

Научная статья

УДК 004.056.52

DOI:10.31854/1813-324X-2023-9-5-121-129



Экспериментальное исследование метода защиты от атаки клонирования бумажных сертификатов

✉ Дмитрий Алексеевич Флакман, flxdima4951@gmail.com

ООО «Научно-производственное предприятие Новые Технологии Телекоммуникаций», Санкт-Петербург, 195256, Российская Федерация

Аннотация: В работе экспериментально исследуется метод защиты бумажных сертификатов от атаки клонирования, ранее теоретически описанный в одной из работ автора. Предлагаемый метод основывается на использовании цифровых водяных знаков. Для защиты от атаки клонирования производится анализ уровня шумов, возникающих при сканировании и печати цифровых водяных знаков. В работе рассмотрены предложенные ранее алгоритмы вложения цифровых водяных знаков в изображение и последующего их извлечения, а также описывается метод выявления атаки клонирования. Приводятся результаты проведенного экспериментального вычисления вероятностей ошибок первого и второго рода для предлагаемой системы цифровых водяных знаков, которые, в основном, совпали с полученными ранее теоретическими расчетами.

Ключевые слова: цифровые водяные знаки, клонирование, сертификаты продукции, вероятности пропуска и ложной тревоги факта клонирования

Благодарности: Автор выражает благодарность профессору В.И. Коржику за постановку задачи и полезные обсуждения основных результатов работы.

Ссылка для цитирования: Флакман Д.А. Экспериментальное исследование метода защиты от атаки клонирования бумажных сертификатов // Труды учебных заведений связи. 2023. Т. 9. № 5. С. 121–129. DOI:10.31854/1813-324X-2023-9-5-121-129

Experimental Investigation of Protection Method for Detection of Cloning Attack on Paper Certificates

✉ Dmitriy Flaksman, flxdima4951@gmail.com

Research and Production Enterprise “Novye Tekhnologii Telekommunikatsii”, Ltd, St. Petersburg, 195256, Russian Federation

Abstract: A method of paper certificate protection against a cloning attack is investigated, that was proposed recently theoretically in a paper of the same author. This method is based on the use of digital watermarks. In order to extend watermark approach to a protection against cloning attacks, it has been suggested to execute estimation of the noise power which appear during the image scanning and printing. Algorithms of embedding and extraction of watermarks out of the images are presented along with a method of detecting of the cloning attack after scanning and printing by an attacker. Numerical results of the experiments for the error probabilities of a cloning missing and a false alarm are also presented and are in agreement with theoretical results obtained before.

Keywords: digital watermarks, cloning, certificates, the missing and false alarm probabilities

Acknowledgements: *The author expresses gratitude to Professor V.I. Korzhik for setting the task and useful discussions of the main results of the work.*

For citation: Flaksman D. Experimental Investigation of Protection Method for Detection of Cloning Attack on Paper Certificates. *Proc. of Telecommun. Univ.* 2023;9(5):121–129. DOI:10.31854/1813-324X-2023-9-5-121-129

1. Введение

В современном мире разнообразия рынка товаров и услуг, а также развития и доступности средств и технологий для их подделки, задача защиты авторских прав производителей является первостепенной для большинства компаний. Фальсифицированные банковские документы, счета и другие ценные бумаги – это те атаки злоумышленников, своевременное выявление которых напрямую влияет на успешную деятельность компании. При этом, во многих случаях для того, чтобы осуществлять производство поддельных образцов и документов, мошенникам достаточно иметь в своем распоряжении доступные на сегодняшний день устройства печати и сканирования. Это обстоятельство, в свою очередь, приводит к увеличению на рынке числа фальсификаций бумажных или произведенных из специального пластика сертификатов. В связи с этими обстоятельствами защита изделий, документов и различных товаров от подделок или ложных утверждений уникальных качеств, несомненно, является важной составляющей наиболее актуальных задач в сфере информационной безопасности.

На сегодняшний день распространенным методом борьбы с подобными проблемами является метод бумажных (или пластиковых) сертификатов, подразумевающий использование штрих-кода (например, QR-код или DataMatrix). Тем не менее, указанный метод работает не во всех случаях. Например, если производится «клонирование» сертификата (т. е. сканирование или фотографирование) и затем на основе такого клона создается поддельный, то использование такого сертификата вместе с товаром пониженного качества может остаться не обнаруженным. При этом кажущаяся визуальная подлинность сертификата гарантирует его реализацию по цене оригинала.

С целью повышения надежности сертификатов возможно также использование метода вложения цифровых водяных знаков (ЦВЗ). В этом случае, для установки подлинности будет необходим дополнительный конфиденциальный цифровой ключ, доступный исключительно собственнику продукта [1]. Но, несмотря на свои преимущества, указанный метод не гарантирует защиты изделий от возможного «клонирования» сертификатов.

Еще одним подходом в использовании вложений ЦВЗ для решения указанной проблемы является искажение отдельных блоков информации, включая штрих-коды. Данный метод описан в работе [2]. Другой подход предполагает изменение

фона на специальный текстурный шаблон на основе гауссовского шума, характеристики которого чувствительны к процедуре печати и сканирования [3]. Однако стоит учитывать, что подобные искажения существенно влияют на структуру обрабатываемого объекта.

Метод, предложенный в статье [4], использует анализ различных особенностей изображения в частотной и пространственной областях. Для этого в первом случае используется коррекция изображения, определение набора локальных максимумов для оригинала и его последующее сравнение с набором аналогичных характеристик подделки. Во втором случае, к оригиналу и подделке применяется преобразование для получения изображений определенного вида, в результате которого оценивается равномерность цвета, яркость и расстояния между их частями. Так же для выявления фальсифицированной продукции проводятся исследования применения методов машинного обучения [5]. Однако для эффективной работы нейронных сетей требуется подготовка большого объема исходных обучающих данных.

В настоящей работе исследуется оригинальный метод защиты бумажных сертификатов, который позволяет выявить попытку «клонирования». Рассматриваемый метод основывается на использовании ЦВЗ и на том факте, что любые дополнительные операции над изображением, будь то сканирование, печать или цифровая обработка изображения, неминуемо приведут к увеличению мощности шума в подделываемом злоумышленником сертификате.

Предлагаемый метод подходит как для цветных изображений, так и для изображений в градациях серого, в том числе и для матричных штриховых кодов, таких как QR-код или DataMatrix.

Дальнейшие результаты структурированы следующим образом:

- во втором разделе представлено общее описание работы системы ЦВЗ;
- в третьем разделе рассматривается алгоритм вложения ЦВЗ, использующий в своей основе дискретно-косинусное преобразование и широкополосные сигналы, как это предполагалось ранее в работе [6, 7];
- в четвертом разделе описывается метод устранения геометрических искажений и алгоритм извлечения вложенных данных;
- в пятом разделе рассматривается алгоритм обнаружения атаки клонирования, основанный на оценке шумов изображения;

– в шестом разделе представлены результаты экспериментов, подтверждающих работоспособность предлагаемого метода;
 – в заключении подводятся итоги полученных результатов и предлагаются возможные направления для проведения дальнейшего исследования.

2. Общая схема вложения ЦВЗ и метода клонирования

Рассмотрим общую схему работы предлагаемой системы ЦВЗ (рисунок 1).

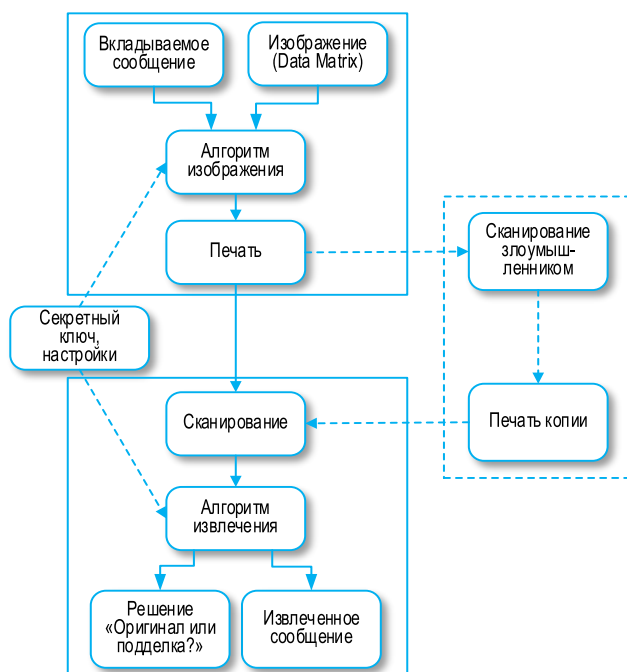


Рис. 1. Общая схема использования системы ЦВЗ и процедуры клонирования

Fig. 1. General Scheme of Using the DW System and Cloning Procedure

На вход алгоритма вложения поступает вкладываемое сообщение, покрывающее изображение, секретный ключ, а также различные второстепенные настройки алгоритма. Размер вкладываемого сообщения зависит от размеров будущей стеганограммы и физического носителя изображения. Например, для изображения 460×460 точек при печати на бумагу в размере 4×4 см можно вложить 128 бит. На выходе алгоритма вложения получается защищенное изображение (стеганограмма), которое распечатывается на физический носитель (бумагу, пластик и т. п.). Распечатанную стеганограмму назовем сертификатом.

Сертификат поступает на вход алгоритма извлечения, однако на вход также может прийти и поддельный сертификат (копия оригинального). Для работы алгоритма извлечения также необходимо знать секретный ключ. Результатом работы алгоритма извлечения является вложенное сообщение, а также решение о наличии факта подделки.

3. Алгоритм вложения

Разберем подробнее алгоритм вложения. Общая схема алгоритма представлена на рисунке 2.

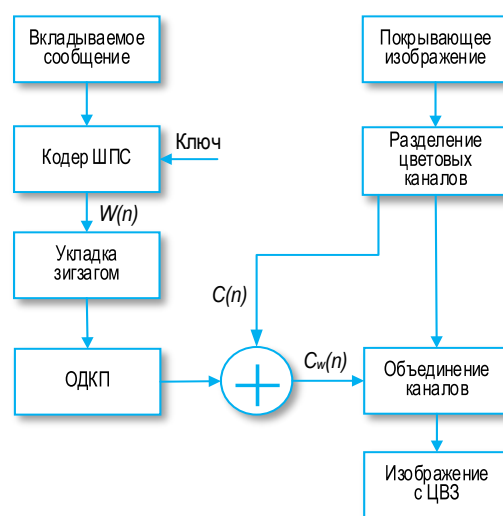


Рис. 2. Блок-схема алгоритма вложения ЦВЗ

Fig. 2. Scheme of DW Embedding

Покрывающим изображением может выступать как цветное, так и изображение в градациях серого. В частности, в этом качестве может выступать двумерный матричный штрихкод, например, DataMatrix (см. рисунок 3). Если защищается цветное изображение, то для вложения будет использоваться только его синий цветовой канал. Покрывающее сообщение обозначим как $C(n)$.

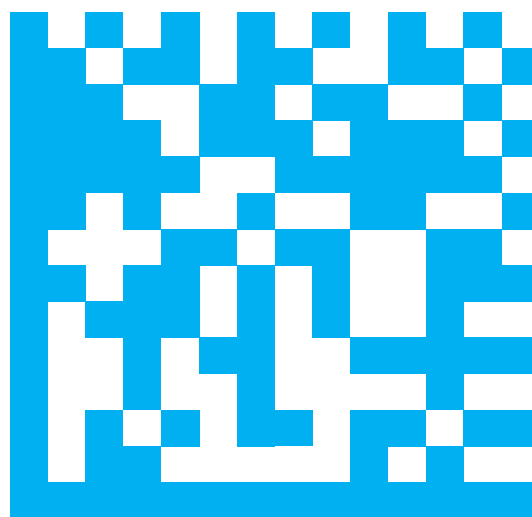


Рис. 3. Изображение DataMatrix кода

Fig. 3. Example of DataMatrix Barcode

Вкладываемое сообщение кодируется с использованием кодера широкополосных сигналов (ШПС). В кодере ШПС используется псевдослучайный сигнал, вырабатываемый на основе секретного ключа с помощью линейного рекуррентного регистра (ЛРР):

$$W^{bi}(n) = \alpha(-1)^{b_i} \pi(n), \quad n = 1, 2, \dots, N_0, \quad (1)$$

где α – глубина вложения; N_0 – длина псевдослучайной последовательности (ПСП), на которой вкладывается один бит информации; $\pi(n)$ – отсчет ПСП (± 1); $b \in (0,1)$ – бит вкладываемого сообщения с индексом i .

Далее полученная последовательность укладывается зигзагом с таким расчетом, чтобы заполнить область «средних частот» дискретно-косинусного преобразования (ДКП). Выбор частотной области ДКП обусловлен тем, что вложение в нее будет наиболее устойчиво к искажениям. К полученной матрице применяется обратное дискретно-косинусное преобразование (ОДКП), в результате которого получается матрица $Cw(n)$. Для получения стеганограммы матрица $Cw(n)$ складывается с покрывающим изображением $C(n)$.

4. Алгоритм извлечения

Блок-схема алгоритма извлечения ЦВЗ представлена на рисунке 4. На вход алгоритма извлечения поступает отсканированное изображение.



Рис. 4. Блок-схема алгоритма извлечения ЦВЗ

Fig. 4. Scheme of DW Extraction

Для надежного извлечения вложенных данных необходимо максимально точно восстановить размер и ориентацию изображения.

В целях устранения искажений используется перспективное преобразование изображений [8]:

$$\begin{pmatrix} \bar{x}' \\ \bar{y}' \\ w \end{pmatrix} = \begin{pmatrix} t_{11} & t_{12} & t_{13} \\ t_{21} & t_{22} & t_{23} \\ t_{31} & t_{32} & t_{33} \end{pmatrix} \begin{pmatrix} \bar{x} \\ \bar{y} \\ 1 \end{pmatrix}, \quad (2)$$

где x', y' – новые координаты точки; x, y – старые координаты точки; $t^{i,j}$ – коэффициенты матрицы преобразования; w – глубина (масштаб).

Для того, чтобы получить коэффициенты преобразования, можно воспользоваться различными методами. Если изображение представляет собой матричный штрихкод, то можно ориентироваться на его структуру, которая предназначена для автоматического позиционирования. При наличии оригинала для сопоставления положения можно воспользоваться методами компьютерного зрения. В крайнем случае, положение можно выбрать визуально в ручном режиме. Подробнее устранение геометрических искажений рассматривалось в статье [8].

После применения перспективного преобразования, для извлечения вложенных данных необходимо вернуться в частотную область. Далее из области средних частот ДКП зигзагом выбирается последовательность отсчетов, которая отправляется на декодер ШПС. Если есть оригинальное изображение, то можно воспользоваться *информированным* декодером ШПС или же *слепым*, если оригинал отсутствует.

5. Алгоритм обнаружения факта клонирования сертификата

Само по себе верное извлечение ЦВЗ не гарантирует того, что мы извлекаем данные из оригинального сертификата, так как он мог быть скопирован и повторно напечатан. Однако любая дополнительная операция, которая при этом производится над ЦВЗ, неминуемо влечет за собой увеличение уровня шумов, в то время как попытка удаления шумов сканирования с высокой вероятностью приведет к повреждению вложения и невозможности его извлечения.

Значение отсчета проверяемой ЦВЗ, в случае, если не было клонирования, имеет вид:

$$C'_t(n) = C_w(n) + N_{p1}(n) + N_{s1}(n), n = 1, 2..N, \quad (3)$$

где $C_w(n)$ – отчеты оригинального ЦВЗ; $N_{p1}(n)$ – шумы печати; $N_{s1}(n)$ – шумы сканирования; N – длина тестируемой последовательности.

Если клонирование произошло, то необратимо появляются дополнительные шумы:

$$C''_t(n) = C_w(n) + N_{p1}(n) + N_{s2}(n) + N_{p2}(n) + N'_{s1}(n), n = 1, 2..N, \quad (4)$$

где $N_{s2}(n)$ и $N_{p2}(n)$ – шумы сканирования и печати злоумышленником; $N'_{s1}(n)$ – шумы сканирования поддельного сертификата.

Для проверки подлинности легитимный пользователь рассчитывает величину:

$$\lambda(n) = C_t(n) - C_w(n), n = 1, 2..N, \quad (5)$$

где $C_t(n)$ – отсчеты проверяемого ЦВЗ.

После этого он рассчитывает нормированную мощность шумов:

$$\Omega = \frac{1}{N} \sum_{n=1}^N \lambda^2(n), \quad (6)$$

где N – длина тестируемой области.

При этом, зная параметры оборудования, на котором производился оригинальный сертификат, можно попытаться подобрать порог для мощности шумов, тогда решение о наличии клонирования будет приниматься по правилу:

$$\begin{cases} \Omega \geq \Omega_0 \Rightarrow \text{клонирование есть} \\ \Omega < \Omega_0 \Rightarrow \text{клонирования нет} \end{cases}, \quad (7)$$

где Ω_0 – некоторый заранее заданный порог.

При принятии решения могут появиться два вида ошибок: P_m – вероятность пропуска клонирования, когда оно в действительности произошло, но не было обнаружено; P_{fa} – вероятность ложной тревоги, когда клонирования не было, но по правилу принимается решение о его наличии.

Определим полную вероятность ошибки как

$$P_e = \frac{1}{2}(P_m + P_{fa})$$

и будем называть оптимальным порогом такую величину $\Omega = \Omega_0$, которая обеспечивает минимум P_e .

Подробный вывод выражения для вероятности ошибок представлен в статье [6]:

$$P_e \approx \Phi\left(\frac{1}{2\pi} \frac{e^{-x^2/2}}{x}\right), \quad x = \frac{\sqrt{N}}{\sqrt{2}(2r+1)}, \quad (8)$$

где Φ – функция Лапласа; r – это величина, которая показывает, во сколько раз дисперсия шумов у атакующего меньше дисперсии шумов у легального пользователя.

Результаты расчета P_e по (8) для различных значений r и N представлены в таблице 1 и на рисунке 5.

ТАБЛИЦА 1. Теоретическая вероятность ошибки при различных значениях r и N (%)

TABLE 1. Theoretical Error Probability for Different Values of r and N (%)

$r \backslash N$	600	800	1000	1200	1500
1	0	0	0	0	0
2	0,0046	0,00053	0,000065	0,0000079	0,00000036
4	0,52	0,24	0,12	0,058	0,021
8	3,7	2,7	2,1	1,6	1,1
16	11	8,7	7,4	6,5	5,4

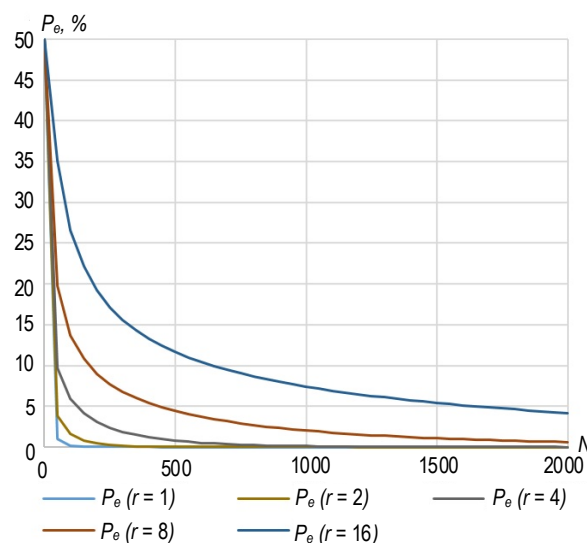


Рис. 5. Зависимость теоретической вероятности ошибки от длины тестируемой области N

Fig 5. Dependency of the Theoretical Error Probability against N

6. Экспериментальные результаты

Перейдем к тестированию системы ЦВЗ. Для начала проверим качество извлечения ЦВЗ. Для теста был сгенерирован двумерный матричный штрихкод типа DataMatrix с размером модуля 22×22 . В нем закодировано текстовое сообщение из 32 знаков (размер изображения на основе кода – 460×460 точек):

DataMatrixxDataMatrixxDataMatrix32

В полученное изображение была произведена серия вложений ЦВЗ с различными параметрами глубины вложения α ($\alpha = 4, 7, 10$) и длины ШПС ($N = 300, 500, 700, 900$).

На первом этапе эксперимента каждый сертификат был напечатан 24 раза на одном листе полуглянцевой бумаги формата А4. Для печати использовался струйный шестичетный фотопринтер Epson L805. Для сканирования использовался сканер Canon Lido 220. Физический размер изображения на бумаге 4×4 см.

После этого было проведено сканирование напечатанных изображений. Для наглядности было выбрано различное разрешение сканирования (200, 300, 400, 600 и 1200 dpi). Результаты извлечения 64, 128 и 256 бит вложенных данных представлены в таблице 2: для наглядности жирным шрифтом выделены результаты экспериментов, в которых средний процент ошибочно извлеченных бит менее 1 %.

По представленным данным можно увидеть, что если требуется вложить 64 бита данных, то можно использовать практически любую совокупность параметров из заданного диапазона, получая приемлемое качество извлечения, при этом разре-

ние сканирования не оказывает значительного влияния на результат. Это обусловлено тем, что все вложение попадает в оптимальную для него область средних частот ДКП.

При использовании 128 бит данных набор подходящих параметров для вложения значительно сужается. Так, глубина вложения, равная 3, уже не кажется подходящей для использования. Так же при разрешении сканирования в 200 dpi наблюдается рост ошибочно извлеченных данных. Это косвенно говорит о том, что при увеличении части спектра ДКП, используемой для вложения, начинает захватываться область верхних частот, которая, в свою очередь, более чувствительна к искажениям.

При попытке использования 256 бит можно заметить, что алгоритм становится наиболее чувствительным к качеству отсканированного изображения, так как само вложение осуществляется в

том числе и в высокие частоты ДКП. В то же время, при значении длины ШПС $N = 900$ происходит превышение максимальной емкости вложения.

На втором этапе эксперимента была имитирована работа злоумышленника. Для этого из отсканированных с разрешением 1200 dpi изображений были подготовлены поддельные сертификаты. При этом для того, чтобы клонированное изображение визуально не отличалось от оригинала, в фоторедакторе была произведена незначительная правка гистограммы распределения цветов. Гистограмма была подогнана под значения оригинальной стеганограммы, которой в реальности у злоумышленника в распоряжении не будет. Каждый поддельный сертификат был распечатан с такими же условиями печати и на такой же бумаге, как и на первом этапе эксперимента.

ТАБЛИЦА 2. Средний процент ошибок при вложении 64/128/256 бит данных

TABLE 2. Average Error Percent in the Case of 64/128/256 Bits Embedding

α	N	Доля ошибочно извлеченных бит, %				
		dpi – разрешение сканирования				
		200	300	400	600	1200
4	300	7,81 / 6,12 / 14,65	7,16 / 3,88 / 4,52	5,54 / 2,83 / 2,24	7,36 / 3,81 / 2,99	7,61 / 3,98 / 2,49
	500	3,19 / 5,11 / 2,73	3,00 / 1,76 / 5,84	3,33 / 1,69 / 3,76	3,13 / 1,56 / 1,07	3,39 / 1,69 / 1,33
	700	1,37 / 10,42 / 28,50	0,52 / 1,46 / 8,01	0,33 / 1,11 / 8,28	0,59 / 0,29 / 3,34	0,85 / 0,42 / 1,56
	900	1,76 / 18,46 / -	0,19 / 1,30 / -	0,19 / 1,01 / -	0,33 / 0,46 / -	0,54 / 0,41 / -
7	300	2,47 / 2,90 / 9,65	2,21 / 1,10 / 1,02	2,35 / 1,17 / 1,16	2,35 / 1,17 / 0,58	3,06 / 1,53 / 0,76
	500	1,30 / 1,82 / 18,47	1,76 / 0,88 / 1,17	1,70 / 0,85 / 1,92	2,08 / 1,04 / 0,55	2,45 / 1,22 / 0,63
	700	0,00 / 3,29 / 22,07	0,00 / 0,10 / 4,07	0,00 / 0,07 / 2,90	0,00 / 0,00 / 0,70	0,00 / 0,00 / 1,03
	900	1,63 / 12,50 / -	0,00 / 0,62 / -	0,00 / 0,00 / -	0,00 / 0,00 / -	0,00 / 0,00 / -
10	300	1,56 / 0,84 / 3,34	1,63 / 0,81 / 0,60	1,63 / 0,81 / 0,80	1,63 / 0,81 / 0,41	1,56 / 0,78 / 0,39
	500	0,39 / 3,78 / 19,47	0,39 / 0,20 / 1,82	0,52 / 0,26 / 1,04	0,72 / 0,36 / 0,18	1,17 / 0,58 / 0,32
	700	0,00 / 3,26 / 21,83	0,00 / 0,00 / 3,60	0,00 / 0,23 / 4,17	0,00 / 0,00 / 0,24	0,00 / 0,00 / 0,59
	900	0,00 / 7,13 / -	0,00 / 0,00 / -	0,00 / 0,16 / -	0,00 / 0,75 / -	0,00 / 0,00 / -

Поддельные сертификаты были так же отсканированы с различным разрешением сканирования. Результаты извлечения вложенных данных представлены в таблице 3: для наглядности жирным шрифтом выделены результаты экспериментов, в которых средний процент ошибочно извлеченных бит менее 2 %.

По полученным результатам можно увидеть, что количество ошибочно извлеченных бит увеличилось. Так, при вложении 256 бит данных на успешное извлечение можно рассчитывать только при определенных наборах параметров. Однако в случае вложения 64 и 128 бит количество ошибок растет не так значительно, поэтому злоумышленник может рассчитывать, что подделка будет успешной. На практике же, небольшой процент ошибочных бит будет исправлен кодом с исправ-

лением ошибок, и подделка успешно пройдет процедуру извлечения.

Для выявления подделки перейдем к измерению шумов. Статистика была получена по результатам представленных выше экспериментов по печати и последующему клонированию сертификата. Измерение шума производилось в частотном представлении только в области средних частот ДКП, примерно соответствующих области вложения.

Для наглядности результаты расчетов по выбору оптимального порога представлены на графиках зависимости вероятностей ошибок P_m и P_{fa} от значения порога Ω_0 . Так как дисперсия шума зависит от разрешения сканирования, то подбор порога удобно осуществлять для каждого разрешения сканирования по отдельности.

ТАБЛИЦА 3. Средний процент ошибок при вложении 64/128/256 бит данных при атаке клонирования
 TABLE 3. Average Error Percent in the Case of 64/128/256 Bits Embedding in Case of a Cloning Attack

α	N	Доля ошибочно извлеченных бит, %				
		dpi – разрешение сканирования				
		200	300	400	600	1200
4	300	14,19 / 18,85 / 28,37	11,85 / 12,11 / 18,06	9,31 / 10,81 / 17,88	9,51 / 8,76 / 14,06	9,38 / 8,29 / 13,14
	500	12,57 / 23,76 / 34,67	5,54 / 11,39 / 23,25	4,69 / 10,06 / 21,26	4,17 / 6,06 / 16,20	3,78 / 6,09 / 15,36
	700	10,94 / 26,33 / 36,42	4,17 / 15,95 / 28,39	2,86 / 12,83 / 25,74	1,76 / 9,77 / 22,64	1,56 / 7,98 / 21,17
	900	13,48 / 29,04 / -	5,47 / 18,43 / -	4,75 / 18,17 / -	1,95 / 13,25 / -	2,51 / 13,35 / -
7	300	3,19 / 4,88 / 15,77	3,39 / 2,51 / 5,88	2,74 / 2,70 / 8,41	3,06 / 2,11 / 5,43	2,86 / 1,80 / 3,55
	500	2,67 / 10,19 / 25,30	2,28 / 2,90 / 13,19	1,83 / 3,97 / 12,44	2,41 / 2,96 / 9,97	2,11 / 1,83 / 7,34
	700	4,82 / 20,02 / 31,96	0,33 / 5,44 / 18,66	0,65 / 5,73 / 18,68	0,07 / 3,78 / 17,78	0,07 / 2,86 / 14,27
	900	7,75 / 25,16 / -	1,37 / 10,81 / -	1,43 / 11,49 / -	0,07 / 5,26 / -	0,14 / 5,97 / -
10	300	1,95 / 2,64 / 11,77	1,95 / 1,11 / 2,86	1,76 / 1,11 / 3,81	1,69 / 0,98 / 1,84	1,63 / 0,81 / 0,97
	500	2,15 / 9,24 / 23,59	0,65 / 5,73 / 16,15	1,11 / 5,70 / 15,36	0,72 / 1,76 / 7,42	0,78 / 0,75 / 6,19
	700	2,60 / 17,42 / 29,84	0,59 / 4,39 / 18,27	0,07 / 5,08 / 17,15	0,00 / 1,56 / 12,61	0,00 / 1,21 / 10,45
	900	5,47 / 22,63 / -	0,26 / 8,58 / -	0,65 / 8,79 / -	1,17 / 9,70 / -	0,21 / 5,61 / -

Графики для значений разрешения 200, 300 и 600 dpi представлены на рисунке 6, соответственно. Статистика для каждого графика посчитана по результатам 288 экспериментов. По графику для разрешения сканирования в 200 dpi можно сделать вывод, что подобрать порог Ω_0 , при котором общая вероятность ошибки будет близка к нулю, невозможно. Так, при значении порога $\Omega_0 = 1270$ общая вероятность $P_e \approx 19\%$. Однако при разрешении сканирования в 300 dpi уже можно выбрать порог $\Omega_0 \approx 1050$, при котором общая вероятность ошибки становится $P_e = 4\%$. Для разрешения сканирования в 600 dpi можно подобрать порог, при котором общая вероятность ошибки будет близка к нулю. Например, при значении порога $\Omega_0 = 950$ общая вероятность $P_e \approx 0\%$.

Из графиков (см. рисунок 6) можно заключить, что при увеличении разрешения сканирования становится проще отделить оригинальные стеганограммы от поддельных. Для наглядности построим график зависимости дисперсии шума от разрешения сканирования (рисунок 7), который показывает, что при малых значениях разрешения сканирования графики сближаются. Это обстоятельство также подтверждает, что при достаточно высоком качестве оборудования у проверяющего (или, как минимум, сопоставимым с оборудованием злоумышленника), появляется надежный метод обнаружения поддельных сертификатов, так как попытка клонировать сертификат неминуемо внесет дополнительный шум, уровень которого не удастся замаскировать.

Расчет дисперсии и порога Ω_0 в представленных выше экспериментах производился для области средних частот, при этом длина тестируемой области N составляла 31740 отсчетов. В теоретических же расчетах значение N не превышало 2000.

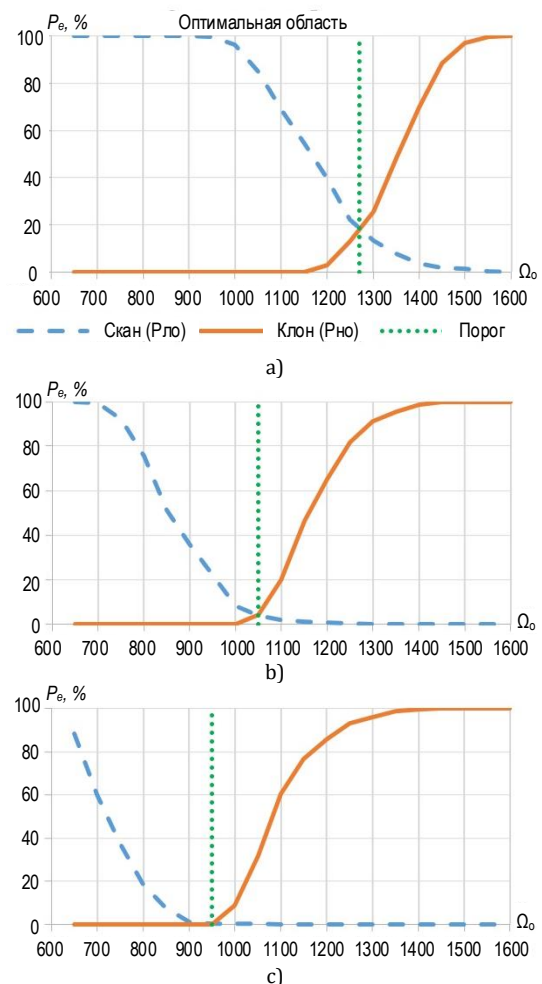


Рис. 6. Зависимость P_m и P_{fa} от величины порога Ω_0 при разрешении сканирования 200 dpi (а), 300 dpi (б) и 600 dpi (с)

Fig. 6. Dependence of P_m and P_{fa} against Ω_0 for Scanning Resolution 200 dpi (a), 300 dpi (b) and 600 dpi (c)

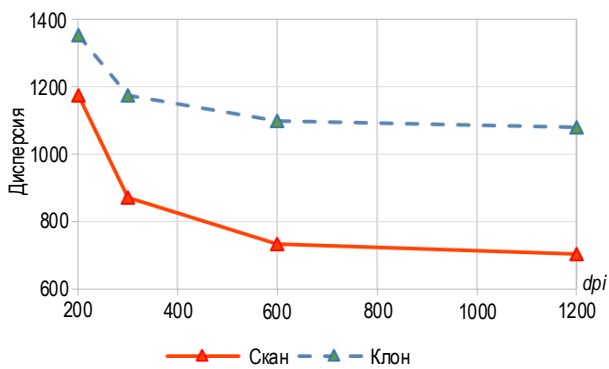


Рис. 7. Зависимость дисперсии шума от разрешения сканирования

Fig. 7. Dependence of the Noise Dispersion on the Scanning Resolution

Для наглядного сравнения экспериментов с проведенными ранее теоретическими исследованиями, проведем расчет полной вероятности ошибки P_e для оптимального порога при различных длинах тестируемой последовательности N (рисунок 8).

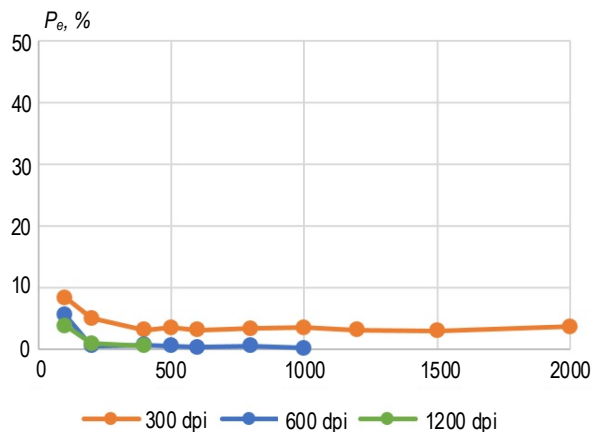


Рис. 8. Экспериментальная зависимость вероятности ошибки от длины тестируемой области N при различных значениях dpi

Fig. 8. Experimental Dependence of the Error Probability on the Length of the Tested Area N at Different dpi Values

Для удобного сравнения теоретических и экспериментальных данных отобразим результаты на одном увеличенном графике (рисунок 9).

Привести значение dpi к теоретическому значению r не представляется возможным, однако можно заметить, что графики для разрешения в 600 и 1200 dpi сопоставимы друг с другом и соотносятся с теоретическими для значений $r = 2$ и $r = 4$. А при разрешении в 300 dpi, график согласуется с теоретическим значением $r \approx 6$. Однако он не стремится к 0 %, а выпрямляется при вероятности ошибки в 4 %. Это обусловлено тем, что при малом dpi второстепенные факторы, влияющие на вероятность ошибки, начинают оказывать заметное влияние.

Список источников

1. Коржик В.И., Анфиногенов С.О., Кочкарёв А.И., Федянин И.А., Жувикин А.Г., Флакман Д.А. Цифровая стеганография и цифровые водяные знаки. Часть 2. Цифровые водяные знаки. СПб: СПбГУТ, 2017. 198 с.

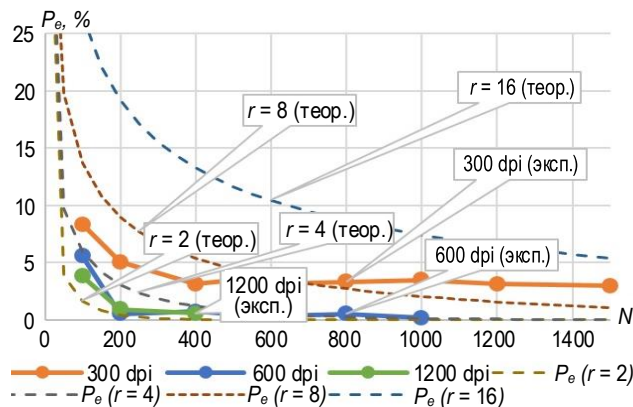


Рис. 9. Сравнение зависимости от N теоретической и экспериментальной вероятности ошибки

Fig. 9. Comparison of Theoretical and Experimental Values of Error Probability against the Length N

Заключение

В настоящей работе был экспериментально исследован метод обнаружения атаки клонирования, предложенный ранее в работе [6]. Проведены эксперименты для оценки его эффективности, включающие печать и последующее сканирование изображений, а также аналогичные операции с поддельными сертификатами. Для указанных экспериментов проведена оценка вероятности пропуска, а также ложного обнаружения атаки клонирования. В результате исследования определено подходящее пороговое значение уровня шумов, которое обеспечивает наименьшую вероятность ошибки.

На основе полученных статистических данных можно сделать вывод о том, что предлагаемый метод может быть успешно применен для защиты от атаки клонирования бумажных сертификатов. Стоит заметить, что для эффективной работы метода требуется определение порога уровня шумов, который, в свою очередь, зависит от параметров используемого оборудования, качества имеющихся материалов и параметров вложения, таких как физический размер сертификата.

Для дальнейшего исследования применимости метода в более широком диапазоне практических задач (например, защита товарных этикеток, печатных документов и т. п.) требуется проведение дополнительных экспериментов по определению оптимального порогового значения уровня шумов для различных параметров системы и условий ее использования, таких как качество бумаги, повреждение или загрязнение сертификата на момент сканирования, а также параметры используемого оборудования, и др.

2. Tkachenko I. Generation and analysis of graphical codes using textured patterns for printed document authentication. D.Sc Thesis. Montpellier: Université de Montpellier, 2015.
3. Nguyen H.P., Delahaies A., Restraint F., Nguyen D.H., Pic M., Morain-Nicolier F. A watermarking technique to secure printed QR codes using a statistical test // Proceedings of the IEEE Global Conference on Signal and Information Processing (GlobalSIP, Montreal, Canada, 14–16 November 2017). IEEE, 2017. PP. 288–292. DOI:10.1109/GlobalSIP.2017.8308650
4. Chen C., Li M., Ferreira A., Huang J., Cai R. A Copy-Proof Scheme Based on the Spectral and Spatial Barcoding Channel Models // IEEE Transactions on Information Forensics and Security. 2019. Vol. 15. PP. 1056–1071. DOI:10.1109/TIFS.2019.2934861
5. Taran O., Bonev S., Voloshynovskiy S. Clonability of Anti-counterfeiting Printable Graphical Codes: A Machine Learning Approach // Proceedings of the ICASSP 2019 – 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP, Brighton, UK, 12–17 May 2019). 2019. PP. 2482–2486. DOI:10.1109/ICASSP.2019.8682967
6. Коржик В.И., Старостин В.С., Флакман Д.А. Разработка метода использования цифровых водяных знаков для защиты от атаки клонирования бумажных сертификатов // Труды учебных заведений связи. 2021. Т. 7. № 2. С. 79–84. DOI:10.31854/1813-324X-2021-7-2-79-84
7. Korzhik V., Starostin V., Yakovlev V., Flaksman D., Bukshin I., Izotov B. Digital Watermarking System for Hard Cover Objects Against Cloning Attacks // Proceedings of the XXth Conference of Open Innovations Association FRUCT (Oulu, Finland, . 27–29 October 2021). IEEE, 2021. PP. 79–85. DOI:10.23919/FRUCT53335.2021.9599967
8. Solomon C., Breckin T. *Fundamentals of digital signal processing*. Wiley, 2011.
9. Korzhik V., Starostin V., Yakovlev V., Flaksman D. Digital Watermark System with an Ability of its Extraction from Hard Copies of Data // Труды учебных заведений связи. 2019. Т. 5. № 3. С. 75–85. DOI:10.31854/1813-324X-2019-5-3-75

References


1. Korzhik V.I., Anfinogenov S.O., Kochkaryov A.I., Fedyanin I.A., Zhuvikin A.G., Flaksman D.A. *Digital steganography and digital watermarks. Part 2. Digital watermarks*. St. Petersburg: The Bonch-Bruевич Saint Petersburg State University of Telecommunications Publ.; 2017. 198 p.
2. Tkachenko I. *Generation and analysis of graphical codes using textured patterns for printed document authentication*. D.Sc Thesis. Montpellier: Université de Montpellier; 2015.
3. Nguyen H.P., Delahaies A., Restraint F., Nguyen D.H., Pic M., Morain-Nicolier F. A watermarking technique to secure printed QR codes using a statistical test. *Proceedings of the IEEE Global Conference on Signal and Information Processing, GlobalSIP, 14–16 November 2017, Montreal, Canada*. IEEE; 2017. p.288–292. DOI:10.1109/GlobalSIP.2017.8308650
4. Chen C., Li M., Ferreira A., Huang J., Cai R. A Copy-Proof Scheme Based on the Spectral and Spatial Barcoding Channel Models. *IEEE Transactions on Information Forensics and Security*. 2019;15:1056–1071. DOI:10.1109/TIFS.2019.2934861
5. Taran O., Bonev S., Voloshynovskiy S. Clonability of Anti-counterfeiting Printable Graphical Codes: A Machine Learning Approach. *Proceedings of the ICASSP 2019 – 2019 IEEE International Conference on Acoustics, Speech and Signal Processing, UK, 12–17 May 2019*. IEEE; 2019. p.2482–2486. DOI:10.1109/ICASSP.2019.8682967
6. Korzhik V., Starostin V., Flaksman D. Elaboration of Digital Watermarking Method for a Protection of Cloning Attack on Paper Certificates. *Proceedings of Telecommun. Univ.* 2021;7(2):79–84. DOI:10.31854/1813-324X-2021-7-2-79-84
7. Korzhik V., Starostin V., Yakovlev V., Flaksman D., Bukshin I., Izotov B. Digital Watermarking System for Hard Cover Objects Against Cloning Attacks. *Proceedings of the XXth Conference of Open Innovations Association FRUCT*. IEEE; 2021. p 79–85. DOI:10.23919/FRUCT53335.2021.9599967
8. Solomon C., Breckin T. *Fundamentals of digital signal processing*. Wiley, 2011.
9. Korzhik V., Flaksman D. Digital Watermark System with an Ability of its Extraction from Hard Copies of Data. *Proceedings of Telecommun. Univ.* 2019;5(3):75–85. 2019. DOI:10.31854/1813-324X-2019-5-3-75

Статья поступила в редакцию 16.05.2023; одобрена после рецензирования 01.07.2023; принята к публикации 02.08.2023.

The article was submitted 16.05.2023; approved after reviewing 01.07.2023; accepted for publication 02.08.2023.

Информация об авторе:

ФЛАКСМАН
Дмитрий Алексеевич

программист ООО «Научно-производственное предприятие Новые Технологии Телекоммуникаций»
 <https://orcid.org/0000-0002-0326-4592>