УДК 004.056: 621.397

В. Ю. Корольов, к. т. н.;
В. В. Поліновський;
В. А. Герасименко

ПЕРСОНАЛІЗАЦІЯ МОБІЛЬНИХ ТЕЛЕКОМУНІКАЦІЙНИХ ЗАСОБІВ МЕТОДОМ ДИСТАНЦІЙНОГО РОЗПІЗНАВАННЯ ВІК-КОДУ

Розширення функціональності сучасних мобільних телефонів висуває нові вимоги до забезпечення безпеки інформації, що зберігається у цих засобах. На основі дистанційного розпізнавання фотографічного образу коду ВІК-ключа запропоновано нові методи персоналізації стаціонарних і мобільних обчислювальних та телекомунікаційних пристроїв, котрі обладнані оптичним каналом реєстрації інформації. Ефективність описаних методів підтверджується результатами розпізнавання ВІК-ключів, зчитаних камерами серійних мобільних телефонів і Web-камерами десктопів і ноутбуків.

Безпека телекомунікаційних систем суттєво залежить від здатності систем персоналізації мобільних пристроїв протистояти їх несанкціонованому використанню. Відомо, що вартість інформації, яка зберігається в мобільних засобах, часто значно вища її носія. Ефективність персоналізації мобільних телефонних пристроїв, як і складних технічних систем, полягає у створенні багаторівневих систем безпеки, які можуть протистояти несанкціонованому доступу з гарантованою стійкістю. Відомі технічні рішення систем контролю доступу до мобільних засобів, що ґрунтуються на стандартних криптографічних процедурах аутентифікації та ідентифікації, із введенням PIN-коду, не можна назвати дійсно персоналізованими, оскільки після вмикання на початку роботи цими пристроями можуть користуватись неавторизовані особи [1, 3, 5].

Об'єм світового ринку технологій ідентифікації (ID-Technologies) у 2007 році оцінюється корпорацією BCC Inc. на рівні 15 млрд. дол. США. Широкий клас пристроїв контролю доступу і засобів аутентифікації ґрунтується на методах розпізнавання зображень ідентифікаторів. Зростанню кількості систем ідентифікації на базі введення оптичних зображень сприяє збільшення роздільної здатності і чутливості ПЗС-матриць, зниження вартості пристроїв і камер на їх основі, а також доступність відкритих програмних бібліотек обробки візуальної інформації.

За даними аналітичної компанії ABI Research загальна кількість проданих мобільних телефонів основними виробниками: Nokia, Motorola, Samsung, Sony Ericsson і LG за 2006 рік досягла 1 млрд. одиниць. Доля камерафонів (мобільний телефон з камерою) у 2006 році оцінюється як 70...80 % від переліку всіх моделей мобільних засобів в залежності від регіону. За прогнозами компанії Gartner до 2009 року майже половина мобільних телефонів, що планують продавати у Японії, будуть обладнані 3-мегапіксельною камерою. В інших країнах у 2005 році стандартом була 1,3-мегапіксельна камера, а перехід до 2-мегапіксельних камер було здійснено у 2006 році. На сьогоднішній день процент продаж камерафонів досягає 75...90 % від загальної кількості моделей мобільних телефонів, запропонованих у 2007 році переліченими виробниками. Наведені статистичні дані і прогнози вказують на актуальність розробки систем персоналізації і аутентифікації, які використовують оптичний канал реєстрації інформації, і здатні працювати у масових пристроях, тобто є доступними пересічному покупцеві. Тому, в основу побудови таких пристроїв можуть бути покладені принципи використання ключа-ідентифікатора Бардаченко.

Конструктивно ВІК-ключ [2] — це набір з 14 сегментів, що таються навколо осі (рис. 1). Отвір у кожному сегменті відображає двійковий розряд, який відповідає нулю або одиниці, що встановлюється у потрібне положення механічним обертанням рухомої пластини навколо осі на 180°. Отже, головною перевагою ВІК-безпеки є оперативна зміна значень розрядів кодової комбінації вручну, тобто без використання будь-яких електронних або механічних допоміжних засобів, та можливістю оптичного розпізнавання

Рис. 1

кодової комбінації. Розширення вектора кодів ключа-ідентифікатора Бардаченко з 28 біт до 256 виконується методами гамування [4].

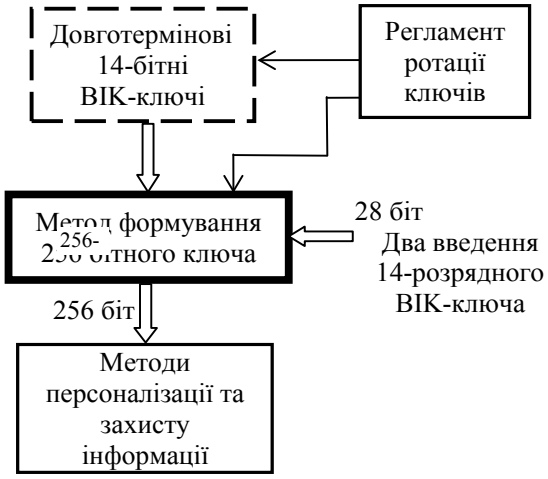

Рис. 2. Модель формування 256-бітного ключа на основі 28-бітного

На структурній схемі (рис. 2) показано узагальнену модель функціонування системи безпеки і персоналізації терміналів ПЕОМ, ноутбуків та мобільних телекомунікаційних засобів. Для отримання 256-бітного ключа користувач вводить у систему два рази ВІК-ключ з різними комбінаціями (сеансовий ключ), під час яких в пристрій захисту інформації передається послідовність біт. У відповідності з регламентом зміни довготермінових комбінацій виконується ротація кодових комбінацій, які визначають параметри роботи алгоритму формування 256-бітного ключа. В якості довготермінового ключа пропонується використати ВІК-ключ з маркерами [4].

Запропоновано метод персоналізації мобільних засобів за допомогою оптичного каналу реєстрації інформації та ВІК-ключа, доцільність використання якого обґрунтовано в роботі [4]. Розроблений алгоритм розпізнавання відрізняється малою обчислювальною складністю і низькою ємнісною складністю. Завдяки цьому час перетворення образу ключа-ідентифікатора Бардаченко у кодову послідовність становить 3...4 секунди з урахуванням часу, необхідного телефону на фотографування.

Інформаційними ознаками ВІК-коду в образі ключа є координати отворів, порядок їх розташування і положення відносно осі ключа. Оскільки зображення — це впорядкована сукупність пластин (інколи різного кольору), то для складання карти ознак об’єктів був використаний метод бінарної сегментації поля образу за заданим порогом. Розпізнавання в образі ключа-ідентифікатора ВІК-коду полягає в виконанні таких етапів:

1. Пошук об’єктів зображення, що відповідають отворам та іншим деталям ключа.
2. Декодування координат отворів в значення розрядів ВІК-ключа.

Реалізуючи цю задачу для мобільних пристроїв необхідно взяти до уваги такі особливості:

— моделі мобільних телефонів, що мають вбудовану камеру, суттєво відрізняються за своїми апаратними можливостями, до яких слід віднести: частоту процесора, об’єм оперативної пам’яті, роздільну здатність камери, якість знімків тощо;

— частота процесорів в телефонах на порядок менша, ніж в ПЕОМ, тобто становить від 50 MHz в найдешевших моделях до 500 MHz в дорогих смартфонах. Крім того, програми на мобільних телефонах виконуються на віртуальній Java-машині в режимі інтерпретації, що значно сповільнює виконання програм (в порівнянні з виконанням власного машинного коду процесора);

— розмір оперативної пам’яті, доступної для Java-програм, складає від 500 Kb в дешевих телефонах, що виділяють майже всю пам’ять для програм, до декількох мегабайт в смартфонах, які дозволяють паралельно виконувати декілька програм;

— знімки, що можна отримати на рівні Java-програми, мають обмежені розміри: як правило 128×96 або 160×120 пікселів навіть для телефонів, які підтримують більші розміри знімків, що пов’язано з обмеженням обсягу оперативної пам’яті для Java-програм.

Перелік етапів перетворення образу ключа у ВІК-код може бути таким:

1. Реєстрація зображення і його попередня обробка.
2. Розрахунок порогового значення і бінаризація зображення у відповідності з порогом.
3. Визначення границь образу ключа у сцені. (рис. 6а).
4. Розпізнавання отворів ключа і перетворення значень їх координат у розрядно-кодову комбінацію ключа-ідентифікатора Бардаченко. (рис. 6б).

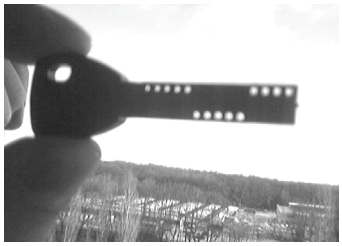

Рис. 3. Фотографія ВІК-ключа, що зроблена камерафоном Sony Ericsson K700i

На рис. 3 показано зображення, отримане за допомогою фотоапарата мобільного телефону Sony Ericsson K700i форматом 640×480 і розрізнені 120 dpi. На жаль для Java-програми доступні лише

зображення 160×120.

На першому етапі отримуємо зображення у стисненому форматі (найчастіше це формат JPEG). В цьому вигляді інформаційні ознаки ключа і отворів досить складно інтерпретувати і обробляти, тому на наступному кроці він переводиться в формат RGB, в якому кожен піксел зображається інтенсивністю червоного, зеленого та синього кольорів.

Для визначення контуру ключа і отворів потрібно розрізнити світлий фон і темний ключ на ньому (бінарна сегментація). При цьому необхідно перетворити вихідний масив, отриманий на попередньому кроці, в двотонове зображення. Емпірично виявлено, що статичне перетворення за відомими алгоритмами не дає прийнятних результатів для алгоритму розпізнавання, оскільки яскравість сегментів ключа на знімках з великою освітленістю є значно вищою ніж яскравість отворів ключа на знімках з низькою освітленістю. Тому спочатку виконується перетворення повнокольорового знімка у відтінки сірого за формулою

$$Grayscale = 0,299R + 0,587G + 0,114B,$$

де R, G і B – інтенсивності червоного, зеленого та синього кольорів, а відповідні коефіцієнти враховують сприйняття хвиль різних довжин людським оком, тобто, накопичується значення яскравостей кольорів отриманого зображення.

Також виконується підрахунок кількості пікселів, що мають різну яскравість (від 0 до 255) з метою отримання гістограми (спектру частот яскравостей зображення). За допомогою експериментів було встановлено, що ця гістограма має два нечітко виражених піка, що відповідають фону зображення (правий) та сегментам ключа (лівий). Проте координати цих локальних максимумів значно відрізняються для різних знімків, тому детерміноване розділення кольорів на «світлі» та «темні» неможливе (рис. 4).

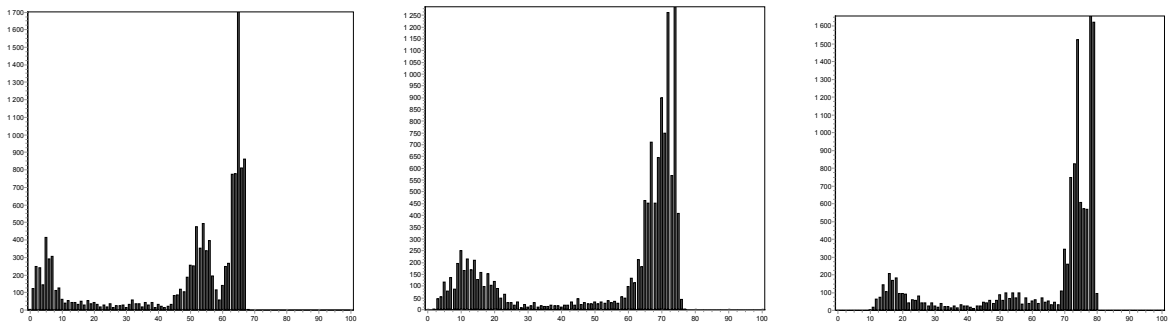

Рис. 4. Приклади гістограм яскравостей кольорів зображень

На наступному етапі виконується розрахунок порогового значення (cV — compare value), яке розділятиме кольори знімку за яскравістю на два типи. Для точного визначення цього значення необхідно знайти координати мінімуму гістограми між двома описаними максимумами. При цьому слід виконати низькочастотну фільтрацію зображення, а потім за згладженою гістограмою визначити координати глобального мінімуму. Цей метод дозволяє отримувати точні результати, але має суттєву обчислювальну складність і тому не може бути застосований у разі обмежених ресурсів пристроїв, таких як масові мобільні телефони.

Для практичної реалізації було обрано спрощений алгоритм, який дозволяє отримати прийнятні результати. Для цього діапазон спектра розбивається на дві частини і в кожній з них знаходяться координати максимумів, які є неточними у випадку розмитості піків. За порогове значення cV приймається середня з них, що також є неточним при різних довжинах піків. Проте аналіз отриманих гістограм свідчить про практичну достатність точності роботи даного алгоритму, який відрізняється мінімальною складністю. Використовуючи отримане значення порогу, далі виконується перетворення знімка у відтінках сірого (рис. 3) в двотоновий формат (рис. 5). При цьому знімок у відтінках сірого зберігається в пам’яті для подальших ітерацій.

Рис. 5. Приклади двотонових образів ключа-ідентифікатора Бардаченко

Наступним етапом є пошук контуру ключа, який виконується скануванням знімка з правого верхнього і нижнього кутів по діагоналям зображення до перетину з ключем (рис. 6 а). Сірий прямокутник відповідає сегментам ВІК-ключа, групи точок 1 і 2 та 3 і 4 — задають спрямовуючі лінії. Перетин ліній може статися як на грані ключа, так і в засвіченому отворі, який зливається з фоном (рис. 5). Тому, після цього виконується сканування від точок перетину вправо до грані ключа вздовж спрямовуючих ліній (рис. 6б), а потім відповідно вверх і вниз (рис. 6в). В результаті визначаються права верхня і права нижня координати ключа (точки C і D).

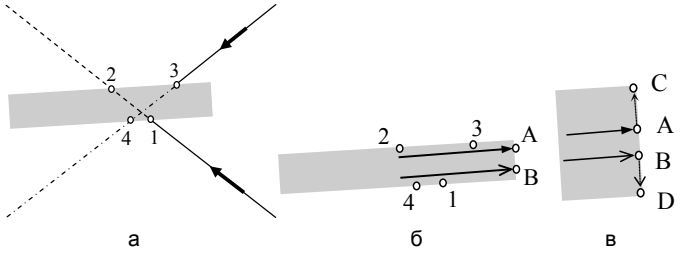

Рис. 6. Ілюстрація етапів алгоритму визначення границь образу ВІК-ключа у сцені

Після визначення координат контуру ключа виконується процедура розпізнавання отворів ключа. При цьому застосовується програмна реалізація кінцевого цифрового автомату, який має декілька змінних, що описують його стан та умови переходу з одного стану в інший.

Змінні, що описують стани кінцевого цифрового автомата, такі:

— кількість білих пікселів зверху у стовпчику на поточній координаті cT (current top);

— кількість білих пікселів знизу у стовпчику на поточній координаті cB (current bottom);

— кількість білих пікселів зверху у стовпчику на попередній координаті pT (previous top);

— кількість білих пікселів знизу у стовпчику на попередній координаті pB (previous bottom);

— кількість білих пікселів зростає зверху Gt (growing top);

— кількість білих пікселів зростає знизу Gb (growing bottom).

Згідно теорії автоматів, значення перелічених змінних визначають умови переходу з одного стану в інший.

Основними змінними, що описують поточний стан автомату, є кількість білих пікселів в верхній та нижній частині в поточному (cT, cB) та попередньому (pT, pB) стовпці пікселів, а також дві логічні змінні — прапорці (Gt, Gb), що вказують на зростання, чи спадання цих кількостей.

pT	cT
Gt	Gb
pB	cB

Рис. 7. Сканувальне вікно алгоритму розпізнавання

В основному циклі розпізнавання перебираються стовпці пікселів справа наліво і для кожного з них розраховуються вказані суми. Далі виконуються однакові дії над змінними, пов'язаними з верхньою і нижньою частинами ключа, які реалізують пошук отворів ключа. Також виконуються додаткові дії для розрізнення поодиноких пікселів чи їх груп на гранях ключа від «справжніх» отворів. Слід зазначити, що реалізовані для цього критерії не є універсальними і в деяких випадках можуть давати неправильні результати (пропуск отвору чи хибна його фіксація). Проте такі випадки не є типовими і спричинені лише просвічуванням червоних сегментів ключа. Крім того, спроба виправити алгоритм для однієї з помилок (хибна фіксація отвору) призводить до пропуску отворів для слабо освітлених знімків і навпаки. Проте, на практиці для ключа з чорними сегментами вказані проблеми не виникають.

Вихід з підпрограми можливий, якщо виконується одна з таких умов:

— сума поточних сум білих пікселів перевищує половину висоти ключа, що можливо лише при сильному просвічуванні червоного сегмента ключа;

— обидві змінні Gt і Gb вказують на поточне зростання сум, що можливо за тих самих умов;

— знаходження всіх отворів ключа.

Експериментально виявлено, що досить часто початкове порогове значення cV не є абсолютно точним для даного знімку, тобто воно може бути дещо завищене, але практично ніколи не буває заниженим. Тому, в отриманому зображенні у відтінках сірого можуть бути не знайдені погано освітлені отвори (частіше за все крайні). Для їх знаходження виконується зменшення порогового значення на деяку величину для повторного виконання дій алгоритму, починаючи з перетворення знімку в двотоновий формат уже з новим значенням порогу для пошуку «темних» отворів.

Вихід з алгоритму можливий в трьох випадках:

— коректне розпізнавання всіх отворів ключа;

— неможливість подальшого розпізнавання внаслідок сильного просвічування червоного сегмента ключа або одночасного зростання змінних Gt і Gb;

— змінна cV дорівнює нулю, що також означає неможливість розпізнавання (значення порогу зменшено до нуля, а необхідна кількість отворів не знайдена). Практично це неможливо, оскільки значно раніше виконується попередня умова виходу.

В першому випадку користувачу пропонується підтвердити введення ключа, а в другому і третьому виводиться частина ключа та отримане зображення для візуального аналізу причини невдалого розпізнавання (погана освітленість, великий кут нахилу ключа, просвічені сегменти ключа).

В цілому даний алгоритм реалізує поставлену мету: швидке розпізнавання ключа без врахування його нахилу. Головною перевагою алгоритму є мінімізована обчислювальна складність: декілька проходів циклу, в яких всі підпрограми мають лінійну або квадратичну обчислювальну складність. На практиці в більшості випадків розпізнавання виконується за один прохід, а при погано освітлених отворах процес розпізнавання потребує до п’яти ітерацій алгоритму. Ємнісна складність алгоритму також зведена до мінімуму: 5×<ширина знімку>×<висота знімку>, що є прийнятним навіть для телефонів з мінімальними можливостями.

Практичне використання даного алгоритму показало його високу ефективність: при достатній освітленості всіх отворів і невеликому куті нахилу ключа процент розпізнавання становить 99,5 %. Алгоритм однаково ефективно працює зі знімками різних розмірів: 128×96 для Siemens CXV65 і 160×120 для Sony Ericsson K700i. При цьому обробка знімку на досить повільному телефоні Siemens CXV65 займає 3...4 секунди, з них до 2 секунд — фотографування і створення знімку телефоном.

На рис. 5 показано приклади перетворених телефоном знімків в двотоновий формат, які наочно демонструють якість отримуваних знімків і проблеми розпізнавання, які при цьому виникають. Всі вказані знімки були коректно розпізнані телефоном, кожний за одну ітерацію алгоритму.

Наступним напрямком розвитку даного алгоритму є його модифікація для роботи з ключем, розташованим під кутом. В алгоритмі, створеному для ПЕОМ, була реалізована така можливість, але для мобільних телефонів необхідно розробляти ефективнішу спрощену версію, що є досить складною задачею з великою кількістю можливих варіантів рішень.

Висновки

Описано новий спосіб дешевої та ефективної персоналізації телекомунікаційних і обчислювальних засобів, що ґрунтується на дистанційному вводі двійкового коду. При цьому, за розміром розрядно-кодових комбінацій ключ ВІК, майже в 2 рази більше, ніж PIN-коди, які зараз використовуються в переважній більшості сучасних мобільних системах. На базі методів гамування запропоновано алгоритм розширення вектора кодів ВІК-ключа до криптографічного стандарту у 256 біт. В основу методу покладено розпізнавання фотографічного образу ВІК-коду, набраного на ключі-ідентифікаторі Бардаченко. Ефективність і раціональність запропонованого методу розпізнавання підтверджено результатами зчитування ВІК-коду, отриманого за допомогою непрофесійних серійних пристроїв оптичної реєстрації інформації мобільних телефонів та їх обробленням

за прийнятний час на масових обчислювальних засобах.

СПИСОК ЛІТЕРАТУРИ

1. Бардаченко В. Ф., Поліновський В. В. Методи персоналізації складних технічних систем, у тому числі комп'ютерних та телекомунікаційних // Вісті академії інженерних наук України. — 2005. — № 4 (27). — С. 7—11.

2. Бардаченко В. Ф., Кариман А. В., Колесницкий О. К., Василецкий С. А., Рашкевич А. А. Анализ современных средств аутентификации для систем защиты информации // УСиМ. — 2004. — №3. — С. 81—92.

3. Бардаченко В. Ф., Корольов В. Ю. Таймерна ВІК-ВАК технологія захисту периферійних пристроїв від несанкціонованого доступу // Вісті академії інженерних наук України. — 2005. — № 4 (27). — С. 12—14.

4. Бардаченко В. Ф., Королёв В. Ю. Концепция построения систем персонализации на базе расширения вектора кодов ВІК-ключа // УСиМ. — 2007. — № 1. — С. 44—53.

5. Поліновський В. В. Використання ВІК-ВАК технологій та таймерних алгоритмів для комп'ютерної телефонії з підвищеним рівнем безпеки // Вісті академії інженерних наук України. — 2005. — № 4 (27). — С. 15—18.

Матеріали статті рекомендовані до опублікування оргкомітетом III Міжнародної науково-технічної конференції «Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування (СПРТП-2007)» (31.05—2.06.2007 р.)

Надійшла до редакції 30.09.07
Рекомендована до друку 04.10.07

Корольов Вячеслав Юрійович — начальник відділу моделювання таймерних обчислювальних систем, ***Поліновський Вячеслав Васильович*** — вчений секретар, ***Герасименко Вячеслав Анатолійович*** — молодший науковий співробітник.

Центр таймерних обчислювальних систем Інституту кібернетики ім. В. М. Глушкова Національної академії наук України