№ 6(34) 2024
НАУКА і ТЕХНІКА СЬОГОДНІ
серії: право, економіка, педагогіка, техніка, фізико-математичні науки

УДК 004.056:004.052

https://doi.org/10.52058/2786-6025-2024-6(34)-799-806

Габорець Ольга Андріївна доктор філософії, доцент, доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки факультету підготовки фахівців для підрозділів кримінальної поліції, Донецький державний університет внутрішніх справ, вул. Велика Перспективна, 1, м. Кропивницький, 25000, https://orcid.org/0000-0001-7791-6795

ЗНАЧЕННЯ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ В СУЧАСНИХ СИСТЕМАХ БЕЗПЕКИ

Анотація. У цьому науковому дослідженні автором проводиться всебічний аналіз біометричної автентифікації як невід'ємної складової сучасних систем інформаційної безпеки. Основна увага приділяється потенціалу біометричних технологій значно підвищити рівень ідентифікації особи, що суттєво перевершує можливості традиційних методів, таких як парольні системи та магнітні ідентифікаційні картки. Вивчення дозволяє оцінити здатність цих технологій забезпечувати точну верифікацію особи на основі унікальних фізіологічних та поведінкових характеристик.

Дослідження висвітлює ключові виклики, з якими стикаються біометричні системи, включно з питаннями конфіденційності та ризиками несанкціонованого доступу до біометричних даних. Автор пропонує комплексні стратегії мінімізації цих загроз, включаючи застосування багатофакторної автентифікації, антиспуфінгові технології, криптографічне забезпечення даних, а також періодичне оновлення систем безпеки. Підкреслюється важливість адаптації біометричних систем до швидкозмінних технологічних умов та нових кіберзагроз, що вимагає неперервного удосконалення та інновацій.

Особлива увага в дослідженні приділяється етичним аспектам використання біометричних технологій та впливу на приватність особи. Розглядаються правові рамки, що регулюють збір та обробку біометричних даних, а також висвітлюються потенційні ризики для особистих прав і свобод. Висновки дослідження наголошують на необхідності створення рівноваги між потребою у забезпеченні високого рівня безпеки та необхідністю захисту особистої інформації.

Ця робота забезпечує глибоке розуміння можливостей та викликів, пов'язаних з імплементацією біометричних технологій у сучасні інформаційні системи, акцентуючи на важливості балансу між інноваційними технологічними рішеннями та етичними стандартами.

Ключові слова: Біометрична автентифікація, цифрова безпека, ідентифікація особи, фізіологічні характеристики, поведінкові характеристики, конфіденційність даних, захист інформації.

Haborets Olha Andriivna PhD, Associate Professor of the Department of Operational-search Activities and Information Security at the Faculty of Training Specialists for Criminal Police Units, Donetsk State University of Internal Affairs, St. Velyka Perspektyvna, 1, Kropyvnytskyi, 25000, https://orcid.org/0000-0001-7791-6795

THE IMPORTANCE OF BIOMETRIC AUTHENTICATION IN MODERN SECURITY SYSTEMS

Abstract. In this scholarly research, the author conducts a comprehensive analysis of biometric authentication as an integral component of modern information security systems. The main focus is on the potential of biometric technologies to significantly enhance the level of personal identification, which substantially surpasses the capabilities of traditional methods such as password systems and magnetic identification cards. The study allows for an assessment of these technologies' ability to provide accurate personal verification based on unique physiological and behavioral characteristics.

The research highlights the key challenges faced by biometric systems, including issues of confidentiality and the risks of unauthorized access to biometric data. The author proposes comprehensive strategies to minimize these threats, including the application of multifactor authentication, anti-spoofing technologies, cryptographic data protection, and periodic updates to security systems. The importance of adapting biometric systems to rapidly changing technological conditions and new cyber threats, which require continuous improvement and innovation, is emphasized.

Particular attention in the study is devoted to the ethical aspects of using biometric technologies and their impact on personal privacy. Legal frameworks regulating the collection and processing of biometric data are examined, along with the potential risks to personal rights and freedoms. The conclusions of the study emphasize the necessity of creating a balance between the need for high-level security and the necessity to protect personal information.

This work provides a deep understanding of the opportunities and challenges associated with the implementation of biometric technologies in modern information systems, highlighting the importance of balancing innovative technological solutions with ethical standards.

Keywords: Biometric authentication, digital security, personal identification, physiological characteristics, behavioral characteristics, data confidentiality, information protection.

Постановка проблеми. У контексті динамічного розвитку інформаційних технологій, забезпечення цифрової безпеки стає стратегічно важливим. Однією з передових технологій у цій сфері є біометрична автентифікація, яка базується на ідентифікації особи за унікальними анатомічними чи поведінковими характеристиками. Висока ступінь унікальності біометричних параметрів робить їх важко підроблюваними, що забезпечує перевагу над традиційними методами автентифікації, такими як парольні системи чи магнітні ідентифікаційні карти.

Біометричні системи мають широке застосування, зокрема в контрольних системах доступу та складних ідентифікаційних системах, що імплементуються у фінансовому секторі, органах правопорядку та медичних установах. Вони забезпечують високий рівень точності автентифікації на основі фізіологічних параметрів – відбитків пальців, геометрії обличчя, сканування сітківки ока – а також поведінкових характеристик, як-от аналіз голосу та динаміка набору тексту.

Однак, застосування біометричних технологій пов'язане з низкою викликів, зокрема з питаннями забезпечення конфіденційності та інтегритету біометричних даних. Ці виклики включають потенційний несанкціонований доступ до біометричної інформації, що може призвести до порушення права на приватність. Також існує ризик створення технологічних вразливостей через неправильне впровадження або налаштування системи, що може компрометувати їхню ефективність та безпеку.

Аналіз останніх досліджень і публікацій. Проблематика оптимізації та забезпечення безпеки біометричних технологій у системах автентифікації залишається важливим напрямком дослідження в сучасній науковій спільноті та активно вивчається українськими дослідниками. Так, Курченко О., Зубик Л. та Щебланін Ю. зазначають, що перед використанням біометричної ідентифікації необхідно ретельно проаналізувати всі переваги та недоліки, а також вжити відповідних заходів для забезпечення захисту інформації та прав осіб. І стверджують, що комбінуючи різні способи біометричної та апаратної автентифікації, можна отримати надійну систему захисту (що підтверджується великою зацікавленістю, яку проявляють до цих технологій провідні виробники програмного забезпечення) [1, с. 55-56].

Коваль Л., Злепко С. та інші стверджують, що поєднання паролів із біометричними характеристиками людини підвищує надійність системи доступу в сотні і тисячі разів [2, с. 110].

Мета дослідження полягає в детальному аналізі сучасних методів біометричної автентифікації, виявленні потенційних загроз конфіденційності біометричних даних і стратегій їх нейтралізації.

Виклад основного матеріалу. Традиційна процедура ідентифікації та автентифікації включає декілька основних компонентів: суб'єкт, який підлягає

ідентифікації, його унікальні ідентифікаційні характеристики, обрану систему автентифікації, та принципи її діяльності, наприклад, біометричну верифікацію. Ця система, зокрема, виконує контроль доступу, надаючи суб'єктам відповідні права доступу. Біометрична автентифікація полягає у верифікації особистості шляхом пред'явлення біометричних даних, які обробляються відповідно до встановленого протоколу верифікації. Процес біометричної автентифікації включає порівняння поданого зразка з еталонним зразком з урахуванням певних параметрів допуску.

Попри переваги, біометрична автентифікація має потенційні ризики та недоліки. Один з таких ризиків — атака через підробку, коли зловмисник використовує фальшивий біометричний зразок, такий як відбиток пальця або образ обличчя, для обходу системи верифікації. Це порушує основні принципи функціонування системи і становить значну загрозу для її безпеки. Інший ризик полягає у можливості витоку шаблонів з бази даних, що може дозволити зловмиснику застосувати методи зворотної інженерії для відтворення біометричних даних та значно збільшити ризик фальсифікації. Незважаючи на ці недоліки, біометричні системи забезпечують додатковий рівень захисту порівняно з традиційними парольними системами, оскільки зловмисникам важче замінити справжній шаблон на підроблений.

Для забезпечення оптимального рівня безпеки та ефективності біометричних систем, слід інтегрувати комплексний набір стратегій нейтралізації загроз, що базуються на передових наукових підходах та методологіях:

Імплементація багатофакторної аутентифікації (MFA): Ця стратегія об'єднує декілька рівнів верифікації ідентичності, включаючи щось, що користувач знає (когнітивний фактор), щось, що користувач володіє (володіння фактором), та щось, що користувач є (інгерентний фактор). Це суттєво ускладнює можливості несанкціонованого доступу.

Застосування технологій виявлення підробок (Anti-Spoofing Technologies): Сучасні системи біометричної автентифікації інтегрують алгоритми, здатні аналізувати фізіологічні та поведінкові індикатори на предмет їх автентичності, такі як аналіз текстури шкіри, детекція пульсації кровоносних судин, що дозволяє ідентифікувати нелегітимні спроби доступу.

Криптографічне забезпечення біометричних даних: Шифрування даних, що зберігаються, гарантує, що навіть у випадку витоку інформації, неавторизовані особи не зможуть її використати. Застосування сучасних алгоритмів шифрування та ключових політик ефективно забезпечує конфіденційність і цілісність біометричних шаблонів.

Оновлення та моніторинг системи: Систематичне оновлення програмного забезпечення та біометричних алгоритмів необхідне для утримання системи в актуальному стані з огляду на нові вектори загроз.

Ретельний моніторинг та аудит системи дозволяють вчасно виявляти потенційні безпекові інциденти та здійснювати відповідні заходи реагування.

Періодичне оновлення біометричних шаблонів: Регулярне оновлення біометричних шаблонів у базі даних забезпечує, що інформація залишається актуальною і недоступною для зловживань, зокрема після компрометації певних даних.

Застосування цих стратегій вимагає розуміння глибинних технологічних та методологічних основ біометричних систем, а також суворе дотримання наукових принципів у процесі їх реалізації. Використання такого комплексного підходу сприятиме створенню більш безпечної та надійної біометричної автентифікації.

Ураховуючи зазначені ризики та недоліки, важливо глибше зрозуміти різноманітні методи біометричної автентифікації, які застосовуються в сучасних системах. Розширене використання цих методів дозволяє оптимізувати заходи безпеки та знизити потенційні загрози. Методи біометричної автентифікації поділяються на дві основні категорії: статичні та динамічні. Статичні методи засновані на фізіологічних характеристиках особи, які є постійними та унікальними для кожної людини від народження. До таких характеристик належать відбитки пальців, структура кровоносних судин під шкірою, візерунки райдужки ока, а також контури обличчя. Ці методи використовуються, наприклад, у системах розпізнавання облич, де технологія ідентифікує особу на основі цифрових зображень або відеозаписів. Такі системи аналізують текстурні особливості та форму обличчя, часто використовуючи алгоритми штучного інтелекту для точної ідентифікації.

З іншого боку, динамічні методи фокусуються на поведінкових особливостях, що виявляються в процесі здійснення рутинних дій. Це може включати особливості клавіатурного почерку, спосіб ходьби, чи послідовність виконання стандартних дій. Ці методи особливо ефективні у випадках, коли важливо виявити унікальний спосіб взаємодії з системою, наприклад, при автентифікації на основі динаміки набору тексту на клавіатурі.

В контексті обробки та класифікації зображень основні технологічні рішення базуються на використанні нейронних мереж, зокрема глибоких згорткових нейронних мереж (CNN). Ці мережі вирізняються здатністю ефективно аналізувати великі обсяги даних, виконуючи розпізнавання та класифікацію об'єктів у відео та на зображеннях. CNN адаптивні, можуть самонавчатися і відрізняються високою швидкістю обробки даних, що робить їх незамінними у сфері комп'ютерного зору.

Ще одним важливим підходом у розв'язанні задач класифікації є використання методу опорних векторів (SVM), який також показав високу ефективність у різноманітних застосуваннях, зокрема у випадках, коли необхідно розрізняти між кількома класами об'єктів на основі векторів

характеристик. Основною метою SVM є знаходження гіперплощини в багатовимірному просторі, яка найефективніше розділяє два класи даних.

Центральним елементом у методі опорних векторів є функція класифікації, задана формулою:

$f(x) = w^T x + b$, де:

x (або ($x_1, x_2, \dots, x_d$)) представляє вектор ознак об'єкта, що класифікується, ω (або $(\omega_1, \omega_2, \dots, \omega_d)$) є вектором ваг, що визначає важливість кожної ознаки в класифікації, b – зміщення, що дозволяє регулювати гіперплощину для оптимального розділення класів.

Класифікація об'єкта визначається знаком функції $f(x)$:

- якщо $f(x) \geq 0$, об'єкт приписується до класу +1;
- якщо $f(x) < 0$, об'єкт приписується до класу -1.

Метод SVM базується на принципі оптимізації, де головним завданням є мінімізація квадратичної функції помилок при одночасній максимізації маржі між класами. Основні об'єкти, які впливають на положення гіперплощини, називаються опорними векторами. Ці об'єкти розташовані найближче до роздільної гіперплощини і є критичними для визначення меж між класами.

У контексті використання SVM для класифікації зображень, цей метод може ефективно аналізувати візуальні характеристики, такі як текстури та контури, за допомогою оптимізованих вагових векторів та зміщень, використовуючи методику глибокого навчання для підвищення точності розпізнавання.

Другий популярний метод, k-найближчих сусідів (k-NN), ґрунтується на іншому принципі: класифікація об'єкта відбувається на основі порівняння його ознак з ознаками k найближчих вже класифікованих об'єктів. Метод k-найближчих сусідів (k-NN) відіграє важливу роль в машинному навчанні, особливо коли мова йде про класифікаційні задачі. Його основний принцип полягає у визначенні класу об'єкта шляхом аналізу класів його найближчих сусідів у просторі ознак. При використанні цього методу, спочатку вибирається число k, яке вказує на кількість сусідів, які будуть розглядатися. Тобто, якщо k = 3, класифікація нового об'єкта відбудеться на основі трьох найближчих до нього об'єктів у навчальному наборі даних.

Ця техніка особливо ефективна в ситуаціях, де межі між класами не чітко визначені. У таких випадках, близькість об'єктів у просторі ознак може допомогти визначити, до якого класу належить новий об'єкт, оскільки подібні об'єкти часто належать до одного класу. k-NN не потребує експліцитного навчання моделі у традиційному розумінні – замість цього, він просто аналізує локальне оточення об'єкта у просторі ознак на момент виконання класифікації.

Крім того, k-NN показує хороші результати у динамічних системах, де дані постійно оновлюються. Завдяки тому, що модель не потребує повторного

навчання з кожним новим набором даних, а лише додавання нових даних у набір для порівняння, метод може швидко адаптуватися до нових умов без значних витрат часу чи ресурсів. Це робить k-NN особливо привабливим для використання в системах, де швидка адаптація до нових даних є критично важливою.

Система біометричної автентифікації, що базується на розпізнаванні рис обличчя, інтегрує передові технології у галузях комп'ютерного зору та машинного навчання для автоматизованої ідентифікації та верифікації особистості. Вона використовує цифрові зображення чи відео для аналізу облич, порівнюючи їх з біометричними профілями, заздалегідь збереженими у базі даних. Основним кроком є створення цієї бази, яка в даному випадку включає зображення з Georgia Tech Face Database, що містить 750 зображень від 50 осіб.

Ці зображення зберігаються у форматі JPEG, розділених на 15 зображень для кожної особи, що дає можливість для детального аналізу різних виразів обличчя та поз. Для ефективного навчання та тестування системи використовуються вибіркові зображення: чотири обрані для навчання та одинадцять для тестування, що створює загальний навчальний набір з 550 зображень і тестовий набір з 200 зображень. Роздільна здатність зображень складає 640×480 пікселів, із середнім розміром облич 150×150 пікселів, оптимізовані для точної ідентифікації.

Зокрема, виклики для алгоритмів розпізнавання включають варіативність умов освітлення, виразів обличчя, а також наявність аксесуарів, які можуть впливати на точність ідентифікації. Для подолання цих викликів використовується аналіз більш ніж 80 біометричних точок на обличчі, що дозволяє програмному забезпеченню створити унікальний числовий код — Face Print для кожної особи. Цей код служить репрезентацією облич у базі даних.

Впровадження двовимірної (2D) технології ідентифікації дозволяє системі ефективно адаптуватися до змін у виразах обличчя та умовах освітлення, що забезпечує високу точність і надійність ідентифікаційних процесів навіть у складних умовах. Це робить систему біометричної аутентифікації вкрай корисною для застосувань, де потрібна швидка та надійна верифікація особи.

Висновки. Аналіз сучасних біометричних технологій автентифікації підкреслює їх значущість у забезпеченні цифрової безпеки та унікальні можливості для точної ідентифікації осіб. Однак, ці технології також супроводжуються серйозними викликами, зокрема щодо забезпечення конфіденційності та інтегритету даних. Важливість розробки ефективних стратегій для захисту біометричних даних і запобігання їх несанкціонованому використанню є критичною у контексті постійного розвитку інформаційних загроз.

Література:

1. Курченко О.А., Зубик Л.В., Щебланін Ю.М. Аналіз застосування біометричних технологій в забезпеченні інформаційної безпеки. Proceedings of the XVI International Scientific and Practical Conference «Principles of science. Ideals, norms, values in science and style of scientific thinking». April 17 – 18, 2023. Tallinn, Estonia. С. 52 – 56.
2. Коваль Л.Г., Злепко С.М., Новіцький Г.М., Крекотень Є.Г. Методи і технології біометричної ідентифікації за результатами літературних джерел. Вчені записки ТНУ імені В.І. Вернадського. 2019. Т. 30 (69) Ч. 1. № 2. С. 104-111.

References:

1. Kurchenko, O.A., Zubyk, L.V., & Shcheblanin, Yu.M. (2023). Analiz zastosuvannia biometrychnykh tekhnolohii v zabezpechenni informatsiinoi bezpeky [Analysis of Biometric Technology Applications in Information Security] – Proceedings of the XVI International Scientific and Practical Conference «Principles of science. Ideals, norms, values in science and style of scientific thinking». (pp. 52-56). Tallinn, Estonia. [in Ukrainian].
2. Koval L.H., Zlepko S.M., Novitskiy H.M., Krekoten E.H. (2019). Metody i tekhnolohii biometrychnoi identyfikatsii za rezultatamy literaturnykh dzherel [Methods and technologies of biometric identification based on the results of literature sources] – 'Scientific Notes of the Vernadsky Taurida National University. (pp. 104-111). [in Ukrainian].