УДК 343.982.3, 004.89, 004.032.26

АНАЛІЗ БІОМЕТРИЧНИХ ІНТЕЛЕКТУАЛЬНИХ МЕТОДІВ АВТЕНТИФІКАЦІЇ ТА ІДЕНТИФІКАЦІЇ ОСОБИ ЗА ВІДБИТКАМИ ПАЛЬЦІВ ТА ЗА ГОЛОСОМ ДЛЯ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

П.О. ФІЛОНЕНКО, Є.І. БАРСУКОВ, О.А. ВИНОКУРОВА

У статі наводяться результати аналізу проблемних питань систем автентифікації осіб. Основною метою аналізу є визначення перспективної моделі біометричної автентифікації та ідентифікації особи для впровадження та застосування в Україні. До основних задач відносяться аналіз існуючих методів біометричної автентифікації та ідентифікації особи за відбитками пальців та за голосом для підвищення стійкості від загроз в сфері інформаційної безпеки. Розглянуто метод виявлення локальних особливостей біометричних образів за допомогою гібридних штучних нейронних мереж.

Ключові слова: біометрія, автентифікація, гібридні інтелектуальні методи, штучні нейронні мережі.

ВСТУП

Існуючі на сьогоднішній день традиційні методи верифікації особи, які засновані на зберіганні певних ключових даних або запам'ятовуванні паролів, не завжди є надійними і зручними, так як є досить висока ймовірність того що ці дані можуть бути загублені або забуті. Для підвищення надійності проходження процедури автентифікації природним кроком стало використання в системах безпеки біометричних технологій.

На сьогоднішній день біометричні системи використовуються за двома напрямками: для контролю фізичного доступу та доступу до інформації. Такі рішення реалізуються на різних споживчих рівнях: приватному, корпоративному, державному, міждержавному.

Для всіх біометричних методів верифікації характерно величезна відмінність між показниками ефективності в лабораторних умовах, які повідомляються розробниками, і результатами тестування незалежними організаціями. Деякі з перспективних методів приведені у табл. 2.1 [1].

Таблиця 1

Незалежні оцінки систем біометрії

Тип біометрії	Тестові організації	Відсоток хибних відмов	Відсоток хибних пропусків
Відбитки пальців (4 пальця)	Fingerprint Verification Competition (2004)	2 %	2 %
Параметри голосу	The National Institute of Standards and Technology (NIST), (2004)	5-10 %	2–5 %

1. ІЄРАРХІЯ БІОМЕТРИЧНИХ СТАНДАРТІВ

Розглянемо стандарти, зазначені в ієрархії, і організації, що займаються їх створенням. Виняток зробимо лише для стандартів щодо розрахунку продуктивності та інших технічних характеристик біометричних систем, тому що вони зараз самі "сирі" і багато в чому безпосередньо залежать від стану та затвердження стандартів інших груп (рис. 1).

У 2001 р. в США при Міжнародному комітеті з стандартам в інформаційних технологіях (International Committee for IT Standards, INCITS) у листопаді того ж року був створений технічний комітет M1, основним завданням якого стала прискорена розробка стандартів з біометрії для використання в США і в міжнародних стандартах.

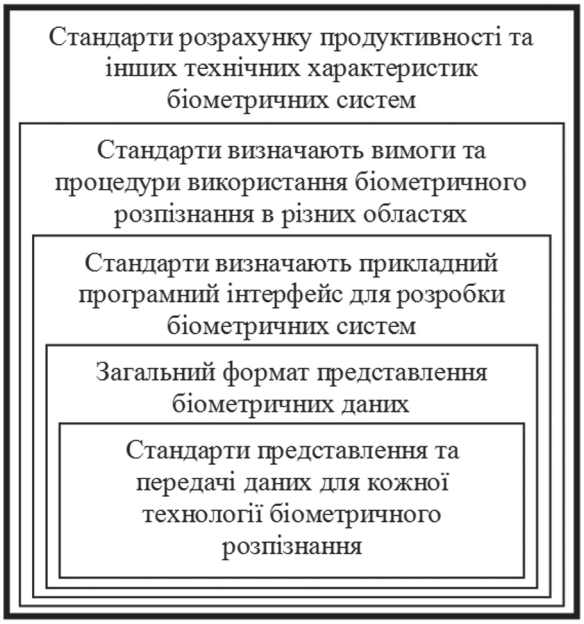

Рис. 1. Ієрархія стандартів з біометрії

На міжнародному рівні цими завданнями займається підкомітет SC37 (Subcommittee 37) об'єднаного технічного комітету з інформаційних технологій JTC 1 Міжнародної організації стандартизації ISO (International Organization for Standardization) та Міжнародної електротехнічної комісії (International Electrotechnical Commission, IEC), створений у червні 2002 р. [2].

У нього входить близько 20 країн, в тому числі і Росія. У Росії створено підкомітет N7 по

біометрії в рамках Технічного комітету Держстандарту ТК355 по автоматичної ідентифікації, який діє у складі SC37 і займається адаптацією і випуском російських стандартів з біометрії. Група М1 входить до SC37 як представник США і технічна консультаційна група (Technical Advisory Group) (рис. 2).

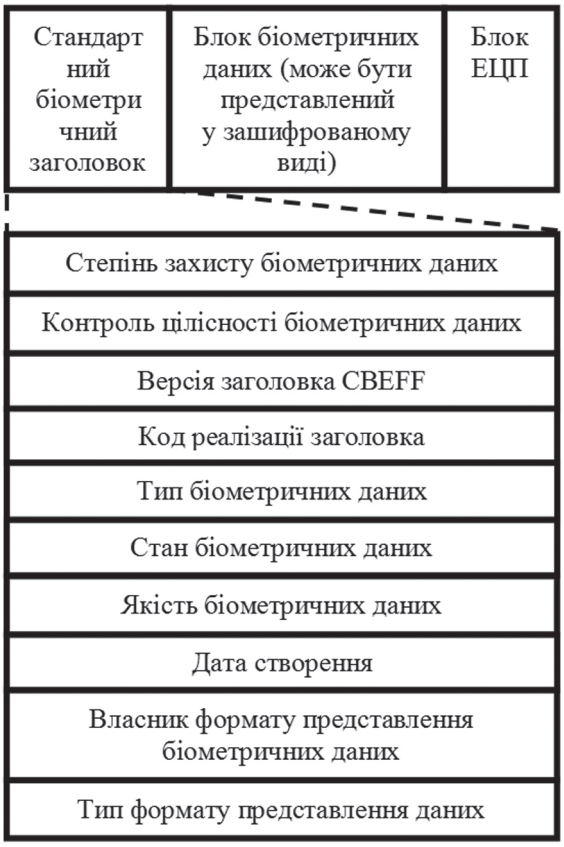

Рис. 2. Склад Common Biometric Exchange File Format

Напрямки діяльності М1 і SC37 аналогічні, тому зупинимося на описі робіт М1, так як вони почалися раніше і деякі з них лягли в основу біометричних стандартів JTC1 SC 37 ISO / IEC.

Використання біометрії в сфері фінансових послуг - стандарт X9.84.

З стандартів, які визначають вимоги щодо використання біометрії в різних промислових галузях, прийнятий стандарт "ANSI X9.84-2000. Biometrics Management and Security for the Financial Services Industry" [3] Американського національного інституту стандартів, розроблений робочою групою X9.F4 акредитованого ANSI комітету стандартів X9. Згодом вийшла його оновлена версія X9.84-2003.

X9.84 визначає мінімальні вимоги безпеки при побудові біометричних систем для сфери фінансових послуг, а також механізми і правила криптографічного захисту процесів одержання, обробки і зберігання біометричних даних.

Зокрема, в стандарті викладені вимоги за такими темами:

– управління біометричними даними та їх захист під час життєвого циклу;

– використання біометричної технології для ідентифікації і автентифікації співробітників і клієнтів банків;

– застосування біометричної технології в системах контролю і управління доступом;

– інкапсуляція біометричних даних;

– технологія захищеної передачі біометричних даних.

Виділимо основні вимоги щодо безпеки для біометричних систем в X9.84.

– біометрична система повинна запобігати можливість обробки біометричних даних, що надійшли до системи з неавторизованого зчитувального біометричного пристрою.

– біометрична система повинна бути побудована так, щоб біометричні дані могли вступити до неї тільки через авторизовані інтерфейси з використанням прийнятих процедур.

– у біометричну систему повинні бути вбудовані механізми захисту для виявлення і запобігання використання штучних біометричних характеристик (наприклад, муляжів).

– там, де це необхідно, в біометричну систему повинні вбудовуватися механізми захисту для запобігання витоку або втрати біометричних даних.

– біометрична система повинна обмежувати доступ до шаблонів, тобто запобігати можливість: реконструкції бази шаблонів за допомогою перехоплених біометричних даних; - обробки запитів на верифікацію в обхід бази шаблонів.

Ідеологія, з якої виходили творці X9.84, спиралася на те, що біометричні характеристики людини не абсолютно конфіденційні і не є прихованими даними (голос можна записати на плівку, обличчя і радужку очей сфотографувати, відбиток пальця зняти з предмета і т. д.) . За певних умов біометричні характеристики можна підробити. Тому весь життєвий цикл всередині біометричної системи по X9.84 повинен бути захищений, скануючи засоби авторизовані в системі, всі дані зашифровані, а сама система повинна вміти відрізняти реальні біометричні характеристики людини від їх підробок.

2. АНАЛІЗ МЕТОДІВ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ З ВИКОРИСТАННЯМ ВІДБИТКІВ ПАЛЬЦІВ

Для обчислення біометричного образу за відбитками пальців було проаналізовано існуючий запатентований алгоритми Precise BioMatch та Міжнародний стандарт ISO/IEC 19794 – 2:2005.

Алгоритм Precise BioMatch [4] використовує як переваги традиційних методів виділення ключових точок, так і передові алгоритми порівнювання візерунків. Такий подвійний підхід дозволяє отримати максимальну кількість інформації з відбитку для подальшого якісного аналізу та гарантування вірною автентифікації. Precise BioMatch створена не тільки для алгоритмів автентифікації особистості у великій базі даних (як,

наприклад, алгоритм AFIS – автоматизовані системи ідентифікації відбитків пальців), але і для найкращого підтвердження особи в логічному і фізичному доступі.

Алгоритм Precise BioMatch не прив'язаний до конкретного типу датчика (сканера відбитків). Отже, користувач може зареєструвати відбитки на одному типі датчика, а проходити перевірку на іншому. Це надзвичайно важливо у випадках, коли біометричне розпізнавання відбитка пальця використовується на дуже великій, неконтрольованій відстані. Але як зазначалось це є запатентований метод і для його використання потрібна згода власників.

Міжнародний стандарт ISO/IEC 19794 – 2:2005 встановлює структуру і формат блоку даних по контрольних точках зображення відбитка пальця .

Стандарт поширюється на широкий діапазон прикладних областей, що використовують автоматизоване розпізнавання відбитку пальця. Стандарт містить терміни та визначення, опис правил визначення контрольних точок, формати даних, у тому числі для використання в ідентифікаційних картах [5].

Цей стандарт встановлює правила визначення розташування контрольних точок на відбитку пальця. Для забезпечення взаємодії між різними біометричними системами на підставі розпізнавання відбитків пальців і порівняння індивідуальних і попередньо зареєстрованих записів відбитків пальця необхідно гарантувати сумісність різних методів отримання контрольних точок. Працює з методів досягається дотриманням правил вилучення контрольних точок відбитка пальця, правил запису форматів і форматів ідентифікаційних карт, які є загальними для біометричних систем, і передбачає можливість введення розширених біометричних даних, сумісних з конкретним обладнанням.

Використання подання відбитка пальця з допомогою характерних ознак спирається на загальноприйняту практику. Контрольними точками називають точки, розташовані на зображенні відбитка пальця в місцях закінчення відбитків гребенів або в місцях біфуркації гребенів. Опис зображення відбитка пальця про терміни розташування і орієнтації контрольних точок закінчення і біфуркацій гребенів дозволяє гарантовано визначити, чи є два зображення відбитками одного і того ж пальця. Цей стандарт встановлює правила визначення та кодування розташування і орієнтації контрольних точок.

Існує два основних типи контрольних точок: точка закінчення основи гребеня і точка біфуркації основи гребеня (або точка розгалуження). Крім зазначених типів у відбитках пальців рідше зустрічаються й інші типи інформативних точок, що мають більш складні визначення. Більш складні типи контрольних точок зазвичай є комбінаціями основних типів, зазначених вище. Деякі кінь рольні точки не є ні точками закінчення гребенів, ні точками біфуркації. Подібні точки відносять до додаткового типу «інша контрольна крапка». Тип «інша контрольна точка» не слід використовувати для контрольних точок закінчення гребеня або біфуркації гребеня. Таким чином, цей Стандарт встановлює наступні типи контрольних точок:

– закінчення гребеня (точка біфуркації основи западин);
– біфуркація гребеня;
– інша контрольна крапка.

У залежності від методу визначення положення точки допускається визначати контрольну точку закінчення гребеня як точку біфуркації западини. Вид методу кодування контрольних точок за допомогою точки закінчення гребеня або точки біфуркації западини повинен бути вказана в полі «Тип формату» біометричного інформаційного шаблону.

Розташування контрольної точки визначають за її горизонтальному і вертикальному положенням. Пошук контрольних точок слід проводити на засадах гребенів або западин, витягнутих з цифрового зображення відбитка пальця. Основу гребеня обчислюють поетапним зменшенням зображення гребеня до лінії шириною в один елемент зображення. Основу западини обчислюють поетапним зменшенням площі западини до лінії шириною в один елемент зображення.

Використання інших методів виявлення контрольних точок допускається тільки у випадку, якщо їх результати відповідають результатам методу стоншення, тобто, якщо значення розташувань і орієнтацій контрольних точок, отримані іншим методом, еквівалентні значенням розташуванні й орієнтації контрольних точок, отриманим методом стоншення.

Обчислення координат контрольних точок слід проводити в декартовій системі координат X-Y. Початок системи координат зображення відбитка пальця має розташовуватися в лівому верхньому кутку вихідного зображення. Вісь X за загальноприйнятим у цифровій обробці зображень допущенню повинна бути спрямована зліва направо (позитивний напрямок), вісь Y повинна бути спрямована вниз (позитивний напрямок). У системі координат зображення пальця вісь X повинна бути направлена справа наліво відповідно до рис. 3. Всі значення координат X і Y повинні бути невід'ємними.

Рис. 3. Система координат

Координати X і Y контрольних точок слід визначати з кроком, рівним одному елементу зображення, і з просторовим дозволом, наведеним у полях «Дозвіл по осі X» і «Дозвіл по осі Y». Дозволи зображення по осі X і Y визначають окремо.

У форматі запису контрольних точок відбитка пальця дозвіл системи координат має бути записано в заголовку запису.

Цей стандарт встановлює такі правила визначення та запису значень кутів. Кут орієнтації контрольних точок вимірюють від горизонтальної осі проти годинникової стрілки.

У форматах запису кут орієнтації контрольних точок квантується з кроком квантування рівним куту 1,40625° (360/256], на один молодший біт. Кодування кута у форматах для використання в ідентифікаційних картах залежить від того, що використається формат нормального або компактного розміру.

Орієнтація контрольної точки закінчення гребеня, визначеної через точку біфуркації основи западин.

Контрольна точка закінчення гребеня, визначена через точку біфуркації основи западин, відповідає трьом лініям западин, що зустрічаються в одній точці. При цьому дві западини утворюють гострий кут, а дотична до третьої западині, протилежної лінії гребеня, визначає напрямок біфуркації западини. Напрямок контрольної точки слід вимірювати як значення кута між зазначеної дотичній та горизонтальною віссю, орієнтованої вправо (рис. 4).

Орієнтація контрольної точки біфуркації гребеня, визначеної через точку біфуркації основи гребеня.

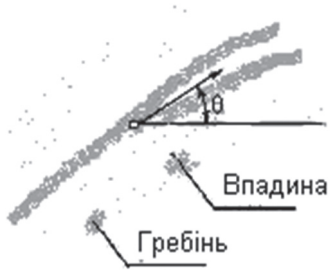

Рис. 4. Розташування і орієнтація контрольної точки закінчення гребеня певної через точку біфуркацій основи западин

Контрольна точка біфуркації гребеня, визначена через точку біфуркації основи гребеня, яка відповідає трьом лініям гребенів, зустрічається в одній точці. При цьому два гребені утворюють гострий кут, а дотична до третього гребеню, протилежному западині, визначає напрямок біфуркації гребня. Напрямок контрольної точки слід вимірювати як значення кута між вказаною дотичної та горизонтальною віссю, орієнтованої вправо.

Напрямок контрольної точки завершення основи гребенів слід вимірювати як значення кута, утвореного дотичній до закінчення гребеня і горизонтальною віссю, орієнтованої вправо. Точку закінчення основи гребенів використовують тільки в одному з двох варіантів форматів, використовуваних в ідентифікаційних картах, в інших варіантах формату використовують точки закінчення гребеня і біфуркації гребеня.

Ядро і дельта є інформативними точками відбитка пальця. Відбиток пальця може не мати або мати одну або більше дельт, а також мати одну чи більше ядер. Цей стандарт встановлює наступні правил визначення розташування та орієнтації ядра і дельти.

Розташування ядра: якщо на зображенні відбитка пальця присутній контрольна точка закінчення гребеня поблизу самого внутрішнього загину гребеня, то розташування ядра визначають за розташуванням контрольної точки закінчення гребеня, найбільш близькою до гребньовій лінії, що має максимальну кривизну. Якщо ядро має вигляд перевернутої букви «U» без найближчих контрольних точок закінчення гребеня, то розташування ядра визначають за розташуванням відповідної контрольної точки закінчення впадини.

Орієнтація ядра: якщо ядро характеризується вираженим напрямком, то значення кута цього напрямку повинно бути записане в полі «Орієнтація ядра», що входить в структуру формату запису контрольних точок. Орієнтацію ядра визначають за значенням кута дотичній до гребневих лініях, розташованим поблизу ядра: напрям дотичній слід визначати з відкритої сторони опуклого гребеня.

Розташування дельти: для визначення розташування дельти необхідно встановити три додаткові точки, кожна з яких розташована між двома сусідніми гребенями в області розбіжності гребенів: тобто в області, в якій паралельні або майже паралельні гребневі лінії розходяться при наближенні до дельті. Розташування дельти визначають як центр мас цих трьох точок.

Орієнтація дельти: для всіх розбіжностей гребеневих ліній визначають кут нахилу дотичної до гребенів в точці, розташованої до розбіжності ліній гребенів. Кут вимірюють від точки розбіжності паралельних гребенів у напрямку від дельти. Розташування ядра і дельти наведено на рис. 5.

Рис. 5. Приклад розташування ядра і дельти

Після створення цифрового біометричного образу за допомогою сканерів, зберігання їх

у базі суттєво зменшує стійкість від атаки зловмисника. Отже образ зберігається в системі до того часу поки не будуть зроблені наступні дії, а саме обчислення біометричних параметрів з пред'явленого образу.

3. АНАЛІЗ МЕТОДІВ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ ЗА ГОЛОСОМ

Системи голосової біометрії не вимагають дорогої апаратної підтримки, універсальність полягає в можливості використання як при безпосередньому контакті з реєструючої апаратурою, так і при віддаленому доступі, наприклад, по каналах телефонних дротових або мобільних ліній. Це дає можливість легко адаптувати системи автентифікації на основі голосової біометрії до різних умов використання і сферам застосування. Тому голосова біометрія є перспективним методом верифікації особистості як з точки зору надійності, так і з точки зору широти областей застосування.

Для обчислення біометричного образу за голосом були проаналізовані декілька перспективних методів розроблених провідними компаніями.

Voice Key Service – система голосової біометричної автентифікації, розроблена російською компанією «Центр мовних технологій» (ЦРТ). Технологія Voice Key використовує унікальні характеристики фізіологічної будови мовного тракту кожної людини. В її основі лежить запатентований компанією ЦРТ алгоритм, який використовує спектрально-формантний метод виділення і порівняння біометричних ознак.

Переваги цієї системи полягають у тому, що дана система має:

– два рівня захисту (порівняння біометричних даних + перевірка пароля);

– верифікація у телефонному каналі;

– можливість працювати в зашумлених умовах;

– незалежність від національної мови або діалекту.

Недоліком є те, що система не володіє можливістю встановлення параметрів для кожної програми.

SPIRIT SV-система – система автентифікації, розроблена російською компанією SPIRIT Corp. Ця система здатні працювати в різних додатках: від автентифікації диктора для локальних систем безпеки до віддаленої автентифікації по телефону, що може бути застосовано, наприклад, для банківських служб та електронної комерції. Конкретне рішення може бути зроблено SPIRIT Corp., Включаючи портінг системи на задану платформу та забезпечення телекомунікаційної підтримки.

Переваги даної системи:

– можливість автентифікації в телефонному каналі;

– можливість працювати в зашумлених умовах;

– незалежність відмов і словників;

– здатна працювати у текстозалежному режимі і в режимі підказок.

Недоліком даної системи є те, що для надійної роботи вимагає обмеження на 10-15 користувачів, що не підходить для використання в умовах більшої чисельності користувачів системи доступу, відсутня можливість додаткової автентифікації (перевірки введеного немовного пароля, наприклад, з клавіатури) для збільшення рівня надійності , система не володіє можливістю встановлення параметрів для кожної програми [6].

Speech Secure – система ідентифікації голосу, розроблена американською компанії Nuance Technology. Спочатку в процесі реєстрації, система за спеціальними алгоритмами, створює модель голосу, використовуючи унікальні характеристики голосу того, хто телефонує. Система зберігає моделі голосу (опис структури голосу і особливостей голосового тракту) як частину профілю абонента. Під час автентифікації (ідентифікації) ці моделі використовуються для визначення ступеня відповідності голосу того, хто телефонує голосам записаних раніше людей. На основі цієї інформації система приймає рішення щодо проведення операції. Система доступна через веб-інтерфейс.

Повна версія включає: машину автентифікації, біометричне додаток ідентифікує людину за унікальною голосової моделі, сервер, веб-сервіси для використання з будь голосової платформою з управлінням базою даних голосових моделей.

Переваги:

– легко інтегрується в систему будь-якої архітектури;

– можливість працювати в зашумлених умовах;

– зменшує ймовірність фальсифікацій і шахрайства при використанні бази даних підозрілих голосів і перемиканні підозрілих абонентів на службу безпеки.

Недолік – володіє надлишком функцій, внаслідок чого має складну настройку.

Більшість сучасних систем зосереджують зусилля на добуванні частотної характеристики мовного тракту людини, відкидаючи при цьому характеристики сигналу збудження [7]. Для відділення сигналу збудження від сигналу мовного тракту вдаються до кепстрального аналізу. Схематично цей метод представлений на рис. 6.

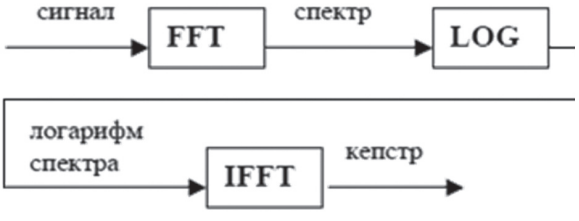

Рис. 6. Загальна схема кепстрального аналізу сигналу (FFT – блок швидкого перетворення Фур'є сигналу, LOG – блок логарифмування спектру, IFFT – блок зворотного швидкого перетворення Фур'є)

Одним із потужних методів, заснованим на кепстральному аналізі сигналу, відноситься метод кепстральних коефіцієнтів лінійного передбачення (LPCC). Перші два етапи цифрової обробки полягають у попередньому посиленні(pre-emphasis) та сегментації на фрейми.

На першому етапі до сигналу застосовується фільтр нескінченною імпульсною характеристики виду:

$$H_{pre}(z) = 1 + a_{pre} z^{-1}. \quad (1)$$

Даний фільтр дозволяє «підсилити» високочастотну область спектра сигналу. Це необхідно потрібно для вирівнювання спектра, тому що вокалізовані ділянки мови характеризуються різко спадаючим спектром. І людиною краще сприймаються частоти вище 1кГц. Значення коефіцієнта зазвичай apre вибирається з проміжку [–1.0, –0.4].

На другому етапі мовної сигнал розбивається в часі на короткі проміжки (фрейми), в яких проводиться кепстральний аналіз. Зазвичай тривалість кадру становить від 20 мс до 40 мс. Вважається, що на цих ділянках мовної сигнал можна вважати квазістаціонарним. До фрейму застосовується віконна функція Хеммінга:

$$\omega(n) = 0.54 - 0.46\cos(\frac{2\pi n}{N}). \quad (2)$$

Алгоритм LPCC починається з обчислення p коефіцієнтів $\{a_k\}^p_k$ авторегресійної моделі для кожного фрейма на основі моделі $\hat{S}$:

$$\hat{S}(z) = \frac{A}{1 - \sum_{k=1}^{p} a_k z^{-k}}. \quad (3)$$

Після того, як усі параметри моделі знайдені, обчислюються кепстральних LPCC-коефіцієнти по рекурсивної функції:

$$c(n) = \begin{cases} 0, n < 0 \\ \log_{\varepsilon}(A), n = 0 \\ a_n + \sum_{k=1}^{n-1} (\frac{k}{n}) c(k) a_{n-k}, 0 < n < p \\ \sum_{k=n-p}^{n-1} (\frac{k}{n}) c(k) a_{n-k}, n > p \end{cases} \quad (4)$$

На основі кінцевого числа коефіцієнтів лінійного передбачення може бути отримано нескінченне число LPCC-коефіцієнтів. Встановлено, що 12-20 коефіцієнтів достатньо для формування оптимального для даного методу вектора ознак. Таким чином, отримавши кепстральні коефіцієнти, які необхідно запам'ятати і використовувати для порівняння в процедурі автентифікації.

Також до потужних методів, заснованих на кепстральному аналізі сигналу, відносяться: метод коефіцієнтів перцептивного лінійного передбачення (PLP) і робасних PLP (PLP-RASTA).

4. ВИЯВЛЕННЯ ЛОКАЛЬНИХ ОСОБЛИВОСТЕЙ БІОМЕТРИЧНИХ ОБРАЗІВ НА ОСНОВІ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ

Для проведення автентифікації по біометричному образу, головною задачею є виділення факторів або так названих локальних особливостей зображень, що унікально характеризували би образ користувача.

Одним з найбільш поширених і ефективних методів знаходження таких факторів є метод головних компонент або компонентний аналіз, що знайшов широке застосування у задачах стиснення даних, розпізнавання образів, кодування, обробки зображень, спектрального аналізу і відомий також в теорії розпізнавання образів як перетворення Карунена-Лоева [8, 9].

Однак якщо обробка даних повинна проводитися у реальному часі, на перший план виходять нейромережеві технології, серед яких слід відмітити правило самонавчання та нейрон Е. Оя. На рис. 7 наведено структуру нейрона Оя [10, 11].

За допомогою правила Оя у вигляді [12]:

$$\begin{cases} w_1(k+1) = w_1(k) + \eta(k) y_1(k)(\tilde{x}(k) - w_1(k) y_1(k)), \\ y_1(k) = w_1^T(k)\tilde{x}(k), \; w_1(0) \neq 0 \end{cases} \quad (5)$$

може бути виділено першу головну компоненту, що забезпечує мінімум критерію

$$E_1^k = \frac{1}{k}\sum_{p=1}^{k} (w_1^T \tilde{x}(p))^2. \quad (6).$$

Далі, як і в процедурі стандартного аналізу головних компонент, з кожного вектора $\tilde{x}(k), k = 1,2,\ldots,N$ віднімається його проекція на першу головну компоненту і обчислюється перша головна компонента різниць, що є другою головною компонентою вихідних даних і ортонормальною першій. Третя головна компонента обчислюється шляхом проекції кожного вихідного вектора $\tilde{x}(k)$ на перші дві компоненти, віднімання цієї проекції з $\tilde{x}(k)$ і находження першої головної компоненти різниць, що є третьою головною компонентою первинного масиву даних. Головні компоненти, що залишилися, обчислюються рекурсивно згідно з описаної стратегії.

Таким чином розглянутий метод дозволяє виділити локальні особливості з біометричного образу, занести його в базу даних як еталонний, та використовувати при автентифікації користувача. Такий метод в значній мірі спрощує та підвищує надійність автентифікації користувачів та дозволяє проводити обробку зображення у реальному часі.

ВИСНОВКИ

У статі проведено аналіз проблемних питань систем автентифікації користувачів. Основною метою аналізу є визначення перспективної моделі біометричної автентифікації та ідентифікації особи для впровадження та застосування в Україні. Розглянуто метод виявлення локальних

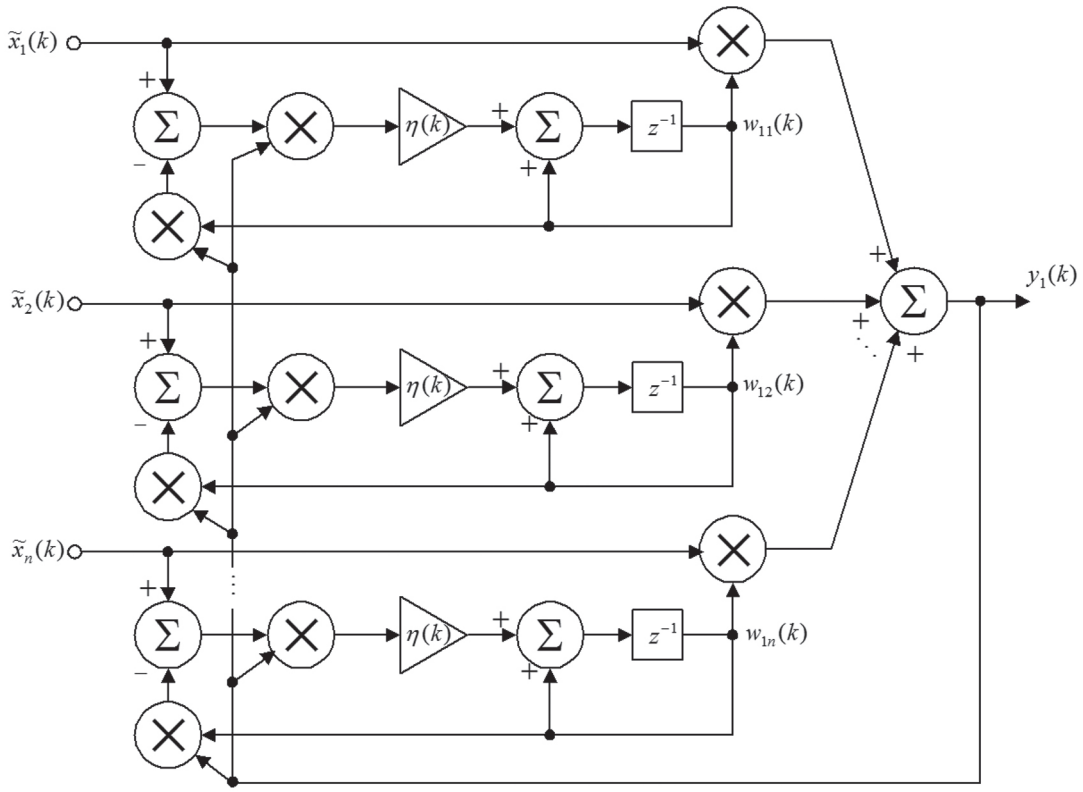

Рис. 7. Нейрон Оя

особливостей біометричних образів за допомогою гібридних штучних нейронних мереж.

Література

[1] *Зубов, Г.Н.* Состояние и перспективы голосовой биометрии [Электронный ресурс] / Г.Н. Зубов, М.В.Хитров // 2007: http://www.chip-news.ru/archive/chipnews/200710/Article_12.pdf

[2] Biometric Standards Activity. [Електронний ресурс] Точка доступу: http://www.biometrics.org/ standards.php.

[3] ANS X9.84:2000. Biometrics Information Management and Security For The Financial Services Industry

[4] Characteristics of biometric systems. Точка доступу: http://www.ccert.edu.cn/education/cissp/ hism/039-041.html

[5] ISO/IEC 19794-2. Finger Minutiae Data.

[6] *Шарий, Т.В.* О проблеме параметризации речевого сигнала в современных системах распознавания речи / Т.В Шарий // Журн. Вісник Донецького національного університету. – 2008. - Сер. А: Природничі науки. - 2. – С. 10-15.

[7] *Doddington, G.R.* Speaker recognition - Identifying people by their voices / G. R. Doddington // Proc. IEEE. – 1985. – 73. – P. 1651-1664.

[8] *Фукунага К.* Введение в статистическую теорию распознавания образов / Фукунага К. – М.: Наука,1979. – 368 с.

[9] *Патрик Э. А.* Основы теории распознавания образов / Патрик Э. А. – М.: Сов. радио, 1980. – 408 с.

[10] *Oja E.* A simplified neuron model as a principal component analyzer / Oja E. // J. of Math. Biology. – 1982. – 15. – P. 267-273.

[11] *Oja E.* Neural networks, principal components, and subspaces / Oja E. // Int. J. of Neural Systems. – 1989. – 1. – P. 61-68.

[12] *Бодянский Е.В.* Искусственные нейронные сети: архитектуры, обучение, применения / Бодянский Е.В., Руденко О.Г. - Харьков: ТЕЛЕТЕХ, 2004. – 369 с.

Поступила в редколлегию 27.04.2012

Філоненко Павло Олександрович, магістрант групи БДІРм-11-1 ХНУРЕ. Область наукових інтересів: дослідження механізмів систем біометричної автентифікації, інформаційні технології.

Барсуков Євген Ігорович, магістрант групи БІКСм-11-1 ХНУРЕ. Область наукових інтересів: дослідження засобів контролю доступу за допомогою біометричних систем по речовому сигналу.

Винокурова Олена Анатоліївна, фото та відомості про автора див. на с. 254.

УДК 343.982.3, 004.89, 004.032.26

Анализ биометрических интеллектуальных методов аутентификации и идентификации личности по отпечаткам пальцев и по голосу для защиты от несанкционированного доступа / П. А. Филоненко, Е. И. Барсуков, Е. А. Винокурова // Прикладная радиоэлектроника: науч.-техн. журнал. – 2012. – Том 11. № 2. – С. 267–274.

В статье приводятся результаты анализа проблемных вопросов систем аутентификации личности. Основной целью анализа является определение перспективной модели биометрической аутентификации и идентификации личности для внедрения и применения в Украине. К основным задачам относятся анализ существующих методов биометрической аутентификации и идентификации личности по отпечаткам пальцев и по голосу для повышения устойчивости от угроз в сфере информационной безопасности. Рассмотрено метод выявления локальных особенностей биометрических образов с помощью гибридных искусственные нейронных сетей.

Ключевые слова: биометрия, аутентификация, гибридные интеллектуальные методы, искусственные нейронные сети.

Рис. 7. Библиогр.: 12 наим.

UDC 343.982.3, 004.89, 004.032.26

Analysis of biometric person authentication and identification intelligent methods by fingerprints and voice for protection from unauthorized access / P.O. Filonenko, E. I. Barsukov, O. A. Vynokurova // Applied Radio Electronics: Sci. Journ. – 2012. Vol. 11. № 2. – P. 267–274.

The paper presents the results of analyzing problems of systems of person authentication. The main purpose of the analysis is to identify promising models of biometric person authentication and identification for introducing and using in Ukraine. The main tasks include analysis of existing methods of biometric authentication and identification by fingerprints and a voice to enhance the stability to threats in information security. The local feature detection method for biometric patterns based on hybrid artificial neural networks is considered.

Keyword: biometrics, authentication, hybrid intelligent methods, artificial neural networks.

Fig.: 07. Ref.: 12 items.