СПУФІНГ-АТАКИ НА БІОМЕТРИЧНІ СИСТЕМИ АВТЕНТИФІКАЦІЇ ТА МЕТОДИ ПРОТИДІЇ АТАКАМ

Кустов А.К.
Науковий керівник – ст. викл., к.т.н. Олешко І.В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки 14, каф. БІТ, тел. (057) 702-14-25)
e-mail: akustov671@gmail.com

Biometric technologies are not completely protected from spoofing attacks. Survival detection methods are the most commonly discussed anti-spoofing measures. Survival detection is one of the important procedures in the registration, verification and identification processes. Therefore, it must be considered as an integral component of the biometric system. In this study raises an important issue of user authentication and protection of its data from spoofing attacks. In addition, the definition of spoofing attack is given. The types of spoofing attacks and methods for countering spoofing attacks are described using the example of a biometric face recognition system.

У наш час автентифікація особистості за її біометричними ознаками є одним із головних напрямків розвитку забезпечення безпеки в різних галузях нашого повсякденного життя (наприклад, медицина, електронні системи голосування, електронна комерція, тощо).

Однак поряд зі зростанням ролі біометричних технологій останнім часом також почастішали спроби підміни біометричних характеристик зареєстрованих користувачів хакерами, з метою вилучення фінансових коштів, отримання конфіденційних даних і т.д.

Найбільшу загрозу для впровадження та використання біометричних систем являють спуфінг-атаки. Спуфінг або спуфінг-атака [1] (англ. Spoofing attack) – в контексті безпеки мережі, це випадок, коли особа або програма маскується під іншу за допомогою фальсифікації даних, і тим самим отримує незаконну перевагу. Існує декілька варіантів спуфінг-атак: відтворення, яке здійснюється шляхом відправки раніше представлених даних законного користувача для перевірки автентичності; моделювання (імітація) даних користувача; атака, при передачі даних в мережі; підміна фізіологічних біометричних характеристик; атака на біометричний шаблон.

Візьмемо для прикладу один з варіантів біометричної системи (далі БС) автентифікації – систему розпізнавання обличчя (Face Recognition System). На сьогоднішній день система розпізнавання обличчя є однією з найбільш розповсюджених та популярних БС у світі, але й через це кожного дня трапляється багато випадків спуфінг-атак, з метою потрапляння у систему, де зберігаються дані звичайних користувачів. Отже давайте розглянемо методи протидії спуфінг-атакам, які застосовуються в наведеній БС. Методи на основі рухів (міміки) або темпоральні методи (динамічні, рідше статичні). Фіксація мимовільних рухів м'язів або дій за запитом. Методи на основі аналізу текстури

(статичні). Пошук особливостей текстури, характерних для надрукованого обличчя (розмитості, збої при друку і т.д.).

Методи на основі аналізу якості зображення (статичні). Аналіз якості зображення реального обличчя і підробленого 2D-зображення (аналіз спотворень, аналіз розподілу дзеркальності). Методи на основі 3D-структури обличчя (динамічні). Фіксація відмінностей у властивостях оптичного потоку, що генерується тривимірними об'єктами і двовимірними площинами (аналіз траєкторії руху). Наведені вище методи дають змогу біометричним системам автентифікації протистояти спуфінг-атакам. Але у кожного методу є свої переваги та недоліки, і потрібно розрізняти ситуації, коли використовувати той, чи інший метод (наприклад, якщо середовище має обмеження до часу відгуку, то не доцільно використовувати метод на основі 3D-структури обличчя, який має повільний відгук (>3 сек.), а краще звернути увагу на метод аналізу якості зображення, який працює в рази швидше (<1 сек.); проте якщо до розроблюваного середовища висуваються вимоги максимального захисту, то ситуація з вибором методу стає зворотною). Автори [2] пишуть, що головними для оцінки будь-якої біометричної системи є два параметри: FAR (False Acceptance Rate) – коефіцієнт помилкового пропуску. FRR (False Rejection Rate) – коефіцієнт помилкової відмови. У таблиці наведені значення коефіцієнтів FAR та FRR для систем біометричної автентифікації по обличчю (БС з використанням методу на основі 3D-структури обличчя, та БС з використанням методу на основі 2D-структури обличчя) та зроблені висновки про ймовірність успішної спуфінг-атаки на ці системи.

Таблиця 1 – Значення коефіцієнтів FAR та FRR

Біометрична система	FAR	FRR	Успішна спуфінг-атака
Розпізнавання обличчя 2D	0.1%	2.5%	Можлива
Розпізнавання обличчя 3D	0.0005%	0.1%	Проблематична

За цими даними можна зробити висновок, існує багато методів захисту біометричних систем від спуфінгу, але жоден з них не може гарантувати користувачеві повний захист. Для максимального захисту потрібно використовувати мультимодальні біометричні системи автентифікації, тобто системи, які складаються з декількох систем (наприклад, автентифікація користувача по голосу та по обличчю).

Список використаних джерел:

1. Pan, G., Sun, L., Wu, Z., Lao, S. Eyeblink-based Anti-Spoofing in Face Recognition from a Generic Webcamera // IEEE Intl. Conference on Computer Vision. – 2007. – P. 1–8.

2. Gorbenko I.D. INFORMATIONAL SECURITY IN CRITICAL INFRASTRUCTURES / Gorbenko I.D., Kuznetsov A.A. – Kharkiv: LAP LAMBERT Academic Publishing, 2017. – С. 396-405.