В.Д. Шкилёв, В. Г. Недиогло, А.Н. Адамчук

ЭЛЕКТРОРАЗРЯДНАЯ ИДЕНТИФИКАЦИЯ ДЕНЕЖНЫХ КУПЮР

Министерство информационного развития,
ул. Пушкина, 42, г. Кишинев, MD-2012, Республика Молдова, schilov@registru.md

Приведенная работа состоит из двух частей, в первой изложена идея высокого уровня защиты купюр, а во второй – технологические аспекты реализации метода.

Часть первая

Идея использования процессов, даже теоретически не поддающихся полному управлению, для высокоуровневой защиты документов не нова. Ещё в конце 1960 годов С. Виснер предложил использовать фотоны с заданными поляризованными состояниями [1]. Технологически идея не реализуема и по сей день, тем не менее предложение С. Виснера действительно было блестящим, хотя бы потому, что на его основе со временем развились новые подходы в криптографии, которые дают надежду разработать, рано или поздно, простые и дешевые технологии изготовления бумажных денег с высочайшим уровнем защиты.

А теперь обсудим не технологию защиты бумажных купюр, а физический эксперимент, проведенный в 1989 году, с помощью которого была еще раз подтверждена интерференция электронов [2]. В этом эксперименте сотрудники Лаборатории перспективных исследований фирмы Хитачи, возглавляемой А. Тономурой, и Университета Гакушуин в Токио пропускали поток электронов через проницаемый барьер, эквивалентный экрану с двумя щелями. После прохождения через барьер каждый электрон попадал на флуоресцентный экран, вызывая короткую вспышку света. Наблюдая за каждой вспышкой, японские экспериментаторы могли фиксировать место попадания каждого электрона. В этом дорогостоящем эксперименте использовались современные позиционно-чувствительные системы счетчиков электронов. Полученные результаты, подтверждающие волновую природу материи, приведены на рис. 1.

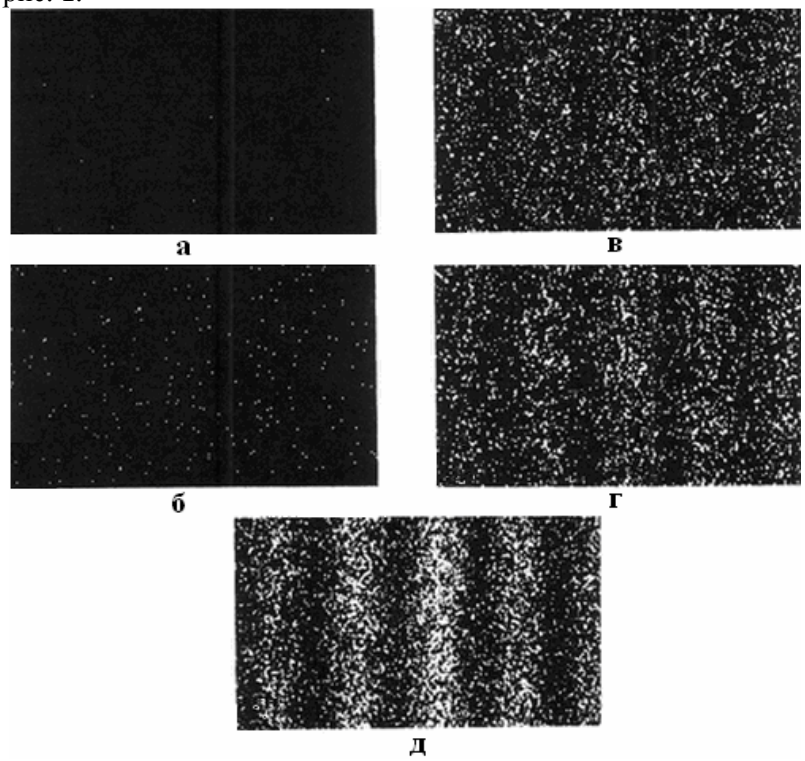

Рис. 1.Экспериментальное подтверждение существования волн материи

© Шкилёв В.Д., Недиогло В., Адамчук А.Н., Электронная обработка материалов, 2010, № 3, С. 4–8.

Вначале (рис. 1,*а* – 10 попаданий электронов в мишень, рис. 1,*б* – 100 попаданий) кажется, что эти вспышки распределены более или менее равномерно по мишени-экрану.

Но со временем начинают появляться намеки на определенную картину (рис. 3,*в* – 3000 попаданий). Возникают ощущения, что вспышки предпочитают появляться в одних местах и избегать другое места экрана (рис. 3,*в*).

На четвертой и пятой экспозициях (рис. 1,*г* и рис. 1,*д* – 20000 и 70000 попаданий электронов в экран соответственно), полученных при значительном увеличении «времени экспонирования» ощущения, превращаются в экспериментальный факт – на мишени появляется чередующий ряд параллельных полос, подтверждающих интерференцию электронов.

Является ли этот эксперимент технологией, которая позволяет создавать бумажные купюры с высочайшим уровнем защиты? Нет, это всего лишь физический эксперимент, делающий намек на то, в какую сторону нужно развивать технологию. Цена вышеописанного эксперимента чрезвычайно высока и многократно превышает стоимость изготовления купюры наиболее часто употребляемого номинала. Технология изготовления бумажной купюры с высоким уровнем защиты должна быть в тысячи раз дешевле и составлять доли процента от номинала купюры.

Результаты и обсуждение

А теперь перейдем к описанию другого физического эксперимента [3], который действительно открывает в перспективе путь к созданию новой технологии.

Схема его проведения чрезвычайно проста. В бумаге электроразрядным способом пробиваются небольшие отверстия. Затем эти образцы сканируются на просвет на обычном сканере и сохраняются в базе данных. Полученные картинки обсчитываются на компьютере, и вычисляется ряд параметров в расположении пятен.

В большинстве экспериментальных работ в этой области [4] описываются особенности физических процессов в межэлектродном промежутке, внимание исследователей на информационные возможности этих технологий [5] ранее практически не обращалось.

Немаловажный фактор, позволяющий легко сканировать места электрического пробоя на бумаге, – это то, что на площадь для пробоя наносился круг черного цвета лазерным принтером. Внутри этого круга предположительно при создании документа строгой отчетности наносится также индивидуальный цифровой код (рис. 2). При отсутствии индивидуального цифрового кода невозможно построить базу данных из-за серьезных математических трудностей, возникающих при использовании распознания образов. База данных строится на совмещении цифровой и волновой (индивидуальной матрицы) информации. По цифровому коду находится документ в базе данных, а по индивидуальной матрице проверяется, поддельный документ или нет. Типичный документ, содержащий индивидуальный цифровой код и индивидуальную картинку, полученную с помощью электрических пробоев, приведен на рис. 2.

Рис. 2. Документ строгой отчетности с защитой индивидуального цифрового кода электроразрядной технологией

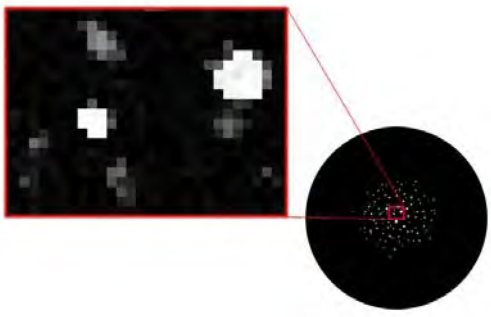

Рис. 3. Типичная индивидуальная картинка, экспериментально полученная с применением электроразрядной технологии

На рис. 3 приведена типичная индивидуальная картинка *(без цифрового кода)*, из которой следует не только индивидуальность картинки в целом, но и неповторимость каждого из пятен.

Эта типичная картина (рис. 3) мало отличается от рис. 1,*б*. Отличие в том, что эксперимент предельно прост и технологичен, а результаты реализуются не на экране дисплея, а непосредственно на бумажном носителе.

Теоретически вероятность повтора матрицы при индивидуальной обработке оценивалась в 10^{-400}. С позиции уровня защиты эта величина равна бесконечности. Технологический аспект проблемы показывает, что бесконечность и 10^{-400} – слабо отличимые понятия.

Нуждается ли эта технология в разработке нового специализированного оборудования? Как ни странно, но нет. При наличии серийного высоковольтного трансформатора на 20–25 кВ и дополнительных общедоступных электротехнических деталей, за 15 минут собирается оборудование для изготовления идентификационной метки. Затраты на разработку и изготовление такого оборудования ничтожны по сравнению с возможными финансовыми потерями [6]

При изготовлении денежных купюр важным признаком можно считать совмещение перфораций, полученных электроразрядным способом, с уже известными полиграфическими способами защиты. Для этого перфорации располагают рядом с цифровым кодом денежной купюры или водяным знаком (рис. 4).

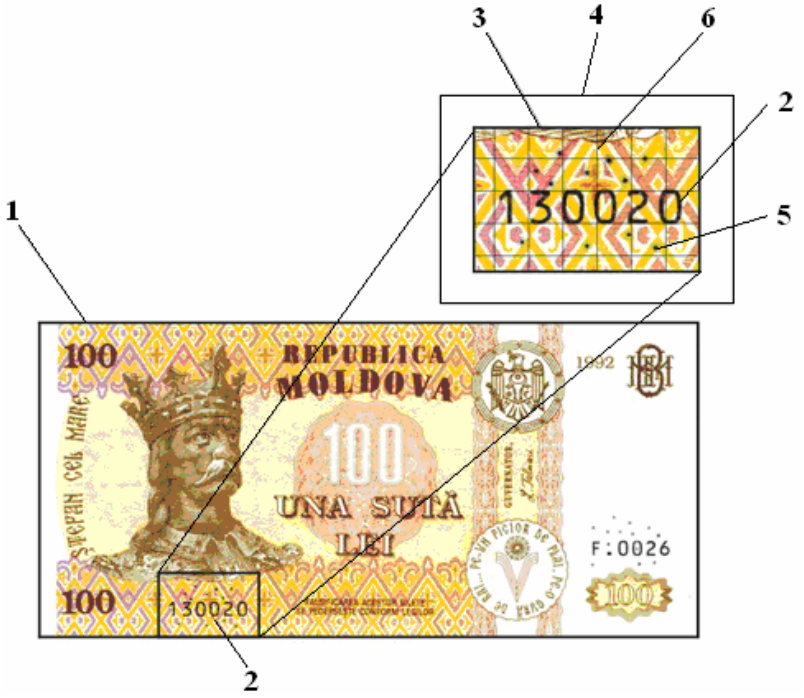

Рис. 4. 100 леев – денежная купюра Республики Молдова: 1 – бумажная основа с водяным знаком, 2 – цифровой код купюры; 3 – информационно-защищенный участок, 4 – декартовая система координат, 5 – перфорации, выполненные электроразрядным способом, 6 – защитный прозрачный слой

Признаков подлинности банкнот достаточно много. Это скрытые радужные полосы; ныряющие металлизированные нити, которые видны на оборотной стороне банкноты в виде блестящих прямоугольников, образующих пунктирную линию, защитные волокна, рельефные изображения, скрытые изображения, водяные знаки, микротекст и т.д. В последнее время (модификации образца 1997 года) Банк России вводит новый идентификационный признак – микроперфорации. Но нам известно, что микроперфорации на 1000- и 5000-рублевых банкнотах России сделаны не электроразрядным способом, а чисто механически, с помощью игл. На 1000-рублевой купюре Банка России с помощью микроперфораций наносится номинал купюры – цифры 1000. Электроразрядным способом это сделать невозможно. Как правило, это считается технологическим недостатком. Но в области идентификации такой «недостаток» становится технологическим преимуществом. На всех банкнотах России – один и тот же рисунок, изображающий номинал купюры. В электроразрядной технологии это случайный неповторимый набор перфораций. Поэтому о такой технологии можно говорить в открытой печати. Технологию легко реализовать, а повторить дважды невозможно. При рассмотрении

банкноты России против источника света на ней видно обозначение номинала, сформированное микроотверстиями (рис. 5). В случае применения электроразрядного процесса – это случайный набор перфораций. Проверка на подлинность осуществляется путем сравнения набора случайно разбросанных перфораций с аналогичным набором, хранящимся в базе данных.

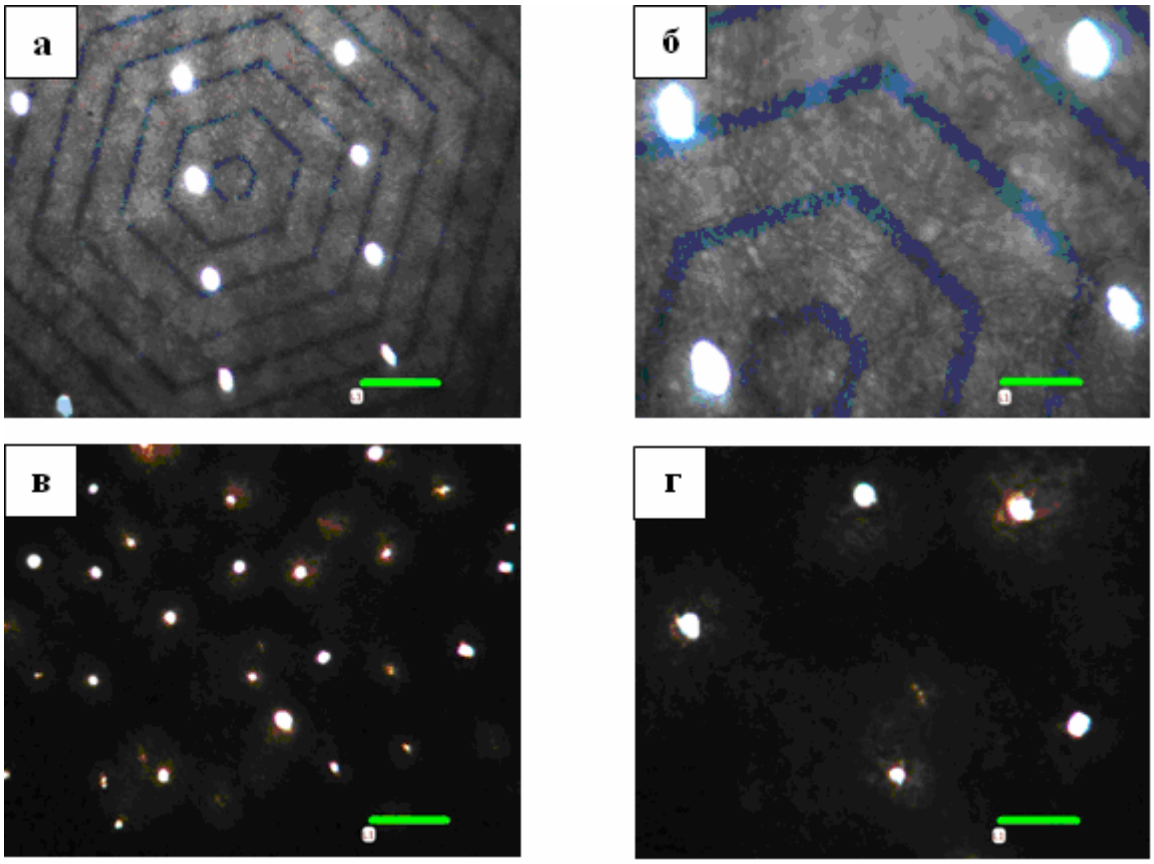

Рис. 5. Перфорации на банкноте Российской Федерации номиналом в 1000 рублей (а и б) – видна полиграфическая защита в виде шестигранников. Электроразрядные перфорации (в и г). Размер реперного отрезка в 200 микрон (а и в) и в 500 микрон (б и г)

Часть вторая

В работах [3, 6] при анализе площадей использовался подход прямого подсчета пикселей, входящих в кольцо. Такой подход обладает рядом недостатков. Он позволяет считать только суммарную площадь пятен по кольцам и выявлять стохастические волны, но не дает возможности подсчитывать количество и координаты отдельных пятен, что резко сужает возможность исследования стохастичности процесса. Поэтому закономерен переход к программе, с помощью которой можно рассчитывать статистические характеристики каждого отдельного пятна. Для этого обычно применяется следующая последовательность шагов. Первое – бинаризация изображения по одному из известных методов (У. Ниблэк, Н. Отс, Дж. Бернсен и др. [7]) с целью получения изображения с резкими границами пятен (рис. 6). При бинаризации изображения яркость каждого пикселя сравнивается с пороговым значением яркости. Если значение яркости пикселя выше значения яркости порога, то на бинарном изображении соответствующий пиксель будет «белым» или «черным» в противном случае.

Второе – выделение отдельных пятен на изображении при помощи рекурсивного или итеративного алгоритмов. Суть итеративного метода заключается в последовательном сканировании изображения с классификацией белых пикселей по принципу связности. В результате получается матрица, в которой все пиксели каждого пятна обозначены каким-то числом, которое можно также считать порядковым номером пятна (рис. 7).

Третье – расчет статистических характеристик отдельного пятна площади, координат центра, дисперсии, скоса и эксцесса. Исходное изображение и набор рассчитанных характеристик можно сохранить в базе данных для применения в работе системы защиты.

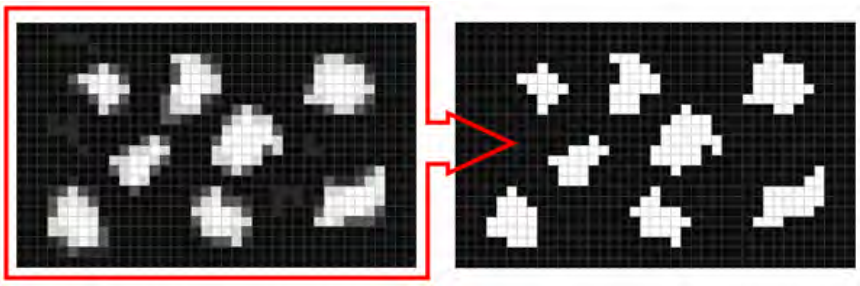

Рис. 6. Изображение до и после бинаризации

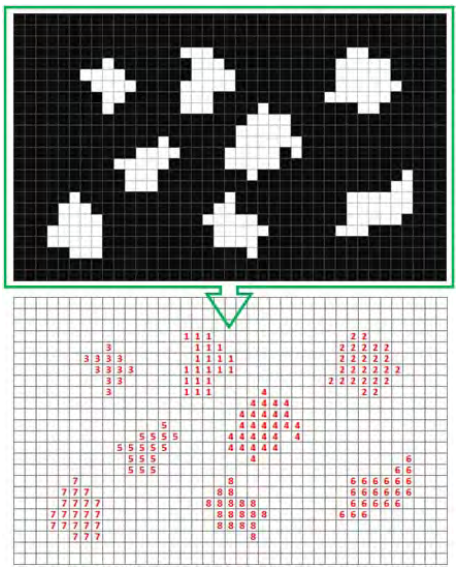

Рис. 7. Выделение отдельных пятен

Заключение

Предложена принципиально новая технология защиты бумажных купюр и документов с высоким уровнем защиты.

ЛИТЕРАТУРА

1. *Wiesner S.* Conjugate coding // Sigact News. 1983. Vol. 15. № 1. P. 78–88.
2. *Tonomura A., Endo J., Mamsuda T., Kawasaki T., and Exawa H.* Demonstration of single – electron buildup of an interference pattern. Amer. J. Phys. Vol. 57. pp. 117-120. 1989.
3. *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.
4. *Ретер Г.* Электронные лавины и пробой в газах. Перевод с английского под редакцией В.С. Комелькова. М.: Мир, 1968. 390 с.
5. *Шкилев В.Д. и др.* Патент Республики Молдова № 3389 «Способ идентификации объектов». MD-BOPI №8, 2007, с. 51.
6. *Шкилев В.Д., Адамчук А.Н.* Новые информационные технологии при изготовлении бумажных купюр с квантовым уровнем защиты. International Conference «Information and Communication Technologies 2009 ICT Chisinau, Republic of Moldova, p. 186–188.
7. *Федоров А.* Бинаризация черно-белых изображений: состояние и перспективы развития. http://iu5.bmstu.ru/~philippovicha/ITS/IST4b/ITS4/Fyodorov.htm.

Поступила 21.10.09
После переработки 28.01.10

Summary

New information technologies for manufacturing of paper banknotes with a high level of protection are presented. The method of documents database formation on the basis of association of the wave and digital information is offered**.**