

БІОМЕТРИЧНА АВТЕНТИФІКАЦІЯ У МОБІЛЬНИХ ТЕЛЕФОНАХ НА ПРИКЛАДІ ЄМНІСНОГО МЕТОДУ АВТЕНТИФІКАЦІЇ ЗА ВІДБИТКОМ ПАЛЬЦЯ

Морозов О.Ю.

Науковий керівник – к.т.н., доц. Гріненко Т.О.

Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Безпеки інформаційних технологій,
тел. (057) 702-14-25; e-mail:oleksii.morozov@nure.ua, тел. (098) 28-15-298

The subject of research was to show the most popular mechanisms of biometrical authentication in mobile devices and applications. The main advantages, properties and where it can be used were presented in work.

Надійна авторизація та автентифікація стають невід'ємними частинами сучасного життя [1]. Біометричні системи розпізнають людей на основі їх анатомічних особливостей. Оскільки ці риси фізично пов'язані з користувачем, біометричне розпізнавання є дуже надійним механізмом. Призначення механізму – стежити, щоб тільки той користувач, що успішно авторизувався, мав змогу отримати доступ до інформації. Таким чином, при грамотній реалізації у відповідних додатках біометричні системи забезпечують високий рівень захищеності інформації [1].

Ємнісний метод найчастіше застосовується у мобільних телефонах, бо володіє рядом таких переваг, як невеликий розмір датчика та захист від автентифікації зображенням пальця. До недоліків таких сканерів можна віднести погану стійкість до муляжів, фізичного пошкодження чи забруднення пальця. Розрізняють 2 види ємнісних сканерів: активні та пасивні. У той час, коли пасивні сканери можна вважати звичайними, активні більш надійні до муляжів та зовнішніх чинників (забруднення та пошкодження пальця). Під муляжем мається на увазі навмисно вироблений макет пальця з відбитком власника мобільного телефону.

Спершу ємнісний датчик відбитка пальця генерує зображення відбитка пальця, використовуючи масив, що містить багато тисяч маленьких пластин конденсатора. Пластини матриці складають «пікселі» зображення: кожна з них діє як одна пластина конденсатора з паралельними пластинами, в той час як дермальний шар пальця, який є електропровідним, діє як інша пластина і є непровідним. Коли палець поміщається на датчик, утворюються слабкі електричні заряди, що утворюють рисунок між гребенями або впадинами пальця і пластинами датчика. Використовуючи ці заряди, датчик вимірює ємність вимірюваної поверхні. Наступним кроком є оцифровка отриманих значень логікою датчика і перевірка на ідентичність отриманих даних з копією на

мобільному телефоні за допомогою алгоритму порівняння відбитків пальців за ключовими точками – кінцевими точками папілярних ліній і точками роздвоєння папілярних ліній.

Алгоритм порівняння відбитків пальців за ключовими точками. Для кожної пари таких точок обчислюють трійки значень: модуль вектора, що з'єднує пару ключових точок, орієнтацію вектора відносно горизонталі та напрямками папілярних ліній з ключовими точками відносно горизонталі. Тобто шаблон містить опис відбитка, заданий у відносних одиницях, що нівелює зміну орієнтації зображення. Алгоритм оцінює відсоток збігів між відповідними трійками значень [2]. Основна проблема, що пов'язана з методом вилучення ключових деталей з використанням процесів стоншення гребенів, пов'язана з тим, що ключові точки в зображенні скелета не завжди відповідають дійсним ключовим точкам в зображенні відбитка пальця. Фактично, безліч помилкових ключових точок витягуються через небажані розриви.

У відмінній якості зображення відбитків пальця налічується близько від 70 до 80 ключових точок, коли в не дуже чіткому зображенні лише від 20 до 30. Відбитки вважаються з одного пальця, якщо два відбитка пальців мають як мінімум 12 збігів по ключовим точкам [2].

На основі отриманих даних система автентифікації робить висновок чи являє собою суб'єкт тим, за кого він себе видає. За результатами дослідження можна зробити висновок, що перевагою ємнісного методу автентифікації за відбитком пальця є компактність такого датчика та стійкість до атак з заміною відбитка на його зображення. В роботі проведені аналіз та дослідження алгоритму порівняння відбитків пальців на основі ключових точок. Його перевага в простоті та швидкодії виконання порівняння відбитків. Недоліком є достатньо велика похибка виявлення коректного зображення відбитку.

Список використаних джерел:

1. Задорожний В.Г. Идентификация по отпечаткам пальцев, Часть 1, 2004, 400 с.
2. A. K. Jain, A. Ross and S. Prabhakar, "An Introduction to Biometric Recognition", IEEE transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, pp. 4-20, January 2004.