УДК 004.056.52 DOI:10.31854/1813-324X-2021-7-2-79-84

Разработка метода использования цифровых водяных знаков для защиты от атаки клонирования бумажных сертификатов

В.И. Коржик[1], **В.С. Старостин**[1], **Д.А. Флаксман**[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация
[2]ООО «Научно-производственное предприятие Новые Технологии Телекоммуникаций», Санкт-Петербург, 195256, Российская Федерация
*Адрес для переписки: flxdima4951@gmail.com

Информация о статье
Поступила в редакцию 06.03.2021
Принята к публикации 29.04.2021

Ссылка для цитирования: Коржик В.И., Старостин В.С., Флаксман 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

Аннотация: *Рассматриваются бумажные (или пластиковые) сертификаты различных изделий для защиты оригинальности продуктов и доказательства прав их собственников. Для этого обычно используются линейные или двумерные штрих-коды. Однако этой меры может оказаться недостаточно, особенно для защиты от таких злоумышленных действий, как клонирование и изготовление копий сертификатов и последующего их использования с контрафактной продукцией. В настоящей работе для защиты от такой атаки, которую мы называем «клонированием» сертификатов, предлагается использовать вложение в них цифровых водяных знаков. Приводится алгоритм обнаружения факта такого клонирования и теоретически рассчитываются вероятности ошибки обнаружения и ложной тревоги для данной атаки, в зависимости от параметров системы.*

Ключевые слова: *сертификаты продукции, клонирование, цифровые водяные знаки, вероятности пропуска и ложной тревоги.*

Введение

Защита различных изделий от подделок или фальсификаций их характеристик и действительных производителей является важной задачей, понимаемой в широком смысле информационной безопасности. Для решения этой задачи значительное распространение получил метод бумажных (или пластиковых) сертификатов – попытка использовать штрих-код (например, Data Matrix). Однако не для всех атак злоумышленников защита может оказаться успешной. Так, при выполнении атаки «клонирования сертификата» злоумышленник считывает (фотографирует) сертификат, а затем производит новый поддельный (возможно и измененный) сертификат, который затем прикрепляется к изделию пониженного качества, при этом его содержание говорит о подлинности продукта и, следовательно, требует его повышенной цены. Известен метод повышения надежности сертификатов при помощи вложения в них цифровых водяных знаков (ЦВЗ), подлинность которых подтверждается использованием специального конфиденциального цифрового ключа, который имеется только у собственника этого продукта [1]. Однако такой подход не может защитить от атаки «клонированием сертификатов». В работе [2] предлагается система ЦВЗ для графических QR-кодов, основанная на искажении формы отдельных блоков, входящих в состав кода, однако данный метод требует изменения структуры самого кода.

В настоящей работе предлагается метод защиты сертификатов от подобной атаки, который использует факт увеличения мощности шума в цифровой копии сертификата, вследствие появления дополнительных операций считывания и печати, выполняемых злоумышленником.

Алгоритм обнаружения факта клонирования

Вложение ЦВЗ осуществляется в частотной области, т. е. после применения к покрывающему объекту дискретно-косинусного преобразования (ДКП).

Вложение одного бита ЦВЗ b_i в N_0 частотных (ДКП) коэффициентов матрицы производится по правилу:

$$C_w^{b_i}(n) = C(n) + \delta(-1)^{b_i} \times \pi(n), \quad n = 1,\ 2, \ldots, N_0, \tag{1}$$

где $C(n)$ – отсчет оригинального сообщения; δ – глубина погружения; $b_i \in (0,\ 1)$ – бит ЦВЗ с номером i; $\pi(n)$ – псевдослучайная последовательность для одного бита широкополосного сигнала (ШПС); N_0 – длина ШПС для одного бита.

Приведенная выше операция применяется для всех бит ЦВЗ, при этом величины $C_w^{b_i}(n)$, n = 1, 2, ..., N_0, i = 1, 2, ..., S, необходимо сохранять в памяти для последующего использования. Если всего вкладывается S бит, т. е. i =1, 2, ..., S, то общая «длина» ЦВЗ для покрывающего объекта будет $N = S \times N_0$.

Рассмотрим математическую модель клонирования сертификата. Обозначим отсчеты ЦВЗ в тесте, проводимом легитимным пользователем, через $C_t^i(n)$.

Тогда, если клонирования не было, то:

$$C_t^{\prime,i}(n) = C_w^{b_i}(n) + N_{p1}(n) + N_{s1}(n), \quad n = 1, 2, \ldots,\ N, i = 1, 2, \ldots,\ S, \tag{2}$$

где $N_{p1}(n)$ – шумы при печати цифрового сертификата легитимным пользователем; $N_{s1}(n)$ — шумы, возникающие при сканировании сертификата легитимным пользователем в процессе тестирования.

Если же было выполнено клонирование, то тогда получаем:

$$C_t^{\prime\prime,i}(n) = C_w^{b_i}(n) + N_{p1}(n) + N_{s2}(n) + N_{p2}(n) + N'_{s1}(n), \quad n = 1, 2, \ldots,\ N, i = 1, 2, \ldots,\ S, \tag{3}$$

где $N_{s2}(n)$ — шумы при сканировании сертификата злоумышленником; $N_{p2}(n)$ – шумы при печати клона злоумышленником; $N'_{s1}(n)$ – шумы при сканировании сертификата легитимным пользователем при тестировании.

Сравнивая выражения (2) и (3), видим, что при клонировании добавляются две новые компоненты аддитивного шума N_{p2}, N_{s2}, которые возникают из-за того, что злоумышленник должен дополнительно считать и отпечатать сертификат. В нашей модели все шумы полагаются гауссовскими случайными величинами с нулевыми средними и дисперсиями (Var) одинаковыми для принтера и сканера, но разными для легитимного пользователя и злоумышленника:

$$Var(N_{p1}) = Var(N_{s1}) = Var(N'_{s1}) = \sigma^2,$$

$$Var(N_{s2}) = Var(N_{p2}) = \frac{\sigma^2}{r}, r \geq 1,$$

где r – некоторый коэффициент, который показывает, что злоумышленник может иметь мощность шума в r раз меньше, чем легитимный пользователь (последнее условие дает некоторую фору злоумышленнику по сравнению с легитимным пользователем).

Ранее предполагалось, что легитимный пользователь сохраняет в своем ПК дата-код сертификата с вложением ЦВЗ, т. е. $C_w^{bi}(n)$, n = 1, 2, ..., N. Затем он, получив от сканера результаты тестирования $C_t(n)$, n = 1, 2..N находит величины $\lambda(n) = C_t(n) - C_w^{bi}(n)$, n = 1, 2..N.

Если клонирования не было, то проверяющий вычисляет:

$$\lambda'(n) = C_t'(n) - C_w^{bi}(n) = C_w^{bi}(n) + N_{p1}(n) + N_{s1}(n) - C_w^{bi}(n) = N_{p1}(n) + N_{s1}(n), \quad n = 1, 2, \ldots,\ N. \tag{4}$$

Если же клонирование было, то проверяющий получит:

$$\lambda''(n) = C_t^{\prime\prime,i}(n) - C_w^{bi}(n) = C_w^{bi}(n) + N_{p1}(n) + N_{s2}(n) + N_{p2}(n) + N'_{s1}(n) - C_w^{bi}(n) = N_{p1}(n) + N_{s2}(n) + N_{p2}(n) + N'_{s1}(n). \tag{5}$$

Тогда суммарная мощность шумов будет:

$E\{\lambda_{nc}^2(n)\} = 2\sigma^2$ – для случая без клонирования,

$E\{\lambda_c^2(n)\} = 2\sigma^2 r'$ – для случая с клонированием,

где $r' = \frac{r+1}{r}$; r – это величина, которая показывает во сколько раз дисперсия шумов у атакующего меньше дисперсии шумов у легального пользователя.

Далее измеряется нормированная мощность шумов:

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

Решение о наличии клонирования принимается по правилу:

$$\begin{cases} \Omega \geq \Omega_0 \Rightarrow \text{клонирование есть} \\ \Omega < \Omega_0 \Rightarrow \text{клонирования нет} \end{cases}, \tag{6}$$

где Ω_0 – некоторый заранее заданный порог.

Расчет эффективности обнаружения атаки клонирования

При принятии решения могут появиться два вида ошибок: P_m – вероятность пропуска клонирования, когда оно в действительности было, но это не обнаружено; P_{fa} – вероятность ложной тревоги, когда клонирования не было, но по правилу (6) 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.

Примем гауссовскую аппроксимацию Ω, т. е. когда $\Omega \in N(E\{\Omega\}, Var\{\Omega\})$, что будет верно согласно центральной предельной теореме [3] при больших N. Рассчитаем величины $E\{\Omega\}, Var\{\Omega\}$ без клонирования и с ним.

Без клонирования:

$$E\{\Omega\} = \frac{1}{N}\sum_{n=1}^{N} E\{\lambda_n^2\} = 2\sigma^2,$$
$$Var\{\Omega\} = \frac{1}{N}\sum_{n=1}^{N} Var\{\lambda^2(n)\} = \frac{8}{N}\sigma^4, \quad (7)$$

поскольку λ_n – это гауссовские случайные величины с нулевым средним и дисперсией $2\sigma^2$ и тогда без клонирования $Var\{\lambda^2(n)\} = 8\sigma^4$ [3].

С клонированием:

$$E\{\Omega\} = 2\sigma^2 r',$$
$$Var\{\Omega\} = \frac{8}{N}\sigma^4(r')2. \quad (8)$$

Тогда вероятности ошибок P_m, P_{fa} и P_e будут иметь выражения:

$$P_m = \int_{-\infty}^{\Omega_0} w_\Omega^c(x)\,dx;$$
$$P_{fa} = \int_{\Omega_0}^{\infty} w_\Omega^{nc}(x)\,dx;\ P_e = \frac{1}{2}\left(P_m + P_{fa}\right). \quad (9)$$

Эти вероятности можно выразить (10) при помощи функции Лапласа [4]:

$$\Phi(x) = \frac{1}{\sqrt{2\pi}}\int_0^x \exp^{\left(-\frac{t^2}{2}\right)} dt.$$

Для нахождения оптимального порога Ω_0 необходимо вычислить производную $P_e'(N)$ в (10), а затем приравнять ее к нулю:

$$\frac{r\sqrt{N}}{2\sqrt{2}\sigma^2(r+1)}\varphi\left(\sqrt{N}\frac{\Omega_0 - 2\sigma^2\frac{r+1}{r}}{\sigma^2 2\sqrt{2}}\frac{r}{r+1}\right) -$$
$$-\frac{\sqrt{N}}{2\sqrt{2}\sigma^2}\varphi\left(\sqrt{N}\frac{\Omega_0 - 2\sigma^2}{\sigma^2 2\sqrt{2}}\right) = 0, \quad (11)$$

где $\varphi(t) = \frac{1}{\sqrt{2\pi}}e^{-\frac{t^2}{2}}$.

Уравнение (11) эквивалентно следующему уравнению:

$$\frac{r}{r+1}\exp\left(-\frac{N}{16\sigma^4}\left(\frac{r}{r+1}\right)^2\left(\Omega_0 - 2\sigma^2\frac{r+1}{r}\right)^2\right) =$$
$$= \exp\left(-\frac{N}{16\sigma^4}(\Omega_0 - 2\sigma^2)^2\right). \quad (12)$$

Дальнейшее упрощение (12) приводит к следующему уравнению:

$$\Omega_0\left(1 - \frac{r}{r+1}\right)\left(\Omega_0\left(1 + \frac{r}{r+1}\right) - 4\sigma^2\right) =$$
$$= \frac{16\sigma^4}{N}\ln\left(1 + \frac{1}{r}\right). \quad (13)$$

Решая уравнение (13) относительно Ω_0, получаем следующее квадратное уравнение:

$$\omega^2\frac{2r+1}{(r+1)^2} - \omega\frac{4}{r+1} - \frac{16}{N}\ln\left(1 + \frac{1}{r}\right) = 0, \quad (14)$$

где введено обозначение $\omega = \frac{\Omega_0}{\sigma^2}$.

Вещественный положительный корень этого уравнения может быть найден по известной формуле:

$$\omega = \frac{r+1}{2r+1}\left(2 + \sqrt{4 + (2r+1)\frac{16}{N}\ln\left(1 + \frac{1}{r}\right)}\right).$$

Тогда окончательно находим величину оптимального порога как:

$$\Omega_0 = \sigma^2\frac{r+1}{2r+1}\left(2 + \sqrt{4 + \frac{16}{N}(2r+1)\ln\left(1 + \frac{1}{r}\right)}\right) \quad (15)$$

При $N \gg 1$ (что, как будет показано далее, типично для практики), получим для Ω_0 по (15) следующее приближение:

$$\Omega_0 \approx 4\sigma^2\frac{r+1}{2r+1}. \quad (16)$$

В таблице 1 показаны результаты расчета по (16) для различных r.

$$P_m = \Pr(\Omega < \Omega_0|H_1) = 0{,}5 + \Phi\left(\sqrt{N}\frac{\Omega_0 - 2\sigma^2\frac{r+1}{r}}{\sigma^2 2\sqrt{2}}\frac{r}{r+1}\right),$$
$$P_{fa} = \Pr(\Omega \geq \Omega_0|H_0) = 0{,}5 - \Phi\left(\sqrt{N}\frac{\Omega_0 - 2\sigma^2}{\sigma^2 2\sqrt{2}}\right), \quad (10)$$
$$P_e = \frac{P_m + P_{fa}}{2} = \frac{1}{2}\left(1 + \Phi\left(\sqrt{N}\frac{\Omega_0 - 2\sigma^2\frac{r+1}{r}}{\sigma^2 2\sqrt{2}}\frac{r}{r+1}\right) - \Phi\left(\sqrt{N}\frac{\Omega_0 - 2\sigma^2}{\sigma^2 2\sqrt{2}}\right)\right).$$

ТАБЛИЦА 1. Расчет оптимального порога Ω_0 по (16)

TABLE 1. Calculation of the Optimal Threshold Ω_0 by (16)

r	1	2	4	8	16
Ω_0	$2{,}66\sigma^2$	$2{,}4\sigma^2$	$2{,}22\sigma^2$	$2{,}06\sigma^2$	$1{,}94\sigma^2$

Для расчета величины P_e при оптимальном пороге Ω_0, найденном по (16), предварительно рассчитаем аргументы функции $\varphi(\cdot)$ в (11):

$$\sqrt{N}\frac{\Omega_0 - 2\sigma^2\frac{r+1}{r}}{\sigma^2 2\sqrt{2}}\frac{r}{r+1} = \\ = r\sqrt{N}\frac{\frac{r+1}{2r+1}\left(2+\sqrt{4+\frac{16}{N}(2r+1)\ln\left(1+\frac{1}{r}\right)}\right) - 2\frac{r+1}{r}}{2\sqrt{2}(r+1)}, \quad (17)$$

$$\sqrt{N}\frac{\Omega_0 - 2\sigma^2}{\sigma^2 2\sqrt{2}} = \\ = \sqrt{N}\frac{\frac{r+1}{2r+1}\left(2+\sqrt{4+\frac{16}{N}(2r+1)\ln\left(1+\frac{1}{r}\right)}\right) - 2}{2\sqrt{2}}. \quad (18)$$

При $N \gg 1$ выражения (17), (18) приводятся, соответственно к следующему виду:

$$-\frac{\sqrt{N}}{\sqrt{2}(2r+1)}, \qquad \frac{\sqrt{N}}{\sqrt{2}(2r+1)} \quad (19)$$

Подставляя (19) в (10), окончательно находим при $N \gg 1$:

$$P_e = \frac{P_m + P_{fa}}{2} \approx \\ \approx \frac{1}{2}\left(1 + \Phi\left(-\frac{\sqrt{N}}{\sqrt{2}(2r+1)}\right) - \Phi\left(\frac{\sqrt{N}}{\sqrt{2}(2r+1)}\right)\right) = \quad (20) \\ = \frac{1}{2} - \Phi\left(\frac{\sqrt{N}}{\sqrt{2}(2r+1)}\right).$$

Из выражения (20) видно, что при $r \to \infty$, $P_e \to 0{,}5$, т. е. алгоритм обнаружения факта клонирования эквивалентен «случайному угадыванию», что соответствует «физическому смыслу», поскольку случай $r \to \infty$ соответствует пренебрежимо малому шуму злоумышленника, добавление которого, конечно, оказывается невозможно обнаружить.

С другой стороны, если $N \to \infty$, то $P_e \to 0$ при любых конечных значениях r, что также совпадает с нашей интуицией, обеспечивая надежное обнаружение факта клонирования.

Для того, чтобы рассчитать вероятность ошибки P_e при конечных величинах N и r, можно воспользоваться следующим приближением функции $\Phi(\cdot)$ [4]:

$$\Phi(x) \approx \frac{1}{2} - \frac{1}{\sqrt{2\pi}}\frac{e^{-\frac{x^2}{2}}}{x}. \quad (21)$$

Подставляя (21) в (20), получаем:

$$P_e \approx \Phi\left(\frac{1}{2\pi}\frac{e^{-\frac{x^2}{2}}}{x}\right), \quad (22)$$

где $x = \frac{\sqrt{N}}{\sqrt{2}(2r+1)}$.

На рисунке 1 показана зависимость P_e от N для различных величин r = 1, 2, 4, 8, 16.

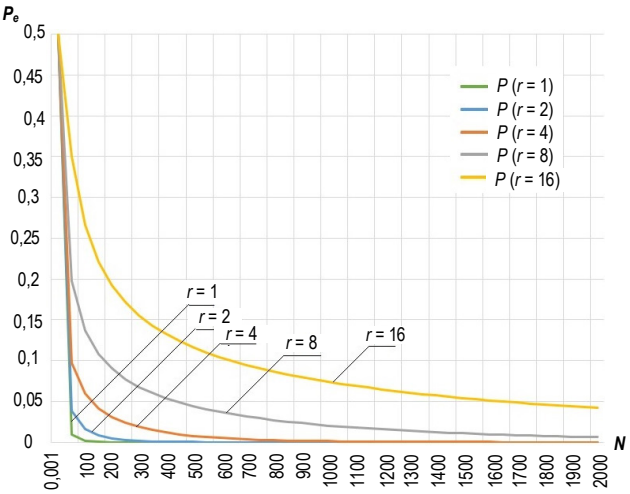

Рис. 1. Зависимости полной вероятности ошибки обнаружения атаки клонирования от длины ЦВЗ N

Fig. 1. Dependences of the Total Error Probability of Detecting a Cloning Attack on the Length N of the Digital Watermark

В таблице 2 показаны результаты расчета P_e для различных значений r и N.

ТАБЛИЦА 2. Расчет P_e при N = 600, 800, 1000, 1200, 1500 и r = 1, 2, 4, 8, 16

TABLE 2. Calculation of P_e when N = 600, 800, 1000, 1200, 1500 and r = 1, 2, 4, 8, 16

$r\backslash N$	600	800	1000	1200	1500
1	0	0	0	0	0
2	0,000046	0,0000053	0,00000065	0,000000079	0,0000000036
4	0,0052	0,0024	0,0012	0,00058	0,00021
8	0,037	0,027	0,021	0,016	0,011
16	0,11	0,087	0,074	0,065	0,054

Заключение

В работе был предложен и теоретически исследован метод обнаружения атаки клонирования. Видно, что он позволяет решить эту задачу при некоторых длинах вкладываемых ЦВЗ и ограничениях на шумы сканера и принтера атакующего. Однако окончательное подтверждение возможности такого вывода требует дополнительных экспериментальных исследований, которые, правда, уже частично проводились – для анализа возможности считывания ЦВЗ с бумажных и пластиковых носителей в работе [5], а также частично рассматривались в работе [6].

Дальнейшие исследования, особенно относящиеся к обоснованию выбора параметра *r*, авторы предполагают выполнить в ближайшем будущем. Наилучшим вариантом стало бы проведение множества экспериментов, включающих в себя печать и сканирование сертификата, подделку сертификата, печать и сканирование поддельного сертификата. Однако при проведении таких экспериментов, кроме основных параметров (размер сертификата, длина ШПС и глубина вложения) стоит учесть также множество второстепенных параметров и настроек алгоритмов вложения/извлечения ЦВЗ, таких как расположение оптимальной области вложения в отчеты ДКП, размеры DataMatrix и др. Это в свою очередь, потребует проведения чрезмерно большого количества операций, проводимых вручную (печать, сканирование), а также серьезные материальные вложения.

В связи с этим предполагается разбить проводимые эксперименты на два этапа: предварительный и основной.

Предварительный этап будет включать в себя выявление образцов шума присущих используемому оборудованию (принтеру и сканеру) и проведение программных (цифровых) экспериментов, в которых реальная печать заменена на виртуальную. Проведение экспериментов виртуально позволит легко автоматизировать процесс, произвести множество экспериментов и подобрать оптимальные настройки используемых алгоритмов.

На основном этапе будут проводиться реальные эксперименты. Вначале необходимо будет подтвердить предварительные результаты путем проведения выборочной печати сертификатов из множества предварительных экспериментов. После чего будет проводиться накопление статистических данных о работе предложенного метода в реальных условиях.

БЛАГОДАРНОСТИ

Авторы благодарят Букшина Ивана Дмитриевича за помощь при проведении расчетов и построении графиков.

Список используемых источников

1. Cox I.J., Miller M.L., Bloom J.A. Digital Watermarking. Elsevier, 2002. 542 p. DOI:10.1016/B978-1-55860-714-9.X5000-7

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. Ван дер Варден Б.Л. Математическая статистика. Пер. с нем. М.: Издательство иностранной литературы, 1960. 435 с.

4. Финк Л.М. Теория передачи дискретных сообщений. М.: Советское радио, 1970.

5. Ho A.T.S., Shu F. A print-and-scan resilient digital watermark for card authentication // Proceedings of the Fourth International Conference on Information, Communications and Signal Processing and The Fourth Pacific Rim Conference on Multimedia (Singapore, 15–18 December 2003). Vol. 2. IEEE, 2003. PP. 1149–1152. DOI:10.1109/ICICS.2003.1292640

6. Коржик В.И., Флаксман Д.А. Система цифровых водяных знаков с возможностью их извлечения из бумажных копий цифровых документов // Труды учебных заведений связи. 2019. Т. 5. № 3. С. 75–85. DOI:10.31854/1813-324X-2019-5-3-75

* * *

Elaboration of Digital Watermarking Method for a Protection of Cloning Attack on Paper Certificates

V. Korzhik[1], V. Starostin[1], D. Flaksman[2]

[1]The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, St. Petersburg, 193232, Russian Federation
[2]Research and Production Enterprise "Novye Tekhnologii Telekommunikatsii", Ltd, St. Petersburg, 195256, Russian Federation

Article info
DOI:10.31854/1813-324X-2021-7-2-79-84
Received 6th March 2021
Accepted 29th April 2021

For citation: Korzhik V., Starostin V., Flaksman D. Elaboration of Digital Watermarking Method for a Protection of Cloning Attack on Paper Certificates. *Proc. of Telecom. Universities.* 2021;7(2):79–84. (in Russ.) DOI:10.31854/1813-324X-2021-7-2-79-84

Abstract: *Paper (or plastic) certificates are considered as a means against different forgery of product quality and brand falsification. It is commonly to use barcodes or data matrices to solve this problem. However such approach does not work usually against such sophisticated attacks as cloning of certificate copies. In the current paper we propose to use a digital watermarking and estimation of inner noises of scanners and printers in order to detect cloning attack effectively. Algorithm of cloning attack detecting is presented. The probabilities of attack missing and false alarm are proved.*

Keywords: *certificate of product, cloning attack, digital watermarking, the probabilities of attack missing and false alarm.*

ACKNOWLEDGMENT

The authors are grateful to Ivan Dmitrievich Bukshin for help with calculations and graphing.

References

1. Cox I.J., Miller M.L., Bloom J.A. *Digital Watermarking*. Elsevier; 2002. 542 p. DOI:10.1016/B978-1-55860-714-9.X5000-7
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. Van der Waerden B.L. *Math Statistics*. Translated from German. Moscow: Inostrannaia literatura Publ.; 1960. 435 p. (in Russ.)
4. Fink L.M. *Theory of Discrete Signal Transmission.* Moscow: Sovetskoe radio Publ.; 1970. (in Russ.)
5. Ho A.T.S., Shu F. A print-and-scan resilient digital watermark for card authentication. *Proceedings of the Fourth International Conference on Information, Communications and Signal Processing and The Fourth Pacific Rim Conference on Multimedia, 15–18 December 2003, Singapore*. IEEE; 2003. vol.2. p.1149–1152. DOI:10.1109/ICICS.2003.1292640
6. Korzhik V., Flaksman D. Digital Watermark System with an Ability of its Extraction from Hard Copies of Data. *Proc. of Telecom. Universities*. 2019;5(3):75–85. (in Russ.) DOI:10.31854/1813-324X-2019-5-3-75-85

Сведения об авторах:

КОРЖИК Валерий Иванович — доктор технических наук, профессор, профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, val-korzhik@yandex.ru
https://orcid.org/0000-0002-8347-6527

СТАРОСТИН Владимир Сергеевич — кандидат физико-математических наук, доцент кафедры высшей математики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, star_vs_47@mail.ru

ФЛАКСМАН Дмитрий Алексеевич — программист ООО «Научно-производственное предприятие Новые Технологии Телекоммуникаций», flxdima4951@gmail.com
https://orcid.org/0000-0002-0326-4592