

АНАЛІЗ БІОМЕТРИЧНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

На сьогоднішній день в індустрії безпеки розпочався новий етап. На загальному фоні найбільш динамічно продовжують розвиватись сучасні системи ідентифікації та захисту інформації. Особливу увагу привертають до себе біометричні засоби захисту інформації (БЗЗІ), що обумовлено їх високою надійністю та досягненим в останній час значним здешевленням [1]. Використання БЗЗІ дозволяє підняти на принципово новий рівень якості автоматизовані системи різнопланового призначення. Це обумовлено перспективністю використання біометрії, універсальністю біометричних характеристик та розвитком інформаційних технологій. Саме в момент такого великого поширення інформації [2,3,4,5,6,26,28] стосовно БЗЗІ постає проблема вибору біометричної технології в залежності від вимог конкретної прикладної задачі, тому створення рекомендації щодо вибору БЗЗІ є актуальною задачею.

У роботі [8] розглянуті БЗЗІ, що застосовуються для аутентифікації, в той час, коли область їх застосування значно ширша. Розгорнута класифікація біометричних систем ідентифікації наведена в [9], але в цій роботі розглядаються переважно системи, що базуються на статичних біометричних характеристиках. Під час її складання технології, що використовують динамічні біометричні характеристики, ще не набули такої поширеності, як в останні роки. В [10] приводиться опис відомих біометричних признаков, в який не включені відомі на сьогоднішній день характеристики такі, як розпізнавання динаміки губ при вимові, динаміки активності мозку та інші. Порівняльна класифікація декількох біометричних систем проводилася в [11], а в [12] порівнюється рівень помилкових спрацьовувань трьох найпоширеніших БЗЗІ. Обидві порівняльні класифікації лише кількісно порівнюють характеристики БЗЗІ, але не показують взаємозв'язок з конкретними задачами. Питання вибору БЗЗІ в проаналізованій літературі освітлюється частково. Робіт, в яких описуються закономірності вибору біометричних технологій в залежності від сфери використання, не виявлено.

Метою даної роботи є створення рекомендації щодо вибору БЗЗІ при вирішенні задачі в конкретній області шляхом аналізу класифікацій, актуальних публікацій, можливостей використання нових біометричних технологій. Використання результатів роботи дозволить легко обирати БЗЗІ, які найбільше підходять для розв'язання тих чи інших завдань.

Пропонується провести класифікацію БЗЗІ за наступними критеріями: форма біологічних даних (ФБД); базова біометрична технологія (ББТ); сфера застосування біометричної технології (СЗБТ). Ці критерії було обрано з огляду на функціональність створюваної рекомендації. Рекомендація, створена на основі класифікації за такими критеріями, дозволить обирати біометричні технології для вирішення задач в конкретній сфері при заданих додаткових умовах.

Зазвичай біометричні технології класифікують за таким критерієм, як форма біологічних даних [7]: біометричні технології, що використовують статичні дані, тобто такі, що не змінюються суттєво впродовж значного терміну (С); біометричні технології, що використовують дані про поведінку, тобто такі, що досліджуються динамічно (Д).

Класифікація БЗЗІ за базовою біометричною технологією [9] виглядає наступним чином: дактилоскопічний аналіз (ДА) [1, 2, 4, 9, 10, 15, 20, 26, 33]; розпізнавання райдужки ока (РО) [1, 9, 10, 41]; розпізнавання сітківки (С) [1, 9, 40, 41]; розпізнавання підпису людини (ПЛ) [1, 9, 10]; розпізнавання по зображенню обличчя (ЗО) [1, 5, 6, 9, 10]; розпізнавання по геометрії кисті, руки (ГКР) [9, 10, 11, 31]; розпізнавання по ДНК (ДНК) [9, 19, 20]; розпізнавання по відбитку долоні (ВД) [1, 9]; розпізнавання по формі вуха (ФВ) [9, 10]; розпізнавання по трьохвимірному зображенню обличчя (ЗО3D) [5, 6, 9]; розпізнавання по розташуванню капілярних судів (РКС) [9, 10, 11, 38]; розпізнавання по почерку, в тому числі клавіатурному (КП) [1, 9, 10, 14, 22]; розпізнавання по характеристикам голосу (ХГ) [1, 9, 11, 35]; розпізнавання по ході (Х) [9, 11, 22]; розпізнавання динаміки підпису людини (ДПЛ) [1, 9, 11]. Попонується розширити дану класифікацію наступними актуальними на сьогоднішній день біометричними технологіями:

розпізнавання електричної активності мозоку (ЕАМ) [23, 39]; розпізнавання по динаміці губ при вимові (ДГВ) [34, 35]; розпізнавання по відбитку губ (ВГ) [36, 37]; розпізнавання по термограмі обличчя (ТО) [1, 5, 6]; розпізнавання по динаміці управління маніпуляторами миша та тачпад (ДуММТ) [11, 22, 32];

Під час створення рекомендації необхідно визначити сферу використання тієї чи іншої біометричної технології. Для цього пропонується провести класифікацію за сферою застосування. На даний момент БЗЗІ застосовуються у наступних сферах: криміналістика (КР), аутентифікація в інформаційних системах (АІС), контроль доступу (КД), медицина (МЕД), криптографія (КРК), ідентифікація на державному та міжнародному рівні (ІМР), управління технічними засобами (УТЗ), встановлення сімейних зв'язків (ВСЗ). Біометричні ознаки застосовувались для ідентифікації в криміналістиці ще починаючи з 1985 року [27]. Одним із перших застосувань біометрії в цій області був дактилоскопічний аналіз. На сьогоднішній день технологій, що дозволяють ідентифікувати розташування папілярних ліній на пальцях, більше 20 [9,18,26,29]. В той же час, із розвитком технологій застосування біометрії у криміналістиці постійно поширюється. Найчастіше біометричні технології вирішують питання розпізнавання людини, отже однією з найпоширеніших областей їх застосування є контроль доступу [9,18,21,25,26,29]. Біометрична характеристика є універсальним ключем, який людина не забуде, як пароль, та не загубить, як смарт-карту. В цій області свого розвитку на сьогоднішній день набувають комбіновані технології, наприклад, використання смарт-карти сумісно з ідентифікацією обличчя. До недавнього часу в області медицини біометричні технології не застосовувались. Шляхом розпізнавання та аналізу деяких [19,20] біометричних ознак можна діагностувати синдром Шершевського-Тернера, синдром Клайнфельтера та інші психосоматичні захворювання. Використання біометричних технологій значно поширилось завдяки розвитку інформаційних систем. Одночасно із вирішенням багатьох питань автоматизації та інформатизації постало питання аутентифікації людини в інформаційній ситсемі [8,30]. На даний момент існують біометричні технології, які розпізнають динаміку користування людиною периферійних пристроїв інформаційної системи: клавіатури, маніпуляторів миша та тачпадів [14]. Зчитування деяких динамічних біометричних ознак дозволяє спростити задачу криптографічного розподілу ключів [22,23]. Справа в тому, що в процесі життєдіяльності людина робить одні й ті ж самі речі постійно з деякими відхиленнями, а отже ці відхилення є не що інше, як випадкова величина, яка чудово підходить для розв'язання задач криптографічного розподілу ключів, адже будь-який такий розподіл має засновуватись на послідовності випадкових, або псевдо-випадкових величин. Після подій 11.09.2002 США розпочали свою програму по міжнародному обміну біометричними даними. В наш час біометрична ознака є частиною паспорта громадян таких країн, як США, Англія, Японія [15,16,17]. До 2012 року в Росії планується введення нових біометричних паспортів [24]. При управлінні робототехнічними засобами часто використовують біометричні технології, переважно основані на розпізнаванні динамічних характеристик [1,9,]. Тобто, для виконання робіт високої точності іноді не вистачає можливостей процесора технічного засоба, тоді в діло вступає людина, але опосередковано, через трансляцію своїх біометричних характеристик на технічний засіб. Найбільш точна, відома на сьогоднішній день, біометрична характеристика це ДНК людини [1]. По ДНК на сьогодні можна не тільки 100% ідентифікувати людину, а й з великою вирогідністю визначити її найближчих родичів.

Також були розглянуті такі допоміжні критерії, як унікальність, постійність, можливість збору, що були оцінені по трьохбальній шкалі [26]. Унікальність (УН) показує, наскільки добре одна людина відрізняється від іншої з біометричної точки зору. Постійність (ПСТ) – це міра того, наскільки обрані біометричні характеристики залишаються незмінними в динаміці, – наприклад, в процесі старіння. Можливість збору (МВЗ) показує, наскільки легко зібрати ту чи іншу біометричну характеристику.

Результатом проведеного аналізу є рекомендація представлена в таблиці 1. Її використання дозволяє спростити задачу вибору БЗЗІ, які підходять під умови конкретних практичних задач. В ході складання таблиці було проаналізовано 20 базових біометричних

технологій, 6 сфер застосування біометричних технологій, 2 форми біологічних даних, та три додаткових критерія.

Таблиця 1 Рекомендація щодо вибору БЗЗІ

ББТ/БД	СЗБТ								Додаткові параметри		
	КРМ	КД	ВС З	МЕ Д	ІМР	КРК	УТЗ	АІ С	УН	ПСТ	МВЗ
ДА/С	+	+	-	+	+	-	-	+	2	3	3
РО/С	-	+	-	+	-	-	-	+	2	2	2
С/С	-	+	-	-	-	-	-	+	2	2	1
ПЛ/С	+	-	-	-	+	-	-	-	1	2	3
ЗО/С	+	+	-	-	+	-	-	+	2	1	1
ТО/С	-	+	-	-	-	-	-	-	2	1	2
ГКР/С	-	+	-	-	-	-	-	-	2	2	1
ДНК/С	+	-	+	+	-	-	-	-	3	3	1
ВД/С	+	+	-	-	-	-	-	-	2	3	2
ВГ/С	-	+	-	+	-	-	-	+	2	1	3
ФВ/С	-	+	-	-	-	-	-	+	2	2	1
ЗОЗД/С	-	+	-	-	-	-	-	+	2	2	1
РКС/С	-	+	-	+	-	-	-	-	2	1	2
КП/Д	-	-	-	-	-	+	-	+	2	2	2
ХГ/Д	-	+	-	+	-	-	+	+	3	2	1
Х/Д	-	+	-	-	-	-	+	-	3	1	1
ЕАМ/Д	-	-	-	-	-	+	+	-	3	2	1
ДВГ/Д	-	-	-	-	-	+	+	+	3	2	1
ДуММТ/ Д	-	-	-	-	-	+	+	+	2	2	2
ДВЛ/Д	-	-	-	-	-	+	-	-	3	2	1

Можна зробити висновок, що біометричні технології найпоширеніше використовуються в області контролю доступу, тобто для вирішення задач ідентифікації та аутентифікації.

В даній роботі наведена рекомендація щодо вибору та застосування БЗЗІ, в її основу було покладено аналіз класифікацій за трьома основними та трьома допоміжними критеріями

Як перспективу розширення області використання біометричних технологій можна розглядати область перманентного обстеження емоційного стану людини з використанням різних біометричних даних.

Список літератури

1. Лакин Г.Ф., «Биометия», -М.: Высш. Шк., 1990 г., 352 с.
2. Чарли Стюарт, Биометрия и ситемы информационной безопасности, «it&securityNEWS», -К.: Ай-Эс-Эс Пресс, 2010, с. 8.
3. Advanced biometric solutions, USA, “Biometric technologies”. [Электронный ресурс] -Режим доступу:
4. <http://www.bioclinkusa.com/teclnology/biomctric.php>.
5. B. Miller, Vital signs of identity, IEEE Spectrum, pp. 22-30, 2004.
6. Ben-Arie J., Nandy D.A. Volumetric/Iconic Frequency Domain Representation for objects With Application for Pose Invariant Face Recognition. Analysis and Machine Intelligence, IEEE Spectrum, pp. 80-87, 2003.
7. Bruneli R., Poggio T. Face Recognition, Features versus Templates, IEEE Trans. [Электронный ресурс] - Режим доступу:
8. <http://www.darpa.mil/iao/HID.htm>.
9. Wikipedia, USA, «Биометрия», [Электронный ресурс] - Режим доступу:
10. <http://ru.wikipedia.org/wiki/Биометрия>
11. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в современных компьютерных системах, 2-е издание: М.: Радио и связь, 2001, 290 с.
12. Кухарев Г. А. Биометрические системы: Методы и средства идентификации личности человека. – СПб.: Политехника, 2001. – 240 с.
13. A. Bromme “A classification of biometric signatures” 2003 International Conference on Multimedia and Expo - Volume 3, pp. 17-20, 2003.
14. Hu Jian-feng “Comparison of Different Classifiers for Biometric System Based on EEG Signals”, [2010 Second International Conference on Information Technology and Computer Science](#), pp. 288-291, 2010.
15. Дубчак О.В., Підгайна К.І., Порівняльний аналіз сучасних біометричних методів аутентифікації, «Захист інформації в інформаційно-комунікаційних системах», -К: НАУ, 2010 р., с. 17.
16. Хоанг Чунг Киен. Методы биометрической идентификации, преимущества и области применения биометрических систем. Сборник научных трудов по материалам 56-ой научно-технической конференции. - М.: МИРЭА, 2007. с. 80-84.
17. Брюхомицкий Ю.А., Казарин М.Н. «Исследование биометрических систем динамической аутентификации пользователей ПК по рукописному и клавиатурному почеркам» -Таганрог: Изд-во ТРТУ, 2004. - 38с.
18. Vladimir Lobantsov, Ekaterina Kubysheva. Новое поколение биометрических паспортов и решений для охраны границ. Biometrics in Aviation Security 2005 Conference Moscow, Russia. [Электронный ресурс] - Режим доступу:
19. http://police.sko.kz/rus/udp/drivers_license.htm.
20. Хоанг Чунг Киен. Анализ и выбор биометрических параметров для создания единой системы удостоверяющих документов с учетом особенностей их использования в СРВ. М.: Научкоёмкие технологии. - №12,2008. - с. 61-69.
21. Хоанг Чунг Киен, Чан Конг Тан. Математическое обеспечение в обработке биометрической информации для создания биометрических паспортов в СРВ. Труды Т32(1) 2008 ИСАРАН с. 267-283.
22. R. Clarke. Human identification in information systems: Management challenges and public policy issues. Information Technology and people. December 1994, pp. 32-35.
23. Galuskin A.I., Utjamishev R.L., Kalashikov V.P. Requirements for planning and testing of equipment for automatic medical diagnosis, Biomedicine, -Dresden: UnD, 1973, pp. 45-49.
24. Biometric technologies, “New Biotech”, Russia, [Электронный ресурс] - Режим доступу:
25. Biometricsguide.ru
26. Брюхомицкий Ю.А., М.Н. Казарин Тестирование биометрических систем контроля доступа Россия, г. Таганрог, ТРТУ, 2004, 78 с.
27. Иванов А.И. Биометрические и нейросетевые механизмы связи с криптографическими механизмами информационной безопасности / Труды научно-технической конференции «Безопасность информационных технологий», - Пенза: ПГУ, 2003, с. 88.
28. Иванов А.И. Биометрические идентификация личности по динамике подсознательных движений, - Пенза: ПГУ, 2000г, 188 с.
29. Национальные стандарты Российской Федерации [Электронный документ] - Режим доступу:
30. <http://lgost.net.ru/doc-7928.html>.
31. Иванов А.И. Нейросетевые алгоритмы биометрической идентификации личности, -М: Высш. Шк., 2004, 130 с.
32. Хоффман, Современные методы защиты информации. М: Радио и св., 1980, 330 с.
33. Security for all, “New Tech’s”, USA, [Электронный ресурс] - Режим доступу:
34. <http://www.sec4all.net/statea287.html>
35. Филлипс П. Д., Мартин Эл., Уилсон Л. Пржибоски М., Введение в оценку биометрических систем, Открытые системы, -М: Высш.шк., 2000, с. 80-88.
36. Хоанг Чунг Киен. Обзор структуры систем биометрической идентификации личности. Доклады IX научного симпозиума, Вьетнамская научно-техническая ассоциация в РФ.- Москва 3-2007, с. 334-343.

37. Иванов А.И. Объединение протоколов аутентификации / Защита информации., – М: Конфидент., 2002 г., с. 100-110.
38. V. Kanhangad , A. Kumar , D. Zhang, Combining 2D and 3D hand geometry features for biometric verification, [2009 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops](#), pp. 39-44
39. Hataichanok Saevanee , Pattarasinee Bhatarakosol , User Authentication Using Combination of Behavioral Biometrics over the Touchpad Acting Like Touch Screen of Mobile Device, [2008 International Conference on Computer and Electrical Engineering](#), Issue Date:December 2008, pp. 82-86
40. P. Sengottuvelan , A. Wahi, Analysis of Living and Dead Finger Impression Identification for Biometric Application, [2007 International Conference on Computational Intelligence and Multimedia Applications](#), Issue Date:December 2007, pp. 466-470
41. Alfredo Grunwald de la Cuesta , Jianguo Zhang , Paul Miller, Biometric Identification Using Motion History Images of a Speaker's Lip Movements, [2008 International Machine Vision and Image Processing Conference](#), Issue Date:September 2008, pp. 83-88
42. Maycel-Isaac Faraj , Josef Bigun, Synergy of Lip-Motion and Acoustic Features in Biometric Speech and Speaker Recognition, [IEEE Transactions on Computers](#), Issue Date:September 2007, pp. 1169-1175
43. Ramesha K. , Srikanth N. , K.B. Raja , Venugopal K.R. , L.M. Patnaik, Advanced Biometric Identification on Face, Gender and Age Recognition, [2009 International Conference on Advances in Recent Technologies in Computing](#), Issue Date:October 2009, pp. 23-27
44. Jalal A. Nasiri , M. Amir Moulavi , H. Sadoghi Yazdi , M. Rouhani , A. Eshghi Shargh, A PSO Tuning Approach for Lip Detection on Color Images, [2008 Second UKSIM European Symposium on Computer Modeling and Simulation](#), Issue Date:September 2008, pp. 278-282
45. Xiangqian Wu , Enying Gao , Youbao Tang , Kuanquan Wang, A Novel Biometric System Based on Hand Vein, [2010 Fifth International Conference on Frontier of Computer Science and Technology](#), Issue Date:August 2010, pp. 522-526
46. Venkatesh N , Srinivasan Jayaraman, Human Electrocardiogram for Biometrics Using DTW and FLDA, [2010 20th International Conference on Pattern Recognition](#), Issue Date:August 2010, pp. 3838-3841
47. V.S. Meenakshi , G. Padmavathi, Security Analysis of Hardened Retina Based Fuzzy Vault, [2009 International Conference on Advances in Recent Technologies in Communication and Computing](#), Issue Date:October 2009, pp. 926-930
48. Zhiyi Qu , Tao Wang , Ruidong Zheng , Yanmin Liu, An Identity Authentication System Based on Face Biometrics and Eye Localization, [2010 International Conference on Measuring Technology and Mechatronics Automation](#), Issue Date:March 2010, pp. 479-483

Рецензент: Литвиненко О.Є.
Надійшла 30.09.2010