

ЗАХИСТ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ШЛЯХОМ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

І.В. Гуменюк, К.В. Сметанін, О.В. Некрилов

Житомирський військовий інститут імені С.П. Корольова, Україна

E-mail: ig_gum@ukr.net

Protection against unauthorized access to information and telecommunications systems by biometric identification of users

The article proposes a method of blocking access to information and telecommunication systems, which is based on the algorithm of biometric identification/authentication by face geometry. It is shown that the application of the proposed method allows you to quickly identify the facts of unauthorized access by insider users of information and telecommunications systems and timely prevent information leaks.

Останні події, які спостерігаються на світовій арені, супроводжуються процесом перерозподілу зон впливу у технологічному та економічному просторі, розвитком інформаційних технологій (ІТ), які породжують нові способи отримання інформації. У зв'язку з цим, забезпечення захисту секретної інформації є актуальним питанням та вимагає від держав, незалежно від їх розвитку, постійного зміцнення національної безпеки, а також спроможності протидіяти загрозам і мінімізувати ризики реального витоку важливих відомостей та даних. При цьому важливо враховувати ефективність роботи автоматизованих підсистем управління доступом та захисту даних для забезпечення безпеки певної системи інформаційної інфраструктури, у тому числі інформаційно-телекомунікаційних систем (ІТС) [1].

Виходячи з даних передумов, сформульовано мету даної роботи, яка полягає у розробленні методу біометричної ідентифікації/аутентифікації і його застосуванні при вирішенні завдань блокування доступу до ІТС інсайдер-користувачами.

На даний момент розвитку ІТ паролльні, які базуються на унікальній персональній інформації, та атрибутивні методи ідентифікації втрачають свою актуальність. Важливою проблемою цих методів є відсутність функціоналу для виявлення підміни авторизованого “легітимного” користувача. Порівняно з цими методами, біометричні характеристики користувача, як спосіб аутентифікації, можуть гарантувати підвищений рівень безпеки, враховуючи невід’ємність біометричних даних конкретної особи [2].

Розроблюваний метод включає такі кроки:

Крок 1. Виявлення та локалізація геометрії обличчя. У даній роботі використано алгоритм Віоли-Джонса. Обраний метод є кращим рішенням, порівняно з іншими алгоритмами, за критеріями ефективності та оперативності розпізнавання обличчя [3].

У загальному вигляді алгоритм здійснює пошук обличчя та її контури (геометрію) за допомогою сканування вікна. Відеозображення, на якому здійснюється пошук об'єкта, подається у вигляді двовимірної матриця

розмірністю (x, y) , кожен піксель якої приймає значення для одотонного зображення $[0; 255]$ та для кольорового зображення формату RGB – $[0; 255^3]$.

Крок 2. Нормалізація зображення за масштабом, яскравістю тощо.

Крок 3. Обчислення набору базових ознак (характеристик) зображення.

Ознаки (примітиви) Хаара – це відображення f :

$$\chi \Rightarrow D_f \quad (1)$$

де D_f – множина допустимих значень ознаки.

За умови, що ознака f_1, \dots, f_n визначена, вираз (1) прийме вигляд $\chi \Rightarrow \{f_1, \dots, f_n\}$, який називається ознакою опису об'єкта.

У процесі пошуку обчислювати всі ознаки Хаара практично не можливо, відповідно класифікатор повинен враховувати лише певну підмножину важливих ознак. Таким чином, для досягнення ефективності функціонування алгоритму та надійної роботи необхідно проводити інтелектуальне навчання класифікатора.

Крок 4. Порівняння обчислених ознак з еталонними.

Загальний алгоритм методу наведено на рис. 1.



Рис. 1. Алгоритм блокування доступу інсайдер-користувачами до ІТС.

Верифікацію запропонованого методу проведено з використанням розробленого авторами спеціалізованого програмного забезпечення [4] на відеозображеннях, отриманих за допомогою відеокамери Infinity SR-DN530SD з роздільною здатністю відеопотоку HDTV 720p.

Умови проведення верифікації:

- до бази даних занесено 4 записи шаблонних користувачів ІТС (кожен запис містить до 30 зображень, прізвище, ім'я, унікальний номер тощо);
- природня (достатня та недостатня) освітленість приміщення – 100 – 400 люкс;
- мінімальна відстань між засобом відеоспостереження та об'єктом ідентифікації складає 0.5 м, максимальна – 2.5;
- кількість експериментів дослідження – 200;
- тестовими користувачами обрано одного з авторів наукової роботи (його дані занесені до БД) та двох інших користувачів, один з яких авторизований;
- одиночна (персональна) та групова ідентифікація.

Результати верифікації наведено на рис. 2–3.

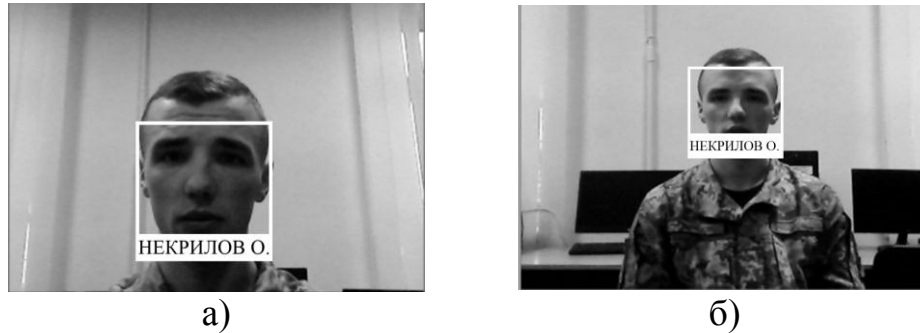


Рис.2. Персональна ідентифікації при достатній освітленості:
а) відстань 0.5 (м); б) відстань 2 (м).



Рис. 3. Групова ідентифікація при достатній освітленості:
а) відстань 0.5 (м); б) відстань 2 (м).

Особливість методу інтелектуальної біометричної ідентифікації/аутентифікації користувачів ІТС полягає у можливості його реалізації у мобільних додатках, що особливо актуально в умовах інформатизації сьогодення. Практичне значення одержаних результатів полягає в можливості: впровадження методу в сучасні системи контролю та пропускового режиму ОІД; інтеграції програмного забезпечення в системи аутентифікації засобів обчислювальної техніки, у тому числі ПЕОМ; блокування доступу до інформації та засобів її обробки для несанкціонованих інсайдер-користувачів тощо.

Література

1. Гуменюк І. В., Басараба М. С., Некрилов О. В. Біометрична ідентифікація у кіберпросторі на основі розпізнавання обличчя // Проблеми теорії та практики інформаційного протидіювання в умовах ведення гібридних війн: тези доповідей наук.-практ. конф. 24 – 25 жовтня 2019 р. Житомир : ЖВІ, 2019. С. 205–207.
2. Нечипоренко О. В., Корпань Я. В. Біометрична ідентифікація і автентифікація особи за геометрією обличчя // Вісник Хмельницького національного університету. Технічні науки. № 4, 2016. С. 133–138.
3. Немкова О. А. Біометрична ідентифікація у кіберпросторі // Системи обробки інформації. Випуск 7 (132), 2015. С. 118–121.
4. “Спеціалізоване програмне забезпечення біометричної ідентифікації/аутентифікації користувачів інформаційно-телекомунікаційних систем на основі геометрії обличчя”, Заявка про реєстрацію авторського права на твір № АПС 95-19. Дата затвердження заявки 28.10.2019.