

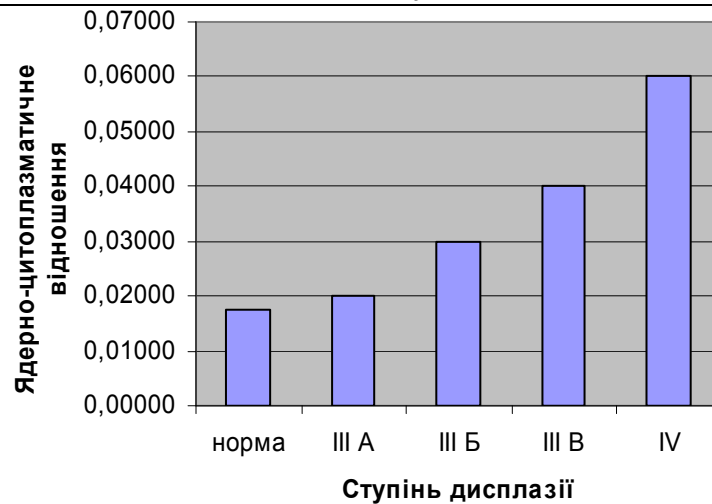


Рис. 2. Графік залежності ядерно-цитоплазматичного відношення $k_{яцв}$ від типу дисплазії епітелію

Висновок

Розроблена інформаційно-аналітична система дає можливість здійснювати морфометричні вимірювання гістологічних і цитологічних зображень. Статистичний аналіз показав, що закон розподілу ядерно-цитоплазматичного відношення є нормальний і дав змогу провести ідентифікацію різних ступенів дисплазії на основі кількісної оцінки $k_{яцв}$.

Література

1. Автандилов Г.Г. Основы количественной паталлогической анатомии / Автандилов Г.Г. – М. : Медицина, 2002. – 240 с.
2. Егорова О. Компьютерная микроскопия / Егорова О., Пантелеев В., Клыкова Е. – М. : Техносфера, 2005. – 300 с.
3. Гмурман В.Е. Теория вероятностей и математическая статистика / Гмурман В.Е. – М. : Высшая школа, 1972. – 368 с.
4. Березький О.М. Алгоритми статистичної обробки біомедичних зображень / О.М. Березький, К.М. Березька, Г.М. Мельник // Матеріали міжнар. конф. „Інтелектуальні системи прийняття рішень та проблеми обчислювального інтелекту” (ISDMCI’2009), м. Євпаторія, 18–22 травня 2009 р. – Херсон : ХНТУ, 2009. – Т. 2. – С. 227–230.
5. Березький О.М. Інформаційно-аналітична система дослідження та діагностування пухлинних клітин на основі аналізу їх зображень / О.М. Березький, Ю.М. Батько, Г.М. Мельник // Вісник Хмельницького національного університету. – Хмельницький, 2008. – № 3. – Т. 1. – С. 120–130.

Надійшла 15.9.2012 р.

Рецензент: к.т.н. Коваль В.С.

УДК 621.391:004.73

К.В. КОЛЕСНИКОВ, С.И. КАУНЕНКО

Черкасский государственный технологический университет

ИСПОЛЬЗОВАНИЕ НЕЙРОСЕТЕВОГО КОНТЕЙНЕРА ДЛЯ ИДЕНТИФИКАЦИИ ПО ОТПЕЧАТКАМ ПАЛЬЦЕВ

Рассматривается алгоритм использования нейросетевого контейнера при биометрической идентификации по рисунку пальца с заполнением личной информации. Данный алгоритм позволяет защитить биометрический шаблон и усилить программную биометрическую защиту для минимизации возможности подмены шаблона с целью взлома.

This algorithm allows to protect the biometric template and strengthen the protection of biometric software to minimize the possibility of substitution pattern in order to break-in.

Ключевые слова: идентификация по отпечаткам пальцев, биометрия, нейросетевой контейнер.

Введение

В настоящее время активно используются биометрические средства аутентификации при доступе к информации, находящейся на ПК, flash-накопителях, при удаленной идентификации и при доступе к ключу формирования ЭЦП [1,2]. Подобные средства имеют разные биометрические датчики ввода информации,

однако, на данный момент, наибольший объем (от 50 до 80 % по разным оценкам) составляют средства, использующие ввод данных о рисунке отпечатка пальца. Этот сектор устройств поддерживается практически всеми фирмами, профессионально занимающимися средствами биометрического ограничения доступа. Применяются на практике три типа сканеров отпечатков пальцев, построенных на разных физических принципах: оптические, емкостные сканеры, сканеры с радиочастотным считыванием. Как правило, представленные продукты биометрической защиты построены с использованием метода «разблокировки ключа». Ключ и биометрический образ хранятся раздельно в системе. Для получения доступа к ключу необходимо пройти биометрическую идентификацию, при этом решение о разблокировке ключа принимается на основе классического решающего правила, имеющего «последний бит» (да/нет).

Постановка задачи

В случае реализации программным способом процедуры обработки данных в процессе биометрической идентификации по рисунку отпечатков пальцев возникает две основных проблемы:

1. Биометрический шаблон не защищен, может быть скомпрометирован или подменен.

Программная биометрическая защита оказывается крайне слабой из-за подмены «последнего бита». «Последний бит» обнаруживается подбором. После его обнаружения хакер для тиражирования успеха выпускает вирус, который позволяет взламывать действующую защиту и получать доступ к конфиденциальной информации.

Задачей данной работы является анализ и обнаружение слабых мест биометрической идентификации по рисунку отпечатка пальцев, а также реализация метода заполнения нейросетевого контейнера личными данными для повышения эффективности метода.

Решение задачи

Одновременно решить обе проблемы удастся, если перейти от классической обработки к использованию высоконадежного нейросетевого преобразователя «биометрия-код», выполненного по требованиям международного стандарта ISO/IEC 27001.

При реализации нейросетевого преобразователя возникает проблема недостаточного объема данных, извлекаемых из рисунка отпечатка пальца.

Обычно анализируются:

- контрольные точки, находящиеся в окончаниях или разветвлениях папиллярных линий, так называемые минуции;
- ширина папиллярных линий, впадин в районе контрольной точки;
- плотность пор в области контрольной точки;
- направление папиллярных линий.

Все перечисленные выше параметры обычно измеряются в окрестностях особых точек (минуций), а биометрический шаблон рисунка отпечатка пальца обычно формируется в виде списка наиболее часто встречающихся минуций с описанием их окрестностей. Список особых точек отпечатка пальца нуждается в обязательной защите, так как по нему легко может быть найден владелец отпечатка пальца.

Реализация нейросетевого преобразователя «биометрия-код» показала, что объем обрабатываемой информации должен быть многократно увеличен путем введения дополнительных областей, не содержащих минуций. Производится контроль перечисленных выше параметров, как в областях, содержащих реальные минуции, так и в пустых областях, без особых точек. При этом внешний наблюдатель не знает, с какой контрольной областью он имеет дело: реальной минуцией или пустой областью контроля параметров рисунка отпечатка пальца.

Объем обрабатываемой информации, при этом подходе к решению задачи, увеличивается в 3-4 раза, что позволяет улучшить стойкость нейросетевого преобразователя «биометрия-код» к атакам подбора за счет увеличения информативности биометрического образа. В качестве безопасного, действительно биометрического шаблона, нейросетевой преобразователь хранит расширенный список контролируемых областей. Добавления «пустых» областей в расширенный список осуществляется с использованием генератора случайных чисел, что позволяет скрыть расположение реальных контрольных точек (минуций) и, тем самым, обеспечить анонимность пользователя.

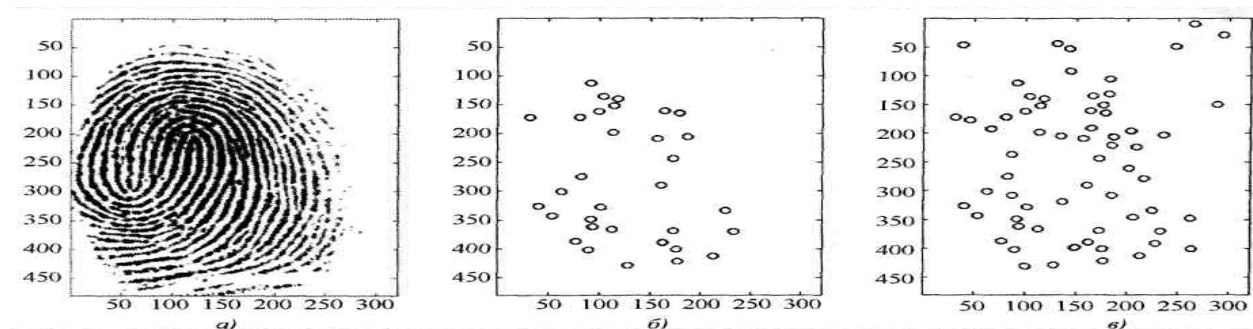


Рис. 1. Пример создания безопасного биометрического шаблона: а – изображение отпечатка пальца; б – места расположения реальных минуций, запоминаемых в обычном биометрическом шаблоне; в – безопасный биометрический шаблон, расширенный за счет дополнительных областей, не содержащих минуций

Нейросетевой преобразователь «биометрия-код» обучают на выдачу заданного личного кода пользователя с использованием безопасного биометрического шаблона и нескольких отпечатков пальца пользователя [3]. Используется алгоритм быстрого обучения, обеспечивающий обучение нейросети, содержащей от 240 до 360 входов и 256 выходов (каждый выход соответствует одному разряду 256 битного личного ключа).

Так, на рисунке 1,б отображены 30 реальных минуций, найденных в реальном отпечатке пальца, показанном на рисунке 1,а. Эти 30 реальных особых точки дополнены тридцатью мнимыми особыми точками, что дает 60 контрольных точек, отображенных на рисунке 1,в. При контроле всего 4 параметров, каждой из 60 контрольных точек, получаем нейросеть с 240 входами. Учет 6 параметров рисунка отпечатка пальца по каждой из 60 контрольных точек позволяет использовать нейронную сеть с 360 входами.

После обучения сети искусственных нейронов, данные о содержании минуций в контрольных точках уничтожают, уничтожают также информацию о личном коде пользователя. Информация об обученной нейронной сети сохраняется в виде таблицы связей и весов нейронов этой сети, в виде так называемого «нейросетевого контейнера».

Алгоритм обучения нейросети:

Шаг 1. Пользователь предъявляет несколько (10–15) отпечатков регистрируемого пальца.

Шаг 2. В каждом отпечатке выполняется поиск минуций.

Шаг 3. Отпечатки выравниваются относительно найденных минуций. Создается множество $M(n)$, в котором запоминаются координаты областей, содержащих найденные минуции, где n – общее количество таких областей.

Шаг 4. С помощью генератора случайных чисел задается множество $D(r)$, в котором запоминаются координаты дополнительных контрольных областей, не пересекающихся с областями в множестве M . Для обеспечения стойкости безопасного биометрического шаблона необходимо, чтобы $r > 3n$.

Шаг 5. Создается безопасный биометрический шаблон путем объединения множеств M и D в множество $B(k)$, где $k = n + r$. При этом задается определенный порядок следования областей множества B в соответствии с их координатами, например, слева направо и сверху вниз.

Шаг 6. Для каждого отпечатка пальца, участвующего в обучающей выборке, в каждой области из множества $B(k)$ вычисляется вектор контролируемых биометрических параметров I_k , включающий:

- наличие/отсутствие минуций в данной области;
- среднюю ширину папиллярных линий и впадин;
- плотность пор;
- направление папиллярных линий.

Шаг 7. Набор, полученных векторов, используется для обучения двухслойной нейронной сети с 256 выходами. Каждый выход соответствует определенному биту извлекаемого криптографического ключа пользователя или его длинного пароля доступа. После этого автомат обучения должен добиться появления нужного кода на выходах нейронных сетей при предъявлении на их входы любого из набора векторов биометрических параметров из обучающей выборки «Свой». При предъявлении нейросети любого набора векторов биометрических параметров из выборки «Чужие», на выходах нейронной сети должны появляться случайные коды. На каждом из выходов должен появляться независимый «белый шум» двух равновероятных состояний «0» и «1». По требованиям для корректной работы допустимо появление корреляции между парами различных разрядов выходного кода, однако, среднее значение модулей коэффициентов корреляции не должно превышать 0,15.

При аутентификации проверяемого рисунка отпечатка пальца сканируют этот рисунок, выравнивают его относительно безопасного биометрического шаблона с использованием предварительно сохраненной в шаблоне вспомогательной информации. В качестве вспомогательной информации могут быть использованы координаты точек наибольшей кривизны папиллярных линий, данные о структуре поля направлений отпечатка или координаты трех-четырёх минуций. Открытая часть шаблона не превышает 3 % от объема полного безопасного биометрического шаблона. Далее, используя сам безопасный биометрический шаблон, выделяют на нем контролируемые области, вычисляют параметры контролируемых областей и подают их на соответствующий вход нейронной сети, а нейронная сеть преобразует входные данные в некоторый выходной код.

Результаты

За счет того, что исчезает «последний бит» (и появляется 256 «последних бит») снимается проблема тиражирования успеха хакерами при взломе одной программы. Если каждая программа имеет свой ключ, подбор ключа является задачей с гарантированно высокой вычислительной сложностью. После взлома биометрической защиты одной программы, создать на основе полученного опыта универсальную программу для автоматического взлома программ других пользователей нельзя.

Так как параметры отпечатка пальца своего пользователя связаны с его личным ключом с помощью безопасного биометрического шаблона, таблицы связей и весов нейронов нейросетевого преобразователя, обеспечивается высокий уровень конфиденциальности, анонимности, обезличивание персональных биометрических данных пользователя. Это позволяет сохранить правовое поле и выполнять требования закона «О персональных данных».

1. Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации / [Малыгин А.Ю., Волчихин В.И., Иванов А.И., Фунтиков В.А.]. – К. : "Монография", 2005. – 273с. – (Издательство Пензенского государственного университета).
2. Малыгин А.Ю. Нейросетевое преобразование биометрического образа человека в код его личного криптографического ключа / Малыгин Александр. – К. : Москва, 2008. – 87 с.
3. Фунтиков В.А. Биометрико-нейросетевое управление криптографическими механизмами защиты информации. «Нейрокомпьютеры: разработка, применение» / Фунтиков В.А. Ефимов О.В.; пер. с англ. Иванов А.И. – М. : Буквица, 2007. – 6– 8 с.

Надійшла 24.9.2012 р.
Рецензент: д.т.н. Снитюк В.Е.

УДК 621.382

Ю.С. КРАВЧЕНКО, С.Ю.КРАВЧЕНКО
Вінницький національний технічний університет

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЕМІСІЙНО-СПЕКТРАЛЬНОГО КОНТРОЛЮ В ПЛАЗМОВІЙ ТЕХНОЛОГІЇ

Досліджена можливість організації контролю плазмохімічних процесів в мікроелектронній технології на основі використання сумарного інтегрального випромінювання декількох спектральних ліній або смуг, зміна інтенсивності яких відображає хід технологічного процесу травлення мікроструктур, зокрема, спектральних ліній збуджених атомів хлору в діапазоні довжин хвиль 725,6– 754,4 нм.

The possibility of controlling plasma processes in microelectronic technology on the basis of the total integral radiation of several spectral lines or bands change in intensity which reflects the technological process of digestion microstructures, in particular, the spectral lines of excited chlorine atoms in the wavelength range 725.6 – 754.4 nm

Ключові слова: плазмохімічна технологія, емісійно-спектральний контроль, чотирехлористий вуглець, ефективність.

Вступ

Питання ефективності контролю в мікроелектронній плазмохімічній технології, яка на даний час практично безальтернативно забезпечує точність відтворення функціонального рельєфного рисунку на кремнієвих пластинах до Ø300 мм на рівні $\leq 0,13$ мкм [1], пов'язане з суттєвим зменшенням розмірів функціональних елементів інтегральних мікросхем і їх ущільненням в межах самої мікросхеми. В основу розробок сучасних систем покладено за ходом технологічного процесу при плазмохімічному травленні мікроструктур здебільшого покладено метод, який ґрунтується на використанні емісійно-спектрального методу дослідження параметрів нерівноважної плазми [2– 3], сутність якого полягає в реєстрації та дослідженні оптичного спектру власного випромінювання збуджених атомів та молекул [4– 6], а переваги забезпечуються можливістю відносно простого оперативного отримання інформації про хід цільового технологічного процесу і його безконтактність.

При достатньо великому співвідношенні сигнал/шум відносно прості задачі управління, наприклад, визначення моменту закінчення цільового процесу травлення, вирішуються на основі візуальної інтерпретації кінетичних кривих сигналу реального часу і порівнянням зі зразковими записом сигналу. Складності для розв'язання цієї простої задачі виникають по мірі зменшення площі пластини, яка піддається плазмовому травленню (в такому випадку складова шуму у співвідношенні сигнал/шум збільшується) [1, 7]. Проблеми виникають також при здійсненні багатостадійних процесів, які пов'язані зі зміною плазмоутворюючих газів та механізму взаємодії хімічно активних частинок плазми з поверхнею твердого тіла.

За таких умов вирішення основної задачі (забезпечення ефективного і надійного контролю плазмохімічного процесу) можливе лише шляхом застосування нетрадиційних підходів як при реєстрації інформаційних сигналів, так і при їх обробці.

Підвищення ефективності емісійно-спектрального контролю плазмохімічних процесів на даний час вирішується різними методами: підвищенням чутливості відповідних фотоелектронних сенсорів, введенням частотного перетворення інформаційного сигналу [8], запровадженням багатоканального контролю [9– 12], використанням сучасної мікропроцесорної техніки [11].

Мета даної роботи – аналіз можливостей підвищення ефективності контролю плазмохімічних процесів в мікроелектроніці за рахунок спрощення структури контролюючих приладів і використання в якості інформаційного сигналу інтегрального власного випромінювання декількох спектральних ліній або смуг продуктів розкладання основної молекули плазмоутворюючого газу.

Аналіз проблеми

Аналіз проблеми будемо проводити на прикладі використання в якості плазмоутворюючого газу чотирехлористого вуглецю або тетрахлорметану (CCl_4). Цей газ широко використовується в мікроелектронній плазмовій технології при плазмохімічному травленні мікроструктур з арсеніду галію, металевих плівок (Al, Cu), інших матеріалів, що знайшли застосування в сучасній мікро- та наноелектроніці [12].