УДК 343.982.3, 004.89

П.О. ФІЛОНЕНКО, О.А. ВИНОКУРОВА

АНАЛІЗ БІОМЕТРИЧНИХ СИСТЕМ АВТЕНТИФІКАЦІЇ ТА ІДЕНТИФІКАЦІЇ З ВИКОРИСТАННЯМ ГІБРИДНИХ ІНТЕЛЕКТУАЛЬНИХ МЕТОДІВ ДЛЯ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Вступ

На сьогодні у розвинених країнах світу, таких як США, Російська Федерація та країни ЄС, існує актуальний напрямок – впровадження біометрії в криптографію. На сучасному етапі виникло два основних методи застосування біометрики: автентифікація особи та криптографія. Традиційним напрямом є використання біометрики для автентифікації, який має велику історію вивчення та застосування (наприклад, в системах контролю та доступу до приміщень та джерел інформації з розмежуванням рівня гарантії).

Застосування біометричних методів (наприклад, для забезпечення секретності та автентифікації інформації) в криптографії має свої особливості. Стійкість методів базується на припущенні, що секретний ключ відомий тільки власнику, і задача збереження секретності ключа є основною задачею в криптосистемі.

Біометричні методи автентифікації особи мають деяку перевагу по відношенню до традиційних:

біометричні шаблони дуже важко фальсифікувати;

в силу унікальності біометричних характеристик достовірність автентифікації за біометричними даними дуже висока;

біометричні ідентифікатори не можна забути або загубити, як пароль чи картку;

біометрична автентифікація потребує наявності власника біометричних характеристик.

Суттєвий поштовх розвитку біометричних технологій дала програма створення паспортно-візових документів нового покоління. На даний момент у міжнародній організації з стандартизації ISO/IEC, комітету JTC1 (Information Technology), підкомітету SC37 (Biometrics) налічується за цією програмою 108 міжнародних біометричних стандартів і проектів, з яких 55 прийнятих та 53 стандарти перебувають у стадії обговорення і розробки [1]. Що дає можливість вивчати цей напрямок та впроваджувати в системи захисту інформації.

Огляд схем процедур біометричної ідентифікації

При дослідженні стандартів підкомітету SC37 було виявлено що для проходження автентифікації особи використовуються класичні схеми перетворення. Одну з таких схем наведено на рис. 1, *а*.

Для реалізації подібних технологій необхідно мати біометричний шаблон (блок 3. рис. 1 ,*а*), що відображає інформаційну частину біометричного образу.

З приведеної схеми випливає, що вона є вкрай вразливою. Для реалізації успішної атаки на біометричний захист достатньо:

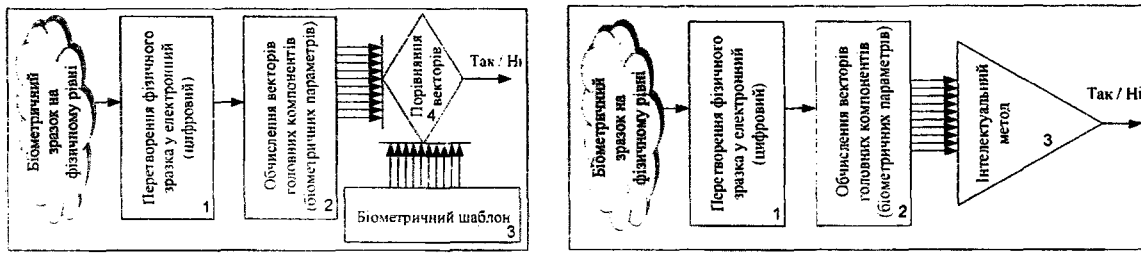
- підмінити біометричний шаблон;
- скомпрометувати біометричний шаблон для виготовлення електронного або фізичного муляжу біометричного образу «Свій».

Також потребує створення захищеної бази зберігання біометричних шаблонів що призводить до додаткових витрат на ресурси.

Одним із шляхів вирішення завдання захисту біометричного шаблону є деяке змінення класичної схеми, а саме заміни зберігання біометричних шаблонів для порівняння на систему з використанням гібридних інтелектуальних систем (рис. 1, *б*).

Як видно з рис. 1, *б*, біометричний шаблон при ідентифікації з використанням інтелектуальних систем відсутній як такий. Замість цього використовуються у порівнянні зв'язки та

вагові коефіцієнти. Таким чином, при використанні схеми, представленої на рис. 1, *б*, виключається атака зловмисникам на підміну чи компрометацію біометричного шаблону.



а *б*

Рис. 1

При створенні інтелектуальної системи США та Російська Федерація намагаються вирішувати цю задачу з різних боків, пропонуючи два різних технічних підходи, які направлені на вирішення складностей використання біометричних даних.

Перший оснований на використанні багатошарових штучних нейронних мереж, що автоматично навчаються модифікувати біометричний образ особи в його секретний ключ [2]. При використанні нейромережевих технологій основною проблемою є навчання багатошарових штучних нейронних мереж. Коли багатошарова нейронна мережа має небагато параметрів, що повинні настроюватися, то можуть бути використані відомі алгоритми навчання, але зі збільшенням параметрів розмірності нейронних мереж зростає і складність задачі навчання. Вирішення проблеми алгоритмів навчання дозволило б вирішити складності використання біометричних даних: нерівномірність інформаційного розподілу, шляхом збагачування даних за допомогою нейромережевого перетворювача.

Друга технологія при генерації ключа з біометричних параметрів використовується метод «нечітких екстракторів» [3]. Відкритий та відповідний йому секретний ключі створюються за допомогою ключа з біометричних параметрів.

Підходи істотно відрізняються. Перша технологія дозволяє отримувати сильні ключі від спеціальних генераторів випадкових чисел. Fuzzy-технологія близька до нейромережевої, але вона не припускає навчання. Fuzzy-логіка проектується однократно, та далі Fuzzy-правила не змінюються.

Біометрична характеристика людини та системи перетворення фізичного образу в цифровий

На даний момент з основних приведених біометричних характеристик людини (райдужна оболонка ока, дактилоскопія, геометрія обличчя та інші) системи розпізнавання по відбитках пальців займає більш половини біометричного ринку. Безліч російських і закордонних компаній займаються виробництвом систем управління доступом, заснованих на методі дактилоскопічної ідентифікації. Внаслідок того, що цей напрям є одним з най давнішніх, він набув найбільшого поширення.

У даному розділі розглядаються порівняльні характеристики статичного біометричного методу. Як порівняльні характеристики, використані наступні показники: FRR при фіксованому значенні FAR [4]. Основними характеристиками будь-якої біометричної охоронної системи є два числа – FAR (False Acceptance Rate) і FRR (False Rejection Rate). Перше число характеризує ймовірність помилкового збігу біометричних характеристик двох людей. Друге – ймовірність відмови доступу людині, що має допуск. Система тим краще, чим менше значення FRR при однакових значеннях FAR.

Як джерело даних по FAR і FRR використовувалися статистичні дані Verifinger SDK, отримані за допомогою сканера відбитків пальців DP U.are.U (табл. 1).

Характерне значення FAR для методу розпізнавання відбитків пальців – 0,001%.

Таблиця 1

False Acceptance Rate	False Rejection Rate
0,1%	0,3%
0,01%	0,4%
0,001%	0,6%
0,0001%	0,9%

Вірогідність помилкового збігу отриманого сканером відбитку пальця для бази даних з N відбитків дорівнює *FAR·N*. Щодня через пункт контролю доступу проходить теж порядку N чоловік. Тоді вірогідність помилки за робочий день *FAR·N2*. Звичайно, залежно від цілей системи ідентифікації вірогідність помилки за одиницю часу може сильно варіюватися, але якщо прийняти допустимим одну помилку протягом робочого дня, то:

$$FAR \cdot N2 \approx 1 \tag{1}$$

$$N \approx \frac{1}{FAR} \tag{2}$$

Тоді отримаємо, що стабільна робота системи ідентифікації при FAR = 0,001% можлива при чисельності персоналу N, що приблизно рівний 300.

Переваги:

- висока достовірність,
- низька вартість пристроїв сканування,
- достатня простота процедури сканування відбитку.

Недоліки:

- папілярний узор відбитку пальця дуже легко ушкоджується дрібними подряпинами, порізами,
- недостатня захищеність від підробки зображення відбитку, частково викликана широким розповсюдженням методу.

Для перетворення фізичного образу в цифровий використовуються сканери. На сьогоднішній день їх існує дуже багато. Вони відрізняються по ймовірності несанкціонованого доступу, часу ідентифікації (пропускна здатність) та ймовірності помилкової тривоги (див. табл. 2).

Таблиця 2

Модель (фірма)	Ймовірність несанкціонованого доступу, %	Ймовірність помилкової тривоги, %	Час ідентифікації (пропускна здатність), *с*
FingerScan (Identix)	0,0001	1,0	0,5
TouchSafe (Identix)	0,001	2,0	1
TouchNet (Identix)	0,001	1,0	3
Startek	0,0001	1,0	1
U.are.U (Digital Persona)	0,01	3,0	1
FIU(Sony, I/O Software)	0,1	1,0	0,3
BioMause (ABC)	0,2	-	1
Кордон (Росія)	0,0001	1,0	1
DS-100 (Росія)	0,001	-	1…3
Veriprint 2100 (Biometric ID)	0,001	0,01	1

Сучасні системи сканування оснащені різними датчиками (температури, сили натиснення і т. п.), які підвищують ступінь захисту від підробок. З кожним днем системи стають все

більш зручними і компактними. Більшість компаній виробляють готові системи, які оснащені усім необхідним, включаючи програмне забезпечення. Інтеграторам в цій області просто немає необхідності збирати систему самостійно, оскільки це невигідно і займе більше часу і сил, чим купити готову і вже недорогу при цьому систему, тим більш вибір буде дійсно широкий.

Алгоритми обчислення біометричного образу

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.

Для обчислення біометричного образу було проаналізовано два існуючих алгоритми: алгоритм Precise BioMatch та алгоритм, запропонований Російсько-Вірменським (Слов'янським) державним університетом.

Алгоритм Precise BioMatch [5] 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 вірної 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). Значить, користувач може зареєструвати відбитки на одному типі датчика, а проходити перевірку на іншому. Це надзвичайно важливо у випадках, коли біометричне розпізнавання використовується на великому, неконтрольованому просторі.

Метод виявлення ключових точок.

Відбиток пальця складається з певної кількості борозен і смужок. Смуги – це підняті частини шкірного покриву, борозни – запалі частини. Смуги складають так звані ключові точки: краї смуг (там, де смуги закінчуються) і роздвоєння – там, де вони розгалужуються [6].

Під час реєстрації ключові точки розташовуються у визначеному місці (рис. 2), а їх розташування один до одного та їх напрям – реєструються. На основі цих даних створюється зразок (шаблон) – інформація, яка згодом буде використана для посвідчення особи користувача.

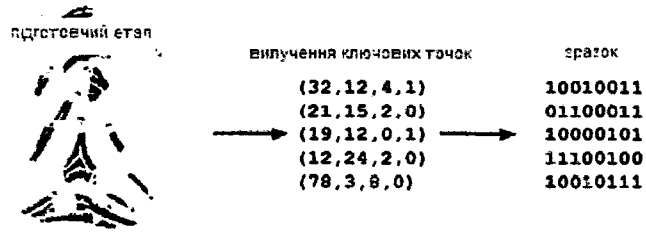


Рис. 2

На етапі зіставлення (рис. 3) лічене зображення відбитка пальця піддається попередній обробці, в ході якої витягуються ключові точки. Вони зіставляються із зареєстрованим зразком, необхідно розташувати в певному місці як можна більшу кількість схожих точок у межах заданих меж. Результатом співставлення, як правило, є набір ключових точок. Потім використовується поріг, що визначає, наскільки великим повинне бути це число, щоб було можливо зіставити відбиток пальця зі зразком.

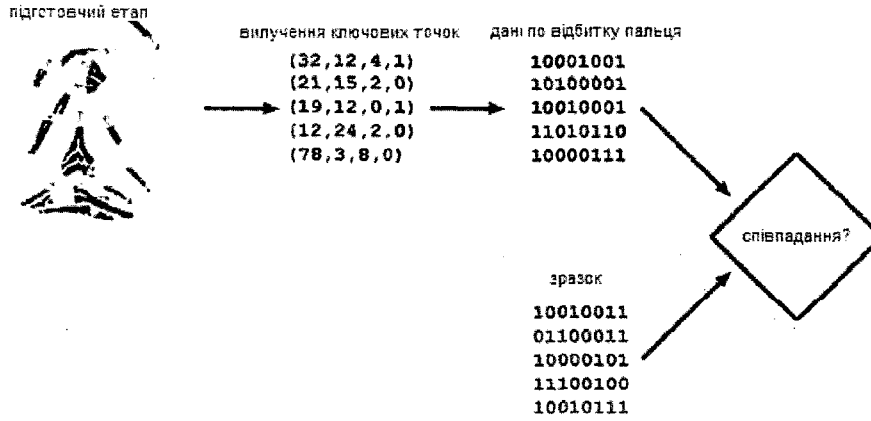


Рис. 3

Переваги:

– використовується в застосуваннях AFIS (Automated Fingerprint Identification System);

– широко відомий, добре досліджений метод;

– алгоритм підходить для множинного зіставлення.

Недоліки:

– так як метод висуває великі вимоги до дозволу і розмірів чутливого датчика, він може бути використаний не у всіх технологіях, що зчитують відбитки пальців. При використанні сканерів, менш досконалих, ніж апаратура AFIS-класу, дає низькі результати;

– люди, які не мають зовсім або мають невелику кількість ключових точок (особливий стан шкірного покриву), не можуть користуватися цією системою. Кількість ключових точок може бути обмежуючим фактором для безпеки алгоритму;

– можливі збої в системі через хибні ключових точок (ділянка, що містить помилку, що виникла із-за низької якості реєстрації, відтворення зображення або нечіткого відбитку смуг).

Метод зіставлення візерунків.

Важливою властивістю алгоритму зіставлення візерунків є те, що до уваги беруться не лише окремо взяті крапки, але і більш охоплюючі характеристики відбитка пальця. Ці характеристики можуть також включати певний відсоток додаткових даних, включаючи товщину смуг, їх кривизну або щільність. У зв'язку з цим збільшенням кількості даних, алгоритм, заснований на зіставленні візерунків, менше залежить від величини сканера і абсолютно не залежить від кількості ключових точок у відбитку пальця. Заснований на зіставленні візерунків, алгоритм, на відміну від методу виділення ключових точок, не зустрічає труднощів при розпізнаванні пальця з відбитком гіршої якості [7].

Алгоритм зіставлення візерунків Precise Biometrics під час реєстрації відбитка визначає наявність вищезазначених додаткових характеристик. Невеликі ділянки відбитка і відстань між ними беруться з загальної картини (рис. 4) з метою максимально збільшити кількість унікальної інформації. Найбільш значимі ділянки навколо ключових точок і ділянки з невеликим радіусом згину. Основна структура та унікальні комбінації смуг також є цінними даними.

Процес підтвердження (рис. 5) починається з попередньої обробки зчитаного зображення відбитка. Зареєстровані візерунки, що зберігаються у зразку, зіставляються з зображенням відбитка,що перевіряється, щоб визначити, наскільки зразок збігається із зображенням. Поріг, що описує найменше припустиме відхилення згодом використовується при визначенні ступеня відповідності відбитка наявному зразку.

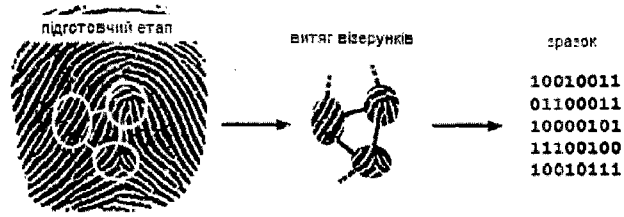


Рис. 4

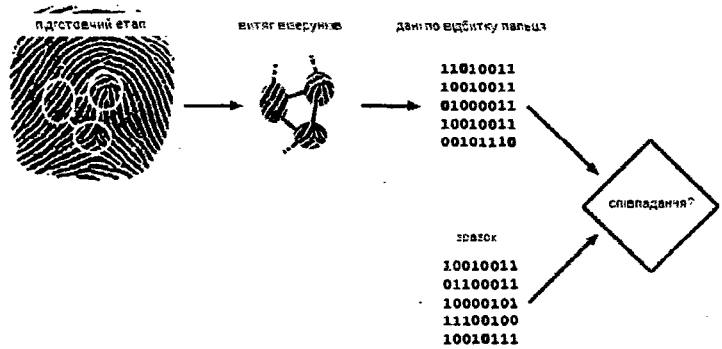


Рис. 5

Переваги:

– прекрасно працює з усіма відомими типами сканерів відбитків пальців;

– будь-який відбиток, який можна записати, може бути зареєстрований, навіть якщо він не має або має невелику кількість ключових точок;

– чудово підходить для здійснення роботи з недостатньою кількістю обчислювальних ресурсів, наприклад смарт-картою.

Недоліки:

– не може використовувати базу даних AFIS (проте, може використовувати необроблені зображення);

– не оптимізований для ідентифікації (тобто для встановлення конкретної особистості, для схеми «один до багатьох »).

Чисті алгоритми зіставлення візерунків і алгоритми, що покладаються тільки на зіставлення ключових точок, не можуть задовольнити всім вимогам. Наприклад, чистий алгоритм виділення ключових точок пред'являє дуже великі вимоги до розмірів пристрою, що зчитує, а, отже, дає погані результати при невеликому розмірі сканера або наявності у користувача невеликої кількості ключових точок. З іншого боку, чистий метод зіставлення візерунків не може працювати зі стандартизованими ключовими точками. Об'єднуючи сильні сторони обох методів, рішення Precise BioMatch пропонує розробникам і кінцевим користувачам кращі технології з обох методик і забезпечує високофункціональні і гнучкі рішення, які враховують найрізноманітніші вимоги до захисту.

Алгоритм Російсько-Вірменського державного університету дещо різниться від Precise BioMatch. Він складається з трьох етапів для класичної схеми процедур біометричної ідентифікації та достатньо двох для використання у схемі процедур біометричної ідентифікації з використанням інтелектуальних систем.

Опис методу

Задача ідентифікації особи по відбитку пальця вирішується шляхом зіставлення ідентифікованого відбитка з еталонними. Коефіцієнт (відсоток) відповідності обчислюється за формулою

$$K = S/\min(p,q)\cdot 100\%, \qquad (3)$$

де S – кількість мінуцій, що співпали, p – кількість мінуцій в еталоном відбитку, q – кількість мінуцій в ідентифікованому відбитку. Відбитки вважаються ідентичними, якщо коефіцієнт відповідності становить 65 % і вище (цей поріг можна змінити).

Метод вирішення даної задачі складається з трьох основних етапів: обробка вихідного зображення, виділення мінуцій і зіставлення мінуцій відбитків пальців.

Для докладного опису методу введемо такі позначення: I – матриця вихідного зображення. Розмірність матриці визначається розміром зображення в пікселях. Елементи матриці – натуральні числа від 0 до 255 (колір пікселя).

Множина W(u,v,n)={(i,j) | |i-u|<n, |j-v|<n} матриці є свого роду віном точки (i,j) розміром n. Вектори P(i,j)=((i-u),(j-v)) и d(i,j)=P(i,j)/|P(i,j)| визначаються для будь-якої точки кожного вікна.

Обробка вихідного зображення.

Як правило, вихідне зображення відбитка (якщо воно не отримано електронним способом [8], має погану якість (пошкоджені лінії, мають різні спотворення і т.д.

Для достовірного визначення мінуцій необхідно обробити зображення і привести до особливого виду (формату). Процес обробки зображення здійснюється наступним чином:

- обчислення орієнтації ліній,
- поліпшення якості ліній,
- бінаризація зображення,
- потоншення ліній зображення.

Обчислення орієнтації ліній.

Для обчислення орієнтації ліній вибираються точки (u,v) ∈ I, розглядаються вікна W (u,v,n), де n залежить від розмірності матриці, визначається вектор, перпендикулярний до прямої, якій належить вибрана точка,і визначаються суми:

$$S_1 = \sum_{(i,j)\in W} g_1(u,v,i,j) \tag{4}$$

$$S_2 = \sum_{(i,j)\in W} g_2(u,v,i,j) \tag{5}$$

$$g_1(u,v,i,j) = \begin{cases} 0, |I(u,v) - I(i,j)| < T, \\ d(i,j), |I(u,v) - I(i,j)|, d_y(i,j) \geq 0, \\ -d(i,j), |I(u,v) - I(i,j)|, d_y(i,j) < 0, \end{cases} \tag{6}$$

$$g_2(u,v,i,j) = \begin{cases} 0, |I(u,v) - I(i,j)| < T, \\ d(i,j), |I(u,v) - I(i,j)|, d_x(i,j) \geq 0, \\ -d(i,j), |I(u,v) - I(i,j)|, d_x(i,j) < 0, \end{cases} \tag{7}$$

де T – постійна величина (на прикладі T = 60), а вектор d (i,j) було визначено вище.

Використовуючи ці формули, для всіх точок (u,v) ∈ I визначається вектор D (u,v):

$$D(u,v) = \begin{cases} \frac{S_1}{|S_1|}, |S_1| > |S_2|, \\ \frac{S_2}{|S_2|}, |S_2| > |S_1|. \end{cases} \tag{8}$$

Цей процес повторюється 5 разів (число 5 вибрано за результатами експериментів). Після першого застосування алгоритму деякі вектори виходять нульовими. При наступних застосуваннях алгоритму якість зображення поліпшується і, отже, кількість нульових векторів зменшується.

Для уточнення напрямків отриманих векторів розглядаються вікна W (u,v,n) для всіх точок (u, v) ∈ I. Використовуючи нульовий вектор D (i, r), для усіх векторів D (i, j) визначають

кут між векторами D (i,r) і D (i,j). Якщо цей кут тупий, то D (i, r) = D (i, r) – D (i, j), у противному випадку D (i,r) = D (i,r) + D (i,j). Обчислюється вектор D (u,v) = D (i,r) / | D (i,r) | для всіх точок вікна W (u,v,n). Цей процес також повторюється 5 разів.

Поліпшення якості ліній.

Використовуючи вектори D (u,v), отримані вище, і середню вагу вікон W (u,v,n), можна поліпшити якість ліній, замінюючи значення всіх елементів матриці на середню вагу їх вікон. У якості ваги береться модуль sinα, де α – кут між векторами D (u,v) і d (i,j), (i,j) $\in$ W. Середня вага вікна обчислюється за формулою

$$I(u,v) = \frac{S(u,v)}{Q(u,v)}, \tag{9}$$

де

$$S(u,v) = \sum_{(i,j)\in W} I(i,j) \,|\sin\alpha|, \tag{10}$$

$$Q(u,v) = \sum_{(i,j)\in W} I(i,j) \,|\sin\alpha|, \tag{11}$$

На етапі виділення мінуцій є зображення відбитків кращої якості з тонкими лініями. Для знаходження мінуцій розглядаються вікна W (u, v, n) для всіх точок (u, v) матриці I (на прикладі n = 2 число n вибирається достатнім – але маленьким, таким, щоб у вікні не виявилися точки чорного кольору з сусідніх ліній).

Вибирається центральна точка вікна і підраховується кількість чорних (ненульових) пікселів, що знаходяться навколо вікна. Піксель в центрі вважається мінуція, якщо він сам ненульовий, і кількість ненульових пікслей навколо вікна – одне (мінуція типу «закінчення») або три (мінуція типу «роздвоєння»). Координати виявлених мінуцій і їх кути орієнтації записуються у вектор M (p), p – кількість мінуцій. Даний підхід дозволяє отримати всі можливі потенційні мінуція. Реальні мінуція визначаються шляхом видалення з множини M (p) сусідніх і крайових точок зображення.

Для видалення сусідніх точок розглядається пара елементів множини M (p). Обчислюється відстань між елементами даної пари. Елементи, відстань між якими менше, ніж задана величина T (на прикладі T = 2), видаляються з безлічі, а в безліч додається середня точка цих елементів. Цей процес виконується для всіх можливих пар елементів множини M (p). У підсумку виходить безліч мінуцій M (r), де r $\leq$p.

На наступному етапі виявляються і видаляються мінуція тих ділянок, які у вихідному зображенні мали погану якість та при поліпшенні якості не відновилися. Видалення цих точок виконується наступним чином: з безлічі M (r) видаляються ті точки (u, v), яким відповідає нульовий вектор D (u, v). Отриману безліч мінуцій позначимо через M (q), де r $\leq$ p. Остаточно безліч реальних мінуцій визначається шляхом видалення крайових точок зображення. З безлічі M (q) видаляються ті точки, відстань яких від краю зображення менше, ніж заздалегідь задана величина T1 (на прикладі T1 = 8). Після завершення цього етапу виходить безліч реальних мінуцій, яка на наступному етапі буде використовуватися для порівняння відбитків пальців.

Алгоритм роботи методу рециркуляційних нейронних мереж

Рециркуляційні нейронні мережі (РНМ) (recirculation neural network) [9] представляють собою багатошарові нейронні мережі, що є аналогом так званих нейронних мереж «bottleneck» [10], які дозволяють вирішувати клас задач по стисненню інформації. Архітектура такої мережі представлено на рис. 6

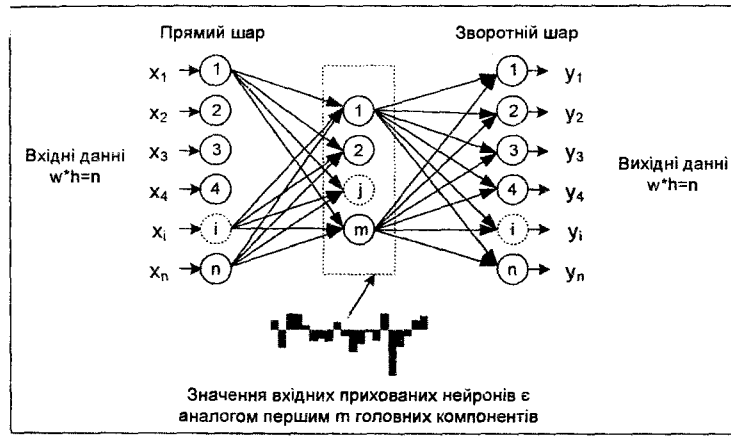


Рис. 6

Обчислення виходів нейронної мережі: $y_{ki} = x_i, k = 0;$

$$y_{ki} = \tanh\left(\sum_{j=1}^{p} y_{k-1,j} w_{kij}\right), k = 1..L, \quad (12$$

де tanh(·) – функція гіперболічного тангенса; k – поточний шар, зростає від 0 до L; p – кількість нейронів у попередньому (k-1) шарі; i – індекс нейрона у поточному шарі; j – індекс нейрона в попередньому шарі; x_i – піксель вхідного зображення; y_{ki} – значення виходів шару k (і вхідні значення наступного шару); w_{kij} – синаптична вага, що з'єднує нейрон j_{k-1} і нейрон i_k; L – індекс останнього шару.

Оскільки мережа ініціалізується випадковими значеннями, відповідності між номерами компонент і нейронами немає. Для реконструкції зображення на вихід нейронів прихованого шару подають обчислені вектори головних компонентів і розраховують значення вихідного шару.

Для навчання мережі застосовується алгоритм корекції синаптичних ваг (зворотне поширення похибки). Для останнього шару обчислюється похибка (різниця між вихідними y_{ki} і еталонними t_i значеннями) і поширюється назад по мережі крізь ваги прихованих нейронів. Величина корекції помилки δ_{ki}:

$$\delta_{ki} = \left(y_{ki} - t_i\right)\left(1 - y_{ki}^2\right), k = L; \quad (13$$

$$\delta_{ki} = \left(\sum_{i=1}^{q} \delta_{k+1,j} w_{k+1,ji}\right)\left(1 - y_{ki}^2\right), k = (L-1)..1, \quad (14$$

де k зменшується від L до 1; q – число нейронів у шарі $k+1$, для РНМ еталоном є вхідні вектори головних компонентів: $t_i = y_{0,i}$.

Подальше коригуються ваги:

$$w_{kij}(t+1) = w_{kij}(t) - \alpha(t)\delta_{ki} y_{k-1,j}, k = 1..L, \quad (15$$

де $\alpha(t)$ – крок навчання; t – дискретний час. Для класичного зворотного поширення швидкість фіксована. Існують евристичні підходи, в яких швидкість змінюється від більшої спочатку до меншої в кінці навчання.

Головна перевага підходу – адаптивний крок, який розраховується індивідуально для кожного шару на кожній ітерації, щоб зробити кращий крок у напрямі мінімізації середньоквадратичної похибки мережі:

$$\alpha(t)=\frac{\sum_{i=1}^{r}\frac{\delta_{ki}^2}{1-y_{ki}^2}}{\left(1+\sum_{j=1}^{p}y_{k-1,j}^2\right)\left(\sum_{i=1}^{r}\delta_{ki}^2\right)}, \qquad (16)$$

де r – число нейронів у шарі k. Слід приймати $\frac{\delta_{ki}^2}{1-y_{ki}^2}=0$ при $1-y_{ki}^2=0$ і $\alpha(t)=0$ при $\sum_{i=1}^{r}\delta_{ki}^2=0$.

Адаптивний крок позбавляє від необхідності вибирати крок вручну, що зменшує вплив людського фактору. Процес навчання сходиться порівняно швидко і стабільно. Для простоти не використовувалося роздільне навчання.

Перед навчанням синаптичні ваги мережі ініціалізуються невеликими випадковими значеннями [-0.01; +0.01].

Навчальний процес складається з послідовності навчальних епох і завершується, коли їх кількість перевищує допустиме значення або помилка нейронної мережі стає менше заданої.

Висновки

У результаті аналізу проблемних питань систем автентифікації осіб були розглянуті можливі моделі біометричної автентифікації у класичному вигляді, які використовуються в біометричних стандартах США, Російської Федерації та країн ЄС щодо підвищення стійкості від загроз в сфері інформаційної безпеки, та з використанням гібридних інтелектуальних методів. Було визначено перспективну модель біометричної автентифікації та ідентифікації особи для впровадження та застосування в Україні.

Список літератури: 1. *Standards* and projects under the direct responsibility of JTC 1/SC 37 Secretariat. Точка доступа: http://www.iso.org/iso/iso_catalogue-/catalogue_tc/catalogue_tc_browse.htm?commid=-313770&published=on 2. *ГОСТ* Р 52633-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации». 3. *Dodis* Y. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data / Dodis Y., Reyzin L., Smith A. // Advances in Cryptology – EUROCRYPT 2004. Christian Cachin and Jan Camenisch, ed. Vol. 3027 of Lecture Notes in Computer Science. Springer – Verlag. – 2004. – P. 79-100. 4. *Characteristics* of biometric systems. Точка доступу: http://www.ccert.edu.cn/education/cissp/hism/039-041.html 5. *ISO/IEC* 7816-11. Personal Verification Through Biometric Methods. 6. *ISO/IEC* 19794-2. Finger Minutiae Data. 7. *ISO/IEC* 19794-4. Finger Image Data. 8. *Задорожный В.* Идентификация по отпечаткам пальцев. // PC Magazine, № 1, 2, 2004. 9. *Bryliuk D., Starovoitov V.* Application of recirculation neural network and principal component analysis for face recognition // The 2nd International Conference on Neural Networks and Artificial Intelligence, October 2-5. 2001, Minsk, Belarus, pp. 136-142. 10. *Haykin S.* Neural Networks: A Comprehensive Foundation . – Pearson Education, Inc., 2005. – 823 p.

Харківський національний
університет радіоелектроніки

Надійшла до редколегії 11.08.2011