

АНАЛІЗ ТРЬОХ БІОМЕТРИЧНИХ МЕТОДІВ АВТЕНТИФІКАЦІЇ ОСОБИ

Х.А. БУГАЄНКО, І.Д. ГОРБЕНКО

Вивчаються стандартні механізми автентифікації особи по відбиткам пальців, по райдужній оболонці ока та по геометрії обличчя Vocord Face Control по 2D-зображенню та 3D-моделям, їх можливості, переваги та недоліки. Проводиться аналіз методів автентифікації особи та вносяться пропозиції по їх вдосконаленню.

Ключові слова: автентифікація, метод, особа, біометрична система, обробка зображення, відбиток пальця, райдужна оболонка ока, геометрія обличчя.

ВВЕДЕННЯ

Актуальність розвитку біометричних технологій ідентифікації особи обумовлена збільшенням числа об'єктів і потоків інформації, які необхідно захищати від несанкціонованого доступу, а саме: криміналістика; системи контролю доступу; системи ідентифікації особи; інформаційна безпека (доступ в мережу, вхід на ПК); облік робочого часу та реєстрація відвідувачів; системи голосування, проведення електронних платежів; автентифікація на Web- ресурсах; різні соціальні проекти, де потрібна ідентифікація людей; проекти цивільної ідентифікації (перетин державних кордонів, видача віз на відвідування країни) і т.д.

Предмет дослідження – стандартні механізми автентифікації особи по відбиткам пальців, по райдужній оболонці ока та по геометрії обличчя Vocord FaceControl по 2D-зображенню та 3D-моделям, їх можливості, переваги та недоліки.

Мета роботи – аналіз методів автентифікації особи та пропозиції по їх вдосконаленню.

Метод дослідження – вивчення літератури, обробка та отримання певних результатів.

На відміну від паперових ідентифікаторів (паспорт, водійські права), пароля або персонального ідентифікаційного номера (PIN), біометричні характеристики не можуть бути забуті або загублені, їх важко підробити і практично неможливо змінити.

Одним із засобів забезпечення доступності інформації є автентифікація. Автентифікація – це перевірка приналежності суб'єкту чи об'єкту доступу пред'явленого їм ідентифікатора; перевірка справжності.

В даній статі будуть розглянуті механізми автентифікації особи за рахунок різних біометричних даних та методів.

Ідентифікація на основі біометричних даних – це засіб автоматичного розпізнавання особистості на базі унікальних фізичних або поведінкових параметрів. Ідентифікація виконується за допомогою порівняння отриманих біометричних характеристик і шаблонів, що зберігаються у базі даних.

В даній статі будуть розглянуті механізми автентифікації особи за рахунок різних біометричних даних та методів. Проаналізувавши, зроблені

відповідні висновки щодо найефективнішого методу автентифікації особи.

1. ОСНОВНІ ГАЛУЗІ ЗАСТОСУВАННЯ БІОМЕТРИЧНИХ ДАНИХ

Інтеграція України до Європи зачіпає не лише економічну і політичну, але і соціальну сферу життя наших громадян. Європейський союз визначив набір протоколів для реалізації ЕАС (доступу до критичних даних (біометричних даних) в своїх електронних паспортах (ЕП, ePassport)). В Україні і в країнах ЄС ведеться робота по впровадженню біометричних паспортів.

Біометричний паспорт – це документ, що дає право на виїзд за межі країни і в'їзд до іноземних країн. Основною відмінністю електронних документів від існуючих паперових аналогів є те, що в них може бути внесений біометричний набір характеристик, замінити які важче ніж надрукований набір даних, і відповідно набагато важче видавати себе за власника паспорта. Біометричні дані є особливо критичною інформацією, доступ до якої мають отримувати виключно ті системи перевірки, які можуть підтвердити свої повноваження на дані дії. Основними джерелами з питань біометричного паспорту є різноманітні публікації організації цивільної авіації ICAO. Це, в першу чергу, Дос 9303, що складається з кількох частин. Основоположною є частина 1 «Машинозчитуємі паспорти» том 2 «Специфікації на електронні паспорти з засобами біометричної ідентифікації».

Основними російськими стартапами по біометричній автентифікації є ГОСТ Р ИСО/МЭК 19794-6 –2006, ГОСТ Р ИСО/МЭК 19794-5 –2006, ГОСТ Р ИСО/МЭК 19794-2 –2005, ГОСТ Р ИСО/МЭК 19794-4 –2006, ГОСТ Р ИСО/МЭК 19785-1 –2008, ГОСТ Р ИСО/МЭК 19794-7 –2009, ГОСТ Р ИСО/МЭК 19795-2 –2006.

Ідентифікація на основі біометричних даних – це засіб автоматичного розпізнавання особистості на базі унікальних фізичних або поведінкових параметрів. Ідентифікація виконується за допомогою порівняння отриманих біометричних характеристик і шаблонів, що зберігаються у базі даних. В залежності від характеристик, які при цьому використовуються.

Біометричні системи поділяються на статичні та динамічні. До методів першої групи відносяться такі види автентифікації: за відбитком пальця, за формою долоні, по розташуванню вен на лицьовій стороні долоні, по сітківці ока, по райдужній оболонці ока, за формою обличчя, по термограмі обличчя, по ДНК, інші методи. До динамічних методів відносять автентифікацію по рукописному почерку, по клавіатурному почерку, по голосу, інші методи. В даний час активно використовуються такі біометричні ознаки, як відбитки пальців, геометрична форма кисті руки, геометрія обличчя, особливості голосу, райдужна оболонка ока, рукописний підпис.

2. АВТЕНТИФІКАЦІЯ ОСІБ ПО ВІДБИТКАМ ПАЛЬЦІВ

Серед всіх біометричних технологій ідентифікація за відбитками пальців є найстарішим і найпоширенішим методом, який успішно застосовується в багатьох областях. У кожної людини свої унікальні і незмінні відбитки пальців. Задача ідентифікації особистості по відбитку пальця вирішується шляхом зіставлення ідентифікованого відбитка з еталонними [1]. Відбитки вважаються ідентичними, якщо коефіцієнт відповідності становить 65% [2] і вище (цей поріг можна змінити).

Відбитки пальців можуть відрізнити один від одного поворотом, зміщенням, зміною масштабу і площею дотику. Пропонований підхід розроблений для порівняння відбитків пальців однакової розмірності і складається з трьох основних етапів [6]:

1. Обробка вихідного зображення (дивись рис. 1).



Рис. 1. Вихідне зображення

- 1.1. Обчислення орієнтації ліній;
- 1.2. Поліпшення якості ліній (дивись рис. 2);



Рис. 2. Зображення після покращення якості

- 1.3 Бінаризація зображення;
- 1.4 Стоншення ліній зображення (дивись рис. 3).



Рис. 3. Зображення після стоншення ліній

2. Виділення мінуцій (див. рис. 4).



Рис. 4. Визначення мінуцій

3. Зіставлення мінуцій відбитків пальців.

- 3.1 Знаходження центру;
- 3.2 Переміщення;
- 3.3 Поворот;
- 3.4 Зміна масштабу (не розглядається).

По даному методу можна виділити основні недоліки та переваги, що показано в табл. 1.

Таблиця 1

Переваги та недоліки методу

Переваги методу	Недоліки методу
<ul style="list-style-type: none"> • висока достовірність — статистичні показники методу вище показників способів ідентифікації по обличчю, голосу, розпису; • низька вартість обладнання; • достатньо проста процедура сканування відбитка. 	<ul style="list-style-type: none"> • папілярний узор відбитка пальця дуже легко можна пошкодити дрібними подряпинами, порізами; • недостатня захищеність від підробки, викликана широким поширенням методу; • залежність від чистоти пальця; • для сухої шкіри якість розпізнавання нижче.

3. АВТЕНТИФІКАЦІЯ ОСІБ ПО РАЙДУЖНІЙ ОБОЛОЧЦІ ОКА

1. Виявлення великого центру зіниці. X-координата — це центр зіниці розраховується за формулою:

$$x_0 = x_1 + x_r / 2.$$

Можемо отримати верхні та нижні координати краю зіниці в місці розташування:

$$(x_p, y_u), (x_r, y_b).$$

У-координата центру зіниці розраховується за формулою:

$$y_0 = y_u + y_b / 2.$$

В результаті отримуємо великий центр зіниці, який знаходиться по координатам (x_0, y_0) .

2. Вирівнювання контуру границі зіниці. Можна записати суму помилок як:

$$E^2 = \sum(x_i^2 + y_i^2 + cx_i + dy_i + e)^2. \quad (1)$$

Якщо ми беремо приватні похідні з рівняння (1) щодо коефіцієнти c, d та e, i – набір кожен до нуля, отримуємо три рівняння та координати x_i, y_i . Ми отримуємо центр зіниці $I(I_x, I_y)$ і радіус R_i через співвідношення вищезгаданих точок краю зіниці. Так само знаходимо центр зовнішньої райдужної оболонки $O(O_x, O_y)$ і радіус R_0 .

3. Якісна оцінка зображення райдужної оболонки. Практично, якість деяких зображень райдужної оболонки настільки жахлива, що помилка, 100-відсотково буде існувати. Щоб уникнути цієї проблеми, необхідно оцінити якість райдужної оболонки зображення. Тільки, коли якість відповідає нашому запиту, ми можемо використовувати це зображення. Головні проблеми поганої якості зображення райдужної оболонки – розмиття, викликане поганим фокусуванням, часом та іншими факторами.

В табл. 2 приведені можливі переваги та недоліки даного методу автентифікації.

Таблиця 2

Переваги та недоліки методу

Переваги методу	Недоліки методу
<ul style="list-style-type: none"> • статистична надійність алгоритму; • захоплення зображення проводиться на відстані від декількох см до декількох метрів, фізичний контакт людини з пристроєм не відбувається; • райдужна оболонка захищена від пошкоджень, тому не змінюється в часі. 	<ul style="list-style-type: none"> • ціна системи, вище ціни системи, заснованої на розпізнаванні пальця або на розпізнаванні особи; • низька доступність готових рішень.

4. АВТЕНТИФІКАЦІЯ ПО ГЕОМЕТРІЇ ОБЛИЧЧЯ VOCORD FACE CONTROL ПО 2D-ЗОБРАЖЕНЮ ТА 3D-МОДЕЛЯМ

VOCORD FaceControl – система автоматичного некооперативного виявлення, простежування і виділення зображень облич, формування векторів ознак по 2D-зображенню і 3D-моделям за рахунок біометричної ідентифікації людини.

А також можна виділити області застосування поданих двох методів, для забезпечення безпеки в місцях масового скупчення людей:

– місця масового перебування людей: площі, стадіони;

– транспортні вузли: аеропорти, вокзали, автостанції;

– додаткові кошти ідентифікації особистості;

– прикордонні паспортно-візові контрольні пункти;

– прохідні і контрольні-пропускні пункти;

– громадські установи.

Для біометричного методу ідентифікації особи по 2D – розпізнаванню розглянемо всі ймовірні переваги та заодно й недоліки, які містяться в даному методі (дивитись табл. 3-4) [5].

Таблиця 3

Переваги та недоліки методу (2D – розпізнавання особи)

Переваги методу	Недоліки методу
<ul style="list-style-type: none"> - не потрібне дороге обладнання; - при відповідному обладнанні можливість розпізнавання на значних відстанях від камери. 	<ul style="list-style-type: none"> - низька статистична достовірність; - пред'являються вимоги до освітлення; - неприйнятність будь-яких зовнішніх перешкод; - не враховують можливі зміни міміки обличчя, вираз повинен бути нейтральним.

Допуск по 2D-зображенню зручний і дешевий, але має обмежену сферу застосування через погані статистичних показників. З формули:

$$FAR * N2 \approx 1 = > N = (1/FAR)1/2. \quad (2)$$

З формули (2) отримуємо $N \approx 30$ - чисельність персоналу організації, при якій ідентифікація співробітника відбувається досить стабільно. Для біометричного методу ідентифікації особи по 3D – моделі розпізнаванню розглянемо всі ймовірні переваги та заодно й недоліки, які містяться в даному методі.

Таблиця 4

Переваги та недоліки методу (3D – розпізнавання особи)

Переваги методу	Недоліки методу
<ul style="list-style-type: none"> • висока достовірність розпізнавання – більше інформації, чим має звичайний знімок; • стійкість розпізнавання до відхилення ракурсу особи від фронтального; • стійкість розпізнавання до неоднорідності освітлення; • відсутність необхідності контактувати з пристроєм; • низька чутливість до зовнішніх факторів. 	<ul style="list-style-type: none"> • має обмежену сферу застосування із-за поганих статистичних показників; • дороге обладнання; • зміна міміки обличчя і перешкоди на обличчі погіршують статистичну надійність методу.

В табл. 5 зведені результати розглянутих двох методів, що базуються на автентифікації особи по геометрії обличчя.

Системи розпізнавання по 3D – зображенню особи дуже специфічні. Вони можуть знадобитися у випадках, коли розпізнавання вимагає відсутності фізичного контакту, але поставити

систему контролю по райдужній оболонці неможливо.

Таблиця 5

Аналіз двох методів

	Стійкість до підробки	Стійкість до доквілля	Простота використання	Вартість	Швидкість	Стабільність біометричної ознаки в часі
Обличчя 2D	4	6	6	10	10	8
Обличчя 3D	9	8	10	5	7	10

Повні дані про FRR і FAR для алгоритмів по 3D – зображенню на сайтах виробників відкрито не наведено. Але для кращих моделей фірми Bioscript (3D EnrolCam, 3D FastPass), які працюють за методом проектування шаблону при FAR = 0.0047% FRR становить 0.103%. Вважається, що статистична надійність методу порівнянна з надійністю методу ідентифікації за відбитками пальців.

ВИСНОВОК

Ця робота присвячена актуальному питанню – ідентифікації особи на основі біометричних даних. Ця методика має ряд переваг: використання тільки фізичних параметрів людини; неможливість підробки біометричних даних.

Ймовірність того, що відбитки пальців у двох людей співпадуть - один до 220 мільйонів. Тобто $1/220000000 = 4,54 \cdot 10^{-9}$.

З райдужної оболонки 11-міліметрового діаметру сучасні алгоритми обробки і аналізу інформації дозволяють отримати в середньому 3,4 біт інформації на 1 мм² площі [3, 4]. Щільність отриманої інформації така що райдужна оболонка має 266 унікальних точок ідентифікації в порівнянні з 10-60 точками для інших біометричних методів [4].

Хоча біометрія представляє собою інтерес як джерело ентропії, дослідження вказують на те, що багато біометричних методів, можливо, не фактично, але пропонують достатню невпевненість з цією метою.

Табл. 6 та 7 ілюструють звітність отриманих результатів по обраним трьом методам автентифікації.

По показнику FAR (false acceptance rate) найбільш надійним буде метод по 2D / 3D моделям, тому що ймовірність хибного співпадання біометричних характеристик двох осіб найменша в порівнянні з останніми двома методами.

По показнику FRR (false rejection rate) найбільш надійним буде метод по райдужній оболонці ока, тому що ймовірність відмови в доступі особи, що має право доступу найменша, а найбільш гіршим по цьому показнику являється метод по відбиткам пальців.

Таблиця 6

Звітність отриманих результатів

Назва методу	FAR	FRR	Ймовірність співпадання	Швидкість обробки	Попит на ринку
По відбиткам пальців	0,01%	10%	$4,54 \cdot 10^{-9}$	$2,5 \cdot 10^{-4}$, с	39%
По райдужній оболонці ока	0,01%	0,05%	10^{-78}	0,3 - 0,5, с	6% - 9%
По 2D / 3D моделям	0,0047%	0,103%	$3,26 \cdot 10^{-7}$	1-2, с	13% - 18%

Таблиця 7

Звітність отриманих результатів

Назва методу	Стійкість до підробки	Стійкість до доквілля	Простота використання	Вартість
По відбиткам пальців	6	10	9	10
По райдужній оболонці ока	10	9	8	7
По 2D / 3D моделям	4/9	6/8	6/10	10/5

Оцінюючи по ймовірності співпадання однакових зображень маємо, що найбільш кращим являється метод по райдужній оболонці ока, так як цей метод має мінімальну ймовірність в порівнянні з двома іншими, а гіршим буде – по 2D / 3D моделям.

Використовуючи дані щодо швидкості обробки одного зображення, то кращим являється метод по відбиткам пальців, а потім йдуть по райдужній оболонці ока та по 2D / 3D моделям.

Оцінюючи методи по стійкості до підробки можна сказати, що під цей параметр підходить як метод по райдужній оболонці ока так і метод по 2D / 3D моделям. По стійкості до доквілля найкращими будуть методи по відбиткам пальців та по райдужній оболонці ока, тому що стійкість роботи системи за різних зовнішніх умов, таких як зміна освітлення або температури приміщення, не залежить.

По показнику складність використання, тобто наскільки складно скористатися біометричним приладом, взагалі то під цей показник попадають усі три методи. Беручи до уваги вартість приладів для ідентифікації особи, то можна сказати, що на даний момент найбільш дорогим буде придбання приладу для ідентифікації особи по 2D / 3D моделям. А найбільш дешевшим являються прилади для ідентифікації особи по відбиткам пальців.

По показнику – попит на ринку [5], то найбільш використовуваним являється ідентифікація особи по відбиткам пальців, яка в свою чергу

займає майже половину світового ринку, потім йде геометрія обличчя (2D / 3D - моделі) та на останньому місці опинився метод по райдужній оболочці ока.

Для райдужної оболонки ока можна збільшити точність системи практично квадратично, без втрат для часу, якщо ускладнити систему, зробивши її на два ока. Для відбитків пальців - шляхом комбінування декількох пальців, шляхом комбінування двох рук, але таке поліпшення можливо тільки при збільшенні часу, що витрачається при роботі з людиною.

Узагальнивши результати для методів, можна сказати, що для середніх і великих об'єктів а так само для об'єктів з максимальною вимогою у безпеці слід використовувати райдужну оболонку в якості біометричного доступу.

Для об'єктів з кількістю персоналу до декількох сотень чоловік оптимальними буде доступ по відбитках пальців. Системи розпізнавання по 3D зображенню особи дуже специфічні. Вони можуть знадобитися у випадках коли розпізнавання вимагає відсутності фізичного контакту, але поставити систему контролю по райдужній оболонці неможливо. Наприклад, при необхідності ідентифікації людини без її участі, прихованою камерою, або камерою зовнішнього виявлення, але можливо це лише при малій кількості суб'єктів у базі і невеликому потоці людей, що знімаються камерою.

Література

- [1] *Anil K. Jain Handbook of Biometrics.* Springer Science+Business Media, 2008.
- [2] *В. Задорожний, Идентификация по отпечаткам пальцев.* PC Magazine, - 2004, - т.1 - №2.
- [3] *Daugman J G.* Biometric personal identification system based on iris analysis - [P].US Patent 5291560, 1994.
- [4] *Wildes R P.* Iris recognition, An Emerging Biometric Technology. //Processing of the IEEE - с.185, 1997.
- [5] *Chang, K. I.* Multiple nose region matching for 3D face recognition under varying facial expression. / K. I. Chang// IEEE Transactions on Pattern Analysis and Machine Intelligence- №28(10), October 2006. -1695-1700 с.

- [6] *H. Lin, A. Jian, S. Pankanti, R. Bolle,* Fingerprint enhancement. //Applications of Computer Vision, 1996.

Надійшла до редколегії 18.04.2012

Горбенко Іван Дмитрович, фото та відомості про автора див. на стор. 190.



Бугаєнко Христина Андріївна, студентка кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки. Наукові інтереси: біометричні методи, їх ефективність, попит на світовому ринку та можливі переваги та недоліки.

УДК 621.391:519.2:519.7

Анализ трех биометрических методов аутентификации личности / К.А. Бугаенко, И.Д. Горбенко // Прикладная радиоэлектроника: науч.-техн. журнал. - 2012. - Том 11. № 2. - С. 262-266.

Изучаются стандартные механизмы аутентификации личности по отпечаткам пальцев, по радужной оболочке глаза и по геометрии лица Vocord Face Control по 2D-изображению и 3D-моделям, их возможности, преимущества и недостатки. Проводится анализ методов аутентификации личности и вносятся предложения по их усовершенствованию.

Ключевые слова: аутентификация, метод, личность, биометрическая система, обработка изображения, отпечаток пальца, радужная оболочка глаза, геометрия лица.

Табл. 7. Ил. 4. Библиогр.: 6 назв.

UDC 621.391:519.2:519.7

Analysis of three biometrical methods of person authentication/ K.A. Bugaenko, I.D. Gorbenco // Applied Radio Electronics: Sci. Journ. - 2012. Vol. 11. № 2. - P. 262-266.

The paper studies standard mechanisms for authenticating a person by fingerprints, by eye iris and the geometry of the face Vocord Face Control of 2D-images and 3D-models, their features, advantages and disadvantages. Besides, analysis of methods of person authentication is done and proposals to perfect them are introduced.

Keywords: authentication, method, person, biometric system, image processing, fingerprint, iris, face geometry.

Tab. 7. Fig. 4. Ref.: 6 items.