УДК 004.056.55

ГЕНЕРАЦІЯ КЛЮЧІВ З БІОМЕТРИЧНИХ ОБРАЗІВ РАЙДУЖНОЇ ОБОЛОНКИ ОКА

М. С. ЛУЦЕНКО, О. О. КУЗНЕЦОВ, Ю. І. ГОРБЕНКО, А. І. ПУШКАРЬОВ, А. О. УВАРОВА

Розглядаються найпоширеніші підходи для створення біометричних криптосистем, зокрема, систем з генерацією ключа. Розробляється нова схема формування ключа методом нечітких екстракторів з біометричних даних райдужної оболонки ока. Запропонована програмна реалізація та проведено експериментальні дослідження алгоритму генерації ключів на основі біометричних даних, отриманих за розробленим методом нечітких екстракторів з райдужної оболонки ока.

Ключові слова: біометрія, біометричні криптосистеми, генерація криптографічних ключів, райдужна оболонка ока.

ВСТУП

На разі актуальним є питання поєднання класичної криптографії з технологією біометрії [1, 2]. Математичні моделі та методи захисту інформації, що засновані на використанні біометричних образів, стають одними з основних елементів у забезпеченні високо надійних ідентифікаційних та верифікаційних систем [3–16]. Наразі, вже існують методи створення біометричних ключів на основі обрисів тіла людини, обличчя, райдужної оболонки ока, голосу, геометрії долоні, відбитків пальців, обрисах судин долоні, динаміки машинного почерку і, навіть, ДНК тощо.

Біометричні дані – це унікальне цифрове представлення (модель) певної біометричної характеристики особи, яке отримане зі зчитувального біометричного пристрою (сканеру). Біометрія має декілька важливих переваг [3, 4]:

- біометрія однозначно ідентифікує осіб;
- отримані біометричні дані більш складні та випадкові, порівняно зі звичайними паролями, тому, вірогідно, матимуть більший запас криптографічної стійкості;
- біометричні дані є практично невід'ємною частиною особи, принаймні їх не можливо просто загубити, як, наприклад, носій – токен або смарт-картку – з ключем;
- біометричні образи при накладенні певних апаратних обмежень у системі, яка їх використовує, не можуть бути скопійовані та відтворені сторонньою особою.

Біометричні дані можуть бути використані у системах з генерацією ключа, у системах з відтворенням ключа та у системах зі зв'язуванням ключа. Залежно від обраного методу біометричні дані можуть як зберігатися в захищеному сховищі як шаблон для порівняння, слугувати доповненням до секретної інформації, що зберігається на певному носії або використовуватися для генерації криптографічного ключа [3–16]. Остання галузь застосування біометричних даних – генерація ключа з біометрії – не вимагає великого об'єму захищеного сховища та взагалі, його існування, має широкі можливості для використання у поєднанні з існуючими криптографічними методами. Наприклад, біометричні дані можуть бути використані як ключ для відомого алгоритму симетричного шифрування.

У біометричній криптосистемі з генерацією ключа псевдовипадкова послідовність (ключ) формується безпосередньо з біометричних даних користувача і не зберігається в системі. Це є незаперечною перевагою порівняно з іншими існуючими методами. Дійсно, такі системи є більш безпечними, але їх важко застосовувати через навіть незначну мінливість біометричних характеристик, оскільки необхідно з приблизно схожих даних згенерувати той самий ключ знову і знову. Також недоліком таких систем є неможливість (або суттєва обмеженість) сформувати новий ключ. Отже, якщо криптографічний ключ коли-небудь буде скомпрометований, то використання цього конкретного біометричного образу та конкретного алгоритму генерації ключа буде неможливе. У системі, де потрібне періодичне оновлення криптографічного ключа, це неприйнятно.

Найпоширенішою технологією, на якій базуються біометричні криптографічні системи з генерацією ключа, є нечіткі екстрактори. Метою цієї роботи є розробка та дослідження методу (нечіткого екстрактора) генерації ключів з біометричних образів райдужної оболонки ока. Розпізнавання райдужної оболонки ока – це автоматизований метод біометричної ідентифікації, який використовує математичні методи розпізнавання образів на фото та відео зображеннях [3–16]. Ця характеристика є складною, унікальною та стабільною. Розпізнавання райдужної оболонки використовує технологію відеокамери з інфрачервоним підсвічуванням для отримання зображень детальних та складних структур райдужної оболонки, які є видимими зовні.

1. РОЗРОБКА СХЕМИ ВИЛУЧЕННЯ БІОМЕТРИЧНИХ ДАНИХ МЕТОДОМ НЕЧІТКИХ ЕКСТРАКТОРІВ З РАЙДУЖНОЇ ОБОЛОНКИ ОКА

Розглянемо сучасний стан існуючих методів вилучення біометричних образів та створення криптосистем з генерацією ключів.

Дагман (англ. John Daugman) запропонував інтегро-диференціальний оператор для локалізації областей райдужки ока разом із видаленням можливих шумів повік [5, 6]. Проте автор не зазначив чи обробляються також шуми від зіниці та вій. Уайлдс (англ. Richard P. Wildes) виконує сегментацію райдужки за допомогою простих операцій фільтрування та гістограми [7]. За даною методикою можливо виявити шуми від повік, проте не від вій або зіниці. Боулз (англ. W. W. Boles) і Боаша (англ. B. Boashah) [8], Лім (англ. Lim) і співавт. [9] і Нох (англ. Noh) [10] головним чином зосереджувалися в своїх розробках на представленні зображення райдужки та узгодженні функції, і не вводили інформацію про сегментацію. Тиссе (англ. Tisse) та інші [11] запропонували метод сегментації на основі інтегро-диференціальних операторів з перетворенням Хафа. Це зменшило час обчислень і виключило потенційні центри поза знімком очей. Вії та зіниця також не враховувались у цьому методі. Ме (англ. Ma) та інші [12] запропонували оброблення райдужки шляхом сегментації та простої фільтрації.

Схема нечіткого екстрактора була модифікована Бойєном (англ. Boyen), в якій до хешування виконується фіксована перестановка біт двійкових послідовностей, отриманих з райдужної оболонки ока. Таким чином, передбачається формування декількох різних криптографічних ключів на основі одних і тих самих біометричних даних, але з використанням різних перестановок. Додатково секретним ключем в такому випадку може слугувати перестановка. Також, передбачається, що компрометація одного ключа не призведе до компрометації біометричних даних особи чи неможливості певної особи користуватися системою.

Хао (англ. Hao), Андерсон (англ. Anderson) and Дагман (англ. Daugman) представили метод генерації криптографічного ключа на основі біометричного методу, який використовує дані райдужки ока та дворівневу методику корекції помилок даних, що об'єднує коди Адамара та Рида-Соломона [6].

1.1. Метод нечітких екстракторів

Метричний простір – це множина M з функцією відстані

$$dis : M \times M \to \mathbb{R}^+ = [0, \infty).$$

У термінах даної роботи, нехай M завжди буде кінцевою множиною, а функція відстані прийматиме лише цілі значення та задовольнятиме такі вимоги:

– виконується аксіома тотожності:

$$dis(x, y) = 0 \text{ при } x = y;$$

– виконується аксіома симетрії:

$$dis(x, y) = dis(y, x);$$

виконується нерівність трикутника:

$$dis(x, z) \le dis(x, y) + dis(y, z).$$

Зосередимось на наступних показниках.

1. Відстань Хеммінга (англ. Hamming metric). Нехай, якщо $M = F^n$ для деякого алфавіту F, тоді $dis(w, w')$ – це кількість позицій, в яких рядки w та w' відрізняються.

2. Множина показників різниці (англ. Set difference metric). Нехай M складається з усіх підмножин універсальної множини U. Для двох множин w, w' їхня симетрична різниця дорівнює

$$w \Delta w' \overset{def}{=} \{x \in w \cup w' \mid x \notin w \cap w'\}.$$

Отже, відстань між двома множинами w, w' – це $|w \Delta w'|$.

3. Відстань редагування (англ. Edit metric). Нехай $M = F^n$, та відстань між w та w' визначається як найменша кількість додавань та видалень символів, необхідних для перетворення w в w'. (Ця метрика відрізняється від відстані Хеммінга, оскільки тут відбувається зсув символів).

Як вже згадувалося, всі три показники належать до біометричних даних.

Передбачуваність випадкової величини A визначається як $\max_a \Pr[A = a]$ і, відповідно, мінімальна ентропія $H_\infty(A)$ дорівнює

$$H_\infty(A) = \min_a -\log_2 \Pr(A = a) =$$

$$= -\log_2 \left(\max_a \Pr[A = a]\right) = \min_a \left\{\log_2 \frac{1}{\Pr[A = a]}\right\},$$

тим самим мінімальна ентропія може розглядатися як найгірший випадок ентропії.

Мінімальна ентропія розподілу послідовності визначає можливість отримати майже однакові випадкові біти.

Статистична відстань є мірою розрізнення. Статистична відстань між двома ймовірними розподілами A і B становить

$$SD(A, B) = \frac{1}{2} \sum_v |\Pr(A = v) - \Pr(B = v)|.$$

Для будь-якої системи, якщо A замінюється на B, вона вестиме себе як оригінальна система з ймовірністю принаймні $1 - SD[A, B]$.

За визначенням, (M,m,l,t,e) -нечітким екстрактором є пара рандомізованих процедур, процедури генерації Gen і процедури відтворення Rep з такими властивостями [10]:

1. Процедура генерації Gen на вході отримує $w \in M$ та на виході формує рядок $R \in \{0,1\}^l$ та допоміжні дані $P \in \{0,1\}^*$.

2. Процедура відтворення Rep приймає на вхід елемент $w' \in M$ і бітовий рядок $P \in \{0,1\}^*$. Властивість коректності нечітких екстракторів гарантує, що, якщо $dis(w,w') \le t$ та R, P були згенеровані за допомогою $(R, P) \leftarrow Gen(w)$, то $Rep(w', P) = R$. Якщо $dis(w,w') > t$, тоді ніякої гарантії не надається щодо вихідних даних.

3. Властивість безпеки гарантує, що для будь-якого розподілу W на M мінімальної ентропії m, рядок R має приблизно рівномірний розподіл навіть у випадку якщо зловмиснику відомо P, якщо $(R, P) \leftarrow Gen(W)$, то $SD((R, P),(U_l, P)) \le e$.

Нечіткий екстрактор ефективний, якщо Gen і Rep виконуються за менше, ніж поліноміальний час.

Іншими словами, нечіткі екстрактори дозволяють витягнути деяку випадковість R з w, а потім успішно відтворити R з будь-якого рядка w', близького до w. У відтворенні використовуються допоміжні дані P, що утворюються під час початкового вилучення; однак P не обов'язково мають зберігатися в таємниці, оскільки R близькі до дійсно випадкової послідовності, навіть, якщо відомі P. Сильні екстрактори дійсно можуть розглядатися як "чіткі" аналоги нечітких екстракторів, що відповідають якщо припустити, що $t = 0$, $P = X$ та $M = \{0,1\}^n$.

1.2. Вилучення біометричних даних з райдужної оболонки ока

Райдужна оболонка ока визнана одним із найнадійніших, унікальних та неінвазійних біометричних методів для отримання біометричних даних особи. Вважається, що ця метрика особи немає залежності від генетики людини, а отже гарантує унікальну ідентифікацію людини. Розпізнавання райдужної оболонки ока розглядається як найбільш надійна та точна біометрична система ідентифікації, яка використовується в сучасну епоху. Більшість комерційних систем розпізнавання оболонок ока використовують запатентовані алгоритми, розроблені Дагманом, і ці алгоритми мають високий рівень коректності розпізнавання особи.

Як фізіологічний параметр розглядається райдужна оболонка ока – кругла пластинка з кришталиком в центрі, одна з трьох складових судинної оболонки ока. Райдужна оболонка знаходиться між рогівкою і кришталиком і виконує функцію своєрідної природної діафрагми, регулюючої надходження світла в око. Райдужна оболонка пігментована. За своєю структурою райдужна оболонка складається з еластичної матерії – трабекулярної мережі. Трабекулярна мережа – сітчасте утворення, що складається з поглиблень, гребінчастих стяжок, борозен, кілець, зморшок, веснянок, судин і інших рис. Завдяки такій кількості складових «візерунок» мережі досить випадковий (вважається, що ймовірність співпадіння двох райдужок різних людей дорівнює 2^{-78}), що веде до великої ймовірності унікальності райдужної оболонки. Візерунок траберкулярної мережі залишається незмінним протягом усього життя людини. Винятком вважається отримання серйозної травми і хірургічне втручання.

У даній роботі усі зображення були взяті з бази даних райдужних оболонок ока CASIA Iris Image Database. Зображення цієї бази даних CASIA-Iris-Interval були захоплені камерою, що є новою розробкою компанії CASIA для захоплення райдужки ока. Завдяки новому дизайну ця камера може захоплювати дуже чіткі зображення райдужки.

Сегментація. Сегментація – це процес пошуку найбільш корисної частини зображення райдужки для подальшої обробки. Це робиться шляхом локалізації зіниці та межі райдужної оболонки, вії та повік. У випадку відсутності належної сегментації, наступні етапи розпізнавання райдужки будуть некоректними через велику кількість сторонніх даних (шум), у результаті будуть сформовані помилкові дані як шаблон. Для швидкої сегментації райдужної оболонки [13–15] можливо локалізувати її простим поєднанням гауссівської фільтрації (англ. Gaussian filtering), виявлення краю райдужки оператором Кенні (англ. Canny edge detection operator) та трансформації Хафа (англ. Hough transform). Трансформація Хафа [16] використовується для визначення радіуса та центру зіниці та райдужки. Оператор Кенні використовується для виявлення країв зображення райдужки, він є достатньо ефективним.

Оператор Кенні. Алгоритм виявлення меж райдужної оболонки ока за допомогою оператора Кенні можна розділити на 5 етапів:

1. Застосувати фільтр Гаусса для згладжування зображення, щоб вилучити шум та вилучити небажані деталі зображення:

$$g(m,n) = G_\sigma(m,n) \cdot f(m,n),$$

де

$$G_\sigma = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{m^2+n^2}{2\sigma^2}}.$$

2. Знайти градієнти інтенсивності зображення. Для цього можна використати будь-який з існуючих

градієнтних операторів: Робертса (англ. Roberts), Собеля (англ. Sobel), Прейвіта (англ. Prewitt), тощо. У результаті

$$M(n,n)=\sqrt{g_m^2(m,n)+g_n^2(m,n)}$$

та

$$\Theta(m,n)=\frac{1}{\tan\left(\frac{g_n(m,n)}{g_m(m,n)}\right)}.$$

3. Застосувати заглушення немаксімумів, щоб позбутися від помилкових даних на виявленому краї. Тобто на основі заданого порогового значення формуються приблизні межі райдужки:

$$M_T(m,n)=\begin{cases}M(m,n), & if\ M(m,n)>T\\ 0, & if\ M(m,n)\le T\end{cases},$$

де T обирається таким, що всі елементи краю збереглися, тоді як більша частина шуму була вилучена.

4. Застосувати подвійний поріг для визначення потенційних меж. Межу, отриману на попередньому етапі, потрібно уточнити. Подамо $M_T(m,n)$ у вигляді масиву даних довжиною k елементів, тобто

$$M_T(m,n)=\{M_{T0}(m,n),M_{T1}(m,n),\ldots,M_{Tk}(m,n)\}.$$

У такому випадку до кожного з таких елементів застосовуватимуться:

$$M_{Ti}(m,n)\begin{cases}M_{Ti}(m,n), & if\ M_{Ti}(m,n)>M_{Ti-1}(m,n),\\ & M_{Ti}(m,n)>M_{Ti+2}(m,n)\\ 0, & otherwise\end{cases}$$

де $M_{Ti-1}(m,n)$ та $M_{Ti+1}(m,n)$ – сусідні елементи за напрямом градієнту $\Theta(m,n)$.

5. Виділити край райдужки, пригнічуючи всі інші ребра, які слабкі і не пов'язані з сильними краями райдужки. Виділити дані, отримані на попередньому етапі за двома пороговими значеннями τ_1 та τ_2 ($\tau_1<\tau_2$) для отримання двох двійкових зображень T_1 та T_2. Слід зауважити, що T_2 зі збільшенням τ_2 містить менше шуму та помилкових меж, проте збільшуються прогалини поміж сегментами межі, відповідно це справедливо і для T_1 зі зменшенням τ_1. Потім необхідно поєднати сегменти T_2, щоб утворити суцільну межу. Для цього, необхідно знайти кінець сегменту T_2 та відстежити його сусідів у T_1, поєднати ці два елементи, а потім продовжити шукати сусідів елементу з T_1 у T_2.

Трансформація Хафа. Зазвичай перетворення Хафа використовується для виявлення певних ліній, проте можливе використання і для виявлення кругової області зображення, в даному випадку, зіниці ока. Отже алгоритм складається з наступних етапів.

1. Створити аккумулятивний простір, який за розміром співпадає з розміром вхідного зображення. Спочатку для кожної комірки встановлено значення 0.

2. Для кожної точки межі (i,j) на зображенні, інкрементуються усі точки, які згідно з рівнянням

$$(i-a)^2+(j-b)^2=r^2$$

можуть бути центром кругу. Такі точки у рівнянні позначені як a.

3. Для кожного можливого значення a, знайденого на попередньому кроці, виконується пошук усіх можливих значень b, які задовольняють рівняння.

4. Виконується пошук локальних максимумів в акумулятивному просторі. Ці точки становлять кола, які були виявлені алгоритмом.

Якщо не відомо радіус кола, який необхідно знайти заздалегідь, можливе використання тривимірного простору акумулятора для пошуку кругів з довільним радіусом. Проте це значно погіршить швидкодію алгоритму.

Цей метод також може виявити кола, які частково знаходяться за межами акумулятивного простору, якщо в цьому просторі ще є достатня кількість області кола.

Нормалізація. Після визначення меж зображення райдужної оболонки необхідно нормалізувати. Це необхідний крок, покликаний компенсувати зміни розмірів зіниці. Локалізована райдужка нормалізується до прямокутного блоку з фіксованим розміром, що відповідає ширині блоку, а кутове зміщення Θ відповідає довжині блоку, як показано на рис. 1.

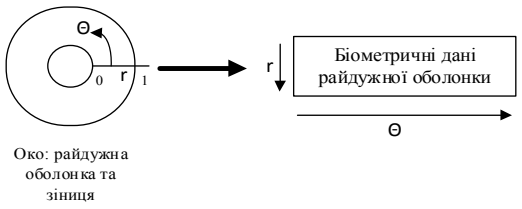

Рис. 1. Схематичне подання нормалізації зображення райдужної оболонки ока

Найпоширенішим способом нормалізації є побудова моделі розгортки Дагмана (англ. Daugman's rubbersheet model) [5, 6]. Формально нормалізація це лінійна модель, яка формується з відповідних кожному пікселю райдужної оболонки, незалежно від її розміру і стану розширення зіниці, пару полярних координат (r,Θ), де r знаходиться на одиничному інтервалі $r\in[0,1]$ і Θ є кут в діапазоні $\Theta\in[0,2\pi]$. Відображення зображення райдужної оболонки (x_i,y_i) та зіниці

(x_p, y_p) від декартової системи координат до безрозмірної неконцентричної полярної системи координат (r,Θ) можна подати так:

$$I\big(x(r,\Theta), y(r,\Theta)\big) \to I(r,\Theta),$$

що складається з

$$x(r,\Theta) = (1-r)\,x_p(\Theta) + x_i(\Theta),$$

$$y(r,\Theta) = (1-r)\,y_p(\Theta) + y_i(\Theta),$$

де:

$x(r,\Theta)$ та $y(r,\Theta)$ визначаються як лінійні комбінації множини точок зорієнтованої межі зіниці $\big(x_p(\Theta), y_p(\Theta)\big)$, так множини кінцевих точок зовнішнього периметру райдужної оболонки $\big(x_i(\Theta), y_i(\Theta)\big)$,

$I\big(x(r,\Theta), y(r,\Theta)\big)$ – область райдужної оболонки ока у декартовій системі кооординат,

$I(r,\Theta)$ – це область райдужної оболонки ока, що представлення в полярних координатах.

Приклад нормалізації зображення райдужки ока наведено на рис. 2.

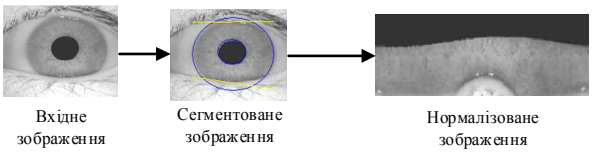

Рис. 2. Формування нормалізованого зображення райдужної оболонки ока

Формування даних. Формування даних – це процес вилучення інформації з зображення райдужки. В ході вилучення даних райдужної оболонки з нормалізованого зображення виділяють контрольну область. До кожної точки обраної області застосовують фільтри Габора (англ. Gabor filter) [13–15], для того, щоб витягти фазову інформацію. Можна застосовувати й інші фільтри, але принцип залишається таким самим. Існує декілька показників, за якими можна порівняти фільтри, а саме [3–16]:

1. FAR (англ. False Accept Rate) – ймовірність помилкової ідентифікації, тобто ймовірність того, що система ідентифікації помилково визнає справжність користувача, якого не зареєстровано в системі.
2. FRR (англ. False Reject Rate) – ймовірність того, що система біоідентифікації не визнає справжність біометричних даних зареєстрованого в ній користувача.
3. EER (англ. Equal error rate) – коефіцієнт рівного рівня помилок, при якому обидві помилки (помилка прийому і помилка відхилення) еквівалентні. Чим менше EER, тим точнішою буде система.

Безсумнівним плюсом фазової складової є те, що вона, на відміну від амплітудної інформації не залежить від контрасту зображення і освітлення. Слід зазначити, що ці дані не можуть бути використані для реконструкції зображень ока. Фільтр Габора дають змогу сформувати інваріантну систему для вилучення біометричних ознак. Фільтр Габора – це лінійний фільтр, який є згорткою перетворень Фур'є гармонійної функції і функції Гауса.

Нехай f позначає частоту синусоїдальної плоскої хвилі, а α і β – просторові константи Гаусової оболонки по осі x' і y', а Θ – орієнтація фільтра Габора. В такому випадку, двовимірний фільтр Габора визначається як:

$$G(x,y,\Theta) = \frac{1}{2\pi\alpha\beta} e^{-\left(\frac{x'^2}{2\alpha^2}\right)-\left(\frac{y'^2}{2\beta^2}\right)} \cos(2\pi f x'),$$

$$x' = x\sin\Theta + y\cos\Theta,$$

$$y' = -x\cos\Theta + y\sin\Theta.$$

Відповідне подання в просторово-частотній області:

$$H(u,v) = e^{-2\pi^2\left[(u-F)^2\alpha^2 + v^2\beta^2\right]}.$$

Обробка біометричних даних. Залежно від обраних алгоритмів сегментації, нормалізації та формування даних, можна отримати різний об'єм біометричних даних. Наприклад, лише фільтр Габора може формувати блоки даних довжиною від 1 до 256 біт. Використання блоків певної довжини залежить від потреб системи, так наприклад, використання блоку довжиною, наприклад, 16 біт надає можливість ігнорувати деякий шум зображення. Оскільки передбачається формування криптографічного ключа з біометричних даних, використання блоку довжиною 256 біт має більший запас стійкості перед криптографічними атаками типу груба сила, проте у таких системах більш високі критерії до відсутності шумів у біометричних даних. Зазвичай, параметри перетворення фільтра Габора обирають компромісно залежно від вимог до рівня криптографічної безпеки системи.

Отже, процедури етапу формування біометричних даних можна подати як це зображено на рис. 3.

Після етапу формування біометричних даних починається етап генерації криптографічного ключа.

1.3. Генерація криптографічного ключа з біометричних даних райдужної оболонки ока методом нечітких екстракторів

Етап генерації ключа складається з двох складових:

- виконання завадостійкого кодування біометричних даних;
- хешування отриманої послідовності.

Завадостійке кодування потрібно, безпосередньо, як реалізація методу нечітких екстракторів.

Процедура хешування опціональна. Вона необхідна для того, щоб компрометація сформованого ключа не призводила до компрометації біометричного образу або не унеможливлювала (не обмежувала) можливості щодо використання певною особою системи. Тобто у разі компрометації ключа, у системі буде на основі тих самих біометричних даних сформовано новий ключ лише з використанням іншого набору параметрів для хешування.

Рис. 3. Запропонована схема обробки зображення для вилучення біометричних даних з райдужної оболонки ока

Завадостійке кодування кодами Ріда-Соломона. Коди Ріда-Соломона – це циклічні коди [1–2], що виправляють помилки, з елементами – блоками довільної довжини. Усі елементи належать полю $GF(2^k)$, усі операції також виконуються в цьому полі. В даній роботі було використано поле $GF(2^8)$ за породжуючим поліномом:

$$y = x^8 + x^4 + x^3 + x^2 + 1.$$

Дамо визначення основним змінним перетворень:

– Нехай $\left\{\alpha^0, \alpha^1, \alpha^2, ..., \alpha^{|F|-2}\right\}$ будуть елементами поля $GF\left(2^8\right)$;

– k означатиме довжину біометричних даних, що підлягають кодуванню, $1 \le k < |F|$;

– m – це кількість помилок, які можуть бути виправлені, $1 \le m < |F| - k$;

– Нехай $n = k + m$ означатиме довжину блоку даних, який отримано після кодування, $2 \le n < |F|$.

Процедура кодування має такий вигляд [1–3].

Вхідні дані: послідовність $M = \left(M_0, M_1, ..., M_{k-1}\right)$, $M_i \in GF\left(2^8\right)$.

Вихідні дані: послідовність $s = \left(s_0, s_1, ..., s_{n-1}\right)$, $s_i \in GF\left(2^8\right)$.

1. Визначимо поліном генератора як:

$$g(x) = \prod_{i=0}^{m-1}\left(x - \alpha^i\right) = \left(x - \alpha^0\right)\left(x - \alpha^1\right)...\left(x - \alpha^{m-1}\right).$$

2. Визначимо поліном послідовності:

$$M(x) = \sum_{i=0}^{k-1} M_i x^i = M_0 x^0 + M_1 x^1 + ... + M_{k-1} x^{k-1}.$$

3. Кодові слова коду Ріда-Соломона визначається як:

$$s(x) = M(x)x^m - \left[\left(M(x)x^m\right) \bmod g(x)\right],$$

$$s(x) = \sum_{i=0}^{n-1} s_i x^i = s_0 x^0 + s_1 x^1 + ... + s_{n-1} x^{n-1}.$$

Процедура декодування виконується в декілька етапів, а саме [1–3]:

1) Обчислення синдрому помилки;
2) Побудова поліному помилки;
3) Знаходження коренів поліному помилки;
4) Визначення характеру помилки та виправлення її.

На сьогодні коди Ріда - Соломона мають дуже широку сферу застосування завдяки їхній здатності знаходити і виправляти багаторазові помилки.

Хешування даних алгоритмом Купина (ДСТУ 7564:2014). Купина (англ. Kupyna) – ітеративна криптографічна функція хешування, прийнята як національний стандарт України ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція хешування» [17].

ДСТУ 7564:2014 визначає функцію хешування, передбачається використання двох основних реалізацій «Купина-256» або «Купина-512», що формують хеш довжиною 256 та 512 біт відповідно.

Алгоритм генерації хешу має наступний вигляд. В ході формування хешу повідомлення доповнюється, далі поділяється на l -бітні блоки $m_0,...,m_t$, після чого виконується обробка кожного блоку шляхом ітеративного виконання функції стиснення ϕ. При цьому формуються значення $h_i = \varphi(h_{i-1}, m_i)$, де $i = 1,...,t$, а початкове значення $h_0 = IV$. Після обробки останнього блоку повідомлення результуюче хеш-значення обчислюється як $H(M) = \Omega(h_t)$, де Ω – завершальне перетворення, що повертає n-бітне значення, кратне 8 ($0 < n \le \frac{l}{2}$).

Основні перетворення. Функція стиснення ϕ складається з перетворень l -бітного блока P і Q та визначається так:

$$\varphi(h,m) = P(h \oplus m) \oplus Q(m) \oplus h .$$

Завершальне перетворення Ω визначається так:

$$\Omega(x) = trunc_n(P(x) \oplus x) .$$

Перед виконанням перетворень P і Q вхідна послідовність подається як внутрішній стан функції хешування довжиною l біт ($l = 512$ або $l = 1024$ залежно від розміру внутрішнього стану). Після завершення виконання перетворень P і Q внутрішній стан знову трансформується у послідовність байт, яка подається на вхід наступної ітерації функції стиснення ϕ або на завершальне перетворення для формування результуючого хеш-значення.

Перетворення P і Q є варіантами блокового шифру, в яких замість циклових ключів використовуються визначені константи. Кількість циклів (r) залежить від розміру внутрішнього стану.

Функція хешування, визначена в ДСТУ 7564:2014, формує хеш-значення для повідомлення, що складається з бітової послідовності довжини від 0 біт (порожній рядок) до $2^{96} - 1$ біт. У даній роботі було використано алгоритм хешування для формування послідовності довжиною 512 біт.

Результати проведених ретельних досліджень [1] криптографічної стійкості ДСТУ 7564:2014 дозволяють зробити висновок про її високий рівень захищеності. Тому алгоритм, що реалізований в ДСТУ 7564:2014, забезпечує стійкість до атак на алгоритми хешування, зокрема до атак знаходження прообразів та здійснення колізій.

Формування криптографічного ключа. Формування ключа відбувається методом нечітких екстракторів за схемою приватного шаблону. Алгоритм генерації ключа схематично подано на рис. 4.

Для покращення властивостей роботи алгоритму використовуватимуться допоміжні дані – біти перевірки завадостійкого коду Ріда-Соломона для виправлення помилок. Нижче наведено алгоритм формування криптографічного ключа запропонованої схеми.

Алгоритм генерації ключа складається із виконання наступних кроків.

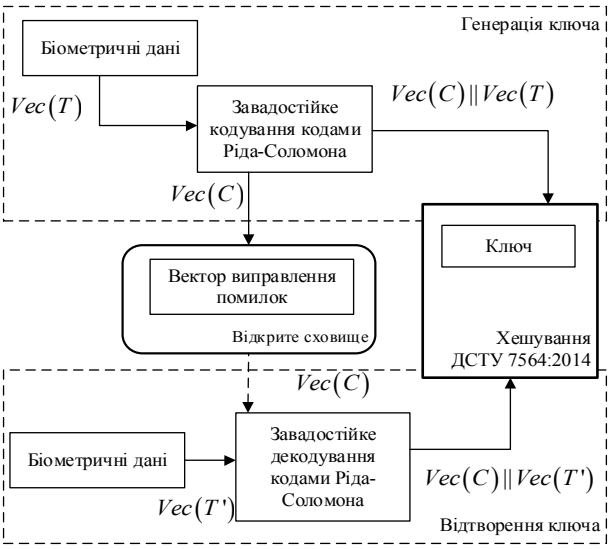

Рис. 4. Схематичне зображення запропонованої біометричної криптографічної системи з генерацією ключа

1. До біометричного образу T довжиною M біт, застосовується кодування кодами Ріда-Соломона. У результаті формується вектор корекції помилок $Vec(C)$

$$Vec(C) = (C_1, C_2, ..., C_n),$$

для n-бітного коду, визначений як $Vec(c_i) = (c_{i,1}, c_{i,2}, ..., c_{i,n})$.

Потім, вектор контрольної суми поєднується з біометричними даними

$$Vec(C) \| Vec(T) .$$

Загалом, послідовність після кодування має вигляд

$$Vec(C,T) = (C_1, C_2, ..., C_n \| T_1, T_2, ..., T_M) .$$

2. Отриманий після кодування вектор корекції помилок $Vec(C)$ може зберігатися у будь-якому відкритому сховищі, наприклад, на смарт-карті або токені.

3. Для формування ключа виконується хешування за алгоритмом хешування Купина-512 послідовності $Vec(C) \| Vec(T)$

$$Key = Hash[Vec(C) \| Vec(T)] .$$

4. У результаті сформована послідовність довжиною 512 біт, яка придатна для використання як криптографічний ключ.

Алгоритм відтворення ключа:

1. До біометричного образу T' довжиною M біт додається вектор корекції помилок, що було сформовано (3.33):

$$Vec'(C,T') = (C_1, C_2, ..., C_n \| T_1', T_2', ..., T_M').$$

2. До отриманої послідовності $Vec'(C,T')$ застосовується декодування алгоритмом Ріда-Соломона. Після успішного декодування формується вектор $Vec(T')$. У разі неможливості правильного декодування послідовності $Vec'(C,T')$ зчитується новий біометричний образ, заново застосовується алгоритм відтворення ключа з п.1.

3. Для формування ключа виконується хешування $Vec(C) \| Vec(T')$ та, залежно від реалізації, з допоміжними даними

$$Key = Hash\left[Vec(C) \| Vec(T')\right].$$

Відтворений ключ можна використовувати за призначенням.

2. ПРОГРАМНА РЕАЛІЗАЦІЯ ТА ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ

2.1. Вхідні та вихідні дані алгоритму генерації

Умовно розділимо алгоритм генерації на два етапи: вилучення біометричних даних та генерацію ключа.

На етапі вилучення біометричних даних вхідними даними буде зображення (двовимірний масив даних) ока певного розміру. Розмір зображення залежить виключно від фізичного обладнання, що було використано для захоплення зображення ока людини. Якщо використовувати зображення ока, що містяться у бібліотеці CASIA, то розмір зображення ока дорівнюватиме 320×280 пікселів.

Розмір вихідних даних також може варіюватися. Використання у алгоритмі фільтрів, таких як фільтр Габора, дає змогу варіювати (квантувати) значення елементів результуючої послідовності біометричних даних у діапазоні від 1 до 256 біт. Кодування блоку пікселів меншою бітовою послідовністю дає змогу зневажити вплив яскравості зображення або інших завад на формування даних, проте знижується ймовірність коректного формування ключа.

Загалом, результатом застосування фільтра Габора є вектор $Vec_{GABOR}(BD)$

$$Vec_{GABOR}(BD) = (BD_1, BD_2, ..., BD_m)$$

довжиною $m = 8192$ елементи, які

$$BD_i \in GF\left(2^k\right), i = 1,2,...,m,\ k = 1,2,...,8,$$

де $GF\left(2^k\right)$ – розширення двійкового поля Галуа ступеня k, де k може приймати значення від ступеня квантування.

Проте зважаючи на те, що отримати повне зображення райдужки ока досить важка задача, оскільки у нормальному стані око людини відкрито неповністю, райдужку можуть частково перекривати верхнє та нижнє повіки, вії. Отже, приблизно ¾ райдужної оболонки ока можливо захопити без спричинення незручностей для користувача системи. У контексті алгоритму це означає, що більш доречно враховувати лише 6144 елементи вектора, отриманого після застосування фільтра Габора, тобто $M = 6144$.

Отже, вихідними даними етапу вилучення даних є вектор

$$Vec_{GABOR}(BD) = (BD_1, BD_2, ..., BD_M)$$

з елементами

$$BD_i \in GF\left(2^8\right), i = 1,2,...,M.$$

Вхідними даними для етапу генерації ключа є бітовий масив довжиною $L = M \times k = 6144 \times 8 = 49152$ біт, що було сформовано з вектора $Vec_{GABOR}(BD)$. Вихідними даними є бітова послідовність довжиною 512 біт – криптографічний ключ.

2.2. Приклад використання програмного забезпечення

Етап вилучення даних з зображення ока подано на рис. 5.

Найчастіше, нормалізоване зображення райдужної оболонки фільтрується набором двовимірних фільтрів Габора з $\Theta = 0^o$, $\Theta = 45^o$, $\Theta = 90^o$ та $\Theta = 135^o$. На рис. 5 подано усі чотири варіанти застосування фільтра. Проте, для того щоб обрати певний фільтр для формування даних у реалізації, була проведена перевірка відповідності даних отриманих після фільтрування до рівномірного розподілу. Сформовані вектори $Vec_{GABOR}(BD)_\Theta$ були перетворені у двійкові послідовності.

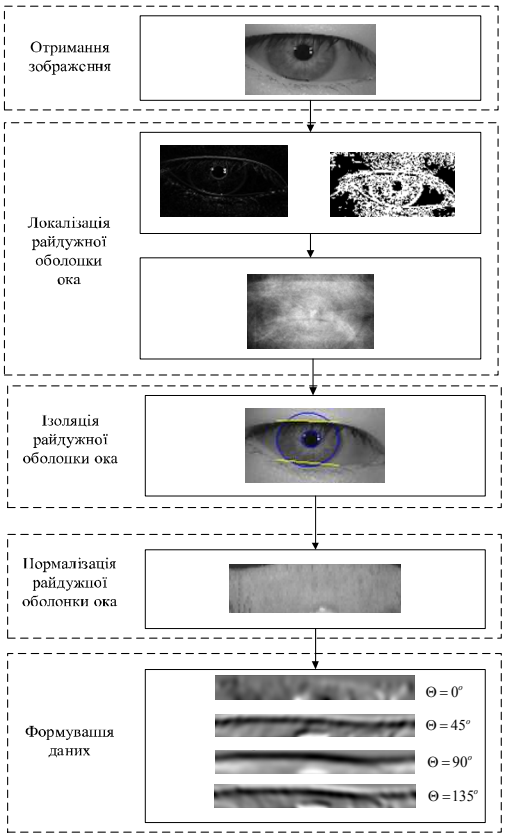

Рис. 5. Результати застосування запропонованої схеми обробки зображення для вилучення біометричних даних з райдужної оболонки ока на етапі вилучення даних

2.3. Експериментальні дослідження алгоритму генерації ключів

Для основних перетворень на обох етапах виконання реалізації було отримано наступні показники швидкодії, як показано у таблиці 1.

Таблиця 1

Оцінка швидкодії запропонованої програмної реалізації алгоритму генерації ключів з райдужної оболонки ока

Операція	Швидкодія, мс
Локалізація райдужної оболонки ока - оператор Кенні - перетворення Хафа	 43,64 826
Ізоляція райдужної оболонки ока	2,9
Нормалізація райдужної оболонки ока	6,58
Формування даних	113,09
Коди Ріда-Соломона - Кодування - Декодування	 1,56 2,14
Хешування алгоритмом Купина	1,02

Для оцінки швидкодії було виконано обчислення часу виконання операції під час обробки кожного з 756 зображень з бази CASIA. Слід зазначити, що не дивлячись на високі показники швидкодії, ці результати можуть бути оптимізовані. Аналіз швидкодії проводилися на обчислювальній платформі з ОС Windows 10 x64, Intel Core i7, 4.7 ГГц. Оцінимо запропонований алгоритм за такими параметрами, як ймовірність помилкової ідентифікації (FAR) та ймовірність того, що система не визнає справжність біометричних даних зареєстрованого в ній користувача (FRR).

В ході аналізу цих параметрів, слід зазначити, що отримані практичні результати доводять, що райдужна оболонка ока дійсно носить унікальний характер. Оскільки, раніше було зазначено, що послідовності, отримані на виході з фільтра Габора, досить схожі з випадковими послідовностями, подальші оцінки наведені для даних, подібних до вихідних послідовностей Габора, проте створених генератором випадкових чисел.

Отже, отримано, що ймовірність помилкової ідентифікації для запропонованого алгоритму досить низка FAR = 0,14%. Більш цікавим з точки зору дослідження є показник ймовірності відхилення справжніх біометричних даних користувача, оскільки в запропонованому алгоритмі застосовується метод нечітких екстракторів. Таким чином, встановлено, що рівень FRR для запропонованого алгоритму дорівнює 19.5%. Це досить високий показник ефективності алгоритму, проте актуальним питанням є підвищення рівня надійності роботи реалізації.

На рис. 6 наведено залежність рівня FRR від виправляючої можливості коду для запропонованої реалізації.

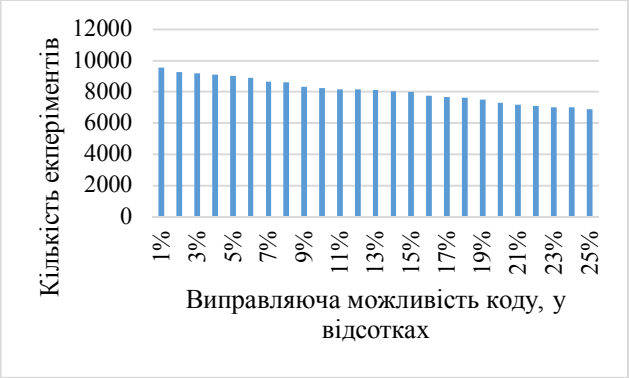

Рис. 6. Залежність ймовірності вдалого декодування від виправляючої можливості кодів Ріда-Соломона

Для виконання даного аналізу формувалася випадкова двійкова послідовність, потім вона підлягала кодуванню кодами Ріда-Соломона, коректуючий вектор запам'ятовувався, а потім вхідна послідовність зазнавала змін відповідно до можливостей виправляючого коду (розглянуто коди, які можуть виправляти від 1% до 25% помилок). Потім відбувалося декодування послідовності. Така процедура повторювалася 10000 разів. На гістограмі наведено кількість успішних декодувань пошкоджених послідовностей. За отриманими результатами можна зробити висновок, що пошук оптимального алгоритму завадостійкого кодування є також перспективним напрямом подальших досліджень.

ВИСНОВКИ

У даній роботі запропоновано алгоритм вилучення біометричних даних з райдужної оболонки ока на основі схеми нечітких екстракторів. Запропонова-

ний алгоритм складається з двох етапів: вилучення даних та генерації криптографічних ключів. На етапі вилучення даних застосовуються такі перетворення: оператор Кенні, перетворення Хафа, фільтр Гауса, модель розгортки Дагмана, двовимірний фільтр Габора. На етапі генерації використовуються алгоритми класичної криптографії: алгоритм кодування Ріда-Соломона, який за свою досить довгу історію існування добре себе зарекомендував, та український національний стандарт хешування «Купина», який було прийнято у 2014 році після детальних досліджень, з високими криптографічними показниками.

Також у роботі було проведено оцінку показників ефективності розробленого алгоритму. Виконання повної процедури вилучення даних та генерації ключа займає менше 1 секунди. Показники ймовірності помилкової ідентифікації FAR та ймовірність помилкового відхилення даних FRR дорівнюють, відповідно, 0,14% та 19.5%.

Література

[1] *Горбенко І.Д.* Прикладна криптологія. Теорія. Практика. Застосування: монографія. / І.Д. Горбенко, Ю.І. Горбенко. – Харків: «Форт», 2012. – 870 с.

[2] *Есин В.І.* Безпека інформаційних систем і технологій./ Есин В.І., Кузнецов О.О., Сорока Л.С.. – Харків: ХНУ ім. В.Н. Каразіна, 2013. – 632 с.

[3] *U. Uludag, S. Pankanti, S. Prabhakar, A. Jain.* Biometric Cryptosystems: Issues and Challenges. Proceedings of the IEEE. – June 2004. – Vol. 92, NO. 6.

[4] *Anil K. Jain, Arun Ross.* An Introduction to Biometric Recognition. IEEE Transactions on circuits and systems for video technology, 2004, Vol. 14, NO. 1, pp. 4–20.

[5] *J. Daugman* How iris recognition works / J. Daugman . – Circuits and Systems for Video Technology, IEEE Transactions, 2004, Vol 14, NO 1, pp. 21–30

[6] *F. Hao, R. Anderson, J. Daugman.* Combining crypto with biometrics effectively. IEEE Transactions on Computers. – 2006. – Vol. 55. – pp. 1081-1088.

[7] *Richard P. Wildes*. Iris recognition: An emerging biometric technology. Proceedings of the IEEE, 1997, Vol. 85, pp. 1348–1363.

[8] *W. W. Boles, B. Boashash.* A human identification technique using images of the iris and wavelet transform, IEEE Trans. Signal Process. – 1998. – Vol. 46, NO. 4. – pp. 1185–1188

[9] *S. L. Lim, K. L. Lee, O. B. Byeon, T. K. Kim.* Efficient Iris Recognition through Improvement of Feature Vector and Classifier. ETRI J. – 2001. – Vol. 23, NO. 2, pp.61–70 .

[10] *K. Bae, S. Noh, J. Kim.* Iris Feature Extraction using Independent Component Analysi. 4th International Conference on Audio-and Video-based Biometric Person Authentication, Guildford, UK. – 2003. – pp. 838–844.

[11] *C. Tisse, L. Martin, L. Torres, M. Robert.* Person identification technique using human iris recognition. Proc. Vis Interface. – 2002. – pp.294–299.

[12] *L. Ma, T. Tan, Y. Wang, D. Zhang*. Efficient iris recognition by characterizing key local variations. IEEE. Image Process. – 2004. – Vol. 13. – pp. 739–750.

[13] *C. Rathgeb, A. Uhl, P. Wild.* Iris-biometrics: from segmentation to template security. Advances in Information Security, Springer. – 2013.

[14] *M.R. Ogiela, L. Ogiela.* Image based crypto-biometric key generation. 2011 Third International Conference on Intelligent Networking and Collaborative Systems, Fukuoka, Japan. – 2011. – pp. 673–678.

[15] *L. Wu, X. Liu, S. Yuan, P. Xiao.* A novel key generation cryptosystem based on face features. In Signal Processing (ICSP), 2010 IEEE 10th International Conference, 2010, pp. 1675–1678.

[16] *Sunil Chawla, Aashish Oberoi.* A Robust Algorithm for Iris Segmentation and Normalization using Hough Transform. Global Journal of Business Management and Information Technology. – 2011. – Vol. 1, No. 2. – pp.69–76

[17] Національний Стандарт України ДСТУ 7564:2014. Інформаційні технології. Криптографічний захист інформації. Функція гешування. – К: 2014. – 41 с.

Надійшла до редколегії 20.12.2018

Луценко Марія Сергіївна, науковий співробітник ПАТ «ІІТ», здобувач кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В.Н. Каразіна. Галузь наукових інтересів – біометрична криптографія, блокові симетричні шифри.

Кузнецов Олександр Олександрович, доктор технічних наук, професор, заступник головного конструктора ПАТ «ІІТ», професор кафедри безпеки інформаційних систем і технологій Харківського національного університету ім. В.Н. Каразіна. Галузь наукових інтересів – криптографія та автентифікація, алгебраїчна теорія кодів, обробка, передача та захист інформації.

Горбенко Юрій Іванович, кандидат технічних наук, виконавчий директор ПАТ «ІІТ», старший науковий співробітник кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В.Н. Каразіна. Галузь наукових інтересів – криптографія та автентифікація, інфраструктура відкритих ключів.

Пушкарьов Андрій Іванович, директор департаменту захисту інформації Адміністрації державної служ-би спеціального зв'язку та захисту інформації України. Галузь наукових інтересів – теорія захисту інформації, інформаційна та кібербезпека держави.

Уварова Анна Олександрівна, провідний інженер Конструкторського бюро «Південне» ім. М. К. Янгеля», здобувач кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В.Н. Каразіна. Галузь наукових інтересів – біометрична криптографія, блокові симетричні шифри.

УДК 004.056.55

Луценко М. С. **Генерация ключей из биометрических образов радужной оболочки глаза** / М. С. Луценко, А. А. Кузнецов, Ю. И. Горбенко, А. И. Пушкарев, А. А. Уварова // Прикладная радиоэлектроника: науч. – техн. журнал. – 2018. – Том 17, №. 3, 4. – С. 104–114.

Рассматриваются наиболее распространенные подходы для создания биометрических криптосистем, в частности, систем с генерацией ключа. Разрабатывается новая схема формирования ключа методом нечетких экстракторов из биометрических данных радужной оболочки глаза. Предложена программная реализация и проведены экспериментальные исследования алгоритма генерации ключей на основе биометрических данных, полученных разработанным методом нечетких экстракторов из радужной оболочки глаза.

Ключевые слова: биометрия, биометрические криптосистемы, генерация криптографических ключей, радужная оболочка глаза.

Табл. 1. Ил. 6. Библиогр.: 17 наим.

UDC 004.056.55

Lutsenko M. **Generation of keys using biometric images of the iris of the eye** / M. Lutsenko, A. Kuznetsov, Yu. Gorbenko, A. I. Pushkarev, A. Uvarova // Applied Radio Electronics: Sci. Journ. – 2018. – Vol. 17, № 3, 4. – P. 104–114.

The most common approaches for creating biometric cryptosystems, in particular, systems with key generation, are considered. A new key generation scheme is being developed using fuzzy extractors from the biometric data of the iris. A software implementation is proposed and experimental studies of the key generation algorithm based on biometric data obtained by the developed method of fuzzy iris extractors are carried out.

Keywords: biometrics, biometric cryptosystems, cryptographic key generation, iris.

Tab. 1. Fig. 6. Ref.: 17 items.