Доклады Национальной академии наук Беларуси

2016 **сентябрь–октябрь** **Том 60 № 5**

ИНФОРМАТИКА

УДК 343.98

А. А. БОРИСКЕВИЧ

МЕТОД ЗАЩИТЫ ЦЕННЫХ ДОКУМЕНТОВ ОТ ПОДДЕЛОК НА ОСНОВЕ ВИЗУАЛЬНОЙ СХЕМЫ РАЗДЕЛЕНИЯ СЕКРЕТА

(Представлено академиком В. А. Лабуновым)

Белорусский государственный университет информатики и радиоэлектроники, Минск, Беларусь
anbor@bsuir.by

Разработан метод защиты ценных документов от подделок, основанный на визуальном зашифровывании высокоразрешающего изображения с идентифицирующей информацией (общий секрет) и его расшифровывании посредством физического процесса наложения щумоподобных теневых изображений (частичные секреты) без использования компьютера и криптографических ключей шифрования. Исследованы криптографические свойства теневых изображений. Представлены результаты компьютерного моделирования.

Ключевые слова: ценные документы, визуальное шифрование, схемы разделения секрета, кодовая таблица, теневое изображение, общий и частичный секреты.

A. A. BORISKEVICH

A PROTECTION METHOD OF VALUABLE DOCUMENTS AGAINST FORGERY BASED ON THE VISUAL SECRET SHARING SCHEME

Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus
anbor@bsuir.by

A method for protecting valuable documents against forgery based on the visual ciphering of a high-resolution image (shared secret) and its deciphering through the physical process of imposing noise-like shadow images without using a computer and cryptographic encryption keys is proposed. The cryptographic properties of shadow images are studied. The computer modeling results are presented.

Keywords: valuable documents, visual encryption, sharing secret scheme, code table, shadow image, general and partial secrets.

Введение. В настоящее время защищенность полиграфической продукции (банкноты, ценные бумаги, документы строгой отчетности и др.) обеспечивается применением полиграфических, голографических, информационных, микропроцессорных и иных защитных элементов, предотвращающих подделку данной продукции [1; 2]. Массовое распространение подделок, выполненных на компьютерной технике, подымает вопрос разработки новых защитных элементов. Независимо от своего характера каждый из элементов защиты должен отвечать ряду базовых требований, реализация которых обязательна и обеспечивает минимально достаточный уровень защищенности от подделки [2]: воспроизводимость защитного элемента в полном объеме, устойчивость во времени при воздействии на документ обычных эксплуатационных факторов и при несанкционированных вмешательствах, нераскрываемость (невоспроизводимость) элемента иными средствами; несохраняемость элементом защиты некоторых своих свойств в случае воздействия на документ с целью его частичной подделки, независимость защитных элементов друг от друга (в противном случае раскрытие одного элемента защиты вызовет раскрытие и всей системы) и контролируемость элемента защиты (возможность установления подлинности).

Актуальной проблемой является разработка таких защитных технологий, которые удовлетворяют повышенным требованиям безопасности и удобства пользования конечным пользователям (дружественность и простота при пользовании, т. е. минимальность конкретных интеллектуальных усилий и максимальная скорость достижения положительного результата при пользовании) и обеспечивают уникальность, постоянство, устойчивость к подделке и компактность.

Одним из эффективных решений данной проблемы является использование визуальной схемы разделения секрета (ВСРС(k, n)) [3–6], в которой идентифицирующая информация (общий секрет) шифруется с помощью n теневых шумоподобных изображений (частичных секретов) и восстанавливается с помощью k и больше теневых изображений (ТИ). Основными преимуществами ВСРС являются регулярность (одинаковые действия производятся для каждого исходного пикселя), независимость (каждый исходный пиксель шифруется независимо от других) и простота (возможность визуального расшифровывания посредством физического процесса наложения шумоподобных ТИ без использования компьютера и криптографических ключей шифрования).

Наиболее практичной схемой ВСРС для защиты ценных документов является схема ВСРС ($k = 2$ из $n = 2$) с $m = 2$ (число пикселов в кодируемом блоке) [3]. Однако при использовании данной схемы увеличиваются размеры ТИ и восстановленного секретного изображения по сравнению с исходным секретным изображением в горизонтальном направлении в 2 раза. Схема ВСРС (2, 2) с $m = 4$ не нарушает соотношение сторон восстановленного изображения, но увеличивает размеры ТИ и восстановленного секретного изображения в горизонтальном и вертикальном направлениях в 2 раза. Кроме того, ТИ, наносимые на ценные документы, должны иметь разрешение, обеспечивающее надежную защиту от ксерокопирования.

В настоящем сообщении представлен новый метод визуального шифрования секретного изображения, который является эффективной основой для построения систем защиты ценных документов от подделок.

Метод визуального шифрования изображения с идентифицирующей информацией. Для увеличения криптографической безопасности визуального шифрования секретных изображений предлагается метод (рис. 1), основанный на формировании высокоразрешающего изображения с идентифицирующей информацией (ВИИИ), выборе оптимальных параметров элементов кодовой таблицы по критериям визульного шифрования (равенство вероятностей p_r выбора строк (r) кодовой таблицы, равенство вероятностей p_{BW} появления черных B и белых W пикселов кодового блока, равенство вероятностей p_{CB} использования кодовых блоков (CB)) и качества ТИ и восстановленного ВИИИ (энтропия, коэффициент межпиксельной корреляции, контраст, линейные размеры).

Для предотвращения угрозы копирования перед визуальным шифрованием разработана процедура формирования ВИИИ размером M × N, основанная на вычислении количества пикселей

Рис. 1. Блок-схема метода защиты ценных документов от подделок на основе ВСРС (2, 2)

ВИИИ по горизонтали и по вертикали в зависимости от требуемого размера распечатки цифрового ВИИИ и ее разрешения в точках на дюйм (.dpi, .dot per inch), превышающего заданный пороговый уровень, преобразовании цветного (или полутонового) изображения в бинарное и иерархическом кодировании ВИИИ с помощью кодовой таблицы с кодовыми блоками различных размеров при сохранении его размера.

Псевдослучайное визуальное кодирование ВИИИ осуществляется с помощью кодовой таблицы на основе ВСРС (2, 2) с использованием кодовых блоков с двумя пикселами ($m = 2$) (табл. 1).

Т а б л и ц а 1. **Кодовая таблица на основе ВСРС (2, 2) с кодовыми блоками размером 1$x$$m$ ($m = 2$)**

Пара пикселов ВИИИ размером M × N	Бинарная псевдослучайная последовательность длиной M × N / 2	Пара пикселов ТИ 1 размером M × N ($m = 2$)	Пара пикселов ТИ 2 размером M × N ($m = 2$)	Пара пикселов восстановленного ВИИИ размером M × N
00	0	10	10	10
Чет(01, 10)	1	01	01	01
Нечет(01, 10)	0	10	01	11
11	1	01	10	11

Для обеспечения безопасности ТИ предложена процедура, основанная на увеличении количества одновременно кодируемых пикселов ВИИИ до двух, равное количеству пикселов кодового блока, при сохранении размеров восстановления ВИИИ, т. е. без расширения его размеров, и вычислении количества появлений каждой пары пикселов 01 и 10 в ВИИИ.

Предложенная кодовая таблица характеризуется множеством параметров ($k = 2$, $n = 2$, $m = 2$, $\alpha = 1/2^{k-1}$, p_r, p_{CB}, p_{BW}) (табл. 1). Параметр α определяет контраст восстановленного ВИИИ. Предложенная кодовая таблица позволяет обеспечить максимальный уровень безопасности информации в понятиях трех критериев качества визуального шифрования: равенство вероятностей p_r выбора строк кодовой таблицы, содержащих различные кодовые блоки ТИ для шифрования пары пикселов ВИИИ, равенство вероятностей p_{BW} появления черных и белых пикселов кодового блока и равенство вероятностей p_{CB} использования кодовых блоков. Максимальный уровень безопасности информации по первому критерию достигается посредством формирования псевдослучайной контентно-зависимой бинарной матрицы с одинаковыми вероятностями появления ее слабокоррелированных единиц и нулей. Достижение максимального уровня безопасности информации по второму и третьему критериям означает, что большая часть одинаковых кодовых блоков с равными вероятностями p_{BW} появления черных и белых пикселов в каждом кодовом блоке используется как при кодировании черной пары пикселов, так и при кодировании белой пары пикселов ВИИИ, что уменьшает возможность предсказания злоумышленниками секретного бита при анализе группы пикселов ТИ и не позволяет извлечь следы ВИИИ из ТИ.

Для генерациии псевдослучайной последовательности с размером M × N / 2 использованы генераторы псевдослучайных последовательностей (ГПСП) (генераторы, основанные на регистрах сдвига с линейной обратной связью [7], блочных и поточных алгоритмах шифрования (AES (Advanced Encryption Standard), RC4) [7–10] и свойствах детерминированного хаоса [11]) с требуемой длинной секретного ключа (>128 бит).

Из табл. 1 видно, что при 00 или четном количестве появления одной из пар (01, 10) псевдослучайно выбирается одна из первых двух строк кодовой таблицы, а при 11 или нечетном количестве появления одной из пар (01, 10) псевдослучайно выбирается одна из последних двух строк кодовой таблицы.

Восстановление ВИИИ (табл. 1) осуществляется посредством физического наложения прозрачного носителя с ТИ1 на ТИ2, нанесенное на ценный документ, т. е. использования логической операции ИЛИ (OR). Каждая восстановленная пара ВИИИ будет черной или белой, если наложение приводит к паре пикселов (11) или к парам пикселов 01 и 10 соответственно.

Численные результаты моделирования. На рис. 2 представлены результаты визуального шифрования секретных изображений «личная подпись» и QR(Quick Response)-кода на основе ВСРС (2, 2) с $m = 2$ без расширения (табл. 1).

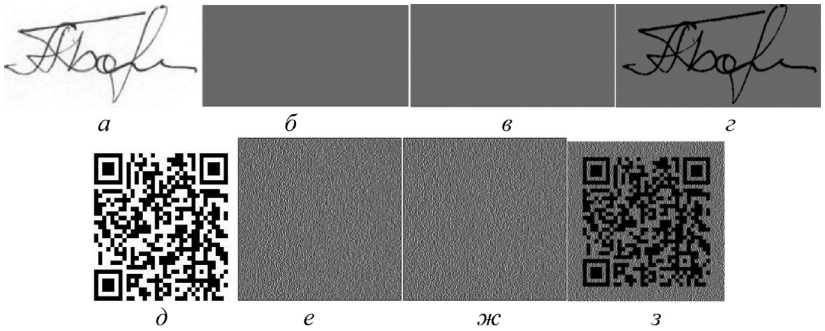

Рис. 2. Визуальное шифрование ВИИИ на основе ВСРС (2, 2) с $m = 2$ без расширения: *а*, *д* – секретные изображения; *б*, *е* – теневые изображения 1; *в*, *ж* – теневые изображения 2; *г*, *з* – восстановленные секретные изображения (операция OR)

Для оценки защищенности сформированных ТИ (частичных секретов) использованы коэффициент $r_{x,y}^{(l)}$ межпиксельной (вертикальной, диагональной и горизонтальной) корреляции [12] и информационная энтропия H бинарных ТИ

$$r_{x,y}^{(l)} = \frac{\mathrm{cov}_l(x,y)}{\sqrt{D_l(x)}\sqrt{D_l(y)}},$$

$$H = -p\log_2 p - (1-p)\log_2(1-p),$$

где $\mathrm{cov}_l(x,y) = N^{-1}\sum_{i=1}^{N}(x_{l,i} - E_l(x))(y_{l,i} - E_l(y))$ – среднее значение ковариации пар l-го типа значений соседних пикселов $x_{l,i}$ и $y_{l,i}$ ТИ; $l = \{V, H, D\}$ – тип вертикальных V, горизонтальных H и диагональных D пар соседних пикселов ТИ; $E_l(x) = N^{-1}\sum_{i=1}^{N} x_{l,i}$ и $D_l(x) = N^{-1}\sum_{i=1}^{N}(x_{l,i} - E_l(x))^2$ – среднее значение и дисперсия значений пикселов $x_{l,i}$ ТИ для пар l-го типа; i и N – индекс и количество пар соседних пикселов, случайно выбранных из ТИ и равное 1000; p и $(1 - p)$ – вероятности появления значений черных и белых пикселов ТИ соответственно.

Из табл. 2 видно, что ВСРС (2, 2) с парой пикселов ($m = 2$) без расширения в 6,25 и 2,0 раза безопаснее, чем ВСРС (2, 2) с парой пикселов ($m = 2$) и четырьмя пикселами ($m = 4$) с расширением соответственно в понятиях коэффициента межпиксельной автокорреляции $r_{x,y}^{(l)}$ теневого изображения независимо от типа визуального шифруемого секретного изображения («личная подпись» и QR-кода).

Т а б л и ц а 2. **Оценка эффективности визуального шифрования секретных изображений на основе ВСРС (2, 2)**

Метрики качества ТИ	Личная подпись			QR-код		
	$m = 2$		$m = 4$	$m = 2$		$m = 4$
	расш.	нерасш.	расш.	расш.	нерасш.	расш.
H_S	1,000	1,000	0,9999	1,0000	1,0000	0,9999
$r_{x,y}^{(l)}$	0,4985	0,0769	0,1639	0,5038	0,0790	0,1619

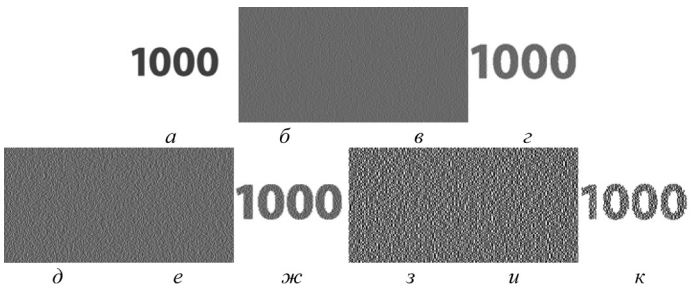

Рис. 3. Визуальное шифрование ВИИИ на основе ВСРС (2, 2) с $m = 2$ без расширения с различными кодовыми блоками формирования ВИИИ: *а* – исходное ВИИИ; *б*, *в*, *д* – теневые изображения 1; *в*, *е*, *к* – теневые изображения 2; *г*, *ж*, *л* – восстановленные ВИИИ с помощью операции OR

На рис. 3 представлены результаты визуального шифрования ВИИИ «1000» размером 20 × 20 мм с разрешением 2500 точек на дюйм на основе ВСРС (2, 2) с m = 2 без расширения (табл. 1) и иерархического кодирования с использованием детерминированной кодовой таблицы с кодовыми блоками размером 2 × 2, 4 × 4 и 16 × 16.

Заключение. Разработан метод защиты ценных документов от подделок, основанный на процедуре формирования высокоразрешающего изображения с идентифицируемой информацией с требуемым разрешением и размером, его визуальном шифровании в виде двух шумоподобных теневых изображений, одно из которых наносится на ценный документ, и визуализации изображения с идентифицируемой информацией посредством другого шумоподобного теневого изображения без использования компьютера и криптографических ключей шифрования. Установлено, что разработанный метод обеспечивает безопасность информации теневых изображений в понятиях следующих критериев визуального шифрования: количество пикселов на дюйм (2540 точек на дюйм), пространство секретных ключей ($>2^{128}$), одинаковые вероятности появления черных и белых пикселов кодового блока, использования кодовых блоков и выбора строки с кодовыми блоками кодовой таблицы, коэффициент межпиксельной корреляции ТИ (0,08) и информационная энтропия (1,0).

Список использованной литературы

1. Технологии защиты денежных знаков и ценных бумаг / В. В. Трухачев, М. Б. Сергеев. – СПб.: ГУАП, 2012. – 110 с.

2. *Бочарова, О. С.* Критерии защищенности документов от подделки и криминалистические требования к элементам и средствам защиты от подделки бланков ценных бумаг и документов с определенной степенью защиты / О. С. Бочарова // Вестн. Полоцкого гос. ун-та. Сер. D. Экономические и юридические науки. – 2015. – № 5. – С. 167–170.

3. *Naor, M.* Visual Cryptography advances in cryptology / M. Naor, A. Shamir // Eurocrypt. – 1995. – P. 1–12.

4. On the security of a copyright protection scheme based on visual cryptography / T.-H. Chen [et al.] – 2009. – N 31. – P. 1–5.

5. *Pal, J. K.* A (2,N) visual cryptography technique for banking applications/ J. K. Pal, J. K. Mandal, K. Dasgupta // International Journal of Network Security & Its Applications (IJNSA). – 2010. – Vol. 2, N 4. – P. 118–127.

6. *Cimato, S.* Visual Cryptography and Secret Image Sharing / S. Cimato, Ching-Nung Yang. – CRC Press, Taylor & Francis Group, 2011. – 545 p.

7. *Фергюсон, Н.* Практическая криптография / Н. Фергюсон, Б. Шнайер. – М.: Изд. Вильямс, 2005. – 416 с.

8. *Зензин, О. С.* Стандарт криптографической защиты – AES. Конечные поля / О. С. Зензин, М. А. Иванов; под ред. М. А. Иванова. – М.: КУДИЦ–ОБРАЗ, 2002. – 176 с.

9. *Панасенко, С. П.* Алгоритмы шифрования. Специальный справочник / С. П. Панасенко. – БХВ–Петербург, 2009. – 576 с.

10. *Singhal, N.* Comparative Analysis of AES and RC4 Algorithms for Better Utilization / N. Singhal, J. P. S. Raina // International Journal of Computer Trends and Technology – July to Aug Issue. – 2011. – P. 177–181.

11. *Kocarev, L.* Chaos–Based Cryptography / L. Kocarev, S. Lian // Theory, Algorithms and Applications. – Springer, 2011. – 395 p.

12. *Борискевич, А. А.* Методология выбора базисных вейвлет-функций на основе статистических и корреляционных характеристик изображений / А. А. Борискевич // Докл. БГУИР. – 2010. – № 5(51). – С. 31–39.

Поступило в редакцию 29.06.2016