ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ЗАЩИТА ИНФОРМАЦИИ

УДК 004.056: 621.397

В. Ю. Королев, канд. техн. наук
Центр таймерных вычислительных систем
Ин-та кибернетики им. В.М. Глушкова НАН Украины
(Украина, 03187, Киев, просп. Акад. Глушкова, 40, корп.1, к. 801,
тел.: (044) 5265585, 5266362, E-mail: dshv937@meta.ua)

Алгоритмизация дистанционного распознавания *BIK*-кода

(Статью представил д-р техн наук В. В. Мохор)

На основе дистанционного распознавания фотографического образа *BIK*-кода ключа-идентификатора (*BIK* — Bardachenko Identification Key) предложен новый способ ввода *BIK*-ключа для идентификации пользователя вычислительных терминалов, оборудованных фото или видеокамерой. Работоспособность описанных методов подтверждена результатами полунатурного моделирования в среде MatLab 7 при регистрации *BIK*-ключей-идентификаторов серийным сканером.

На основі дистанційного розпізнавання фотографічного образу *BIK*-коду ключа-ідентифікатора (*BIK* — Bardachenko Identification Key) запропоновано новий спосіб введення *BIK*-ключа для ідентифікації користувача обчислювальних терміналів, що обладнані фото чи відеокамерою. Працездатність описаних методів підтверджено результатами напівнатурного моделювання у середовищі MatLab 7 при реєстрації *BIK*-ключів-ідентифікаторів серійним сканером.

К л ю ч е в ы е с л о в а : ключ-идентификатор, распознавание, полунатурное моделирование.

Объем мирового рынка технологий идентификации в 2007 г. оценивается корпорацией BBC Inc. в 15 млрд. дол. США. К этим технологиям относится широкий класс устройств контроля доступа и средств аутентификации, основанных на методах распознавания изображений идентификаторов. Число систем идентификации, основанных на вводе оптических изображений, возрастает в связи с увеличением разрешающей способности и чувствительности *CCD*-матриц, снижением стоимости камер на их основе, а также доступностью открытых программных библиотек обработки визуальной информации.

Рассмотрим способ идентификации пользователей вычислительных и телекоммуникационных систем, который основан на использовании перестраиваемого ключа-идентификатора Бардаченко (*BIK* — Bardachenko

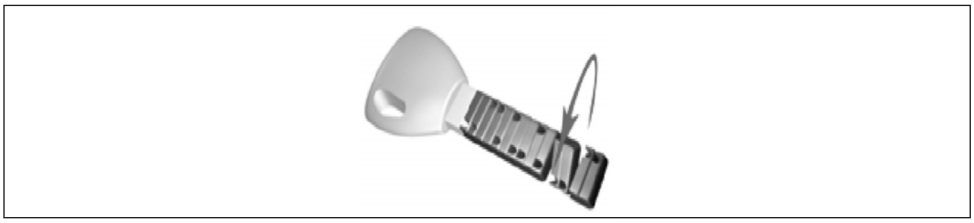

Рис. 1

Identification Key) [1—8] для набора кодовой последовательности, а также дистанционного *BIK*-ридера (фотокамеры и алгоритма распознавания) для ее считывания. Конструктивно *BIK*-ключ представляет собой набор из 14 сегментов, которые могут вращаться вокруг оси (рис. 1). Отверстие в каждом сегменте — двоичный разряд, соответствующий нулю или единице. Сегмент устанавливается в нужное положение механическим поворотом подвижной пластины на 180°. Пластины и ручка ключа изготовлены из пластика с применением дешевой технологии литья в формы. Главным достоинством *BIK*-ключа является оперативная смена значений разрядов кодовой комбинации вручную, т. е. без каких-либо механических или электронных вспомогательных средств. Кроме того, ключ не подвержен электромагнитным и механическим воздействиям и не излучает энергию, выпускается серийно на ОАО Меридиан, и его стоимость составляет приблизительно 0,4 дол. США. Таким образом, в настоящее время *BIK*-ключ — один из самых дешевых идентификаторов.

Среди современных методов идентификации личности с помощью оптического канала считывания информации выделим такие, которые не предусматривают создания специальных условий для регистрации данных, а именно:

метод идентификации субъекта по фотографии лица;

метод идентификации субъекта по штрих-коду, представленному вместе с фотографией.

Идентификация субъекта по фотографии лица существенно затрудняет организацию разграничения прав доступа к высококонфиденциальной информации и делегирование полномочий сотрудникам. Кроме того, правильное установление личности субъекта зависит от ракурса фотосъемки, освещения, расстояния и других условий регистрации фотоснимка. Нестационарные условия получения фотоснимка с помощью камеры требуют разработки сложного алгоритма распознавания с выделением локальных структур лица и соответствующего классификатора с гибкими границами для идентификации субъекта [9]. Сложность реализации мето-

да идентификации субъекта по фотографии лица при неидеальных условиях экспозиции в приемлемые сроки (несколько секунд) требует также значительных вычислительных ресурсов. Поэтому он редко используется для оперативного контроля доступа к ноутбукам [1, 4, 7, 8] и к десктопам, а для ультрамобильных вычислительных устройств со встроенной операционной системой типа Windows Embedded и для карманных персональных компьютеров, смартфонов или коммуникаторов соответствующие решения на рынке отсутствуют.

Идентификация владельцев мобильных средств, в основу которой положено использование штрих-кодов, должна предусматривать у субъекта наличие запасных идентификаторов на случай компрометации ключей и плановой ротации кодовых комбинаций. Очевидно, что организационно такая система является слабой. Следует заметить, что идентификация с помощью штрих-кодов требует наличия специального принтера стоимостью 200—1000 дол. США, а это делает эксплуатацию подобных систем экономически не целесообразной.

BIK-код — это состояние *BIK*-ключа, определяемое позициями отверстий на вращающихся пластинах и их положениями относительно оси. Задача распознавания *BIK*-кода заключается в определении по фотографическому изображению сцены состояния *BIK*-ключа (позиций и положений координат отверстий относительно оси ключа) и декодирование его в разряды двоичного числа. В первоначальных разработках отверстия *BIK*-ключа последовательно считывались ридером, состоящим из оптопары и микроконтроллера (бесконтактный способ [1]). В течение последних десяти лет создано несколько алгоритмов обработки результатов бесконтактного способа ввода *BIK*-ключа для различных конструкций ключа и типов микроконтроллеров.

Предлагаемый способ позволяет выполнять ввод *BIK*-ключа с большего расстояния, чем бесконтактный способ (дистанционно) с помощью оптопар, и считывание ключа в этом случае происходит не последовательно, а параллельно. Это обеспечивает защищенность от несанкционированного считывания ключа злоумышленниками с помощью специальной аппаратуры. Следовательно, предложенный способ ввода ключа является дистанционным.

Актуальность разработки нового способа ввода *BIK*-ключа объясняется наличием устройств, требующих выполнения процедуры идентификации пользователя и обладающих фото- или видео- камерой, подключить к которым ридер с оптопарами нерационально или неоправданно дорого. Примером таких устройств являются мобильные телефоны с фотокамерами [10]. Кроме того, дистанционный ввод *BIK*-ключа может быть ис-

пользован как резервный способ входа в систему с помощью Web-камеры персонального компьютера (ПК) или как один из способов многофакторной идентификации оператора.

Характеристики *BIK*-кода для идентификации собственника вычислительных средств [1—8] следующие:

число разрядов вводимого кода — 28* (256) бит;

способ ввода новой кодовой комбинации — механический ручной набор;

цена носителя кода — 0,4 (0,2)USD;

не требуется дополнительного оборудования.

Звездочка означает, что рекомендуется последовательно вводить два четырнадцатиразрядных *BIK*-ключа с различными *BIK*-кодами. Это позволяет увеличить число кодовых комбинаций и ослабить влияние человеческого фактора. Такой вариант ввода кодовой комбинации необходим для систем, предоставляющих права доступа только при последовательном вводе двух ключей двумя уполномоченными лицами (принцип двух рук). Поэтому комплекс персонализации [8, 11] всегда комплектуется двумя ключами. При этом число вводов ключа ограничивается только удобством эксплуатации системы. Увеличение числа разрядов вводимого кода с 28 до криптографического стандарта в 256 бит обеспечивается алгоритмами расширения вектора кода [4] и регламентом ротации ключей [12]. С этой целью была успешно использована программа гаммирования, реализованная на микроконтроллере фирмы ATMEL стоимостью 0,5 дол. США.

Для того чтобы облегчить процесс запоминания комбинации с учетом особенностей ассоциативных механизмов человеческой памяти, пластины ключа выполнены из разноцветного пластика, а на ребре каждой пластины нанесены буквы и цифры (что обеспечивается литьевыми формами).

Для авторизации доступа к вычислительным ресурсам главным требованием является стойкость системы к перебору ключей доступа в течение заданного периода времени, надежность и простота эксплуатации, возможность оперативной смены кодовой комбинации ключа без использования внешних средств и их низкая стоимость. Оперативность смены кодовой комбинации ключа позволяет в случае его компрометации передать пользователю новый ключ по доверенному каналу без необходимости замены идентификатора или перепрошивки его носителя, что может быть использовано также в случае необходимости делегирования прав доступа другому сотруднику при форс-мажорных обстоятельствах. Оперативность смены кодовой комбинации позволяет использовать ключ в нескольких системах безопасности с различными типами ридеров, а также как ключ к электромеханическому замку.

BIK-ключ является механически перестраиваемым, поэтому возможность компьютерного перебора 2^{28} кодовых комбинаций при идентификации пользователя невозможна без вскрытия корпуса устройства считывания и доступа к его электрическим цепям. Как правило, для обеспечения безопасности [11] число вводов ключа ограничивается пятью попытками, после чего система блокируется и выдается сигнал тревоги. Поэтому доступ к терминалу путем механического подбора практически маловероятен. Следует заметить, что число комбинаций для четырехзначного десятичного *PIN*-кода банкоматов и мобильных телефонов, имеющих фото- видеокамеру, составляет $10000 \approx 2^{13}$, в то время как предложенное решение увеличивает стойкость подобных систем к перебору в 2^{15} раз.

При использовании *BIK*-ключа для защиты информации число разрядов *BIK*-кода может быть увеличено с помощью алгоритмов гаммирования [4]. Предлагаемый способ авторизации пользователя телекоммуникационных и вычислительных средств позволяет достичь лучшего сочетания показателей относительно безопасности, эффективности эксплуатации и стоимости реализации решений, что подтверждено специалистами, в том числе экспертами Национального банка Украины.

Для создания алгоритма распознавания *BIK*-кода использовано полунатурное моделирование процессов оптического ввода ключа-идентификатора, который регистрировался сканером BearPaw 2400 TA с разрешением 600 dpi в режиме фиксации позитива фотопленки слайд-модулем, чтобы на фоне темного изображения ключа получить контрастные белые отверстия. Для моделирования поворота плоскости ключа в области пространственных координат применен пакет Adobe Photoshop 8.0 CE и среда программирования MatLab 7.0 для реализации задачи распознавания образов. Смена значений разрядов ключа-идентификатора выполнялась вручную. Разработанная программа распознавания *BIK*-кода позволила успешно обрабатывать изображения, полученные с фотокамер мобильных телефонов при изменениях значений соответствующих параметров алгоритма. На рис. 2 приведено изображение, полученное с помощью фотоаппарата мобильного телефона Nokia N93 формата 2048×1536, 300 dpi.

В качестве информационных признаков *BIK*-кода в образе ключа использованы координаты центров масс отверстий, порядок их следования и положение относительно оси ключа. Процедура классификации образов реализована на основании детерминированного решающего правила: если площадь объекта определенной яркости находится в заданном диапазоне значений, то этот объект классифицируется соответственно как отверстие, пластина или ручка. Процедуре распознавания *BIK*-кода предшествует предварительная обработка изображения ключа-идентификатора для повышения визуального качества полученных данных [5]. Поскольку изоб-

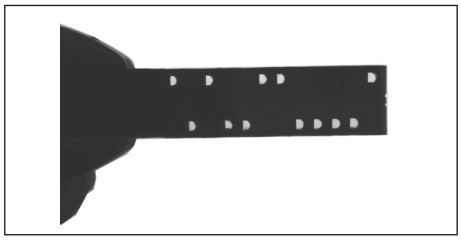

Рис. 2

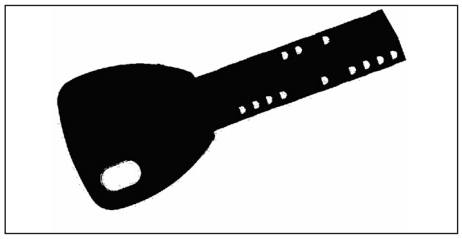

Рис. 3

ражение представляет собой упорядоченную совокупность пластин разного цвета, то для составления карты признаков объектов использован метод бинарной сегментации поля образа по заданному порогу [9].

Распознавание *BIK*-кода требует выполнения нескольких подзадач. Некоторые из них могут выполняться независимо, другие — только последовательно. Поэтому была выполнена алгоритмизация распознавания *BIK*-кода, чтобы довести решение задачи до программы на языке MATLAB.

Распознавание искомых информационных признаков в образе ключа-идентификатора *BIK*-кода состоит из двух этапов:

I. Поиск объектов изображения, соответствующих отверстиям и другим деталям ключа.

II. Декодирование координат отверстий в значения разрядов двоичного числа, соответствующие *BIK*-ключу.

На рис. 3 представлено изображение *BIK*-ключа, полученное по описанному выше методу полунатурного моделирования после бинарной сегментации пороговым методом.

Алгоритм поиска отверстий:

1. Сегментация образа ключа по заданному порогу.

2. Выполнение процедуры поиска объектов обработанного образа.

3. Выделение объектов с площадью, соответствующей отверстию.

4. Запись в массив координат центров масс отверстий (ЦМО), рассчитываемых по формуле [12]:

$$x_c = \frac{1}{N} \sum_{p(x,y)\in\Omega} x, \quad y_c = \frac{1}{N} \sum_{p(x,y)\in\Omega} y,$$

где N — число пикселей; $p\,(x, y)$ — множество точек объектов образа Ω. На рис. 4 представлено изображение выделенных отверстий *BIK*-ключа.

Алгоритм декодирования координат отверстий в значения разрядов двоичного числа, соответствующего коду *BIK*-ключа:

1. Определение положения ручки ключа относительно отверстий (алгоритм определения координат центра массы ручки (ЦМР) аналогичен алгоритму поиска ЦМО).

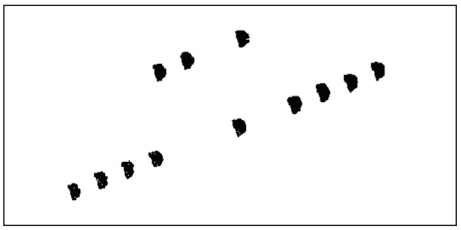

Рис. 4

Рис. 5

2. Расчет угла наклона оси ключа.

3. Сдвиг оси координат в точку ЦМР и поворот координат ЦМО в горизонтальное положение.

4. Декодирование координат отверстий в значения разрядов двоичного числа, соответствующего коду *BIK*-ключа.

Расчет угла наклона оси ключа:

1. Сегментация образа по заданному порогу.

2. Выполнение процедуры поиска объектов обработанного образа.

3. Выделение объектов с площадью, соответствующей сегментам ключа.

4. Заполнение отверстий в сегментах объединением бинарного образа сегментов с образом отверстий.

5. Выполнение морфологических операций заполнения внутренних пустот сегментов для получения однородных прямоугольных участков по следующей формуле [9]: $((S \bigcup O) \oplus B) \Theta B$, где S, O и B — множества пикселей сегментов, пикселей отверстий и пикселей контура; $\oplus$ — операция дилатации; Θ — операция эрозии. На рис. 5 показан образ сегментов *BIK*-ключа после выполнения морфологических операций.

6. Запись в массив координат центров масс сегментов (ЦМС) ключа.

7. Поиск ЦМС, наиболее и наименее удаленного от ЦМР; вычисление параметров уравнения прямой, проходящей через эти две точки.

8. Определение ЦМО, находящихся выше (единицы) и ниже (нули) прямой.

9. Поиск в полученных массивах координат единиц и нулей ЦМС, наиболее и наименее удаленных от ЦМР.

10. Расчет для каждой пары ЦМС значений угла наклона прямой, проходящей через эти две точки. В результате анализа экспериментальных данных, полученных методом полунатурного моделирования, установлено, что угол наклона оси ключа приближается к средним арифметическим значениям наклона прямых, проходящих через неупорядоченные множества координат нулей и единиц. Сдвиг в ЦМР точки начала координат и поворот оси коор-

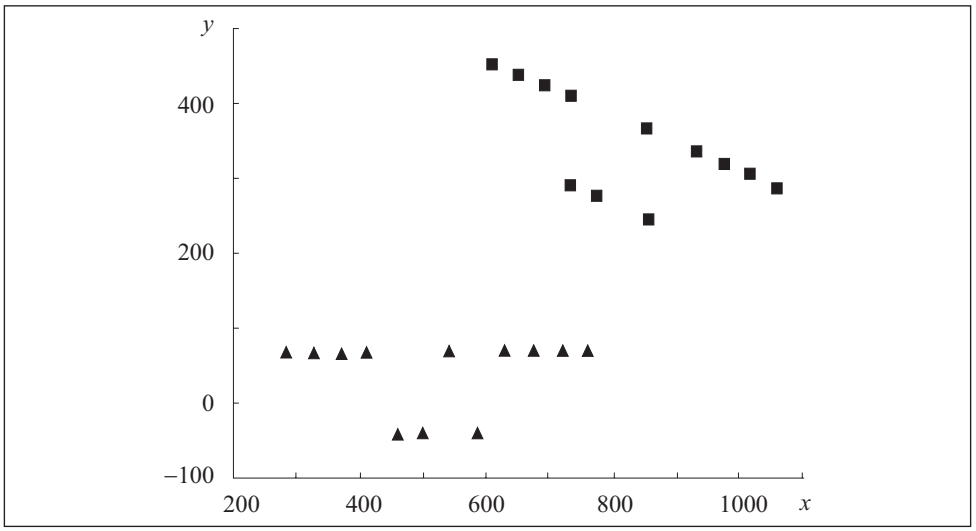

Рис. 6

динат в горизонтальное положение выполняются по формулам [9] $\bar{x} = (x - x_0)\cos\theta + (y - y_0)\sin\theta$, $\bar{y} = -(x - x_0)\sin\theta + (y - y_0)\cos\theta$, где $\bar{x}$, $\bar{y}$ — координаты ЦМО в новой системе координат; x_0, y_0 — координаты ЦМР, в которые перенесено начало отсчета; θ — угол поворота новой системы координат относительно старой; x, y — координаты ЦМО в старой системе координат.

11. Сортировка массива координат по значениям проекций на ось абсцисс ЦМО и выполнение соответствующей перестановки массива значений проекций на ось ординат. На рис. 6 приведен график, на котором квадраты соответствуют координатам ЦМО после регистрации, треугольники — координатам ЦМО в новой системе координат после сдвига и поворота. Наиболее удаленная от начала координат по оси абсцисс точка ЦМО становится начальным значением последовательности разрядов ключа. Значения с положительными координатами проекций на ось ординат соответствуют нулям, а с отрицательными — единицам. Если ручка ключа после регистрации находилась слева, то выходной массив надо переписать в обратном порядке (реверсировать).

Время выполнения программы распознавания *BIK*-кода в среде MatLab 7.0 составило менее 10 с на платформе P4 3ГГц, ОЗУ 1 Гб в операционной системе Windows XP. Экспериментальные данные, полученные для изображений размера, характерного для фотокамер телефонов, также были успешно распознаны по предложенному алгоритму на ПК после изменения значений констант, соответствующих динамическому

диапазону устройства регистрации и его разрешающей способности. Алгоритмы поиска ЦМО, ЦМР и ЦМС ключа могут выполняться независимо, что является основой для многопоточной реализации алгоритма распознавания *BIK*-кода в виде параллельно работающих подпрограмм.

Таким образом, в представленном новом способе ввода *BIK*-ключа для идентификации пользователей телекоммуникационных и вычислительных средств использован дистанционный ввод двоичного кода. В основу способа положен метод распознавания фотографического образа *BIK*-кода, набранного на *BIK*-ключе-идентификаторе. Работоспособность и рациональность предложенного метода распознавания подтверждена результатами полунатурного моделирования изображений, полученных с помощью серийных оптических сканеров, фотоаппаратов мобильных телефонов, и их обработки за приемлемое время на массовых ПК.

The new method of Bardachenko identification key (BIK) input is presented for identification of operator of computing devices which are arranged by photo and video cameras. The method based on photo image distance recognition. The competence of given method is proved by results of BIK-key scale-down modeling on MatLab 7 environment and image recognition taken from serial optical scanner.

1. *Бардаченко В. Ф., Кариман А. В., Колесницкий О. К. и др.* Анализ современных средств аутентификации для систем защиты информации //УСиМ. — 2004. — №3. — С. 81—92.
2. *Патент* Украины UA 85 G06K 19/06. Идентификатор/ Бардаченко В. Ф., Стогний Б. С. и др. — Опубл. — 31.10.1997 , Бюл. № 5.
3. *Патент* России RU 2097519 C1. Идентификатор/Бардаченко В. Ф., Стогний Б. С. и др. — Опубл. — 27.11.1997, Бюл. № 33.
4. *Бардаченко В. Ф., Королев В. Ю.* Концепция построения систем персонализации на базе расширения вектора кодов *BIK*-ключа // УСиМ. — 2007. — № 1. — С. 44—53.
5. *Бардаченко В. Ф., Корольов В. Ю.* Розробка математичного і програмного забезпечення для автоматизованої системи відновлення зображень //Вісті академії інженерних наук України. — 2003. — № 4 (20). — С. 12—15.
6. *Бардаченко В. Ф., Корольов В. Ю.* Алгоритмізація методу за шифрування текстових повідомлень з використанням поліалфавітної перестановки та набірного ключа // Матеріали І Міжнародної наук.-техн. конф.: Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування (СПРТП-2005). — Вінниця : ВНТУ Мін. освіти і науки України. — 2005. — С. 120—121.
7. *Бардаченко В. Ф., Корольов В. Ю.* Таймерна *BIK-BAK* технологія захисту периферійних пристроїв від несанкціонованого доступу //Вісті академії інженерних наук України. — 2005. — № 4 (27). — С. 12—14.
8. *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.
9. *Цифровая* обработка изображений в информационных системах: Учеб. пособие / И. С. Грузман, В. С. Киричук и др. — Новосибирск: изд-во НГТУ. — 2002. — 352 с.

10. *Корольов В. Ю., Поліновський В. В., Герасименко В. А.* Персоналізація мобільних телекомунікаційних пристроїв // Матеріали III Міжнародної наук.-техн. конф.: Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування (СПРТП-2007). — Вінниця : ВНТУ Мін. освіти і науки України. — 2007. — С. 19—20.
11. *Бардаченко В. Ф., Поліновський В. В., Костенко О. В.* Побудова політики безпеки для інформаційних систем з використанням *ВІК-ВАК* технологій // Там же. — 2007. — №1 (31). — С. 3—15.
12. *Корольов В.Ю.* Інтеграція ПАРМ «Віртуальна канцелярія» і системи Intel® vPro на базі рішень *ВІК*-персоналізації // Там же. — 2007. — № 2 (32). — С. 6—15.

Поступила 13.03.07;
после доработки 12.09.07

КОРОЛЕВ Вячеслав Юрьевич, канд. техн. наук, ст. науч. сотр., зав. отд. Центра таймерных вычислительных систем Ин-та кибернетики им. В.М. Глушкова НАН Украины. В 1999 г. окончил Национальный технический университет Украины «КПИ». Область научных исследований — защита информации, цифровая обработка изображений.