МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ФЕСЕНКО Андрій Олексійович

УДК 004.056.5:57.087.1(043.3)

МЕТОДИ ОБРОБКИ ДАНИХ ДЛЯ СИСТЕМ ІДЕНТИФІКАЦІЇ ТА АУТЕНТИФІКАЦІЇ НА ОСНОВІ БІОМЕТРИЧНИХ ХАРАКТЕРИСТИК ОКА

05.13.21 – системи захисту інформації

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2017

Дисертацією є рукопис.

Робота виконана на кафедрі засобів захисту інформації в Національному авіаційному університеті Міністерства освіти і науки України.

Науковий керівник: кандидат технічних наук, доцент
Швець Валеріян Анатолійович,
Національний авіаційний університет,
доцент кафедри засобів захисту інформації.

Офіційні опоненти: доктор технічних наук, професор
Рибальський Олег Володимирович, Національна академія внутрішніх справ МВС України, професор кафедри інформаційних технологій;

кандидат технічних наук, доцент
Карпінець Василь Васильович, Вінницький національний технічний університет, доцент кафедри менеджменту та безпеки інформаційних систем.

Захист відбудеться «27» червня 2017 р. о 15^{00} годині на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті за адресою: 03058, Київ, пр.Космонавта Комарова, 1.

З дисертацією можна ознайомитись в науково–технічній бібліотеці Національного авіаційного університету за адресою: 03058, Київ, пр.Космонавта Комарова, 1.

Автореферат розісланий «27» травня 2017 р.

В.о. ученого секретаря
спеціалізованої вченої ради
д.т.н. професор В.П.Квасніков

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. У кожному суспільстві можна виділити сектори, системи або мережі порушення функціонування яких може привести до колапсу на загальнодержавному, регіональному або місцевому рівнях. Комплекс цих секторів, систем або мереж може входити в склад критичної інфраструктури (таких як, атомна енергетика, авіаційна галузь, хімічна промисловість та інші). Розвиток сучасних інформаційних та комунікаційних технологій (ІКТ), які є основою критичної інфраструктури, характеризується постійним підвищенням рівня вимог до їх безпеки.

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 ІКТ 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.

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 з іншими біометричними об'єктами, ідентифікація по райдужці є стабільнішою і надійною.

Питанням розробки і дослідження нових біометрих методів ідентифікації та аутентифікації в різний час займалися такі вітчизняні й закордонні вчені як В. Вишневський, Я. Дорогий, С. Садиков, А. Саченко, С. Теленик, Л. Чала, М. Шлезінгер, Дж. Даугман та ін.

У 2000–х роках до вирішення завдань розпізнавання по райдужній оболонці ока підключилося безліч наукових лабораторій, найбільших результатів домоглися: група, очолювана Prof. J.Daugman в Cambrige University, UK; група, очолювана Prof. K.Bowyer в University of Notre Dame, IN, USA; Prof. Hugo Proenca, University of Beira Interior, Portugal; Prof. Adam Czajka, Warsaw University of Technology, Poland. У середині 2000–х років почали з'являтися програмно–апаратні комплеск розпізнавання по райдужній оболонці ока, з них найбільш відомими є системи Panasonic, LG, OKI.

Однак у цій галузі є низка завдань які потребують доопрацювання: створення сучасних засобів сканування, поліпшення процедур попередньої обробки зображення, підвищення швидкодії, зменшення об’єму оброблюваної інформації, розв’язання яких має важливе наукове та практичне значення. З цих позицій розробка, удосконалення і дослідження

методів обробки даних (зокрема, процедур попередньої обробки) для систем ідентифікації та аутентифікації на основі біометричних характеристик людського ока є актуальним науковим завданням.

Зв'язок роботи з науковими програмами, планами, темами. Одержані результати дисертаційної роботи безпосередньо пов’язані з виконаням держбюджетних науково–дослідних робіт Національного авіаційного університету та з «Основними науковими напрямами та найважливішими проблемами фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук НАНУ на 2014–2018 роки», з Стратегією національної безпеки України від 26 травня 2015 року № 287/2015 у контексті п. 4.12 «Реформування системи технічного і криптографічного захисту інформації з урахуванням практики держав–членів НАТО та ЄС», НДР 23/14.01.04 «Системи контролю доступу по біометричними ознаками людини».

Мета і задачі дослідження. Метою роботи є підвищення ефективності методів обробки даних в системах ідентифікації та аутентифікації користувачів по райдужній оболонці ока. Під ефективністю розуміємо зменшення об’єму оброблюваної інформації в базах даних систем контролю і управління доступом та підвищення швидкодії обробки даних.

Для досягнення поставленої мети необхідно розв’язати такі **задачі:**

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

2) удосконалити інтегрально–диференціальнйи метод локалізації зображення райдужної оболонки ока для зниження обчислювальних витрат;

3) розробити більш ефективний метод кодування райдужної оболонки ока;

4) розробити метод прийняття рішень для біометричних систем ідентифікації та аутентифікації;

5) розробити програмні засоби для проведення експериментальних дослідженнь запропонованих методів.

Об'єктом дослідження є процес обробки даних в біометричних системах ідентифікації та аутентифікації по райдужній оболонці ока.

Предметом дослідження є методи та моделі попередньої обробки даних в системах ідентифікації та аутентифікації на основі біометричних характеристик людського ока.

Методи дослідження. Використано методи цифрової обробки зображень, методи цифрової фільтрації, методи проектування баз даних, теорія ймовірності для прийняття рішення про аутентифікацію користувача, методи математичної статистики – для оброблення результатів експериментальних досліджень, комп'ютерного моделювання. Моделювання і обробка даних здійснювалася за допомогою програмного забезпечення Matlab та мови програмування C++.

Наукова новизна отриманих результатів полягає в наступному:

1. Удосконалено інтегрально–диференціальний метод локалізації зображення райдужної оболонки ока, який за рахунок попередньої НЧ–

фільтрації (інтегрування) дозволяє зменшити локальні зміни інтенсивності пікселів, а наступна ВЧ–фільтрація (диференціювання) дозволяє виділити межі райдужної оболонки ока, така послідовність дій дозволяє знизити обчислювальні витрати при збереженні високої точності.

2. Вперше запропоновано метод кодування зображення райдужної оболонки ока, який за рахунок фазових відгуків при обробці модифікованим DoG–фільтром зображення райдужної оболонки ока, дозволяє кодувати один піксель зображення, одним бітом інформації і як наслідок зменшує об'єм бази даних систем контролю і управління доступом.

3. Отримав подальший розвиток метод прийняття рішень на основі статистичних критеріїв Неймана–Пірсона, який за рахунок використання нормавоної відстані Хеммінга в біометричних системах ідентифікації по райдужній оболонці ока, дає змогу не зберігати в базі даних еталонне зображення.

Практичне значення одержаних результатів полягає у наступному:

- Удосконалено інтегрально–диференціальний алгоритм локалізації зображення для зменшення області пошуку райдужної оболонки та зменшення обчислювальних витрат.
- Розроблено алгоритм кодування райдужної оболонки ока, за рахунок використання в системах контролю і управління доступом модифікованого DoG–фільтра для отримання бінарного коду райдужки.
- Розроблені програмні модулі попередньої обробки зображення райдужки, DoG–фільтра, обчислення відстані Хеммінга та порогу, модуль порівняння кодів райдужок і прийняття рішень по статистичному критерію.
- Запропонована система ідентифікації та аутентифікації користувача без еталонного зображення райдужки, за допомогою застосування бінарного коду райдужки (фазові відгуки DoG–фільтра) і нормованої відстані Хеммінга з використанням статистичного критерію Неймана–Пірсона, що дало змогу зменшити об'єм бази даних систем контролю і управління доступом, що в свою чергу зменшує час доступу до неї.

Результати дисертації використовуються у навчальному процесі кафедри засобів захисту інформації Національного авіаційного університету. Розроблені методи доведені до придатних інженерних рішень та були впроваджені в ПАТ «Миронівський хлібопродукт», ТОВ «Акксон Софт»

Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, що виносяться на захист, отримані автором самостійно. У роботах, написаних у співавторстві, автору належить:[1,2]– аналіз систем і підходів біометричної ідентифікації; [5]–дослідження і визначення оптимального критерію виявлення; [6]– програмне моделювання визначення меж райдужної оболонки ока; [7]–дослідження інформативності коефіцієнтів Фурьє для біометричних систем ідентифікації та аунтентифікації по райдужній оболонці ока.

Із робіт, опублікованих у співаавторсиві, у дисертаційній роботі використовуються результати, отримані особисто здобувачем.

Апробація результатів дисертації. Основні положення дисертаційної роботи доповідалися та обговорювалися на науково–технічних конференціях та семінарах, серед яких: Міжнародна науково–практична конференція «Актуальні питання забезпечення кібернетичної безпеки та захисту інформації» (Київ–2015); Всеукраїнська науково–практична конференція «Стан та удосконалення безпеки інформаційно–телекомунікаційних систем (SITS)» (Миколаїв, 2015 р.); Міжнародна науково–практична конференція «Інформаційні технології та взаємодії» (IT&I) (Київ, 2016); науково–практична конференція «Проблеми кібербезпеки інформаційно–телекомунікаційних систем» (Київ, 2017); Міжнародна науково–практична конференція «ABIA» (Київ, 2017 р.); Міжнародна науково–практична конференція «ITSEC» (Київ, 2017).

Публікації. За тематикою дослідження опубліковано 13 наукових праць, серед них 7 статей у фахових наукових виданнях та 6 у збірниках праць конференцій.

Структура та обсяг роботи. Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел. Загальний обсяг дисертації становить 155 сторінок, в тому числі 123 сторінки основного тексту, ілюстрацій – 40, таблиць – 12.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність теми дисертаційної роботи, зазначено її зв’язок з науковими програмами, планами та темами, сформульовано мету та задачі досліджень, охарактеризовано наукову новизну та практичне значення отриманих результатів. Наведено відомості про впровадження результатів роботи, їх апробацію та публікації.

У першому розділі охарактеризовано предмет дослідження, а також проведено аналіз сучасних підходів, методів і систем біометричної ідентифікації та аутентифікації користувачів кожен з яких, має свої переваги і недоліки. У табл. 1 наведено порівняння біометричних методів.

Проаналізувавши біометричні методи, визначимо найбільш важливі характеристики для відповідних систем, також зауважимо що деякі біометричні методи більш зручні, ніж інші. Найбільш важливими характеристики для біометричних методів ідентифікації є такі: 1) захищеність біометричного методу (універсальність, унікальність, ефективність, вимірність, стійкість до спроб обману, механічна міцність); 2) доступність для користувача; 3) вартість; 4) простота використання.

Метод ідентифікації по РОО має високу та середню відповідність вимог до перерахованих характеристик.

Унікальним для кожної особистості статичним ідентифікатором є райдужна оболонка людського ока.

Системи найбільш поширені на ринку СКУД з використанням райдужки та їх параметри представлені в табл. 2.

Таблиця 1

Порівняння біометричних характеристик із загальними вимогами

Біометрична Характеристика	Універсаль–ність	Унікаль–ність	Сталість	Вимірю–ваність	Ефектив–ність	Доступ–ність	Захище–ність
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
Райдужна оболонка ока	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 голосу	С	Н	Н	С	Н	В	Н
Клавіатурний почерк	Н	Н	Н	С	Н	С	С

Відповідность вимогам: Н – низька С – середня В – висока

Таблиця 2

Системи найбільш поширені на ринку СКУД з використанням райдужки

Система	Параметри					
	Фокусна відстань, м	Час на зйомку, с	Максимальна кількість записів в БД	Пропускна можливість системи користувачі в 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
Securimetrics Pier 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

Об’єм баз даних (БД) систем контролю і управління доступом (СКУД) на базі райдужної оболонки ока (РОО) залежить від розрядності коду. Якщо розрядність коду райдужки 8×256 біт, то ймовірність повторення коду райдужки (КР) приблизно 1:10000. Відповідно кількість еталонних записів в БД повинна бути менша ніж 10000 записів, отже для збільшення кількісті записів в БД СКУД по РОО потрібно отримати стійкий код РОО, який не буде повторюватися (буде унікальний для кожної з кількості 2^{33} особи).

Більшість біометричних технологій спроможні тільки на роботу в верифікаційному режимі порівняння "один до одного". У такому режимі особа спочатку декларується (картою або іншим способом), і програмою для

прийняття рішення "так/ні", а потім відшуковується запис і порівнює її із шаблоном досить виконати зіставлення з одним зареєстрованим шаблоном.

В даннний час є приклади використання технології розпізнавання райдужної оболонки в аеропортах, яка використовується для пасажирів міжнародних рейсів і може бути застосована замість пред'явлення ними паспорта. Пасажири, яким доводиться часто здійснювати авіаперельоти, змогли взяти участь в програмі Privium і отримати свій Iris–код, занесений в базу даних.

Таким чином вимоги до роботи СКУД змінюються, а саме: необхідна здатність алгоритмів розпізнавання райдужної оболонки працювати в ідентифікаційному режимі пошуку **"один до багатьох"**, в якому особа попередньо не декларуються і система повинна самостійно визначити особистість, здійснивши повний інтенсивний пошук в базі зареєстрованих даних. При великих обсягах пасажиропотоку об’єм БД системи збільшується у велику кількість разів. Тому задача зменшення об’єму БД і прискорення швидкості доступу до неї стає все більш актуальною.

Як показали результати аналізу, проведеного у першому розділі, зробимо наступний висновок: суттєвим недоліком систем ідентифікації та аутентифікації на основі біометричних характеристик ока є низька швидкість роботи та обмежена кількісь записів в БД СКУД по РОО.

Другий розділ присвячено методам попередньої обробки РОО.

Біометрична система може бути розділена на дві підсистеми: модуль реєстрації та модуль ідентифікації рис.1.

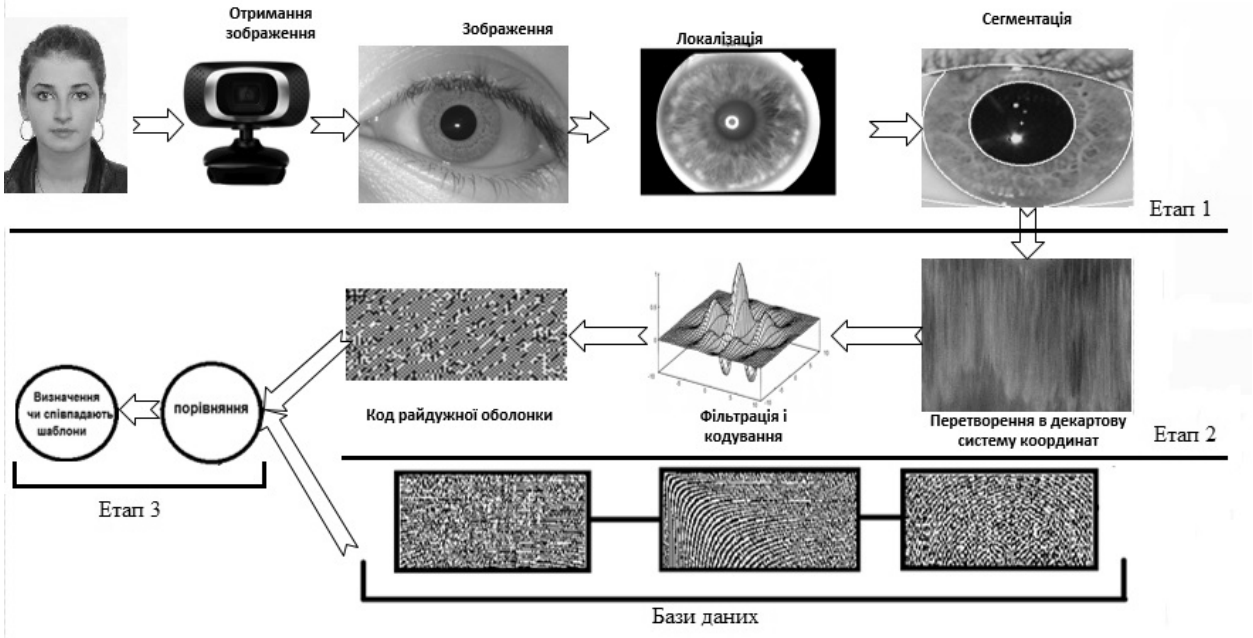

Рисунок 1– Біометрична система заснована на райдужці ока

Модуль ідентифікації відповідає за розпізнавання людини. У процесі ідентифікації, біометричний сенсор отримує характеристику людини, що підлягає ідентифікації і перетворює в формат шаблону. Отриманий шаблон

передається в блок зіставлення, який порівнює його з шаблонами, збереженими в базі даних, щоб визначити чи збігаються шаблони.

На першому етапі рис.1 із зображення обличчя локалізується зображення ока, а потім сегментується РОО.

В роботі пропонується наступне виділення області ока на зображенні, реалізація данного підходу описується за допомогою процедур 1–4.

Процедура 1: Отримане зображення обличчя людини *I(x,y)*, де $x=[1,M]$, $y=[1,N]$ N і M розмірність вхідного зображення, зазначимо, що розмірність має бути кратною 2.

Процедура 2: Виділення зони розташування ока $I'(x,y)$, згідно біометричних особливостей, де $x'=\left[1,\frac{M}{2}\right]$, $y'=\left[1,fix\frac{2N}{3}\right]$.

Процедура 3: Вирахування зміни яскравості $dI_{x'}=\begin{cases} I'_{x'} \le rift;\ dI_{x'} \\ I'_{x'} > rift;\ dI_{x'}+1. \end{cases}$,

$dI_{y'}=\begin{cases} I'_{y'} \le rift;\ dI_{y'} \\ I'_{y'} > rift;\ dI_{y'}+1. \end{cases}$

Процедура 4: Визначення області ока, використовуючи особливості зміни яскравості на зображенні $I'\{x',y'\}=\{\min(dI_{x''})\}\cap\{\min(dI_{y''})\}$.

Після виділення області знаходження РОО, для її локалізації використовується декілька методів (табл. 3), але вони мають певні недоліки

Таблиця 3

Методи які застосовуються в СКУД для отримання текстурних ознак РОО та їх недоліки

Метод	Недоліки
Робертса	Низька точність із–за використання маски 2x2. Розриви контурів зображення.
Собеля	Оснований на методі Робертса. Використовує маску 3x3. Розриви контурів. Використовуються попередньо визначені вагові коефіцієнти
Канні	Оснований на методі Робертса. Використовуються два порога. Використовує маску 3x3.Розрив контурів.
Перетворення Хафа	Потрібні повні апріорні дані (тип фігури). Повинна бути висока якість зображення.
Віоли–Джонса	Потрібні повні апріорні дані (тип фігури). Модельна робота методу. Необхідна точні налаштування.
Градієнтний інтегрально–деференціальний (широко застосовується в даний час)	Велика тривалість обчислень. Використовує градієнт яскравості.

Для усунення недоліків, а саме підвищення швидкодії градієнтного інтегрально–диференціального методу його було удосконалено. Дане удосконалення реалізується в процедурах 5–7.

Процедура 5: Сегментація зображення зіниці та РОО. В результаті отримуємо матрицю $I''(x,y)=I'(x',y')*H(x',y')$, де $H(x',y')$ – двомірна імпульсна характеристика інтегрально–диференціального фільтра, $I'(x',y')$ – зображення РОО.

Процедура 6: Знаходження радіусів райдужної оболонки ока і зіниці за допомогою використання псевдокоду

y=y'/2=const
for (n=1:x')
if min(I'(y',n))
$r_p=r_p+1$
end
if minmin(I'(y',n))
$r_i=r_i+1$
end
end.

Процедура 7: Перетворення з полярної в декартову систему координат. В результаті локалізації райдужки визначають кільцеву область, що підлягає аналізу. це дозволяє отримати еквівалентне представлення області аналізу у вигляді прямокутної області інтересу.

Порівняння швидкодії градієнтного інтегрально–диференціального метод і удосконаленого інтегрально–диференціального методу представлено на рис. 2.

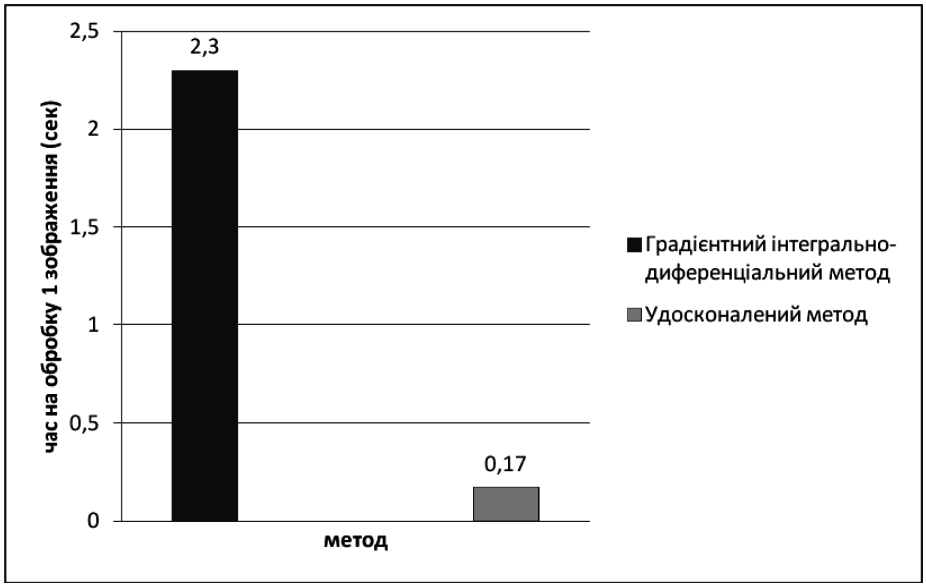

Рисунок 2– Порівняння швидкодії Градієнтного інтегрально–диференціальний метод і удосконаленого інтегрально–диференціального методу

Отримане прямокутне зображення РОО кодується. Для кодування РОО в даний час використовують фільтр Габора.

Фільтри Габора мають недолік, що полягає в недостатній обчислювальній ефективності. Для усунення недоліків розроблено більш ефективний метод кодування з використанням модифікованого DoG–фільтра.

Класичний DoG–фільтр був запропонований для отримання АЧХ яка наближалась до прямокутної форми, тобто мала більш крутий скат в порівнянні з фільтром Гауса і відсутностю бокових пелюсток.

В роботі для отримання *Iris*–коду РОО будемо застосовувати значення фаз відгуків фільтра. Але ці відгуки повинні мати постійний стрибок для їх відмінності. Виходячи з обробки сигналів ми знаємо, що якщо АЧХ проходе через 0 осі частот то фази гармонік отримують постійний стрибок на π. Щоб

фази вищих гармонік не стрибали при декількох переходах АЧХ через 0, потрібно щоб АЧХ мала всього один перехід через 0, а потім поступово наближалась по своєму значенню до 0. Таким чином фази гармонік фільтрованого зображення РОО будуть мати значення які знаходяться в межах від 0 до π та від π до 2π. Якщо АЧХ фільтра представ–вити кривою яка отримується різницею двох гаусіанів рис. 3 то імпульсну характерис–тику фільтра отримуємо як двовимірне дискретне перетворення Фур'є

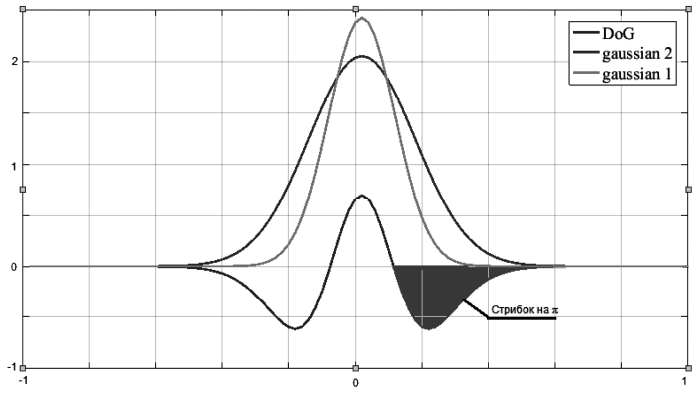

Рисунок 3–АЧХ модифікованого DoG–фільтра

$$\dot{h}(x,y)=\frac{1}{N^2}\sum_{k=1}^{k_{\max}}\sum_{n=1}^{n_{\max}}\{DoG\}e^{+j\frac{2\pi ik}{N}}, \qquad (1)$$

де *n, k* –довжина маски фільтра в частотній області, маска квадратна $m_{\max}=k_{\max}$, *x,y* – просторові координати – цілі числа.

АЧХ фільтра описується наступною формулою

$$DoG=\left[g(n,k\sigma_1)-g(n,k\sigma_2)\right], \qquad (2)$$

де $\sigma_2>\sigma_1$, $\sigma_2=S\sigma_1$, *S*– коефіцієнт розширення. $\sigma_1=\frac{\Delta\omega}{|\hat{\omega}|}$, де $\hat{\omega}=\pm1$ – нормована частота, $\Delta\omega\le|\hat{\omega}|$.

Фазовий відгук РОО отримується з виразу

$$\varphi_{Ir}=-\arctan\frac{\mathrm{Im}\left[I(x,y)*\dot{h}(x,y)\right]}{\mathrm{Re}\left[I(x,y)*\dot{h}(x,y)\right]} \qquad (3)$$

Операція в квадратних дужках – це згортка зображення РОО з імпульсною характеристикою удосконаленого DoG–фільтра.

Для кодування зображення РОО, використовується вираз

$$Iris=\begin{cases}1, & 0\le\varphi_{Ir}<\pi\\ 0, & \pi\le\varphi_{Ir}<2\pi\end{cases} \qquad (4)$$

Вибір розрядності кода райдужки. Так як зараз населення Землі становить 7.3×10^9 людей, то вірогідність спів падіння РОО буде $1.369\text{x}10^{-10}$. Для впевненості, що код КР райдужки не буде повторюватися, його розрядність повинна бути більша як 2^{33}. Сучасні процесори мають 64 розряди і для виключення помилки переповнення розрядної сітки будем використовувати 56 розрядів в одному стовпчику коду РОО, кількість стовпців буде відповідати кутовому дозволу 1°, тобто 360 стовпців. Загальна вірогідність повторення коду РОО буде визначаться як умовна ймовірність 56–ти розрядного кода з можливістю повторення в одном із 360 стовпчиків, $P(2^{-56}|360)=4{,}996\text{x}10^{-15}$.

Таким чином, можемо зробити наступний висновок: 1) Фільтр Габора поступається в обчислювальної ефективності DoG–фільтру. Тому система ознак на основі DoG–фільтра може виявитися більш ефективною. 2) Фази відгуку DoG–фільтра несуть інформацію про локальну структуру зображення і не чутливі до змін яскравості і контрасту. 3) Швидкодія DoG–фільтра є більш вища, ніж фільтра Габора (рис.4). Перераховані властивості дозволяють зробити висновок, що використання фазових відгуків DoG–фільтра в якості ознак текстури райдужки є перспективним.

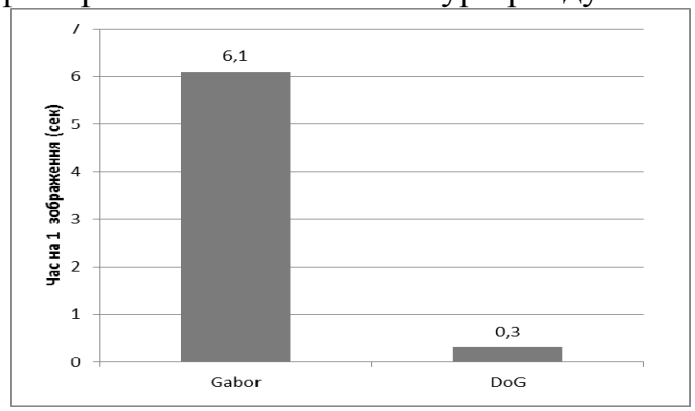

Рисунок 4 – Порівняння швидкодії фільтра Габора і модифікованого DoG–фільтра

Третій розділ присвячено розробці методів прийняття рішень щодо ідентифікації та аутентифікації користувачів з використанням біометрії.

Код райдужки складається із значень текстурних ознак у вузлах ортогональної сітки. Якщо використовуються фази відгуку вейвлету Габора, то на кожен вузол припадає два біта інформації. Для ознак на основі відгуку DoG–фільтра на один вузол припадає один біт. У системі ідентифікації КР обробляється наступним чином: 1) В процесі реєстрації КР зберігається в базі даних для подальшого порівняння; 2) При спробі розпізнавання, коли в систему надходить зображення райдужки, для неї обчислюється КР, який порівнюється з кожним кодом у БД.

В роботі пропонується у якості критерію міри схожості двох райдужок використовувати нормалізовану відстань Хеммінга (HD) між *N*–розрядними двійковими кодами ідентифікованої (I) райдужки і зареєстрованими (R) значеннями кодів, зберігаються в базі даних:

$$HD(IC_I, IC_R) = \frac{1}{N}\sum_{i=1}^{N} IC_{Ii} \oplus IC_{Ri,} \qquad (5)$$

де IC_I, IC_R – коди райдужок, IC_{Ii}, IC_{Ri} – *i*– ий біт код IC_A.

Для повністю співпадаючих КР нормована відстань Хеммінга буде дорівнювати 0. Максимальне значення *HD*=1. При введенні ідентифікованого зображення райдужки неминуче виникають спотворення, викликані зміною умов освітлення (зміни яскравості і контрасту), поворотом голови, що супроводжується поворотом отриманого зображення і його деформацією вздовж осей координат, зміною відстані до камери. Методи прийняття рішень повинні бути стійкими до цих спотворень, зрозуміло, у певних межах. Вибором системи ознак і нормалізацією зображення райдужки вдалося компенсувати можливі спотворення, крім спотворень повороту. Існуючі методи співставлення інформації про структуру райдужної оболонки з еталоном чутливі до бічного нахилу голови в процесі зйомки. Пропонується

методика, що дозволяє досягнути стійкості до повороту вхідного зображення. Вона передбачає зміну процедури реєстрації і новий метод ідентифікації. При реєстрації нового користувача метод передбачає створення з отриманого вхідного зображення декількох копій, повернених в обидві сторони на різні фіксовані кути. Для кожного такого зображення обчислюється код і всі вони поміщаються в БД. При ідентифікації код вхідного зображення буде порівнюватися з кодами всіх копій еталонів, а рішення про збіг двох райдужок приймається за мінімальною відстанню між ними. В якості міри схожості двох райдужок пропонується наступна величина:

$$HD_{\min}(IC_1, IC_2) = \min HD_i(IC_1, IC_2), \qquad (6)$$

де IC_1 – багатосекційний код у базі даних, i – номер секції, IC_2 – код розпізнаваної райдужки, HD_i – відстань Хеммінга між IC_2 и i – ї секцією IC_1.

Залежність відстані Хеммінга для КР від кута нахилу голови, отримана за допомогою розробленої системи експериментальних досліджень. Визначення цього кута може бути виконано на основі статистичного аналізу чутливості відстані Хеммінга до повороту. На рис.5 представлена залежність відстані Хеммінга для КР від кута нахилу голови, отримана за допомогою розробленої системи експериментальних досліджень.

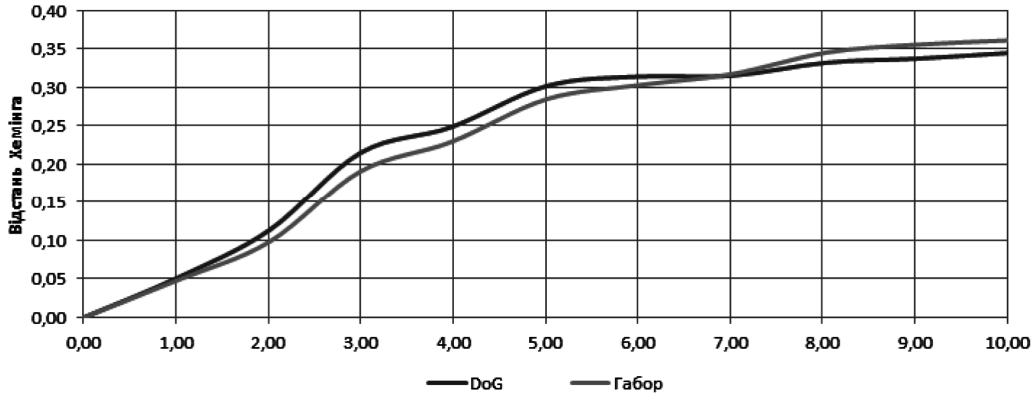

Рисунок 5 – Чутливості відстані Хеммінга до нахилу голови для фільтрів Габора $(\omega_0 = \pi/8, \theta = 0)$, і DoG–фільтра $(\sigma = 0{,}1)$

Якщо припустити, що біти ознак статистично незалежні, то математичне очікування відстані Хеммінга для різних райдужок повинно бути рівним 0,5. Для однакових райдужок за відсутності перешкод математичне очікування відстані Хеммінга і його дисперсія рівні 0. Під дією перешкод математичне очікування відстані Хеммінга для однакових райдужок збільшується і досягає межі 0,5. Вибір кутового кроку при формуванні шаблону райдужки є компромісом. З одного боку, за рахунок зниження впливу повороту зображення при зменшенні кутового кроку зменшується ймовірність прийняття хибного рішення, оскільки збільшується різниця математичних очікувань відстаней Хеммінга для однакових і різних райдужок. З іншого боку, це веде до збільшення розміру КР, і як наслідок, до збільшення часу ідентифікації.

Пропонується наступна методика вибору кутового кроку. Вибір кутового кроку $\Delta\alpha$ будемо розглядати як оптимізаційну задачу, яка має своєю метою мінімізацію наступної функції:

$$G(\Delta\alpha) = c_{AR} P_{AR}(\Delta\alpha) + c_{IA} P_{IA}(\Delta\alpha) + c_{ICC} V_{DB} \frac{2\alpha_{\max}}{\Delta\alpha}, \quad (7)$$

де c_{AR} – вартість втрат при забороні доступу зареєстрованому користувачеві, $P_{AR}(\Delta\alpha)$ – ймовірність заборони доступу зареєстрованому користувачеві, c_{IA} – вартість втрат при забороні доступу зареєстрованому користувачеві, $P_{IA}(\Delta\alpha)$ – ймовірність дозволу доступу незареєстрованому користувачеві, c_{ICC} – вартість одноразового обчислення відстані Хеммінга, V_{DB} – кількість користувачів, зареєстрованих в БД.

Залежності $P_{AR}(\Delta\alpha)$ і $P_{IA}(\Delta\alpha)$ можуть бути визначені наступним чином. Щільність ймовірностей відстані Хеммінга для КР незареєстрованих осіб залишається незмінною, що випливає з пропозиції про статистичної незалежності бітів КР. Щільність ймовірностей для відстані Хеммінга залежить від $\Delta\alpha$. При цьому до випадкової величини *HD* – відстані Хеммінга, для зареєстрованих райдужок, додається величина $\Delta HD(\Delta\alpha)$, розподіл якої визначається наведеним вище графіком чутливості. Закон розподілу результуючого випадкової величини $HD + \Delta HD(\Delta\alpha)$ виходить зсувом вихідного закону на величину $\Delta HD(\Delta\alpha)$. Знаючи закони розподілу ймовірностей відстані Хеммінга для зареєстрованих і незареєстрованих користувачів, можливо визначити $P_{AR}(\Delta\alpha)$ і $P_{IA}(\Delta\alpha)$. В існуючих системах поріг *C* вибирається однаковим для всіх райдужок. Якщо HD < C, фіксується збіг, інакше – розбіжність. Ймовірність прийняття помилкового рішення складається з двох частин:

$$P_{Error} = P_{AR} + P_{IA}, \quad (8)$$

де $P_{AR} = \int_{C}^{1} P_{Au}(HD_{\min}) dHD_{\min}$ – ймовірність заборони доступу зареєстрованому користувачеві, $P_{IA} = \int_{0}^{C} P_{lm}(HD_{\min}) dHD_{\min}$ – ймовірність дозволу доступу незареєстрованому користувачеві, *C* – значення порогу, P_{Au} – ймовірність появи на вході системи автентичній райдужки, P_{lm} – ймовірність появи на вході системи неаутентичної райдужки, $P_{Au}(HD)$ – умовна щільність розподілу відстані Хеммінга для аутентичних райдужек, $P_{lm}(HD)$ – умовна щільність розподілу відстані Хеммінга для неаутентичних райдужок.

При прийнятті рішення про збіг двох кодів можливо чотири результати. У двох випадках відповідь вірна, в двох інших – ні. Два правильні рішення – це дозвіл доступу авторизованому користувачеві і відмова в доступі неавторизованому. Неправильне рішення – це дозвіл доступу неавторизованому користувачу і, відповідно, відмова авторизованому.На Рис. 6 проілюстровано, як різні рішення пов’язані між собою.

Лівий горб, зображений білим, формує порівняння однакових очей з однаковими. Правий горб, намальований чорним, формує порівняння різних очей між собою. З цього графіка береться число, яке добре розділяє два горба. Для того щоб кількісно охарактеризувати роздільність двох класів

може бути використаний критерій роздільності *d*. Якщо μ_1 *і* μ_2 – математичні очікування, а ξ_1 і ξ_2 середньо–квадратичні відхилення, критерій *d* може використову–ватися для оцінки якості ознак. Чим краще роздільна здатність ознаки, тим більше значення приймає *d.* Методика вибору порогу детально розроблена статистичною теорією прийня–ття рішень. Три критерії вибору порогу: 1) критерій Байєса; 2) мінімаксний; 3) критерій Неймана–Пірсона.

$$d = \frac{|\mu_1 - \mu_2|}{\sqrt{(\xi_1^2 + \xi_2^2)/2}}. \qquad (9)$$

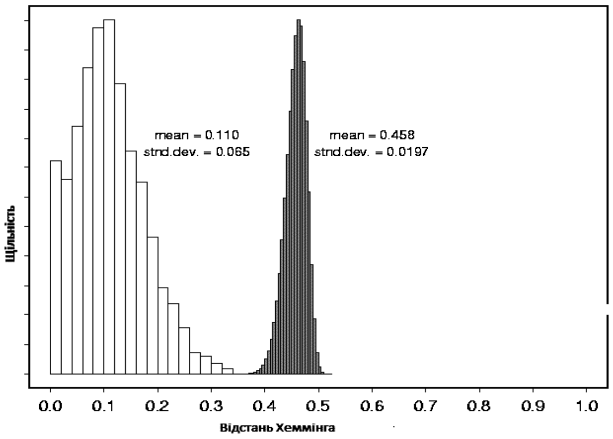

Рисунок 6 – Умовні щільності розподілу ймовірностей значень ВХ

Всі три критерії в залежності від ситуації можуть бути використані в системі ідентифікації особистості. Дослідження законів розподілу відстаней Хеммінга у присутності випадкових спотворень показали, що для різних райдужок закони розподілу можуть відрізнятися. На рис.7 наведено полігони частот для різних райдужок. Визначення нормалізованих відстаней Хеммінга для кожної пари спотворень зображень однієї і тієї ж райдужки дає оцінку закону розподілу відстаней Хеммінга для райдужок однієї людини. Порівняння кожного з перекручених зображень з безліччю зображень інших райдужок дає оцінку закону розподілу відстаней для райдужок порушників.

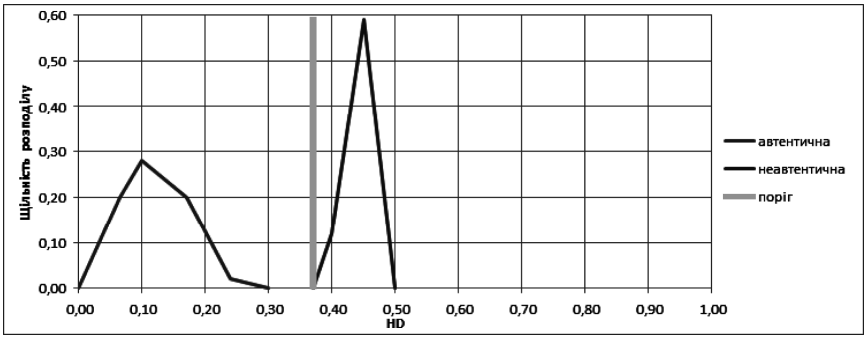

Рисунок 7 – Полігони частот для райдужок, що належать різним людям

При цьому використовувалась наступна модель спотворень:

$$I(x, y) = C(S(R(I(x, y))) + N(x, y), \qquad (10)$$

де *C* – перетворення яскравості і контрасту, *S* – перетворення масштабування, *R* – поворот, $I(x, y)$ – зображення, *N* – гаусів шум.

Розподіл ймовірностей для різних райдужок істотно відрізняються. Причина цього у властивостях структури зображення райдужної оболонки (наявність яскраво виражених особливостей, їх кількість і т.д.). Підвищення ефективності може бути досягнуто шляхом визначення індивідуального порогу для кожної райдужки з бази еталонів. Визначення індивідуального порогу відбувається в зміненою процедурою реєстрації. Комп'ютерними

методами моделюється введення великої кількості змінених райдужок, а оброблені дані можуть бути представлені у вигляді графіків, аналогічних рис.7, але обидві криві відповідають не всім, а єдиному класу. Отримане за результатом моделювання значення порогу зберігається в базі даних разом з кодом і використовується в процедурі ідентифікації.

Перевірка користувача є більш простим завданням. Для цього захоплює зображення райдужної оболонки і обчислюється код. У базі даних знаходиться відповідний запис на перевіряємого користувача і визначається нормована відстань Хеммінга *HD*. Якщо відстань *HD* нижче порога, перевірка вважається пройденою. Для прийняття рішення про автентичності користувача використовуються статистичні критерії. Вибір критерію залежить від апріорних даних РОО. Експериментально встановлено чутливість результатів порівняння райдужних оболонок до повороту зображення (нахилу голови при зйомці). У роботі пропонується методика, яка б знизила таку залежність і зменшує, таким чином, вірогідність можливої помилки. У процедуру реєстрації додано моделювання повороту вхідного зображення на певні кути і обчисленні кодів для кожного з них зі збереженням результатів в базі даних. Значення кутів повороту можуть бути визначені на основі аналізу чутливості нормалізованої відстані Хеммінга до повороту зображення. У зміненій процедурі ідентифікації рішення приймається по найменшій відстані з однієї з копій еталона.

Залежність обсягу бази даних від статистичного критерію наведено в табл.4.

Таблиця 4

Залежність обсягу бази даних від статистичного критерію

Об’єм бази даних на одного користувача				
Згідно ISO/IEC 19794–6:2011		65596 байт		Зменшення об’єму
Критерій	Байєса	65604 байт	немає	
	Неймана–Пірсона	2528 байт	В 25 раз	
	Мінімаксний	2536 байт	В 25 раз	

Висновки до розділу наступні: В якості критерія міри схожості для порівняння двох бінарних кодів РОО вибрано нормовану відстань Хеммінга, а розглянувши статистичні критерії вибору порогу для прийняття рішень визначено, що оптимальним критерієм буде критерій Неймана–Пірсона.

Четвертий розділ присвячено експериментальному дослідженню запропонованих у роботі методів.

У роботі запропонована система ідентифікації та аутентифікації користувача без еталонного зображення райдужки, яка складається з двох програмних модулів.

Модуль реєстрації виконує наступні функції: 1) отримання зображення райдужної оболонки ока; 2) локалізація райдужки ока; 3) нормалізація зображення райдужної оболонки; 4) виділення ознак, перетворення їх в формат шаблону, збереження в базі даних.

Модуль ідентифікації виконує наступні функції: 1) отримання зображення райдужної оболонки ока; 2) локалізація райдужки ока; 3) нормалізація зображення райдужної оболонки; 4) виділення ознак, перетворення їх в формат шаблону і порівняння з шаблонами, збереженими в базі даних; 5) прийняття рішення.

Оцінимо достовірність, з якою визначена роздільна здатність систем ознак, розглянутих в роботі, до яких входять математичні очікування і середньоквадратичні відхилення відстаней Хеммінга для однакових і різних райдужок.

Оцінка математичного очікування $\tilde{\mu}$ та дисперсії розподілена по нормальному закону і має параметри:

$$M(\tilde{\mu}) \approx \tilde{\mu}; D(\tilde{\mu}) \approx \frac{\xi^2}{n}, \tag{11}$$

де n – кількість реалізації випадкової величини.

Оцінка дисперсії $\tilde{\xi}^2$ розподілена по нормальному закону, має параметри:

$$M(\tilde{\xi}) \approx \tilde{\xi}; D(\tilde{\xi}^2) \approx \frac{2}{n-1}\tilde{\xi}^4. \tag{12}$$

Випадків порівняння ідентичних радужек в ході кожного експерименту було 676. Випадків порівняння різних райдужок – 1000. Випадків порівняння різних райдужок досить, щоб знехтувати похибкою оцінки математичного очікування і середньоквадратичного відхилення для нормованої відстані Хеммінга. Для експерименту з ознаками на основі DoG–фільтра найкращими параметрами використовуючи (10) отримуємо абсолютну помилку для математичного очікування 10^{-4}. Однак оскільки значення визначалися з точністю до другого знака після коми $\tilde{\mu} = 0{,}17 \pm 0{,}005$ з ймовірністю близькою до 1. За формулою (11) отримуємо помилку для дисперсії 10^{-7}. З урахуванням того, що результати були отримані з точністю до другого знака після коми $\tilde{\xi}^2 \approx 0{,}05 \pm 0{,}005$. Згідно з правилами наближених обчислень можна зробити висновок, що два знака після коми критерію d можна вважати вірними. Для значень d в інших експериментах, можна зробити такий же висновок.

Для порівняння запропонованого методу з методом Дж. Даугмана, необхідно розрахувати P_N– ймовірність вірного пропуску користувача, яка залежить від FAR– значення коефіцієнта помилкового пропуску, та кількості зареєстрованих зображень РОО. В експерименті значення FAR було обрано 10^{-3} при наявності 676 зображень РОО. Тоді отримаємо розрахункове P_N=0,9934.

Крім цього, в експериментальній частині роботи були отримані наступні результати:

1. При експериментах з фільтрами Габора з постійними параметрами були отримані наступні оптимальні параметри фільтру: $(\omega_0 = \pi/8, \theta = 0)$ кількість блоків коду 8×256. При цьому досягається значення критерію якості ознак $d = 1.99$.

2. При експериментах з DoG–фільтрами з постійними параметрами були отримані наступні параметри фільтра: = 0,1; кількість коду 56×360. При цьому досягається значення критерію якості ознак $d = 2.20$.

3. Провівши порівняння з відомим методом табл. 5, робимо висновок, що запропонований метод не поступається в якісних показниках існуючому методу.

Таблиця 5

Результат експериментальних досліджень

Параметр	Метод Дж.Даугмана	Запропонована система
Кількість помилок	6±1	6±1
Позитивних рішень	669±3	670±2
Виміряне FAR	0,00447±0,00410	0,00298±0,00554
Виміряне P_N	0,99553±0,00600	0,99702±0,04460

У додатках вміщено акти впроваджень результатів дисертаційної роботи та фрагменти кодів програм, що відображають практичну частину дисертаційного дослідження.

ВИСНОВКИ

Результатом виконаної роботи є розв’язання актуальної наукової задачі розробки й дослідження методів обробки даних (зокрема, процедур попередньої обробки) для систем ідентифікації та аутентифікації користувачів на основі біометричних характеристик людського ока, які використовуються на об’єктах критичної інфраструктури.

У процесі виконання дисертації отримані такі вагомі результати:

1. На основі проведеного аналізу сучасних підходів, методів і систем біометричної ідентифікації користувачів обрано один з найбільш надійних методів ідентифікації та аутентифікації, а саме індентифікація по райдужній оболонці ока, який по сукупності якостей має вагомі переваги перед іншими, а також має великі перспективи застосування в СКУД.

2. Удосконалено інтегрально–диференціальний метод локалізації зображення райдужної оболонки ока, який за рахунок удосконаленого алгоритму локалізації ока на зображенні, дозволяє зменшити область пошуку меж райдужної оболонки та знизити обчислювальні витрати при збереженні високої точності методу та підвищує швидкодію в 13,5 раз.

3. На основі запропонованого алгоритмічного рішення розроблено метод кодування РОО при застосуванні модифікованого DoG–фільтра, що дало можливість підвищити швидкодію в 20 разів для попередньої обробки зображень РОО завдяки отриманню однозначного бінарного кода, що в свою чергу дало можливість зменшити об’єм БД в 25 разів.

4. Розроблено метод прийняття рішень для систем біометричної ідентифікації і аутентифікації з використанням статистичного критерію Неймана–Пірсона на основі КР без еталонного зображення РОО з використанням нормованої відстані Хеммінга.

5. У роботі запропонована система ідентифікації та аутентифікації користувача без еталонного зображення райдужки (складається з двох програмних модулів), за допомогою застосування бінарного коду райдужки (фазові відгуки DoG–фільтра) і нормованої відстані Хеммінга з використанням статистичного критерію Неймана–Пірсона, що дало змогу зменшити об’єм бази даних систем контролю і управління доступом, що в свою чергу зменшує час доступу до неї.

Розроблені програмні засоби і проведено експериментальне дослідження програмних модулів з цілью оцінки швидкодії та оцінки об’єму БД СКУД, що підтвердило придатність розроблених методів для захисту таких процедур та об’єктів критичної інфраструктури, як захист входу в комп'ютерну систему; прикордонний контроль; контроль доступу; протидія тероризму; Інтернет–безпека тощо.

ПУБЛІКАЦІЇ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Фесенко А.О. Основні біометричні характеристики, сучасні системи та технології біометричної аутентифікації/ А.О.Фесенко, В.А.Швець// Безпека інформації. – 2013. – №2, Том 19. – С. 99 – 111.

2. Фесенко А.А. Современные методы цифровой идентификации личности/ А.А.Фесенко, В.А.Швец// Системи управління, навігації та зв'язку. – 2013. – Вип. 1. – С. 291–296.

3. Фесенко А.О. Кодування та розпізнавання текстурних ознак райдужної оболонки для задач біометрії/А.О.Фесенко// Зв’язок – 2014. – №4. –С.56–62.

4. Фесенко А.А. Метод принятия решений в системе инденти–фикации личности по изображению радужной оболочки глаза/ Зв’язок. – 2015. – №3. – С.23–31.

5. Фесенко А.А. Критерий обнаружения как влияющий фактор объема базы данных, биометрических систем контроля доступа /А.О.Фесенко, В.А.Швец// Захист інформації. – 2016. – №4, Том 18. – С. 308 – 313.

6. Фесенко А.О. Локалізація меж райдужної оболонки ока на основі його зображення/ Ю.Я.Самохвалов, А.О. Фесенко, В.А.Швець// Інформаційна безпека. –2017.– №1(25)№2(26). – С.120–125.

7. Фесенко А.А. Информативность коэффициентов Фурье в аутентификации по радужной оболочке глаза/ Фесенко А.А., Фесенко В.А., Швець В.А , Швець А.В. // Захист інформації – 2017. – №1, Том 19. – С. 33 – 42.

8. Фесенко А.О. Огляд експеременталної системи індентифікації особи за зображенням райдужної оболонки ока/ А.О. Фесенко, М.О.Рябий// Актуальні питання забезпечення кібернетичної безпеки та захисту інформації. –2015: І міжнар. наук.–практ. конф., 22–28 лютого 2015 р. : тези доп. – К. : Вид–во Європейського університету,2015. С. 113–117.

9. Фесенко А.О. Метод індентифікації користувачів на базі райдужної оболонки ока/А.О.Фесенко, В.А.Швець//SITS'2015:XII

всеукраїнська наук.–практ.. конф. 09–12 червня 2015 р.: тези доп.– К. :Вид–во ТОВ "Ділова інформація",2015. С.81–84.

10. Фесенко А.О. Критерії вибору порогу при ідентифікації за райдужною оболонкою ока/А.О.Фесенко, О.Г.Оксіюк// IT&I:III Міжнародна наук.–практ. конф. 8–10 листопада 2016р.: тези доп.– К.:Вид–во Виданично–поліграфічний центр «Київський університет»,2016. С.284–286

11. Фесенко А.О. Біометричні технології в в системах контролю і управління доступом (СКУД)/ А.О.Фесенко, О.Г.Оксіюк, В.О.Фесенко// Проблеми кібербезпеки інформаційно–телекомунікаційних систем: II наук.–практ. конф. 23–24 березня 2017 року: тези доп.– К.:Вид–во Виданично–поліграфічний центр «Київський університет»,2017. С.360–365

12. Швец В.А. Использование преобразования Фурье в аутентификации по радужной оболочке глаза/ В.А. Швец, В.А.Фесенко, А.А.Фесенко, В.В.Швец// Матеріали XIII Міжнар. наук.–тех. конф. «АВІА–2017». – 19–21 квіт. 2017р.: тези доп. – К. НАУ, 2017. – Т.1. – С. 2.50–2.53.

13. Фесенко А.О. Цифрові фільтри зображень/Фесенко А.О.,Оксіюк О.Г., Фесенко В.О.// ITSEC: матеріали VII Міжнар. наук.–тех. конф. – 16–18 трав. 2017р.: тези доп. – К.: НАУ, 2017. – С. 36.

Анотація

Фесенко А.О. Методи обробки даних для систем ідентифікації на основі біометричних характеристик ока.– Рукопис.

Дисертація на здобуття наукового степеня кандидата технічних наук за спеціальностю 05.13.21– системи захисту інформації – Національний авіаційний університет, Київ 2017. Дисертаційна робота присвячена вирішенню важливої науково–технічної задачі розробці методів обробки даних для систем біометричної ідентифікації по біометричним характеристикам ока.

Проведено аналіз сучасних підходів, методів, моделей попередньої обробки даних для біометричних систем ідентифікації і аутентифікації по райдужній оболонці ока.

Вперше запропоновано підхід в ідентифікації для біометричної системи по райдужн оболонці ока без еталон зображення.

Розроблено інтегрально–деференціальний метод локалізації, який дає можливість зменшити обчислювальні витрати при збереженні високої точності методу.

Розроблено метод кодування зображення райдужної оболонки ока, який дає можливість кодувати один піксель зображення одним бітом інформації.

Запропоновано систему ідентифікації і аутентифікації без еталонного зображення райдужної оболонки ока, використовуючи код райдужки і статистичні критерії з використанням нормованої відстані Хеммінга як міри схожості двох кодів.

Ключові слова: біометрична ідентифікація, код райдужної оболонки, прийняття рішень, статистичні критерії, нормована відстань Хеммінга.

Анотация

Фесенко А.А. Методы обработки данных для систем идентификации на основе биометрических характеристик ока.– Рукопись. Диссертация на получение научной степени кандидата технических наук по специальности 05.13.21– системы защиты информации – Национальный авиационный университет, Киев 2017. Диссертация посвящена решению важной научно–технической задачи разработке методов обработки данных для систем биометрической идентификации по биометрическим характеристикам глаза методов

Проведен анализ современных подходов, методов, моделей предварительной обработки данных для биометрических систем индентификации и аутентификации по радужной оболочке глаза.

Впервые предложен подход в индентификации для биометрической системы по райдужной оболочке глаза без еталонного изображения.

Разработан интегрально–диференциальный метод локализации, который дает возможность уменшить вычеслительные затраты при сохранении высокой точности метода.

Разработан метод кодирования изображения райдужной оболочки глаза, который дает возможность кодировать один пиксель изображени одним битом информации.

Предложено систему индентификации и аутентификации без еталонного изображения радужной оболочки глаза, используя код радужки и статистические критерии с использованием нормированого растояния Хеминга как меры сходства двух кодов.

Ключевые слова: биометрическая идентификация, код радужной оболочки, принятия ришений, статистические критерии, нормиваное растояние Хемминга.

ABSTRACT

Fesenko A.O. Methods of data processing for identification systems based on eye biometrics. – Manuscript.

Thesis for a Candidate of Technical Science degree in specialty 05.13.21 – information security systems. – National Aviation University, Kyiv, 2017**.**

Thesis is devoted to applied scientific research task to developing data processing methods for biometric identification systems by eye biometrics.

The analysis of current approaches, methods and different biometric identification systems was carried out and showed that by set of characteristics widespread use of identification by the iris eye has notable advantages over other biometric features and unlimited prospects of application in security systems. However, essential disadvantage of such systems is the algorithmic complexity and high demands for computing resources as well as high cost. In this regard, current research in the area of developing new methods for data processing and iris image recognition, that are resistant to different types of interference, arising during shooting, that would allow to improve system characteristics and reduce demands to hardware, thereby reducing its value are very important.

Existing algorithms for iris localization have several disadvantages, which reduces the performance of biometric systems.For the first time was proposed and developed approach to identify users by improved integral-differential algorithm of localization iris image, that allows at first determine the region of the eyes at human face image and by the following the procedures integration (low-frequency filtering) performed pixel brightness averaging (image blurring), and further differentiation (high-frequency filtering) allows to allocate boundaries of the iris. This approach helps reduce search area of iris boundaries and reduce computational complexity while maintaining high accuracy of the method and significantly increases the speed of finding iris boundaries.

For the first time was proposed and developed the method of encoding iris using modified DoG-filter that allows receiving the iris code where each image pixel corresponds to one bit of information. To obtain *Iris*–code proposed to use the values of modified filter phase feedbacks. Phase submitting images can get rid of the influence of uneven illumination in the identification by the iris of the eye. These feedbacks have permanent jump over 0 of frequency axis that distinguishes them. When frequency response passes through 0 of frequency axis then harmonic phases receive permanent jump on π. When receiving just one crossing over 0 of frequency axis, frequency response is gradually approaching by its value to 0. Therefore harmonics phases of filtered iris image would have values that are located within 0 to π and π to 2π, which corresponds to 0 or 1 in the iris binary code. This reduces iris code size and as a result reducing size of Access control system database, which have time privilege compared with using Gabor filter.

Developed method for identifying users without iris image sample, such approach to solving the problem became possible by receiving clear iris binary code (DoG-filter responce) and using normalized Hamming distance as a criterion of binary codes similarity measure, with further using Neyman-Pearson statistical criterion for decision making. Applying this approach to the decision making made it possible to reduce Access control system database size, which in turn decreases the access time to it. This approach makes it possible to solve two classes of problems – iris code search in the database with the aim to identify and preliminary control access to objects that are under the protection. Experimentally sensitivity of iridescent shells comparison to image rotation (tilting the head when shooting). In this paper, the technique that would reduce this dependence and reduce thus the likelihood of possible errors. On the registration changed simulation input image rotation on certain corners and calculation codes for each of them to save the results in a database. The value of rotation angles can be determined based on sensitivity analysis Hamming distance to rotate the image. In a change to the identification decision is made by the smallest distance from one of the copies of the pattern.

Was developed special software and conducted experimental research of program modules with purpose of performance evaluation and assessment of access control systems database volume, which confirmed the suitability of developed methods for protection and critical infrastructure: secured access to

computer system, border control, access control, terrorism counteracting, Internet security and more.

The result of the work done is solving actual scientific problem of development and research methods for biometric data processing systems based on the characteristics of the human eye.

Keywords: biometric identification, iris code, decision making, statistical criteria, normalized Hamming distance.

Підписано до друку 26.05.17. Зам. №26-05(3)/17.
Формат 60x84/16. Обл. вид. арк. 1,22. Наклад 100 прим.
Друк «НВФ «Славутич-Дельфін».
пр-т Космонавта Комарова, 1.
Тел./факс: 406-74-41