УДК 004.056
DOI: 10.20535/SRIT.2308-8893.2022.3.05

ПРОЦЕС КЕРУВАННЯ ЗАХИЩЕНІСТЮ ДАНИХ ПІД ЧАС ВІДДАЛЕНОЇ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ

А.А. АСТРАХАНЦЕВ, Г.Є. ЛЯШЕНКО

Анотація. Системи віддаленої біометричної автентифікації за останній час набули значного поширення через необхідність користування загальними пристроями та виконання платежів через Інтернет. Оскільки саме біометричні методи більш зручні для користувачів і нині швидко замінюють паролі, то стає актуальним завданням передавання біометричної інформації відкритою мережею без її компрометації. Метою роботи є модернізація системи віддаленої автентифікації для підвищення рівня прихованості і захищеності біометричних даних користувача. Запропоновано застосування найкращих за критерієм захищеності методів формування біометричного шаблону, методів мережевої стеганографії для підвищення прихованості та впровадження інтелектуальної системи прийняття рішень. Такі вдосконалення дозволять підвищити захищеність і прихованість даних для процесу віддаленої автентифікації.

Ключові слова: біометричний шаблон, віддалена автентифікація, атаки, мережева стеганографія.

ВСТУП

Натепер дедалі більшого попиту набули інтернет-магазини, онлайн-банкінг та інші послуги, під час яких користувач користується віддаленим передаванням своєї особистої інформації. Під час онлайн-оплати послуг (магазини, комунальні платежі, купівля квитків та ін.) дуже важливим є захист персональних даних користувача. Дедалі частіше під час віддаленої автентифікації користувача використовується біометрична автентифікація [1, 2]. Вона базується на використанні таких невід'ємних та унікальних для кожної людини фізичних характеристик, як відбитки пальців, зображення райдужної оболонки ока, геометрії обличчя, або поведінкових характеристик. Оскільки ці характеристики не можуть бути відновлені або замінені у випадку викрадення чи втрати, то завдання забезпечення захищеності даних під час передавання мережею або в процесі однобічного перетворення даних для унеможливлення використання зловмисником є дуже важливими.

Мета роботи: удосконалення процесів, що відбуваються під час віддаленої біометричної автентифікації та під час передавання автентифікаційних даних мережею, огляд можливих атак у мережі та обрання методів, які допоможуть підвищити захищеність даних під час віддаленої автентифікації для передавання відкритими каналами зв'язку.

БІОМЕТРИЧНА АВТЕНТИФІКАЦІЯ: ЗАГАЛЬНІ ПРИНЦИПИ ТА МОЖЛИВІ АТАКИ

У загальному вигляді схему біометричної автентифікації зображено на рис. 1, *а*, *б*. Система автентифікації в базі даних зберігає біометричні шаб-

лони зареєстрованих користувачів, дані про них та інструкції щодо режиму доступу певних об'єктів. Біометричний датчик на вході зчитує унікальні біометричні характеристики користувача, система порівнює їх з тими, що внесені до бази даних, авторизує користувача і в разі збігу характеристик користувача з шаблоном, що внесений до бази даних, надає рішення щодо допуску до певної інформації/об'єктів/тощо.

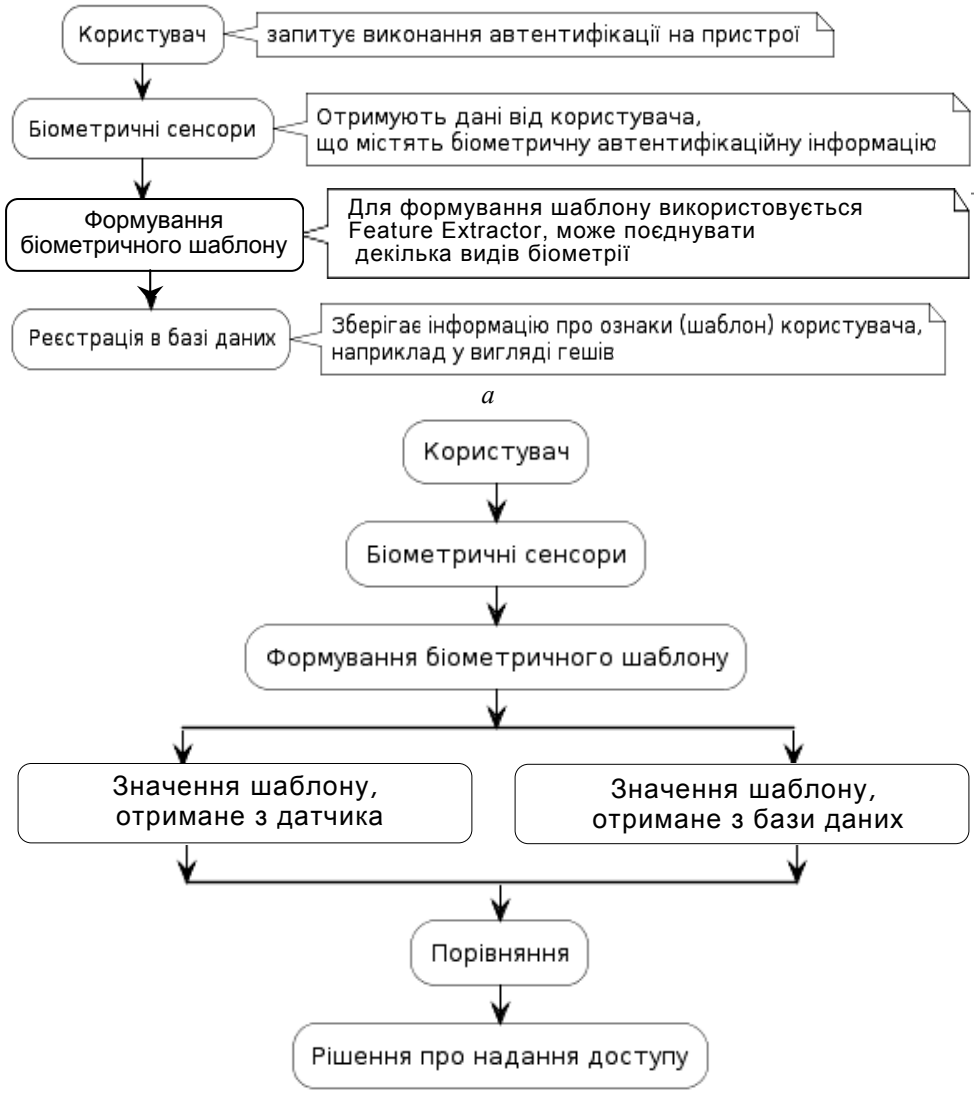

Рис. 1. Узагальнена схема біометричної автентифікації: фаза реєстрації (*а*), фаза перевірки (*б*)

Під час віддаленої автентифікації дані, що мають автентифікувати користувача, передаються мережею, під час чого можуть бути спотворені завадами в каналах зв'язку та скомпрометовані в результаті різних типів атак. Біометричні характеристики людини є унікальними і невід'ємними. Це дає великі переваги для правильного надання доступу з використанням цих характеристик, але вони не можуть бути замінені, тому передавати їх у відкритому вигляді або навіть зашифрованому неможливо.

На систему віддаленої автентифікації можливі різні типи атак (рис. 2). На самому початку системи передавання даних можлива фальсифікація даних (spoofing attack) — використання фальсифікованих біометричних характеристик користувача, поновлення та використання старих даних, які використовувалися раніше під час автентифікації. Також існує ймовірність атаки у вигляді несанкціонованого доступу до сформованого біометричного шаблону під час автентифікації, його підміна або підміна шаблону (substitution attack) [1, 13], який зберігається в базі даних. Небезпечною є атака маскарад (masquerade attack), коли цифровий образ може бути створений із шаблону біометричного образу. Існує ймовірність впливу з метою підміни рішення під час порівняння біометричних шаблонів.

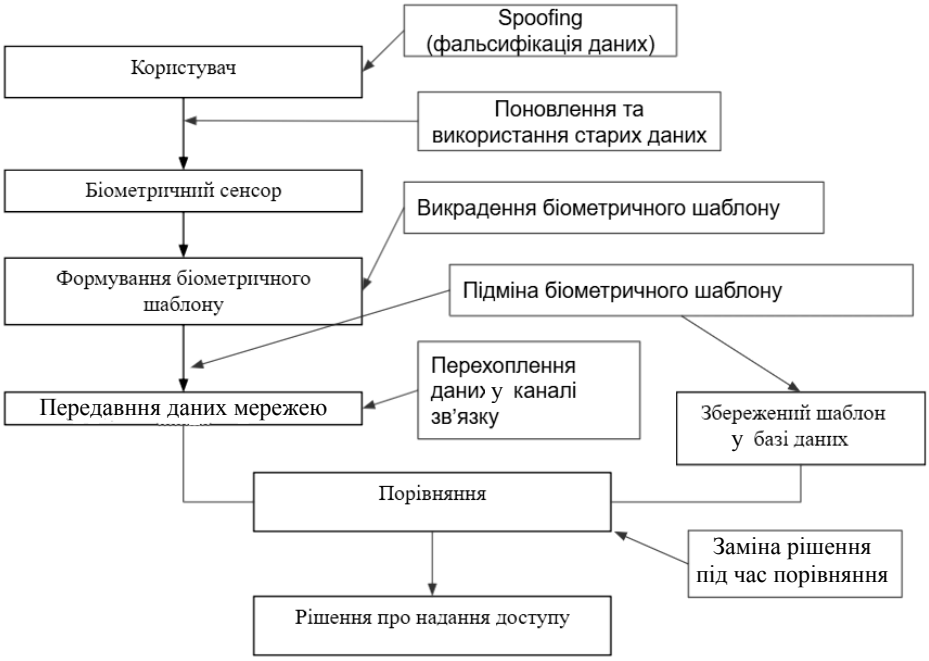

Рис. 2. Можливі вразливості в системі віддаленої біометричної автентифікації

Окрім зазначених атак, під час передавання даних каналом зв'язку є загроза того, що дані будуть перехоплені.

Під час спуфінгових атак зловмисник для отримання доступу в систему використовує штучно створені біометричні ознаки. Наприклад, маску обличчя, надруковане зображення райдужної оболонки ока тощо, або імітує поведінкові характеристики, що використовуються під час динамічної автентифікації, наприклад, динамічний підпис. Такі загрози виникають на етапі роботи з датчиками, що розпізнають особу, тому для захисту від таких загроз потрібно вжити заходів, що будуть попереджати від розпізнавання підроблених зразків. Прикладом біометричних властивостей, які мають високий рівень захищеності від підроблень, є такі властивості, як температура, електрична провідність, пульсоксиметрія та опір шкіри.

Для боротьби зі спуфінгом на рівні пристроїв використовують апаратні методи. Вони полягають в інтеграції у сканер спеціальних апаратних пристроїв, які дозволять розпізнавати конкретні характеристики живих біомет-

ричних зразків (рухи ока, тепло пальців та ін.); вони також можуть перевіряти реакцію на зовнішні сигнали, що потребують наявність певного користувача. Наприклад, для того, щоб попередити використання підробних відбитків пальців, що створені зі штучного матеріалу сканери відбитків пальців, застосовують механізми виявлення підробних відбитків.

Для вирішення проблеми використання підроблених зображень використовують ідентифікацію користувачів за рухами зіниць, які виникають у разі змін їх розмірів.

На рівні функцій використовують програмні методи. Ці методи інтегруються в системі після сканерів. Робота таких методів полягає в екстракторі ознак і вони працюють уже з послідовностями ознак, отриманих за певний проміжок часу.

Під час перших етапів роботи системи автентифікації важливо уникнути можливості відновлення старих, уведених іншим користувачем даних для отримання несанкціонованого доступу.

Для здійснення біометричної автентифікації після сканування певних біометричних ознак формується біометричний шаблон. Біометричний шаблон — це цифрове подання даних, вилучених з біометричного зразка. Вони зберігаються в базі даних і використовуються під час порівняння для автентифікації. Існує ризик поновлення створеного шаблону та використання старих даних. Є ймовірність підміни шаблону на інший та перехоплення шаблону в каналі зв'язку у процесі передавання, тому важливим завданням є захист шаблонів.

ОГЛЯД ВИМОГ ТА ПІДХОДІВ ДО ЗАХИСТУ БІОМЕТРИЧНОГО ШАБЛОНУ

Ідеальна біометрична схема захисту шаблону повинна мати такі чотири властивості [7].

1. Різноманітність: безпечний шаблон не повинен дозволяти порівняльний пошук по базах даних, тим самим забезпечуючи конфіденційність користувача.

2. Можливість ануляції: має бути простою для відкликання скомпрометованого шаблону та перевипуску нового, заснованого на тих же біометричних даних.

3. Безпека: отримання оригінальної біометричної інформації із сформованого шаблону повинно бути обчислювально важким. Ця властивість перешкоджає відновленню біометричних ознак з викраденого шаблону.

4. Продуктивність: схема захисту біометричного шаблону не повинна погіршити продуктивність розпізнавання.

Основним викликом розроблення біометричної схеми захисту шаблону, який задовольняє всі згадані вимоги, є необхідність оброблення мінливих даних користувача.

Нагадаємо, що декілька зображень однієї біометричної ознаки не призводять до того ж набору значень. Із цієї ж причини не можна зберігати біометричний шаблон у зашифрованій формі (наприклад, за допомогою стан-

дартних методів шифрування, таких як RSA, AES та ін.), а потім оцінювати відповідність у зашифрованому домені.

Варто звернути увагу на те, що шифрування не є гладкою функцією і невелика різниця значень, що витягуються з початкових біометричних даних, призведе до дуже великої різниці в зашифрованому результаті. При цьому варіант з розшифровуванням шаблону і оцінюванням відповідності між збереженим та розшифрованим шаблонами, не є безпечним, оскільки має зберігатися сам біометричний шаблон. Отже, стандартні методи шифрування не є корисними для забезпечення захисту біометричних шаблонів.

Розглянемо основні схеми захисту біометричного шаблону, що натепер набули поширення. Згідно із працями [7, 12, 14], підходи до захисту можна поділити на 2 напрями: підходи на основі перетворення властивостей та біометричні криптосистеми (рис. 3).

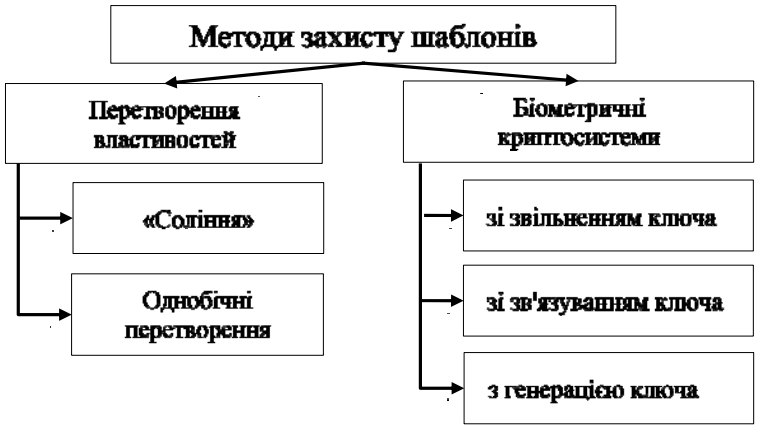

Рис. 3. Спрощена класифікація методів захисту шаблону

У декількох джерелах [14, 15] пропонують додаткові методи: гомоморфну криптографію, гібридні методи, а також методи на основі стеганографії та ватермаркінгу.

У підходах на основі перетворення властивостей біометричні дані обробляються за допомогою деякої функції-перетворення і далі зберігається лише вже трансформований шаблон. Залежно від типу функції-перетворення цей підхід поділяється на методи «соління» та однобічні перетворення.

У методах на основі «соління» функція-перетворення може бути оберненою [12], тобто, якщо ключ перетворення відомий по трансформованому шаблону, можна відтворити оригінальний. Безпека таких систем базується на захищеності ключа чи пароля. У методах на основі однобічних перетворень зазвичай обчислювально важко відновити оригінальний шаблон за трансформованим, навіть якщо ключ відомий [7].

Біометричні криптосистеми [1] у свою чергу поділяються на системи зі звільненням ключа (key release cryptosystems), системи зі зв’язуванням ключа (key binding cryptosystems) та системи з генерацією ключа (key generation cryptosystems).

У біометричних криптосистемах користувачеві не потрібно запам’ятовувати паролі та/або використовувати додаткові пристрої для

зберігання, передавання та ін. Біометрична криптосистема в будь-який час і в будь-якому місці ініціалізується шляхом вилучення «на льоту» необхідних параметрів з наданих біометричних зображень (з можливими помилками, стиранням тощо) без шкоди для цих зображень.

АНАЛІЗ ЕФЕКТИВНОСТІ ІСНУЮЧИХ МЕТОДІВ ЗАХИСТУ БІОМЕТРИЧНОГО ШАБЛОНУ

Розглянемо наведені вище методи й оцінимо їх переваги та недоліки. За результатами аналізу сформуємо набір правил для вибору найкращого рішення в кожній окремій ситуації.

Основні методи захисту шаблону такі [7, 12, 13]:

Методи «соління». Соління або біохеш — це підхід захисту шаблону, у якому біометричні ознаки перетворюються за допомогою функції, визначеної специфічним ключем або паролем користувача. Оскільки трансформація може бути обернена, то ключ повинен бути надійно збережений користувачем та поданий під час автентифікації. Ця потреба в додатковій інформації у вигляді ключа збільшує ентропію біометричного шаблону і, отже, ускладнює для противника вгадування шаблону.

Можна відзначити переваги методу «соління». По-перше, це ефективний метод перетворення вхідних біометричних даних у високоентропійні за рахунок збільшення ентропії біометричних даних з накладанням на біометричні зразки псевдовипадкових послідовностей. По-друге, використання ключа дозволяє збільшити відстань Хемінга між даними біометричних зразків. Схема прийняття рішення за біометричної ідентифікації повинна враховувати значення кількості бітів, які збігаються у разі порівняння біометричних зразків.

Обмеження. 1. Якщо специфічний ключ користувача скомпрометований, шаблон більше не є безпечним, тобто, якщо противник отримує доступ до ключа та трансформованого шаблону, він може відновити оригінальний біометричний шаблон. 2. Оскільки порівняння відбувається у перетвореному вигляді, механізм «соління» повинен бути розроблений таким чином, щоб продуктивність розпізнавання не погіршувалася, навіть під час змін у біометричних даних користувача.

Використання нечітких контейнерів на основі застосування методів «соління» є ефективним методом побудови множини подань біометричних даних біометричного зразка.

Методи на основі однобічних перетворень. За цього підходу біометричний шаблон шифрується за допомогою однобічної функції перетворення. Параметри функції перетворення визначаються ключем, який повинен бути доступним під час автентифікації. Основною характеристикою такого підходу є те, що навіть якщо ключ та/або трансформований шаблон відомі, то обчисленням важко (через складність грубої сили) для противника відновити оригінальний біометричний шаблон.

Перевагою методу є те, що навіть якщо ключ скомпрометований, ця схема забезпечує кращу безпеку, ніж метод «соління». Заміна шаблону та ануляція можуть бути реалізовані за допомогою специфічних функцій.

Обмеження. Основним недоліком такого підходу є компроміс між невідповідністю та однобічністю функції перетворення. Функція перетво-

рення, з одного боку, має зберігати подібність (функції одного користувача повинні мати високу подібність у перетвореному просторі, а функції різних користувачів бути досить різнорідними після трансформації), а з другого боку, повинна бути однобічною. Важко спроектувати функції перетворення, які одночасно задовольняють обидві умови. Крім того, функція перетворення також залежить від біометричних ознак, які потрібно використовувати у певному застосуванні.

Біометричні криптосистеми. Традиційно, біометричні криптосистеми на нечітких екстракторах, а також системи, що їм передують, на нечітких контейнерах [2, 13], будуються з використанням завадостійкого кодування. На початковому етапі біометричні дані в певному сенсі об'єднуються з елементами завадостійких кодів (наприклад, з кодовими словами або синдромними послідовностями). Для нечітких екстракторів додатково утворюється відкритий допоміжний рядок (helper data), який допомагає вилучати секретний параметр на нечітких заданих біометричних даних. На етапі використання застосовується завадостійке декодування, що усуває можливу невизначеність (викликану завадами, стиранням тощо) у наданих біометричних шаблонах користувача. Якщо відмінності в наборах характеристик невеликі (не перевищують можливості коригувальних кодів), то нечіткі екстрактори (контейнери) дозволяють однозначно відновити секретний параметр (біометричний ключ).

До класу біометричних криптосистем належать три групи систем.

1. *Біометричні системи зі звільненням ключа* [1, 14]. У режимі звільнення ключа біометрична автентифікація здійснюється незалежно від механізму звільнення ключа, біометричний еталон і ключ зберігаються окремо один від одного, сам ключ звільняється після успішної біометричної автентифікації.

2. *Біометричні системи зі зв'язуванням ключа* [1, 14]. У криптографічних системах такого типу ключ і біометричний еталон криптографічно пов'язані між собою. Ключ за певним алгоритмом пов'язується з біометричним еталоном користувача і зберігається в такому вигляді в базі даних, відповідно розкрити ключ може тільки власник біометричних параметрів. У таких системах передбачається (проте не є необхідним) використання допоміжних даних (helper data) для демаскування зашумлених біометричних даних.

Як перевагу криптосистем цього типу слід відзначити те, що цей підхід є толерантним для змін (варіацій) даних користувача, і ця толерантність визначається здатністю коду з виправлення помилок.

Обмеження. 1. Відповідність необхідно виконати за допомогою схем корекції помилок, і це виключає використання складних схем порівняння. Це може призвести до зменшення точності порівняння. 2. Загалом біометричні криптосистеми не призначені для забезпечення різноманітності та анулюції. Проте намагаються ввести ці дві властивості в біометричні криптосистеми, головним чином, використовуючи їх у поєднанні з іншими підходами, такими як «соління». 3. Допоміжні дані мають бути ретельно розроблені.

3. *Біометричні системи з генерацією ключа* [1]. У такій біометричній криптосистемі ключ формується безпосередньо з біометричних даних кори-

стувача і не зберігається в базі даних. Варто звернути увагу на те, що якщо схема генерує той самий ключ, незалежно від шаблону вхідних даних, він має високу основну стабільність, але нульову ентропію, що зумовлює високе значення FAR. З іншого боку, якщо схема створює різні ключі для різних шаблонів того ж користувача, схема має високу ентропію, але нестабільність зумовлює високе значення FRR. Можна вивести ключ безпосередньо з біометричних ознак, однак важко одночасно досягти високої ентропії та високої стабільності.

Перевагою методу є пряма генерація ключа з біометрії.

Обмеження. Важко генерувати ключ з високою стабільністю та ентропією.

Сценарій та початкові дані відіграють важливу роль у виборі схеми захисту шаблону [7]. Наприклад, у застосуванні біометричної верифікації, такої як банкомат банку, проста схема «соління», заснована на PIN-коді користувача, може бути достатньою для забезпечення захисту біометричного шаблону. З іншого боку, під час проходження процедур аеропорту однобічне перетворення є більш придатним підходом, оскільки він забезпечує як захист шаблону, так і можливість ануляції (відкликання), не покладаючись на будь-які інші вхідні дані від користувача. Біометричні криптосистеми є більш доцільними у додатках з порівняннями на карті.

Іншим основним чинником, що впливає на вибір схеми захисту шаблону, є вибрана біометрична ознака, її набір функцій та ступінь варіацій даних користувачів. Дизайн схеми захисту шаблону залежить від конкретного типу біометрії, що використовується. Так однобічні функції були запропоновані для відбитків пальців, але важко спроєктувати відповідне перетворення для райдужної оболонки ока (iris-code). Навпаки, може бути простішим розроблення біометричної криптосистеми для райдужної оболонки ока як бінарного рядка фіксованої довжини, де можна легко застосувати стандартні методи кодування з коригуванням помилок. Крім того, якщо варіації всередині даних одного типу для одного користувача досить великі, то неможливо застосувати однобічне перетворення або створити біометричну криптосистему. Тому навіть у конкретному сценарії більш ніж одна схема захисту шаблону може бути прийнятною, а вибір відповідного підходу може базуватися на ряді таких факторів, як продуктивність розпізнавання, обчислювальна складність, вимоги до пам'яті.

Оцінимо основні характеристики системи за умови використання наведених методів формування біометричного шаблону. Як характеристики системи біометричної автентифікації будемо використовувати помилки першого роду, коли визначається ймовірність помилкової відмови в доступі клієнту, який має право доступу FRR (False Rejection Rate), та помилки другого роду як імовірність помилкового доступу, коли система помилково пізнає чужого клієнта як свого FAR (False Acceptance Rate).

ОЦІНЮВАННЯ ЙМОВІРНОСТІ ПОМИЛКИ ПІД ЧАС ВІДДАЛЕНОЇ АВТЕНТИФІКАЦІЇ

Нехай на шаблон S довжиною l_S біт накладаються кодові слова двійкового коду (n,k,d), що коригує помилки. При цьому під n будемо розуміти за-

гальну довжину кодових слів, k — довжина інформаційних слів і d — кодова відстань. Таких слів буде

$$N = l_s / n,$$

при цьому кількість кодових слів $N_c = 2^k$. Перетворення визначається операцією побітового складання слів шаблону S_i коду C_i:

$$S_i \oplus C_i = SC_i \;\; i = \overline{1, N}.$$

Кодова відстань визначає можливості коригувати та визначати помилки. Код може під час декодування гарантовано виправити помилки кратністю $t = (d-1)/2$ та виявити помилки кратністю $d-1$.

Кодові слова генеруються за випадковими значеннями інформаційних слів $k_i \;\; i = 1, N$. Таким чином, ключова послідовність, за якою генеруються кодові слова, повинна бути випадковою і мати довжину

$$K = kN = \frac{k}{n} l_s \text{ (бітів)},$$

де співвідношення $R = k / n$ визначає швидкість коду.

Схема прийняття рішення порівнює зашумлені образи, які зберігаються на сервері з прийнятими з каналу зв'язку. Порівняння виконується за виразом

$$SC_i^C \oplus SC_i^K = SC_i^P, \;\; i = \overline{1, N},$$

де N — кількість кодових слів, що зашумлять біометричні образи; SC_i^C — зашумлений біометричний образ, що зберігається на сервері; SC_i^K — зашумлений біометричний образ, що перевіряється на сервері.

Під час порівняння отримаємо результат

$$SC_i^P = S_i^K \oplus C_i^K \oplus S_i^C \oplus C_i^C = (S_i^K \; S_i^C) \oplus (C_i^K \; C_i^C),$$

де C_i^C — кодова послідовність, що зашумляє біометричний образ, який зберігається на сервері; C_i^K — кодова послідовність, що зашумляє біометричний образ, який перевіряється на сервері.

Сума кодових слів, які надійшли з каналу зв'язку та зашумлені в біометричних шаблонах на сервері, дає кодові слова лінійного блокового коду (n, k, d). Отримаємо

$$SC_i^P = (S_i^K \; S_i^C) \oplus C_i^P, \;\; i = \overline{1, N},$$

де $C_i^P = C_i^{KC \oplus_i^K}$ — кодові слова лінійного блокового коду (n, k, d).

Імовірність того, що під час декодування виникнуть помилки (які будуть визначатися як розбіжність S_i^K і S_i^C) визначається

$$p_e = 1 - \frac{N_c}{N_b}.$$

Під час автентифікації кількість помилкових кодових слів не повинна перевищувати значення порога T (дозволена для коректної роботи кількість помилок). У такому випадку отримаємо оцінку FAR імовірності помилкового доступу, коли система помилково пізнає чужого як свого:

$$FAR = \sum_{j=0}^{T} C_N^j p_e^j (1 - p_e)^{N-j}.$$

Декодування кодових слів коду (*n,k,d*) дозволяє гарантовано виявити помилки кратністю $d-1$. Таким чином, код виявляє помилки з імовірністю

$$p_{i\text{д}} = \sum_{j=1}^{d-1} C_n^j p_{\text{д}}^j (1 - p_{\text{д}})^{N-j}.$$

Використовуючи цей вираз, отримаємо оцінку помилки першого роду FRR:

$$FRR = 1 - \sum_{j=1}^{T} C_N^j p_{i\text{д}}^j (1 - p_{i\text{д}})^{n-j}.$$

ЗАСТОСУВАННЯ МЕТОДІВ СТЕГАНОГРАФІЇ ДЛЯ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ПРОЦЕСУ АВТЕНТИФІКАЦІЇ

Для підвищення захищеності (шляхом збільшення прихованості) біометричних даних можливе використання різних методів мережевої стеганографії, які дозволяють приховати сам факт передавання даних, необхідних для автентифікації мережею. Для застосування використано методи на основі вбудовування даних у поля мережевих протоколів.

Запропоновану схему захисту процесу віддаленої біометричної автентифікації з додаванням етапів вбудовування та завадостійкого кодування показано на рис. 4. Блоки, що відрізняють її від початкової схеми, наведені затемненим кольором.

Як показано у праці [11], для задач мережевої автентифікації найкращі показники забезпечують такі методи мережевої стеганографії: HICCUPS (0,21); TranSteg, LACK (0,18); RSTEG (0,15) та SCTP (0,12), де в дужках наведено значення векторів пріоритету.

Метод HICCUPS забезпечує найвищий рівень прихованості у зашумлених каналах, оскільки виконує маскування інформації під «природні» завади. Метод TranSteg використовується для приховування даних в IP телефонії, а також для передавання потокового відео. Для приховування інформації даний метод стискає корисне навантаження мережевого пакета за рахунок перекодування голосових даних з мінімальною втратою якості голосу і на місце, що звільнилось, в область корисного навантаження пакета вносять стеганограму; відповідно цей метод ефективний під час активної голосової чи відео сесії. Метод LACK також використовує активну RTP сесію, але його принцип дії заснований на внесенні затримки для відправлення певних голосових пакетів, корисне навантаження яких замінено. Метод RSTEG ґрунтується на повторному пересиланні пакетів і його використання для найбільшої прихованості також рекомендовано в каналах зв'язку з низьким співвідношенням сигнал/шум.

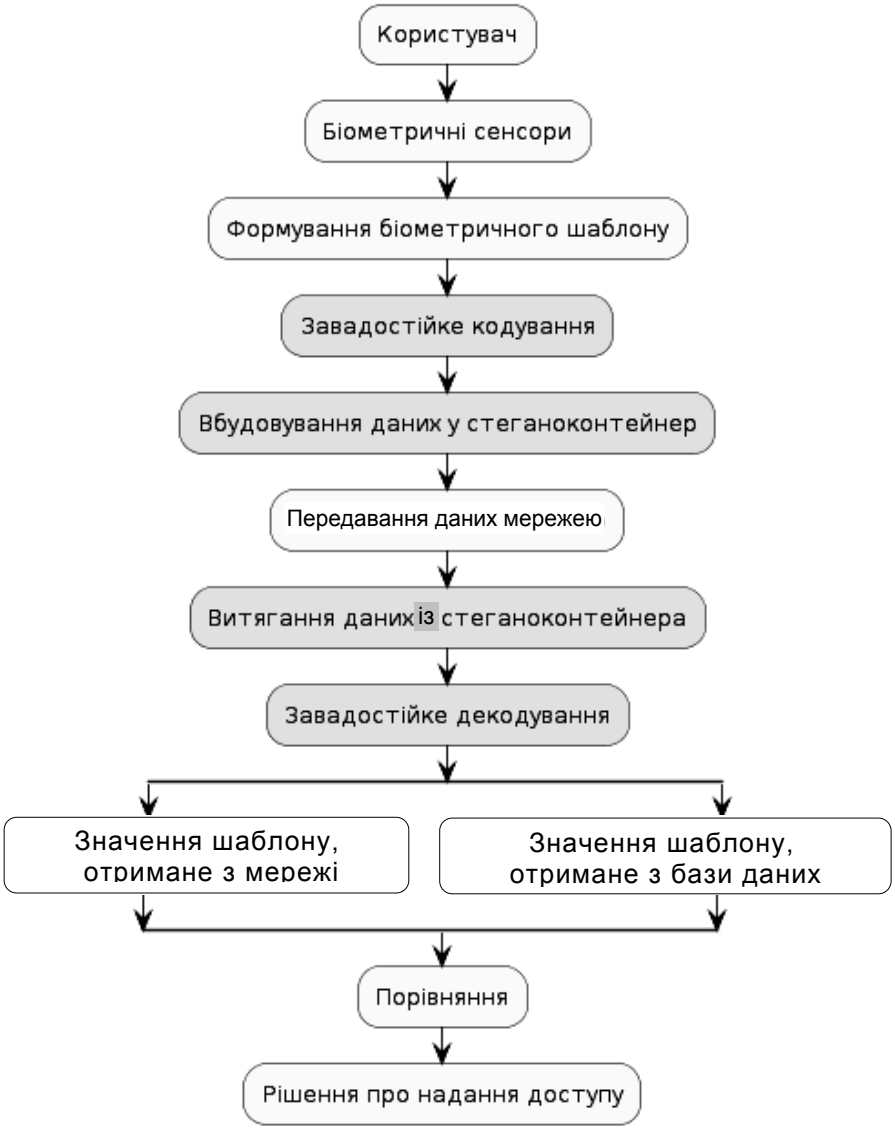

Рис. 4. Модифікована схема захисту віддаленої біометричної автентифікації

Для остаточного визначення найбільш ефективних методів вбудовування та покращення роботи системи віддаленої автентифікації в цілому побудуємо інтелектуальну систему, що буде ідентифікувати умови на вході, визначати поточний сценарій та обирати на основі правил для нього набір методів захисту.

ЗАСТОСУВАННЯ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ СИСТЕМИ ВІДДАЛЕНОЇ АВТЕНТИФІКАЦІЇ

Розглянемо запропоновану систему прийняття рішень (рис. 5). Нехай на її вхід подається набір початкових даних (блок «Вхідні дані», рис. 5), який для

досліджуваного випадку містить інформацію про стан каналу зв'язку та інформацію про характер отриманих біометричних ознак користувача.

Рис. 5. Узагальнена схема прийняття рішень

Інформація про стан каналу [10] включає такі параметри (дослідження проводилися на прикладі LTE/5G мережі):

- параметри потужності сигналу та якості: потужність сигналу RSRP (Reference Signal Receive Power), якість сигналу RSRQ (Reference Signal Received Quality), співвідношення сигнал/шум SINR (Signal-to-Interference-plus-Noise Ratio), доступна пропускна здатність Cell Bandwidth, використовувана схема модуляції та кодування MCS (Modulation and Coding Scheme);
- наявність фонових сесій за протоколами IP, TCP, RTP, SCTP та ін.

На основі пропускної здатності, співвідношення сигнал/шум та параметрів якості/потужності визначається гранична кількість повторно переданих пакетів, що дозволяє задати пропускну здатність стеганографічних методів, які використовують повторне передавання (RSTEG, HICCUPS).

Наявність активних сесій аналізується за допомогою програмного забезпечення на пристрої користувача і може впливати на вибір методу, що використовує заміну певних полів у заголовку.

Для навчання мережі підготовлена вибірка мережевих станів, отримана з телефонів Samsung Galaxy S21, яка містить стани каналу від RSRP = =-0 дБм до -120 дБм, якість RSRQ змінюється в діапазоні від -5 до -18 дБ, пропускна здатність: 10–15МГц. На цьому етапі проводиться підготовка тестової вибірки до навчання та аналізу ефективності різних типів нейронних мереж для оброблення тестових даних.

Інформація про характер отриманих біометричних ознак користувача формується як результат роботи блоків отримання біометричних даних із сенсорів та формування біометричного шаблону (див. рис. 4) і включає такі елементи, як попереднє оброблення зображення, витягнення біометричних ознак та об'єднання біометричних ознак.

Процедури попереднього оброблення отриманих від сенсорів даних та витягнення біометриних ознак включають у себе стандартні процедури роботи із зображеннями, які, наприклад, у випадку оброблення райдужної оболонки ока, включають [16] нормалізацію зображення, застосування фільтра Габора, Гауса чи Лапласа та генерацію коду райдужної оболонки.

Процедура об’єднання біометричних ознак (рис. 6) передбачає пріоритезацію отриманих біометричних ознак, додавання генератору шуму для приховування полів незаповнених ознак, процедуру перемежування і завадостійкий кодер, на параметри якого впливає описана інформація про стан каналу.

Рис. 6. Процедура об’єднання біометричних ознак

Перед початком роботи системи мають бути сформовані всі дозволені сценарії роботи. Множина сценаріїв має зберігатися у спеціальній базі знань. Архітектура бази даних включає всі зазначені поля стану каналу і поле, що містить сформовані біометричні ознаки користувача. Також до неї включені поле з переліком можливих методів захисту та поле з набором дозволених алгоритмів. Обрання того чи іншого сценарію відбуватиметься на основі навчання відповідної нейронної мережі. Для недопущення випадку DoS (Denial of Service) атаки в базі знань має бути прописаний «найгірший» сценарій, який буде працювати у будь-яких умовах, але можливо з гіршими характеристиками (нижча швидкість та прихованість, більша надмірність шаблону).

Використовуючи вхідні дані, система (див. рис. 5), обирає згідно із заданими заздалегідь критеріями відповідності сценарій, що максимально відповідає поточному стану. Після цього з бази знань обирається набір доступних для цього сценарію методів захисту.

Приклад роботи системи і формування рішення подано на рис. 7. У цьому прикладі маємо низький рівень потужності за низької якості, що згідно із працею [17] буде відповідати параметру якості каналу (CQI) 7-9. Це дозволить обрати алгоритм модуляції 16QAM і швидкості кодування 1/3; також немає інформації про додаткові сесії, відповідно має бути обраний стійкий до завад алгоритм захисту — біометрична система зі зв’язуванням ключа та алгоритм приховування RSTEG або HICCUPS.

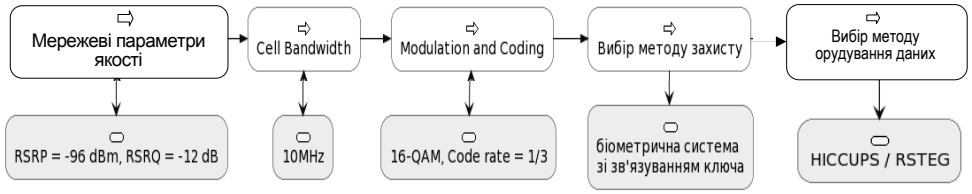

Рис. 7. Приклади роботи інтелектуальної системи прийняття рішень

ВИСНОВКИ

У роботі вирішено актуальне завдання підвищення захищеності процесу віддаленої біометричної автентифікації шляхом покращення захищеності системи віддаленої автентифікації та застосування інтелектуальної системи прийняття рішень. Запропонована система дозволяє на основі інформації про наявні біометричні ознаки користувача обрати найкращий за заданими критеріями спосіб їх перетворення в захищений біометричний шаблон. На основі інформації про параметри каналу зв'язку запропонована система дозволяє обрати метод підвищення прихованості шляхом використання мережевої стеганографії.

У роботі запропоновано новий підхід для підвищення захищеності шляхом додавання завадостійкого кодування та використання методів мережевої стеганографії. Визначено основні атаки на систему та запропоновано методи мінімізації ймовірності їх реалізації. Проаналізовано методи формування біометричного шаблону користувача та надано рекомендації щодо їх використання.

Наукова новизна роботи полягає в застосуванні інтелектуальної системи прийняття рішень для підвищення захищеності процесу віддаленої автентифікації; уперше запропоновано використовувати мережеву стеганографію для підвищення прихованості процесу віддаленої автентифікації.

Практична значущість роботи полягає в можливості використання запропонованої системи для підвищення захищеності віддаленої біометричної автентифікації користувачів у бездротових/мобільних мережах зв'язку.

ЛІТЕРАТУРА

1. M.S. Lutsenko, O.O. Kuznetsov, D.I. Prokopovich-Tkachenko, and V.P. Zverev, "Comparative analysis of biometric cryptosystems," (in rus), *Applied radio electronics*, vol. 17, no. 3, 4, pp. 182–191, 2018.
2. A.A. Kuznetsov, R.V. Sergienko, and A.A. Uvarova, "Fuzzy extractor on noise-tolerant codes for biometric cryptography," (in rus), *Radio engineering*, vol. 208, issue. 195, pp. 224–234.
3. Y. Dodis, R. Ostrovsky, L. Reyzin, and A.D. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. Comput*., vol. 38, no. 1, pp. 97–139, 2008.
4. Y. Dodis, L. Reyzin, and A. Smith, *Fuzzy Extractors. A Brief Survey of Results from 2004 to 2006.* Available: http://www.cs.bu.edu/~reyzin/papers/fuzzysurvey.pdf)
5. A. Juels and M. Sudan, "A fuzzy vault scheme," *Des. Codes Cryptography*, vol. 38, no. 2, pp. 237–257, 2006.
6. Anil K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Circ. Syst. Video Technol.*, vol. 14, no. 1, pp. 4–20, 2004.
7. Anil K. Jain, K. Nandakumar, A. Nagar, "Biometric template security," *EURASIP J. Adv. in Signal Process.*, pp. 1–17, 2008.
8. M. Upmanyu, A.M. Namboodiri, K. Srinathan, and C.V. Jawahar, "Efficient biometric verification in encrypted domain," *ICB '09: Proc. of the Third Int. Conf. on Biometrics.*, pp. 899–908, 2009.
9. U. Uludag, S. Pankanti, S. Prabhakar, and Anil K. Jain, "Biometric cryptosystems: issues and challenges," *Proc. IEEE 2004*, 92(6), pp. 948–960.

10. A. Astrakhantsev, G. Liashenko, and A. Shcherbak, "Noise resistance of remote authentication via LTE network," *Information and Telecommunication Sciences*, vol. 2, pp. 38–43, 2020.
11. G. Liashenko, A. Astrakhantsev, and V. Chernikova, "Network steganography application for remote biometrie user authentication," *IEEE 9th International Conference On Dependable Systems, Services And Technologies (DESSERT)*, pp. 326–330, 2018.
12. P. Jayapriya, R.R. Manimegalai, and R. Kumar Lakshmana, "A Survey on Different Techniques for Biometric Template Protection," *Journal of Internet Technology*, vol. 21, no. 5, 2020.
13. P. Poongodi and P.Betty, "A Study on Biometric Template Protection Techniques," *International Journal of Engineering Trends and Technology (IJETT)*, vol. 7, no. 4, 2014.
14. Edwin T.L. Rampine and Cynthia H. Ngejane, "A Brief Overview of Hybrid Schemes for Biometric Fingerprint Template Security," in *Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP 2016)*, pp. 340–346.
15. A. Sarkar and Binod K. Singh, "A Review on Different Biometric Template Protection Methods," *Recent Advances in Computer Science and Communications*, vol.14, issue 5, pp. 1551–1572, 2021.
16. V.G. Chernikova, A.A. Astrakhantsev, and G.Ye. Lyashenko, "Study of the characteristics of the iris biometric identification system", *Weapons systems and military equipment*, no.1 (53), pp.195–202, 2018.
17. 3GPP [TS 38.214]: NR; Physical layer procedures for data. Available: https://www.tech-invite.com/3m38/tinv-3gpp-38-214.html

Надійшла 23.06.2022

INFORMATION ON THE ARTICLE

Andrii A. Astrakhantsev, ORCID: 0000-0002-6664-3653, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Ukraine, e-mail: andrii.astrakhantsev@nure.ua

Galyna Ye. Liashenko, ORCID: 0000-0002-1741-9161, Kharkiv National University of Radio Electronics, Ukraine, e-mail: halyna.liashenko@nure.ua

DATA PROTECTION MANAGEMENT PROCESS DURING REMOTE BIOMETRIC AUTHENTICATION / A.A. Astrakhantsev, G.Ye. Liashenko

Abstract. Remote biometric authentication systems have recently become widespread due to the need to use common devices and make payments over the Internet. Because biometric methods are more user-friendly and now quickly replace passwords, the task of transmitting biometric information over an open network without compromising it is becoming urgent. This work aims to upgrade the remote authentication system to increase the secrecy and security of user biometric data. In order to achieve this goal, it is proposed to use the best security methods for forming biometric templates, network steganography to increase secrecy, and the introduction of an intelligent decision-making system. These improvements will increase the security and privacy of data during the remote authentication process.

Keywords: biometric template, remote authentication, attacks, network steganography.