УДК 004.93
DOI https://doi.org/10.17721/ISTS.2021.1.53-60

О. М. Кулінич, orcid.org/0000-0002-0643-6898,
olmaxol@i.ua
А. С. Роскот, orcid.org/0000-0002-8063-4104,
nroskot144@gmail.com
Інститут спеціального зв'язку та захисту інформації
НТУУ КПІ імені Ігоря Сікорського, Київ, Україна

СИСТЕМА БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ НА ОСНОВІ НЕЙРОННИХ МЕРЕЖ

Біометричний підхід вважають одним із найактуальніших у системах ідентифікації та автентифікації. В основі біометричного методу лежить аналіз унікальних характеристик людини. Розпізнавання обличчя – важливе завдання, адже є першим етапом ідентифікації, щоб виявити, кому належить обличчя і чи є воно в базі даних, спочатку потрібно його локалізувати. Для розв'язання цієї задачі застосовують різні підходи, серед них: емпіричні методи, метод на основі навчання, метод на основі порівняння із шаблоном, метод на основі контурних моделей. У розпізнаванні обличчя системі, яка розв'язує таку задачу, необхідно врахувати сукупність факторів: відмінності облич різних людей, зміна ракурсу обличчя, можливість наявності певних особливостей, зміна виразу обличчя, наявність перешкод на зображенні, що можуть частково перекривати об'єкт, умови зйомки. Штучний інтелект є і полем для розвитку, і викликом. Зважаючи на те, що розробки машинного навчання та штучного інтелекту часто орієнтовані на оброблення великих масивів даних, а алгоритми машинного навчання прямо залежать саме від якості інформації, яку він обробляє, то втручання та дезінформація можуть вивести з ладу подальшу роботу алгоритму, що може призвести до неправильних висновків, у коректності яких буде важко переконатися, оскільки великі масиви даних. Вибір методу для розв'язання задачі виявлення обличчя залежить від конкретної задачі й умов, в яких повинен функціонувати алгоритм. У статті розглянуто та проаналізовано можливості нейронних мереж для застосування в системі багатофакторної автентифікації. Розглянуто варіанти можливих реалізацій із використанням штучної мережі, перспективи розвитку цих мереж і їхню важливість у наш час. Проаналізовано сучасні дослідження у вказаній сфері серед провідних країн світу. Одним із методів для застосування є алгоритм розпізнавання облич EIGENFACE. Розглянуто перспективи використання нейронних мереж, штучного інтелекту, виконано огляд особливостей навчання штучної нейронної мережі й алгоритму EIGENFACE для застосування в системі багатофакторної автентифікації та запропоновано етапи для вдосконалення цього алгоритму на основі теорії нечітких множин. У роботі з'ясовано, що таке нейронна мережа, штучний нейрон, роботу алгоритму розпізнавання Eigenface, оскільки знання принципу роботи алгоритму значно полегшує застосування на практиці, розглянуто процес навчання з метою подальшої можливої реалізації. Запропоновано додаткові етапи вдосконалення алгоритму за допомогою теорії нечітких множин, яка стає потужним інструментом для побудови інтелектуальних апаратно-програмних систем розпізнавання образів. Упровадження в алгоритм нечіткого фільтра обчислює нечіткий приріст, так що зображення стають менш чутливими до локальних змін структур, меж об'єктів. Фільтр забезпечуватиме високий ступінь розрізнення між шумом і структурними об'єктами зображення. Сегментація дозволяє розбивати зображення на менші частини, що значно покращує розпізнавання системою.

Ключові слова: *захист інформації; автентифікація; ідентифікація; штучний нейрон; штучна нейронна мережа; нечіткі множини.*

1. ВСТУП

У сучасному глобалізованому суспільстві розвиток технологій і постійний обмін інформацією є основою прогресу. Важко уявити життя без засобів передачі інформації. Проблема захисту інформації є пріоритетною, а питання захисту інформації від витоку, несанкціонованого доступу – невід'ємна складова національної безпеки.

Системи зберігання стратегічно важливих даних є недосконалими, що наражає державу на

небзайнезпеку та на певному етапі поступається місцем у боротьбі розвідувальних служб іншим державам. За винятком цього, варто зазначити, що не тільки державні установи несуть відповідальність за витікання конфіденційної інформації про громадян.

Розвиток та інтеграція штучного інтелекту, машинного навчання нині є вагомим напрямком. У двох провідних держав світу – США та Китаю, розвиток штучного інтелекту є однією з першочергових задач. Найімовірніше, що протягом найближчого часу військові, розвідувальні й інші спеціальні структури триматимуть курс саме на розвиток упровадження використання систем на базі штучного інтелекту та машинного навчання. Потенціал для використання цих технологій у контексті безпеки досить об'ємний і мало досліджений.

На початку XXI століття до розв'язання завдань розпізнавання за біометричними даними під'єдналося безліч наукових лабораторій, найбільших результатів домоглися групи на чолі з професором Джоном Густавом Догманом у Кембриджському університеті (Велика Британія) та професором Кевіном Боуєром в Університеті Нотр-Дам (США), а також професором Уго Проенка – Університет Внутрішньої Бейри (Португалія), професором Адамом Чайка – Варшавська політехніка (Польща). Огляди [1–4] представляють понад 200 робіт із цієї тематики, і це лише незначна частина досліджень. У світі проблемами оброблення та розпізнавання зображень обличчя людини займаються: колектив лабораторії математичних методів обробки зображень факультету обчислювальної математики й кібернетики Московського державного університету імені М. В. Ломоносова під керівництвом професора А. С. Крилова, дослідницька група в Інституті фізики імені Б. І. Степанова Національної академії наук Білорусії під керівництвом доктора фізико-математичних наук Г. І. Желтова, Інститут систем оброблення зображень.

Проблеми розпізнавання за формою обличчя уважно вивчають дослідницькі групи у США (П. Дж. Флінн, А. Росс, Мічиганський державний університет), Англії, Португалії, Польщі, Білорусі. Системи розпізнавання за райдужною оболонкою ока розроблено фірмами IriTech, LG, OKI, Panasonic, Sagem, Neurotechnology, Morpho.

У зв'язку зі збільшенням кількості біженців із зон ведення бойових дій (Сирія, Ірак, Лівія) й активним упровадженням біометричних технологій по Russian Society of Appraisers для їхньої реєстрації виникають проблеми через постійне збільшення об'єму бази даних еталонів і, як наслідок, збільшення часу ідентифікації та автентифікації, а також важливою проблемою є робота системи в режимі один до багатьох [1–4].

Актуальність теми дослідження. Автентифікація людини, тобто підтвердження того, що особа є тим, за кого себе видає, поза всяких сумнівів є актуальним завданням, практичним розв'язанням якого зайняті тисячі й мільйони людей по всьому світу.

Варіанти можливих реалізацій:

- інструменти для аналізу даних у величезному обсязі та з нескінченними можливостями до самовдосконалення через залучення машинного навчання;
- система авторизації на основі нейронних мереж;
- оптимізація роботи систем за допомогою вираховування оптимальних і найшвидших варіантів дій;
- поліпшення захисту існуючих систем методом пошуку в них прогалин за допомогою штучного інтелекту;
- моделювання потенційних ситуацій за допомогою штучного інтелекту та машинного навчання під час підготовки кадрів [5].

Основним завданням алгоритму розпізнавання облич є його впровадження в систему автентифікації для вдосконалення методів захисту інформації, а також зменшення ризиків входження в систему неавторизованих користувачів. Історично в інформаційній сфері сформувалися два напрями захисту від несанкціонованого доступу, які в системах фізичного захисту називають системами управління доступом (СУД), а в комп'ютерній сфері – системами ідентифікації та автентифікації.

Автоматизація цих процесів, зокрема і за допомогою новітніх технологій – важлива складова розвитку сучасного суспільства. Те ж саме можна сказати і про завдання ідентифікації, тобто встановленні особи людини шляхом пошуку його запису в базі даних. Розвиток систем комп'ютерного зору, цифрового оброблення зображень, збільшення потужності обчислювальних засобів останнім часом дало можливість ставити і розв'язувати задачі автоматичної реєстрації, виокремлення, розпізнавання складних, часто змінюваних, важко модельованих і формалізованих об'єктів як біометричних ознак живих організмів. Таким чином, завдання автентифікації та ідентифікації людини тепер вирішуються за допомогою автоматичних біометричних систем, складаючи одну з нових областей прикладної математики, біометричну ідентифікацію.

Ідентифікацію і автентифікацію можна вважати основою програмно-технічних засобів безпеки

тому, що решту сервісів розраховують на обслуговування іменованих суб'єктів. Ідентифікація і автентифікація – це перша лінія захисту інформаційного простору комп'ютерної системи. Саме від коректності розв'язання цих двох завдань залежить, чи можна дозволити доступ до ресурсів системи конкретному користувачеві. Система захисту виконує ідентифікацію та автентифікацію на основі певної унікальної інформації, яка характеризує конкретного користувача системи [6].

2. ПОСТАНОВКА ЗАДАЧІ

Одним із головних напрямів розвитку захисту інформації є вдосконалення існуючих і створення нових систем і засобів, які б задовольняли основні властивості інформації: конфіденційність, цілісність, доступність.

Біометричний підхід вважають одним із найактуальніших у системах ідентифікації та автентифікації. В основі цього методу лежить аналіз унікальних характеристик людини. Його умовно поділяють на фізіологічний і поведінковий методи. Прикладами для фізіологічних можуть слугувати: відбитки пальців, малюнок райдужної оболонки ока, розпізнавання обличчя, долонь рук, сітківки ока тощо, а для поведінкових: підпис, рукописний, клавіатурний почерк, натискання на клавіатуру [7].

Розпізнавання обличчя є важливим завданням, адже є першим етапом ідентифікації. Щоб виявити, кому належить обличчя і чи є воно в базі даних, спочатку потрібно його локалізувати. Для розв'язання такої задачі застосовують різні підходи, серед них: емпіричні методи, метод на основі навчання, метод на основі порівняння із шаблоном, метод на основі контурних моделей. Під час розпізнавання обличчя системі, яка розв'язує задачу, необхідно врахувати сукупність факторів: відмінності облич різних людей, зміна ракурсу обличчя, можливість наявності певних особливостей, зміна виразу обличчя, наявність перешкод на зображенні, що можуть частково перекривати об'єкт, умови зйомки.

Штучний інтелект є як полем для розвитку, так і викликом. Зважаючи на той факт, що розробки машинного навчання та штучного інтелекту часто орієнтовані на оброблення великих масивів даних, а алгоритми машинного навчання прямо залежать саме від якості інформації, яку він обробляє, то втручання та дезінформація можуть вивести з ладу подальшу роботу алгоритму, що може призвести до неправильних висновків, у коректності яких буде важко переконатися, оскільки великі масиви даних. Вибір методу для розв'язання задачі виявлення обличчя залежить від конкретної задачі й умов, в яких повинен функціонувати алгоритм [8].

Метою цієї роботи є аналіз існуючого алгоритму розпізнавання облич на основі нейронних мереж Eigenface та його вдосконалення на базі теорії нечітких множин для підвищення рівня захищеності систем багатофакторної автентифікації у ході використання за рахунок більш надійних методів автентифікації користувачів.

3. АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Сучасні дослідження показують, що на основі нейронної мережі можна побудувати систему розпізнавання обличчя людини по зображенню. У нових методах виокремлення ключових ознак для опису об'єкта здійснюється шляхом автоматичного аналізу навчальної вибірки. Проте більша частина інформації щодо ознак вводиться вручну. Для автоматичного застосування таких аналізаторів вибірка має бути досить великою та охоплювати всі можливі ситуації. Головний принцип системи розпізнавання – представити вхідні зображення у вигляді однієї спільної матриці, яка буде складатися із суми базисних компонент зображень.

Штучні нейронні мережі різної топології застосовують для розв'язання різних задач, саме наявність багатьох типів мереж забезпечує їхнє широке використання у різних сферах для розв'язання задач розпізнавання, прогнозування, класифікації, ідентифікації та багатьох інших. З використанням нейронних мереж вирішується проблема проєктування й оптимізації мереж зв'язку, тобто знаходження оптимального шляху трафіка між вузлами, а також для отримання ефективних рішень у галузі їхнього проєктування.

Із часів фундаментальної роботи Віоли та Джонса прискорений каскад із простими ознаками залишається найбільш популярним та ефективним підходом у розробленні програм для практичної детекції облич. Проста природа ознак дозволяє швидко оцінювати і рано відкидати неправильні результати пошуку. Тим часом, прискорений каскад створює групу простих ознак для досягнення точної класифікації облич [9]. Оригінальний детектор Віоли – Джонса використовує ознаки Хаара, які швидко вираховуються, та їх достатньо для опису фронтальних зображень облич. Тим не менш, через простоту ознак Хаара алгоритм відносно слабкий у неконтрольованому середовищі.

В останні роки спостерігається сплеск уваги до нейронних мереж. Посилений інтерес виник, коли Алекс Крижевський за допомогою конвуляційних нейронних мереж переміг у конкурсі ImageNet, понизивши рекорд помилок у класифікації з 26 % до 15 %, що тоді стало проривом.

Сьогодні "глибоке навчання" є основою багатьох систем великих компаній: Facebook використовує нейронні мережі для алгоритмів автоматичного виставлення тегів, Google – для пошуку серед фотографій користувача, Amazon – для генерації рекомендацій товарів, Pinterest – для персоналізації домашньої сторінки користувача, а Instagram – для пошукової інфраструктури.

Задача автоматичного розпізнання облич нині є досить актуальною і через велику кількість наукових досліджень цього питання, і через великий потенціал використання вказаної технології у комерційних проєктах [10].

4. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Для ефективного використання алгоритму розпізнавання необхідно додатково забезпечити як мінімум один етап, а саме вдосконалити якість зображення шляхом фільтрації шумових складових і сегментації або кластеризації.

У статті пропонується аналіз проблеми ефективного розпізнавання облич та її розв'язання за рахунок використання систем штучного інтелекту на базі нечітких множин в алгоритмі Eigenface, оскільки якість результату розпізнавання залежить від ракурсу, положення, умов освітленості приміщень і поворотів відносно осей.

Штучний нейрон – вузол штучної нейронної мережі, що є спрощеною моделлю природного нейрона. Математично, штучний нейрон зазвичай представляють як деяку нелінійну функцію від єдиного аргументу – лінійної комбінації всіх вхідних сигналів.

Штучна нейронна мережа – це набір шарів із так званими штучними нейронами. Штучний нейрон (рис. 1) імітує властивості біологічного нейрона. На вхід штучного нейрона надходить деяка множина сигналів (координат): x_1, x_2, …, x_n, кожний з яких є виходом іншого нейрона. Кожен вхід множиться на відповідну синаптичну вагу w_1, w_2, …, w_n [11, 12].

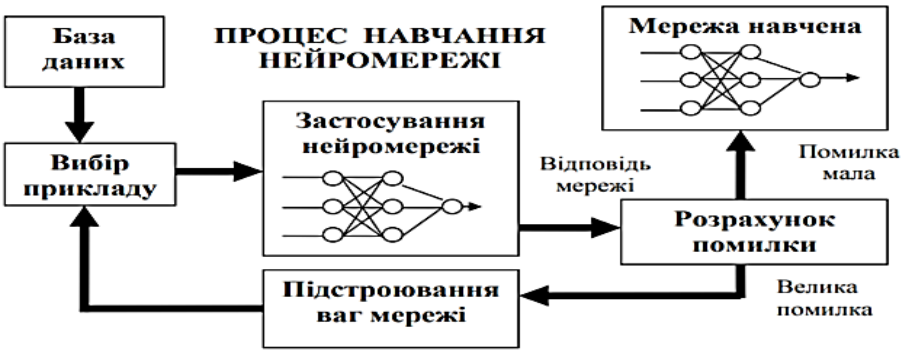

Рис. 1. Процес навчання нейронної мережі

Усі добутки підсумовують, визначаючи рівень активації нейрона NET. Далі сигнал NET перетворюється активаційною функцією F і дає вихідний нейронний сигнал OUT. Активаційна функція може бути лінійною функцією, логічною функцією [13] або функцією гіперболічного тангенса.

Залежно від способу передавання результатів активаційній функції по нейронних шарах нейронні мережі ділять на різні класи.

Оскільки всі штучні нейронні мережі базуються на концепції нейронів, з'єднань і переданих функцій, існує подібність між різними структурами або архітектурами нейронних мереж. Більшість змін походить із різних правил навчання. Нейромережі складені з простих елементів, що діють паралельно. Можна навчити нейромережу, регулюючи значення ваг між елементами. Зазвичай мережа регулюється або навчається так, щоб приватний вхід вів до цільового виходу [15]. На рис. 2 представлено процес навчання нейронної мережі [16].

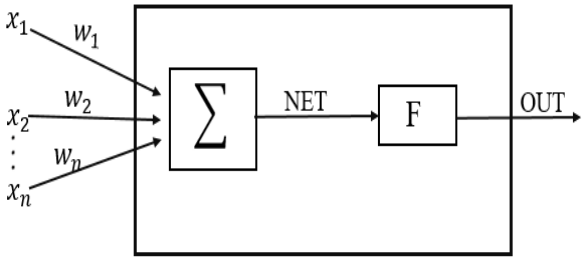

Рис. 2. Структура штучного нейрона

Система, яка виконує нечітке оброблення, має дві основні особливості: по-перше, нечіткий фільтр обчислює нечіткий приріст таким чином, щоб він був менш чутливим до локальних змін структур зображення, таким як кордони об'єктів. По-друге, функція приналежності формується так, щоб адаптуватися до шумових складових для виконання нечіткого згладжування (передбачається, що шум рівномірно розподілений по всьому зображенню). Основна ідея нечіткого фільтра така: значення пікселя визначають залежно від значень навколишніх сусідніх пікселів. Фільтр повинен забезпечувати високий ступінь розрізнення між шумом і структурними об'єктами зображення. Щоб вирішити це завдання для кожного пікселя обчислюється оціночний ступінь, який характеризує те, наскільки великий або малий приріст у певному напрямку. Конструювання нечіткого фільтра базується на такому спостереженні: малий нечіткий приріст відповідає шуму, великий нечіткий приріст – межам об'єктів.

Просте збільшення центрального пікселя (x, y) у напрямку *D(D€ {NW,N,NE,E,SE,S,SW,W})* визначається як різниця між пікселем із координатами (x, y) і одним із сусідніх пікселів у напрямку D. Значення збільшення позначається $\nabla_{D(x,y)}$, наприклад:

$$\nabla_N (x, y) = I(x,y-1) - I(x, y), \quad (1)$$

$$\nabla_{SW} (x, y) = I(x-1,y+1) - I(x, y). \quad (2)$$

Якщо два значення збільшень із трьох малі, то можна припустити, що в цьому напрямку відсутні межі об'єктів. Таким чином, щоб визначити нечіткий приріст, потрібно розглянути його якісне поняття мале. Цьому поняттю в рамках теорії нечітких множин відповідає нечітка множина мале. Функція приналежності m_k (u) поняття мале може визначатися як

$$m_k(u)=\begin{cases} 1-\frac{|u|}{k}, & 0 \le |u| \le k, \\ 0, & |u| > k \end{cases} \quad (3)$$

де *k* – адаптивний параметр. Графік виразу побудовано на рис. 3а.

Рис. 3. Функції приналежності якісних понять: а) мале; б) позитивне; в) негативне

Значення нечіткого збільшення для пікселя в напрямку NW обчислюється за такими правилами:

if (∇_{NW}(x,y) мале) and (∇_{NW}(x–1,y+1)) мале)

or (∇_{NW}(x,y) мале) and (∇_{NW}(x+1,y–1) мале)

or (∇_{NW}(x–1,y+1) мале) and (∇_{NW}(x+1,y–1) мале)

then ∇^F NW (x,y) мале. (4)

Вісім таких нечітких правил застосовуються для кожного з напрямків. Як уже згадано раніше, щоб виконати нечітку фільтрацію зображення необхідно усунути шумові складові пікселів шляхом модифікації значень пікселів, тому позначимо модифікаційний параметр difX. Для обчислення значення difX використовуємо пару нечітких правил для кожного напрямку. Сутність цих правил полягає в наступному: якщо передбачається відсутність меж об'єкта в певному напрямку, то чітке значення приросту в цьому напрямку може бути використано для обчислення модифікаційного значення difX.

Відповідно перша частина функціонування алгоритму фільтрації зображень – виявлення меж структурних об'єктів, може бути реалізована у вигляді нечіткого збільшення, друга частина алгоритму повинна бути реалізована у вигляді схеми, яка здатна розрізняти позитивне і негативне значення для нечіткого збільшення:

λ^+_{NW}: if (∇^F NW (x,y) мале) and (∇_{NW} (x,y) позитивне)

then c – позитивне

λ^-_{NW}: if (∇^F NW (x,y) мале) and (∇_{NW} (x,y) негативне)

then c – негативне. (5)

Останній крок – дефазифікація результату: необхідно визначити модифікаційне значення difX, яке буде додано до поточного значення пікселя:

$$\Delta = \frac{L}{8} \sum_{Dedir} (\lambda^+_D - \lambda^-_D), \quad (6)$$

де *D* – означення напрямку, *L* – кількість градацій сірого.

Таким чином, розглянуто перший етап, який має виконувати система розпізнавання образів. Варто зауважити, що цей етап є дуже важливим, тому що багато в чому саме від якості попередньо обробленого зображення залежить стабільна роботи системи в цілому. Наступний етап пов'язаний із сегментацією і виокремленням контурів об'єктів. Мета етапу – знаходження об'єкта на зображенні [17].

В основу алгоритму Eigenface покладено використання фундаментальних статичних характеристик: середніх (математичне очікування) та коваріаційної матриці, застосування методу головних компонент. Як і будь-який інший алгоритм сфери комп'ютерного навчання (machine learning), його необхідно спершу навчити первинній виборці (training set), яка складається з певної кількості зображень облич, які хочемо розпізнавати. Як тільки модель стане навченою, слід подати на вхід деяке зображення і в результаті отримаємо відповідь на питання: якому зображенню із загальної вибірки з найбільшою вірогідністю відповідає дане та чи належить дане зображення виборці взагалі.

Головний принцип алгоритму – представити вхідні зображення у вигляді однієї спільної матриці, яка буде складатися із суми базисних компонент зображень:

$$\Phi_i = \sum_{j=1}^{K} w_j u_j, \quad (7)$$

де Φ_i – відцентроване зображення обличчя, w_j – ваги, u_j – власні вектори.

Маючи w як ваговий коефіцієнт вибраної значущої частини обличчя та u як вибрану ділянку обличчя, вибір необхідної ділянки обличчя можливо описати процесом сегментації. Процес сегментації – це процес, у ході якого відбувається розбиття зображення на складові об'єкти. Причому зазвичай використовується таке формальне визначення. Нехай F – це позначення сітки всіх пікселів зображення, тобто набір усіх пар:

$$F_{MxN} = \{(i,j)\} : i = 1,2,\dots,N; j = 1,2,\dots,M.$$

При цьому $\bigcup_{i=1}^{N} \mathrm{Fi} = \mathrm{F}, \mathrm{Fi} \cap \mathrm{Fj} = 0, i \neq j$ [18].

Система сегментації складається з багатошарового персептрона, який виконує адаптивну багаторівневу сегментацію, використовуючи мітки, отримані за допомогою методу нечіткої кластеризації. Ваги нейронної мережі не можуть бути ініційовані випадковим числом, усі вони встановлюються в 1. Щоб забезпечити більше двох стабільних станів на виході нейрона, розроблена спеціальна функція активації. Ця функція складається з набору сигмоподібної функції з множинними рівнями. Мультисигмоїда утворюється шляхом суперпозиції зсунутих сигмоїдальних функцій і виражається в такий спосіб:

$$f(x) = \sum_{k} \left(\frac{y_k - y_{k-1}}{1 + e^{-\frac{(x-\theta_k)}{\theta_0}}} + y_{k-1} \right) \times$$
$$\times [u(x - y_{k-1} \cdot d^a) - u(x - y_k \cdot d^a)], \quad (8)$$

де u – крокова функція, θ_k – пороги, y_k – цільовий рівень кожної сигмоїди, θ_0 – параметр крутизни, d – ступінь сусідства, a – параметр активності сусідства. Пороги і цільові величини виводяться з функції помилки. Оскільки діапазон значень стану нейронів вхідного шару залежить від кількості нейронів наступного шару, то значення порогів адаптовані таким чином, щоб відображати цю залежність [19].

Нейронна мережа працює з інтенсивностями пікселів. Іншими словами, мережа не змінює значення нечіткої приналежності пікселів для того, щоб зменшити помилку, а замість цього вона відображає початкові значення пікселів на такі значення, які зменшують середню кількість нечіткості відповідно до початкового розподілу. Таким чином, вихід нейронної мережі спочатку розглядається в термінах сірого кольору, який далі перетворюється на нечіткість для визначення помилки. Інформація про значення приналежності пікселів може бути корисна в подальшому залежно від призначення системи.

5. ВИСНОВОК

Узагальнюючи викладене, можна зробити такі висновки: розвиток технологій штучного інтелекту та машинного навчання розпочав нову добу розвинення суспільства, орієнтованість провідних країн світу зумовлює значне пришвидшення цього процесу і тягне за собою як наслідок трансформацію всього світового порядку. Роль цифрового виміру та безпеки цифрової інформації стає все більш значущою і її важливість зростатиме разом із цифровізацією світу, тому одним із вагомих питань безпеки є інформація та її захист, пошук нових шляхів та вдосконалення тих, що вже існують. У цій роботі з'ясовано, що таке нейронна мережа, штучний нейрон, описано роботу алгоритму розпізнавання Eigenface, оскільки розуміння принципу роботи алгоритму значно полегшує застосування на практиці, також розглянуто перспективи розвитку цих мереж і важливість у наш час, навчання з метою подальшої можливої реалізації. Запропоновано додаткові етапи вдосконалення алгоритму за допомогою теорії нечітких множин, яка стає потужним ін-

струментом для побудови інтелектуальних апаратно-програмних систем розпізнавання образів. Упровадження в алгоритм нечіткого фільтра обчислює нечіткий приріст, так що зображення стають менш чутливими до локальних змін структур, меж об'єктів. Фільтр забезпечуватиме високий ступінь розрізнення між шумом і структурними об'єктами зображення. Сегментація дозволяє розбивати зображення на менші частини, що значно покращує розпізнавання системою.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Журавель И. Краткий курс теории обработки изображений [Електронний ресурс]. – Режим доступу: http://matlab.exponenta.ru/ imageprocess/index.php.

[2] Вежневец А. Методы сегментации изображений: автоматическая сегментация / А. Вежневец, О. Баринова // Сетевой журнал Компьютерная графика и мультимедия. 2006. [Електронний ресурс]. – Режим доступу: http://cgm.computergraphics.ru/ content/view/147.

[3] Bowyer K.W., Hollingsworth K., Flynn P.J. A Survey of Iris Biometrics Research: 2008-2010, in Handbook of Iris Recognition, Mark Burge and Kevin W. Bowyer, editors, Springer, 2012.

[4] Boyd M., Carmaciu D., Giannaros F., et al. MSc Computing Science Group Project Iris Recognition. Imperial College, London. 2010.

[5] Макс Тегмарк "Життя 3.0. Доба штучного інтелекту" / пер. з англ. Зорина Кораблiна. Видавництво "Наш формат", 2019. Розділ 3, підрозділ "Зброя" та "Кібервійна". С. 137–147.

[6] Основы компьютерной безопасности: курс лекций. Учебное пособие (издание третье). Галатенко В.А. Под редакцией академика РАН В.Б Бетелина. – М.: ИНТУИТРУ "Интернет университет Информацион-ных технологий", 2006. – 208 с.

[7] Криптография и безопасность сетей: Учебное пособие/ Фороузан Б.А.; Перевод с английского под редакцией А.Н. Берлина. – М.: Интернет-Университет Информационных Технологий: БИНОМ. Лаборатория знаний, 2010. – 784 с.: ил., табл. – (Основы информационных технологий). (465–467).

[8] https://bintel.org.ua/nukma/shtuchnij-intelekt-i-rozvidka/ – "How to Win the Battle Over Data. The United States Dithers While Authoritarians Seize the Day" by Eric Rosenbach and Katherine Foreign Affairs. September 17, 2019. Режим доступу: https://www.foreiqnaffairs.com/articles/2019-09-17/how-win-battle-over-data.

[9] P. A. Viola and M. J. Jones. Rapid object detection using a boosted cascade of simple features. In Proc. IEEE Conference on Computer Vision and Pattern Recognition, 2001.

[10] Krizhevsky A., Sutskever I., Hinton G. E. Imagenet classification with deep convolutional neural networks //Advances in neural information processing systems. –2012. – С. 1097–1105.

[11] The Artificial Neural Networks Handbook: Part 4: вебсайт. URL: https://dzone.com/articles/the-artificial-neural-networks-handbook-part-4.

[12] What is an artificial neuron and why does it need an activation function? [Електронний ресурс]. – Режим доступу: https://towardsdatascience.com/what-is-an-artificial-neuron-and-why-does-it-need-an-activation-function-5b4c1e971d80.

[13] Активаційні функції [Електронний ресурс]. – Режим доступу: http://um.co.ua/1/1-1/1-12496.html.

[14] Моделі нейронних мереж [Електронний ресурс]. – Режим доступу: [https://dl.khadi.kharkov.ua/mod/page/view.php?id=106611&forceview=1].

[15] Навчання нейронної мережі [Електронний ресурс]. – Режим доступу: http://um.co.ua/10/10-7/10-78023.html

[16] Простими словами про складні: Що таке нейронні мережі? [Електронний ресурс]. – Режим доступу: https://phoneinfo8.info/prostimi-slovami-pro-skladni-sho-take-neironni-mereji/.

[17] Farbiz F. Fuzzy Techniques in Image Processing / F. Farbiz, B. Menhaj // New York: Springer-Verlag, vol. 52, Studies in Fuzziness and Soft Computing, ch. A fuzzy logic control based approach for image filtering. – 2000. – pp.194 – 221.

[18] Сарапулов Віктор Сергійович Дослідження EIGENFACE алгоритму розпізнавання обличь та його реалізація у MATLAB середовищі. Міжнародний науковий журнал // № 5, 2016.

[19] V. Boskovitz, H. Guterman. An Adaptive Neuro-Fuzzy System for Automatic Image Segmentation and Edge Detection // IEEE TRANSACTION ON FUZZY SYSTEM, VOL.10, NO.2, APRIL 2002.

Стаття надійшла до редколегії **07.06.2021**

Multifactor authentication system based on neural networks

The biometric approach is considered one of the most relevant in identification and authentication systems. The biometric method is based on the analysis of unique human characteristics. Face recognition is an important task, because it is the first stage of identification, to find out who owns the face and whether it is in the database, you must first locate it. To solve this problem, different approaches are used among them: empirical methods, method based on learning, method based on comparison with a template, method based on contour models. When recognizing a face, the system that solves this problem must take into account a number of factors: differences in the faces of different people, changing the angle of the face, the possibility of certain features, changing facial expressions, the presence of obstacles in the image that may partially obscure the subject. Artificial intelligence is both a field for development and a challenge. Due to the fact that the development of machine learning and artificial intelligence is often focused on processing large data sets, and machine learning algorithms directly depend on the quality of the information it processes, interference and misinformation can disable further operation of the algorithm, which can lead to incorrect conclusions, the correctness of which will be difficult to verify because of the large data sets. The choice of method for solving the problem of face detection depends on the specific problem and the conditions in which the algorithm should operate.In this article the possibilities of neural networks for application in the system of multifactor authentication are considered and analyzed. Options for possible implementations using an artificial network, prospects for the development of these networks and the importance in our time are considered. Modern research in this field among the leading countries of the world is analyzed. One of the methods for application is the EIGENFACE face recognition algorithm. Prospects for the use of neural networks, artificial intelligence, review of the features of learning artificial neural network and algorithm EIGENFACE for use in multifactor authentication and proposed steps to improve this algorithm based on fuzzy set theory. The paper clarified what a neural network, an artificial neuron, the operation of the Eigenface recognition algorithm is, because knowledge of the principle of the algorithm greatly facilitates its application in practice, the learning process is considered for further possible implementation. Additional stages of algorithm improvement with the help of fuzzy set theory are offered, which becomes a powerful tool for building intelligent hardware and software pattern recognition systems. The introduction of a fuzzy filter into the algorithm calculates the fuzzy increment so that the images become less sensitive to local changes in structures, boundaries of objects. The filter will provide a high degree of distinction between noise and structural objects of the image. Segmentation allows you to split images into smaller parts, which greatly improves system recognition.

Keywords: *information protection, authentication, identification, artificial neuron, artificial neural network, fuzzy sets.*

Олег Кулінич,
кандидат технічних наук, доцент, Інститут спеціального зв'язку та захисту інформації Національний технічний університет України "Київський політехнічний інститут", Київ, Україна.

Oleg Kulinich,
Candidate of Technical Sciences, Associate Professor, Institute of Special Communication and Information Protection, National Technical University of Ukraine "Kyiv Polytechnic Institute", Kyiv, Ukraine.

Анастасія Роскот,
курсант Інституту спеціального зв'язку та захисту інформації Національний технічний університет України "Київський політехнічний інститут", Київ, Україна.

Anastasia Roskot,
cadet at the Institute of Special Communications and Information Protection, National Technical University of Ukraine, Kyiv Polytechnic Institute, Kyiv, Ukraine.