УДК 004.65
Чорнобай К. Ю., Грибков С.В.
Національний університет харчових технологій

РОЗРОБКА БЮДЖЕТНОЇ СИСТЕМИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ З ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ

Чорнобай К. Ю., Грибков С. В. Розробка бюджетної системи біометричної ідентифікації з використання нейронних мереж. В роботі проведено дослідження методів і підходів по створенню бюджетної системи біометричної ідентифікації. Система має архітектуру клієнт-сервер, клієнтська частина буде кроссплатформенною та орієнтована для мобільних пристроїв. Для обробки зображення використовується бібліотека з відкритим кодом Open Source Computer Vision Library та більшу частину по ідентифікації буде здійснюватися з використанням нейронних мереж.
Ключові слова – системи захисту, біометрична ідентифікація, обробка зображення, нейронні мережі.

Чорнобай К. Ю., Грибков С. В. Разработка бюджетной системы биометрической идентификации по использованию нейронных сетей. В работе проведено исследование методов и подходов по созданию бюджетной системы биометрической идентификации. Система имеет архитектуру клиент-сервер, клиентская часть будет кроссплатформенной и ориентирована для мобильных устройств. Для обработки изображения используется библиотека с открытым кодом Open Source Computer Vision Library и большую часть по идентификации будет осуществляться с использованием нейронных сетей.
Ключевые слова - системы защиты, биометрическая идентификация, обработка изображения, нейронные сети.

Chornobay K. U., Hrybkov S.V. Development of budget biometric identification system using neural networks. The paper focuses on the methods and approaches to create the budgetary system of biometric identification. The system have client-server architecture, the client part will be cross-platform and oriented for mobile devices. To process the image, an Open Source Computer Vision Library will be used and most of the identification will be done using neural networks.
Keywords - protection systems, biometric identification, image processing, neural networks.

Актуальність. Проблема захисту інформаційних ресурсів стала найактуальнішою в сучасному кібернетичному суспільстві, що вже не може уявити своє життя без використання мобільних пристроїв та доступу до ресурсів мережі Інтернет. Постійне вдосконалення пристроїв зв'язку та засобів спілкування дозволяє людині підвищити свою комунікацію . За рахунок багатьох ресурсів мережі Інтернет люди зберігають доволі багато корпоративної та приватної інформації на різних серверах, що мають різні ступені захисту. Проблеми захисту інформації на сьогодні одна з актуальних проблем, адже постійно зростають обсяги втраченої комерційної та конфіденційної інформації за рахунок несанкціонованого доступу. Основним фактором втрати інформації залишається людський фактор, бо користувач, який має доступ до інформації, може втратити засоби ідентифікації особи або їх можуть викрасти чи підробити.

Актуальним напрямом дослідження та розробка біометричних засобів аутентицікації, що базуються на використанні різних технічних та програмних засобів.

Аналіз останніх досліджень і публікацій. Проблемам захисту інформаційних ресурсів, а також його забезпечення присвячено багато наукових й практичних робіт вітчизняних та зарубіжних спеціалістів з даного напряму. Авторами роботи [1] розглянуто основи інформаційної безпеки в комп'ютерних мережах та інформаційно-обчислювальних системах. У роботі [2] висвітлюють основні особливості захисту інформаційних ресурсів, що функціонують у корпоративних мережах, а також запропоновано підходи оцінки ефективності їх захисту. Роботи [3, 4] присвячені проблемам захисту конфіденційної та комерційної інформації у бездротових локальних мереж, наведено типи основних загроз та атак, а також описано комплекс заходів щодо їх усунення та підвищення якості безпеки. Автори роботи [5] дослідили способи забезпечення і реалізації аутентифікації та авторизації у web-орієнтованих системах. Автор роботи [6] розглядає різні стандарти та протоколи аутентифікації, підходи їх використання у web-додатках. У роботі [7] розглядаються проблеми реалізації механізмів аутентифікації та авторизації у web-орієнтованих системах, а також запропоновано підхід створення модуля аутентифікації та авторизації користувачів на основі JWT маркерів. Робота [8,9] присвячена огляду основних видів біометричної ідентифікації та їх реалізації, а також розглянуто усі їх недоліки та перспективи розвитку. У роботі [10] автори виділяють актуальний напрямок біометричної ідентифікації за обличчям людини, а також розглянуто методи ідентифікації за геометрією обличчя, адже риси обличчя і форма черепа кожної людини індивідуальні.

Виділення невирішених раніше частин загальної проблеми. Більшість розробок, що мають впровадження та ефективно використовуються, як правило направлені на ідентифікацію за

відбитками пальців та райдужної оболонки ока, що використовуються у різних системах захисту. Такі системи захисту, як правило використовують для доступу до пристроїв або у певне приміщення. Організація доступу з використання біометричної ідентифікації для доступу до інформаційних систем мають обмежене застосування та, як правило, у спеціалізованих організація. Сьогодні стає можливим використання в якості засобів зчитування біометричних параметрів для ідентифікації мобільні засоби комунікацій з фотоелементами. Крім цього, певні фірми виробники мобільних пристроїв обладнують свої пристрої засобами ідентифікації за відбитками пальців, голосом, обличчям. Деякі фірми запатентували системи біометричної ідентифікації та їх використовують в своїх брендах, а саме Sony, Apple. Але актуальною задачею залишається створення системи біометричної ідентифікації на основі обличчя людини, геометрії обличчя, рис обличчя і форм черепа, що є індивідуальними для кожної людини. Впровадження біометричних засобів ідентифікації потребують багато вкладень у апаратно-технічні засоби, тому доступні не всім державним та приватними установам.

Формлювання мети дослідження. Необхідно провести дослідження та аналіз підходів по створенню бюджетної системи біометричної ідентифікації для підвищення ефективності захисту доступу до інформаційних ресурсів різного рівня. Інтеграція системи повинна проходити без особливих проблем, а також система повинна складатися з двох основних елементів, а саме: серверної частини, що буде забезпечувати саме ідентифікацію та надання доступу до інформаційних ресурсів; клієнтської частини, що буде функціонувати на мобільному пристрої та забезпечувати знімання та передачі зчитаних біометричних параметрів.

Виклад основного матеріалу досліджень. Управління роботою організації багато в чому зводиться до запобігання причин, що перешкоджають виконанню її функцій. Одна з таких причин - порушення повноважень доступу на території об'єктів або до джерел конфіденційної інформації і обчислювальних ресурсів організації. Щоб розмежувати доступ співробітників і клієнтів організації на її об'єкти або до інформації, що становить певну значимість, існують спеціальні автоматизовані системи.

Процес ідентифікації полягає в пред'явленні користувачем ідентифікатора та зіставлення його зі зразками ідентифікаторів всіх користувачів в системі. Найбільшого поширення ідентифікація отримала в областях, де безпосередній контакт людини з системою не передбачений, наприклад, в системах розпізнавання осіб. Як перевірка особистості користувача при доступі до ресурсів сучасних комп'ютерних систем не використовується з причин значно меншій надійності в порівнянні з аутентифікацією.

Існуючі системи аутентифікації користувачів:

- парольні системи (найпростіший і найпоширеніший спосіб);
- системи PKI (криптографічні сертифікати);
- системи одноразових паролів;
- біометричні системи.

В основі більшості механізмів аутентифікації користувачів лежать ключі та паролі, тому даний спосіб має найбільшого поширення. Через свою «відкритість», а також велику кількість ПО для злому паролів, дана система є найбільш вразливою.

Для того, щоб система функціонувала з необхідними рівнями швидкодії і надійності, необхідно правильно обрати, що використовувати в якості ідентифікатора і аутентифікатора.

На основі проведених досліджень створено бюджетну систему біометричної ідентифікації. В основі системи покладено клієнт-серверну архітектуру. Серверна частина підтримує роботу бази даних зображень облич, а також сукупність модулів для здіснення ідентифікації та ведення статистики ідентифікації. Клієнтська частина буде реалізована в якості кроссплатформенного додатку, що буде забезпечувати зчитування зображення обличчя, формування відправлення фото до серверної частини для ідентифікації та отримання відповіді про її результат.

Планується впровадження клієнтського додатку на мобільні пристрої під управлінням операційної системи сімейства Android та обладнаних фотокамерою, а також на комп'ютери різної архітектури з підключеною веб-камерою під управлінням операційних сімейств Windows або Linux.

Клієнтська частина є кроссплатформенною та орієнтована в першу чергу на використання мобільних пристроїв з камерами. Для обробки зображення буде використовуватися бібліотека з відкритим кодом Open Source Computer Vision Library (OpenCV), що створена була саме для роботи з пристроями відео зйомки та складної обробки зображень, а також має модулі по

ідентифікації об'єктів. Ця бібліотека була створена компанією Intel®, щоб затвердити загальний стандартний інтерфейс комп'ютерного зору для програмних продуктів в цій області та для сприяння їх більшого розвитку, а також для створення нових моделей використання персональних комп'ютерів. Модулі бібліотеки OpenCV забезпечують [12]:

- функції введення/виведення при роботі як із стандартними пристроями, так і цифровими пристроями фото та відео зйомки;
- виконання алгоритмів фільтрації та перетворення обробки зображення;
- повний цикл використання методів інтелектуального аналізу для обробки зображення;
- визначення та опис плоских примітивів;
- аналіз руху об'єкту та його відстеження;
- реалізацію більшості алгоритмів пошуку об'єктів на зображенні;
- управління пристроями зчитування відеоінформації;
- обробку трьохвимірних об'єктів.

Основним алгоритмом ідентифікації людини на основі зображення її обличчя буде послідовність наступних кроків:

- виявлення факту присутності людини на зображенні;
- виділення контуру фігури людини;
- визначення ракурсу голови (анфас, профіль);
- виділення з зображення обличчя основних параметрів за шаблонами;
- порівняння параметрів з еталонами та ідентифікація.

Для реалізації основних кроків алгоритму достатньо функціоналу бібліотеки OpenCV, але, на думку авторів, для ідентифікації користувачів за зображенням обличчя запропоновано використовувати метод нейронних мереж, що дозволяє вирішувати складні завдання по ідентифікації візуальних та аудіо образів. Нейронні мережі не програмуються в звичному сенсі цього слова, вони навчаються. Можливість навчання - одне з головних переваг нейронних мереж перед традиційними алгоритмами. Технічно навчання полягає в знаходженні коефіцієнтів зв'язків між нейронами. В процесі навчання нейронна мережа здатна виявляти складні залежності між вхідними даними і вихідними, а також виконувати узагальнення. Це означає, що в разі успішного навчання мережа зможе повернути вірний результат на підставі даних, які були відсутні в навчальній вибірці, а також неповних або пошкоджених частково даних. В якості образів можуть виступати різні за своєю природою об'єкти: символи тексту, зображення, зразки звуків тощо. При навчанні мережі пропонуються різні зразки образів із зазначенням того, до якого класу вони відносяться. Зразок, як правило, представляється як вектор значень ознак. При цьому сукупність усіх ознак повинна однозначно визначати клас, до якого належить зразок. У разі, якщо ознак недостатньо, мережа може співвідносити один і той же зразок з декількома класами, що невірно. Після закінчення навчання мережі їй можна пред'являти невідомі раніше образи і отримувати відповідь про належність до певного класу.

Коли мережі пред'являється якийсь образ, на одному з її виходів повинен з'явитися ознака того, що образ належить цьому класу. У той же час на інших виходах повинен бути ознака того, що образ даного класу не належить. Якщо на двох або більше виходах є ознака приналежності до класу, вважається, що мережа «не впевнена» в своїй відповіді. Нейронні мережі базуються на паралельній обробці інформації і мають здатність до самонавчання, тобто отримувати обґрунтований результат на підставі даних, що не зустрічалися в процесі навчання.

До властивостей та переваг нейронних мереж доцільно віднести:

- масовий паралелізм;
- розподілене представлення інформації і обчислення;
- можливість самонавчання та схильність до виділення загальних характеристик;
- можливість пристосовуватися до різних вхідних даних та задач;
- при наявності певних відхилень чи помилок дає ефективний результат;
- мінімальні вимоги.

Основними параметрами при аналізі зображення обличчя людини будуть наступні:

- основні контури обличчя, очей, брів, рота, носа, що є характерними і подібними для усіх людей, але не однаковими, та слугують для побудови певної карти контурів для первинної ідентифікації та характеризуються яскравими переходами на зображенні;

- яскравість, що дає змогу виявити основні контури, а також виявити особливості кожної людини при однакових умовах освітлення;
- колір, що слугує точною ознакою об'єкта за рахунок того, що несе додаткову інформацію про відтінок шкіри.

Перевагою створеної системи ідентифікації є досить гнучка інтеграція з будь-якою інформаційною системою чи комплексом, що мають базу даних під управлінням основних СУБД. Система блокує доступ та не дає пройти навіть до аутентифікації та ідентифікації у системах в які вона інтегрується. Також до переваг необхідно віднести незначні вимоги до її налаштування. Мобільна частина написана під систему Android, та забезпечує функції фотографування та передачі інформації через мережу до серверної частини. Такий спосіб підвищує ідентифікацію та аутентифікації в інформаційних системах, а також є дуже бюджетним. До недоліків необхідно відвести те, що при здійсненні фото все залежить від якості знімку, що не завжди можуть забезпечити бюджетні мобільні телефони нижньої цінової категорії, але якщо здійснювати знімки саме з них, а потім проходити ідентифікацію з такого мобільного пристрою то забезпечується певний додатковий ефект захисту. Також необхідно відмітити про недоліки розпізнавання на основі нейронної мережі, адже, як показали випробовування, завжди існує невірний варіант ідентифікації, але для уникнення такої ситуації доцільно робити тренування мережі на основі декількох знімків обличчя та бажано при різному освітленні. Але все ж таки підвищити якість ідентифікації можливо лише використовуючи змішані підходи біометричної з іншими видами ідентифікації.

Для забезпечення високого рівня захисту необхідно використовувати комбіновані біометричні системи аутентифікації, що передбачає поєднання деяких типів біометричних характеристик для ідентифікації. Це дозволяє задовольнити найсуворіші вимоги до ефективності системи аутентифікації. Наприклад, аутентифікація за відбитками пальців може легко поєднуватися зі скануванням руки. Така структура може використовувати всі види біометричних даних людини і може застосовуватися там, де доводиться форсувати обмеження однієї біометричної характеристики. Комбіновані системи є більш надійними з точки зору можливості імітації біометричних даних людини, так як важче підробити цілий ряд характеристик, ніж фальсифікувати одну біометричну ознаку.

Висновки. Використання створюваної системи біометричної ідентифікації дуже широка та орієнтована на державні та комерційні об'єкти з обмеженим фінансуванням, такі як дитячі садочки, школи, університети, лікарні та ін. Одним з напрямків використання даної системи є використання її для аутентифікації в сучасних web-додатках та для доступу до комерційних бездротових локальних мереж Wi-Fi, що стане додатковим захистом від несанкціонованого доступу.

1. Емельянова Н.З., Партыка Т.Л., Попов И.И. Защита информации в персональном компьютере. - М.: Форум , 2009. - 368 с.
2. Кононова В.О., Грибков С.В., Харкянен О.В. Оцінка засобів захисту інформаційних ресурсів / В.О. Кононова, С.В. Грибков, О.В. Харкянен // Вісник Національного університету «Львівська політехніка», Львів : Видавництво Львівської політехніки, №806, 2014, с. 99 – 105.
3. Визавитин О. И. Практика защиты информации в Wi-Fi сетях на основе современных программно-аппаратных средств // Молодой ученый. — 2016. — №5. — С. 182-184.
4. Чорнобай К.Ю., Грибков С.В. Аналіз та шляхи вирішення проблем захисту комерційних бездротових локальних мереж Wi-Fi / К.Ю. Чорнобай, С.В. Грибков // Вісник Національного університету «Львівська політехніка», серія «Автоматика, вимірювання та керування», Львів : Видавництво Львівської політехніки, №880, 2017, с. 99 – 103.
5. Шелупанова А.А., Груздева С.Л., Нахаева Ю.С. Аутентификация. Теория и практика обеспечения доступа к информационным ресурсам. / А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева – М. : Горячая линия – Телеком, 2009. – 552 с.
6. Обзор способов и протоколов аутентификации в веб-приложениях / Д. Выростков – Режим доступу до ресурсу : https://habrahabr.ru/company/dataart/blog/262817/.
7. Олійник Г.В., Грибков С.В. Використання JWT маркерів для аутентифікації та авторизації користувачів у WEB – додатках / Г.В. Олійник, С.В. Грибков // Вісник Національного університету «Львівська політехніка», серія «Автоматика, вимірювання та керування», Львів : Видавництво Львівської політехніки, №880, 2017, с. 86 – 93.
8. Anil K. Jain, Kathik Nandakumar, Biometric Authentication: System Security and User Privacy. IEEE Computer, November 2012, IEEE Computer Society. All rights reserved. Reprinted with permission.
9. Брагина Е.К., Соколов С. С. Современные методы биометрической аутентификации: обзор, анализ и определение перспектив развития / Е.К. Брагина, С. С. Соколов // Вестник астраханского государственного технического университета. – 2016. –№1(61). – С. 40–44.
10. Вакуленко А., Юхин А. Биометрические методы идентификации личности: обыкновенный выбор // Сборник научных трудов 1 Международной научно-практической конференции "Мировой опыт применения

биометрических решений в составе комплексних систем безопасности". – К. : "Информация-Украина". – 2006. – С. 79–82.
11. Фисенко В. Т., Фисенко Т. Ю., Компьютерная обработка и распознавание изображений: учеб. пособие. – СПб : СПбГУ ИТМО, 2008. – 192 с.
12. Bradsky G., Kaehler A. Learning OpenCV – O'Reilly, 2008. – 508 p.