DOI: 10.6084/m9.figshare.9788444
УДК 004.93; 004.056

Шабала Євгенія Євгенівна
Кандидат технічних наук, доцент кафедри кібербезпеки та комп'ютерної інженерії, *orcid.org/0000-0002-0428-9273*
Київський національний університет будівництва і архітектури, Київ
Клюєва Вікторія Василівна
Асистент кафедри кібербезпеки та комп'ютерної інженерії, *orcid.org/0000-0003-1267-0717*
Київський національний університет будівництва і архітектури, Київ

БІОМЕТРИЧНІ МЕТОДИ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ НА ТЕРИТОРІЮ АЕРОПОРТУ

Анотація. *На сьогодні на стан глобальної безпеки в авіаперевезеннях впливає ряд негативних процесів, які призвели, зокрема, до значного зростання терористичних загроз. Реалізація цих загроз завдає значної шкоди як на національному рівні, так і на міжнародній арені. Авіаційна галузь потребує особливого ставлення до питань безпеки. Це спонукає до розуміння необхідності вирішення нагальної проблеми з метою мінімізації, ліквідації та попередження загроз різних типів із залученням біометричних систем ідентифікації особистості та контролю доступу до аеропорту. Технологія розпізнавання осіб досягла великих успіхів в останні роки. Тепер комп'ютери можуть ідентифікувати осіб, які не перебувають в зоні з добрим освітленням і широким радіусом огляду. Бічного огляду рухомого зображення вже може бути достатньо для штучного інтелекту, щоб ідентифікувати особистість. Розгляуто відомі біометричні методи захисту від несанкціонованого доступу та запропоновано використання алгоритму визначення контурів Канні, як одного з найефективніших методів розпізнавання особистості.*

Ключові слова: біометрія; методи захисту; дактилоскопія; алгоритм Канні; оператор Собеля

Актуальність та аналіз проблеми

З кожним роком у світі зростає кількість надзвичайних ситуацій, які виникають на території аеропорту, більшість яких викликані терористичними актами. Тому нині гостро постає питання розроблення більш сучасних методів і засобів побудови автоматизованих систем комплексного захисту аеропорту і прилеглих до нього зон [1; 2].

Виклад основного матеріалу

Підсистема ідентифікації особистості передбачає автоматизовану систему, яка включає пакет додатків, що забезпечує біометричну ідентифікацію особистості за допомогою комбінації таких методів: ідентифікації особистості за дактиловідбитком; ідентифікації особистості за обертонами голосу; ідентифікації особистості за характерними ознаками зображення обличчя особи [3].

Єдиним беззаперечним способом ідентифікації на сьогодні є виявлення за допомогою технічних пристроїв біологічних характеристик особи та перевірка їх відповідності заздалегідь сформованим особистим шаблонам. Для систем захисту інформації передусім цінність являють статичні методи, що фіксують незмінні характеристики особи, притаманні їй від народження [4].

Дактилоскопічний метод. Дактилоскопія – метод ідентифікації людини за відбитками пальців, спрямований на визначення рисунка шкіри. Відбиток, отриманий за допомогою спеціального сканера, датчика або сенсора, перетворюється в цифровий код і порівнюється з раніше введеним еталоном. Переваги доступу за відбитком пальця – простота використання, зручність і надійність. Процес ідентифікації триває секунди і не вимагає зусиль [5].

На відбитку пальця є мінуції – унікальні для кожного узору точки зміни структури папілярних ліній – їх закінчення, роздвоєння, розрив тощо. Система визначає для кожної мінуції її координати і орієнтацію папілярних ліній у цій точці. Еталонний відбиток містить приблизно 70 мінуцій. Оцінку K результату порівняння відбитків та еталону можна обчислювати за формулою:

$$K = \frac{D^2 \cdot 100\%}{pq},$$

де D – кількість збігів мінуцій зчитаного та еталонного відбитків; p, q – кількість мінуцій еталону та відбитку [3].

Дактилоскопічні датчики бувають різних типів:

– оптичні;

– оптико-волоконні;
– роликові;
– напівпровідникові;
– зарядові (capacitive – DC);
– ємнісні (capacitive – AC);
– термочутливі;
– радіочастотні;
– ультразвукові тощо.

Відповідно різняться їх експлуатаційні характеристики та вартість [4].

Розпізнавання за голосом. Аутентифікація людини за голосом – один з традиційних способів розпізнавання особи. Оскільки цей метод безконтактний і не вимагає від людини особливих зусиль, ведуться роботи зі створення голосових замків і систем обмеження доступу до інформації. Інтерес у цій області пов'язаний ще й з прогнозами повсюдного впровадження голосових інтерфейсів. Принцип дії базується на такому: кожен сплеск голосового сигналу відповідає деякому фрагменту мовлення. Це може бути одна літера, їх поєднання або коротке слово. Після фрагментації слідує оцифрування фрагментів відповідно до частотних показників. Оскільки голосова ідентифікація не потребує контакту і не вимагає від людини особливих зусиль, ведуться роботи зі створення голосових замків і систем обмеження доступу до інформації.

Ідентифікація за формою обличчя – за допомогою відеокамери будується 2D- або 3D-образ обличчя, при цьому виявляються контури брів, очей, носа, губ, підборіддя, вух та ін. Потім між ними обчислюється відстань і будується множина варіантів залежно від повороту обличчя, нахилу, зміни міміки. Достовірність такого порівняння оцінюється у 86-93%. Для сканування потрібна камера високої роздільної здатності, щоб відстань між центрами зіниць була еквівалентна 200 пікселям, та відповідне освітлення і певна відстань до обличчя [6; 8].

Перешкодою до точної ідентифікації може стати накладання гриму або суттєва зміна частини обличчя (пластична хірургія).

Ідентифікація за термограмою обличчя – базується на неповторності розподілу на обличчі кровоносних судин, які виділяють тепло. Для сканування необхідна термочутлива камера інфрачервоного діапазону. Система може працювати в цілковитій темряві, на результати розпізнання не впливають переохолодження обличчя або його перегрів, природне старіння шкіри, пластичні операції, грим, накладні елементи. Цей метод, на відміну від попереднього, дає змогу розрізняти близнят, його вважають ефективнішим за 2D- або 3D-сканування.

Малюнок райдужної оболонки ока. Людська райдужка має специфічну структуру і містить багато текстури інформації. Просторові структури, які спостерігаються в райдужці, унікальні для кожного індивіда. Кольорові ознаки райдужної оболонки недостатньо надійні, оскільки вони можуть змінюватися з віком. Основна проблема при побудові системи ідентифікації – ефективне виділення і подання текстурной інформації, що містяться в райдужній оболонці. Є безліч різних методів отримання зображення райдужної оболонки. Більшість пристроїв для зйомки райдужки не мають пристрою наведення, але замість цього використовується візуальний зворотний зв'язок, який базується на використанні дзеркала або відеозображення. Зворотний зв'язок дає змогу користувачеві правильно помістити око в поле зору камери з малим кутом зору. Фокус встановлюється в реальному часі (швидше, ніж інтервал між кадрами) шляхом вимірювання сумарної енергії високочастотної частини двовимірного спектра Фур'є для кожного з кадрів, і максимізації цієї енергії шляхом переміщення лінз об'єктива або шляхом звуковий зворотного зв'язку із суб'єктом [Фесенко]. У порівнянні з іншими біометричними методами, ідентифікація за райдужкою ока людини є більш ефективною, стабільнішою і надійною.

Для досягнення поставленої мети пропонується використовувати алгоритм визначення контурів Канні, який складається з таких кроків: згладжування; визначення градієнта; пошук локальних максимумів градієнта; подвійна порогова фільтрація з трасуванням. Розглянемо кожний крок детальніше.

Першим кроком алгоритму Канні для зменшення шумів та підвищення якості визначення контурів зображення є згладжування (або розмиття) цифрового зображення. Згладжування досягається завдяки послабленню високих частот цифрового зображення в частотній ділянці.

Низькочастотна фільтрація цифрового зображення здійснюється ядром Гауса:

$$S = \left[s_{ij} \right]_{i=1,\, j=1}^{n,m};$$

$$h_{ij} = \frac{1}{2\pi\sigma^2} e^{\frac{-(i^2+j^2)}{2\pi\sigma^2}},$$

де i, j, s — значення яскравості пікселя з координатами i, j ; σ — масштаб гауссіана. Для фільтрації пропонується використовувати лінійний фільтр з апертурою 5 5 та σ =1,4.

$$H = \begin{pmatrix} 0{,}0121 & 0{,}0261 & 0{,}0337 & 0{,}0261 & 0{,}0121 \\ 0{,}0261 & 0{,}0561 & 0{,}0724 & 0{,}0561 & 0{,}0261 \\ 0{,}0337 & 0{,}0724 & 0{,}0935 & 0{,}0724 & 0{,}0337 \\ 0{,}0261 & 0{,}0561 & 0{,}0724 & 0{,}0561 & 0{,}0261 \\ 0{,}0121 & 0{,}0261 & 0{,}0337 & 0{,}0261 & 0{,}0121 \end{pmatrix}.$$

Зображення після фільтрації $F = \left[f_{ij} \right]_{i=1,\, j=1}^{n,m}$ отримують в результаті згортки:

$$F = S * H,$$

де * – оператор двовимірної згортки; S – матриця цифрового зображення; H – лінійний фільтр (1).

Визначення градієнта. Наступним кроком алгоритму Канні є визначення градієнта цифрового зображення, тобто напрямку та норми максимальної швидкості зміни яскравості в кожній точці цифрового зображення [4; 9; 10]. Розрахунок градієнта зображення після фільтрації F виконується за допомогою оператора Собеля [4] з масками M_x та M_y:

$$M_x = \begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix}, \quad M_y = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix}.$$

Складові градієнтів $G_x = \left[g_{x_{ij}} \right]_{i=1,\, j=1}^{n,m}$ та $G_y = \left[g_{y_{ij}} \right]_{i=1,\, j=1}^{n,m}$ за просторовими кординатами:

$$G_x = F * M_x;$$

$$G_y = F * M_y.$$

Тоді норма $G = \left[g_{x_{ij}} \right]_{i=1,\, j=1}^{n,m}$ та кут $A = \left[\alpha_{x_{ij}} \right]_{i=1,\, j=1}^{n,m}$ градієнта цифрового зображення:

$$g_{ij} = \sqrt{g_{x_{ij}}^2 + g_{y_{ij}}^2};$$

$$\alpha_{ij} = arctg\left(\frac{g_{x_{ij}}}{g_{y_{ij}}} \right).$$

Пошук локальних максимумів градієнта. В результаті застосування оператора Собеля в ділянці постійної яскравості цифрового зображення, тобто ділянці, де немає різких перепадів або контурів, отримують малі або близькі до нуля за модулем вектори градієнта. У точках, що відносяться до контурів, норма вектора значно більша, а напрямок – у бік збільшення яскравості зображення. Тому точки цифрового зображення, в яких досягається локальний максимум модуля градієнта в напрямку вектора градієнта цифрового зображення відносять до контурів, позначають Kij та визначають за виразом:

$$K_{ij} = \begin{cases} (G_{ij} = Max(G_{ij-1}, G_{ij}, G_{ij+1}) ? G_{ij} : 0, якщо\, \tilde{\alpha}_{ij} = 0^\circ; \\ (G_{ij} = Max(G_{i+1\,j-1}, G_{ij}, G_{i-1\,j+1}) ? G_{ij} : 0, якщо\, \tilde{\alpha}_{ij} = 45^\circ; \\ (G_{ij} = Max(G_{i-1\,j}, G_{ij}, G_{i+1\,j}) ? G_{ij} : 0, якщо\, \tilde{\alpha}_{ij} = 90^\circ; \\ (G_{ij} = Max(G_{i-1\,j-1}, G_{ij}, G_{i+1\,j+1}) ? G_{ij} : 0, якщо\, \tilde{\alpha}_{ij} = 135^\circ, \end{cases}$$

де Max(x, y, z) – операція визначення максимального з елементів x, y, z .

Вираз $? a : b$ видає значення a, якщо попередній вираз приймає значення “істина”, і значення b у іншому випадку; $\tilde{\alpha}_{ij}$ – кут вектора градієнта в кожній точці цифрового зображення після квантування, проведеного таким чином:

$$\tilde{\alpha}_{ij} = \begin{cases} \left[\frac{\alpha_{ij}}{45^\circ} \right] \cdot 45^\circ, \; якщо\, 0^\circ \le \alpha_{ij} < 157{,}5^\circ; \\ \left[\frac{\alpha_{ij} - 180^\circ}{45^\circ} \right] \cdot 45^\circ, \; якщо\, 157{,}5^\circ \le \alpha_{ij} < 337{,}5^\circ; \\ \left[\frac{\alpha_{ij} - 360^\circ}{45^\circ} \right] \cdot 45^\circ, \; якщо\, 337{,}5^\circ \le \alpha_{ij} < 360^\circ. \end{cases}$$

Подвійна порогова фільтрація з трасуванням. Останнім кроком алгоритму Канні є подвійна порогова фільтрація з трасуванням ділянки невизначеності, метою застосування якого є уточнення отриманих на попередньому кроці контурів шляхом використання конкретних значень верхнього T_H та нижнього T_L порогів:

$$\tilde{K}_{ij} = \begin{cases} 1, якщо\, K_{ij} \ge T_H; \\ 1, якщо\, (T_L < K_{ij} < T_H)\, \&\, \& \\ (K_{i-1\,j-1} > T_H \| K_{i-1\,j} > T_H \| K_{i-1\,j+1} > T_H \| K_{ij-1} > T_H \| \\ K_{ij+1} > T_H \| K_{i+1\,j-1} > T_H \| K_{i+1\,j} > T_H \| K_{i+1\,j+1} > T_H); \\ 0, якщо\, K_{ij} \le T_{L.} \end{cases}$$

Точки, що задовольняють умову $K_{ij} \ge T_H$, достовірно належать контуру цифрового зображення. Точки, що потрапили до ділянки невизначеності, тобто задовольняють умову $T_L < K_{ij} < T_H$, але розташовані в безпосередній близькості до одного з вертикальних, горизонтальних або діагональних напрямків, також визначаються як точки, що належать результуючим контурам цифрового зображення [7].

Висновок

У результаті аналізу відомих біометричних методів захисту від несанкціонованого доступу на територію аеропорту запропоновано використання комплексу біометричних методів визначення особистості разом з інтелектуальним відеоспостереженням, методів оброблення відеоінформації, що дасть змогу відслідковувати об'єкти, які цікавлять персонал аеропорту, аналізувати траєкторії руху й поведінку людей, реєструвати потенційно небезпечних осіб та в автоматичному режимі проводити їх ідентифікацію.

Список літератури

1. Васюхин М.И. Основы интерактивных навигационно-управляющих геоинформационных систем: мо- ногр. [Текст] / М.И. Васюхин – Лира. − 2006. − 536 с.

2. Оленин Ю.А. Проблемы комплексного обеспечения охранно-территориальной безопасности и физической защиты особо важных объектов [Текст] / Ю.А. Оленин // Охранные системы. – 2002 . − № 3 (27). − С. 7 − 26.

3. Васюхін М.І., Гулевець В.Д., Головко Б.Б. Підвищення рівня безпеки аеропорту та прилеглих до нього зон / Н.М. Лобанчикова // Вісник НАУ. – 2009. – № 1. – С. 205–208.

4. Чередниченко В. Б. Біометричні методи у системах захисту інформації [Текст] / В.Б. Чередниченко, К.Е. Чередниченко // Системи обробки інформації. – 2012. – 4(1) . – С. 145 – 148.

5. Мороз А.О. Біометричні технології. Методи дактилоскопії [Текст] / А.О. Мороз // Математичні машини і системи. – 2011. – № 3. – С. 58 – 65.

6. Мороз А.О. Біометричні технології ідентифікації людини. Огляд систем. [Текст] / А.О. Мороз // Математичні машини і системи. – 2011. – №1. – С. 39 – 45.

7. Трифонова К.О. Визначення контурів райдужної оболонки ока для системи біометричної ідентифікації людини [Текст] / К.О. Трифонова, Е.І. Гришикашвілі, А.Р. Агаджанян // Праці Одеського політехнічного університету. – 2015. – 1(45) . – С. 107 – 112.

8. Canny, J. A Computational Approach to Edge Detection / J. Canny // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 1986. – Vol. 8, No. 6. – PP. 679. – 698..

9. Гришенкова Н. П. Обзор методов идентификации человека по радужной оболочке глаза [Текст] / Н.П. Гришенкова, Д.Н. Лавров // Математические структуры и моделирование. – 2014. – № 1(29). – С. 43 – 64.

10. Гонсалес Р. Цифровая обработка изображений [Текст] / Р. Гонсалес, Р. Вудс; пер. с англ. П.А. Чочиа // Техносфера. – 2006. – 1070 с.

Стаття надійшла до редколегії 18.03.2019

Шабала Евгения Евгеньевна
Кандидат технических наук, доцент кафедры кибернетической безопасности и компьютерной инженерии, *orcid.org/0000-0002-0428-9273*
Киевский национальный университет строительства и архитектуры, Киев
Клюева Виктория Васильевна
Ассистент кафедры кибербезопасности и компьютерной инженерии, *orcid.org/0000-0003-1267-0717*
Киевский национальный университет строительства и архитектуры, Киев

БИОМЕТРИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА НА ТЕРРИТОРИЮ АЭРОПОРТА

Аннотация. *В настоящее время на состояние глобальной безопасности в авиаперевозках влияет ряд негативных процессов, которые привели, в частности, к значительному росту террористических угроз. Реализация этих угроз наносит значительный ущерб как на национальном уровне, так и на международной арене. Авиационная отрасль требует особого отношения к вопросам безопасности. Это побуждает к пониманию необходимости решения насущной проблемы с целью минимизации, ликвидации и предупреждения угроз различных типов с привлечением биометрических систем идентификации личности и контроля доступа в аэропорт. Технология распознавания лиц достигла больших успехов в последние годы. Теперь компьютеры могут идентифицировать лица, не стоящие в зоне с хорошим освещением и широким радиусом обзора. Бокового обзора движущегося изображения уже может быть достаточно для искусственного интеллекта, чтобы идентифицировать индивидуальность. Рассмотрены существующие биометрические методы защиты от несанкционированного доступа и предлагается использование алгоритма определения контуров Канни, как одного из эффективных методов распознавания личности.*

Ключевые слова: биометрия; методы защиты; дактилоскопия; алгоритм Канни; оператор Собеля

Shabala Yevheniia
Ph.D., associate professor, Department of cyber security and Computer Engineering, *orcid.org/0000-0002-0428-9273*
Kyiv National University of Construction and Architecture, Kiev
Klyuyeva Victoriya
Assistant, Department of Cybersecurity and Computer Engineering, *orcid.org/0000-0003-1267-0717*
Kyiv National University of Construction and Architecture, Kyiv

BIOMETRIC METHODS OF PROTECTION AGAINST UNPASSED ACCESS TO THE AIRPORT TERRITORY

Abstract. *At present, a number of negative processes affect the global security situation in air transport, which led, in particular, to a significant increase in terrorist threats. The realization of these threats causes significant damage both at the national level and internationally. The aerospace industry requires special attention to safety issues. This leads to an understanding of the need to address the urgent problem in order to minimize, eliminate and prevent the various types of threats involving biometric identification systems and access control to the airport. The technology of recognizing individuals has made great strides in recent years. Now computers can identify individuals who are not in the field with good illumination and wide viewing radius. A side view of a moving image may already be sufficient for artificial intelligence to identify a feature. The article examines the existing biometric methods of protection against unauthorized access and proposes the use of the algorithm for determining the contours of Canny as one of the most effective methods of personality recognition.*

Keywords: biometrics; methods of protection; fingerprinting; Canny's algorithm; Sobel's operator

References

1. Vasyukhin, M.I. (2006). Basics of interactive navigational and controlling geoinformation systems: monographs. Lira. 536.

2. Olenin, Y.A. (2002). Problems of integrated provision of security and territorial security and physical protection of especially important objects. Security systems, 3 (27), 7-26.

3. Vasiukhin, M.I., Gulevets, V.D., Golovko, B.B. (2009). Improvement of the security level of the airport and its adjoining zones. Bulletin of the NAU, 1, 205-208.

4. Cherednichenko, V.B., Cherednichenko, K.E. (2012). Biometric Methods in Information Security Systems. Systems of Information Processing, 4 (1), 145-148.

5. Moroz, A.O. (2011). Biometric Technologies. Methods of fingerprinting, 3, 58-65.

6. Moroz, A.O. (2011). Biometric human identification technologies. System overview. Mathematical Machines and Systems. Institute of Mathematical Machines and Systems NAU of Ukraine, 1, 39-45.

7. Trifonova, K.O., Grishikashvili, E.I., Aghajanyan, A.R. (2015). Determination of the iris of the iris for a biometric human identification system. Proceedings of the Odessa Polytechnic University, 1 (45), 107-112.

8. Canny, J.A. (1986). Computational Approach to Edge Detection, IEEE Transactions on Pattern Analysis and Machine Intelligence, 8 (6), 679-698.

9. Gryshenkova, N.P. (2014). A review of methods for identifying a person through the iris of the eye. Mathematical Structures and Modeling, 1 (29), 43-64.

10. Gonzalez, R. (2006). Digital Image Processing. Trans from English PAS Chochia. Technosphere, 1070.

Посилання на публікацію

APA *Shabala, Ye. & Klyuyeva, V. (2019). Biometric methods of protection against unpassed to the airport territory. Management of Development of Complex Systems, 38, 51 – 55, [in Ukrainian], dx.doi.org\10.6084/m9.figshare.9788444.*

ДСТУ *Шабала Є.С. Біометричні методи захисту від несанкціонованого доступу на територію аеропорту [Текст] / Є.С. Шабала, В.В. Клюєва // Управління розвитком складних систем. – 2019. – № 38. – С. – 51 – 55, dx.doi.org\10.6084/m9.figshare.9788444.*