УДК 004.056.5 **DOI:10.30837/rt.2023.2.213.03**

О.О. КУЗНЕЦОВ, д-р техн. наук, Д.О. ЗАХАРОВ

ЗАСТОСУВАННЯ МОДЕЛЕЙ ГЛИБОКОГО НАВЧАННЯ ДЛЯ ГЕНЕРАЦІЇ КРИПТОГРАФІЧНОГО КЛЮЧА ІЗ ЗОБРАЖЕННЯ ОБЛИЧЧЯ

Вступ

Біометрія традиційно вважається важливою сферою сучасної кібербезпеки [1 – 3]. Наприклад, біометричні методи автентифікації широко використовуються в різних додатках: криміналістика, електронна комерція, захист авторських прав, електронний документообіг, системи контролю доступу та багато іншого [1, 4, 5].

В останні роки інтерес до біометричних методів різко зріс. Від традиційних біометричних систем, заснованих на порівнянні отриманих біометричних зображень із збереженими еталонними копіями, сучасні технології перейшли до формування криптографічних ключів «на льоту» [5 – 7]. Цю проблему вирішують так звані нечіткі екстрактори, які дозволяють однозначно відновити секретний ключ з неточно відтворених біометричних даних за участю допоміжних даних (допоміжного рядка), які є публічними.

Традиційно нечіткі екстрактори, як і попередні їм нечіткі контейнери [4], будуються з використанням методів кодування з виправленням помилок. На початковому етапі біометричні дані в певному сенсі «зливаються» з елементами кодів, що виправляють помилки (наприклад, з кодовими словами або синдромальними послідовностями). Для нечітких екстракторів додатково формується відкритий допоміжний рядок (допоміжний рядок), який «допомагає» у вилученні секретного параметра з нечіткої біометрії. На етапі безпосереднього використання використовується завадостійке декодування, яке усуває можливу невизначеність (спричинену спотвореннями, стираннями тощо) у наданих користувачем біометричних зображеннях. Якщо відмінності в наборах характеристик невеликі (не перевищують коригуючу здатність кодів), то нечіткі екстрактори (сховища) дозволяють однозначно відновити секретний параметр (біометричний ключ).

Наступним кроком у розвитку таких технологій стане побудова повноцінних біометричних криптографічних систем, в яких біометричні персональні дані повинні використовуватися як джерело унікальних секретних параметрів. У цьому випадку користувачеві не потрібно буде запам’ятовувати криптографічні ключі (паролі) та/або використовувати додаткові пристрої для їх зберігання, передачі тощо. Біометрична криптосистема ініціалізується у будь-який час і в будь-якому місці шляхом вилучення необхідних параметрів “на льоту” з наданих біометричних зображень (з можливими неточностями, стираннями тощо) без шкоди для цих зображень. При цьому необхідно забезпечити максимальний набір послуг і гарантій безпеки з урахуванням особливостей побудови біометричних криптосистем.

У статті [8] запропоновано нову схему нечіткого екстрактора, яка використовує криптосистему коду McEliece [9]. Криптографія на основі коду є важливим напрямком у розвитку постквантових методів захисту інформації [10 – 14]. В роботах [10, 15, 16] показано, що використання методів на основі коду дозволяє забезпечити високу стійкість як до класичного, так і до квантового криптоаналізу. Незважаючи на численні спроби криптоаналізу [10, 12, 17 – 19], схема МакЕліса на основі кодів Гоппи [9, 18, 20] є надійною альтернативою сучасним криптосистемам з відкритим ключем. Зокрема, варіант класичної схеми McElice був представлений серед фіналістів третього етапу NIST PQC [21].

Екстрактор, запропонований у [8], оперує біометричними даними, представленими у вигляді наборів бінарних векторів. Передбачається, що різні набори одного користувача відрізняються один від одного не більше ніж на 25 % (цей поріг відповідає граничним можливостям виправлення помилок кодів). Проте в роботі [8] не запропоновано методів отримання таких бінарних наборів з будь-яких біометричних зображень (обличчя, пальці, сітківка та райдужка, вени, вушні раковини чи щось інше).

Метою цієї статті є розробка нечіткого екстрактора для генерації криптографічно надійних ключів із біометричних зображень людських облич.

Методи глибинного навчання для отримання набору біометричних характеристик

Більшість раніше реалізованих алгоритмів діставання фіч за певним зображенням I повертає вектор фіч з дійсних чисел $f(I) \in R^{n_f \times 1}$ фіксованого розміру n_f.

У дослідженні будемо використовувати попередньо навчені екстрактори [22, 23]. Обидва алгоритми використовують підхід глибокого навчання: спочатку формується набір триплетів, де кожен елемент має форму $\left\{A^{(t)}, P^{(t)}, N^{(t)}\right\}$, де $A^{(t)}$ та $P^{(t)}$ – зображення однієї людини, а $A^{(t)}$ та $N^{(t)}$ – двох різних (тут A, P, N відповідають термінам *anchor*, *positive* та *negative*, що відображають вищезгадані відносини) [22, 23]. Потім алгоритм намагається знайти такі параметри нейронної мережі, щоб мінімізувати функцію втрат $L(T)$ на цій множині триплетів.

Датасет для оцінки екстрактора фіч

Для оцінки екстрактора фіч використаємо датасети [25, 26].

Спочатку розбиваємо зображення людей на n_b груп, де в кожній групі зберігаються зображення лише однієї людини. Припустимо, що кожна група складається з n_i зображень. Таким чином, якщо візьмемо два зображення з однієї групи – матимемо зображення однієї людини; якщо два зображення взято з двох різних груп – матимемо зображення різних людей. Позначимо *j* зображення в *i* групі як $I_{i,j}$

Окрім поділу зображень на групи, для подальшої оцінки точності також потрібно буде розділити зображення на пари. Позначимо набір пар як P, кожен елемент p якого визначається чотирма елементами $\{p(n_1), p(i_1), p(n_2), p(i_2)\}$, де $p(n_1), p(i_1)$ відповідають першому зображенню в групі $p(n_1)$ з порядковим номером $p(i_1)$. Так само для $p(n_2), p(i_2)$. Відповідно, якщо $p(n_1) = p(n_2)$, то маємо зображення однієї людини, в той час якщо ці два числа різні – то двох різних людей.

Тюнінг порогового гіперпараметра

Для подальшого аналізу також важливо знайти такий пороговий гіперпараметр τ, який максимізував би точність класифікації «це два зображення однієї людини» і «двох різних людей» (назвемо це двійковою точністю). Припустимо, що маємо сформований набір пар P і запускаємо наш класифікатор на цьому наборі пар із певним значенням порогу τ. Визначимо двійкову точність α_{bin} на цій множині як

$$\alpha_{bin}(P,\tau) = \frac{N_+(P,\tau)}{|P|},$$

де $N_+(P,\tau)$ – кількість правильно ідентифікованих пар на множині P, використовується поріг τ. Тепер спробуємо підібрати $\tilde{\tau}$ таке, що максимізує $\alpha_{bin}(P,\tau)$. Іншими словами,

$$\tilde{\tau} = \arg\max_{\tau} \alpha_{bin}(P,\tau) = \arg\max_{\tau} N_+(P,\tau).$$

Зробимо це наступним чином: беремо інтервал $(\tau_{\min}, \tau_{\max})$, на якому є шукане $\tilde{\tau}$ і рухаємось з $\tau_{\min}$ до $\tau_{\max}$ маленьким шагом $\Delta\tau$ ($\Delta\tau \in \tau_{\min}, \tau_{\max}$), обчислюючи значення $\alpha_{bin}(\tau)$ для кожного τ. Присвоїмо $\tilde{\tau}$ значення τ, яке дало найбільше значення $\alpha_{bin}(\tau)$.

Важливе зауваження: такий алгоритм потрібно робити окремо для кожного алгоритму, оскільки різні моделі виводять вектор $f(I)$ по-різному. Наприклад, для моделі *Face Recognition* маємо $\tilde{\tau} \approx 0.365$, в той час як для моделі *Keras Facenet* маємо $\tilde{\tau} \approx 155$, тому різниця в значеннях є значною.

На рис. 1 та 2 можна побачити залежність $\alpha_{bin}(\tau)$ для різних значень τ для моделей *Keras Facenet* та *Face Recognition* відповідно.

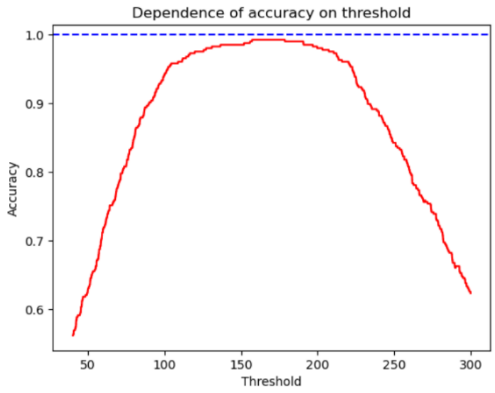

Рис. 1. Залежність $\alpha_{bin}(\tau)$ для моделі *Keras Facenet*

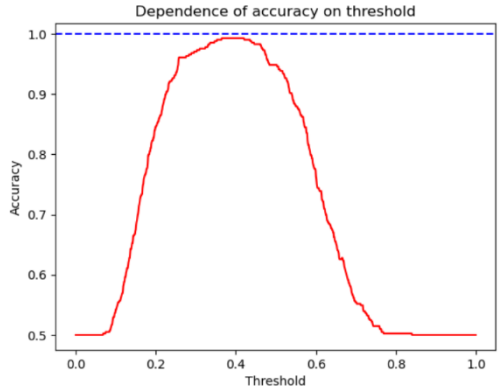

Рис. 2. Залежність $\alpha_{bin}(\tau)$ для моделі *Face Recognition*

Оцінка екстрактора фіч

Існує багато методів оцінки точності цих нейронних мереж. На перший погляд, можна застосувати оцінку F_1 [27] або просто використати значення $\alpha_{bin}(\tilde{\tau})$. Однак нам потрібно оцінити не те, наскільки точно модель класифікує бінарно, а наскільки схожі два вектори, коли вони відповідають зображенням однієї людини, і наскільки вони відрізняються, коли відповідають зображенням різних людей. Таким чином, пропонуємо використовувати деяку неперервну функцію точності від двох зображень $\alpha_{\text{cont}}(I,J)$, яку будемо називати *неперервною точністю*. Насправді, побачимо, що α_{cont} та α_{bin} сильно відрізняються.

Наприклад, застосуємо наступну функцію:

$$\alpha_{cont}(I,J)=\begin{cases}\left[1-\left(\dfrac{d(I,J)}{\tilde{\tau}}\right)^{\eta_1}\right]_+, I\equiv J,\\ \left[1-\left(\dfrac{\tilde{\tau}}{d(I,J)}\right)^{\eta_2}\right]_+, I\not\equiv J.\end{cases}$$

де $[z]_+ := \max\{0,z\}$.

Ця функція зображена на рис. 3. Інтуїтивне пояснення таке: коли нейронна мережа виводить відстань, близьку до $\tilde{\tau}$, вона дуже невпевнена щодо свого вибору, тому точність нижча порівняно з випадком, коли вона виводить значення, яке далі від $\tilde{\tau}$ (звичайно, у

правильному напрямку). Зауважимо, що функція також має два гіперпараметри η_1 та η_2, які використовуються для створення великого нахилу поблизу $\tilde{\tau}$ та меншого нахилу далі від $\tilde{\tau}$.

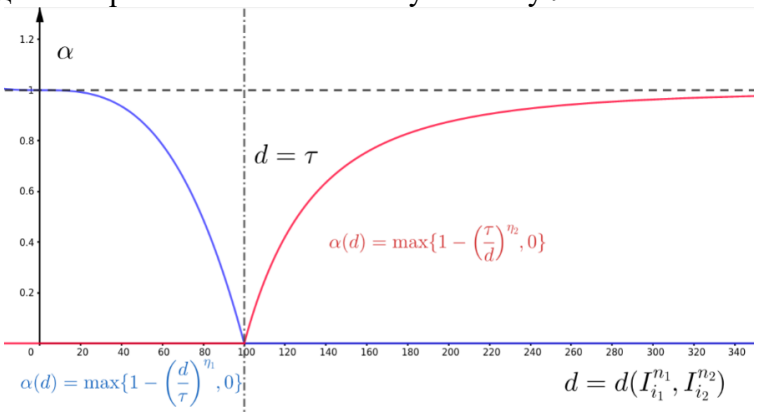

Рис. 3. Залежність $\alpha_{\text{cont}}(d)$ для $\eta_1 = \eta_2 = 3, \tilde{\tau} = 100$.
Синім відмічено випадок $I \equiv J$, червоним – $I \not\equiv J$

Зауваження: ця функція буде мати зміст лише для $\tilde{\tau}$, що максимізує двійкову точність. Дійсно, якщо, наприклад, покласти $\tau = 0$, то функція взагалі не буде визначена для випадку $I \equiv J$. Проте, якщо значення $\tilde{\tau}$ обрано таким чином, що двійкова точність вища за, скажімо, 90 % (хоча реальне значення близько 99 %), функція дає точне представлення ефективності екстрактора.

Визначимо кумулятивну точність за допомогою сформованого набору пар P. У цьому випадку визначимо загальну кумулятивну точність на наборі пар A_{cont} як середньоквадратичне значення набору безперервних точностей, застосованих до кожної пари в цьому наборі:

$$A_{\text{cont}}^2 = \frac{1}{|P|} \sum_{p \in P} \alpha_{\text{cont}}^2 (I_{p(n_1),p(i_1)}, I_{p(n_2),p(i_2)}).$$

Також визначимо загальну кумулятивну двійкову точність A_{bin} як просто бінарну точність при порозі $\tilde{\tau}$, тобто

$$A_{\text{bin}}(P) = \alpha_{\text{bin}}(P, \tilde{\tau}).$$

Конвертер вектора фіч

Як казали раніше, конвектор вектора фіч повинен, враховуючи дійсний вектор фіч $f(I)$, сформувати бінарну строку $s(I)$ довжини n_s, де I – це зображення. Оскільки у нашому випадку $n_f = n_s = k = 128$, це суттєво спрощує задачу. Нехай маємо вектор

$$f(I) = \begin{bmatrix} f(I)_1 \\ f(I)_2 \\ \vdots \\ f(I)_k \end{bmatrix} \in \mathbb{R}^k$$

і нам потрібно сформувати

$$s(I) = \begin{bmatrix} s(I)_1 \\ s(I)_2 \\ \vdots \\ s(I)_k \end{bmatrix} \in \{0,1\}^k$$

згідно з деяким правилом $\phi: \square^{k} \to \{0,1\}^{k}$. В цьому випадку визначимо ϕ наступним чином:

$$s(I)_j = \begin{cases} 1, f(I)_j > 0 \\ 0, f(I)_j \le 0 \end{cases}.$$

Також визначимо бінарну відстань $\delta(I,J)$ між зображеннями I та J як

$$\delta(I,J) = \frac{1}{k}\sum_{j=1}^{k} \left| s(I)_j - s(J)_j \right|.$$

Аналогічно можемо визначити схожість зображень $\sigma(I,J)$ як $\sigma(I,J) = 1 - \delta(I,J)$.

Подивимося, який результат отримаємо, застосовуючи ϕ до деяких зображень із нашого набору даних. Як можна побачити з рис. 4, два двійкові рядки однієї особи майже збігаються. Згідно з нашим визначенням подібність між цими двома зображеннями становить приблизно 86 %, що є відносно хорошим результатом. Але для двох різних людей, наприклад як показано на рис. 5, двійкові рядки суттєво відрізняються, і в наведеному прикладі подібність дорівнює 50 %, що є відносно невеликим значенням, як і очікувалося.

1010011011110000101110010010111000010

1010011010100000101101011010111000010

Рис. 4. Бінарна строка для пари зображень однієї особи.
Зеленим позначено однакові символи, а червоним – різні.
Для демонстрації включено лише 36 рядкових символів

1010011010100000101101011010111000010

1100001000010100011101001110000101011

Рис. 5. Бінарна строка для пари зображень двох різних людей.
Зеленим позначено однакові символи, а червоним – різні.
Для демонстрації включено лише 36 рядкових символів

Оцінимо точність такого конвертера на більшому наборі даних. По-перше, пропонуємо розділити множину пар P на дві інші множини: P_{same} – набір пар зображень однієї особи та P_{diff} – набір пар зображень різних людей, згідно з тим, як ми формували набір пар P, $|P_{same}| = |P_{diff}| = |P|/2$.

Для оцінки точності будемо використовувати два значення: σ_{same} – середня схожість між бінарними строками, сформованими для множини пар однієї людини, і σ_{diff} – для множини пар різних людей. Визначимо їх наступним чином:

$$\sigma_{same} = \frac{1}{\left|P_{same}\right|} \sum_{p \in P_{same}} \sigma\left(I_{p(n_1),p(i_1)}, I_{p(n_2),p(i_2)}\right),$$

$$\sigma_{diff} = \frac{1}{\left|P_{diff}\right|} \sum_{p \in P_{diff}} \sigma\left(I_{p(n_1),p(i_1)}, I_{p(n_2),p(i_2)}\right).$$

Результати експериментів

У табл. 1 – 4 включено всі базові параметри, описані раніше для двох наборів даних (*lfw* і *CelebA*) і двох моделей (*Keras Facenet* і *Face Recognition*). Для обох наборів даних використано приблизно 1 тисячу зображень (тобто майже однакову кількість пар).

Таблиця 1

Бінарна точність

Набір даних	Keras Facenet	Face Recognition
Lfw	99.3%	98.2%
CelebA	94.8%	93.2%

Таблиця 2

Неперервна точність

Набір даних	Keras Facenet	Face Recognition
Lfw	84.0%	81.9%
CelebA	75.8%	74.8%

Таблиця 3

Схожість пар зображень однієї людини

Набір даних	Keras Facenet	Face Recognition
Lfw	77.3%	88.8%
CelebA	73.7%	88.5%

Таблиця 4

Схожість пар зображень двох різних людей

Набір даних	Keras Facenet	Face Recognition
Lfw	50.8%	79.7%
CelebA	51.7%	80.9%

Як бачимо, для всіх наборів даних двійкова точність обох моделей перевищує 93 %. Однак безперервна точність нижча, і це логічний результат, оскільки безперервна точність завжди повинна мати менше значення. Це досягається завдяки тому, що ми визначили двійкову відстань як середнє значення одиниць і нулів, тоді як при застосуванні формули безперервної точності всі нулі залишаються нулями, але всі одиниці відображаються на інтервал (0,1), який завжди не перевищує 1. Ця точність завжди відносно висока для обох моделей, але в наборі даних *CelebA* маємо значення близько 75 %.

Щодо значень σ, модель *Keras* має значну перевагу над моделлю *Face Recognition*: за нашим правилом ϕ, ця модель видає найбільше значення $\sigma_{\text{same}} - \sigma_{\text{diff}}$, що перевищує 20 %. В свою чергу, модель *Face Recognition* має значну меншу різницю, яка навіть менша за 10 %. Можливо, інший спосіб визначення ϕ може зробити модель *Face Recognition* більш точною, оскільки її бінарна точність більша за модель *Keras,* і це є чудовою темою для майбутніх публікацій.

Для збільшення значення різниці для подальших досліджень потрібно визначити ϕ більш складним способом, а саме – створити нейронну мережу, яка навчиться максимізувати точність перетворювача.

Реалізацію функцій і методів, згаданих у попередніх розділах, можна знайти у [28].

Code based нечіткий екстрактор

У статті [8] запропоновано новий нечіткий екстрактор криптографічно надійних ключів із біометричних даних. Цей екстрактор використовує криптосистему на основі коду McEliece [9].

Кожен сформований біометричний двійковий вектор інтерпретуємо як слово [8]:

$$B^* = I \cdot G_X + e^* . \quad (1)$$

Якщо ми використовуємо допоміжну строку, ми припускаємо, що слово B^* складається з спотвореної вектором e^* частини B_k^* та несекретної допоміжної строки $P_{n-k} = I \cdot G_{X_2} = B_k \cdot G_{X_1}^{-1} \cdot G_{X_2}$, де [8]:

- матриця G_{X_1} сформована k рядками матриці G_X, номери стовпців відповідають довільно обраними k позиціями вектору B;
- матриця G_{X_2} сформована $n-k$ колонками, що залишились від матриці (1);
- матриця G_X це публічний ключ в криптосистемі McEliece.

Показники ефективності біометричного екстрактора

Важливими характеристиками біометричної автентифікації є частота помилкових відхилень (FRR) і частота помилкових прийомів (FAR):

- FRR – характеризує рівень помилкових відмов, тобто це ймовірність того, що біометрична система помилково відхилить спробу доступу авторизованого користувача;
- FAR – характеризує рівень помилкових акцептів, тобто це ймовірність того, що біометрична система помилково прийме спробу доступу неавторизованого користувача.

Для оцінки цих ймовірностей розглянемо два випадки.

Припустимо, що в результаті сканування та обробки біометричних даних сформовано двійковий рядок (1), де вага Хеммінга (кількість ненульових позицій) вектора помилок e^* характеризує можливі відмінності B^* з еталонним біометричним набором B.

Кількість ненульових позицій вектору e^* визначається ймовірністю появи ненульового символу в e^*, тобто ймовірність спотворення одного символу кодового слова $c_X = I \cdot G_X$. Для авторизованого та неавторизованого користувача ці ймовірності різні.

В и п а д о к 1. Нехай вектор (5) належить авторизованому користувачу. Позначимо ймовірність спотворення одного символу в c_X як p_0. Тоді значення FRR можна оцінити за формулою [8]

$$FRR = 1 - \sum_{i=0}^{t} C_k^i p_0^{\,i} (1 - p_0)^{k-i} . \quad (2)$$

Табл. 3 надає емпіричну оцінку цієї ймовірності, отриману на наборах даних *Lfw* і *CelebA* з використанням моделей глибокого навчання *Keras Facenet* і *Face Recognition*. Бачимо, що для різних варіантів обробки біометричних ознак оцінка ймовірності p_0 дещо відрізняється. Приймаємо оцінку ймовірності p_0 за критерієм мінімального ризику, тобто розглядаємо найгірший сценарій (з найбільшою ймовірністю):

- $p_0 \approx 0,263$ для моделі *Keras Facenet*;
- $p_0 \approx 0,125$ для моделі *Face Recognition*.

В и п а д о к 2 . Нехай вектор (1) належить неавторизованому користувачу. Позначимо ймовірність спотворення одного символу як p_1. Тоді значення FAR можна оцінити за формулою [8]

$$FAR = \sum_{i=0}^{t} C_k^i p_1^{\,i} (1-p_1)^{k-i} \ . \qquad (3)$$

Емпірична оцінка ймовірності p_1 наведена в табл. 4. Приймаємо оцінку ймовірності p_1 за критерієм мінімального ризику, тобто розглядаємо найгірший сценарій (найменшої ймовірності):

- $p_1 \approx 0,483$ для моделі *Keras Facenet*;
- $p_1 \approx 0,191$ для моделі *Face Recognition*.

Завдання екстрактора полягає в мінімізації FRR і FAR для різної довжини згенерованих паролів і різних ймовірностей p_0 та p_1.

Оцінка та порівняння FRR та FAR

Розглянутий екстрактор заснований на використанні кодових криптосистем, які використовують лінійний блок $(n, k, d = 2t+1)$ із швидким (поліноміальної складності) декодуванням. Найбезпечнішим варіантом вважається використання двійкового коду Goppa з параметрами

$$(n, k, d) = (2^m, 2^m - mt, 2t+1)$$

для деякого додатного цілого m.

У експериментах ми сформували бінарні строки довжини $n = 128$, тобто для $m = 7$. У табл. 5 показано параметри k, d кодів Гоппи для різних значень t. У таблиці також наведено розрахункові значення FRR і FAR для різних випадків. У таблиці виділено випадок із FRR ≈ FAR.

Таблиця 5

Оцінки FRR та FAR для різних кодів Гоппи довжини 128

t	*k*	*d*	Keras Facenet		Face Recognition	
			FRR	FAR	FRR	FAR
8	72	17	0.9987	1.88E-11	0.5532	0.0512
9	65	19	0.9877	4.94E-09	**0.2912**	**0.1800**
10	58	21	0.9262	8.09E-07	0.1026	0.4368
11	51	23	0.7229	7.60E-05	0.0212	0.7417
12	44	25	0.3663	0.0036	0.0022	0.9366
13	37	27	**0.0830**	**0.0744**	8.18E-05	0.9939
14	30	29	4.66E-03	0.5023	6.85E-07	0.9999
15	23	31	1.77E-05	0.9673	3.63E-10	1.0000

Висновки

У статті розглянуто застосування моделей глибокого навчання *Keras Facenet* і *Face Recognition* для генерації криптографічно надійних послідовностей (ключів, пін-кодів, паролів). У експериментах використовувались набори даних *Lfw* і *CelebA* з нечітким екстрактором на основі криптосистем на основі коду з [8]. Досягнуті результати демонструють перспективність даної теми та можливість використання в різних криптографічних додатках. Наприклад, вдосконалення систем авторизації доступу за паролем, генерування первинної ентропії в криптографічних алгоритмах тощо.

Розглянуто різні варіанти побудови нечіткого екстрактора з кодами Гоппи довжиною 128 біт. Найефективнішими виявилися: за співвідношенням FRR і FAR – модель глибокого навчання *Keras Facenet* і криптосистеми на основі коду з використанням допоміжного рядка

– (128, 37, 27) коду Гоппи з формуванням 37-бітного пароля. Це забезпечує можливість помилок FRR ≈ FAR < 10%.

Перспективним напрямком подальших досліджень є використання криптосистем із кодами Гоппи значно більшої довжини. Це значно зменшить ймовірність FRR і FAR. Крім того, цікавим напрямком досліджень є алгоритми багатофакторної автентифікації з формуванням криптографічно надійних ключів.

Список літератури:

1. S. Chakraborty and D. Das. An Overview of Face Liveness Detection // arXiv:1405.2227 [cs], May 2014, Accessed: Feb. 12, 2021. [Online]. Available: http://arxiv.org/abs/1405.2227
2. C. Rathgeb and A. Uhl. A survey on biometric cryptosystems and cancelable biometrics // EURASIP Journal on Information Security, vol. 2011, no. 1, p. 3, Sep. 2011, doi: 10.1186/1687-417X-2011-3.
3. U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain. Biometric cryptosystems: issues and challenges // Proceedings of the IEEE, vol. 92, no. 6, pp. 948–960, Jun. 2004, doi: 10.1109/JPROC.2004.827372.
4. M. Lutsenko, A. Kuznetsov, A. Kiian, O. Smirnov, and T. Kuznetsova. Biometric Cryptosystems: Overview, State-of-the-Art and Perspective Directions // Advances in Information and Communication Technology and Systems, Cham, 2021, pp. 66–84. doi: 10.1007/978-3-030-58359-0_5.
5. Z. Jin, A. B. J. Teoh, B.-M. Goi, and Y.-H. Tay. Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation // Pattern Recognition, vol. 56, pp. 50–62, Aug. 2016, doi: 10.1016/j.patcog.2016.02.024.
6. M. Lutsenko, A. Kuznetsov, Y. Gorbenko, I. Oleshko, Y. Pronchakov, and Y. Kotukh. Key Generation from Biometric Data of Iris // 2019 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Sep. 2019, pp. 1–6. doi: 10.1109/UkrMiCo47782.2019.9165457.
7. A. Kuznetsov, I. Oleshko, K. Chernov, M. Bagmut, and T. Smirnova. Biometric Authentication Using Convolutional Neural Networks // Advances in Information and Communication Technology and Systems, Cham, 2021, pp. 85–98. doi: 10.1007/978-3-030-58359-0_6.
8. A. Kuznetsov, A. Kiyan, A. Uvarova, R. Serhiienko, and V. Smirnov. New Code Based Fuzzy Extractor for Biometric Cryptography // 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T), Oct. 2018, pp. 119–124. doi: 10.1109/INFOCOMMST.2018.8632040.
9. R. J. McEliece. A Public-Key Cryptosystem Based On Algebraic Coding Theory // Deep Space Network Progress Report, vol. 44, pp. 114–116, Jan. 1978.
10. R. Overbeck and N. Sendrier. Code-based cryptography // Post-Quantum Cryptography. D. Bernstein, J. Buchmann and E. Dahmen, Eds. Berlin, Heidelberg: Springer, 2009, pp. 95–145. doi: 10.1007/978-3-540-88702-7_4.
11. W. Wang, J. Szefer, and R. Niederhagen. FPGA-Based Niederreiter Cryptosystem Using Binary Goppa Codes // Post-Quantum Cryptography, Cham, 2018, pp. 77–98. doi: 10.1007/978-3-319-79063-3_4.
12. M. Bardet, J. Chaulet, V. Dragoi, A. Otmani and J.-P. Tillich. Cryptanalysis of the McEliece Public Key Cryptosystem Based on Polar Codes // Post-Quantum Cryptography, Cham, 2016, pp. 118–143. doi: 10.1007/978-3-319-29360-8_9.
13. I. von Maurich, L. Heberle, and T. Güneysu. IND-CCA Secure Hybrid Encryption from QC-MDPC Niederreiter // Post-Quantum Cryptography, Cham, 2016, pp. 1–17. doi: 10.1007/978-3-319-29360-8_1.
14. D. Moody and R. Perlner. Vulnerabilities of 'McEliece in the World of Escher // Post-Quantum Cryptography, Cham, 2016, pp. 104–117. doi: 10.1007/978-3-319-29360-8_8.
15. D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds. Post-Quantum Cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009. doi: 10.1007/978-3-540-88702-7.
16. T. Takagi, Ed., Post-Quantum Cryptography, vol. 9606. Cham: Springer International Publishing, 2016. doi: 10.1007/978-3-319-29360-8.
17. V. M. Sidelnikov and S. O. Shestakov. On insecurity of cryptosystems based on generalized Reed-Solomon codes // Discrete Mathematics and Applications, vol. 2, no. 4, pp. 439–444, Jan. 1992, doi: 10.1515/dma.1992.2.4.439.
18. N. Sendrier. Niederreiter Encryption Scheme // Encyclopedia of Cryptography and Security, H. C. A. van Tilborg and S. Jajodia, Eds. Boston, MA: Springer US, 2011, pp. 842–843. doi: 10.1007/978-1-4419-5906-5_385.
19. R. Canto Torres and N. Sendrier. Analysis of Information Set Decoding for a Sub-linear Error Weight // Post-Quantum Cryptography, Cham, 2016, pp. 144–161. doi: 10.1007/978-3-319-29360-8_10.
20. Classic McEliece: Intro. https://classic.mceliece.org/index.html (accessed Feb. 12, 2021).
21. Classic McEliece: NIST submission. https://classic.mceliece.org/nist.html (accessed Feb. 12, 2021).
22. F. Schroff, D. Kalenichenko, and J. Philbin. FaceNet: A unified embedding for face recognition and clustering // 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Jun. 2015, pp. 815–823. doi: 10.1109/CVPR.2015.7298682.
23. Machine Learning is Fun! Part 4: Modern Face Recognition with Deep Learning ; by Adam Geitgey ; Medium https://medium.com/@ageitgey/machine-learning-is-fun-part-4-modern-face-recognition-with-deep-learning-c3cffc121d78 (accessed Sep. 02, 2022).

24. Y. Taigman, M. Yang, M. Ranzato, and L. Wolf. DeepFace: Closing the Gap to Human-Level Performance in Face Verification // 2014 IEEE Conference on Computer Vision and Pattern Recognition, Jun. 2014, pp. 1701–1708. doi: 10.1109/CVPR.2014.220.

25. G. B. Huang, M. Mattar, T. Berg, and E. Learned-Miller. Labeled Faces in the Wild: A Database forStudying Face Recognition in Unconstrained Environments // presented at the Workshop on Faces in "Real-Life" Images: Detection, Alignment, and Recognition, Oct. 2008. Accessed: Sep. 02, 2022. [Online]. Available: https://hal.inria.fr/inria-00321923

26. Z. Liu, P. Luo, X. Wang, and X. Tang. Deep Learning Face Attributes in the Wild // arXiv, Sep. 24, 2015. doi: 10.48550/arXiv.1411.7766.

27. A. A. Taha and A. Hanbury. Metrics for evaluating 3D medical image segmentation: analysis, selection, and tool // BMC Medical Imaging, vol. 1, no. 15, pp. 1–28, 2015, doi: 10.1186/s12880-015-0068-x.

28. D. Zakharov. Binary Encoder // Sep. 02, 2022. Accessed: Sep. 04, 2022. [Online]. Available: https://github.com/ZamDimon/Binary-Encoder

29. J. H. van Lint and G. van der Geer. Classical Goppa codes // Introduction to Coding Theory and Algebraic Geometry, J. H. van Lint and G. van der Geer, Eds. Basel: Birkhäuser, 1988, pp. 22–24. doi: 10.1007/978-3-0348-9286-5_5.

30. A. Kuznetsov, A. Kiian, V. Babenko, I. Perevozova, I. Chepurko, and O. Smirnov. New Approach to the Implementation of Post-Quantum Digital Signature Scheme // 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), May 2020, pp. 166–171. doi: 10.1109/DESSERT50317.2020.9125053.

31. G. Hua. Facial Recognition Technologies // Encyclopedia of Big Data, L. A. Schintler and C. L. McNeely, Eds. Cham: Springer International Publishing, 2022, pp. 475–479. doi: 10.1007/978-3-319-32010-6_93.

32. C. Libby and J. Ehrenfeld. Facial Recognition Technology in 2021: Masks, Bias, and the Future of Healthcare // J Med Syst, vol. 45, no. 4, p. 39, Feb. 2021, doi: 10.1007/s10916-021-01723-w.

33. K. A. Gates. Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance. NYU Press, 2011.

34. P. J. Grother, M. L. Ngan, and K. K. Hanaoka. Ongoing Face Recognition Vendor Test (FRVT. Part 2: Identification // NIST, Nov. 2018, Accessed: Aug. 26, 2022. [Online]. Available: https://www.nist.gov/publications/ongoing-face-recognition-vendor-test-frvt-part-2-identification.

Надійшла до редколегії 11.05.2023

Відомості про авторів:

Кузнецов Олександр Олександрович – д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: kuznetsov@karazin.ua, ORCID: https://orcid.org/0000-0003-2331-6326

Захаров Дмитро Олегович – Харківський національний університет імені В.Н. Каразіна, студент 2-го курсу, кафедра прикладної математики; Україна; e-mail: zamdmytro@gmail.com, ORCID: https://orcid.org/my-orcid?orcid=0000-0001-9519-2444