичної інфраструктури від різних загроз. Ідентифікація користувачів, яка продовжується подальшою їх аутентифікацію, є основою систем безпеки об’єктів критичної інфраструктури, оскільки ці процедури дозволяють виявити несанкціонованих користувачів інформаційно комунікаційних систем на початкових етапах – встановити автентичність та визначити повноваження суб’єкта при його допуску в систему, контроль встановлених повноважень в процесі сеансу роботи, реєстрацію дій тощо [15].

Однією з актуальних задач розвитку інформаційних технологій на сучасному етапі є забезпечення надійного захисту інформації. Існуючі сьогодні методи захисту інформації поділяють на: апаратні, програмні, змішані; останні поєднують у собі як апаратні, так і програмні засоби.

Задача захисту інформації є особливо актуальною в умовах активного розвитку систем електронної торгівлі та банківських операцій, систем дистанційного навчання та великих корпоративних мереж, де циркулює конфіденційна інформація.

Важливою та ще не вирішеною проблемою захисту інформації є ефективна ідентифікація користувача, який отримує доступ до конфіденційної інформації [1]. Традиційний парольний захист має ряд очевидних недоліків. Наприклад, у разі порушення конфіденційності пароля, це часто може залишитися непоміченим його власником, відразу порушується захист всієї інформації, до якої він (власник) має доступ.

Як альтернатива парольній системі або її доповнення може розглядатися ідентифікація користувачів за біометричними характеристиками. Біометричні технології ідентифікації, аутентифікації мають низку переваг перед традиційними і знаходять все більше застосування в комп'ютерних системах [2]. Біометричне підтвердження, а не проста перевірка пароля, який може бути вкрадений, перехоплений або вгаданий, є ключовим при розширенні Інтернет-торгівлі, створенні нових систем безпеки інформації в корпоративних мережах та системах дистанційного навчання та тестування.

З точки зору надійності, найбільш ефективними на сьогодні методами ідентифікації та

аутентифікації є біометричні, які дозволяють вирішити проблеми втрати паролів та особистих ідентифікаторів. Серед біометричних технологій (яких на сьогодні є досить широкий спектр) однією із найперспективніших є біометрія з використанням райдужної оболонки ока (РОО), яка має специфічну структуру і містить багато текстурної інформації. Просторові структури, які спостерігаються в райдужці, унікальні для кожного індивіда, а індивідуальні відмінності з'являються в процесі анатомічного розвитку. Крім того, у порівнянні іншими біометричними об'єктами, ідентифікація по райдужці є стабільнішою і надійною.

Задача біометричної ідентифікації і методи її реалізації розглянуті в багатьох роботах різних вчених. Наприклад, роботи Іванова А. І., Сорокіна І. А., Рибчинко Д. Є. присвячені дослідженню динамічних методів біометричної ідентифікації, зокрема, динаміці рукописного почерку та клавіатурного почерку . У роботах Юркова П. Ю., Бабенко Л. К., Федорова В. М., Каткова О. Н., Дворянкина С. В. розглянуті методи динамічної біометричної ідентифікації за голосовим сигналом. Роботи Диденко С. М., Шапцева В. А. присвячені дослідженню динамічних методів ідентифікації користувачів за почерком миші, зокрема за допомогою математичного апарату нейронних мереж. Темі розробки методів статичної біометричної ідентифікації і зокрема ідентифікації за портретом обличчя присвячені роботи Старовойтова В. В., Муриніна А. Б., Цуркова В. І.

Згідно з дослідженням аналітичного порталу Biometrics.ru, біометричні системи робочого часу користуються найбільшою популярністю в ритейлі (23,0%) та сфері послуг (24,3%). Також значну частку займають виробничі (19%) та медичні (7,8%) підприємства.

З точки зору застосування в інформаційних системах, одним з найбільш перспективних способів ідентифікації користувача є ідентифікація за райдужною оболонкою ока. Це пов'язано з рядом факторів. По-перше, райдужна оболонка потенційно одна з найрізноманітніших біометрика. Так теоретична ймовірність того, що дві різні людини мають один і той же малюнок райдужної оболонки, приблизно дорівнює 10-78, В той час як все населення Землі становить менше 1010. По-друге, малюнок райдужної оболонки досить слабо змінюється з віком, особливо в порівнянні з лицьової біометрією. По-третє, безконтактний спосіб отримання зображень райдужної оболонки робить привабливим її застосування в різних галузях [3,4]. При цьому втрата райдужної оболонки зазвичай пов'язана з фізичною неможливістю користуватися сервісами інформаційної системи [16].

1.2 Огляд сучасних методів біометричної ідентифікації

Проблема ідентифікації особи існує досить давно, людині завжди необхідно було бути чітко впевненою, що вона спілкується з потрібною їй особою, тому проблема ідентифікації була і є актуальною. У загальному випадку ідентифікація об'єкта – це його впізнання, ототожнення із ким-небудь (чим-небудь). Якщо ж говорити про область інформаційних технологій, то даний термін зви-чайно означає встановлення особистості користувача. Цей процес необхідний для того, щоб система надалі змогла ухвалити рішення щодо видачі людині дозволу для роботи на комп'ютері, доступу до закритої інформації й т.ін. Таким чином, ідентифікація є одним із основних понять в інформаційній безпеці.

Сьогодні існує декілька способів ідентифікації користувачів. У кожного з них є свої переваги і недоліки, завдяки чому деякі технології підходять для використання в одних системах, інші – в інших. В загальному випадку існують три методи ідентифікації [2,4]:

- парольна ідентифікація;
- апаратна ідентифікація;
- біометрична ідентифікація.

Як ми вже зазначали процес ідентифікації нас цікавить з точки зору інформаційної безпеки та інформаційних систем. Історично спочатку для інформа-ційних систем використовувалась парольна ідентифікація.

Парольна ідентифікація.

До недавнього часу парольна ідентифікація була єдиним способом визначення особистості користувача. В першу чергу це пов’язано з тим, що парольна ідентифікація найбільш проста як у реалізації, так й у використанні. Кожен зареєстрований користувач будь-якої системи отримує набір персональних реквізитів (звичайно використовуються пари логін – пароль). Далі за кожної спроби входу – людина повинна вказати свою інформацію. Завдяки тому, що такі ідентифікатори унікальні для кожного користувача, то на їх підставі система й робить висновок про особистість користувача та ідентифікує його. Головна перевага парольної ідентифікації – це простота реалізації й використання. Крім того, введення парольної ідентифікації не вимагає зовсім ніяких витрат: даний процес реалізований в усіх інформаційних системах та мережах. Проте такий спосіб ідентифікації має певні недоліки: по-перше – це залежність надійності ідентифікації і від користувачів (від складності обраних ними паролів); по-друге, користувачі не хочуть запам'ятовувати паролі, тому вони їх або забувають, або починають записувати на папері, що призводить до значного зниження рівня інформаційної безпеки.

Апаратна ідентифікація

У даному випадку ідентифікація ґрунтується на визначенні особистості користувача за якимось предметом, ключі (спеціальні електронні), що знаходяться в її ексклюзивному користуванні. Існують два типи ключів – карткові (на базі електронних карт), наприклад, магнітні карти, смарт-карти. Інший тип ключів – це так звані токени (пристрої, які мають свою власну пам'ять і підключаються до одного із зовнішніх портів USB, LPT, COM).

Магнітні картки є менш надійним засобом ідентифікації – це пов’язано в, першу чергу, з тим, що вони не захищені від копіювання інформації, а по друге, вони досить чутливі до механічних ушкоджень, проте основна їх перевага – це простота використання та реалізація.

Ідентифікація на основі смарт-карти та токенів більш надійна. В даному випадку можливо використовувати так звану двофакторну ідентифікацію – тобто спочатку користувач надає для ідентифікації ключ, який виконує низку необхідних дій (наприклад, генерує відкритий та закритий ключі, які використовує для ідентифікації), а потім очікується певна дія з боку користувача (наприклад, ввід пароля). Головною перевагою цього методу ідентифікації є досить висока надійність. Проте цей спосіб має також суттєві недоліки. По-перше, ключ можна загубити, або його можуть вкрасти. По-друге, даний метод ідентифікації потребує додаткових витрат на його реалізацію.

Крім цього, існує ще два різновиди апаратної ідентифікації – це штрих-кодова ідентифікація та радіочастотна ідентифікація RFID. У загальному випадку штрих-кодова ідентифікація використовується для ідентифікації товарів у торгівлі, проте може використовуватися і для ідентифікації особи (людині видається картка з нанесеним штрих-кодом за допомогою якої вона ідентифікується). Основною перевагою цього методу ідентифікації є простота реалізації, проте він має багато недоліків – штрих-код містить інформацію у відкритому вигляді, тому його досить просто підробити. Метод радіочастотної ідентифіка-ції базується на використанні двох пристроїв – базового блока або пристрою зчитування та транспондера, або RFID-позначки. Принцип ідентифікації наступний: у RFID-позначці записується вся інформація, необхідна для ідентифікації особи, яка потім передається пристрою зчитування. Тобто, особа, якій необхідно пройти ідентифікацію, повинна просто мати при собі RFID-позначку, яка сама, опинившись у зоні дії зчитувача, отримує від нього запит на ідентифікацію особи й у відповідь передає всю необхідну інформацію. на відповідь у за-пит. Обмін інформацією між позначкою та зчитувачем здійснюється за допомогою радіосигналів. Основними перевагами цього способу є відносна простота реалізації, відсутня необхідність прямого контакту, простота використання, висока швидкість роботи. Проте є і декілька суттєвих недоліків – по перше, це те, що можна вивести з ладу всю систему ідентифікації, якщо створити досить сильні перешкоди у відповідному радіодіапазоні, по-друге, вартість такої системи ідентифікації досить висока і, по-третє, RFID-

позначку можна вкрасти і видати себе за іншу особу.

Біометрична ідентифікація.

Біометрія – це методика розпізнавання та ідентифікації людей на основі їх індивідуальних і унікальних характеристик[2]. Біометричні властивості включають в себе відбитки пальців, форму особи, малюнок райдужної оболонки ока, малюнок сітківки, геометрію руки, мова, почерк, особливості друку на клавіатурі і навіть візерунок вен на зап'ясті.

Ідентифікувати людину можливо за ознаками, пов'язаними з її фізіологічними особливостями, які однозначно ідентифікують особу. До таких ознак можна віднести: геометричну будову руки, відбитки пальців, особливості малюнка сітківки ока, райдужну оболонку ока, портрет (наприклад, інфрачервону карту людини), характеристики і особливості мови, рукописний почерк, клавіатурний та комп’ютерний почерк, інші фізіологічні особливості людини, що робить її «особливою».

Головною причиною, через яку для ідентифікації особи стали використовувати біометричні ідентифікатори – це те, що вони є у кожної людини та те, що вони унікальні для кожної людини. Тобто, до переваг біометричної ідентифікації слід віднести, по-перше, те, що біометричні ідентифікатори на відміну від інших методів неможливо втратити чи забути; по-друге, біометричні ідентифікатори складно підробити, тому даний метод є найбільш надійним; по-третє, кожна людини володіє унікальними біометричними ознаками, тому точність біометричної ідентифікації близька до ста відсотків.

До недоліків слід віднести, по-перше, те, що реалізація системи біометричної ідентифікації потребує відносно великих грошових вкладень; по-друге, що деякі біометричні ідентифікатори можна підробити, наприклад (відбитки пальців, підпис або голос).

Ідентифікація особистості людини по зображенню райдужної оболонки ока (РОО) – швидко розвивається метод біометрії, вже має широке застосування в системах контролю доступу. Він заснований на тому, що малюнок райдужної оболонки ока має індивідуальну, слабо змінюється з часом структуру. Унікальність структури райдужної оболонки ока відома з найдавніших часів [3]. Ідея ідентифікації особистості по РОО була запропонована офтальмологами в 1936 році. У 1958 році письменник Ян Флемінг висловив її в одному зі своїх детективів про Джеймса Бонда «Операція 'Кульова Блискавка'». За мотивами цього твору в 1984 році був знятий фільм «Ніколи не кажи ніколи».

Особливість ідентифікації за біометричними параметрами базується на їх винятковості. Ймовірність того, що знайдуться дві людини з однаковими ознаками, дуже мала (наприклад, ймовірність того, що в двох різних людей на однакових пальцях однієї руки співпадатимуть відбитки пальців, рівна 1/24 млн, тобто практично є нульовою). Основні характеристики перерахованих вище методів біометричної ідентифікації наведені в таблиці 1.1 [10].

Таблиця 1.1 – Основні характеристики методів біометричної ідентифікації

Метод отримання біометричних параметрів	Ймовірність відмови у доступі %	Ймовірність помилкової ідентифікації «чужого» (без використання муляжу) %	Ймовірність помилкової ідентифікації «чужого» (з використанням муляжу) %	Збереження таємниці образу у процесі ідентифікації абонента	Вартість технічної реалізації в грошовому еквіваленті, у.о.
Геометрична будова руки	0,2…4	0,2….1	10…75	Неможливо приховати	Від 600 до 3000
Відбитки пальців	2...6	0,0001	10...70	Неможливо приховати	Від 60 до 600
Особливості малюнка сітківки ока	0,4	6...10	_____	Неможливо приховати	Приблизно 4000
Райдужна оболонка ока	0,2…2	0,0001	_____	Неможливо приховати	Від 500 до 6000
Портрет обличчя	1…9	_____	_____	Неможливо приховати	55000
Рукописний почерк	0,5…5	0,5…5	0,5...5	8-10…10-40	_____
Клавіатурний та комп’ютерний почерк	3…9	3...9	_____	6-10…10-12	_____
Характеристики і особливості мови	0,5...5	0,5...5	25...90 (запис)	10-16…10-30	1...60

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

Існує цілий комплекс заходів із забезпечення захисту інформації, проте вони не є на сто відсотків ефективними. Для підвищення ефективності систем захисту останнім часом

пропонується використовувати так звані біометричні системи ідентифікації. Біометричні системи ідентифікації встановлюють особу за індивідуальними біометричними параметрами людини.

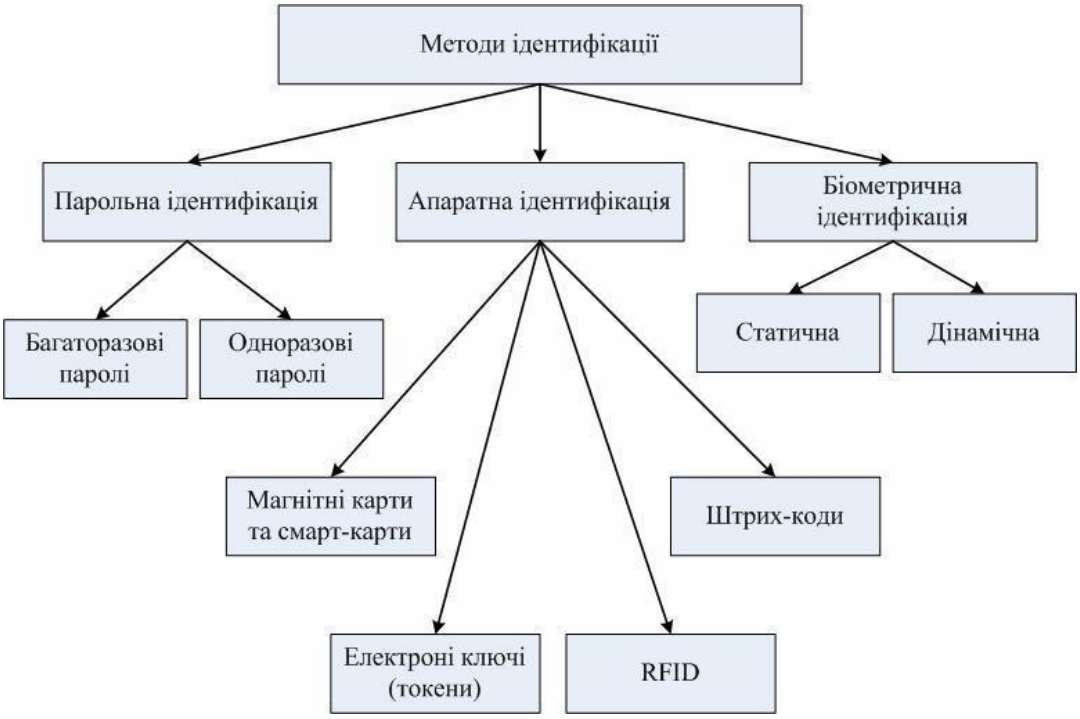


Рисунок 1.1 – Класифікація методів ідентифікації

Методи біометричної ідентифікації діляться на дві великі групи: статичні методи, які ґрунтуються на фізіологічних характеристиках людини та динамічні методи, які ґрунтуються на особливостях поведінки людини - підсвідомих рухах в процесі виконання якої-небудь дії.

Статичні та динамічні методи біометричної ідентифікації – це два взаємопов’язані та взаємодоповнюючі напрями. Основною перевагою статичних методів біометричної ідентифікації є їх відносна незалежність від психологічного стану користувача, малих затрат зусиль користувача, і, як наслідок, можливість організації біометричної ідентифікації великих потоків людей [2].

Біометрична ідентифікація на основі динамічних характеристик, як правило, простіша в реалізації, оскільки, як правило, не вимагає дорогого устаткування і може обмежуватися тільки програмним забезпеченням, яке вимагає мінімальну підтримку фахівця в процесі експлуатації [1].

Сама біометрія виникла ще в XIX столітті, в переважній більшості її використовували у криміналістиці для ідентифікації особи злодія. За тривалий час біометрія розвинулась у досить складний та ефективний апарат ідентифікації особи. При розгляданні біометричних системи існує декілька основних понять, які використовуються:

– біометрія – це прикладна область знань, яка використовується при створенні різних

автоматизованих систем контролю доступу до унікальних ознак, які притаманні кожній окремій людині;

– біометричні характеристики – це ознаки притаманні кожній особі, які є унікальними для цієї особи;

– біометричний зразок – це шаблон обраної біометричної характеристики;

– ідентифікація – перевірка наявності запропонованого ідентифікатора у переліку зареєстрованих;

– аутентифікація – перевірка приналежності особі ідентифікатора, який вона пред’явила ;

– реєстрація – це створення за будь-якою біометричною характеристикою (або декількома характеристиками) шаблона, який ставиться у

– відповідь до особи, яка реєструється.

Звідси зрозуміло, що біометрична ідентифікація надає одну беззаперечну перевагу на відміну від інших засобів ідентифікації – її неможливо загубити чи забути, вона завжди з особою і завжди незмінна. Завдяки саме цій особливості систем біометричної ідентифікації їх можливо використовувати для забезпечення безпеки інформації.

Ми вже зазначали, що кожній людині притаманні унікальні ознаки – біометричні ідентифікатори, за якими досить просто чітко ідентифікувати людину. Коли біометрична ідентифікація тільки почала розвиватися, люди знали та використовували лише три такі біометричні ідентифікатори – це відбитки пальців, голос та підпис. Причому тривалий час вважалось, що першими для ідентифікації почали використовувати підпис та голос, але пізніше стало відомо, що у давньому Єгипті для ідентифікації використовувались і відбитки пальців. Отже, таке тривале використання цих трьох біометричних ідентифікаторів призвело до того, що саме вони мають найбільш чіткі методи та методики їх використання. Потім, з розвитком медицини було з’ясовано, що людина має ще декілька унікальних біометричних ознак, які можливо використовувати для ідентифікації особи. Причому було також встановлено, що ці біометричні ідентифікатори людини можна поділити на дві групи – статичні (також називаються фізіологічними) та динамічні (також називаються психологічними):

– фізіологічні (статичні) – засновані на фізіологічній (статичній) характеристиці людини, тобто унікальних властивостях, які властиві їй від народження і є невід'ємними від неї;

– психологічні (динамічні) – засновані на поведінковій (динамічній) характеристиці людини, особливостях, характерних для підсвідомих рухів у процесі відтворення будь-якої дії.

Слід зазначити, що психологічні методи є менш надійними ніж фізіологічні. Сьогодні завдяки розвитку технологій крім відбитків пальців, голосу та підпису можна використовувати ще декілька біометричних ознак. До фізіологічних методів ідентифікації відносяться [1, 7, 11]:

1) За відбитками пальців;
2) За формою долоні;
3) За сітчаткою ока;
4) За геометрією обличчя;
5) За розташуванням вен на лицьовій стороні долоні;
6) За термограмою обличчя (розташування артерій під шкірою обличчя);
7) За райдужною оболонкою ока;
8) За геометрією вуха;
9) За допомогою ДНК.

Психологічних методів значно менше і до них відносяться:

1) За голосом;
2) За підписом (або почерком);
3) За клавіатурним почерком.

Поступово були виявлені й інші біометричні параметри, які дозволяють ідентифікувати особу з імовірністю, близькою до 100 відсотків. Кожний із цих біометричних ідентифікаторів має свої переваги та недоліки. Одні з них забезпечують стовідсоткову ідентифікацію, проте для них не існує ефективних способів реалізації, реалізація інших досить дорога або вони не забезпечують стовідсотковий результат. Проте усі біометричні ідентифікатори забезпечують точність, безпеку та надійність значно вище ніж парольна чи апаратна ідентифікація.

На сьогодні існує близько 20-ти біометричних ідентифікаторів, які можна використовувати, проте історично так склалось, що до найбільш розповсюджених методів біометричної ідентифікації відносяться способи, засновані на використанні наступних біометричних ідентифікаторів [1]:

- відбитки пальців;
- райдужна оболонка ока;
- сітківка ока;
- геометрія обличчя;
- геометрія долоні;
- почерк (або підпис);
- ідентифікація за голосом.

Таблиця 1.2 - Порівняння біометричних методів із загальних вимог

Біометрія	Універсальність	Унікальність	Сталість	Вимірюваність	Ефективність	Доступність	Захищеність
Відбиток пальця	С	В	В	С	В	С	В
Геометрія обличчя	В	Н	С	В	Н	В	Н
Форма кисті	С	С	С	В	С	С	С
Райдужка	В	В	В	С	В	Н	В
Сітківка	В	В	С	Н	В	Н	В
Динаміка підпису	Н	Н	Н	В	Н	В	Н
Розпізнавання по голосу	С	Н	Н	С	Н	В	Н
Клавіатурний почерк	Н	Н	Н	С	Н	С	С
Термографія обличчя	В	В	Н	В	С	В	В
Н низька С- середня В- висока							

Ці методи дозволяють ідентифікувати особу з досить високою ймовірністю. Крім цих біометричних ідентифікаторів сьогодні вже можна використовувати біометричну ідентифікацію на основі інших біометричних ідентифікаторів, які дозволяють забезпечити точність ідентифікації особи у межах близьких до 100 відсотків. До таких методів відносяться – ідентифікація на основі термо-грами обличчя, термограми долоні та геометрії вуха. Крім того, слід зазначити, що виявлено біометричний ідентифікатор, який дозволяє отримувати стовідсотковий результат під час проведення ідентифікації особи – це ідентифікація на основі ДНК людини. Проте цей метод має досить суттєвий недолік – він досить складний і для проведення ідентифікації буде потрібний значний обсяг часу.

Отже, можна зробити висновок, що усі біометричні ідентифікатори дозволяють здійснювати ідентифікацію особи, проте кожний із них має свої особливості, переваги та недоліки. На рисунку 1.2 показана загальна класифікація методів біометричної ідентифікації.

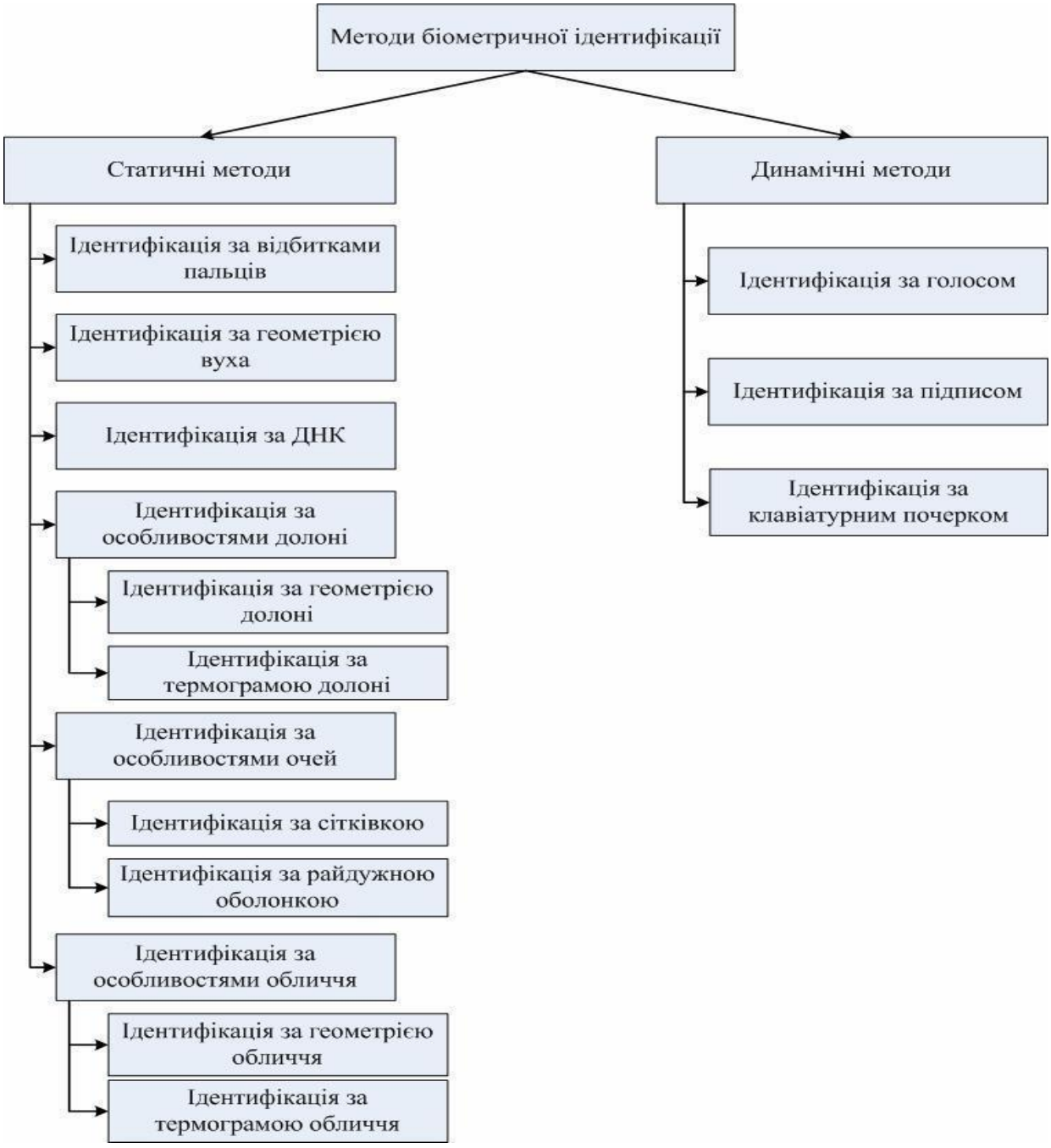


Рисунок 1.2 – Класифікація методів біометричної ідентифікації

Основні статичні біометричні характеристики, а також види їх реалізації наведені в таблиці 1.3.

Таблиця 1.3 – Реалізація фізіологічних біометричних характеристик

Біометрична характеристика	Реєструючий пристрій	Зразок	Досліджувані риси
Геометрична будова руки	Запатентований настінний пристрій	Тривимірне зображення зверху і боків кисті	Висота і ширина кісток і суглобів кисті і пальців
Відбиток пальця	Периферійний пристрій настільного комп'ютера, карта стандарту PC card, миша, мікросхема або зчитувальний пристрій, вбудований в клавіатуру	Зображення відбитку пальців (оптичне, на кремнієвому фотоприймачі, ультразвукове, або безконтактне)	Розташування і напрям гребінчастих виступів і розгалужень на відбитку пальців, дрібні деталі
Особливості малюнка сітківки ока	Запатентований настільний або настінний пристрій	Зображення сітківки	Розташування кровоносних судин на сітківці
Райдужна оболонка ока	Відеокамера, здатна працювати в інфрачервоному діапазоні, камера для ПК	Чорно-біле зображення райдужної оболонки ока	Смужки і борозенки на райдужній оболонці ока
Портрет обличчя	Відеокамера, камера для ПК, фотоапарат	Зображення особи (оптичне або теплове)	Відносне розташуванняі форма носа, розташування скул

На стадії розробки знаходяться нові біометричні технології, пов'язані з іншими фізіологічними характеристиками.

Порівняння ДНК — це найдосконаліша на сьогодні біометрична технологія, що дає прямий доказ ідентичності особи, — крім однояйцевих близнят, в яких однаковий генотип. Цей метод інколи називається дактилоскопією ДНК, що збиває з пантелику і вводить в оману, оскільки відбитки пальців не «проникають до рівня генома». Біометричні системи, засновані на порівнянні ДНК, можуть бути введені в дію лише згодом.

Відбиток долоні — в цій системі використовується розташування ліній на долоні людини, повністю аналогічно технології, що використовує відбитки пальців.

Судинні рисунки — розташування вен в різних частинах тіла людини, включаючи зап'ястя і тильну сторону долоні.

Сигнали, що виробляються серцем (мозком, легенями), — в цій системі користувач торкається датчика «біодинамічного підпису» («Biodynamic signature» sensor) і залишається з ним в контакті деякий час (залежно від точності вимірів — до 8 секунд). За цей час датчик ідентифікує індивідуальні параметри людини.

Використання даної технології отримало значне поширення у системі автоматичної ідентифікації за відбитками пальців (AFIS-Automatic Fingerprint Identification System), що

використовується поліцією Сполучених Штатів та країнах Європи і понад 30 країнах світу. Перевагами доступу за відбитками пальців є простота використання, зручність і надійність. Весь процес ідентифікації займає мало часу і не вимагає зусиль від тих, хто використовує дану систему доступу. Дослідження також показали, що використання відбитка пальця для ідентифікації особи є найбільш зручним з усіх біометричних методів. Ймовірність помилки при ідентифікації користувача набагато менше порівняно з іншими біометричними методами. Крім того, пристрій ідентифікації за відбитком пальця не вимагає багато місця на клавіатурі або в механізмі.

Сьогодні основні напрями використання систем біометричної ідентифікації – це:

– системи контролю доступу;

– системи інформаційної безпеки (контроль доступу до мережевих ресурсів, робочих станцій);

– системи голосування;

– системи обліку робочого часу та реєстрації співпрацівників;

– системи переведення електронних платежів;

– системи громадської ідентифікації (перетин державних кордонів, видача віз у посольствах);

– авторизація на різних віртуальних та інформаційних сервісах;

– системи аутентифікації на Web-ресурсах.

Отже, попит на системи біометричної ідентифікації досить великий и використовуються вони у досить різних сферах. Згідно з оцінками різних фінансових аналітиків загальний обсяг ринку біометричних технологій (з урахуванням негативних ринкових тенденцій) за 2010 рік становив 1,5…1,6 мільярдів доларів. На рисунку 1.3 показано діаграму розвитку ринку біометричних технологій за період з 2006 року по 2014 рік.

Взагалі для розв’язання задачі ідентифікації особи у кожному з зазначених напрямів можна використовувати будь-який метод біометричної ідентифікації розглянутий у попередньому розділі, проте в залежності від конкретних умов задачі ідентифікації не завжди можна використовувати будь-який метод ідентифікації. Також значний вплив на популярність системи біометричної ідентифікації здійснює розвиток того чи іншого методу. Тобто метод може надавати ймовірність ідентифікації близьку до ста відсотків, але при цьому відсутні пристрої для його реалізації або чітко не визначена методика реалізації методу ідентифікації.

Також на інтенсивність використання методу біометричної ідентифікації впливає його популярність, наприклад, ідентифікація за відбитками пальців ві-дома досить давно, тому переважна більшість систем біометричної ідентифікації використовує саме її. Інший приклад – це ідентифікація за формою вуха, цей метод розроблено досить недавно і тому про нього

досить мало відомо і відповідно систем, які використовують цей метод також дуже мало, хоча він дає ймовірність ідентифікації близьку до 100 відсотків.

Рисунок 1.3 – Діаграма розвитку ринку біометричних технологій

Трохи інша ситуація з ідентифікацією на основі ДНК – і метод досить відомий, і імовірність ідентифікації становить 100 відсотків, проте складність самого методу та час проведення ідентифікації призвели до того, що даний метод використовується тільки у криміналістиці. Отже, можна зробити наступний висновок – на сьогодні, використовуються усі методи ідентифікації, проте деякі використовуються значно частіше ніж інші. На рисунку 1.4 показано діаграму використання методів біометричної ідентифікації.

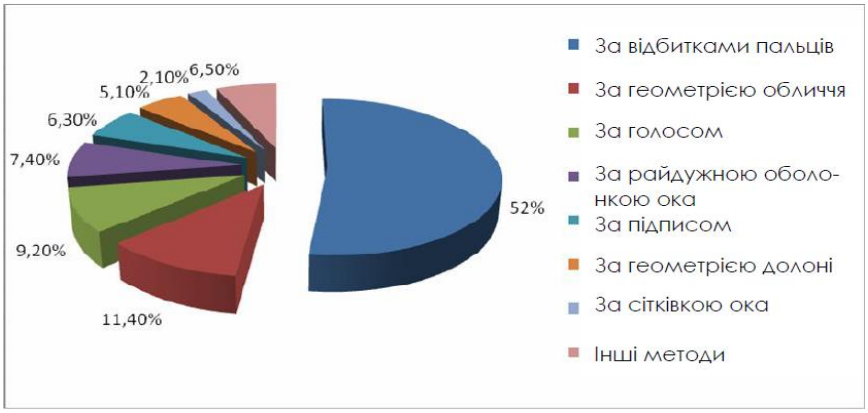


Рисунок 1.4 – Діаграма використання методів біометричної ідентифікації

У загальному випадку системи біометричної ідентифікації працюють за наступним принципом. Усі системи спочатку працюють у режимі реєстрації, тобто спочатку система повинна отримати та зберегти певний біометричний ідентифікатор, за допомогою якого

надалі буде здійснюватися ідентифікація користувача. В залежності від типу системи вона може використовувати декілька біометричних ідентифікаторів (наприклад, якщо здійснюється ідентифікація за відбитками пальців, або за параметрами ока). Після отримання біометричного ідентифікатора система перетворює його за допомогою відповідних засобів в електронний вигляд. Ця стадія роботи системи біометричної ідентифікації називається реєстрація, тобто система отримує первісну інформацію, необхідну для її подальшої роботи. Звичайно система біометричної ідентифікації не зберігає зображення відбитка пальця, сітківки ока, геометрії долоні і т. ін.

У системі зберігається так званий шаблон ідентифікатора, який являє собою одну або декілька цифрових послідовностей, які були отримані під час оброблення біометричного ідентифікатора. Тобто, біометричний ідентифікатор, який надав користувач через спеціальний пристрій–реєстратор перетворюється в електронний вид, який потім проходить декілька стадій оброблення за різними алгоритмами (тип алгоритму та кількість обробок залежить від типу біометричного ідентифікатора), внаслідок чого отримується шаблон, за допомогою якого потім здійснюється безпосередньо процедура ідентифікації користувача.

У таблиці 1.4 представлено порівняння біометричних методів по приватним вимогам, що пред'являються до систем електронного підпису [16].

Таблиця 1.4 - Порівняння біометричних методів по приватним вимогам, що пред’являються до систем електронного підпису

Біометричний метод	Ціна	Зручність використання	Експлуатаційні характеристики
Відбиток пальця	С	В	С/В
Обличчя	С	Н	С
Форма кисті	В	С	С
Райдужка	В	В	С
Сітківка	В	Н	С
Динаміка підпису	С	В	С
Розпізнавання по голосу	Н	В	Н
Клавіатурний почерк	Н	С	Н
Судини кисті	С	В	С
Термограмма лиця	С	Н	С
	Н- низька С- середня В- висока		

Ціна низька для всіх методів, які не потребують спеціального апаратного забезпечення; висока для систем розпізнавання за формою кисті, сітківці, і райдужці, оскільки потрібно спеціальне дороге оптичне обладнання. Незручно використовувати пристрої, які вимагають

інтерактивне управління користувачем, наприклад, коли користувач повинен помістити своє обличчя, райдужку або сітківку в рамку, яка зазвичай відображається на дисплеї пристрою сканування.

Зручно використовувати методи, які не вимагають ніякого зворотного зв'язку (наприклад, натискання пальцем на сенсор, друк слова, проголошення фрази). Інші біометричні методи використовують планшети, електронне перо (по розпізнавання динаміці підпису) або оптичне обладнання, вимагає середніх експлуатаційних витрат.

Найдорожчі технології не обов'язково є найбільш точними. З усіх наведених останні 25 років найбільшу увагу приділялася ідентифікації за відбитками пальців і розпізнавання голосу. Не так давно в зв'язку зі змінами вимог широко вивчаються ідентифікація по обличчю і райдужці. Привабливість систем ідентифікації по райдужній оболонці можна досягти шляхом зниження вартості системи.

Інший важливий фактор, що враховується при розробці систем біометричної ідентифікації - середовище використання. Всі методи підходять для керованого середовища будинку або офісу. Методи, що вимагають використання громіздкого або крихкого сенсора, незручні для мобільних додатків. Пристрої ідентифікації в громадському місці, такі як банківські термінали, повинні розроблятися в більшій мірі з точки зору довговічності та міцності; в такому середовищі краще використовувати пасивну біометрію (без прямої взаємодії з користувачем) або біометричні методи, в яких використовуються адаптивні сенсори. Частота виконання ідентифікації впливає на вибір відповідного методу. У середовищі, де ідентифікація виконується часто (наприклад, в банках), вимоги відрізняються від вимог, що пред'являються там, де ідентифікація виконується рідко. Для середовища з частою ідентифікацією підходять тільки ті біометричні методи, які досить швидкі і вимагають мінімального взаємодії з користувачем. Порівняння біометричних методів по зручності з різними додатками наведено в таблиці 1.5.

Наведений аналіз представляє розробку методу біометричної ідентифікації в термінах спеціальних вимог, що пред'являються середовищем використання пристрою ідентифікації. З вищесказаного можна зробити висновок, що не існує ідеального біометричного методу.

Всі біометричні методи мають відповідні переваги та недоліки. Однак, деякі біометричні методи більш зручні, ніж інші в певних програмах. Найбільш важливими характеристики методу ідентифікації є такі:

- захищеність біометричного методу (універсальність, унікальність,
- ефективність, вимірність, стійкість до спроб обману, механічна міцність);
- доступність для користувача;
- вартість;

– простота використання.

Таблиця 1.5 - Порівняння біометричних методів по зручності з різними додатками

Біометрія	Середовище		
	Дім/офіс	Мобільне	Громадське місце
	(ПК/робоча станція/лептоп)	(довільне місце) (мобільний телефон, лептоп)	(банківський термінал/платіжний термінал
Відбиток пальця	Так	Так	Так
Геометрія обличчя	Так	Так(за виключенням телефона)	Так
Форма кисті	Так	Ні	Незручно
Райдужка	Так	Ні	Так
Сітківка	Незручно	Ні	Ні
Динаміка підпису	Так	Незручно	Незручно
Розпізнавання по голосу	Так	Так	Ні (шум)
Клавіатурний почерк	Так	Так	Ні (не скрізь є клавіатури)
Судини кисті	Так	Ні	Ні

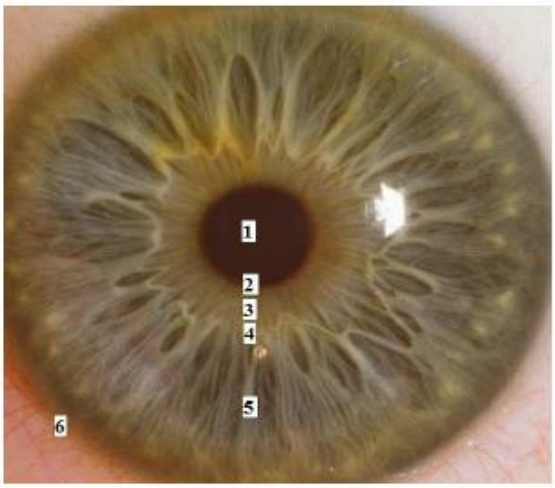
Метод ідентифікації по райдужній оболонці ока має всі перераховані характеристики. Порівняння біометричних методів по їх придатності для багаторазової ідентифікації наведено в таблиці 1.6.

Таблиця 1.6 - Порівняння біометричних методів по їх придатності для багаторазової ідентифікації

Біометричний метод	Придатність для великої кількості ідентифікацій
Відбиток пальця	Добра, метод простий в використанні
Обличчя	Добра
Форма кисті	Середня/метод мало практичний
Райдужка	Середня/метод мало практичний
Сітківка	метод мало практичний
Динаміка підпису	Добра,сильна аналогія між електронним і рукописним підписом
Розпізнавання по голосу	Середня
Клавіатурний почерк	метод мало практичний;схожий, але більш дорогий чим ПІН-код
Судини кисті	Середня/метод мало практичний
Термограмма лиця	Добра

1.3 Око як об'єкт розпізнавання

Райдужна оболонка ока, райдужка (iris, давньогрецьке ≪веселка≫) – тонка рухома діафрагма ока у хребетних. Вона становить саму передню частину оболонки очного яблука і має вигляд кругової, вертикальної пластини з круглим отвором, називаним зіницею. Райдужка відіграє роль діафрагми, яка регулює кількість світла, що надходить в око, для чого зіниця при сильному світлі звужується, а при слабкому розширюється. Зовнішнім своїм краєм райдужка з'єднана з війковими тілом і склерою, внутрішній же її край, що оточує зіницю, вільний [20]. Приклад зображення райдужної оболонки наведено на рисунку 1.5.



(1-зіниця, 2-пігментна межа зіниці, 3-зіничний пояс, 4 – автономне кільце, 5 –циліарний пояс, 6- корінь райдужки)

Рисунок 1.5 - Зображення райдужної оболонки

Розміри і форма. Райдужка має кільцеву форму і розміри в середньому по горизонталі A ≈ 12.5 міліметрів і по вертикалі B ≈ 12.0 міліметрів [20]. Зовнішній контур райдужної оболонки, її межа з склерою - майже ідеальний еліпс, і може бути наближено представлена колом. Зовнішній контур райдужної оболонки постійний і має практично однакову форму і розміри для всіх людей. Внутрішня межа райдужки задається зіницею. У здорової людини зіниця кругла, а його центр кілька зміщений щодо центру райдужки у напрямку до кінчика носа [20, 21]. Досить часто зустрічаються незначні децентрації і відхилення форми зіниці від кругової (рис. 1.6).

Децентрація і відмінність від кругової форми визначаються патологіями, і наростають з віком. Варіації положення центру і відносини радіуса зіниці в заданому напрямку до середнього можуть досягати 20% для однієї людини.

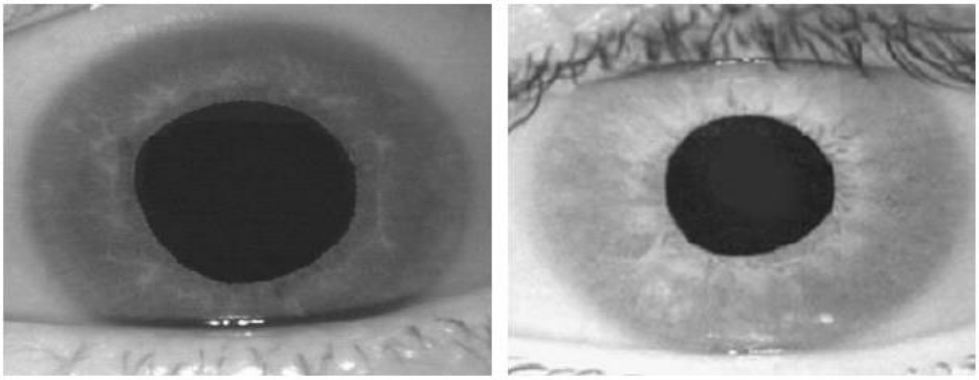


Рисунок 1.6 - Приклади некруглих зіниць

Проведені статистичні дослідження зображень райдужної оболонки дозволяють сформулювати взаємні обмеження на розміри і положення зіниці і райдужної оболонки:

$$r_p > \frac{1}{7} r_I,$$
$$r_p < \frac{3}{4} r_I,$$
$$r_p > d = \sqrt{(x_I - x_p)^2 + (y_I - y_p)^2},$$
$$2(r_I - r_p - d) > r_I - r_p + d,$$

де (xp; yp) — координати центру кола, апроксимуючи зіницю, rp — радіус цього кола, (xI ; yI), rI — координати центра і радіус кола райдужки, d — відстань між центрами кіл зіниці і райдужної оболонки. Перша з нерівність (1.1) значить, що радіус райдужки не може перевершувати радіус зіниці більш ніж в 7 разів. Друга нерівність дає обмеження з іншого боку: зіниця не може займати більше 75% райдужки. Третє нерівність визначає, що центр райдужки лежить всередині зіниці.

Четверте - відрізки між колами зіниці і райдужної оболонки відсічені прямою, яка проходить через їх центри, не відрізняються по довжині більш ніж в два рази.

Зображення райдужки. Зображення райдужки обумовлений радіально розташованими нитками (трабекулами) переплетеними між собою сполучною тканиною, що йдуть в різних напрямках, і унікальний для кожної людини. Малюнок райдужки у більшості людей малоконтрастний (діапазон яскравості точок зображення райдужної оболонки набагато менший діапазону яскравостей зображення ока, що включає темну зіницю і світлу склеру). Крім того, деякі типи райдужки мають тонку текстуру (на них немає великих яскравих або темних елементів). Це висуває високі вимоги до системи реєстрації зображення. Залежно від довжини хвилі світла, в якому реєструється райдужка, на ній виявляються різні деталі, причому їх вираженість залежить від типу очей. Наприклад, більшість світлих очей дає

найбільш чіткий малюнок у видимому світлі. При переході в інфрачервоний діапазон цей малюнок поступово розмивається і майже зникає на довжинах хвиль 900 нм. Навпаки, структури темних очей, характерних для жителів екваторіального поясу, практично непомітні в видимому світлі, але чітко проявляються в інфрачервоному діапазоні. Тому до цих пір залишається не вирішене питання, яка довжина хвилі оптимальна.

Стійкість зображення. Формування структур райдужки в основному закінчується на восьмом місяці внутрішньоутробного розвитку і в подальшому житті практично не зазнає змін, за винятком викликаних травмами або патологіями очей. Зміна кольору райдужної оболонки (насичення пігментом) триває в перші кілька років життя, але, не змінює форму її елементів. Остаточно колір очей встановлюється до 10-12 років. У літніх людей очі іноді бліднуть, що пов'язано з депігментацією, яка відбувається через розвитку склеротичних і дистрофічних процесів. В цілому, протягом великого періоду життя форма елементів райдужки залишається постійною [20-24]. Це дозволяє говорити про високу стійкість зображення райдужної оболонки.

Інформативність. Оскільки райдужка є практично плоским об'єктом простої форми і незмінних розмірів, варіації її зображення, створювані зміною умов реєстрації, малі (щодо інших біометричних даних) і легко можуть бути компенсовані, дозволяючи відокремити інформацію, яка дійсно відноситься до індивідуальності даної райдужки, від випадкових спотворень при спостереженні. Райдужка має складний малюнок, що складається з багатьох деталей. Тому з зображення райдужної оболонки можна отримати велику кількість параметрів (висока інформативність). Як показано в [25], інформаційна ємність зображення райдужної оболонки радіусом 200 пікселів становить не менше 200 біт.

Варіації зображень райдужної оболонки. В ідентифікації по райдужці, як і в будь-якій проблемі розпізнавання, основна складність полягає в отриманні параметрів об'єкта, унікальних в класі йому подібних і інваріантних щодо умов реєстрації та зміни самого об'єкта. Таким чином, параметри малюнка райдужної оболонки необхідно витягти з її зображення, відсіявши варіації двох класів: варіації самої райдужної оболонки і зміни умов зйомки.

Зміни райдужки як такої. Зміни РОО можна розділити на довготривалі зміни малюнка і швидкі зміни форми, які визначаються скороченням / розширенням зіниці. Райдужна оболонка, виконуючи функцію діафрагми, володіє великою рухливістю. Основа райдужки складається з сполучної тканини, що має архітектуру решітки, в яку вставлені судини, що йдуть радіально, від периферії до зіниці. Ці судини разом з сполучною тканиною утворюють еластичний скелет райдужки, що дозволяє їй легко змінюватися за величиною. Самі рухи райдужної оболонки здійснюються м'язовою системою, що залягає в її товщі. Ця система складається з м'язових волокон, які частково розташовуються кільцеподібно навколо зіниці,

утворюючи м'яз, звужують зіницю (сфінктер), а частина розходяться радіально від зіничного отвору і утворюють м'яз, який розширює зіницю (дилататор). М'язи діють взаємообернено: при звуженні зіниці сфінктер розтягує дилататор, а при розширенні дилататор розправляє сфінктер. Завдяки цьому досягається точність і швидкість рухів райдужки. Сфінктер іннервується парасимпатичною нервовою системою, а дилататор - симпатичною. Під впливом змін освітленості, при переміщенні фокуса уваги і в залежності від фізичного та психічного стану зіниця постійно змінює свій розмір. Зіниця також здійснює аперіодичні мимовільні рухи (гіппус). В результаті цих рухів зіниці змінює розмір райдужки і, відповідно, деформується її малюнок.

Зміни умов реєстрації. Рогівка ока відображає навколишні предмети. Ці відображення, особливо відблиски від джерел світла, перекривають картину райдужки і можуть створювати варіації яскравості зображення у багато разів більші, ніж інформативні елементи райдужки. Тому стає неможливим не використовувати власне підсвічування. У цьому полягає принципова відмінність розпізнавання райдужної оболонки ока від систем, що використовують зображення обличчя. Для особи стороння засвітка також є великою проблемою, проте, на зображенні особи, освітленого стороннім, випадково розташованими джерелом, можна виявити інваріантні ознаки, як то: розміри і форму елементів особи, його рельєф і т.п., а для райдужки це неможливо. Підсвічування повинна давати в області реєстрації райдужок освітленість в кілька разів перевищує ту, що створюється сторонніми джерелами. Видиме світло з такою інтенсивністю викликає велику незручність. Тому у всіх сучасних системах використовується інфрачервоне підсвічування.

Просторове положення щодо камери. Так як райдужка є об'єктом невеликого розміру, то для отримання її зображення прийнятної якості (в фокусі і достатнього дозволу) потрібно дуже точне позиціювання очей (голови) користувача. Наприклад, навіть при отриманні зображення райдужної оболонки з діаметром 100 пікселів, що визначається стандартом [26] як низькоякісне, на камері з дозволом 1000x800 пікселів, очей користувача повинен потрапити в зону 9x7 сантиметрів.

Кутова орієнтація відносно камер. Поворот щодо осі - променя зору камери. Точне визначення кута цього повороту, а отже, нормування можливі для бінокулярних систем або монокулярних з допоміжною камерою, яка знімає особу метою позиціонування. У монокулярной системі можливе кутове нормування по положенню слізного мішка ока, але методи пошуку слізного мішка на зображенні ненадійні, а визначений кут має похибки в кілька градусів. Таким чином, в монокулярной системі при порівнянні зображень райдужок потрібно виставляти еталон декількома зображень, поверненим на різні кути в межах можливих змін нахилу голови користувача. Даний факт в відповідне число разів збільшує час, витрачений на порівняння, ймовірність помилкового допуску.

Для більш чіткого розуміння проаналізуємо найбільш поширені системи на ринку СКУД у таблиці 1.7.

Провівши аналіз найбільш поширених систем ідентифікації та аутентифікації по РОО, зазначимо, що у них всіх без виключення обмежена кількість записів в БД.

Таблиця 1.7 - Системи найбільш поширені на ринку СКУД з використанням райдужки

	Параметри					
Система	Фокусна відстань, м	Час на зйомку, с	Максимальна кількість записів в БД	Пропускна можливість системи користувачів за хв.	FAR	FRR
LG -3000	0.1	0.04	1000	10	0,00066	0,00078
OKI IRISPASS-WG	0.45	30	1000	1-2	0,00066	0,00078
Panasonic BM-ET300	0.35	0.5	10000	10	0,00066	0,00078
SecurimetricsPier 2.3	0.12	0.008	2000	30	0,00066	0,00078
Sarnoff IOM	3	8	50000	30	0,00066	0,00078
Циркон 4	0.4	2	2000	12-30	0,00066	0,00078
Eyswipe- Nano	0.3	2	50000	20	0,00066	0,00078

Отже, сучасні вимоги такі, що необхідна здатність алгоритмів розпізнавання райдужної оболонки працювати в ідентифікаційному режимі пошуку "один до багатьох", в якому особа попередньо не декларуються за допомогою магнітних карт або інших ідентифікаторів (документів), і алгоритми повинні самостійно визначити особистість, здійснивши повний інтенсивний пошук в базі зареєстрованих даних. Таким чином, більшість біометричних технологій спроможні тільки на роботу в верифікаційному режимі порівняння "один до одного". У такому режимі особа спочатку декларується, і програмою для прийняття рішення "так / ні" досить виконати зіставлення з одним зареєстрованим шаблоном.

1.4 Висновки до першого розділу

Порівняння різних біометричних методів ідентифікації показало, що за сукупністю якостей широке використання ідентифікації по райдужній оболонці ока має помітні переваги перед більшістю інших біометричних характеристик і необмежені перспективи застосування в системах безпеки. Однак суттєвим недоліком таких систем є алгоритмічна складність і високі вимоги до обчислювальних ресурсів, а також висока вартість. У зв'язку з цим, актуальні дослідження в області розробки нових методів аналізу і розпізнавання зображення райдужної оболонки та сітківки ока, які при стійкості до різних видів перешкод, що виникають при зйомці, дозволили б поліпшити характеристики системи і знизити вимоги до апаратури, зменшивши її вартість.

1.5 Постановка мети і задач дослідження

У атестаційній магістерської роботі треба вивчити та дослідити залежності між індивідуальними біометричними параметрами людини для її унікальної ідентифікації, розробка відповідного метода, моделі, а також вивчення та підвищення ефективності методів обробки даних в системах ідентифікації та аутентифікації користувачів по райдужній оболонці ока.

Метою роботи є розробка модифікованого метода ідентифікації людини за райдужною оболонкою ока на основі перетворення Ерміта [5-7], який використовує локальні характеристики райдужної оболонки.

Для досягнення поставленої мети необхідно вирішити такі задачі:

– проаналізувати сучасні підходи, методи і системи біометричної ідентифікації та аутентифікації користувачів;

– дати опис перетворенню Ерміта стосовно до задачі обробки зображень;

– вирішити задачу ідентифікації по райдужній оболонці ока;

– описати та розробити метод розпізнавання людини по райдужній оболонці ока на основі згорток з функціями перетворення Ерміта;

– провести ряд експериментів на базі даних CASIA-IrisV3 [8].

2 СИСТЕМИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

2.1 Принципи функціонування системи біометричної ідентифікації

У попередньому розділі ми з'ясували, що системи біометричної ідентифікації стають доволі розповсюдженими. Це пов'язано з двома факторами: по-перше, – це те, що системи біометричної ідентифікації більш надійні, а, по-друге, – ціни на подібні системи почали знижуватися. Цілком зрозуміло, що кожна система біометричної ідентифікації має свої особливості, які цілком залежать від типу біометричного ідентифікатора, який використовується у тій чи іншій системі. Проте всі вони мають і деякі спільні риси, які притаманні усім системам. У першу чергу – це принцип функціонування та загальна схема роботи системи біометричної ідентифікації [2, 3].

У загальному випадку системи біометричної ідентифікації працюють за наступним принципом. Усі системи спочатку працюють у режимі реєстрації, тобто спочатку система повинна отримати та зберегти певний біометричний ідентифікатор, за допомогою якого надалі буде здійснюватися ідентифікація користувача. В залежності від типу системи вона може використовувати декілька біометричних ідентифікаторів (наприклад, якщо здійснюється ідентифікація за відбитками пальців, або за параметрами ока). Після отримання біометричного ідентифікатора система перетворює його за допомогою відповідних засобів в електронний вигляд. Ця стадія роботи системи біометричної ідентифікації називається реєстрація, тобто система отримує первісну інформацію, необхідну для її подальшої роботи.

Звичайно система біометричної ідентифікації не зберігає зображення відбитка пальця, сітківки ока, геометрії долоні і т. ін. У системі зберігається так званий шаблон ідентифікатора, який являє собою одну або декілька цифрових послідовностей, які були отримані під час оброблення біометричного ідентифікатора. Тобто, біометричний ідентифікатор, який надав користувач через спеціальний пристрій–реєстратор перетворюється в електронний вид, який потім проходить декілька стадій оброблення за різними алгоритмами (тип алгоритму та кількість обробок залежить від типу біометричного ідентифікатора), внаслідок чого отримується шаблон, за допомогою якого потім здійснюється безпосередньо процедура ідентифікації користувача.

У будь-якому випадку незалежно від типу біометричного ідентифікатора, який застосовується системою, загальний алгоритм функціонування системи біометричної ідентифікації може бути наданий у вигляді, показаному на рисунку 2.1, а спрощена структурна схема системи біометричної ідентифікації показана на рисунку 2.2.

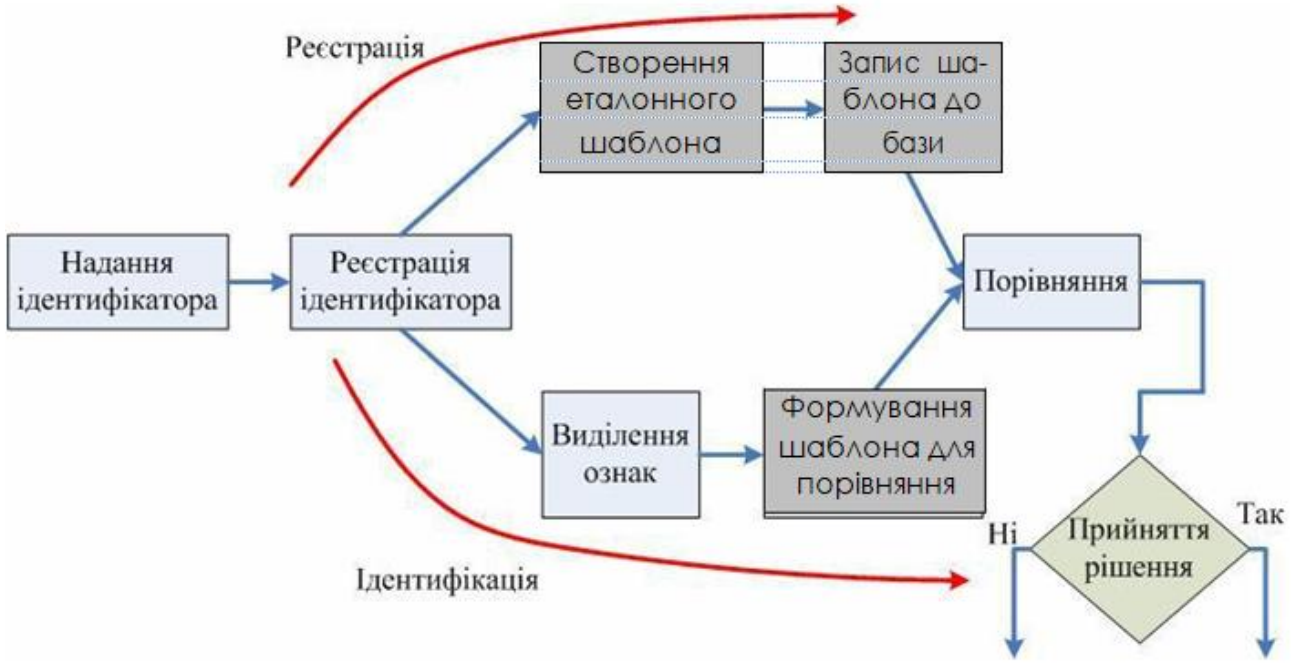


Рисунок 2.1 – Загальний алгоритм функціонування систем біометричної ідентифікації

Рисунок 2.2 – Спрощена структурна схема системи біометричної ідентифікації

Після того, як процес реєстрації здійснено, система здатна проводити процес ідентифікації, тобто встановлення відповідності особи та визначення її прав на виконання тих чи інших дій.

Слід зазначити, що процес ідентифікації у біометричних системах в цілому поділяється на два види – ідентифікацію та верифікацію. Звичайно різниця між цими двома поняттями надто тонка і досить часто один процес плутають з іншим. Проте слід чітко їх відрізняти, якщо підходити до визначення цих процесів, то можна зазначити, що:

– *ідентифікація* – це порівняння типу “один-до-багатьох”, тобто здійснюється порівняння наданого біометричного ідентифікатора з усіма шаблонами біометричних ідентифікаторів, які є у базі. У результаті цього порівняння вияв-ляється декілька найбільш

схожих шаблонів (ті, які мають найбільшу вірогідність відповідності), а потім за допомогою будь-якого математичного критерію приймається рішення про найбільш ідентичний шаблон. Тобто у даному випадку система ідентифікації дає відповідь на питання: «Хто ви?». У даному режимі система ідентифікації може працювати повністю автоматично, або у контакті з людиною на етапі вибору найбільш ідентичного шаблона;

– *верифікація* – це порівняння типу “один-до-одного”, тобто здійснюється порівняння наданого ідентифікатора з відповідним шаблоном з бази. Однак в даному випадку необхідно надати додатковий ідентифікатор, який дозволяє вибрати з бази відповідний шаблон. Наприклад спочатку вводиться логін корис-тувача, а потім надається відповідний біометричний ідентифікатор. У даному випадку система відповідає на питання: «Чи дійсно ви та людина за яку себе видаєте?». У цьому режимі система ідентифікації працює набагато швидше та в повністю автоматичному режимі.

Цілком зрозуміло, що система біометричної ідентифікації здатна працювати у двох режимах, проте більшість систем працює саме у режимі верифікації. Необхідно зазначити, що може виникнути ситуація, коли еталонний зразок біометричного ідентифікатора, який зберігається у базі, не буде збігатися зі знов запропонованим біометричним ідентифікатором. Це може бути пов’язано,

У першу чергу, з тим, що при повторному наданні біометричного ідентифікато-ра користувач трохи змінив геометричні умови його надання, наприклад при ідентифікації за відбитками пальців він міг докласти пальця до сканера під іншим кутом, або при ідентифікації за сітківкою ока він міг нахилити голову і таким чином змінити кут падіння світла в око. Цілком зрозуміло, що спосіб та методи покращення наданого біометричного ідентифікатора залежать від типу самого біометричного ідентифікатора, тобто, якщо ідентифікація відбувається за відбитками пальців використовуються одні методи, якщо ідентифікація відбувається за райдужною оболонкою ока, або сітківкою, то використовуються зовсім інші методи.

2.2 Формальна модель процесу ідентифікації біометричною системою

Розглянемо яким чином здійснюється формалізація процесу ідентифікації у системах біометричної ідентифікації. Для того, щоб побудувати модель біометричної ідентифікації нам, по-перше, необхідно мати множину об’єктів ідентифікації; по-друге, множину (простір) ознак, які використовуються для ідентифікації, та правило на основі якого будуть прийматися рішення про ідентифікацію. На рисунку 2.3 показана формальна модель процесу біометричної

ідентифікації.

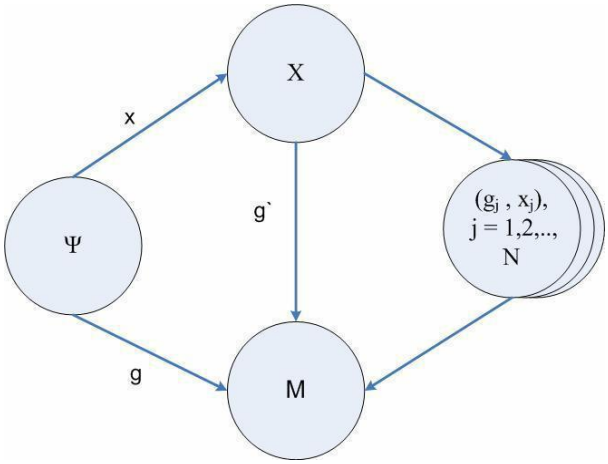


Рисунок 2.3 – Формалізація процесу біометричної тифікації

Позначимо через Ψ – множину об'єктів ідентифікації, де ω: ω~∈Ψ – об'єкт ідентифікації, тоді g(ω): Ψ → M, де M {1,2,...m} – індикаторна функція, яка поділяє простір об'єктів Ψ на m класів Ψ_1 , Ψ_2 ,..., Ψ_m , які не перетинаються. Індикаторна функція звичайно системі невідома.

Визначимо через X – простір ознак (признаків, характеристик) ідентифікатора. Тоді x(ω): Ψ → X – це функція, яка ставить у відповідність кожному об'єкту ω точку x(ω) у просторі ознак. Вектор x(ω) – це образ об'єкта, який сприймає система.

У просторі ознак визначено множини точок $K_i \subset X$, i = 1,2,..., m , які не перетинаються та відповідають об'єктам одного класу. Тоді прийняття рішення про ідентифікацію буде відбуватися за правилом g`(x): X → M, тобто здійснюється оцінка для g (ω) на основі x(ω), тому можна записати що g(x) = g(x(ω)).

Нехай $x_j = x(\omega_j)$; j = 1,2,...; N – доступна системі інформація про функції g(ω) та x(ω), але самі ці функції системі невідомі. Тоді (g_j , x_j), j = 1,2,..., N є множина можливих прецедентів (тобто множина можливих відповідей на питання ідентифікації). Отже, у даному випадку задача полягає в побудові такого правила g`(x), яке дозволить проводити ідентифікацію з мінімальним числом помилок. Для того щоб досягти мінімальної кількості помилок, нам необхідно внести декілька припущень. Якщо вважати простір доступних системі ознак евклідовим, тобто $X = R_l$, то якість роботи правила ідентифікації можна виміряти частотою виникнення вірних рішень щодо ідентифікації. Це можливо, якщо множину об'єктів Ψ наділити певною вірогідністю. Тобто для кожного об'єкта розрахувати ймовірність ідентифікації (найбільш частіше визначається дослідним шляхом). Тоді розв'язання задачі може бути записане у вигляді: min P{g`(x(ω)) ≠ g(ω)}.

2.3 Параметри системи біометричної ідентифікації

При оцінці ефективності роботи будь-якої системи ідентифікації використовуються деякі параметри або характеристики, які характеризують роботу системи з того чи іншого боку. Звичайно системи біометричної ідентифікації мають наступні параметри [7, 9, 10, 11]:

1) Помилка першого виду FRR (False Reject Rate) – ймовірність того, що система ідентифікації не зможе ідентифікувати зареєстрованого користувача (або часто говорять, що система приймає «свого» за «чужого»).

2) Помилка другого роду FAR (False Accept Rate) – ймовірність того, що система ідентифікації ідентифікує не зареєстрованого користувача (тобто прийме «чужого» за «свого»).

3) Час спрацьовування – показує скільки проходить часу з моменту надання біометричного ідентифікатора і до моменту надання доступу або відмови у доступі.

4) Тип зчитувача біометричного ідентифікатора – контактний або дистанційний.

5) Кількість біометричних ознак, які використовуються для ідентифікації.

6) Стійкість системи до муляжів (штучні копії біометричних ідентифікаторів).

7) Автономність – характеризує функціональну незалежність системи від апаратно-програмних засобів.

8) Можливість централізовано керувати значною кількістю територіально розподілених пристроїв ідентифікації.

Отже, можна дійти висновку, що ідеальна система біометричної ідентифікації повинна мати наступні характеристики:

- помилки першого та другого роду FFR = 0 і FAR = 0;
- час спрацьовування – декілька мілісекунд;
- кількість зареєстрованих користувачів необмежена;
- зчитування біометричного ідентифікатора відбувається дистанційно;
- абсолютна стійкість до муляжів;
- повна автономність та централізоване керування.

Цілком зрозуміло, що досягти ідеальної системи поки що неможливо, тому необхідно виділити найбільш критичні параметри і покращувати саме їх. До таких параметрів, в першу чергу, відносяться ймовірність помилок першого та другого виду FFR та FAR. Крім цих двох параметрів також виділяють ще два додаткових параметри, які відносяться до процесу реєстрації користувачів, – це помилка реєстрації FTE (Failure to Enroll Rate) та ймовірність помилки збирання даних FTA (Failure to Acquire Rate). FTE (Failure to Enroll Rate) визначає

відсоток людей, які не можуть бути зареєстровані у системі через будь які перешкоди. FTA (Failure to Acquire Rate) визначає ймовірність того, що людина взагалі не зможе зареєструватися у системі та проходити подальшу ідентифікацію. Звичайно це відбувається з людьми, які мають слабко виражені біометричні ідентифікатори, або якщо ідентифікатор було пошкоджено хворобами (напри-клад, катаракта ока).

У загальному випадку значення цих параметрів задається при настройці системи, проте надалі можна розрахувати для кожного користувача так звані персональні значення цих параметрів.

Помилка першого роду FRR показує кількість відмов у ідентифікації зареєстрованим особам, тому вона як і FTE може бути визначена для кожної людини окремо. FRR дорівнює відношенню кількості відмов у доступі до загальної кількості спроб.

Параметр FAR також можливо розрахувати персонально, проте для його правильного розрахунку потрібно зробити значну кількість незалежних спроб ідентифікуватися різними користувачами. Тоді можна сказати, що FAR дорівнює відношенню кількості вдалих незалежних спроб пройти ідентифікацію як певний користувач до загального числа незалежних спроб ідентифікації.

Взагалі параметри FAR та FRR дуже тісно пов’язані один з одним, цілком зрозуміло, що більш критичним параметром є FAR, бо відмова в доступі «своєму» не нанесе такої значної шкоди ніж надання доступу «чужому». Тому при впровадженні системи цілком зрозуміло, що значення FAR повинно бути як можна меншим, проте зменшення значення FAR призводить до різкого збільшення значення FRR, тобто система починає масово відмовляти у доступі зареєстрованим користувачам, що також не є хорошим показником роботи. Тому необхідно дуже чітко виставляти значення FAR та FRR, для цього найчастіше за все використовують комплексну оцінку ефективності системи біометричної ідентифікації – ERR.

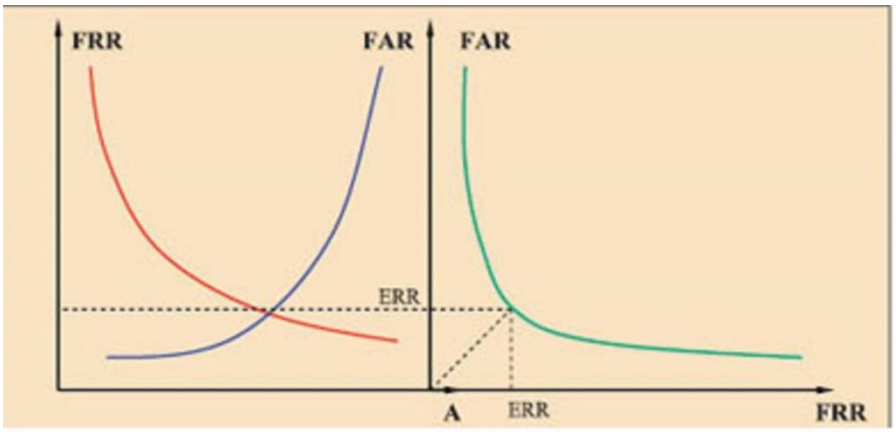
ERR – це точка, в якій ймовірність виникнення помилки першого виду дорівнює ймовірності виникнення помилки другого виду, тобто FAR = FRR. Чим менше значення ERR, тим краще система буде функціонувати. Проте в будь-якому випадку значення ERR досить велике для FAR, тому спочатку ви-значається сама точка ERR, а потім встановлюється значення FAR трохи нижче визначеного значення. При цьому значення FRR автоматично зростає. З досліджень відомо, що значення FAR необхідно встановлювати у межах від 0,001 до 0,1, відповідно значення FRR буде знаходитися у межах від 0,05 до 0,15.

На рисунку 2.4 надано графік залежності помилок першого та другого роду один від одного та визначена точка рівності ймовірностей.

Проте існує ще одна особливість поведінки помилки другого виду, яка пов’язана з режимом роботи системи біометричної ідентифікації. Нам знайомо, що система ідентифікації

може працювати фактично у двох режимах – у режимі ідентифікації (порівняння один-до-багатьох) та у режимі верифікації (порівняння один-до-одного).

На рисунку 2.5 показано графік залежності значення FAR від розміру бази шаблонів системи, який отримано для системи ідентифікації за райдужною оболонкою ока для різних початкових значень FAR.



FAR – ймовірність помилки другого виду
FRR – ймовірність помилки першого виду
ERR – точка порівняння ймовірностей
A – значення порога виявлення

Рисунок 2.4 – Залежність FAR та FRR

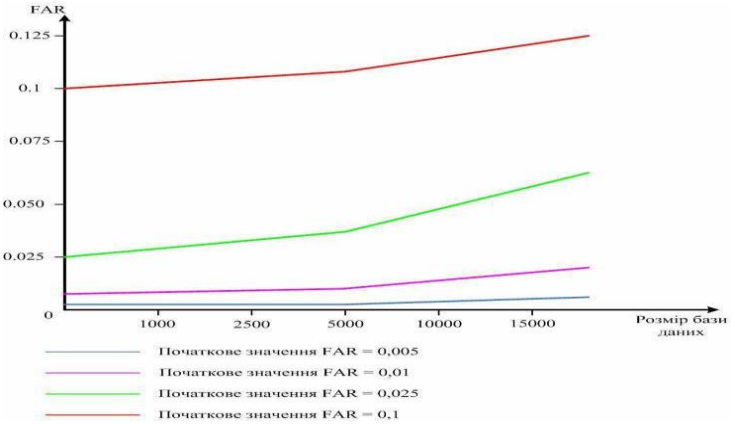


Рисунок 2.5 – Залежність FAR від розміру бази даних

З рисунка видно, що при збільшенні розміру бази даних значення FAR починає збільшуватися, причому, якщо початкове значення FAR буде встановлено досить малим, то таке збільшення буде невеликим. Слід враховувати, що дуже мале значення FAR призводить до великого значення FRR, що, у свою чергу, також не є дуже хорошим результатом.

Якщо система працює у режимі верифікації, то ніяких проблем не виникає, бо здійснюється порівняння наданого біометричного ідентифікатора з його еталонним шаблоном, який було зареєстровано у системі (відповідний шаблон для порівняння обирається за допомогою додаткової ідентифікації, наприклад, пароля). У випадку, коли система працює у режимі ідентифікації здійснюється порівняння наданого біометричного ідентифікатора з усіма шаблонами, які є у базі системи. Як наслідок цього, чим більше

шаблонів знаходиться у базі системи ідентифікації, тим більше стає значення FAR. Причому залежність має практично лінійне зростання. Але слід зазначити, що чим менше початкове значення FAR, тим менше воно зростає зі зростанням бази шаблонів системи.

3 ІДЕНТИФІКАЦІЯ ЗА ГЕОМЕТРІЄЮ ОКА

3.1 Ідентифікація на основі параметрів ока

У даному випадку в якості біометричного ідентифікатора використовуються такі параметри ока, як:

- райдужна оболонка ока (РОО);
- сітківка ока.

Райдужна оболонка являє собою тонку рухливу діафрагму ока з отвором (зіницею) в центрі, яка розташована за рогівкою, між передньою і задньою камерами ока, перед кришталиком. Практично світлонепроникна. Містить пігментні клітини, колові м'язи, що звужують зіницю, і радіальні, що розширюють її.

Сітківка (лат. retina) – внутрішня оболонка ока, яка є периферичним відділом зорового аналізатора. Містить фоторецепторні клітини, що забезпечують сприйняття і перетворення електромагнітного випромінювання видимої частини спектра в нервові імпульси, а також забезпечує їх первинне оброблення. Має унікальне розташування кровоносних судин.

Роговиця ока розташована на передній частині очного яблука, має приблизно кільцеву форму і розмір близько 11 міліметрів. Форма і розміри зовнішньої межі роговиці постійні (не змінюються з часом) і практично однакові для всіх людей. Внутрішня межа райдужки задається зіницею, що знаходиться приблизно в її центрі. У загальному вигляді внутрішню і зовнішню межу роговиці можна вважати концентричними колами (рис. 3.1).

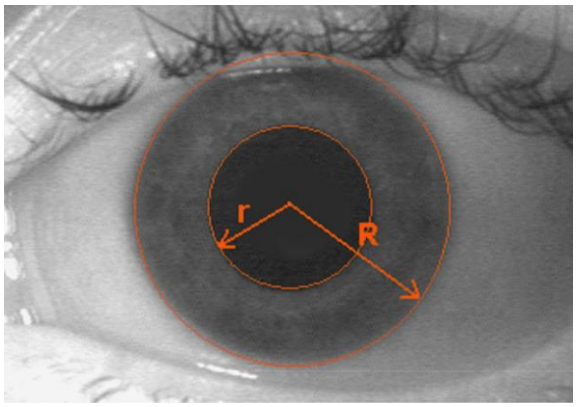


Рисунок 3.1 – Райдужна оболонка ока з радіусом R ≈ 5,5 мм зовнішньої межі й радіусом внутрішної межі r = 0,1R…0,7R

Роговиця складається з пігментованої з’єднувальної тканини, яка може організовувати різні елементи, розташування яких унікальне для кожної людини. До таких елементів відносяться:

– поглиблення, буває двох типів – лакуни й крипти;

– гребінчасті стяжки або гребені;

– борозни (боріздки);

– кільця;

– промені;

– веснянки;

– корони.

На рисунку 3.2 показані деякі з елементів райдужної оболонки.

Будь-який біометричний ідентифікатор повинен мати такі властивості:

– стійкість, тобто він повинен не змінюватися з часом;

– виразність;

– інформативність.

Райдужна оболонка практично не змінюється протягом усього життя людини. Таким чином, райдужна оболонка є параметром, який є найбільш важливим для біометричної ідентифікації, – стійкість, тобто форма роговиці залишається постійною протягом усього життя людини.

Роговиця є плоским об'єктом простої форми і практично незмінних роз-мірів. Варіації її зображення, створювані зміною умов реєстрації, малі і відносно легко можуть бути компенсовані, дозволяючи відокремити інформацію, що відноситься до індивідуальних особливостей даної роговиці від випадкових спотворень при спостереженні, тобто райдужна оболонка має виразність.

Зображення роговиці містить значну кількість структурних елементів унікальних ознак, тобто райдужна оболонка має великий ступінь інформативності.

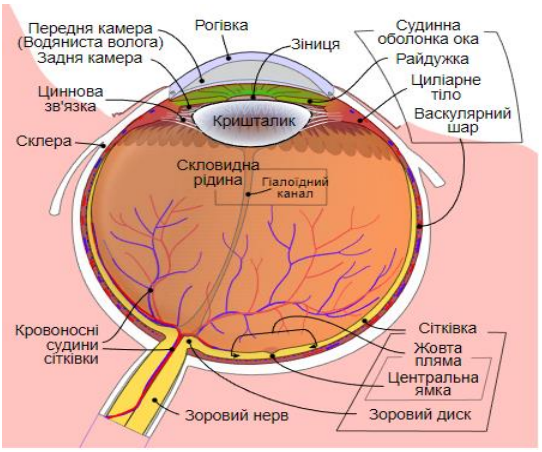


Рисунок 3.2 – Елементи райдужної оболонки

Наявність цих властивості у райдужної оболонки призвело до того, що на неї звернули значну увагу як на об'єкт автоматичного біометричного розпізнавання. Використання райдужної оболонки для біометричної ідентифікації поча-лося тільки у 1994 році, проте вже розроблено низку надійних та стійких методів ідентифікації на основі РОО і відповідні програмно-апаратні комплекси автоматичного розпізнавання.

3.2 Методи розпізнавання на основі райдужної оболонки ока

На сьогодні як ми вже зазначали, існує кілька методів ідентифікації на основі РОО. Проте у загальному випадку всі вони діють за однією і тією ж самою схемою, яка показана на рисунку 3.3.

Рисунок 3.3 – Спрощена схема процеса ідентифікації на основі РОО

Дана схема складається з кількох етапів:

- отримання зображення ока;
- аналіз якості зображення РОО;
- виділення райдужної оболонки на зображенні;

– нормування розмірів зображення райдужної оболонки;

– обчислення ознак і формування з них набору роговиці;

– порівняння отриманого набору з еталонним.

Виділення роговиці на зображенні.

Даний етап полягає у пошуку на отриманому зображенні відносно темно-

го об'єкта, близького за формою до кола, що містить всередині себе ще один концентричний темніший об'єкт (зіницю). У більшості систем на даному етапі необхідно забезпечити виконання тільки однієї умови – усередині зіниці повинен знаходитися яскравий відблиск певної форми (відблиск від освітлювача).

Дане завдання може бути вирішене багатьма способами, наприклад, пошук концентричних кіл за допомогою перетворення Хафа, або використання коррелятора для пошуку відблиску заданої форми з подальшим виявленням ко-нтурів зіниці, що містить цей відблиск, і далі – концентричної зіниці райдужної оболонки.

Методи виділення зіниці і зовнішньої межі РОО базуються на детекторах краю і виділення кіл за допомогою перетворення Хафа. Проте для перетворення Хафа потрібно багато часу. Алгоритми виділення зіниці орієнтовані на діаметр зіниці 10…60 пікселів. Як правило, межі зіниць таких розмірів мають досить чіткі перепади яскравості або зафарбовані одним відтінком вручну (як у базі зображень CASIA). Тому для виділення меж зіниці більшість алгоритмів використовує стандартні детектори краю (Canny, Sobel тощо). Зображення, що надходять на обробку в таких системах, мають діаметр зіниці 150…500 пікселів і детектори краю, застосовані до них, не дозволяють виділити чіткі перепади, або їх виділяють надмірно багато.

Специфічним є наявність повік, які у більшості випадків закривають верхню і нижню частини роговиці. Деякі системи, можуть виділяти повіки явним чином і відкидають помилкові дані із закритих ділянок. Інші системи виділення повік як такі не використовують, а закриті частини виявляють за великою відмінністю при порівнянні декількох послідовних знімків. На рисунку 3.4 показано зображення ока і результати виділення роговиці.

Нормування розмірів зображення райдужної оболонки необхідне за двух причин:

– через розходження масштабів знімків;

– через зміну відносного розміру зіниці.

Нормування до єдиного масштабу здійснюється досить просто, на етапі виділення роговиці був отриманий еліпс, що наближає зовнішній контур райдужної оболонки, завдання вирішується афінним перетворенням цього еліпса до деякого заданого кола.

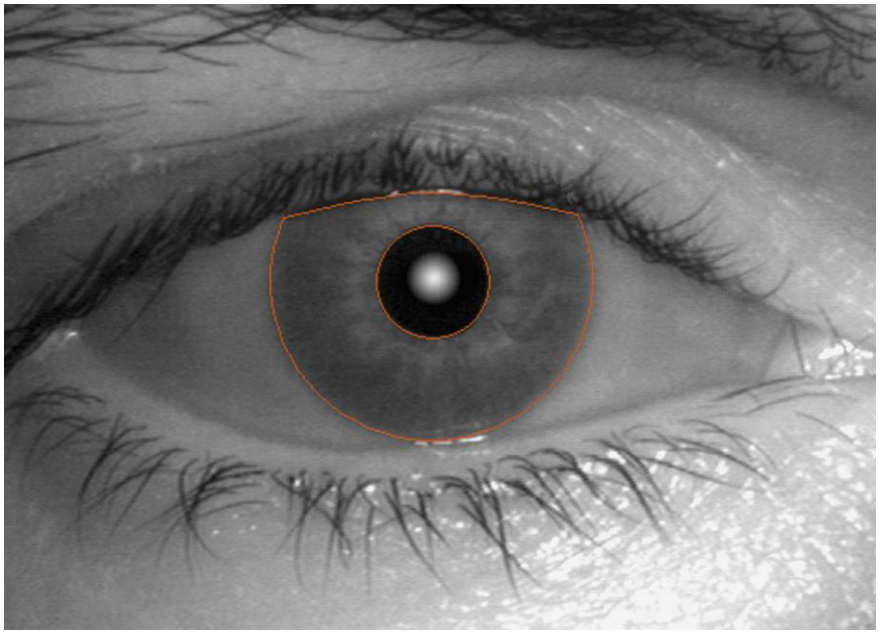


Рисунок 3.4 – Виділення РОО на зображенні ока

Значно складніше усунути варіації, викликані зміною розмірів зіниці. Фізично роговиця являє собою нерівномірне за товщиною кільце. Переміщення елементів кільця при зміні внутрішнього радіуса нелінійне. Більше того, при пульсації зіниці деякі елементи роговиці можуть здійснювати не тільки поступальні рухи уздовж радіусів, а й обертальні відносно цента. Це є однією з основних перешкод підвищення точності систем розпізнавання за роговицей.

На рисунку 3.5 надане зображення одного і того ж самого ока, отримані з однієї і тієї самої камери з інтервалом у кілька хвилин, але за різних умов освітлення.

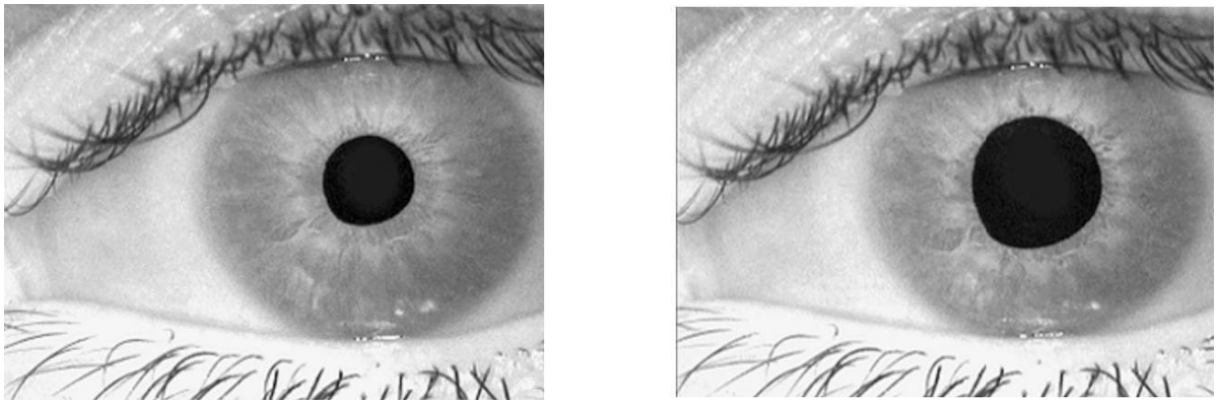


Рисунок 3.5 – Зміна розмірів РОО й зіниці при зміні умов освітлення

Оскільки роговиця є майже круглим об'єктом, з добре вираженою варіацією структури уздовж радіусів і практично однорідними текстурами вздовж концентричних кіл, має сенс розглядати її у полярній системі координат. Перетворення системи координат може бути зроблено явно або неявно, як це робиться, обчислюючи диференціальні ознаки вздовж

концентричних кіл.

Обчислення ознак і формування еталона

На етапі обчислення ознак і формування еталона роговиці вирішується завдання факторизації, тобто обчислення набору характеристик зображення, що мають найменший розкид для знімків даної людини і найбільший розкид між знімками різних людей. Оскільки кількість ознак досить мала порівняно з розмірами зображення, попутно вирішується завдання зменшення розмірності даних. Якщо всі попередні етапи стосувалися лише геометричної, але не яскравісної нормалізації зображення, то на даному етапі необхідно обчислювати ознаки інваріантні до змін яскравості (яскравість, контрастність, нерівномірність освітлення). Також можливо буде позбутися шумів зображення. Цим умовам добре задовольняють спектральні і близькі до них вейвлет-перетворення.

3.3 Проблеми ідентифікації на основі райдужної оболонки ока

Ідентифікація особистості на основі райдужної оболонки має дуже великий ступінь надійності й точності, проте існує й низка проблем. У першу чергу, це те, що для успішної ідентифікації необхідно щоб око потрапило у поле зору об'єктива камери під певним діапазоном кутів. Решта проблем пов'язані з особливостями структури ока людини і показані на рисунку 3.6.

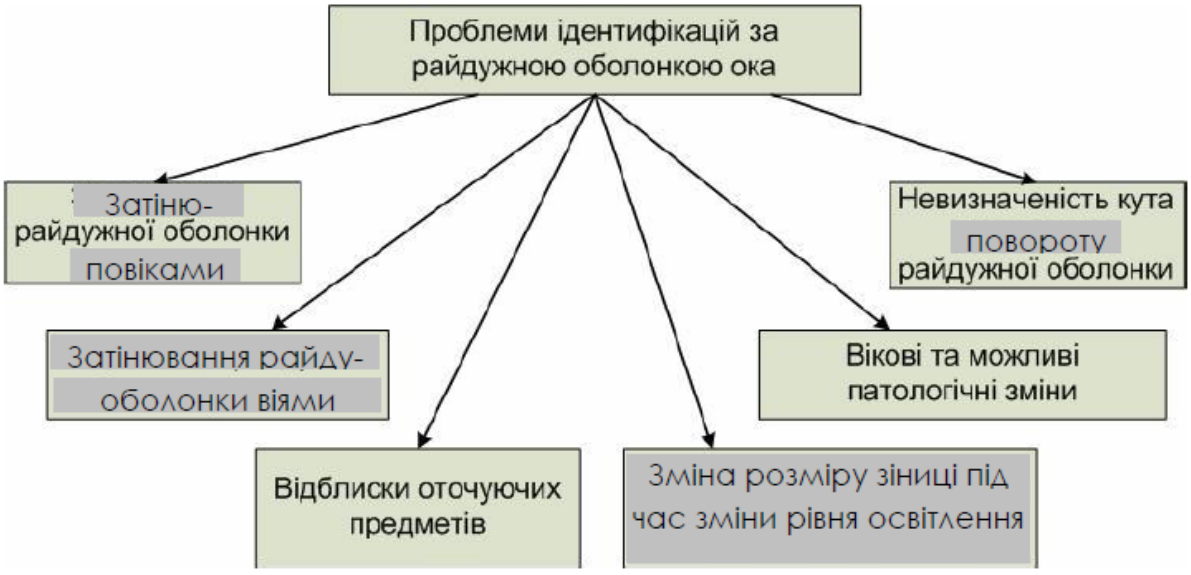


Рисунок 3.6 – Проблеми ідентифікації на основі райдужної оболонки

1) Затінення роговиці повіками. Ця проблема може вирішуватися спеціальним алгоритмом пошуку повік або відбраковуванням частин зображення при порівнянні послідовних кадрів.

2) Затінення роговиці віями, що стирчать донизу. Алгоритм пошуку повік на подібних знімках відпрацьовує успішно і з великою впевненістю, про-те виділена ним область, не підходить для розпізнавання. Проблема може вирішуватися алгоритмом відбраковування за послідовністю зображень. Роговиця і повіки з віями рухаються відносно одна одної, тому ті частини зображення, де вії і повіки нависають над роговицей, постійно змінюються (вії поперемінно закривають різні частини роговиці). Навпаки, відкриті ділянки роговиці на нормованому зображенні відносно стабільні.

3) Відблиски від навколишніх предметів на роговиці. Роговиця працює як сферичне дзеркало, відбиваючи навколишній світ. Ці відбиття (особливо відо-браження джерел світла, плям сонячного світла і ділянок денного неба) можуть бути в кілька разів яскравішими деталей роговиці і повністю пригнічувати їх. Для вирішення цієї проблеми застосовують високоінтенсивне у вузькій області спектра освітлення (що значно перевершує сонячне за освітленістю, найчастіше використовують інфрачервоне випромінювання) і реєстрацію зображення у цій самій області спектра.

4) Різний розмір зіниці при змінних умовах зйомки. Як уже зазначалось, афінне перетворення зображення роговиці до стандартного розміру вирішує цю проблему лише у першому наближенні, тому що розтягування роговиці підпорядковується нелінійному, надто складному закону. Для вирішення цієї проблеми пропонується, наприклад, запам'ятовувати розмір зіниць людини при реєстрації у системі, а при розпізнаванні домагатися акомодації (розширення чи звуження) зіниць до цього розміру, маніпулюючи яскравістю спеціального джерела видимого світла.

5) Патологічні й вікові зміни. На роговиці дуже чітко відбивається стан організму, у тому числі різного роду патології (хвороби, травми, отруєння). У зв'язку з цим виникає питання про стійкість (за часом) розпізнавання об'єкта, підданого цим змінам. Проте, на роговиці існує значна кількість вроджених ознак і ознак, які не змінюються протягом усього життя. Вроджені та набуті ознаки розділити практично неможливо, проте людину можна розпізнавати на підставі збігу навіть незначної кількості ознак. Необхідний мінімум – це 30% і навіть у цьому випадку ймовірність помилкового допуску не перевищує 10–6.

6) Невизначеність кута повороту роговиці. У системі з реєстрацією двох роговиць або у системі, що комбінує роговицю й обличчя, цієї проблеми не існує. Для так званої «одноокої» системи можна визначати кут за конфігурацією повік, децентрацією зіниці або за якоюсь важливою характерною ознакою на рогівці. Всі ці ознаки можуть змінюватися з часом. У такому випадку залиша-ється перебирати кути повороту (істотно збільшується час

роботи системи) або вираховувати ознаки, інваріантні до повороту (таких ознак в десятки разів менше, отже, сильно знижується надійність системи).

Крім усього вищеперерахованого системи біометричної ідентифікації повинні бути стійкими до використання підробок. Для систем ідентифікації на основі райдужної оболонки в якості підробки можуть застосовувати або об'ємну фотографію роговиці або макет ока, так само можуть застосовувати відчуження біометричних ознак (у даному випадку «вирване» око).

Існує два способи вирішення цієї проблеми:

1) За спектром відбиття роговиці. Роговиця «живого» ока постійно зволожується, «мертве» око швидко пересихає. Спектри відбиття вологої і сухої рогівк відрізняються.

2) За реакцією ока на освітлення. Зіниця певним чином і з певним запізненням реагує на зовнішні подразники (спалах світла, гучний звук і т.д.), при-чому ця реакція керується головним мозком.

Будуючи графік реакції зіниці (пупілограму) і відносячи її до моменту, коли був поданий імпульс-подразник, то можна з високою надійністю відкинути спроби фальсифікації. Пупілограми дають ще одну цікаву можливість. Як відомо, пупілограма служить характеристикою фізичного функціонального стану людини (норма, перезбуджена, пригноблена). За пупілограмою з великою точністю можна встановити, наскільки працездатна людина на даний момент, а також визначити стан сп'яніння або впливу стимуляторів. Така можливість цін-на для систем безпеки, що встановлюються на об'єктах, де потрібен не тільки допуск певних осіб, але й перевірка їх працездатності (операторські АЕС, авіа-диспетчерські тощо).

3.4 Принципи ідентифікації особистості по райдужній оболонці ока

У якості двох основних характеристик будь-якої біометричної системи можна прийняти помилки першого та другого роду. Наприклад, у теорії радіолокації їх зазвичай називають «помилкова тривога» або «пропуск мети», а в біометрії найбільш усталені поняття – FAR (False Acceptance Rate) і FRR (False Rejection Rate). Перше значення характеризує ймовірність помилкового збігу біометричних характеристик двох людей. Друге – ймовірність відмови доступу людині, що має допуск. Система тим краща, чим менше значення FRR (помилка першого роду) при однакових значеннях FAR (помилка другого роду). Іноді використовується і порівняльна характеристика EER, визначальна крапка в якій – графіки FRR і FAR перетинаються (рисунок 3.7).

Щоб зрозуміти ймовірності FAR та FRR, можна оцінити, як часто будуть виникати помилкові збіги, якщо встановити систему ідентифікації на прохідній організації з чисельністю персоналу N осіб. Ймовірність помилкового збігу, отриманого сканером відбитка пальця для бази даних з N відбитків, дорівнює FAR·N. І кожного дня через пункт контролю доступу проходить теж близько N осіб. Тоді ймовірність помилки за робочий день FAR·(N·N). Звичайно, залежно від цілей системи ідентифікації ймовірність помилки за одиницю часу може сильно варіюватися, але якщо взяти допустимим одну помилку протягом робочого дня, то отримаємо формулу:

$$FAR \times N^2 \approx 1 \Rightarrow N \approx \sqrt{\frac{1}{FAR}}$$

Тоді очевидно, що стабільна робота системи ідентифікації при FAR=0.1%=0.001 можлива при чисельності персоналу N≈30.

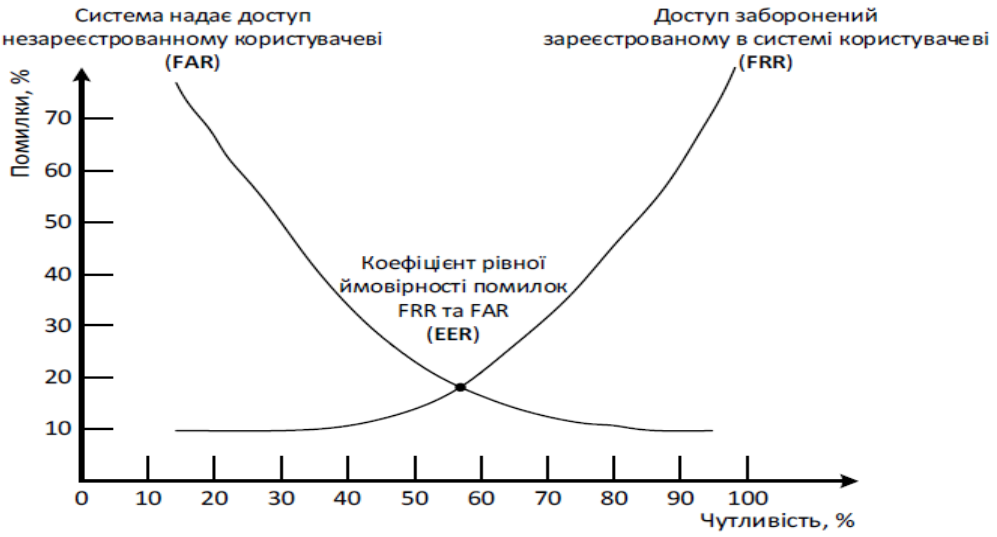


Рисунок 3.7 – Порівняльна характеристика EER

Дактилоскопія (розпізнавання відбитків пальців) – найбільш розроблений на сьогоднішній день біометричний метод ідентифікації особи. Кожна людина має унікальний папілярний візерунок відбитків пальців, завдяки чому і можлива ідентифікація.

Якості джерела даних FAR та FRR використовувалися статистичні дані VeriFinger SDK, отримані за допомогою сканера відбитків пальців DP U.are.U. За останні 5-10 років характеристики розпізнавання за пальцем зробили незначний крок уперед, так що наведені цифри непогано показують середнє значення сучасних алгоритмів. Характерне значення FAR для методу розпізнавання відбитків пальців – 0.001%. З формули 1 одержимо, що стабільна робота системи ідентифікації при FAR=0.001% можлива при чисельності персоналу N≈300.

Райдужна оболонка ока є унікальною характеристикою людини. Малюнок райдужної оболонки формується на восьмому місяці внутрішньоутробного розвитку, остаточно стабілізується у віці близько двох років і практично не змінюється протягом життя, окрім як у результаті сильних травм або різких патологій. Метод є одним з найбільш точних серед біометричних.

Характеристики FAR та FRR для райдужної оболонки ока найкращі у класі сучасних біометричних систем (за винятком, можливо, методу розпізнавання за сітківкою ока). У роботі наведені характеристики бібліотеки розпізнавання райдужної оболонки алгоритму – EyeR SDK, які відповідають перевіреній за тими ж базам алгоритмом VeriEye. Характерне значення FAR – 0.00001%.

Відповідно до формули 1 N≈3000 – чисельність персоналу організації, при якій ідентифікація співробітника відбувається достатньо стабільно.

Тут варто відзначити важливу особливість, що відрізняє систему розпізнавання за райдужною оболонкою від інших систем. У разі використання камери дозволу від 1.3МП можна захоплювати два ока на одному кадрі. Так як ймовірності FAR та FRR є статистично незалежними, то при розпізнаванні за парою очей значення FAR буде приблизно дорівнювати квадрату значення FAR для одного ока. Наприклад, для FAR 0,001% при використанні двох очей ймовірність помилкового допуску буде дорівнювати 8-10%, при FRR всього в два рази вище, ніж відповідне значення FRR для одного ока при FAR=0.001%.

3-D розпізнавання особи представляє собою досить складне завдання. Повні дані про FRR і FAR для алгоритмів цього класу на сайтах виробників відкрито не наведені. Але для кращих моделей фірми Bioscript (3D EnrolCam, 3D FastPass), що працюють за методом проеціювання шаблону, при FAR=0.0047% FRR становить 0.103%. Вважається, що статистична надійність методу порівнювана з надійністю методу ідентифікації за відбитками пальців.

Розпізнавання за венами руки – це нова технологія у сфері біометрії, широке застосування її почалося 5-10 років тому. Інфрачервона камера робить знімки зовнішньої або внутрішньої сторони руки. Малюнок вен формується завдяки тому, що гемоглобін крові поглинає ІЧ-випромінювання. У результаті ступінь віддзеркалення зменшується і вени видно на камері у вигляді чорних ліній. Спеціальна програма на основі отриманих даних створює цифрову згортку. Не потрібний контакт людини зі скануючим пристроєм.

Технологія порівнянна за надійністю з розпізнаванням за райдужною оболонкою ока, у чомусь перевершуючи її, а у чомусь поступаючись.

Значення FRR і FAR наведено для сканера Palm Vein. Згідно з даними розробника при FAR 0,0008% FRR становить 0.01%.

Результати досліджень стабільності роботи системи ідентифікації персоналу для різних

біометричних методів наведено у таблиці 3.1.

Таблиця 3.1 – Загальна таблиця стабільності роботи системи ідентифікації персоналу

№	Біометрична характеристика (ознака)	FAR, %	Кількість персоналу, N≈
1.	Відбиток пальця	0.001	300
2.	Райдужна оболонка ока	0.00001	3000
3.	3-D розпізнавання особи	0.0047	145
4.	Вени руки	0,0008	350

Отже, узагальнивши результати для методів, можна сказати, що для середніх і великих об’єктів, а так само для об’єктів з максимальною вимогою до безпеки слід використовувати райдужну оболонку в якості біометричного доступу та розпізнавання за венами рук. Для об’єктів з кількістю персоналу до декількох сотень осіб оптимальним буде доступ за відбитками пальців. Системи розпізнавання за 3D зображенням особи вельми специфічні. Вони можуть знадобитися у випадках, коли розпізнавання вимагає відсутності фізичного контакту, або поставити систему контролю за райдужною оболонкою неможливо. Наприклад, при необхідності ідентифікації людини без його участі, прихованою камерою, або камерою зовнішнього виявлення, це можливо лише при малій кількості суб’єктів у базі і невеликому потоці людей, що знімаються камерою.

Порівняння різних біометричних методів ідентифікації показало, що за сукупністю якостей широке використання ідентифікації по РОО має помітні переваги перед більшістю інших біометричних характеристик і необмежені перспективи застосування в системах безпеки. Однак суттєвим недоліком таких систем є алгоритмічна складність і високі вимоги до обчислювальних ресурсів, а також висока вартість. У зв'язку з цим, актуальні дослідження в області розробки нових методів аналізу і розпізнавання зображення райдужної оболонки, які при стійкості до різних видів перешкод, що виникають при зйомці, дозволили б поліпшити характеристики системи і знизити вимоги до апаратури, зменшивши її вартість. Також, визначено, що людська райдужка має специфічну структуру і містить багато текстури інформації. Просторові структури, які спостерігаються в райдужці, унікальні для кожного індивіда. Кольорові ознаки райдужної оболонки недостатньо надійні, оскільки вони можуть змінюватися з віком. Основна проблема при побудові системи ідентифікації - ефективне виділення і подання текстурной інформації, що містяться в райдужній оболонці..

Схема алгоритму обробки зображення ока в системі ідентифікації особистості по зображенню райдужки приведена на рисунку 3.8.

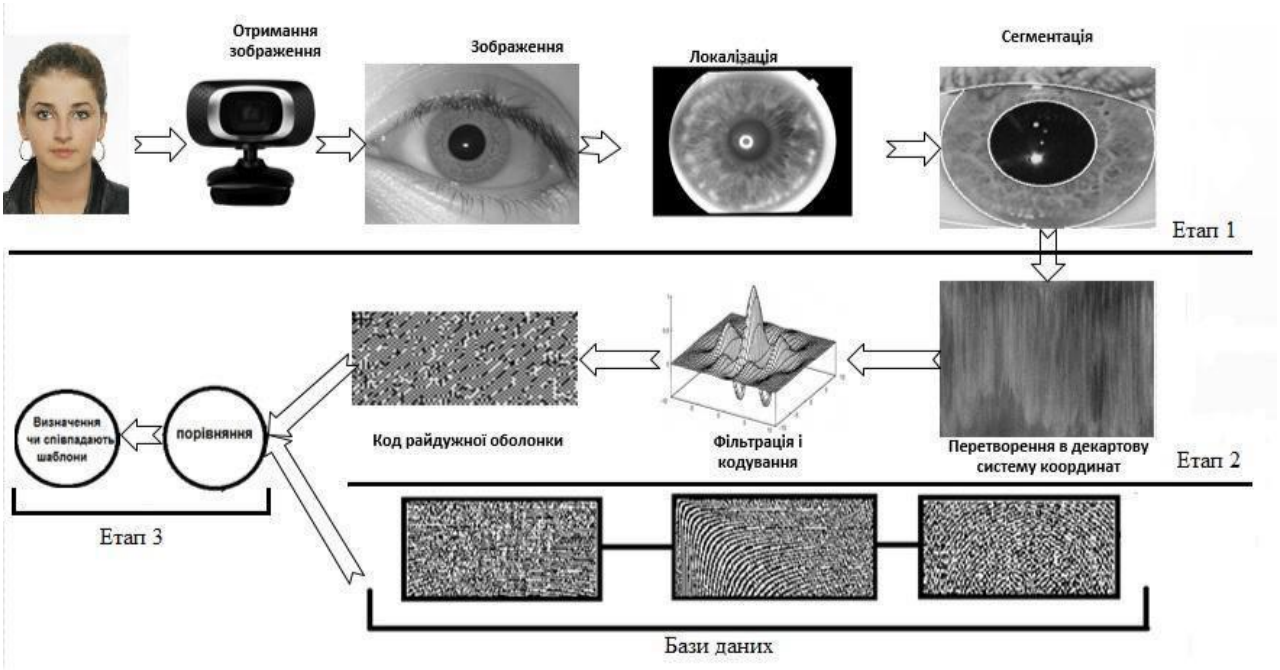


Рисунок 3.8 - Біометрична система заснована на райдужці ока

3.5 Формалізація вимог до зображення райдужки

Для забезпечення стабільного високого швидкодії при ідентифікації по райдужці важливо, щоб використовувані зображення відповідали певним мінімальним вимогам [5-7]:

Просторова роздільна здатність системи отримання зображення повинно бути як мінімум 3,2 ліній / мм при контрасті 60%, цифрове зображення повинно мати дозвіл як мінімум 17 пікселів / мм. При цьому гарантується, що зображення вільні від артефактів, що виникають в результаті недостатньої частоти дискретизації. Якість фокусування має зберігати задану просторову роздільну здатність. На рисунку 3.9 представлено зображення райдужної оболонки з достатнім дозволом і якістю фокусування.

Діаметр зіниці не повинен перевищувати 7мм, а діаметр лімба повинен бути не менше 14 мм.

Зображення повинно мати динамічний діапазон як мінімум 256 біт, при цьому як мінімум 7 біт інформації про яркість повинні бути не схильні до впливу шуму. Якщо на зображенні присутні відблиски, то їх яскравість не повинна перевищувати 255. Інші області ока (зіниця, райдужка, склера) повинні мати яскравості в діапазоні 0-255.

Рисунок 3.9 - Приклад зображення райдужної оболонки

1) Зображення райдужної оболонки повинно мати як мінімум 90 рівнів, які поділяють райдужку і склеру і як мінімум 50 рівнів, які поділяють райдужку і зіницю для всіх кольорів очей.

2) В усякому разі, 70% райдужки має бути не закрита відблисками, повікою, віями, або іншими перешкодами.

3) Масштаб зображення повинен бути таким, щоб райдужка що має розмір 14 мм мала діаметр 200-300 пікселів. Зображення повинно бути досить велике, щоб відстань між краєм райдужки і межею зображення було як мінімум 70 пікселів (рис. 2.4).

4) Відношення сигнал / шум має бути не менше 40 дБ, включаючи будь-які шуми, що вносяться методами стиснення зображень.

5) Зображення повинно пред'являтися в стандартній орієнтації: верхня повіка повинна бути розташована у верхній частині зображення, слізний проток правого ока повинен знаходитися в правій частині зображення, лівого - в лівій.

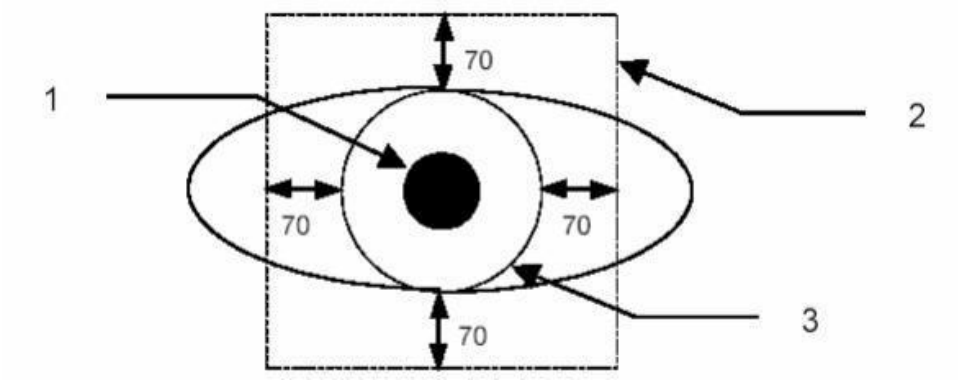
Для досягнення максимальної ефективності розпізнавання слід дотримуватись таких вимог:

– голова повинна знаходитися у вертикальному положенні, її нахил не повинен перевищувати 10°. Система розпізнавання може вимірювати і компенсувати нахил голови;

– спостережуване око має бути відкрите як можна ширше.

– окуляри повинні бути зняті.

– жорсткі контактні лінзи і пофарбовані м'які контактні лінзи повинні бути видалені.



(1.Межа зіниці, 2. Межа зображення 3.Межа райдужки)

Рисунок 3.10 - Необхідний масштаб зображення

3.6 Отримання і обробка зображення райдужної оболонки ока

Одержувані зображення райдужної оболонки, крім областей які становлять інтерес, містять «непотрібні» частини (тобто повіку, зіниця і т.д.) Тому зображення не може бути використано безпосередньо. Більш того, зміна відстані між камерою і райдужкою може призвести до зміни розміру однієї і тієї ж райдужки. Крім того, райдужка освітлюється нерівномірно. Для ефективного розпізнавання, на оригінальному зображенні необхідно локалізувати райдужку, порівнянн методів виділення контурів наведено в таблиці 3.1, нормалізувати її зображення, і знизити вплив вищезгаданих факторів. Попередня обробка зображення райдужної оболонки описана в наступних розділах.

Для забезпечення достатньої для розпізнавання деталізації зображення райдужної оболонки система введення зображення повинна забезпечувати розширення не менше 50 пікселів на радіус райдужки. В даний час, в основному використовуються системи введення зображення з роздільною здатністю 100-140 пікселів на радіус райдужки. Для введення зображення використовують ПЗС камери з роздільною здатністю 640 × 480, чутливі до ближнього інфрачервоного випромінювання, невидимому для людини, з довжиною хвилі 700-900нм. Деякі пристрої введення зображення мають ширококутову камеру для грубої локалізації ока і камеру з малим кутом зору, яка налаштовується за результатами локалізації ока і забезпечує введення зображення райдужної оболонки з високою роздільною здатністю. Існує безліч різних методів отримання зображення райдужної оболонки. Більшість пристроїв для зйомки райдужки не мають пристрою наведення, але замість цього використовується візуальний зворотний зв'язок, яка базується на використанні дзеркала або відеозображення. Зворотній зв'язок дозволяє користувачеві правильно помістити око в поле зору камери з

малим кутом зору. Фокус встановлюється в реальному часі (швидше, ніж інтервал між кадрами) шляхом вимірювання сумарної енергії високочастотної частини двовимірного спектра Фур'є для кожного з кадрів, і максимізації цієї енергії шляхом переміщення лінз об'єктива або шляхом звуковий зворотного зв'язку з суб'єктом [7, 8].

Таблиця 3.2 - Порівняння методів виділення контурів

Метод	Недоліки	Застосування
Робертса	Низька точність із-за використання маски 2x2. Розриви контурів зображення.	Чутливий до шуму
Собеля	Базується на методі Робертса. Використовує маску 3x3. Розриви контурів. Використовуються попередньо визначені вагові коефіцієнти	Грубе наближення градієнта яскравості
Канні	Базується на методі Робертса. Використовуються два порога. Використовує маску 3x3.Розрив контурів	Межі мають деяку кінцеву товщину. Тому необхідно виконати потоншення ліній придушенням не максимальних точок в перпендикулярному до межі напрямку, тобто в напрямку градієнта
Превіта	Передбачено 8 ядер, що відповідають різним напрямкам, що підвищує точність визначення меж	Велика складність обчислень (в 8 разів більше, ніж при Собелі)
Градієнтний інтегрально-диференціальний	Тривалість обчислень. Використовує градієнт яскравост	Широке застосування на практиці в СКУД, в біології та медицині
DoG	Збільшується чіткість країв і дрібних деталей на зображенні	Дуже неточно позначаються межі гострих кутів. Компоненти фільтра схильні реагувати на шум, а не тільки на край.

4 РОЗРОБКА МЕТОДУ ІДЕНТИФІКАЦІЇ ЛЮДИНИ ЗА РАЙДУЖКОЮ ОКА

4.1 Перетворення Ерміта

Перетворення Ерміта [1] є відомим методом для вирішення біометричних завдань [2,3,4]. У перетворенні Ерміта обчислюються згортки функції інтенсивності зображення з функціями перетворення Ерміта (похідними функції Гаусса) в кожній точці зображення, тобто аналізуються локальні властивості зображень. Також широко відомим методом в обробці зображень є метод моментів Гауса-Ерміта [2], еквівалентний перетворенню Ерміта [4] з точністю до знаків згорток для непарних функцій перетворення Ерміта. У методі моментів Гауса-Ерміта замість згорток шукаються кореляції функції з похідними функції Гаусса. Зазвичай при використанні цих методів в задачах ідентифікації розглядаються лише знаки згорток в кожній точці, а потім проводиться порівняння бінарних матриць, складених із знаків згорток,

У даній роботі запропоновано метод знаходження найбільш інформативних точок текстури райдужної оболонки на основі перетворення Ерміта. Для цього аналізується сума модулів згорток функції інтенсивності зображення з функціями перетворення Ерміта з найбільш інформативними номерами [5] у всіх точках області параметризації райдужної оболонки. Точки з максимальним значенням суми відповідають характерним точкам текстури зображення райдужної оболонки. При цьому виявлено, що для запропонованого методу зменшення кількості збережених ключових точок райдужної оболонки не призводить до сильних втрат в якості розпізнавання.

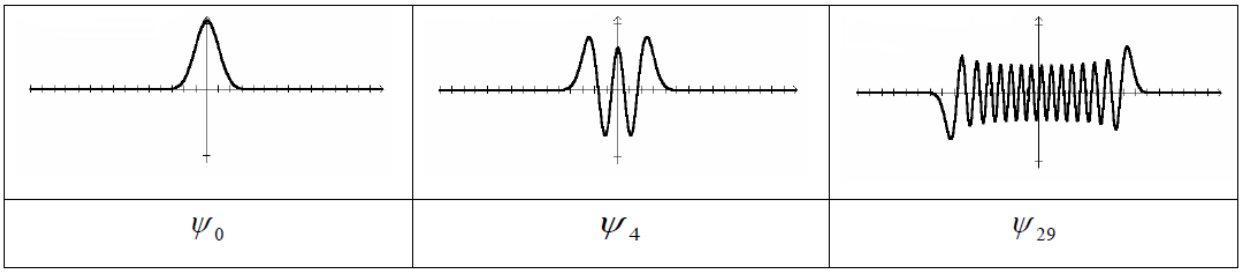
У мультібіометріческіх системах розпізнавання людини [6,7], розмір коду кожної біометричної складової і швидкість розпізнавання важливі більше, ніж 100% точність розпізнавання за однією ознакою. Тому запропонований метод ключових точок для ідентифікації по райдужній оболонці може застосовуватися для розпізнавання людини одночасно з іншими біометричними показниками, такими як голос, зображення осіб і відбитки долонь, пальців.

4.2 Функції Ерміта

В якості базисних функцій в роботі взяті функції Ерміта (рис. 4.1). Одновимірні

функції перетворення Ерміта ϕ можуть визначатися через функції Ерміта наступним чином:

$$\psi_n(x) = \frac{(-1)^n e^{x^2/2}}{\sqrt{2^n n!\sqrt{\pi}}} \cdot \frac{d^n(e^{-x^2})}{dx^n}, \qquad \varphi_n(x) = \frac{e^{-x^2/2}}{\sqrt[4]{\pi}} \cdot \psi_n(x).$$



ψ_0 ψ_4 ψ_{29}

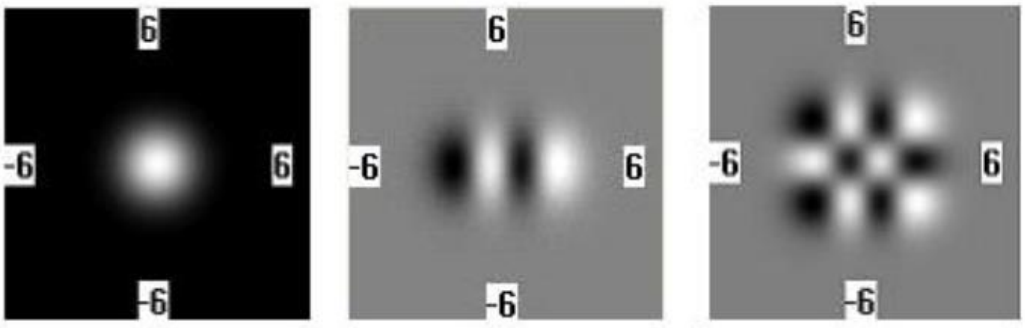
Рисунок 4.1 - Приклади одновимірних функцій Ерміта

Функції Ерміта мають наступні властивості:

– є власними функціями перетворення Фур'є: $F(\psi_n) = i^n \psi_n$;

– є локалізованими з обчислювальної точки зору як в просторовому, так і в частотному просторах

– утворюють повну ортонормированном систему функцій в просторі L_2 (−∞, + ∞). Двовимірні функції Ерміта представимо у вигляді відповідних творів одновимірних функцій Ерміта (рис. 4.2): $\psi_{n,m}(x, y) = \psi_n(x) \cdot \psi_m(y)$.



$\psi_{0,0}$ $\psi_{3,0}$ $\psi_{3,2}$

Рисунок 4.2 - Приклади двовимірних функцій Ерміта

Даний частотно-просторовий базис представляється досить перспективним для вирішення ідентифікаційних завдань біометрії. Раніше в завданню ідентифікації людини за райдужною оболонкою ока нами запропонований метод, який використовує даний базис при аналізі інтегральних характеристик райдужної оболонки [9,10].

Перетворення Ерміта. Нехай I(x, y) - функція інтенсивності вихідного зображенняψ_n,

m (x, *y*) - m, n-я двовимірна функція Ерміта. Перетворення Ерміта для функції (x, y) визначається в кожній точці (x_0 , y_0) Значеннями згорток I (x, y) з функціями перетворення Ерміта для обраного кінцевого набору індексів (m, n) [6]:

$$M_{m,n}(x_0, y_0) = (I(x,y) * \phi_{m.n}(x, y))(x_0, y_0) = \iint I(x, y) \cdot \phi_{m,n}(x_0 - x, y_0 - y)\, в_x\, d_y.$$

На відміну від проекційного методу Ерміта [9], це перетворення зазвичай використовує лише невеликі значення m і n і описує локальні характеристики зображення.

В методі перетворення Ерміта для зображень райдужних оболонок очей використовуються знаки формул перетворення в різних точках зображення:

$$L_{m,n} = \operatorname{sgn}(M_{m,n}(x_0, y_0)).$$

У даній роботі проведено вибір оптимальних номерів функцій Ерміта, використовуваних в алгоритмі, і вибір критерію ідентифікації цим методом.

4.3 Задача ідентифікації людини за райдужною оболонкою ока

На вхідному зображенні виділяється райдужна оболонка ока, наводиться до деякого загального нормалізоване увазі. Далі визначається володар найбільш схожою райдужної оболонки в базі даних на основі розробленого методів параметризації і побудови векторів властивостей (кодів).

Виділення райдужної оболонки ока. Як правило, зіницю ока темніше сусідніх областей, тому шукається приблизний центр зіниці шляхом проектування зображення в горизонтальному і вертикальному напрямках за формулами:

$$X_{cent} = \arg \min_x \sum_y I(x, y)$$

$$Y_{cent} = \arg \min_y \sum_x I(x, y)$$

Далі уточнюється центр зіниці і кордони райдужної оболонки [1]. При цьому шукається максимальний стрибок похідної згладженої середньої інтенсивності по круговому контуру:

$$\max_{r,x_o,y_o}\left|G_\sigma(r)*\frac{\partial}{\partial r}\oint_{r,x_o,y_o}\frac{I(x,y)}{2\pi r}ds\right|$$

де * позначає згортку двох функцій, здійснює згладжування функції інтенсивності; Gσ (r) - функція Гаусса з параметром σ (ширина гаусіана бралася рівній 2 пікселям для внутрішнього кордону райдужної оболонки і 5 - для зовнішньої);

(x0 , y0) – можливі координати центру зіниці, r ϵ[rmin , rmax] - можливі радіуси.

Кордони райдужної оболонки; інтегрування ведеться по круговому контуру (рис. 4.3). Для обчислення зовнішнього кордону райдужної оболонки розглядається частина кругового контуру, виділена на рисунку 4.3 (б)/

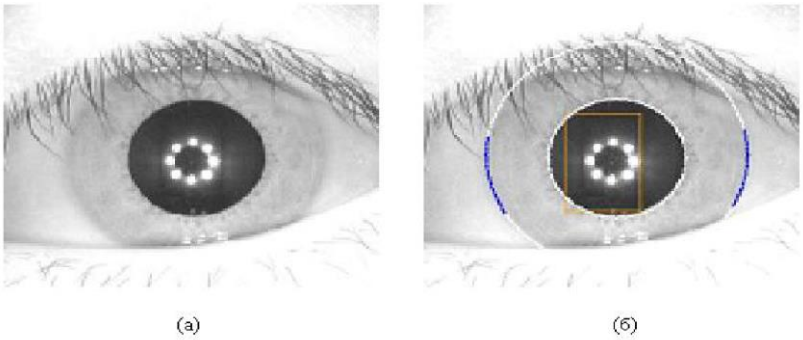


Рисунок 4.3 - (а) - вихідне зображення; (а) - зображення з виділеної райдужки

Нормалізація райдужної оболонки. Результатом попереднього пункту є дві не концентричні окружності - зовнішня і внутрішня кордону райдужної оболонки. Далі вводиться псевдополярна система координат і райдужна оболонка перекладається в прямокутник (рис. 4.4 б).

Рисунок4.4 - (а) - зображення ока з введеної псевдополярної системою координат; (б) нормалізоване зображення райдужної оболонки

Для подальшої параметризації нами використовується тільки контрольна область, що включає праву верхню чверть нормалізованого зображення, тому що на ліву половину нормалізованого зображення часто потрапляють вії, а на нижню - повіку (рис. 4.5).

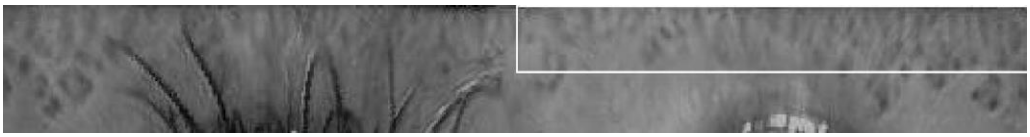


Рисунок 4.5 - Нормалізоване зображення з виділеної контрольної області

Параметризація райдужної оболонки і складання бінарних кодів. Для кожної точки контрольній ділянці нормалізованого зображення обчислюються значення

$$L_{m,n}(x_0, y_0) = \mathrm{sgn}(I(x, y))*m.n(x, y))(x_0, y_0).$$

Далі для кожної пари значень (m, n) складається бінарна матриця розміру розглянутої частини нормалізованого зображення зі значеннями Lm, n .

Порівняння зображень райдужних оболонок. На стадії порівняння відбувається порівняння бінарних матриць для кожної пари індексів(m, n). При цьому попередньо проводиться проріджування отриманих матриць для зменшення кількості проведених операцій (в поточній версії алгоритму беруться тільки кожен десятий піксель по осі x і кожен другий піксель по осі y).

В якості метрики порівняння зображень райдужних оболонок використовується відстань Хеммінга між відповідними зріджені матрицями райдужних оболонок (Ham (L)), дорівнює кількості незбіжних значень в матрицях. За значеннями $Ham(L_{1,0})+Ham(L_{2,0})$ та $Ham(L_{1,0})+ Ham(L_{2,1})$ виконується сортування зображень з бази даних по відстані до розглянутого перевіряється зображення. Вибір даних значень індексів буде обгрунтований нижче. По кожному з цих двох значень в базі даних шукається володар найближчій райдужної оболонки. У разі збігу володарів алгоритм вважає, що порівняння успішно закінчено. Що стосується розбіжності володарів вважається, що метод не може коректно провести верифікацію і користувачеві пропонується ще раз зробити знімок очі для ідентифікації.

Щоб метод був стійкий до невеликих поворотів очі, використовується також циклічний зсув (рисунок 4.6) нормалізованого зображення на 3, 6, 9, 12, 15, 18, 21 пікселів як вправо, так і вліво (нормалізоване прямокутне зображення має розміри 512 x 64 пікселів, тому циклічний зсув його на 3 пікселя відповідає повороту вихідного зображення приблизно на 2º). Таким чином, враховуються кути повороту очі від -14º до 14º.

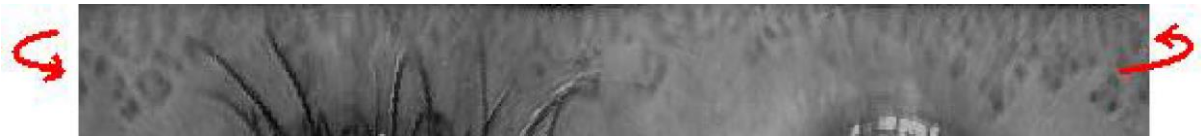


Рисунок 4.6 - Циклічний зсув нормалізованого зображення вправо

4.4 Результати роботи методу

При складанні результатів розглядалися зображення бази даних CASIA-IrisV3 (2655 зображень). Кожне зображення параметризовані описаним методом. Для вибору номерів функцій Ерміта, що беруть участь в параметризації, проведено аналіз, результати якого наведені в таблиці 4.1. У першому стовпці вказані значення $H_{m,n}$ = Ham(Lm, n), за якими відбувається порівняння зображень. У другому стовпці - кількість невірно визначилися очей з БД за відповідним значенням H, в третьому стовпці - це ж значення у відсотках від загальної кількості очей в базі даних.

З таблиці 4.1 видно, що найкращий результат досягається на значеннях $Ham(L_{1,0})$ + $Ham(L_{2,0}$) і $Ham(L_{1,0})$ + $Ham(L_{2,1})$, тому ці значення і взяті для порівняння райдужних оболонок. Всього в досліджуваній базі даних виявилося 22 зображення, для яких володар найближчій оболонки за значенням Ham $(L_{1,0})$ + $Ham(L_{2,0})$ не збігається з володарем райдужної оболонки за значенням Ham $(L_{1,0})$ + Ham $(L_{2,1}$), Що становить 0.82%.

Таблиця 4.1 - Результати аналізу методу для різного вибору значень індексів (m, n)

Значення	Кількість невірно визначених очей з БД за відповідним значенням H	Кількість невірно визначилися очей з БД за відповідним значенням H в %
$H_{1,0}$	56	2.1
$H_{1,1}$	62	2.33
$H_{2,0}$	238	8.96
$H_{2,1}$	251	9.45
$H_{0,1}$	176	6.62
$H_{3,0}$ і вище	понад 400	більше 15
$H_{1,0} + H_{2,0}$	15	0.56
$H_{1,0} + H_{2,1}$	21	0.79
$H_{1,1} + H_{2,0}$	22	0.82

Проведено порівняння запропонованого методу з існуючими методами ідентифікації особистості по райдужній оболонці ока. FAR - False Acceptance Rate - значення, що показує у відсотках, в скількох випадках метод визначив невірного володаря райдужної оболонки. FRR - False Rejection Rate - показник, що показує у відсотках, в скількох випадках метод не визначив володаря райдужної оболонки, присутнього в базі даних. Описаний алгоритм показав значення FAR = 0, FRR = 0.82% (22 зображення з 2655). Однак більшість з цих 22 зображень містять лише малу частину інформації про райдужну оболонку в області, що цікавить параметризації (повіку потрапляють в праву верхню чверть нормалізованого зображення). Приклад такого зображення наведено на рисунку 4.7. Якщо для цих зображень застосувати алгоритм, який визначає наявність століття [10], то цей алгоритм визначає повіку на 17 зображень з цих 22. Таким чином, залишається 5 зображень без перекриттів зображення райдужної оболонки на контрольній ділянці, на яких алгоритм не визначив володаря райдужної оболонки. Це становить 0.18% від всіх зображень в базі даних.

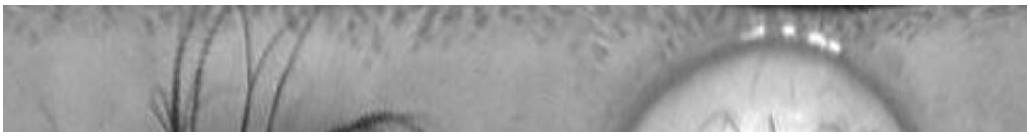


Рисунок 4.7 - Приклад нормалізованого зображення з накладенням століття на контрольну область розпізнавання

Таблиця 5.2 - Порівняння методів ідентифікації

МЕТОД	FAR (%)	FRR (%)	БАЗА ДАНИХ
Запропонований	0	0.82	CASIA-IrisV3
Запропонований з урахуванням визначення наявності повіку ока	0	0.18	CASIA-IrisV3
Tan	0.001	1.13	CASIA V1.0
Wildes	0.01	6.5	CASIA V1.0
Romero-Ramirez	0	9.71	CASIA V1.0

4.5 Висновки з розділу

Реалізовано модифікований метод ідентифікації людини за райдужною оболонкою ока на основі локальних характеристик райдужної оболонки. Експерименти показали високу якість ідентифікації, порівняну з середніми промисловими результатами. Зокрема, помилка другого роду 0,18% при помилці 1-го роду менш 0,01% (точніше неможливо уточнити на публічно доступних базах) дозволяє використовувати розроблену технологію для ідентифікації користувача в операційній системі і прикладних програмах.

Також слід зазначити, що перетворення райдужної оболонки в код на основі функцій Ерміта є повністю необоротним перетворенням, що дозволяє використовувати дану технологію в тому числі і в розподілених мережах, де накладені додаткові обмеження на характер переданої в мережі інформації.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

5.1 Загальні питання з охорони праці

Умови праці на робочому місці, безпека технологічних процесів, машин, механізмів, устаткування та інших засобів виробництва, стан засобів колективного та індивідуального захисту, що використовуються працівником, а також санітарно-побутові умови повинні відповідати вимогам нормативних актів про охорону праці. В законі України «Про охорону праці» [28] визначається, що охорона праці - це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження життя, здоров'я і працездатності людини у процесі трудової діяльності.

При роботі з обчислювальною технікою змінюються фізичні і хімічні фактори навколишнього середовища: виникає статична електрика, електромагнітне випромінювання, змінюється температура і вологість, рівень вміст кисню і озону в повітрі. Повітря забруднюється шкідливими хімічними речовинами антропогенного походження за рахунок деструкції полімерних матеріалів, які використовуються для обробки приміщень та обладнання. Неправильна організація робочого місця сприяє загальному і локальній напрузі м'язів шиї, тулуба, верхніх кінцівок, викривлення хребта і розвитку остеохондрозу. На всіх підприємствах, в установах, організаціях повинні створюватися безпечні і нешкідливі умови праці. Забезпечення цих умов покладається на власника або уповноважений ним орган (далі роботодавець). Умови праці на робочому місці, безпека технологічних процесів, машин, механізмів, устаткування та інших засобів виробництва, стан засобів колективного та індивідуального захисту, що використовуються працівником, а також санітарно-побутові умови повинні відповідати вимогам нормативних актів про охорону праці. Роботодавець повинен впроваджувати сучасні засоби техніки безпеки, які запобігають виробничому травматизмові, і забезпечувати санітарно-гігієнічні умови, що запобігають виникненню професійних захворювань працівників. Він не має права вимагати від працівника виконання роботи, поєднаної з явною небезпекою для життя, а також в умовах, що не відповідають законодавству про охорону праці. Працівник має право відмовитися від дорученої роботи, якщо створилася виробнича ситуація, небезпечна для його життя чи здоров'я або людей, які його оточують, і навколишнього середовища.

5.1.1 Правові та організаційні основи охорони праці

Основним організаційним напрямом у здійсненні управління в сфері охорони праці є усвідомлення пріоритету безпеки праці і підвищення соціальної відповідальності держави, і особистої відповідальності працівників.

Державна політика в галузі охорони праці визначається відповідно до Конституції України Верховною Радою України і спрямована на створення належних, безпечних і здорових умов праці, запобігання нещасним випадкам та професійним захворюванням. Відповідно до статті 3 Закону України «Про охорону праці» [28] (далі – Закону) законодавство про охорону праці складається з Закону, Кодексу законів про працю України [29], Закону України "Про загальнообов'язкове державне соціальне страхування від нещасного випадку на виробництві та професійного захворювання, які спричинили втрату працездатності" [30] та прийнятих відповідно до них нормативно-правових актів, норм міжнародного договору (ратифіковані Конвенції і Рекомендації МОТ, директиви Європейської Ради).

На законодавчому рівні визначено такі пріоритетні напрямки з безпеки праці:

– кожен працівник несе безпосередню відповідальність за порушення зазначених Законом, нормами і правилами вимог;

– напрямки реалізації конституційного права громадян на їх життя і здоров’я в процесі трудової діяльності:

– пріоритет життя і здоров’я працівників по відношенню до результатів виробничої діяльності підприємства;

– повна відповідальність роботодавця за створення належних – безпечних і здорових умов праці;

– соціальний захист працівників, повне відшкодування збитків особам, які потерпіли від нещасних випадків на виробництві та професійних захворювань;

– комплексне розв’язання завдань охорони праці;

– підвищення рівня промислової безпеки шляхом забезпечення суцільного технічного контролю за станом виробництв, технологій та продукції, а також сприяння підприємствам у створенні безпечних та нешкідливих умов праці;

– соціальний захист працівників, повне відшкодування збитків особам, які потерпіли від нещасних випадків на виробництві та професійних захворювань;

– використання економічних методів управління охороною праці, участь держави у фінансуванні заходів щодо охорони праці;

– використання світового досвіду організації роботи щодо поліпшення умов і підвищення безпеки праці на основі міжнародної співпраці.

Користувачі персональних комп'ютерів, для яких ця робота є головною, підлягають медичним оглядам: попереднім — під час влаштування на роботу і періодичним — протягом професійної діяльності раз на два роки. Жінок з часу встановлення вагітності та в період годування дитини грудьми до роботи з ПК не допускають.

Наявні трудові відносини між працівниками і роботодавцями в Україні за темою дипломного проекту регулюються Кодексом законів про працю (КЗпП) України, відповідно до якого права працюючої людини на охорону праці охороняються всебічно та норми охорони праці неухильно інтегровані до правил внутрішнього розпорядку організації/підприємства.

5.1.2 Організаційно-технічні заходи з безпеки праці

В організації/підприємстві проводиться навчання і перевірка знань з питань охорони праці відповідно до вимог Типового положення про порядок проведення навчання і перевірки знань з питань охорони праці, затвердженого наказом Держнаглядохоронпраці України від 26.01.2005 N 15, зареєстрованого в Міністерстві юстиції України 15.02.2005 за N 231/10511 [31].

Обов'язковими вимогами враховане наступне:

– ознайомлення з правилами безпеки праці, одержання відповідних інструктажів засвідчується у журналі інструктажів.

– перед допуском до самостійної роботи кожен працівник має право на навчання з питань охорони праці і роботодавець зобов'язаний, і проводить таке навчання у вигляді двох інструктажів з питань охорони праці:

1) вступного, який проводять працівники служби охорони праці об'єкта господарювання з усіма працівниками, яких приймають на роботу незалежно від їхньої освіти та стажу роботи за програмою, в якій подають загальні питання охорони праці із врахуванням її особливостей на об'єкті господарювання;
2) первинного, який проводять керівники структурних підрозділів на місці праці з кожним працівником до початку їхньої роботи на цьому робочому місці.
3) Проходження працівником цих інструктажів з питань охорони праці підтверджується записами у відповідних журналах обліку інструктажів і

скріплюється підписами осіб, які проводили інструктажі та осіб, які отримали інструктажі.

4) Повторний (не рідше одного разу в 6 місяців);
5) Позаплановий (при зміні правил охорони праці);
6) Поточний (проводять з працівниками перед виконанням робіт, на яких оформляється наряд-допуск)

– обов'язкові організаційні заходи перед початком, під час і після завершення роботи повинні включати перевірку (візуально) наявності і справності електрообладнання та його заземлення, а під час виконання роботи вимогу «не залишати без нагляду обладнання, яке працює». Після закінчення роботи - вимагається прибирання робочого місця, відключення всіх електроприладів від електромережі.

5.2 Аналіз стану умов праці

Робота над методом ідентифікації людини за райдужкою ока проходитиме в офісі. Для даної роботи достатньо однієї людини, для якої надано робоче місце зі стаціонарним комп'ютером.

5.2.1 Вимоги до приміщень

Геометричні розміри приміщення зазначені в табл. 5.1.

Таблиця 5.1 – Розміри приміщення

Найменування	Значення
Довжина, м	6
Ширина, м	3
Висота, м	2,5
Площа, $м^2$	18
Об'єм, $м^3$	45

Згідно з [32] розмір площі для одного робочого місця оператора персонального комп'ютера має бути не менше 6 кв. м, а об'єм — не менше 20 куб. м. Отже, дане приміщення цілком відповідає зазначеним нормам.

Для забезпечення потрібного рівного освітленості кімната має вікно та систему загального рівномірного освітлення, що встановлена на стелі. Для дотримання вимог пожежної безпеки встановлено порошковий вогнегасник та систему автоматичної пожежної сигналізації.

5.2.2 Вимоги до організації місця праці

При порівнянні відповідності характеристик робочого місця нормативним основні вимоги до організації робочого місця за [33] і відповідними фактичними значеннями для робочого місця, констатуємо повну відповідність.

Таблиця 5.2 - Характеристики робочого місця

Найменування параметра	Фактичне значення	Нормативне значення
Висота робочої поверхні, мм	750	680 ÷800
Висота простору для ніг, мм	730	не менше 600
Ширина простору для ніг, мм	660	не менше 500
Глибина простору для ніг, мм	700	не менше 650
Висота поверхні сидіння, мм	470	400 ÷500
Ширина сидіння, мм	400	не менше 400
Глибина сидіння, мм	400	не менше 400
Висота поверхні спинки, мм	600	не менше 300
Ширина опорної поверхні спинки, мм	500	не менше 380
Радіус кривини спинки в горизонтальній площині, мм	400	400
Відстань від очей до екрану дисплея, мм	800	700 ÷800

Приміщення кабінету має об’єм 45 м^3, площу – 18 м^2.

Температура в приміщенні протягом року коливається у межах 18–24°С, відносна вологість — близько 50%. Система вентилювання приміщення — природна неорганізована, а опалення — централізоване.

Розміщення вікон забезпечує природне освітлення з коефіцієнтом природного освітлення не менше 1,5%, а загальне штучне освітлення, яке здійснюється за допомогою восьми люмінесцентних ламп, забезпечує рівень освітленості не менше 200 Лк.

За ступенем пожежної безпеки приміщення належить до категорії В.

5.2.3 Навантаження та напруженість процесу праці

За фізичним навантаженням робота відноситься до категорії легкі роботи (Іа), її виконують сидячи з періодичним ходінням. Щодо характеру організування виконання дипломної роботи, то він підпадає під нав'язаний режим, оскільки певні розділи роботи необхідно виконати у встановлені конкретні терміни. За ступенем нервово-психічної напруги виконання роботи можна віднести до II – III ступеня і кваліфікувати як помірно напружений – напружений за умови успішного виконання поставлених завдань.

Під час виконання робіт використовують ПК та периферійні пристрої (лазерні та струменеві), що призводить до навантаження на окремі системи організму. Такі перекоси у напруженні різних систем організму, що трапляються під час роботи з ПК, зокрема, значна напруженість зорового аналізатора і довготривале малорухоме положення перед екраном, не тільки не зменшують загального напруження, а навпаки, призводять до його посилення і появи стресових реакцій.

Наявні психофізіологічні небезпечні та шкідливі фактори:

а) фізичного перевантаження:

- статичного;
- динамічного;

б) нервово-психічного перевантаження:

- розумового перенапруження;
- монотонності праці;
- перенапруження аналізаторів;
- емоційних перевантажень.

Роботу за дипломним проектом визнано, таку, що займає 50% часу робочого дня та за восьмигодинної робочої зміни рекомендовано встановити додаткові регламентовані перерви тривалістю 15 хв через кожну годину роботи.

5.3 Виробнича санітарія

На підставі аналізу небезпечних та шкідливих факторів при виробництві (експлуатації), пожежної безпеки можуть бути надалі вирішені питання необхідності забезпечення працюючих достатньою кількістю освітлення, вентиляції повітря, організації заземлення, тощо.

5.3.1 Аналіз небезпечних та шкідливих факторів при виробництві (експлуатації) виробу

Роботу, пов'язану з ЕОП з ВДТ, у тому числі на тих, які мають робочі місця, обладнані ЕОМ з ВДТ і ПП, виконують із забезпеченням виконання НПАОП 0.00-7.15-18 [36] «Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями», які встановлюють вимоги безпеки до обладнання робочих місць, до роботи із застосуванням ЕОМ з ВДТ і ПП. Переважно роботи за проектами виконують у кабінетах чи інших приміщеннях, де використовують різноманітне електрообладнання, зокрема персональні комп'ютери (ПК) та периферійні пристрої.

Основними робочими характеристиками персонального комп'ютера є наступні:

- робоча напруга U = +220В ± 5%;
- робочий струм I = 2А;
- споживана потужність P = 350 Вт.

Робоче місце має відповідати вимогам Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних машин, затверджених постановою Головного державного санітарного лікаря України від 10.12.98 N 7 [33].

Аналіз небезпечних та шкідливих виробничих факторів виконується у табличній формі (табл. 5.3).

Таблиця 5.3 – Аналіз небезпечних і шкідливих виробничих факторів

Небезпечні і шкідливі виробничі фактори	Джерела факторів (види робіт)	Кількісна оцінка	Нормативні документи
1	2	3	4
Фізичні			
- підвищений рівень напруги електричної мережі, замикання якої може відбутися через тіло людини	-//-	4	[34]
- недостатність природного світла	порушення умов праці (вимог до приміщень)	2	[35]
- недостатнє освітлення робочої зони	порушення гігієнічних параметрів виробничого середовища	3	[35]
Психофізіологічні:			

Продовження табл. 5.3

1	2	3	4
- нервово-психічна перевантаження (розумове, перенапруження аналізаторів-зорових)	- пошук інформації для постановки теми; - пошук та аналіз аналогів і літератури; - пошук наявних технологій, моделювання та аналіз алгоритмів; - виконання роботи за темою диплома, тестування; - оформлення роботи	4	[36] [33]
- фізичні (статичне – сидіння)	порушення умов праці (організації місця праці- сидіння користувача,) та організації робочого часу - безпервна робота)	2	[36] [33]

5.3.2 Пожежна безпека

Приміщення оснащено системою автоматичної пожежної сигналізації, має 1 вогнегасник ВП-5 із зарядом вогнегасної речовини 8-12 кг, відповідно до вимог чинного законодавства України. Проходи до засобів пожежогасіння вільні, не захаращуються та у разі потреби забезпечувати евакуацію всіх людей, які перебувають у приміщенні через один евакуаційний вихід з дверима на шляху евакуації, що відчинятися в напрямку виходу з будівлі від робочого місця. В приміщенні наявна затверджена «План-схема евакуації з кабінету (приміщення)».

Пожежна безпека при застосуванні ЕОМ забезпечується:

1) системою запобігання пожежі,

2) системою протипожежного захисту,

3) організаційно-технічними заходами.

Згідно ДБН В.2.5-28:2018 [35] таке приміщення, площею 25 м^2, відноситься до категорії "В" (пожежонебезпечної) та для протипожежного захисту в ньому проектом передбачено устаткування автоматичною пожежною сигналізацією із застосуванням датчиків-сповіщувачів РІД-1 (сповіщувач димовий ізоляційний) в кількості 1 шт., і застосуванням первинних засобів пожежогасіння.

Горючими матеріалами в приміщенні, де розташовані ЕОМ, є:

1) поліамід – матеріал корпусу мікросхем, горюча речовина, температура самозаймання 420º С,

2) полівінілхлорид – ізоляційний матеріал, горюча речовина, температура запалювання 335º С, температура самозаймання 530º С,

3) склотекстоліт ДЦ – матеріал друкарських плат, важкогорючий матеріал, показник горючості 1.7А, не схильний до температурного самозаймання,

4) пластикат кабельний №.489 – матеріал ізоляції кабелів, горючий матеріал, показник горючості більше 2.1,

5) деревина – будівельний і обробний матеріал, з якого виготовлені меблі, горючий матеріал, показник горючості більше 2.1, температура запалювання 255º С, температура самозаймання 399º С.

Продуктами згорання, що виділяються на пожежі, є: окис вуглецю; сірчистий газ; окис азоту; синильна кислота; акромін; фосген; хлор і ін. При горінні пластмас, окрім звичних продуктів згорання, виділяються різні продукти термічного розкладання: хлорангідридні кислоти, формальдегіди, хлористий водень, фосген, синильна кислота, аміак, фенол, ацетон, стирол.

5.4 Гігієнічні вимоги до параметрів виробничого середовища

Збільшення освітленості сприяє поліпшенню працездатності навіть в тих випадках, коли процес праці практично не залежить від зорового сприйняття. При поганому освітленні людина швидко втомлюється, працює менш продуктивно, виникає потенційна небезпека помилкових дій і нещасних випадків.

Освітленість приміщення має велике значення при роботі на ПЕОМ. Вона багато в чому визначається колірною і мережевий обстановкою. Для зменшеного поглинання світла стеля і стіни вище панелей (1,5-1,7м.). Якщо вони не облицьовані звукопоглинальним матеріалом, фарбуються білою водоемульсійною фарбою (коефіцієнт відбиття повинен бути не менше 0,7). Для забарвлення стіни панелей рекомендується віддавати перевагу світлим фарбам.

Природне освітлення, коли робочі місця з ПЕОМ розташовуються в один ряд по довжині приміщення на відстані 0,8 - 1,0 м від стіни з віконними прорізами, і екрани знаходяться перпендикулярно цієї стіни. Основний потік природного світла при цій повинен бути зліва. Не допускається спрямування основного світлового потоку природного світла праворуч, ззаду і спереду працює на ПЕОМ. Оптимальна відстань очей до екрана відео монітора повинна становити 60-70 см, допустиме не менше 50 см. Розглядати інформацію ближче 50 см не рекомендується.

У приміщенні, де розташовані ЕОМ передбачається природне бічне освітлення, рівень якого відповідає ДБН В.2.5-28:2018 [35]. Джерелом природного освітлення є сонячне світло. Регулярно повинен проводитися контроль освітленості, який підтверджує, що рівень освітленості задовольняє [33] і для даного приміщення в світлий час доби достатньо природного освітлення.

Розрахунок освітлення.

Для будівель виробництв світловий коефіцієнт приймається в межах 1/6 - 1/10:

$$\sqrt{a^2 + b^2} \cdot S_b = (1/8 \div 1/10) \cdot S_n \tag{5.1}$$

де S_b – площа віконних прорізів, м^2;

S_n – площа підлоги, м^2.

$$S_n = a * b = 6 * 3 = 18 м^2$$

$$S_{вік} = 1/8 * 18 = 2{,}25 м^2$$

Приймаємо 2 вікна площею $S = 1{,}13 м^2$ кожне.

Розрахунок штучного освітлення виробляється по коефіцієнтах використання світлового потоку, яким визначається потік, необхідний для створення заданої освітленості при загальному рівномірному освітленні. Розрахунок кількості світильників *n* виробляється по формулі (5.2):

$$n = \frac{E \cdot S \cdot Z \cdot K}{F \cdot U \cdot M} \tag{5.2}$$

де *E* – нормована освітленість робочої поверхні, визначається нормами – 300 лк;

S – освітлювана площа, м^2; S = 18 м^2;

Z – поправочний коефіцієнт світильника (Z = 1,15 для ламп розжарювання та ДРЛ; Z = 1,1 для люмінесцентних ламп) приймаємо рівним 1,1;

K – коефіцієнт запасу, що враховує зниження освітленості в процесі експлуатації – 1,5;

U – коефіцієнт використання, залежний від типу світильника, показника індексу приміщення і т.п. – 0,575

M – число люмінесцентних ламп в світильнику – 2;

F – світловий потік лампи – 5400лм (для ЛБ-80).

Підставивши числові значення у формулу (4.2), отримуємо:

$$n = \frac{300 * 18 * 1{,}1 * 1{,}5}{5400 * 0{,}575 * 2} \approx 1$$

Приймаємо освітлювальну установку, яка складається з одного світильника, який складаються з 2-х люмінесцентних ламп загальною потужністю 160 Вт, напругою – 220 В.

5.5 Вентилювання

Здійснюється провітрювання приміщення, в залежності від погодних умов, тривалість повинна бути не менше 10 хв. Найкращий обмін повітря здійснюється при наскрізному провітрюванні.

5.6 Розрахунок захисного заземлення (забезпечення електробезпеки будівлі).

Загальний опір захисного заземлення визначається за формулою:

$$R_{ззп} = \frac{R_з \cdot R_п}{R_п \cdot n \cdot \eta_з + R_з \cdot \eta_п}, \quad (5.3)$$

де Rз - опір заземлення, якими когут бать труби, опори, кути і т.п., Ом;

Rш - опір опори, яке з'єднує заземлювачі, Ом;

п - кількість заземлювачів;

ηз - коефіцієнт екранування заземлювача; приймається в межах 0,2 ÷ 0,9; ηз = 0,7

ηш - коефіцієнт екранування сполучної стійки; приймається в межах 0,1 ÷ 0,7; ηш = 0,5;

Опір заземлення визначається за формулою:

$$R_з = \frac{\rho}{2\pi \cdot l} \cdot \left(\ln \frac{2 \cdot l}{d} + \frac{1}{2} \ln \frac{4 \cdot t + l}{4 \cdot t - l} \right), \quad (5.4)$$

де ρ - питомий опір ґрунту, залежить від типу грунту, Ом·м;

для піску - 400 ÷ 700 Ом·м; приймаємо ρ = 400 Ом·м;

l - довжина заземлювача, м; для труб - 2-3 м; l = 3 м;

d - діаметр заземлювача, м; для труб - 0,03-0,05 м; d = 0,05 м;

t - відстань від середини забитого в ґрунт заземлювача до рівня землі, м; t = 2 м.

$$R_з = \frac{400}{2 \cdot 3{,}14 \cdot 3}\left(\ln\frac{2 \cdot 3}{0{,}05} + \frac{1}{2}\ln\frac{4 \cdot 2 + 3}{4 \cdot 2 - 3}\right) = 110 \text{ , Ом}$$

Опір смуги, що з'єднує заземлювачі, визначається за формулою:

$$R_ш = \frac{\rho}{2\pi \cdot L} \cdot \ln\frac{2 \cdot L^2}{b \cdot t^1}\text{ ,} \qquad (5.5)$$

де L - довжина смуги, що з'єднує заземлювачі (м) і приблизно дорівнює периметру будівлі: $П_{буд.} = 42 \cdot 2 + 38 \cdot 2 = 160$ м; L = 160 м;

b - ширина смуги, м; b = 0,03 м;

t_1 - глибина заземлення від рівня землі, м; t_1 = 0,5 м.

$$R_п = \frac{400}{2 \cdot 3{,}14 \cdot 160} \cdot \ln\frac{2 \cdot 160^2}{0{,}03 \cdot 0{,}5} = 5{,}99\text{, Ом}$$

Кількість заземлювачів захисного заземлення визначається за формулою:

$$n = \frac{2 \cdot R_з}{4 \cdot \eta_з}\text{,} \qquad (4.6)$$

де 4 - допустимий загальний опір, Ом;

2 - коефіцієнт сезонності.

Визначаємо загальний опір захисного заземлення:

$$R_{ззп} = \frac{110 \cdot 5{,}99}{5{,}99 \cdot 79 \cdot 0{,}7 + 110 \cdot 0{,}5} = 1{,}7 \text{ Ом}$$

Висновок: дане захисне заземлення буде забезпечувати електробезпеку будівлі, так як

виконується умова: $R_{ззп} < 4$ Ом.

При виникненню пожеж при роботі на ПЕОМ від таких можливими джерел запалювання як:

– іскри і дуги коротких замикань;

– перегрів провідників, резисторів та інших радіодеталей ПЕОМ, від тривалої перевантаження та наявність перехідного опору;

– іскри при розмиканні і розмиканні ланцюгів;

– розряди статичної електрики;

– необережному поводженню з вогнем, а також вибухи газо-повітряних і паро-повітряних сумішей.

4.7 Екологія

Діяльність за темою магістерської роботи, а саме: метод ідентифікації людини за райдужкою ока в процесі її виконання впливає на навколишнє природнє середовище і регламентується нормами діючого законодавства: Законом України «Про охорону навколишнього природного середовища» [38], Законом України «Про забезпечення санітарного та епідемічного благополуччя населення» [39], Законом України «Про відходи» [40].

В процесі діяльності з виконанням дипломного проектуванням виникають процеси поводження з відходами ІТ галузі. Нижче надано перелік відходів, що утворюються в процесі роботи:

– Відпрацьовані люмінесцентні лампи - I клас небезпеки.

– Змінні носії інформації - IV клас небезпеки.

– Відпрацьовані вогнегасники - IV клас небезпеки.

– Макулатура - IV клас небезпеки.

Висновки до розділу

В даному розділі проведено аналіз потенційних небезпечних та шкідливих виробничих факторів, причин пожеж. Розглянуті заходи, які дозволяють забезпечити гігієну праці і виробничу санітарію. На підставі аналізу розроблені заходи з техніки безпеки та рекомендації з пожежної профілактики.

Завданням даної магістерської роботи було розглянути метод ідентифікації людини за райдужкою ока, і як результат було проаналізовано цей метод. Згідно з аналізу в подальшому розроблятиметься реальна система. Так як в процесі проектування використовувалося інформація із Інтернету та ін., то аналіз потенційно небезпечних і шкідливих виробничих чинників виконується для умов праці з використанням персонального комп'ютера на якому буде аналізуватися метод ідентифікації людини за райдужкою ока.

ВИСНОВКИ

Результатом виконаної атестаційної роботи магістра є розв’язання актуальної наукової задачі розробки й дослідження методів ідентифікації людини за райдужною оболонкою ока.

ІТ ідентифікації людини, з застосуванням мультимодальних біометричних методів, має суттєві переваги. Завдяки поєднання методів, що враховують відразу кілька біометричних характеристик, можна підвищити захищеність інформаційних ресурсів від несанкціонованого доступу загалом.

В роботі запропонований модифікований метод ідентифікації людини, на основі локальних характеристик райдужної оболонки ока, знайдені локальним методом перетворення Ерміта. Він дозволяє значно зменшувати кількість збережених ключових точок райдужної оболонки без сильної втрати якості розпізнавання. Послідовне використання методу знаків і методу ключових точок дозволяє отримати надійний метод розпізнавання. Цей метод досить перспективний для використання в мультибіометричних системах розпізнавання людей. При побудові коду райдужної оболонки використовуються тільки найбільш інформативні функції перетворення Ерміта.

На основі методу перетворення Ерміта розроблений також метод, який використовує тільки ключові точки райдужної оболонки. Цей метод дозволяє значно зменшувати кількість збережених ключових точок райдужної оболонки без сильних втрат в якості розпізнавання.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1) Иванов А. И. Биометрическая идентификация личности по динамике подсознательных движений [Текст] – Пенза: Издательство Пензенского государственного университета, 2000 – 188 с..

2) Голубев Г. А. Современное состояние и перспективы развития биометрических технологий [Текст] / Г. А. Голубев, Б. А. Габриелян // Нейрокомпьютеры. Разработка. Применение. № 10, 2004, – С. 39 – 46.

3) Беленков В. Д. Электронные системы идентификации подписей [Текст] – Защита информации. Конфидент. 1997, № 6, – С.39 – 42.

4) Plomondon R. Automatic signature verification and writer identification – the state of the art [Text] / Plomondon R., Lorette G. // Pattern Recognition 1999 – Vol. – 22, № 2 – p. 107 – 131.

5) Диденко С. М. Автореферат диссертации: «Разработка и исследование компьютерной модели динамики системы «пользователь-мышь»» [Текст] – Тюмень 2007. – 25 с.

6) Расторгуев С. П. Программные методы защиты информации в компьютерах и сетях [Текст] – М.:“Яхтсмен”, 1993. – 150 с.

7) Рыбченко Д. Е. Критерии устойчивости и индивидуальности клавиатурного почерка при вводе ключевых фраз [Текст] // Специальная техника средств связи. Серия. Системы, сети и технические средства конфиденциальной связи. – Пенза, ПНИЭИ, 1997 – Выпуск № 2. – С.104 –107.

8) Колядин Д. В. О проблеме верификации подписи в системах контроля доступа. [Електроний ресурс] – Режим доступу: http://cs.mitp.ru/docs.research/signature.html

9) Griess F. D. Project Report: Online signature verification [Electronic resource]/ Griess F. D., Jain A. F. – Access to the reousrce: http://www.cse.msu.edu/cgi-user/web/tech/document?ID=449

10) Дворянкин С. В. Речевая подпись [Текст] / Под ред. заслуженного деятеля науки РФ, д.т.н. проф. А. В. Петракова. – М.: РИО МТУСИ, 2003 – С. 183 – 184.

11) Широчин В. П. Динамическая аутентификация на основе анализа клавиатурного почерка. [Електронний ресурс] / В. П. Широчин, А. В. Кулик, В. В. Марченко – Режим доступу: http://www.masters.donntu.edu.ua/2002/fvti/aslamov/files/bio_autentification.htm

12) Resources Related to Biometrics and People with Disabilities. [Electronic resource] – The International Center for Disability Resources on the Internet. – Access: http://www.icdri.org/biometrics/biometrics.htm.

13) Рабинер Л. Р. Цифровая обработка речевых сигналов: Пер. с англ. [Текст]/ Л. Р.

Рабинер, Р. В. Шафер / Под ред. М. В. Назарова, Ю. Н. Прохорова.– М.: Радио и связь, 1981.– 495 с.

14) Рыбченко Д. Е. Анализ клавиатурного почерка аппаратом нечетких множеств для целей ограничения доступа и аудита [Текст] / Д. Е. Рыбченко, А. И. Иванов // Специальная техника средств связи. Серия. Системы, сети и технические средства конфиденциальной связи. – Пенза, ПНИЭИ, 1996 – Выпуск №1., – С.116 – 119.

15) Болл Р.М. Руководство по биометрии [Текст] / Пер. с англ. Н.Е. Агаповой. – М.: Техносфера, 2007. – 368 с.

16) Лебеденко Ю.И. Биометрические системы безопасности. [Текст] – Тула: Изд-во ТулГУ, 2012 – 160 с.

17) Matt Bishop Introduction to Computer Security [Text] – University of California - Davis – ISBN: 0321247442

18) Flom L. Iris recognition system [Text] / Flom L., Sar A. // United States Patent 4641349. Filed February 20, 1985.

19) Daugman J. High condence personal identication by rapid video analysis of iris texture [Text] // Proc. IEEE Internat. Carnahan conf. on security technology, 1992. – P. 50-60.

20) Wildes R.P. A system for automated iris recognition [Text] / Wildes R.P., Asmuth J.C., Green G.L. et al. // Proc. of the 2nd IEEE Workshop on Applications of Computer Vision. 1994. – P. 121-128.

21) Boles W. A human identication technique using images of the iris and wavelet transform [Text] / Boles W., Boashash B. // IEEE Trans. Signal Process. 1998. – V.46. – N.4. – P.1185-1188.

22) Multiple Biometric Grand Challenge (MBGC - 2007) [Electronic resource] // Access: http://www.nist.gov/ itl/iad/ig/mbgc.cfm

23) John Daugman High Confidence Visual Recognition of Persons by a Test of Statistical Independence [Text] // IEEE Transaction on Pattern Analysis and Machine Intelligence – vol. 15 – no. 11 – p. 1148-1161, 1993.

24) R. P. Wildes Iris Recognition: An Emerging Biometric Technology [Text] // Proceedings of The IEEE – vol. 85 – no. 9 – p. 1348-1363, 1997.

25) Соколов І.А., Будзко В.І., Синіцин І.М., Побудова інформаційно-телекомунікаційних систем високої доступності [Текст] / І.А. Соколов, В.І. Будзко, І.М. Синіцин // Системи високої доступності, 2005 – т.1 – №1 – с. 6-14.

26) Синіцин І.М. Метрологічні і біометричні технології і системи [Текст] / І.М. Синіцин, А.В. Губін, О.С. Ушмаєв // Історія науки і техніки. – №7, 2008 – С.41-44.

27) База даних CASIA-IrisV3 [Електроний ресурс] / Режим доступу: http://www.cbsr.ia.ac.cn/IrisDatabase.htm.

28) Закон України "Про охорону праці". Вводиться в дію Постановою ВР № 2695-XII

від 14.10.92, ВВР, 1992, № 49, ст.669. - Режим доступу: www. URL: https://zakon.rada.gov.ua/laws/show/2694-12

29) Кодекс законів про працю України. Затверджується Законом № 322-VIII від 10.12.71 ВВР, 1971. Режим доступу: www. URL: https://zakon.rada.gov.ua/laws/show/322-08

30) Закон України "Про загальнообов'язкове державне соціальне страхування від нещасного випадку на виробництві та професійного захворювання, які спричинили втрату працездатності". Наказ від 21 грудня 2000 року N 2180-III. Режим доступу: www. URL: https://dnaop.com/html/2065/doc-zakon-ukrajini-pro-zagalynoobovjazkove-derzhavne-socialyne-strahuvannya-vid-neshhasnogo-vipadku-na-virobnictvi-ta-profesijnogo-z

31) Про затвердження Типового положення про порядок проведення навчання і перевірки знань з питань охорони праці (НПАОП 0.00-4.12-05). Наказ від 26.01.2005 №15. Режим доступу: www. URL: https://zakon.rada.gov.ua/laws/show/z0231-05

32) Санітарні норми мікроклімату виробничих приміщень ДСН 3.3.6.042-99. Постанова N 42 від 01.12.99. Режим доступу: www. URL: https://zakon.rada.gov.ua/rada/show/va042282-99

33) Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ДСанПІН 3.3.2.007-98. Затверджено Постановою Головного державного санітарного лікаря України 10 грудня 1998 р. N 7. Режим доступу: www. URL: https://zakon.rada.gov.ua/rada/show/v0007282-98

34) Електробезпека в будівлях і спорудах. Вимоги до захисних заходів від ураження електричним струмом. Наказ від 1 липня 2016 року N 204. Режим доступу: www. URL: http://epicentre.co.ua/dstu/doc28522.html

35) ДБН В.2.5-28:2018 «Природне і штучне освітлення». Режим доступу: www. URL: http://www.minregion.gov.ua/wp-content/uploads/2018/12/V2528-1.pdf

36) НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями». Зареєстровано в Міністерстві юстиції України 25 квітня 2018 р. за № 508/31960. Режим доступу: www. URL: https://zakon.rada.gov.ua/laws/show/z0508-18

37) ДСТУ Б В.1.1-36:2016 «Визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою». Наказ від 15.06.2016 №158. Режим доступу: www. URL: https://zakon.rada.gov.ua/rada/show/v0158858-16

38) Закон України «Про охорону навколишнього природного середовища» . Вводиться в дію Постановою ВР № 1268-XII від 26.06.91, ВВР, 1991, № 41, ст.547. Режим доступу: www. URL: https://zakon.rada.gov.ua/laws/show/1264-12

39) Закони України «Про охорону навколишнього природного середовища». Вводиться в дію Постановою ВР № 4005-XII від 24.02.94, ВВР, 1994, № 27, ст.219. Режим

доступу: www. URL: https://zakon.rada.gov.ua/laws/show/4004-12

40) Закон України «Про відходи». Відомості Верховної Ради України (ВВР), 1998, № 36-37, ст.242. Режим доступу: www. URL: https://zakon.rada.gov.ua/laws/show/187/98-вр

ДОДАТОК А.

Електронні плакати

МЕТОД ІДЕНТИФІКАЦІЇ ЛЮДИНИ ЗА РАЙДУЖКОЮ ОКА

Виконав: ст.гр.КІ-18дм
Любенецький Д.А.
Керівник: доц. Барбарук В.М.

Біометричні системи аутентифікації

- Біометричні системи аутентифікації - системи аутентифікації, що використовують для посвідчення особи людей їх біометричні дані.
- Біометрична аутентифікація - процес докази і перевірки автентичності заявленого користувачем імені, через пред'явлення користувачем свого біометричного способу і шляхом перетворення цього образу відповідно до заздалегідь визначеним протоколом автентифікації.

Технології біометричної аутентифікації

Відбиток пальця

Райдужна оболонка ока

Геометрія обличчя

Геометрія руки

Підшкірні вени

Структура ДНК

Мотівація

Технологія	Плюси	Мінуси
Пароль, PIN -код, ключові слова і так далі	1. Низька вартість 2. Немає необхідності носити аутентифікатор 3. Висока швидкість розпізнавання при роботі з великими базами	1. Користувачі часто застосовують короткі легко підбирані паролі 2. Існують можливості перехоплення паролів 3. Необхідність регулярно міняти паролі 4. Складно запам'ятати велику кількість паролів
Відбиток пальця, особливості райдужної оболонки ока, форми кисті рук і т.д.	1. Унеможливлюється несанкціонованого використання аутентифікатора; 2. Забезпечується висока міра захисту від імітації; 3. Відпадає необхідність обов'язкового носіння аутентифікатора; 4. Виключається втрата або псування аутентифікатора, забудькуватість, передача третім особам і т.п.); 5. Відсутні витрати на виготовлення, купівлю	1. Неможливо отримати статичний ключ 2. Можливість помилок першого і другого роду (пропуск або помилкова тривога)

Мета роботи та постановка задачі

Метою роботи є розробка модифікованого методу ідентифікації людини за райдужною оболонкою ока на основі перетворення Ерміта, що використовує локальні характеристики райдужної оболонки.

Для досягнення поставленої мети необхідно вирішити такі задачі:

- проаналізувати сучасні підходи, методи і системи біометричної ідентифікації та аутентифікації користувачів;
- дати опис перетворенню Ерміта стосовно до задачі обробки зображень;
- вирішити задачу ідентифікації по райдужній оболонці ока;
- описати та розробити метод розпізнавання людини по райдужній оболонці ока на основі згорток з функціями перетворення Ерміта;
- провести ряд експериментів за допомогою базі даних CASIA-IrisV3.

Класифікація методів ідентифікації

Рисунок 1

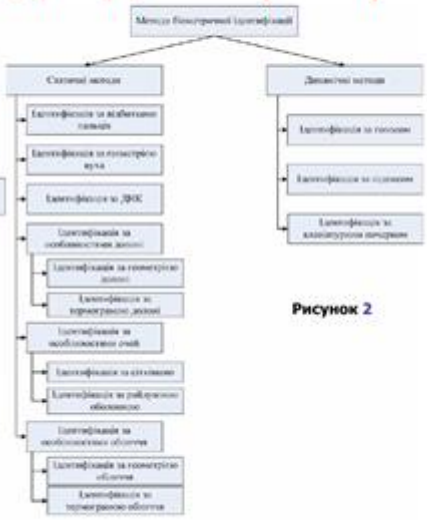
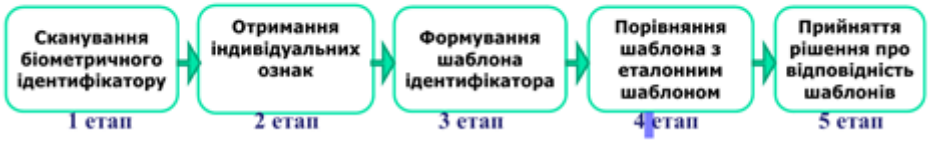


Рисунок 2

Методи біометричної ідентифікації людини

Метод отримання біометричних параметрів	Ймовірність відмови у доступі %	Ймовірність помилкової ідентифікації «чужого» (без використання муляжу) %	Ймовірність помилкової ідентифікації «чужого» (з використанням муляжу) %	Збереження технічних образу у процесі ідентифікації абонента	Вартість технічної реалізації в грошовому еквіваленті, у.о.
Геометрична будова руки	0,2…4	0,2…1	10…75	Неможливо присвоїти	Від 600 до 3000
Відбитки пальців	2…6	0,0001	10…70	Неможливо присвоїти	Від 60 до 600
Особливості малюнка сітківки ока	0,4	6…10	_____	Неможливо присвоїти	Приблизно 4000
Райдужна оболонка ока	0,2…2	0,0001	_____	Неможливо присвоїти	Від 500 до 6000
Портрет обличчя	1…9	_____	_____	Неможливо присвоїти	55000
Рукописний почерк	0,5…5	0,5…5	0,5…5	5-10…10-40	_____
Клавіатурний та контактний почерк	3…9	3…9	_____	5-10…10-12	_____
Характеристики і особливості мови	0,5…5	0,5…5	25…90 (запис)	10-15…10-30	1…60

Принципи функціонування системи біометричної ідентифікації



Спрощена структурна схема системи біометричної ідентифікації

Ідентифікація на основі параметрів геометрії ока

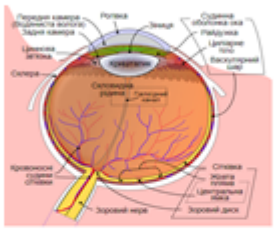


Рисунок 1 – Елементи райдужної оболонки

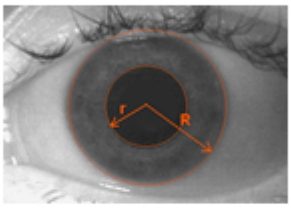


Рисунок 2 – Райдужна оболонка ока з радіусом R ≈ 5,5 мм зовнішньої межі й радіусом внутрішньої межі r = 0,1R...0,7R

Метод розпізнавання на основі райдужної оболонки ока

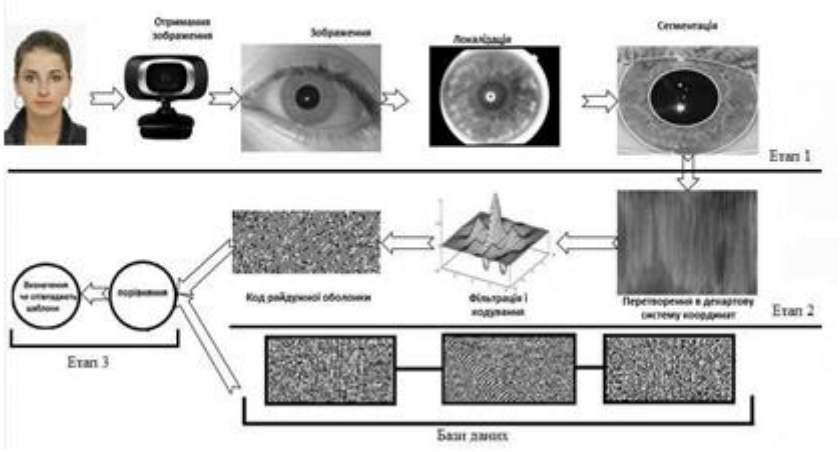
Спрощена схема процеса ідентифікації на основі РОО

Виділення РОО на зображенні ока

Зміна розмірів РОО й зіниці при зміні умов освітлення

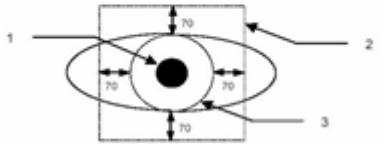
Виділення роговиці на зображенні.
Даний етап полягає:
- у пошуку на отриманому зображенні відносно темного об'єкта, близького за формою до кола, що містить усередині себе ще один концентричний темніший об'єкт (зіницю). У більшості систем на даному етапі необхідно забезпечити виконання тільки однієї умови – усередині зіниці повинен знаходитися яскравий відблиск певної форми (відблиск від освітлювача).

Біометрична система заснована на райдужці ока



Аналіз зображення райдужної оболонки

Рисунок 1 – Порівняльна характеристика EER



(1.Межа зіниці, 2. Межа зображення 3.Межа райдужки)
Рисунок 2 - Необхідний масштаб зображення

$$FAR \times N^2 \approx 1 \Rightarrow N \approx \sqrt{\frac{1}{FAR}}$$

Ймовірність помилки за одиницю часу може сильно варіюватися, але якщо взяти допустимим одну помилку протягом робочого дня, то отримуємо

Перетворення Ерміта

$$\psi_n(x) = \frac{(-1)^n e^{x^2/2}}{\sqrt{2^n n!\sqrt{\pi}}} \cdot \frac{d^n(e^{-x^2})}{dx^n}, \quad \varphi_n(x) = \frac{e^{-x^2/2}}{\sqrt[4]{\pi}} \cdot \psi_n(x)$$

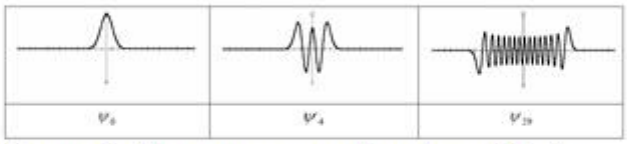


Рисунок 1 - Приклади одновимірних функцій Ерміта

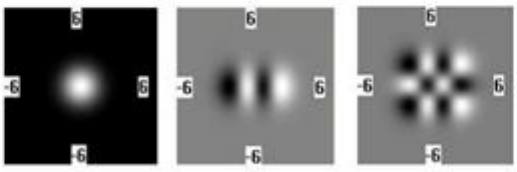


Рисунок 2 - Приклади двовимірних функцій Ерміта

Задача ідентифікації людини за райдужною оболонкою ока

Загальна схема розв'язання задачі ідентифікації по райдужній оболонці ока

Метод ідентифікації людини за райдужною оболонкою ока

Виділення райдужної оболонки ока

$$X_{cent} = \arg\min_{x} \sum_{y} I(x,y)$$

$$Y_{cent} = \arg\min_{y} \sum_{x} I(x,y)$$

Уточнення центру зіниці й кордонів райдужної оболонки

$$\max_{r,x_0,y_0} \left| G_\sigma(r) * \frac{\partial}{\partial r} \oint_{r,x_0,y_0} \frac{I(x,y)}{2\pi r} ds \right|$$

Кордони райдужної оболонки

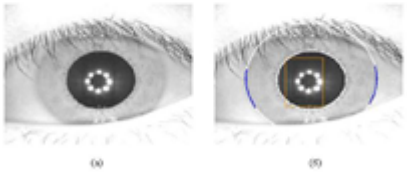


Рисунок 1 - (а) - вихідне зображення; (а) - зображення з виділеної райдужки

Нормалізація райдужної оболонки

Рисунок 2 - (а) - зображення ока з введеної псевдополярної системою координат; (б) нормалізоване зображення райдужної оболонки

Метод ідентифікації людини за райдужною оболонкою ока

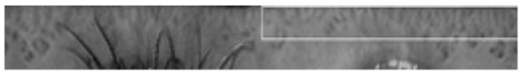


Рисунок 1 - Нормалізоване зображення з виділеної контрольної області

Параметризація райдужної оболонки і складання бінарних кодів.

$$L_{m,n}(x_0, y_0) = \mathrm{sgn}(I(x, y)) * m.n(x, y))(x_0, y_0).$$

Порівняння зображень райдужних оболонок.

Результати роботи методу

Таблиця 1 - Результати аналізу методу для різного вибору значень індексів (m, n)

Значення	Кількість невірно визначених очей з БД за відповідним значенням H	Кількість невірно визначилися очей з БД за відповідним значенням H в %
$H_{1,0}$	56	2.1
$H_{1,1}$	62	2.33
$H_{2,0}$	238	8.96
$H_{2,1}$	251	9.45
$H_{2,1}$	176	6.62
$H_{3,0}$ і вище	понад 400	більше 15
$H_{1,0}+H_{3,0}$	15	0.56
$H_{1,0}+H_{2,1}$	21	0.79
$H_{1,1}+H_{2,0}$	22	0.82

Таблиця 2 - Порівняння методів ідентифікації

МЕТОД	FAR (%)	FRR (%)	БАЗА ДАНИХ
Запропонований	0	0.82	CASIA-IrisV3
Запропонований з урахуванням визначення наявності повіку ока	0	0.18	CASIA-IrisV3
Tan	0.001	1.13	CASIA V1.0
Wildes	0.01	6.5	CASIA V1.0
Romero-Ramirez	0	9.71	CASIA V1.0

Результати роботи методу

Таблиця 1 - Результати аналізу методу для різного вибору значень індексів (m, n)

Значення	Кількість невірно визначених очей з БД за відповідним значенням H	Кількість невірно визначилися очей з БД за відповідним значенням H в %
$H_{1,0}$	56	2.1
$H_{1,1}$	62	2.33
$H_{2,0}$	238	8.96
$H_{2,1}$	251	9.45
$H_{2,1}$	176	6.62
$H_{3,0}$ і вище	понад 400	більше 15
$H_{1,0}+H_{3,0}$	15	0.56
$H_{1,0}+H_{2,1}$	21	0.79
$H_{1,1}+H_{2,0}$	22	0.82

Таблиця 2 - Порівняння методів ідентифікації

МЕТОД	FAR (%)	FRR (%)	БАЗА ДАНИХ
Запропонований	0	0.82	CASIA-IrisV3
Запропонований з урахуванням визначення наявності повіку ока	0	0.18	CASIA-IrisV3
Tan	0.001	1.13	CASIA V1.0
Wildes	0.01	6.5	CASIA V1.0
Romero-Ramirez	0	9.71	CASIA V1.0

Висновки

Реалізовано модифікований метод ідентифікації людини за райдужною оболонкою ока на основі локальних характеристик райдужної оболонки.

Експерименти показали високу якість ідентифікації, порівняно з середніми промисловими результатами. Зокрема, помилка другого роду 0,18% при помилку 1-го роду менш 0,01% (точніше неможливо уточнити на публічно доступних базах) дозволяє використовувати розроблену технологію для ідентифікації користувача в операційній системі і прикладних програмах.