Висновки: Працюючи над роботою, було досліджено принцип роботи алгоритму, його характеристики, спосіб шифрування та дешифрування даних, його криптостійкість і, як наслідок, доцільність практичного використання.

У ході роботи було створено програмний продукт з графічною оболонкою, який реалізовує заданий алгоритм шифрування з розміром слова в 32 біти, 100 раундами та 128-байтовим ключем.

Література

1. Методи криптографії. 2017. URL : https://www.dkws.org.ua/article.php?id=80
2. Алгоритм шифрування RC5. 2013. URL : https://studbooks.net/1590228/informatika/algoritm_shifrovaniya
3. RC5. 2015. URL : https://ru.wikipedia.org/wiki/RC5

УДК 004.56.53

АВТОМАТИЗАЦІЯ КОНТРОЛЮ ДОСТУПУ НА ОСНОВІ МЕРЕЖЕВИХ ПРОГРАМ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ ЛЮДИНИ

Т. О. Лукашук

Контроль доступу на основі мережевих програм розпізнавання обличчя людини відноситься до біометричних методів контролю доступу, над якими сьогодні працюють передові організації світу, такі як: Amazon, Google, IBM і т. д. Біометричні методи розпізнавання людини доволі давно використовуються правоохоронними органами, для ідентифікації людей. Ідея для створення методів аутентифікації та авторизації на основі біометричних даних людини на сьогоднішній день має доволі велике поширення, наприклад в багатьох смартфонах на сьогоднішній день використовуються оптичні сканери відбитку пальця для авторизації користувачів, також використовуються методи розпізнавання обличчя, за допомогою його геометрії, які наприклад в останній моделі iPhone X, називаються FaceID. Біометричні системи авторизації – це зручно, швидко та надійно. Про надійність цих систем, говорить те, що їх використовують в Пентагоні. До недавніх пір головним фактором, який заважав цим системам розвиватись – це була їхня ціна, але з розвитком технологій на сьогоднішній день ситуація змінилась.

Біометричні системи аутентифікації:

Біометрична система аутентифікації – це система аутентифікації, яка використовує для підтвердження особистостей їхні біометричні данні. Процес доказу і перевірки належності заявленого користувачем імені, через представлення користувачем свого біометричного зразку, шляхом перероблення цього зразка відповідно до заранння визначеного протоколу.

Біометричні системи аутентифікації поділяються на 2 види: Статичні методи та Динамічні методи.

Статичні методи основані на фізіологічних характеристиках людини, які присутні від народження до смерті, які знаходяться при людині на протязі всього життя, і які не можуть бути втрачені, вкрадені або скопійовані. Наприклад: аутентифікація по відбитку пальця, геометрії руки, геометрії лиця, термограмі лиця.

Динамічні методи біометричної аутентифікації та ідентифікації основані на поведінкових характеристиках людей, тобто основані на характерних для підсвідомих рухів в процесі відтворення або повторення якої-небудь звичайної дії. Наприклад: Аутентифікація по голосу чи почерку.

Біометричні системи аутентифікації повинні відповідати 5 параметрам:

1) Всезагальність: Даний признак повинен бути присутній у всіх людей без виключення.

2) Унікальність: Біометрія відкидає існування двох людей з однаковими фізичними та поведінковими параметрами.

3) Постійність: Для коректної аутентифікації необхідно постійність в часі.

4) Вимірюваність: Спеціалісти повинні мати можливість виміряти признак яким-небудь приладом для подальшого занесення в базу даних.

5) Прийнятність: Суспільство не повинне бути проти збору і вимірювання цього біометричного параметру.

Аутентифікація людини за допомогою параметрів обличчя:

Аутентифікація людини на основі мережевих програм розпізнавання обличчя може відбуватися двома шляхами, які відрізняються між собою:

Аутентифікація по термограмі лиця

Спосіб заснований на дослідженнях, які показали, що термограма особи унікальна для кожної людини. Термограма виходить за допомогою камер інфрачервоного діапазону. На відміну від аутентифікації по геометрії особи, даний метод розрізняє близнят. Використання спеціальних масок, проведення пластичних операцій, старіння організму людини, температура тіла, охолодження шкіри обличчя в морозну погоду не впливають на точність термограми. Через невисоку якість аутентифікації, метод на даний момент не має широкого поширення.

Аутентифікація по геометрії лиця

Біометрична аутентифікація людини по геометрії особи досить поширений спосіб ідентифікації і аутентифікації. Технічна реалізація представляє собою складну математичну задачу. Широке застосування мультимедійних технологій, за допомогою яких можна побачити достатню кількість відеокамер на вокзалах, аеропортах, площах, вулицях, дорогах і інших місцях скупчення людей, стало вирішальним у розвитку цього напрямку. Для побудови тривимірної моделі людського обличчя, виділяють контури очей, брів, губ, носа, і інших різних елементів особи, потім обчислюють відстань між ними, і за допомогою нього будують тривимірну модель. Щоб знайти цю унікальну шаблону, відповідного певній людині, потрібно від 12 до 40 характерних елементів. Шаблон повинен враховувати безліч варіацій зображення на випадки повороту особи, нахилу, зміни освітленості, зміни виразу. Діапазон таких варіантів варіюється в залежності від цілей застосування даного способу (для ідентифікації, аутентифікації, віддаленого пошуку на великих територіях і т. д.). Деякі алгоритми дозволяють компенсувати наявність у людини очок, капелюхи, вусів і бороди.

Показано що, найбільш ефективний засіб ідентифікації в системах контролю за персоналом заснован використанні нейронних мережевих програм. Використання нейронних мереж дозволяє досить ефективно і швидко проводити комплексний контроль за персоналом: вести контроль за робочим часом працівників, контролювати присутність працівників на робочому місці, виявляти не санкціоніровні переміщення людей по приміщенням з обмеженим доступом та інше. Використання нейронних мережевих програм дозволяє виключити людину, як найбільш ненадійний елемент захисту інформації.

УДК 004.931

СИСТЕМА БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ОСОБИ

К. В. Меркулова, Є. О. Жабська

Технології автоматичного виявлення та розпізнавання обличь використовуються у багатьох сучасних системах комп’ютерного зору: біометрична ідентифікація, людино-машинний інтерфейс, зір роботів, комп’ютерна анімація, відеоконференції. Потреба до надійної ідентифікації особистості призвела до зростання інтересу до біометрії.