УДК 004

Є.Ситнік, магістр гр. КІ-21М-1,4,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ РОЗПІЗНАННЯ ОБРАЗІВ У СТРУКТУРІ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ БАНКІВСЬКОЇ УСТАНОВИ

У статті програмне забезпечення, яке призначено для системи розпізнання образів у структурі технічного захисту інформації банківської установи. Метою розробки є дослідження та програмна реалізація системи розпізнання образів у структурі технічного захисту інформації банківської установи. Об'єктом дослідження є процес розпізнання образів у структурі технічного захисту інформації банківської установи. Предметом дослідження є методи розпізнання образів у структурі технічного захисту інформації банківської установи. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи розпізнання образів у структурі технічного захисту інформації банківської установи. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп'ютерна інженерія, розпізнання образів, технічний захист інформації

Постановка проблеми. Завдяки експоненціальному зростанню ІКТ-технологій індустрія цифрового банкінгу досягла величезних успіхів у зручних, ефективних і швидких фінансових транзакціях. У результаті з'явилися численні нові банківські послуги, продукти та можливості для бізнесу. Розумна автентифікація за обличчям – це передова технологія, яка використовується в мобільному банкінгу. Користувачі можуть використовувати цю технологію для перевірки своєї ідентифікації за допомогою функції розпізнавання обличчя камери на своєму мобільному пристрої. Цей метод використовує складні алгоритми, які можуть аналізувати обличчя людини та виділяти відмінні характеристики, які можна побачити на ньому.

Атрибути зображень різних осіб потім класифікуються за допомогою алгоритмів навчання та методу кластеризації K-середніх. Для автентифікації осіб використовуються штучна нейронна мережа (ANN), адаптивна нейронна система нечіткого висновку (ANFIS) і комп'ютерна система дерева рішень (DT). У цьому запиті використовується обличчя. Крім того, метод Wild Horse Optimizer (WHO) використовувався для підвищення точності та оптимізації систем машинного навчання шляхом зважування функцій кластера. Нечітка логіка використовується для прийняття рішень щодо автентифікації на основі результатів алгоритмів машинного навчання. Найкраща функція з широкого набору даних вибирається за допомогою техніки, заснованої на еволюційних алгоритмах.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи розпізнання образів у структурі технічного захисту інформації банківської установи.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи розпізнання образів у структурі технічного захисту інформації банківської установи.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем розпізнання образів у структурі технічного захисту інформації банківської установи.

– Дослідження системи розпізнання образів у структурі технічного захисту інформації банківської установи.

– Програмна реалізація системи розпізнання образів у структурі технічного захисту інформації банківської установи.

Об'єктом дослідження є процес розпізнання образів у структурі технічного захисту інформації банківської установи.

Предметом дослідження є методи розпізнання образів у структурі технічного захисту інформації банківської установи.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу.

Як можна використовувати розпізнавання зображень у фінансових установах:

1. Виявлення шахрайства

Однією з головних проблем у фінансовій сфері є запобігання та виявлення шахрайства, яке може призвести до значних збитків і репутаційної шкоди. Розпізнавання зображень може допомогти фінансовим установам перевірити особу та автентичність клієнтів, документів і транзакцій. Наприклад, розпізнавання зображень можна використовувати для сканування та перевірки паспортів, водійських прав та інших форм ідентифікації, а також для їх порівняння із зображеннями обличчя, зробленими камерами чи мобільними пристроями. Розпізнавання зображень також можна використовувати для виявлення аномалій і невідповідностей у чеках, рахунках-фактурах, квитанціях і контрактах, а також для позначення підозрілих дій і поведінки.

2. Кредитний скоринг

Іншим важливим аспектом фінансів є оцінка кредитоспроможності та профілю ризику позичальників і кредиторів. Розпізнавання зображень може допомогти фінансовим установам покращити свої моделі та алгоритми оцінки кредитоспроможності шляхом включення альтернативних джерел даних і функцій. Наприклад, розпізнавання зображень можна використовувати для аналізу профілів у соціальних мережах, поведінки в Інтернеті та особистих уподобань потенційних клієнтів, а також для отримання інформації із зображень їхніх активів, власності та способу життя. Розпізнавання зображень також можна використовувати для моніторингу ефективності та стану кредитів і застави, а також для прогнозування ймовірності дефолту та повернення.

3. Обслуговування клієнтів

Третій спосіб використання розпізнавання зображень у фінансах – покращення обслуговування клієнтів і покращення досвіду. Розпізнавання зображень може допомогти фінансовим установам пропонувати більш персоналізовані та зручні послуги та продукти своїм клієнтам, а також підвищити їхню лояльність і задоволеність. Наприклад, розпізнавання зображень можна використовувати для створення чат-ботів і віртуальних помічників, які можуть розпізнавати емоції, наміри та потреби клієнтів і реагувати на них, а також надавати відповідні рекомендації та рішення. Розпізнавання зображень також можна використовувати для біометричної автентифікації та способів оплати, таких як розпізнавання обличчя, сканування відбитків пальців і розпізнавання райдужної оболонки ока.

4. Аналіз ринку

Четвертий спосіб використання розпізнавання зображень у фінансах – це підтримка аналізу ринку та прийняття рішень. Розпізнавання зображень може допомогти фінансовим установам отримати розуміння та інформацію з різних джерел візуальних даних, таких як супутникові зображення, аерофотознімки та відеопотоки. Наприклад, розпізнавання зображень можна використовувати для вимірювання та прогнозування економічної діяльності, попиту та пропозиції в різних секторах, регіонах і країнах, а також для визначення тенденцій і закономірностей. Розпізнавання зображень також можна використовувати для оцінки та порівняння ефективності та вартості різних компаній, продуктів і брендів.

5. Відповідність нормативним вимогам

П’ятий спосіб використання розпізнавання зображень у фінансах – це забезпечення відповідності нормативним вимогам і звітності. Розпізнавання зображень може допомогти фінансовим установам дотримуватися правил і стандартів, встановлених владою та регуляторами, а також уникнути покарань і штрафів. Наприклад, розпізнавання зображень можна використовувати для автоматизації та оптимізації процесів збору, перевірки та подання даних, а також для зменшення помилок і ризиків. Розпізнавання зображень також можна використовувати для моніторингу та аудиту діяльності та операцій фінансових установ, а також для виявлення будь-яких порушень і повідомлень про них.

6. Майбутні перспективи

Розпізнавання зображень – це потужний і універсальний інструмент, який можна використовувати у фінансах для підвищення ефективності, точності, безпеки та інновацій. Однак розпізнавання зображень також стикається з деякими проблемами та обмеженнями, такими як якість даних, конфіденційність, етика та упередженість. Тому фінансовим установам необхідно обережно й обережно приймати та впроваджувати розпізнавання зображень, а також слідувати найкращим практикам і вказівкам. Розпізнавання зображень не замінює людське судження та досвід, а радше доповнює та сприяє. Розпізнавання зображень може допомогти фінансовим установам досягти своїх цілей і завдань, а також створити цінність і вплив на своїх клієнтів і зацікавлених сторін.

Ідентифікація облич людей у розумних банківських системах за допомогою штучних нейронних мереж

Використання мобільного телефону для здійснення банківських транзакцій стало звичайною та популярною практикою в епоху цифрових технологій та Інтернету [1]. Безпека та автентифікація користувачів стають все більш важливими з розвитком мобільного банкінгу та зростанням кількості користувачів [1]. Щоб покращити та полегшити це, інтелектуальна автентифікація обличчя була представлена як нова та потужна технологія [3]. Рівень безпеки біометричних пристроїв має бути підвищений, щоб забезпечити ефективну систему, особливо для онлайн-банкінгу [4]. Мобільна автентифікація може бути відповідним рішенням, яке дозволяє здійснювати онлайн-банкінг, мобільний банкінг і мобільні платежі таким чином, щоб легко забезпечити безпеку [5 , 6]. Лише автентифікація чутлива до атак; у випадках крадіжки або довірених третіх осіб безпеку можна легко порушити [7]. Хакери можуть легко зламати безпеку, оскільки більшість паролів виглядають слабкими. Безпечне банківське обслуговування дає клієнтам впевненість у тому, що їхня інформація в безпеці та що вони можуть з упевненістю здійснювати безпечні операції [8]. Для створення безпеки в системі онлайн-банкінгу, однією з яких є Мобільний банк, наразі були представлені різні методи [9]. Кожен із цих методів намагався виявити атаку за допомогою певної логіки та стратегії та запобігти проникненню в систему [10]. Незважаючи на багато зусиль, які були зроблені, ці методи все ще стикаються з проблемами безпеки та не можуть підтримувати належне покриття безпеки в цих системах [11]. Тому в цій статті ми представимо модель, яка використовує оптимізовані гібридні можливості для виявлення ідентичності зразків і автентифікації людей за допомогою онлайн-зображення мобільного телефону [12]. Запропонована в статті модель реалізована на основі підходів штучних нейронних мереж (ШНМ), адаптивних нейронних нечітких мереж (АНФІС) та дерев рішень (ДТ) для автентифікації особи. Однак ці методи самі по собі не мають високої точності. Тому ми використали алгоритм оптимізації дикого коня, щоб покращити продуктивність цих систем машинного навчання, і ми використали нечітку комбінацію результатів, щоб прийняти остаточне рішення. У цій роботі алгоритм автентифікації обличчя для мобільного банкінгу моделюється за допомогою програмного забезпечення MATLAB, а потім реалізуються та перевіряються плани, методи та інші запропоновані елементи для потрібної системи. Нарешті, результати моделювання порівнюються з іншими методами автентифікації. У цьому контексті ми спробуємо створити інтелектуальну технологію для безпечного та зручного банківського обслуговування, яка базуватиметься на ідентифікації людей на основі

зображень їхніх облич під час дзвінків з мобільного телефону. Поки що етап автентифікації використовувався в мобільному банкінгу, а існуючі алгоритми в цій галузі є проникними та мають слабкі місця в безпеці. У цьому контексті, після огляду існуючих методів автентифікації та їх порівняння, представлено новий інтегрований метод, заснований на гібридній моделі, оптимізованій за допомогою ВООЗ у мобільному банкінгу, для встановлення більшої безпеки та точності. Технологія розпізнавання обличчя (FRT) відома як обладнання для підтримки перевірки особи та автентифікації. Було досягнуто великих успіхів у розробці точних і стійких до втручання рішень FRT за допомогою технологій машинного навчання (ML) і штучного інтелекту (AI), як на чіпі, так і в хмарі. Ці розробки привели до більшої впевненості банків у використанні цієї технології для широкого спектру програм і варіантів використання. Використання еволюційних алгоритмів як нового підходу в цій статті може допомогти створити гібридну модель ідентифікації. Виходячи з цього, ми змогли допомогти підвищити безпеку FRT за допомогою проблеми зіставлення ознак, отриманої з набору зображень людей за допомогою генетичного алгоритму. Банки також безпосередньо використовують можливості машинного навчання, технології штучного інтелекту та еволюційних алгоритмів для покращення біометричних характеристик і розпізнавання особи. Це важливо і дає банкам впевненість, що біометрична технологія є безпечною та надійною. Звичайним методам виявлення та аналізу рис обличчя здебільшого не вистачає надійності та тривалий час обчислень. Ця стаття має на меті виявити способи, за допомогою яких машини можуть навчитися автоматично інтерпретувати інформацію в обличчях без необхідності ручної кластеризації функцій, використовуючи підхід глибокого навчання. Важливі внески поточної роботи підсумовуються таким чином:

– Вона представляє систему автентифікації за обличчям із реалізацією на основі машинного навчання з використанням гібридної моделі для динамічної автентифікації.

– Запропонована гібридна техніка була розроблена та перевірена за допомогою метаевристичного алгоритму ВООЗ у м’якому моделюванні на основі автентифікації людей для підвищення точності розпізнавання.

– Сегментація ознак, отриманих із різних типів зображень, базується на моделі кластеризації на основі K-середніх для трьох наборів методів машинного навчання: ANFIS, ANN і Дерево рішень (DT).

– Використання системи нечіткої логіки для прийняття рішень для ідентифікації людей з найвищою можливою точністю.

– Генетичний алгоритм використовувався для зіставлення ознак, вибору цих ознак і зменшення функцій шляхом видалення ознак, несумісних з реальними людьми в кожній системі. У цьому випадку мобільна реалізація виконується процесорами всіх типів телефонів.

В даний час системи автентифікації користувачів мобільних телефонів за допомогою PIN-коду, відбитків пальців і методів розпізнавання обличчя мають ряд обмежень. У статті [13] проведено порівняння одномодальних і мультимодальних поведінкових біометричних особливостей, тоді як досліджувані техніки розглядають різні дії, такі як набір тексту, прокручування, малювання чисел і натискання на екрані. Для кожної модальності реалізована окрема рекурентна нейронна мережа (RNN) з потрійними втратами. Потім виконується зважена комбінація різних модальностей на рівні балів.

Посилання [14] реалізує комплексний підхід до безпеки розумного дому, який покращує конфіденційність і безпеку за допомогою двох різних технологій, що розвиваються, а саме автентифікації обличчя та розпізнавання мовлення за допомогою його мобільного телефону/планшета/ПК. Для здійснення всього процесу використовуються нейронні мережі. Конфіденційність даних і обмеження ресурсів мобільних пристроїв були двома основними проблемами автентифікації, для вирішення яких у статті [15] запропоновано гібридне рішення. У першому часткове семантичне шифрування використовується для здійснення шифрування на основі алгоритму Пайє. На відміну від цього, останній розгортає глибоку згорточну нейронну мережу та локальну потрійну

комбінацію шаблонів для досягнення розпізнавання обличчя.

Оскільки глибокі нейронні мережі (DNN) не стійкі до вхідних збурень, моделі розпізнавання обличчя (FRM) у DNN страждають від цієї вразливості. Згідно з представленим методом [16], ворожі атаки розроблені після змін збереження ідентичності в обличчях, і в цій ситуації спостерігаються дефекти FRM для розпізнавання зображень, що належать до тієї самої ідентичності. Моделювання цих семантичних змін, що зберігають ідентичність, здійснюється через збурення, обмежені напрямком і величиною в прихованому просторі Style GAN. Важливим моментом є те, що семантична надійність FRM визначається статистичним описом збурень, які призводять до збоїв у FRM.

Щоб розвинути продуктивність розпізнавання обличчя на основі відео, пропонується нова семантична модель підпростору [17 , 18]. Важлива мета полягає в тому, щоб створити відповідний низьковимірний підпростір для кожної людини, на основі якого будується семантична модель для категоризації ключових кадрів людини в певні класи. Згодом, після семантичної класифікації, ключові кадри, що належать до тих же класів, використовуються для навчання лінійних класифікаторів для розпізнавання. Цікаво, що масштабні експерименти з базою даних відео з великими обличчями (XM2VTS) показують, що вищезгадана методологія досягає значного підвищення продуктивності порівняно з традиційними методами.

Як правило, для підтвердження особи користувача автентифікація користувача смартфона здійснюється за допомогою механізмів (пароль або шаблон безпеки). До переваг цих механізмів можна віднести простоту, дешевизну, швидкість для частого входу. З цим досвідом вони пошкоджуються так само, як напад плечем або розмазування. Цю проблему можна вирішити шляхом автентифікації користувачів за допомогою їх поведінки (тобто поведінки дотиків) під час використання смартфонів. Така поведінка включає тиск пальця, розмір і час натискання під час натискання клавіш. Вибір функцій (із цих поведінок) може відігравати важливу роль у продуктивності процесу автентифікації. Таким чином, мета статті [19 , 20] полягає в тому, щоб запропонувати добре організовану техніку автентифікації, яка забезпечує неявну автентифікацію для користувачів смартфонів, не накладаючи додаткових витрат на спеціальне обладнання та враховуючи обмежені можливості смартфона. Спочатку, відповідно до ставлень фільтра та оболонки, розміщуються методи вибору ознак оцінки, а потім використовується найкращий метод, щоб запропонувати метод неявної автентифікації. Слід зазначити, що оцінка цих методів проводиться відповідно до випадкового класифікатора лісу.

Розпізнавання обличчя вказує на те, що це єдині дані, доступні в реальному світі в багатьох функціональних програмах, що призводить до значного покращення продуктивності для більшості існуючих підходів FAR на основі глибокого навчання. Пропонується просторово-семантичне навчання (SSPL), метод, який вимагає двох кроків для навчання [11]. Щоб дізнатися про просторово-семантичні відносини з великомасштабних немаркованих даних обличчя, спочатку будуються три допоміжні завдання: завдання ротації фрагментів (PRT), завдання сегментації фрагментів (PST) і завдання класифікації фрагментів (PCT). Зокрема, PRT використовує самоконтрольоване навчання, щоб використовувати переваги просторової інформації, що міститься на фотографіях обличчя. На основі моделі аналізу обличчя PST і PCT відповідно охоплюють семантичну інформацію зображень обличчя на рівні пікселів і на рівні зображення. Другий крок – перенесення просторово-семантичних знань, отриманих із допоміжної діяльності, до завдання FAR. Це дає змогу точно налаштувати попередньо підготовлену модель за допомогою відносно невеликої кількості позначених даних. Описано технології побудови смарт-камер для семантичної обробки зображень на основі ядер ELcore [12]. Розглянуто етапи семантичного аналізу зображення для розпізнавання облич. На ELcore DSP-ядер виявлені та впроваджені на практиці ресурсомісткі алгоритми. Запропоновано метод автоматичного порівняльного маркування м’якої біометрії обличчя [13]. Проводяться подальші дослідження щодо необмеженого розпізнавання обличчя людини з використанням цієї порівняльної м’якої

біометрії в галереї з мітками людей (і навпаки).

Стаття [13] представила просту та ефективну нечітку нейронну мережу типу 2 на основі глибокого навчання на основі Фур'є для проблем великої розмірності. Правила будуються безпосередньо шляхом швидкого перетворення Фур'є. Вхідна матриця/вектор сегментована, і кожен сегмент представляє нечітке правило. Верхні/нижні межі спрацьовування правила отримують шляхом перетворення Фур'є. Вихід обчислюється простим методом редукції типу. Усі попередні та наступні параметри оптимізовано простим градієнтним спуском і розширеним фільтром Калмана на основі нечіткої коретропії. Розмір ядра звичайних фільтрів на основі коретропії визначається нечіткою системою. Збіжність методу навчання доводиться методом Ляпунова. Ефективність запропонованого підходу підтверджується задачею розпізнавання обличчя (1024 вхідних змінних), розпізнаванням цифр англійського рукописного тексту (1024 вхідних змінних) і задачею моделювання з набором даних реального світу (32 вхідні змінні). Моделювання та порівняння демонструють перевагу представленої схеми.

Згідно з дослідженнями, проведеними в цьому розділі, кожне дослідження представляло новий метод вирішення проблеми підтвердження особи. Досліджувані методики мають переваги та недоліки, які зазначені в табл. 1 . Важливим питанням, яке не було досліджено за допомогою всіх методів, є відсутність довіри до методів автентифікації людей у цих дослідженнях, які будуть використовуватися для мобільного банкінгу. Щоб забезпечити різноманітність методів, заснованих на гібридній моделі, у цій роботі було зроблено спробу посилити надійність запропонованої системи автентифікації. Критерій надійності для автентифікації в цьому дослідженні підвищується за допомогою техніки нечіткої логіки та нечітких правил, що її керують.

Дослідження щодо використання біометричних технологій у банках нещодавно набули важливого значення для кращого розпізнавання нових клієнтів, безпечної автентифікації існуючих клієнтів, захисту транзакцій з великою вартістю та боротьби з шахрайством. Цікаво, що більшість традиційних фізичних відділень банків використовують біометрію. У цьому контексті останні цифрові платформи також використовують біометрію. Ця технологія вважається єдиним надійним інструментом для гарантування ідентифікації та гарантування банківської безпеки в усіх каналах.

Тенденції, що призводять до впровадження біометрії серед банків, численні та включають наступне:

– Поява мобільних телефонів і багатогранної біометричної автентифікації на основі мобільних телефонів.

– Поява біометричних банківських карт означає «прощай з пін-кодами».

– Міжканальний прийом. Біометрія запроваджується в усіх банківських каналах – за підтримки відкритих банківських API, нормативних актів, таких як PSD2, які надихають на використання біометрії в сценаріях багатофакторної автентифікації, і пристроїв Інтернету речей, які підтримують голос і відео, і все частіше стикаються з біометрією.

У цій статті обговорювалися онлайн і мобільний банкінг і методи автентифікації. Також були досліджені проблеми безпеки в мобільному банкінгу. У цьому контексті було представлено новий метод вирішення основної проблеми безпеки та автентифікації в мобільному банкінгу. Запропонований метод є комбінацією методів інтелектуального аналізу даних, включаючи методи глибокого навчання, включаючи штучну нейронну мережу (ANN), адаптивну нейронну нечітку мережу (ANFIS) і алгоритм дерева рішень C4.5, усі покращені за допомогою оптимізації дикого коня BOO3 алгоритм. Далі описані етапи реалізації схеми автентифікації особи за допомогою облич людей на основі запропонованої гібридної моделі. Основою гібридного моделювання цієї роботи є сумісність рис, витягнутих із зображень обличчя людей для автентифікації.

Цей процес включає:

Етап 1: набір даних, який використовується в цій статті, може містити будь-які типи даних, які використовуються у сфері мобільного банкінгу. Однак, оскільки ця робота

зосереджена на автентифікації реальних осіб, ми спробуємо використати набір зображень. Різних людей слід використовувати з різних точок зору. Посилання [48 , 49] можуть бути серед наборів даних, використаних у цьому дослідженні.

Етап 2: розробка вдосконаленої методології є важливим питанням у літературі з аналізу даних, і його часто ігнорують як крок у процесі аналізу даних. Важливим моментом є те, що в реальних додатках машинного навчання спостерігається протилежна ситуація і уникається бажана точність. У цій ситуації, порівняно з існуючими методами машинного навчання, намагаються використовувати модифіковані або посилені підходи цих методів. Також для підготовки даних розглядаються дві основні задачі:

– Виконуючи проекти інтелектуального аналізу даних, організовуйте дані в стандартизованій формі, щоб вони були готові до обробки за допомогою інтелектуального аналізу даних та інших комп'ютерних інструментів.

– Набір даних має бути підготовлений таким чином, щоб забезпечити найкращу продуктивність методів аналізу даних.

Етап 3: пов'язаний з категоріями, вибір категорій для інтеграції має бути обраний таким чином, щоб ці категорії доповнювали одна одну, і кожну з них слід коротко пояснити. Розділення навчальної та тестової вибірок для категорій, які доповнюють одна одну, здійснюється на основі ознак, отриманих на етапі обробки даних. У цьому випадку ми застосували контрольовану техніку кластеризації нечітких K-середніх до набору зразків зображень, щоб навчити систему машинного навчання. Цей набір даних містить 77 ознак, отриманих із зображень обличчя суб'єктів.

Етап 4: на цьому етапі для кожної категорії ознак використовується техніка вибору ознак на основі генетичного алгоритму, щоб вибрати набір ознак, які мають найбільшу сумісність у правильній оцінці людей. На основі запропонованих алгоритмів класифікація та розділення вибірок виконується за допомогою комбінованої класифікації, і на цьому етапі виконується зіставлення даних на основі редукції ознак за допомогою запропонованого алгоритму прийняття рішень та застосування їх до даних навчання людей. Для цього кроку визначається цільова функція узгодженості, яка представлена в наступному розділі.

Етап 5: на цьому етапі нашої роботи ми будемо використовувати алгоритм ВООЗ для вдосконалення кожної системи машинного навчання на основі призначених їм функцій. Метою цього етапу є підвищення точності систем машинного навчання на основі зважування специфічних особливостей кожної системи.

Етап 6: Результати, отримані за категоріями, об'єднуються у формі більшості голосів. На цьому етапі вибрані значення для кінцевого результату отримують на основі категорій і на основі нечіткого колективного рішення щодо даних із відповідей. Нечіткі правила, що керують цим рішенням, представлені в наступному розділі.

Розробка структурної схеми

Структурна схема системи наведена на рисунку 1.

Структурно система складається з наступних частин:

1. Відеокамера спостереження, з якої поступає інформація систему розпізнання образів.

2. Система розпізнання образів, яка складається з наступних блоків:

– Блок читання картинки з відеокамери. Він призначений для читання картинок з відеокамери й подання даних на блок аналізу та виділення ознак за допомогою багатопрохідної схеми розпізнавання образів на основі кластерного аналізу.

– Блок аналізу та виділення ознак за допомогою багатопрохідної схеми розпізнавання образів на основі кластерного аналізу. Він є основою системи, й за допомогою нижчеописаного алгоритму проводить розпізнання осіб, та машин, які перетнули межу території банківської установи.

– Блок класифікації та опису об'єкта. Він дозволяє, виходячи з даних, отриманих від блоку аналізу та виділення ознак за допомогою багатопрохідної схеми розпізнавання образів на основі кластерного аналізу, розподілити куди заносити отримані дані, у поля бази даних,

які відповідають за осіб, або у поля бази даних, які відповідають за машини.

3. База даних журналювання розпізнаних образів. У цю баз даних заносяться усі дані, які відносяться до розпізнаних об’єктів, будь то людина, або автомобіль.

4. База даних образів облич. У цій базі даних зберігаються фотографії усіх працівників установи та відвідувачів, з виділенням характерних точок, для кожного обличчя, за якими можливо ідентифікувати або працівника банку, або відвідувача.

5. База даних образів цифр та букв на номерах автомобілів. У цій базі даних зберігаються образи усіх цифр та букв, з яких можуть складатися номера автомобілів, а також номера усіх автомобілів, які перетинали кордон приміщення банківської установи, який встаткований відеокамерами спостереження.

Так як розпізнавання образів відбувається за допомогою алгоритму багатопрохідної схеми розпізнавання образів на основі кластерного аналізу, то наведемо цей алгоритм.

Багатопрохідна схема розпізнавання образів на основі кластерного аналізу

Багатопрохідна схема складається в послідовній класифікації тих самих образів спочатку за допомогою образонезалежних алгоритмів розпізнавання, а потім – алгоритмів, що використовують особливості образів номерів автомобілів, і особливості розпізнавання осіб людини.

Метою багатопрохідної схеми розпізнавання з навчанням є адаптація до особливостей образів. При цьому на кількість і характеристики використовуваних образів не накладається істотних обмежень.

Багатопрохідна схема розпізнавання містить у собі попереднє розпізнавання образів, формування бази даних результатів попереднього розпізнавання, додаткове самонавчання на підставі отриманих результатів розпізнавання, наступні перерозпізнавання образів з урахуванням самонавчання, формування остаточних результатів.

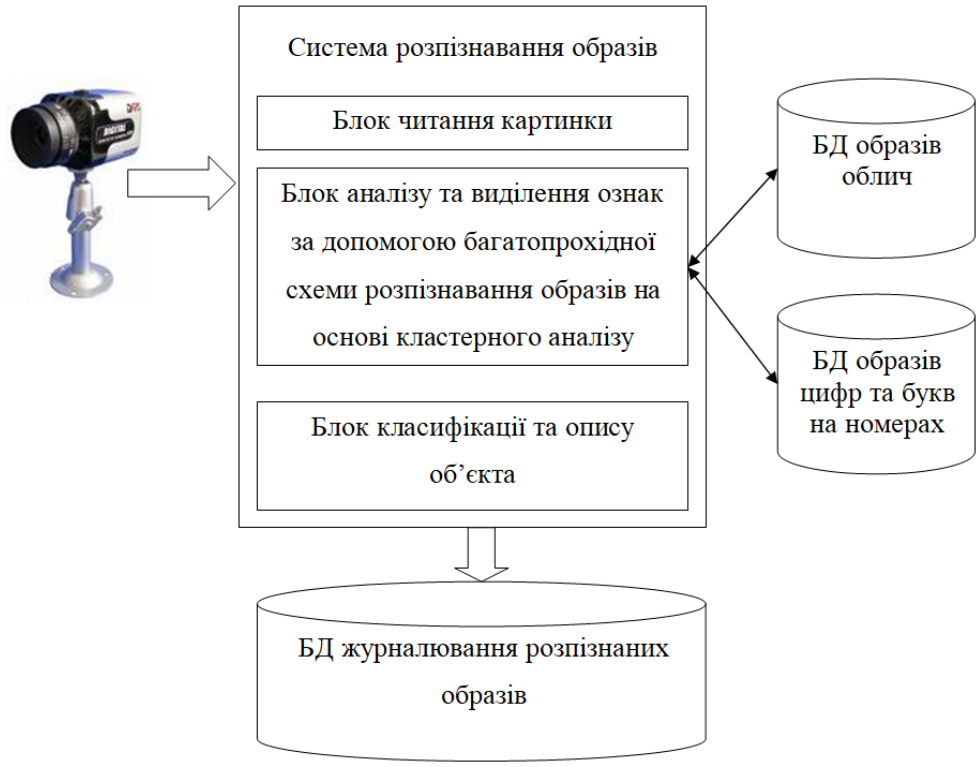

Рисунок 1 – Структурна схема системи

Навчальна вибірка готується першим проходом розпізнавання, що за допомогою образонезалежного алгоритму розпізнавання образів $\Re 1$. Алгоритм $\Re 1$ надає колекції альтернатив (варіанти розпізнавання з оцінками) образів, що відповідають розпізнаним образам, і атрибути образів.

Крім цього перший прохід забезпечує валидацію образів, тобто позначку надійно розпізнаних образів, за допомогою наступних двох механізмів:

– облік оцінок альтернатив, сформованих алгоритмом з монотонними оцінками
– словникове або контекстне підтвердження досить довгого слова.

Комбінація цих механізмів валідирує частину результатів розпізнавання. Таким чином, множина розпізнаних образів розбито на підмножини, що задаються розмірами й атрибутами образа. Як контейнер навчання, призначеного для зберігання розмічених образів, може виступати база даних, що формується на диску, або динамічна структура в оперативній пам'яті.

Метою навчання є побудова набору кластерів, частина яких надійно відділений друг від друга, а кластери, що залишилися, містять вказівки на їхню близькість до інших з погляду обраної Хаусдорфової метрики.

У нашій програмі для кластеризації ми використовували алгоритм ланцюгового розгорнення, алгоритм відноситься до групи методів одиночного зв'язку. Алгоритм кластеризації, що базується на відстані Хаусдорфа й наведений в [4] якісно відрізняється від широко відомих методів, насамперед, через структуру інформації, що підлягає класифікації під час навчання й цілей кластеризації. Мінімізація числа кластерів, швидкодія й інші питання класичної кластеризації мають для нас важливе, але не першорядне значення.

Результатом кластеризації служить множина об'єктів, кожний з яких містить суму стандартизованих ненормалізованих растрів, із близькими ознаками й загальними атрибутами, ланцюгова відстань між якими не перевищує певного заздалегідь межі. Кожний із кластерів крім успадкованих ознак має потужність (числом складових його растрів).

Ознаки кластера використовуються на етапі побудови еталонів накладення, що повинні сформувати базу надійних кластерів, а для кластерів, що залишилися, відповістити на запитання про можливість їхнього використання. Аналіз кластерів образів певного алфавіту містить кілька операцій:

– Перейменування кластера, що складається в розпізнаванні центра сумарного растра (або всієї суми растрів, розглянутого як напівтоновий образ) досить точним алгоритмом розпізнавання образів. Від перерозпізнавання очікується зняття систематичних помилок алгоритму першого проходу, що не зобов'язаний бути адаптивним до особливостей накреслень використовуваних образів.

– Об'єднання двох різноїменних прилеглих кластерів з метою перейменування одного з них. Вирішує завдання, аналогічні завданням перейменування кластера.

– Знищення кластера, тобто вивід ненадійно розпізнаного кластера з розгляду.

– Угруповання кластера з одним або декількома різноїменними з ним кластерами. Фіксує неможливість або ненадійність розрізнення результатів, отриманих накладенням кластерів з однієї групи.

Після первинного аналізу кластерів залишаються тільки надійні кластери, що володіють достатньої валідністю й потужністю. Серед надійних кластерів проводиться ітераційний процес пошуку образів, оскільки на картинці перебувають не просто якісь образи, а образи, що відбуваються з одного або декількох образів. Кластери розбиваються на кілька груп їх складових, і, можливо, по своїх атрибутах (якщо атрибути присутні). Якщо в процесі аналізу виявиться, наприклад, що на картинці присутня тільки один образ, але є кілька кластерів якої-небудь букви, то в остаточну вибірку кластерів треба взяти тільки один, кращий у деякому змісті, а інші можуть бути помилками розпізнавання, помилками сегментації, можуть виникнути через погану якість зображення.

Ітераційний процес аналізу первинних кластерів закінчується формуванням еталонів алгоритму накладення, що здатний відповісти на ряд питань, пов'язаних з можливістю розрізнення близьких образів. Алфавіт розпізнавання, містить ряд образів невідмінних друг від друга у всій множині накреслень цих образів, для яких, проте, необхідно на якімсь із етапів розпізнавання ухвалити рішення щодо виборі одного зі значень. Подібні по

накресленню друковані образи, близькість яких визначається властивостями алгоритмів розпізнавання образів, також є джерелом помилок образонезалежних алгоритмів.

У той же самий час у межах одного образа, як правило, деякі з образів алфавіту й родинних образів помітні геометрично, наявність же декількох образів на картинці може як утруднити, так і спростити розпізнавання близьких образів. Після завершення етапу аналізу кластерів, що досліджує подібні можливі конфліктні ситуації, стають відомим, наскільки добре побудовані еталони можуть дозволяти колізії родинних образів і образів з однаковим накресленням у різних образах. Інформація про це втримується в переліку груп різноїменних родинних образів і в списку відстаней між нерозрізненими образами.

З оброблених кластерів може бути витягнута множина еталонних кістякових і розширених образів, міра близькості до яких забезпечує достатні характеристики якості розпізнавання. Можливе подання еталонів, що складає із трьох об'єктів:

– кістякова підмножина SKEL, що містить значення растра кластерів у границях щирого кістякового образа;

– розширена підмножина COVER, що містить нулі в границях щирого розширеного образа, мабуть, COVER $\supseteq$ SKEL;

– опис штрафу, що залежить від відстані до найближчої точки кістяковий або розширений образи, що обчислюється за допомогою функцій Pen(i, j, M), аргументами якої є координати точки й множина M.

Кожне з підмножин є матрицею того ж розміру, що й стандартизовані растри, що підлягають кластеризації, і залежать від обсягу й інших характеристик кластера. Накладення, тобто обчислення міри близькості довільного образа й еталона E=||eij|| відбувається в кілька етапів, першим з яких є центрування образа. Для відцентрованого, тобто стандартизованого, образа R =||rij|| підраховується сума покомпонентних добутків значень растрів R і E:

$$\Sigma(R,E) = \Sigma\, \delta\,(rij=1 \wedge eij>0) \bullet eij -$$
$$\Sigma\, Pen(i,j,SKEL(S,\alpha))(\,(rij=0 \wedge eij>0) -$$
$$\Sigma\, Pen(i,j,COVER(S,\beta))(\,(rij=1 \wedge eij<0),$$

яка містить у собі як позитивні добутки точок растра, що потрапили в кістякову область, так і негативні компоненти точок, що не потрапили в розширену область, і штраф за недолік точок у кістяковій зоні. У цьому вираженні присутні як позитивні значення суми растрів, що склали кластер, так і негативні штрафні значення. У такий спосіб обчислена близькість відповідає на запитання про те, наскільки добре розпізнаваний образ відповідає розподілу даного кластера, тобто поліпшує імовірнісні властивості оцінок накладення. Зрозуміло, не слід забувати не тільки про евристичні штрафи, що не володіють імовірнісною природою, але й про обсяг кластера, що породжує кістякову область, тому що утворення малих кластерів не є чимсь винятковим для більшості картинок. Внесок штрафів у загальну суму також поліпшує оцінки за умови оптимізації штрафів за видалення від границі розширеного образа. Результатом накладення є альтернатива:

$$(S(E),\ W\bullet\Sigma(R,E)),$$

де S(E) – код образа кластера з растром E.

W – масштабний коефіцієнт для одержання оцінок, при цьому успадковуються властивості кластера (кегль, атрибути образа).

Спосіб центрування стандартизованого розпізнаваного растра, що полягає в сполученні геометричних центрів вихідного растра, розширюваного симетрично до стандартних розмірів, не може дати задовільних результатів у загальному випадку накладення. Пошук центра доповнюється зрушеннями розпізнаваного растра в невеликій околиці геометричного центра еталона з вибором найкращого результату накладення. Кластерному накладенню властивий ряд проблем, пов'язаних із проблемою пошуку геометричного центра образа. Центрування стандартизованих растрів не дозволяє розпізнавати образи із сильно деформованою рамкою. Для складних випадків центрування

необхідне залучення інших алгоритмів, наприклад, обчислення моментів або використання поліграфічних базових ліній.

Відзначимо, що обчислення досить трудомістких оцінок накладення може бути прискорено перериванням підрахунку суми в ситуації набору значного числа штрафів. Значна різниця в розмірах растрів R і E дозволяє прийняти рішення про відмову накладення даного еталона, це міркування в сукупності з фільтрацією по атрибутах еталонів також прискорюють алгоритм накладень.

Еталони містять ряд додаткових ознак, наприклад, для заборони перерозпізнавання образа по кластеру, породженого цим же образом без участі інших образів.

Побудована система еталонів дозволяє використовувати алгоритм накладення як алгоритм, що формує після перегляду всіх еталонів, що задовольняють розміру розпізнаваного образа, колекцію альтернатив, породжених найближчими еталонами. Також можливе використання еталонних накладень і як алгоритм-експерта, що перевіряє гіпотези про те, наскільки добре досліджуваний образ може бути розпізнаний з деяким заданим кодом образа. Можуть бути отримані наступними результатами перевірки близькості розпізнаваного образа одному з еталонів із заданим кодом:

– найменша відстань досягнута на еталоні, далекому від інших еталонів;

– найменша відстань досягнута на еталоні, що потрапив у групу близьких різноїменних еталонів;

– перевірка близькості не може бути зроблена через відсутність еталонів з даним кодом образа.

Отриманий результат може бути проінтерпретований на відміну від образонезалежного алгоритму-експерта, що відповідає тільки на питання про близькість досліджуваного образа до одному з еталонів, у такий спосіб. Перший результат залежно від того, чи є кластер досить представницьким (великий обсяг, валідність його растрів, що склали), може бути визнаний надійним або рекомендаційним як для обчислення автономних оцінок, так і для рішення конфліктів. Другий результат може бути визнаний надійним тільки для перевірки приналежності образа до всієї групи еталонів, у цьому випадку до колекції альтернатив, збагачуваної кластерною інформацією, можуть бути додані відсутні альтернативи родинних образів. Тобто другий результат фіксує конфлікт родинних або нерозрізнених альтернатив як нерозв'язний у рамках кластерної моделі, що може надалі вирішуватися за допомогою словникового пошуку, словникової корекції. Третій результат є відмовою кластерного накладення. У цьому випадку неможливе порівняння двох образів, код одного одного з яких є присутнім в еталонах, а іншого відсутній.

Очікувана відсутність ряду еталонів припускає комбінування результатів образонезалежного алгоритму й алгоритму кластерного накладення, адаптивного до образів у розпізнаваній картинці. Схема комбінування будується в припущенні, що значна частина (80-90%) картинок уже розпізнана без помилок, внаслідок чого для частки, що залишилася, дорозпізнаваємих образів можливе застосування достатнє трудомістких алгоритмів розпізнавання образів. Це означає, що комбінувати кластерне накладення доцільно з алгоритмом, точність якого перевищує точність алгоритму $\Re 1$ розпізнавання образів на першому проході. Комбінування з більше точним алгоритмом (наприклад, з нейронною мережею) забезпечує як збереження кластерних оцінок у випадку успішно розпізнаних обома алгоритмами образів і дозволених конфліктів, так і збереження точності алгоритму $\Re 1$ з одночасним зниженням його оцінок у випадку не підтвердження його результатів надійними кластерами. Це поліпшує й точність, і монотонність оцінок. Використання образонезалежного алгоритму дозволяє розпізнавати й виставляти оцінки образам, для яких не зібралися підтверджувальні еталони. Недоліком описаного комбінування є одержання оцінок різної природи: як образонезалежних, так і кластерних, зіставлення яких у загальному випадку важко. Початкові параметри схеми комбінування, у першу чергу відносяться порогів оцінок, по яких приймається рішення про надійність розпізнавання, можуть змінюватися

після завершення кластеризації, за рахунок чого відбувається додаткова адаптація до результатів першого проходу розпізнавання картинок.

Властиво дорозпізнавання, тобто другий прохід розпізнавання, містить у собі розпізнавання комбінованим алгоритмом як окремо стоячих, так і склеєних і розсипаних образів, які деяким чином були сегментовані на першому проході. Дорозпізнавання рядка образів починається з експертної оцінки як незмінених, так і сегментованих розпізнаних образів. Кожний розпізнаний образ піддається експертизі на предмет підтвердження оцінки його провідної альтернативи алгоритмом, використовуваним як експерт. Образи, що не одержали підтвердження, перерозпізнаються; деякі групи образів піддаються повторної сегментації. Сегментація, що навіть опирається на той самий перелік відрізків розрізування, при використанні іншого алгоритму розпізнавання образів може дати інші результати визначення границь образів. У той же час відзначимо, що часто успішно працює алгоритм розрізування (як, втім, і склейки), заснований винятково на кластерному розпізнаванні, без складання переліку відрізків можливого розрізування, хоча чисто кластерне розпізнавання працює не завжди у зв'язку із уже згадуваною проблемою можливої неповноти кластерів. Перерозпізнані ланцюжки образів конкурують зі своїми прототипами, утвореними на першому проході. Порівнянню підлягають слова, для яких можливо не тільки обчислення функцій над оцінками образів, що склали слово, але й підтвердження словниково-лінгвістичними методами.

Таким чином, побудований комбінований алгоритм (позначимо його $\mathfrak{R}2$) дозволяє поліпшувати точність і монотонність оцінок розпізнавання як за допомогою образонезалежного алгоритму, так і за рахунок надійних еталонів кластерного накладення. Крім цих поліпшень не можна не відзначити ще одного результату другого проходу, що складається в тому, що в перерозпізнаних рядках частина образів одержала додаткову валідацію від надійних еталонів. По суті справи частина образів, що не одержала такий валідації, може бути змінена наступними етапами розпізнавання, а валидированні образи з високою ймовірністю не можуть піддаватися змінам. Окремо слід зазначити валідацію системою еталонів, що містить один єдиний образ, така гіпотеза перевіряється під час кластеризації.

Висновки. У статті теоретичне узагальнення й рішення наукового завдання дослідження методів розпізнання образів у структурі технічного захисту інформації банківської установи. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем розпізнання образів у структурі технічного захисту інформації банківської установи. Досліджена система розпізнання образів у структурі технічного захисту інформації банківської установи. На основі отриманих результатів досліджень створена програмна реалізація системи розпізнання образів у структурі технічного захисту інформації банківської установи. Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання розпізнання образів у структурі технічного захисту інформації банківської установи. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56.
2. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.

3. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». Lecture Notes on Data Engineering and Communications Technologies, 2023, 178, pp. 208–223.
4. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022,
5. Smirnov O., Smirnova T., Anas M. Al-Oraiqat, Drieiev O., Polishchuk L., Sheroz Khan, Yassin M. Y. Hasan, Aladdein M. Amro, Hazim S. AlRawashdeh «Method for Determining Treated Metal Surface Quality Using Computer Vision Technology». Sensors (Basel, Switzerland) Volume 22, Issue 16, 6223, 2022.
6. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». SN Computer Science, Vol 2, 337, 2021. https://doi.org/10.1007/s42979-021-00739-w
7. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, Cracow, Poland, 22-25 September 2021. P. 414-418.
8. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». 4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) - 2021, Lviv, Ukraine, September 21-25, 2021. P. 255-260.
9. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.
10. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
11. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
12. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». CEUR Workshop Proceedings Volume 2654, 2020, Pages 1-14.
13. Smirnov O., Kuznetsov A., Onikiychuk A., Makushenko T., Anisimova O., Arischenko A. «Adaptive pseudo-random sequence generation for spread spectrum image steganography». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 161-165.
14. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
15. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
16. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.
17. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
18. Smirnov, O., Kuznetsov, A., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», CEUR Workshop Proceedings Volume 2608, 2020, Pages 646-660.
19. Zhurakovskyi, B., Tsopa, N., Batrak, Y., Odarchenko, R., Smirnova, T «Comparative analysis of modern formats of lossy audio compression». Workshop Proceedings, 2020, 2654, стр. 315-327.
20. Smirnov O. Kuznetsov A., Zaicenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
21. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.