УДК 681.518

О. О. Капшук,
кандидат технічних наук, доцент

РЕАЛІЗАЦІЯ ТЕХНОЛОГІЙ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ ОСІБ В ІНФОРМАЦІЙНИХ СИСТЕМАХ І ТЕХНОЛОГІЯХ

Розглядаються 2D- і 3D-технологии розпізнавання обличчя людини, їх реалізація, проблеми надійності і основні напрями застосування в інформаційних системах і технологіях.

Ключові слова: технологии, распознавание образов, 2D- распознавание образов, 3D-распознавание образов, идентификация, авторизация, учет.

Наразі основним способом захисту інформації від несанкціонованого доступу є впровадження так званих засобів AAA (Authentication, Authorization, Accounting — аутентифікація, авторизація, управління правами користувачів). При застосуванні цієї технології користувач одержує доступ до інформаційних ресурсів лише після того, як успішно пройшов процедури ідентифікації й аутентифікації.

Варто при цьому враховувати, що на світовому ринку IT-послуг сегмент засобів AAA постійно зростає. На цій тенденції наголошується в аналітичних оглядах IDC, Gartner і інших консалтингових фірм [1].

Зауважимо, що питання розмежування доступу вирішуються в обов'язковому порядку при створенні будь-якої інформаційної системи. У наш час, коли системи стають дедалі розподіленішими, важко переоцінити важливість коректного розмежування такого доступу. При цьому потрібен дедалі надійніший захист систем аутентифікації як від зовнішніх, так і від внутрішніх зловмисників. Практично з моменту створення перших, розрахованих на багато користувачів, операційних систем для обмеження доступу використовуються паролі. Системи парольної аутентифікації постійно вдосконалюються, а вимоги до формування паролів стають все жорсткішими.

Варто зазначити, що користувачі не схильні ускладнювати собі життя і прагнуть користуватися якомога менш складними паролями. Чим складніші паролі, тим складніше їх запам'ятати, тим вища ймовірність того, що користувачі для отримання доступу до різних інформаційних ресурсів і програмних додатків, у тому числі і для аутентифікації в операційних системах, використовуватимуть один і той самий пароль, до того ж записуючи його на папері. Ці обставини суттєво зменшують надійність систем парольного захисту інформаційних систем.

Для підвищення надійності інформаційних технологій дедалі частіше застосовують програмно-апаратні засоби ідентифікації і аутентифікації, які можна розділити на три групи: електронні, біометричні та комбіновані. При цьому, як показує практика, традиційні методи персональної ідентифікації, базовані на застосуванні паролів або матеріальних носіїв (у вигляді пропуску, паспорта, посвідчення водія, електронних ключів і карт), вже не відповідають сучасним вимогам до надійності при визначенні особи. Пароль можна забути або перехопити, матеріальний носій — скопіювати, втратити або передати іншій особі. Саме це не дає можливість традиційним системам контролю доступу забезпечувати належний рівень надійності, що, у свою чергу, призводить до істотних фінансових втрат. Як наслідок, компанії шукають ефективніші методи забезпечення безпеки, звідси і тенденція переходу до біометричних систем, тобто до таких систем, де верифікація або ідентифікація людини відбувається, виходячи з унікальних біометричних особливостей кожного конкретного індивідуума .

На сьогодні, у зв'язку зі зростанням індустрії безпеки та посиленням боротьби зі злочинністю і тероризмом, ідентифікація особи за допомогою біометричних технологій є одним з найперспективніших і таких, що бурхливо розвиваються, напрямів.

За даними Міжнародної біометричної групи США (International Biometric Group — IBG), системи ідентифікації по зображенню обличчя в 2009 р. посідають друге місце (11,4%) на світовому ринку (рис.1) після систем, що використовують для ідентифікації відбитки пальців [2].

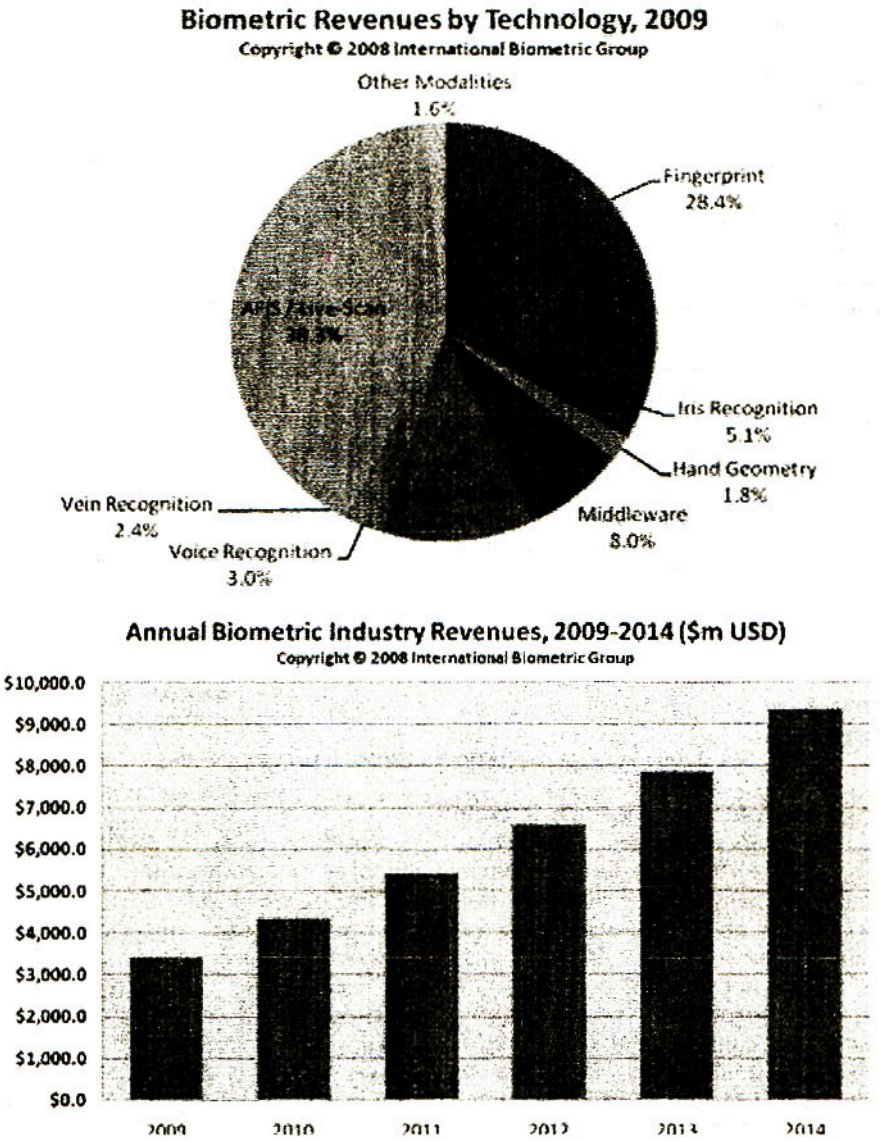

Рис.1 — Прибутки від використання біометричних технологій на світовому ринку в 2009 р. та прогноз до 2014 р. [2]

Технології ідентифікації із використанням для розпізнавання 2D- і 3D-зображення обличчя осіб — один із напрямів в біометричній індустрії, що швидко розвивається. Ця сфера біометрії багатьом здається привабливою, оскільки ми впізнаємо один одного, в першу чергу, по обличчю. Дані технології, за відповідністю фактору соціальної прийнятності, виходять на перше місце серед інших біометричних технологій, оскільки є безконтактними.

У даний час в мережі Інтернет реалізаціям технологій біометричної ідентифікації в системах контролю та управління доступом (СКУД) присвячено велику кількість публікацій. На жаль, вони мають прикладний характер, присвячуються конкретним реалізаціям СКУД, а питання надійності ідентифікації і впливу на них різних методів і алгоритмів ідентифікації практично не розглядаються.

Принцип дії технологій розпізнавання обличчя

У загальному випадку завдання ідентифікації обличчя по 2D-зображенню складається з кількох етапів (рис.2). Перший — це ви-

значення місцеположення обличчя на зображенні. Для цього початкове зображення сканують вікном меншого розміру, і кожного разу визначають деяку міру схожості зображення у вікні з людським обличчям.

Цей етап найбільш обчислювально трудомісткий, оскільки потрібно проводити сканування зображення для різних розмірів вікна, а також кожного разу знаходити ступінь схожості зображення у вікні з обличчям. Формально, зображення обличчя може задаватися структурно (обличчя — це овал, на якому всередині розташований ніс, симетрично очі і т.п.), за кольором шкіри (якщо фон має колір, відмінний від кольору шкіри), статистично і списком прикладів зображень обличчя. Після того, як обрано вікно, про яке з великою ймовірністю можна сказати, що воно містить тільки обличчя людини, розпочинаються етапи нормалізації зображення й отримання антропометричних характеристик обличчя, що використовуються далі для ідентифікації обличчя. При розпізнаванні застосовують набір методів: статистичних (метод головних компонент (Principal Component Analysis PCA), одновимірних (Hidden Markov Models HMM) і псевдодвовимірних прихованих лінійних, Марківські моделі (P2DHMM)), нейромережеві методи, Вейвлети Габора (Gabor Wavelet), еластичних графів, метод характерних точок та ін. [3].

Рис. 2 — Узагальнена структурна схема системи розпізнавання

Ефективність указаних методів істотно залежить від властивостей зображень. Необхідно, щоб всі зображення знімалися з однаковим ракурсом й освітленням. Для всіх методів потрібно, щоб розміри зображення і обличчя були однакові, внаслідок чого, для порівняння ефективності різних методів, потрібне їх тестування на однакових базах даних. Існує кілька загальноприйнятих поширених баз даних: Olivetty Research Ltd. ORL (AT&T), Yale Face Database, MIT (Massachusetts Institute of Technology) Database, FERET та ін. [4–7].

Результати тестування означених вище алгоритмів з використанням найпоширенішої бази ORL за даними [8] наведені в табл. 1.

Таблиця 1 — **Результати тестування алгоритмів**

Алгоритм	Розпізнавання, %
Метод головних компонент	80
Лінійний дискримінант Фішера	91
Одновимірна Марківська Модель	84
Двовимірна Марківська Модель	99.5
Вейвлети Габора	95.5

Комбінування цих методів дає високий відсоток розпізнавання, проте зображення, що отримуються на практиці, вимагають попередньої обробки, яка полягає у визначенні місцезнаходження обличчя на зображенні, маштабування розмірів зображення обличчя до еталонного, вирівнювання гістограми освітленості. При цьому потрібно не втратити якість зображення. Наприклад, якщо потрібно отримати якість розпізнавання, схожою з якістю на базі ORL, то роздільна здатність скануючого пристрою повинна в результаті давати зображення обличчя приблизно 100 x 100 пікселів [8].

Основна відмінність 3D-технологій розпізнавання обличчя від 2D-технологій полягає в тому, що для розпізнавання використовується 3D-модель обличчя, яка будується з використанням методів і засобів 3D-сканування об єктів. Така модель несе більше інформації про обличчя і тому дає змогу суттєво підвищити надійність роботи систем розпізнавання.

У сучасних системах 3D-сканування використовують два основні підходи: технологія стерео і технологія освітлення обличчя

структурованим світлом. У першому випадку використовується звичайне джерело освітлення і декілька зображень з відеокамер, при обробці яких будується 3D-модель обличчя. При іншому підході обличчя освітлюється структурованим світлом (невидимого інфрачервоного спектра) від трьох джерел, відбите від обличчя випромінювання уловлюється цифровою відеокамерою; при цьому збирається близько 40 000 вимірювальних точок [9]. Оскільки в 3D-сканерах обличчя на основі структурованого світла використовуються свої джерела світла, надійність результату застосування цього обладнання в поганих умовах освітленості гарантована.

Як основні характеристики обличчя у 3D-технологіях використовується сукупність антропометричних точок і відстані між ними (від кількох десятків до десятків тисяч). Наприклад, програма FaceIt компанії Identix визначає близько 80 ключових антропометричних точок обличчя і фіксує їх як вузли моделі (рис.3) [10]. Відстані між ними використовуються програмою для розпізнавання обличчя осіб.

Порівняльний аналіз 2D- і 3D-технологій

Як відомо, розпізнавання обличчя, що використовує 2D зображення, чутливе до змін освітлення. Інтенсивність світла, яке відбивається від обличчя, є функцією геометрії та альбедо обличчя, властивостей камери і джерела освітлення. Враховуючи складність цієї функції, важко побудувати моделі й алгоритми, які дають змогу надійно розпізнавати обличчя. Для подолання вказаних вище труднощів розроблено багато алгоритмів, що пропонують різні сценарії освітлення та нормалізації 2D-зображень, які дещо поліпшують надійність роботи систем розпізнавання. Слід зауважити, що при використанні 3D-зображень зміни в освітленні тільки впливають на текстуру зображення обличчя, а його форма залишається непошкодженою.

Інший чинник, який суттєво впливає на результати розпізнавання 2D-зображень, — це зміни положення обличчя при скануванні. Для компенсації впливу цього чинника запропоновані алгоритми приведення 2D-зображення до канонічного вигляду. Проте таке перетворення впливає на точність розміщення базових точок на обличчі, які використовуються при розпізнаванні, і не уможливлює вирішення цієї проблеми. Крім того, в 2D-технології це завдання майже неможливо вирішити, зважаючи на проекційну природу 2D-зображення.

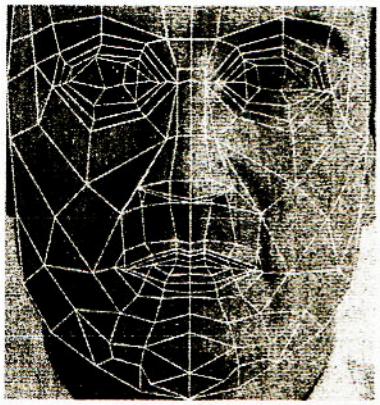

Рис. 3 — Антропометричні точки обличчя

Використовуючи 3D-зображення, проблему зміни положення обличчя при скануванні можна просто вирішити шляхом рендерингу 3D-зображення відповідно до потрібної пози. Це дає змогу за допомогою морфологічної 3D-моделі оцінювати 3D-форму невидимих частин обличчя, використовуючи нефронтальні вхідні 2D-зображення і генерувати фронтальні 2D-зображення реконструйованих облич шляхом рендерингу. Інша проблема, що пов'язана з позою, полягає в тому, що фізичні розміри обличчя в 2D-зображеннях невідомі і залежать від відстані до сканера. Проте в 3D-зображеннях фізичні розміри обличчя відомі і є невід'ємною частиною сканованих даних.

У порівнянні з 2D-зображеннями 3D-зображення кращі з погляду отримання даних про геометрію обличчя. Традиційні 2D-технології розпізнавання обличчя базуються на використанні ділянок обличчя з великим контрастом — наприклад, очі, рот, ніс і границі обличчя, а зони з низьким контрастом, такі як, наприклад, границя щелепи і щоки, важкі для опису їх з використанням напівтонових зображень. При використанні 3D-зображень немає суттєвої різниці при описуванні областей з високим і низьким контрастами. Тут потрібно зауважити, що двовимірні технології не є конкурентними, вони швидше

доповнюють тривимірну технологію розпізнавання осіб.

Основний недолік технологій розпізнавання з використанням 3D-зображень — це висока вартість технічних засобів 3D-сканування і значно більша обчислювальна складність обробки 3D- даних порівняно з 2D-даними.

Надійність технологій розпізнавання обличчя

Основна проблема всіх технологій біометричної ідентифікації полягає в тому, що результати ідентифікації людини носять імовірнісний характер і залежать від багатьох чинників.

У біометрії параметри надійності задаються помилкою FRR (False Reject Rate), коли система не впізнала «свого», і помилкою FAR (False Accept Rate), коли система пропустила «чужого». Повні дані про FRR і FAR для 3D-технологій розпізнавання обличчя на сайтах виробників зазвичай не наводяться. За даними, наведеними в [11], для найкращих моделей фірми Bioscript (3D EnrolCam, 3D FastPass) при FAR = 0,0047% FRR становить 0,103%. Особливий інтерес становить японська міні-система розпізнавання осіб, яка легко вмонтовується в зручному для користувача місці, підключається через USB порт або Ethernet до будь-якого PC. Імовірність помилки становить 0,00001%, її вартість — $1550 (лютий 2010 р.) [12]. Вважається, що статистична надійність 3D-технології розпізнавання обличчя дорівнює надійності методу ідентифікації за відбитками пальців.

Слід відзначити розробки компанії Identix, яка при реалізації 3D-технології розпізнавання обличчя не тільки використовує геометричну 3D-модель, а й доповнює її описом поверхні шкіри (текстури). При цьому фотографується ділянка шкіри обличчя, що розбивається на кілька дрібніших блоків, де система виявляє особливі лінії, пори та інші текстурні елементи. За повідомленнями компанії Identix, це дає змогу підвищити ефективність ідентифікації на 20–25% [10].

Висновки. Технології розпізнавання із використанням 2D- і 3D-зображень обличчя осіб, як видно з проведеного аналізу, в даний час суттєво удосконалюються, підвищується їх надійність, зменшується вартість апаратних і програмних засобів, що дає змогу використовувати їх не тільки для побудови систем контролю й управління доступом в інформаційних системах і технологіях, а й використовувати також у розробках нових інформаційних сервісів, а саме йдеться про:

— пошук зображень в Інтернеті, пошук на основі візуальних даних — наприклад, зображень, що схожі на вказаний зразок або містять заданий об'єкт (наприклад, обличчя), уточнення результатів пошуку зображень, проведеного на основі текстових даних за допомогою аналізу візуальної інформації — наприклад, фільтрація дублюючих зображень;

— автоматичну обробку та поліпшення візуальної якості зображень, особливо портретних (баланс, колір обличчя і зубів, видалення червоних очей і т.п.) [13];

— автоматичне фокусування на обличчі людини при фотографуванні;

— відео-контроль за появою нових рухомих об'єктів (детектування вторгнення);

— управління комп'ютерними системами за допомогою жестів, без миші і клавіатури;

— системи стеження за станом операторів складних систем з метою запобігання збоям в їх роботі через втому, відволікання, засипання тощо;

— сервіси для соціальних мереж і блогів: автоматичне створення невеликих копій для попереднього перегляду фотографій користувачів в такий спосіб, щоб вони містили тільки обличчя (при тому, що на фото може бути людина в повний зріст на тлі інших об'єктів), щоб полегшити знаходження потрібної людини в результатах пошуку в мережі;

— веб-камери, що утримують обличчя людини в «полі зору» і повертаються вслід за зміною його положення;

— аутентифікація користувачів в системах дистанційного навчання.

Рассматриваются 2D- и 3D-технологии распознавания лица человека, их реализация, проблемы надежности и основные направления применения в информационных системах и технологиях.

Ключевые слова: технологии, распознавание образов, 2D- распознавание образов, 3D-распознавание образов, идентификация, авторизация, учет.

2D- and 3D facial recognition, their realization, problems of reliability and basic directions of application in the information systems and technologies are examined.

Key words: technologies, facial recognition, reliability, 2D Facial Recognition, 3D Facial Recognition, authentication, authorization, accounting.

Література

1. Парольная защита: прошлое, настоящее, будущее [Електронний ресурс]. Режим доступу: http://www.compress.ru/Article.aspx?id=20509.

2. Biometrics Market and Industry Report 2009-2014 [Електронний ресурс]. Режим доступу: http://www.biometricgroup.com/reports/public/market_report.php.

3. Face Recognition Edited by Kresimir Delac and Mislav Grgic. Published by the I-Tech Education and Publishing, Vienna, Austria, 2007.

4. Olivetty Research Ltd. ORL (AT&T). [Електронний ресурс]. Режим доступу: http://www.uk.research.att.com.

5. MIT (Massachusetts Institute of Technology) Database.[Електронний ресурс]. Режим доступу: ftp://whitechapel.media.mit.edu/pub/images.

6. FERET Database. [Електронний ресурс]. Режим доступу: http://www.nist.gov/humanid/feret.

7. Yale Face Database. [Електронний ресурс]. Режим доступу: http://cvc.yale.edu.

8. *Волченков М. П., Самоненко И. Ю.* Об автоматическом распознавании лиц. [Електронний ресурс]. Режим доступу: http://www.intsys.msu.ru/magazine/archive/v9%281-4%29/volchenkov-135-156.pdf .

9. Технология трехмерного распознавания лиц. [Електронний ресурс]. Режим доступу: http://www.procctv.ru/

10. *Жук Г.* Компьютерное распознавание лица. [Електронний ресурс]. Режим доступу: http://digimedia.ru/articles/digital-tales/bezopasnost/sistemy-raspoznavaniya/

11. *Моржаков В.* Современные биометрические методы идентификации. [Електронний ресурс]. Режим доступу: http://www.bdi.spb.ru/index.htm

12. Охранная система 3D face-контроля. [Електронний ресурс]. Режим доступу: http://www.best-promoitems.com/rus/face-control.php

13. Технологии компьютерного зрения SeeStorm. [Електронний ресурс]. Режим доступу: http://www.seestorm.ru/technologies/cv/