

2. Кавун С.В. Аналіз стану інформаційної безпеки в системах дистанційного навчання. / С.В. Кавун, О.А. Сахно // Збірник наукових праць «Фінансово-кредитна діяльність: проблеми теорії та практики». – Харків: Вид. ХІБС УБС НБУ.– 2010. – № 1(8). – Частина II. – С. 222-234.
3. Украина - на шестом месте по уровню экономической преступности. – [Электронный ресурс]. – Режим доступа: http://www.prostobiz.ua/biznes/upravlenie_biznesom/stati/ukraina_na_shestom_meste_po_urovnyu_ekonomicheskoy_prestupnosti
4. Выход украинских предприятий на мировой рынок капитала с помощью IPO. – [Электронный ресурс]. – Режим доступа: http://www.rusnauka.com/35_PWMN_2008/Economics/38471.doc.htm

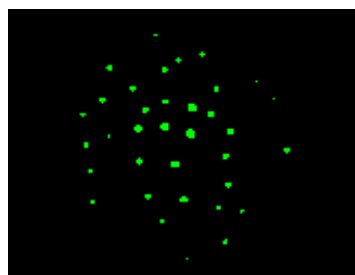
ВЫЧИСЛЕНИЕ ВЕРОЯТНОСТИ ПОВТОРА, МЕТОДЫ РАСПОЗНАВАНИЯ И СРАВНЕНИЯ ЭЛЕКТРОРАЗРЯДНОЙ МЕТКИ БУМАЖНЫХ ДОКУМЕНТОВ

Игорь ОГЛИНДЭ,

*Министерство информационных технологий
и телекоммуникаций (Республика Молдова)*

The technology of protection of paper carriers by means of Electrodigit Technology, mathematical features of the given labels is investigated, proved them no reproducibility and singularity, the likelihood analysis of possibility of repetition of an Electrodigit Technology is carried out, possible algorithms of definition of authenticity of labels are resulted at comparison.

На прошлой конференции Securitatea Informationala господином Шкилёв Владимир, Недиогло Виктор и Адамчук Аркадий был представлен патент об электро-разрядной защите бумажных документов. Схема проведения эксперимента чрезвычайно проста: на бумаге электро-разрядным способом пробиваются небольшие отверстия; затем полученные образцы сканируются на просвет на обычном сканере и сохраняются в базе данных или подписываются цифровым кодом, в котором содержится информация о метке.



Целью исследований было выявление вероятности повтора метки и как следствие подделки документа. При проведении ряда экспериментов было обнаружено, что полученные отверстия имеют разные величины от 1-го до 30 пикселей и разные формы полимино. Теоретически, если даже одно отверстие сформировано из 15 пикселей, то оно может принимать до 27.394.666 различных форм, что дает нам уже возможность с уверенностью сказать, что практически невозможно пробить повторно такое же отверстие. Можно сказать, что каждое отверстие уникально в своем роде.

При ряде математических расчетов используя комбинаторный метод, было выявлено, что вероятность появления отверстий в том же месте, размером в один пиксель, нанесенных на метку очень мала:

$$C_n^r = \frac{n!}{r!(n-r)!}$$

80 отверстий – $0.2334 * 10^{-253}$, **100 отверстий** – $0.1119 * 10^{-307}$,

120 отверстий – $0.9665 * 10^{-358}$

А если учесть и вероятность повтора формы отверстий, то вероятность уменьшается далеко за 10^{-450} . Так что с позиции уровня защиты эта величина равна бесконечности. Технологический аспект проблемы показывает, что бесконечность и 10^{-450} – слабо отличимые понятия. Данные расчеты доказывают, что электроразрядная технология защиты документов эффективна и безопасна – даже производитель этой метки не в состоянии создать две одинаковые метки.

Для распознавания меток было предложено несколько методов. Один из них состоит в следующем: метка сканируется, после чего осуществляется бинаризация изображения. Таким образом, можно получить различные математические характеристики метки, такие как число отверстий, величина и интенсивность расположений отверстий, площадь распределения, координаты и многие другие. Эти характеристики можно также использовать, как генератор случайных чисел, характерных для каждой метки в отдельности. Данный метод дает возможность составить единый цифровой код для каждой метки. Также из этих характеристик можно составить базу данных. Эту базу данных в дальнейшем можно использовать для сравнения и выявления подлинности меток. То есть при повторном сканировании и бинаризации метки, можно сравнивать характеристики и сказать с какой-то долей вероятности о подлинности метки. Такой метод хорош, если повторное сканирование происходит в тех же идеальных условиях что и первое, что на практике невозможно из-за изменений характеристик метки при сканировании под разными углами поворота.

Для решения этой проблемы было предложено несколько математических методов. На метку наносятся реперные точки для удобства определения координат и других характеристик отверстий, в дальнейшем используя различные алгоритмы, можно определить подлинность метки. Другой возможный метод без реперных точек состоит в вычислении после бинаризации центра тяжести каждого отверстия и площади, определяются два самых отдаленных отверстия и центры тяжести этих

отверстий можно использовать как реперы. Эти алгоритмы дают нам возможность при повторном сканировании не зависимо от угла расположения метки на сканере определить подлинность метки.

После определения характеристик точек для дальнейшей обработки меток можно использовать различные алгоритмы: теория графов и геометрические алгоритмы дают нам много возможностей. Например, **Алгоритм Краскала** для построения минимального остовного дерева, триангуляция **Делоне** и многие другие.

По итогам серии опытов и создания программ, где будут использоваться различные алгоритмы, можно будет сделать вывод о том какой алгоритм и какие методы будут наиболее эффективны и применимы на практике и наименее затратные и ресурсоемкие. Итоги данных работ в дальнейшем будут опубликованы и представлены на будущих конференциях.

Литература:

- 1) Шкилев В.Д., Адамчук А.Н., Недиогло В.Г. Электроразрядная технология защиты документов особой важности (*строгой отчетности*) Электронная обработка материалов, №2, 2008, с. 4-10.
- 2) Томас Кормен, Чарльз Лейзерсон, Рональд Риверст, Клифорд Штайн. Алгоритмы построение и анализ.
- 3) Шкилев В.Д. и др. Патент Республики Молдова № 3389 «Способ идентификации объектов». MD-ВОПІ №8, 2007, с. 51.

ТЕНЕВАЯ ИНФОРМАЦИОННАЯ ЭКОНОМИКА

Григорий БОРТЭ,

Экономическая Академия Республики Молдова

С развитием информационных технологий, проблема правонарушения в данной области становится всё более и более актуальной. Криминальные сообщества находятся в постоянном поиске путей получения дохода из любых возможных источников, и бизнес, основанный на вредоносном программном обеспечении, в наше время не является исключением в наши дни. Они ищут новые возможности для отмывания денег, и Internet стал для этого очень удобным средством. Ущерб, нанесенный данным криминальным сектором пользователям, компаниям и даже государствам не может быть переоценен. В этом отношении, Республика Молдова – не исключение. Молдавской экономике нужна защита от компьютерного криминала и теневой информационной экономики.

В соответствии с данными, предоставляемыми всемирным банком, теневая экономика составляет порядка 35,2% от мировой экономики. Конечно, эта оценка очень приближительна, относительна и усреднена, ведь, например, в США теневой