Текстурные методы защиты полиграфических документов, стойкие к подбору ключа

В.А. Федосеев[а,б]

[а] *Самарский национальный исследовательский университет имени академика С.П. Королева, 443086, Московское шоссе, 34, Самара, Россия*
[б] *Институт систем обработки изображений РАН – филиал ФНИЦ «Кристаллография и фотоника» РАН, 443001, ул. Молодогвардейская, 151, Самара, Россия*

Аннотация

В работе предлагаются текстурные методы защиты полиграфических документов скрытыми изображениями, которые в отличие от известных аналогов обеспечивают стойкость к атаке подбора ключа на основе спектрального анализа изображения документа. Стойкость обеспечивается за счёт наложения нескольких текстур, имеющих согласованные параметры, что увеличивает переборное множество при проведении атаки, а также за счёт разделения полезной информации между различными текстурами. В работе приводятся результаты экспериментальных исследований, подтверждающих работоспособность предложенных методов.

Ключевые слова: латентное изображение; текстурный водяной знак; полиграфический документ; текстурный анализ; спектральный анализ; визуальная криптография

1. Введение

Одним из самых распространённых способов защиты важных полиграфических документов и ценных бумаг от подделки и/или несанкционированного копирования является использование скрытых (латентных) изображений [1], также называемых текстурными водяными знаками (ТВЗ) [2]. Они представляют собой специальные метки, образованные вариациями каких-либо параметров регулярной (двумерной квазипериодической) текстуры, покрывающей документ или его отдельные части. Типичными примерами подобной вариации параметров являются изменение шага (периода) текстуры, пространственной ориентации, смещения относительно точной периодичности повторения (фазы) или формы текстурного примитива. Локальная средняя яркость текстурированной области документа при этом не меняется, чем обеспечивается визуальная неразличимость латентного изображения.

Методы, реализующие данный принцип, известны с середины 1970-х гг. и широко применяются для защиты паспортов, виз, денежных знаков и прочей защитной полиграфической продукции. К их числу относятся запатентованные методы «Вариация направления линий» («Line angle variation») [3], «Вариация масштаба» [4], «Invisible Personal Information» [5], «Isocheck/Isogram» [6] и ряд других. Извлечение информации, встроенной этими методами, возможно при знании параметров текстур, использованных при сокрытии изображения. В частности, для двух последних методов, которые основаны на смещении фазы текстуры, скрытая информация может быть выявлена физически путём наложения на документ согласованной с текстурой оптической решётки (рис. 1). Таким образом, для получения доступа к скрытой информации злоумышленнику достаточно восстановить параметры используемых текстур, которые таким образом составляют секретный ключ рассматриваемой системы защиты информации.

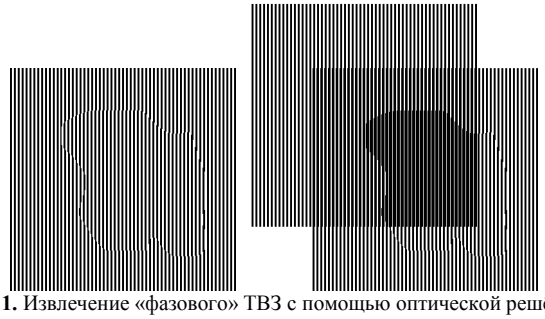


Рис. 1. Извлечение «фазового» ТВЗ с помощью оптической решётки.

Ранее коллективом, членом которого является автор работы, проводились исследования, имевшие целью определение параметров текстур, несущих скрытую информацию, с последующим её восстановлением [2, 7-10]. В результате этих исследований был разработан универсальный метод, позволяющий с высокой точностью восстанавливать ключ системы текстурных водяных знаков (параметры текстуры) и с его помощью извлекать скрытую информацию. Данный метод заключается в поиске наиболее значимых периодических текстур на спектре изображения документа, восстановлении их параметров и последующей фильтрации изображения по первой-второй гармоникам всех найденных текстур. Поскольку при наличии скрытого изображения несущие его текстуры заполняют только часть плоскости, то в результате их фильтрации встроенная информация становится различимой. Существование подобной атаки свидетельствует о недостаточной защищённости рассматриваемого метода встраивания ТВЗ и, следовательно, об актуальности его модификации, которая позволила бы сделать рассмотренную атаку менее действенной.

Данная работа посвящена разработке модифицированных методов встраивания ТВЗ, обладающих повышенной стойкостью к рассмотренной атаке и её аналогам. Для этого были рассмотрены несколько различных подходов, оценена их эффективность и на основе проведённого анализа предложен итоговый комбинированный вариант

модифицированной системы ТВЗ. В работе приводятся теоретические оценки эффективности предложенных методов и результаты их экспериментальной апробации.

2. Базовый метод встраивания ТВЗ и атака на него

2.1. Базовый метод встраивания ТВЗ

Рассмотрим упрощённую модель базового метода встраивания ТВЗ.

Пусть предпечатный экземпляр полиграфического документа (цифровое изображение) имеет размеры $N_1 \times N_2$. Поскольку печать документа осуществляется в высоком разрешении, то такое изображение может иметь несколько десятков тысяч пикселей по каждой размерности. Пусть встраивание ТВЗ осуществляется в один цветовой слой данного изображения, который посредством текстуры должен передавать постоянную на всём пространстве изображения яркость $v \in [0,255] \cap \mathbb{Z}$, то есть полутоновой оригинал результирующего текстурированного изображения имеет вид

$$I_v(n_1, n_2) = v, \tag{1}$$

где $0 \le n_1 < N_1$, $0 \le n_2 < N_2$. Обозначим

$$Tex_v(n_1, n_2; \omega, \varphi, \delta, \theta) \tag{2}$$

изображение, представляющее собой строго периодическую текстуру, имеющую пространственную частоту ω, направление φ, смещение δ, форму структурного элемента θ (не будем конкретизировать способ описания формы) и среднюю яркость v.

Упрощение модели заключается в том, что на практике яркость оригинала часто не является постоянной, а плавно меняется по пространственным координатам. В этом случае заполняющая документ текстура также не будет строго регулярной. Однако для этого случая на практике вместо строго периодической текстуры используется результат растрирования исходного изображения методом амплитудной модуляции [11], для которой определены те же параметры $\omega, \varphi, \delta, \theta$. Таким образом, на рассматриваемом уровне абстракции эти два случая аналогичны друг другу.

Пусть встраиваемая информация (текстурный водяной знак, или латентное изображение) задаётся матрицей W того же размера, содержащей двоичные значения: $W(n_1, n_2) \in \{0;1\}$. Тогда базовый метод встраивания ТВЗ можно определить следующим образом:

$$I_v^W(n_1, n_2) = W(n_1, n_2) \cdot Tex_v(n_1, n_2; \omega_1, \varphi_1, \delta_1, \theta_1) + (1 - W(n_1, n_2)) \cdot Tex_v(n_1, n_2; \omega_2, \varphi_2, \delta_2, \theta_2), \tag{3}$$

то есть область определения изображения заполняется двумя текстурами в соответствии с маской W.

Следует отметить, что для того, чтобы использование двух текстур было незаметным для человеческого глаза, текстуры в (3) подбираются таким образом, что только одна из четырёх пар параметров: (ω_1, ω_2), (φ_1, φ_2), (δ_1, δ_2) или (θ_1, θ_2) содержит различающиеся значения. В результате при $\omega_1 \ne \omega_2$ формула (3) фактически описывает алгоритм «Вариация масштаба» [4], при $\varphi_1 \ne \varphi_2$ – алгоритм «Вариация направления линий» [3], при $\delta_1 \ne \delta_2$ – «Invisible Personal Information» [5], при $\theta_1 \ne \theta_2$ – алгоритм вариации структурного элемента [12].

2.2. Метод атаки на базовый метод и подходы к её противодействию

Как уже отмечалось выше, принцип взлома системы ТВЗ, описанной в п. 2.1, заключается в восстановлении параметров текстур, использованных для формирования скрытого изображения, и фильтрации изображения полиграфического документа с учётом найденных параметров.

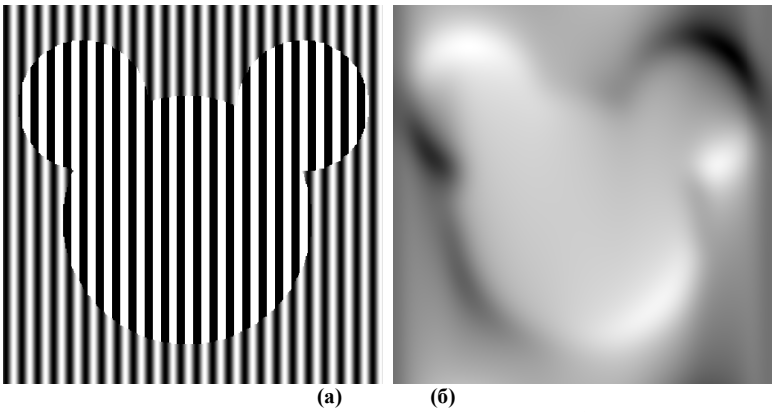
Конкретно, разработанный метод для случая обнаружения одного ТВЗ состоит из следующих последовательно выполняемых этапов:

1. Отыскание регулярных текстур на изображении и восстановление их параметров на основе спектрального анализа. Алгоритм, реализующий данный этап, подробно описан в работе [13] и основывается на свойствах дискретного спектра несинусоидальных периодических сигналов, который содержит периодические всплески (пики) на кратных гармониках. Таким образом, алгоритм заключается в поиске таких «пиковых решёток» на двумерном спектре.
2. Формирование на основе найденных параметров банка фильтров Габора [14] и линейная фильтрация изображения каждым из фильтров.
3. Формирование вещественных полей признаков на основе полученных результатов фильтрации (комплексных откликов). Для этого отклики представляются в виде пары изображений: модуля и фазы, которая предварительно разворачивается.

4. Отбор информативных полей признаков. Как показала практика применения данной атаки [9, 10], модули откликов чаще информативны при $\omega_1 \neq \omega_2$, $\varphi_1 \neq \varphi_2$ или $\theta_1 \neq \theta_2$, а в случае $\delta_1 \neq \delta_2$ более информативными являются фазовые составляющие откликов.
5. Многокомпонентная кластеризация на два класса по отобранному множеству полей признаков.

Ключевыми в данном методе являются этапы 1 и 2. Таким образом, модификация системы ТВЗ должна быть иметь целью снижение эффективности хотя бы одного из них. То есть она должна либо усложнить задачу обнаружения и восстановления параметров несущих текстур на основе анализа спектра изображения, либо добиться эквивалентности откликов этих текстур на фильтры Габора.

Второй подход, заключающийся в противодействии второму этапу рассмотренной атаки, в принципе применим на практике, что иллюстрирует пример на рис. 2, где фактически проведено встраивание по формуле (3), где $\theta_1 \neq \theta_2$: в центре используется прямоугольный шаблон текстуры, а по краям – синусоидальный, причём обе текстуры совпадают по остальным ключевым параметрам. На рисунке 2б показан модуль отклика фильтра Габора, согласованного с параметрами текстур на рис. 2а. из этого рисунка можно увидеть, что вдали от границ текстур отклик имеет высокие по модулю значения, которые было бы трудно различить даже визуально, если бы не «затемнения», возникающие на границе текстур. Тем не менее, можно говорить о том, что в конкретном рассмотренном примере фильтр Габора не позволяет извлечь скрытый ТВЗ.



(а) **(б)**

Рис. 2. ТВЗ, встроенный за счёт использования прямоугольной и синусоидальной текстур (а) и попытка его извлечения фильтром Габора (б).

Однако подобный подход (противодействие габоровской фильтрации) имеет существенные недостатки. Во-первых, возвращаясь к примеру на рис. 2, синусоидальный сигнал не может быть перенесён на бумагу традиционно используемыми технологиями печати [15]. Во-вторых, в случае успешного подбора шаблонов текстур, переносимых на бумагу, для различения которых неэффективен фильтр Габора, атакующий может воспользоваться любым другим узкополосным фильтром, что с большой вероятностью возымеет успех. Кроме того, для извлечения таких ТВЗ существуют методы, восстанавливающие основные текстурные шаблоны на изображении и коррелирующие изображение с каждым из них [16]. Поэтому более перспективным видится первый подход, который и разрабатывается в следующем разделе – модификация алгоритма встраивания ТВЗ, усложняющая задачу восстановления параметров несущих текстур.

3. Методы повышения стойкости базового метода за счёт маскирования периодическими структурами

3.1. Общий подход

Рассмотрим изображение размерами $N \times N$, заполненное двумерной периодической текстурой с размером структурного элемента $T \times T$. Модуль дискретного спектра такого изображения содержит пики на частотах $\Omega_{10} = N/T \cdot (1,0)$ и $\Omega_{01} = N/T \cdot (0,1)$ - это первые гармоники по двум ортогональным направлениям. Кроме того, спектр может содержать пики на всех частотах вида $\Omega_{km} = k\Omega_{10} + m\Omega_{01}$, где $k, m \in \mathbb{Z}$. Таким образом, спектр может содержать до $N/(N/T) \times N/(N/T) = T^2$ пиков.

В атаке, рассмотренной в разделе 2.2, банк фильтров пополняется частотами $\Omega_{01}, \Omega_{10}, \Omega_{11}$ для каждой найденной на изображении текстуры (для извлечения ТВЗ типа «Вариация масштаба» также целесообразно рассматривать частоты $\Omega_{02}, \Omega_{20}, \Omega_{22}$), что на практике практически гарантирует попадание в «варьируемую частоту» и не вызывает серьёзных вычислительных затрат. Между тем, если бы вариация текстуры проводилась на частотах Ω_{km}, где k и m существенно превышает единицу, то для атаки на такой ТВЗ потребовалось бы существенно увеличивать множество перебираемых частот.

Попробуем оценить это множество из практических соображений. Прототип полиграфического документа может иметь очень большие пространственные размеры, достигающие нескольких десятков тысяч пикселей по каждому из измерений. Разумеется, спектральный анализ таких изображений – чрезвычайно трудоёмкая задача, поэтому при проведении атаки будет анализироваться спектр фрагмента. Для определённости предположим, что для анализа используется фрагмент с линейным размером $N = 2048$ (см. рис. 3). Тогда при $T = 2048/16 = 128$ частота первой гармоники (и минимальный период «пиковой решётки») на дискретном спектре составят 16 отсчётов, что является

достаточным интервалом для обнаружения локальных максимумов. При меньшей частоте на практике (при условии погрешностей печати-сканирования) обнаружение пиков не всегда удаётся осуществить безошибочно. Таким образом, при полученных размерах наибольший объём перебираемых значений не составляет $P_{\max} = T^2 = 2^{14}$. По результатам исследований с реальными отсканированными и синтезированными изображениями, проведённых в работе [9], можно сказать, что наименьший объём перебора может составить $P_{\min} = 8 \cdot 8 = 2^6$, то есть будем исходить из предположения, что при высоком качестве печати-сканирования различимыми на спектре являются не менее 8 первых пиков по каждой из осей.

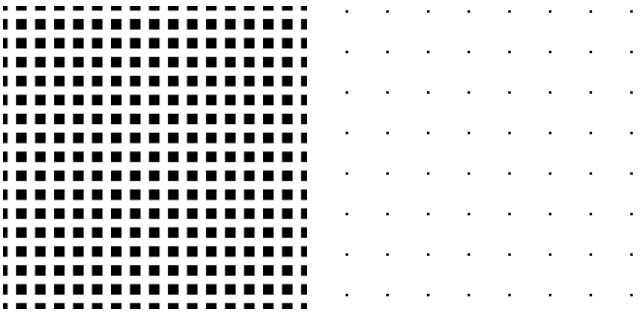
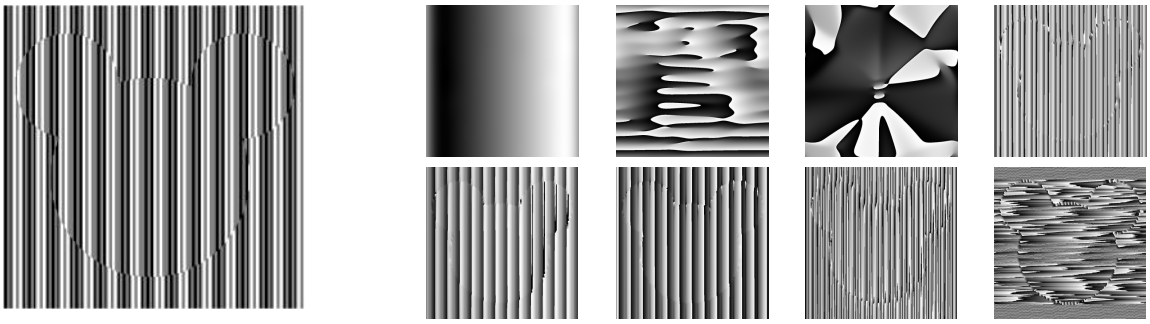


Рис. 3. Периодическая текстура с N=2048 и T=128 и фрагмент её спектра, содержащий 8 линейных гармоник.

Как можно осуществить вариацию текстуры на заданной частоте? Первый подход осуществить фильтрацию спектра, что сразу позволит достичь требуемого спектрального результата, однако после подобных изменений полученная в пространственной области текстура скорее всего не сможет быть напечатана. Для гарантии переносимости на бумагу изображение должно формироваться в пространственной области как двумерная кусочно-постоянная функция. Поэтому для вариации текстур в дальних гармониках в данной работе рассматривается другой подход: формирование изображения как композиции нескольких текстур, причём первые гармоники текстур, несущих ТВЗ, являются дальними гармониками других текстур, *маскирующих* ТВЗ.

Для апробации данного подхода рассмотрим изображение на рис. 4, представляющее собой взвешенную сумму фазового ТВЗ [5] и маскирующей текстуры вдвое большего периода. При отсутствии маскировки такой ТВЗ извлекается без каких-либо проблем. Однако, как показывает рис. 4б, базовая версия атаки (без полного перебора по всем найденным гармоникам) не позволяет получить ни одного поля признаков, подходящего для извлечения встроенной информации. Таким образом, мы получили простейший пример модифицированного ТВЗ, устойчивого к атаке на основе анализа спектра. В следующем подразделе мы обобщим данный подход.



(а) **(б)**

Рис. 4. ТВЗ с маскировкой (а) и признаки, полученные при попытке применения для него стандартной атаки (б).

3.2. Модифицированные методы встраивания ТВЗ и оценки их стойкости

Формула встраивания информации для примера на рис. 4а имеет вид

$$\begin{aligned} I_v^W(n_1,n_2) &= \alpha_C Tex_v\left(n_1,n_2;\omega^C,\varphi^C,\delta^C,\theta^C\right)+ \\ &+\alpha_V\left(W(n_1,n_2)\cdot Tex_v\left(n_1,n_2;\omega_1^V,\varphi_1^V,\delta_1^V,\theta_1^V\right)+\left(1-W(n_1,n_2)\right)\cdot Tex_v\left(n_1,n_2;\omega_2^V,\varphi_2^V,\delta_2^V,\theta_2^V\right)\right), \end{aligned} \quad (4)$$

где индексы C (от слова const) характеризуют параметры постоянной (маскирующей) текстуры, а индексы V (от слова variable) характеризуют параметры варьирующихся текстур, образующих встраиваемый ТВЗ. Коэффициенты в формуле (3) подбираются из условия

$$\alpha_C + \alpha_V = 1.$$

Как уже отмечалось в разделе 3.1, объём перебора при осуществлении атаки при встраивании (3) и фиксированных размерах изображения и структурного элемента маскирующей текстуры находится в пределах

$$2^6 = P_{\min} \le P \le P_{\max} = 2^{14}. \quad (5)$$

Если ориентироваться на нижнюю границу этого отрезка, то этого явно недостаточно, чтобы сделать атаку неэффективной. Однако можно усложнить формулу (4), добавив большее количество маскирующих и несущих текстур. В этом случае формула встраивания будет выглядеть следующим образом:

$$I_v^W(n_1,n_2) = \alpha_C \sum_{i=0}^{M_C-1} \beta_i^C Tex_v\left(n_1,n_2;\omega_i^C,\varphi_i^C,\delta_i^C,\theta_i^C\right) + \\ +\alpha_V \sum_{j=0}^{M_V-1} \beta_j^V \left(W_j(n_1,n_2)\cdot Tex_v\left(n_1,n_2;\omega_{j,1}^V,\varphi_{j,1}^V,\delta_{j,1}^V,\theta_{j,1}^V\right) + \left(1-W_j(n_1,n_2)\right)\cdot Tex_v\left(n_1,n_2;\omega_{j,2}^V,\varphi_{j,2}^V,\delta_{j,2}^V,\theta_{j,2}^V\right)\right), \quad (6)$$

где

$$\sum_{i=0}^{M_C-1} \beta_i^C = \sum_{j=0}^{M_V-1} \beta_j^V = 1.$$

Рассмотрим по отдельности каждое из изменений. Увеличение числа маскирующих текстур усложняет визуальное восприятие изображения, однако ввиду ограничений снизу на расстояние между пиками спектра использование нескольких масок не позволяет увеличить множество перебираемых значений. То есть маскировка одной текстурой максимального периода даёт тот же эффект, что и маскировка двумя текстурами вдвое меньшего периода, обеспечивающими то же минимальное расстояние между пиками. Поэтому, несмотря на допустимость варианта (4), будем полагать, что на практике всё же целесообразнее использовать $M_C = 1$.

Второе изменение заключается в одновременном встраивании нескольких изображений W_j, которые должны в итоге формировать одно скрытое изображение следующим образом:

$$W = \underset{j=0}{\overset{M_V-1}{XOR}} W_j. \quad (7)$$

Благодаря свойствам функции XOR, для точного извлечения встроенного изображения W необходимо обнаружить и восстановить все без исключения W_j. Таким образом, для успешной атаки становится необходимым не только перебрать все P вариантов (5) частот, но и отобрать из них неизвестное количество, которые в совокупности модулируют встроенный ТВЗ. Если на практике известно наибольшее возможное значение $M_V - M_{V\max}$, то для восстановления W потребуется P фильтраций (что составляет основное время атаки), а также

$$\sum_{m=1}^{M_{V\max}} C_P^m \quad (8)$$

операций XOR над наборами изображений с проверкой информативности результата (C_P^m - число сочетаний из P по m). Формула (7) даёт возможность представить $M_V - 1$ из M_V изображений W_j в виде псевдослучайного шаблона, состоящего из блоков определённого размера (см. рис. 5а), что в свою очередь затрудняет этап отбора информативных полей признаков при проведении атаки (отклики на варьируемые текстуры могут выглядеть так же и иметь близкие характеристики, что и отклики на кратные гармоники, в которых отсутствует пространственная вариация).

Рис. 5. Иллюстрация возможности комбинации нескольких встраиваемых ТВЗ, имеющих блочную структуру.

На рис. 5 показан пример, показывающий принципиальную возможность извлечения информации по формуле (7) при блочной структуре W_j. На рисунке показан встраиваемый W_j, состоящий из 32×32 блоков, результат его извлечения (соответствующее поле признаков) и результат формирования изображения W. Последнее изображение, несмотря на небольшие погрешности, достаточно точно воссоздаёт встроенный водяной знак (отметим также, что

применение голосования большинства по каждому блоку над изображением 5в позволит ещё больше снизить погрешности).

Одним из недостатков подхода (6) является невозможность выбрать большое значение параметра M_V. Поскольку каждое изображение W_j извлекается с некоторой погрешностью (см. рис. 5б), то существенное увеличение их числа повлечёт серьёзные ошибки при восстановлении изображения W. Использование же низкого значения M_V повышает уязвимость метода. В этой связи предлагается следующее усложнение формулы (6):

$$\begin{aligned} I_v^W(n_1,n_2) &= \alpha_C \sum_{i=0}^{M_C-1} \beta_i^C Tex_v\left(n_1,n_2;\omega_i^C,\varphi_i^C,\delta_i^C,\theta_i^C\right)+ \\ &+\alpha_V \sum_{j=0}^{M_V-1} \beta_j^V \left(W_j(n_1,n_2)\cdot Tex_v\left(n_1,n_2;\omega_{j,1}^V,\varphi_{j,1}^V,\delta_{j,1}^V,\theta_{j,1}^V\right)+\left(1-W_j(n_1,n_2)\right)\cdot Tex_v\left(n_1,n_2;\omega_{j,2}^V,\varphi_{j,2}^V,\delta_{j,2}^V,\theta_{j,2}^V\right)\right)+ \\ &+\alpha_F \sum_{k=0}^{M_F-1} \beta_k^F F_k(n_1,n_2) Tex_v\left(n_1,n_2;\omega_k^F,\varphi_k^F,\delta_k^F,\theta_k^F\right), \end{aligned} \quad (9)$$

где

$$\sum_{i=0}^{M_C-1}\beta_i^C = \sum_{j=0}^{M_V-1}\beta_j^V = \sum_{k=0}^{M_F-1}\beta_k^F = 1,$$

$$\sum_{k=0}^{M_F-1} F_k(n_1,n_2) = 1, \quad (10)$$

$$M_F > 2, \quad (11)$$

$$\alpha_C + \alpha_V + \alpha_F = 1. \quad (12)$$

В формуле (9) индексы F (от слова fragment) характеризуют параметры дополнительных маскирующих текстур, не заполняющих всю область изображения и не образующих ТВЗ. Заполнение такими текстурами производится для тех пикселей, для которых бинарные маски $F_k(n_1,n_2)$ имеют значение 1. Условия (10) и (12) позволяют сохранить среднюю интенсивность на уровне v, а благодаря условию (11) дополнительные текстуры не образуют отдельный водяной знак. Отметим также, что дополнительные текстуры $Tex_v\left(n_1,n_2;\omega_k^F,\varphi_k^F,\delta_k^F,\theta_k^F\right)$ не обязаны также иметь блочную структуру.

Для извлечения встроенной методом (9) информации существует 2 способа. Первый – использование формулы (7). В этом случае погрешность при извлечении информации не возрастает относительно предыдущего метода, однако появляется дополнительная сложность для атакующего в различении фрагментарных маскирующих текстур и текстур, несущих одно из встроенных изображений W_j. Они отличаются тем, что для последних существует текстура, занимающая оставшуюся область изображения, таким образом, атакующему требуется не только обнаружить все текстуры, заполняющие не всю плоскость изображения, но и попарно состыковать их для отыскания тех текстур, которые представляют интерес при извлечении информации.

Второй способ – использовать для формирования итогового ТВЗ все текстуры, таким образом формула извлечения приобретёт вид:

$$W = \left(\underset{j=0}{\overset{M_V-1}{XOR}} W_j\right) \oplus \left(\underset{k=0}{\overset{M_F-1}{XOR}} F_k\right). \quad (7)$$

Этот способ также приведёт к проблемам для атакующего – количество сочетаемых изображений вырастет с M_V до $M_V + M_F$. Однако это спровоцирует и негативный эффект, заключающийся в увеличении погрешности при извлечении санкционированными методами, что было рассмотрено выше. По этой причине первый способ представляется нам более предпочтительным.

4. Экспериментальная апробация предложенных методов

В ходе работ была проведена апробация предложенных методов на небольшом количестве текстур, имевшая целью проверить их практическую реализуемость.

Для начала осуществлялось встраивание простейшим из предложенных методов по формуле (4), то есть в ситуации, когда одна текстура маскирует один ТВЗ. Исследование проводилось при $\omega_2^V = 2\omega_1^V = 8\omega^C$ (то есть встраивался ТВЗ типа «Вариация масштаба») и при различных значениях параметра α_V (и согласованного с ним $\alpha_C = 1-\alpha_V$). Для проверки успешности маскировки изображение подвергалось атаке [9] без полного перебора кратных гармоник, то есть фильтрация осуществлялась в окрестности частот $\Omega_{01},\Omega_{10},\Omega_{11},\Omega_{02},\Omega_{20},\Omega_{22}$ для каждой обнаруженной текстуры. Успешность проведения атаки оценивалась двумя способами: во-первых, проверялось наличие хотя бы одной из частот,

несущих ТВЗ, в банке фильтров, во-вторых, определялся отклик, имеющий наиболее высокий показатель близости к встроенному изображению, и визуально проверялось его соответствие встроенной информации. Второй способ позволяет не отнести к ложным пропускам ТВЗ случаи, когда правильная частота не определилось, но найдена близкая ей частота, позволяющая извлечь информацию. Для оценки близости поля признаков, имеющего вещественные значения, и бинарного водяного знака, проверялись доля правильно извлечённых бит, PSNR, коэффициент корреляции. Наилучшим по результатам эмпирического анализа оказался последний показатель.

Результаты эксперимента в виде графиков зависимости коэффициента корреляции ρ от коэффициента относительной доли ТВЗ α_V отражены на рис. 6. Полученные результаты (согласующиеся с данными визуальных наблюдений) свидетельствуют, что атака не срабатывает при $\alpha_V \le 0,3$. Для проверки принципиальной возможности извлечения информации при таких значениях α_V на рис. 6 показана вторая кривая, характеризующая искомый показатель при известных параметрах текстуры (то есть при санкционированном извлечении информации с использованием верного ключа). На графике видно, что информация является извлекаемой и при $\alpha_V \le 0,3$.

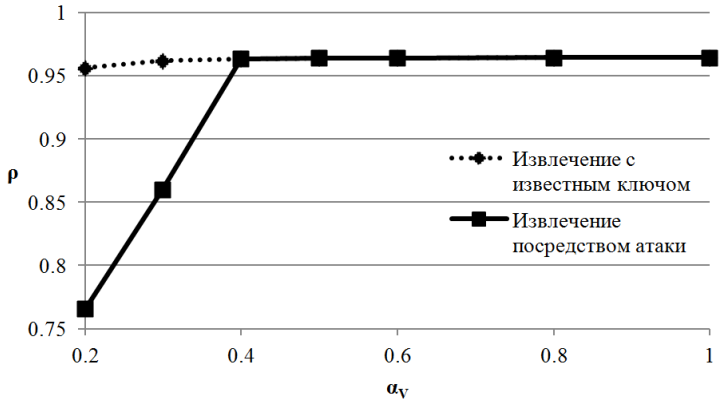


Рис. 6. Точность извлечения ТВЗ, маскированного одной текстурой, при известном и неизвестном ключе.

На рис. 7 представлены аналогичные графики, полученные при анализе изображения, содержащего $M_V = 2$ встроенных по формуле (6) изображения без какой-либо маскирующей текстуры (фактически для маскировки использовалась одна из текстур, несущих ТВЗ, а вторая имела первую гармонику на частоте Ω_{31} маскирующей текстуры). Целью эксперимента являлась проверка возможности извлечения обоих встроенных изображений и исследование влияния коэффициентов β_j^V на стойкость к атаке. Графики показывают качество извлечения второго изображения в зависимости от β_2^V. Как и в первом эксперименте, атака не срабатывает при значении коэффициента, не превышающем 0,3. На рисунке 8 показаны увеличенные фрагменты текстур, использовавшихся в данном эксперименте. На рисунке 9 показан результат извлечения обоих встроенных изображений с использованием верного ключа.

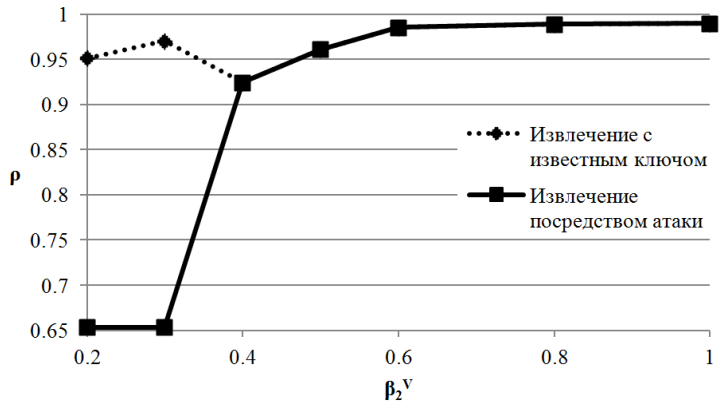


Рис. 7. Точность извлечения ТВЗ, маскированного одной другим водяным знаком, при известном и неизвестном ключе.

Последний эксперимент был повторён при встраивании по формуле (6) и значениях параметров $M_V = 2$ и $M_C = 2$. В одном случае оба изображения встраивались методом “Вариация масштаба”, в другом – методом «Invisible Personal Information». Эксперименты показали, что и в том, и в другом случае удаётся скрыть от взлома оба встроенных изображения при $\alpha_V \le 0,3$.

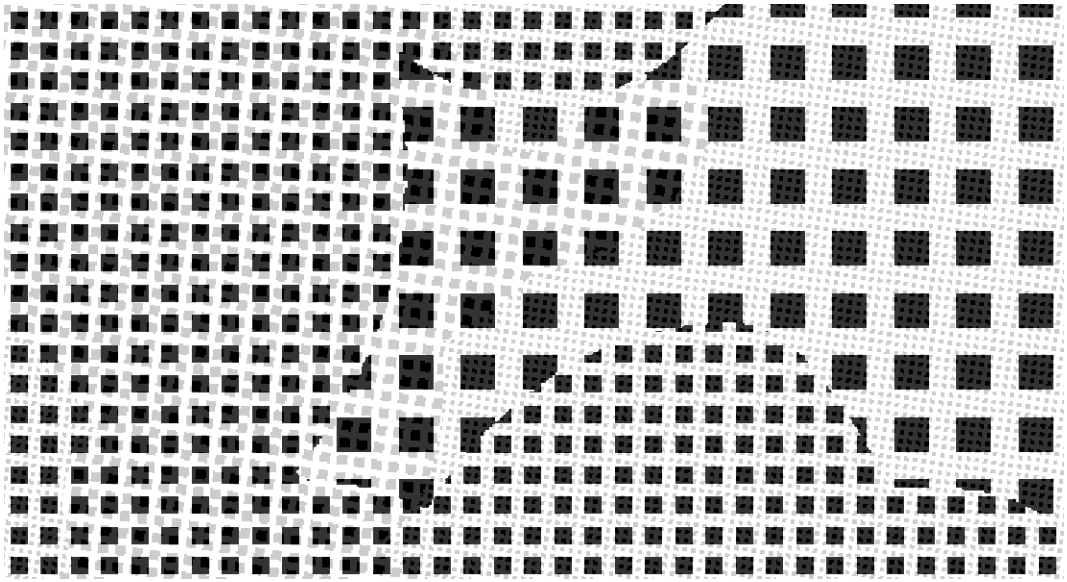
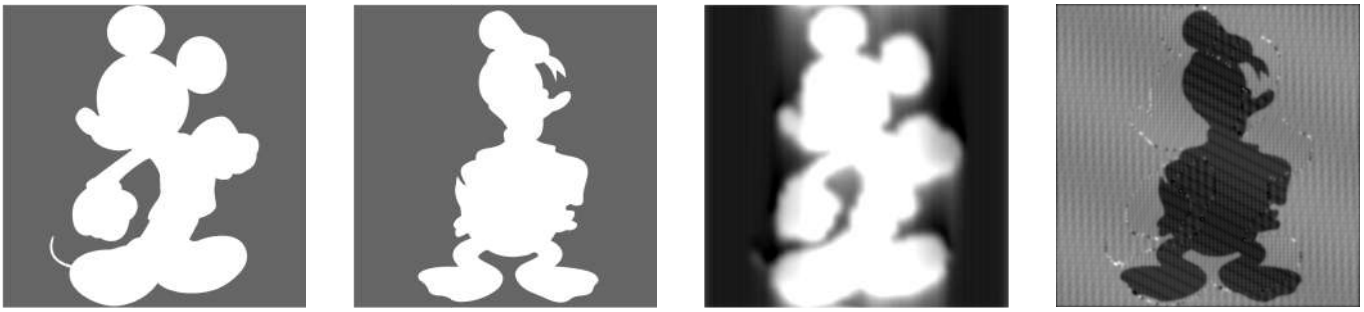


Рис. 8. Увеличенный фрагмент изображения с двумя ТВЗ, скрытыми за счёт вариации четырёх текстур.



(а) **(б)** **(в)** **(г)**

Рис. 9. Оригинальные маски ТВЗ (а)-(б) и результаты извлечения ТВЗ из изображения на рис. 8.

5. Заключение

В работе предложен ряд модифицированных алгоритмов встраивания текстурных водяных знаков (латентных изображений) в полиграфические документы, позволяющих обеспечить защиту от атаки на основе спектрального анализа, ранее разработанной при участии автора и весьма успешной для стандартных алгоритмов встраивания ТВЗ.

Предложенные методы используют:

- маскирующую текстуру, заполняющую всю область документа и скрывающую гармоники текстур, несущих ТВЗ;
- встраивание нескольких изображений в одну область документа, с формированием итогового результата как функции XOR от встроенных изображений;
- дополнительные маскирующие текстуры, заполняющие часть области документа, которые можно ошибочно принять за текстуры, несущие скрытую информацию.

В зависимости от специфики документа и требуемой степени защиты на практике могут применяться различные методы из числа предложенных. Эксперименты с использованием пробных реализаций предложенных методов показали работоспособность последних и обозначили ограничения на параметры, выполнение которых на практике обеспечивает стойкость предложенных методов к рассматриваемой атаке.

В дальнейшем планируется более углубленное исследование предложенных методов, а также их дальнейшее усовершенствование за счёт дополнения секретного ключа.

Благодарности

Работа выполнена при поддержке РФФИ (гранты 15-07-05576 и 16-41-630676) и Минобрнауки РФ в рамках гранта президента РФ МК-1907.2017.9.

Литература

[1] Павлов, И.В. Контроль подлинности документов, цен-ных бумаг и денежных знаков / И.В. Павлов, А.И. Потапов. – М.: Техносфера, 2006. – 472 с.

[2] Сергеев, В.В. Метод извлечения водяных знаков из текстурированных полиграфических документов / В.В. Сергеев, В.А. Федосеев // Компьютерная оптика. – 2014. – Т. 38(4). – С. 825-832.

[3] Hutton, R.G. Documents of value including intaglio printed transitory images, U.S. Patent 4,033,059, American Banknote Company, New York / R.G. Hutton, T. Merry. – 1977.

[4] Mowry, W. Protected document bearing watermark and method of making, U.S. Patent 4, 210, 346, Burroughs Cor-poration / W. Mowry, M. McElligott, V. Tkalenko, J. Baran, C. Ingalls. – 1977.
[5] Koltai, F. Anti-counterfeiting method and apparatus using digital screening, U.S. Patent 6, 104, 812, Juratrade Limited / F. Koltai, L. Baros, B. Adam, F. Takacs. – 1998.
[6] van Renesse, R.L. Hidden and Scambled Images – a Review / R.L. van Renesse // SPIE Conference on Optical Se-curity and Counterfeit Deterrence Techniques IV. – 2002. – P. 333-348.
[7] Fedoseev, V.A. Extraction method for textural watermarks of various linear raster patterns orientation type/ V.A. Fedoseev, V.A. Mitekin // Proceedings of the IASTED International Conference on Automation, Control, and Information Technology: Information and Communication Technology (ACIT-ICT 2010), June 15 – 18, 2010, Novosibirsk, Russia. – 2010. – P. 15-19.
[8] Sergeyev, V. Gabor Filter Based Attack on Printed Documents Protection Methods via Digital Watermarks / V. Sergeyev, V. Fedoseev, V. Mitekin // Proceedings of the 2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 18-20 July 2012, Piraeus-Athens, Greece. – 2012. – P. 265-268. – DOI 10.1109/IIH-MSP.2012.70
[9] Sergeyev, V. Extraction of Latent Images from Printed Me-dia" / V. Sergeyev, V. Fedoseev // Proceedings of SPIE. – 2015. – V. 9875. – P. 98750X. – DOI:10.1117/12.2228405.
[10] Fedoseev, V. Selection of Relevant Filter Responses for Extraction of Latent Images from Protected Documents / V. Fedoseev, E. Mishkina // Lecture Notes in Computer Science. – 2016. – Vol. 9972. – P. 523-531. – DOI: 10.1007/978-3-319-46418-3_46
[11] Lau, D.L. Modern digital halftoning / D.L. Lau, G.R. Arce. – New York: Marcel Dekker, 2011.
[12] Shibata, N. Digital watermarking system for making a digital watermark with few colors, U.S. Patent 6 268 866, NEC Corporation / N. Shibata. – 1998.
[13] Fedoseev, V.A. An Algorithm for Evaluating the Spectral Characteristics of Regular Textures / V.A. Fedoseev // Pattern Recognition and Image Analysis. – 2015. – V. 25(1). – P. 22–26. – DOI: 10.1134/S1054661815010058.
[14] Movellan, J. Tutorial on Gabor Filters / J. Movellan. – Technical report, MPLab Tutorials, University of California, San Diego, 2005.
[15] Kipphan, H. Handbook of print media: technologies and production methods / H. Kipphan. – Springer Science & Business Media, 2001.
[16] Митекин, В.А. Численные методы и программный комплекс цифрового стегоанализа текстурированной печатной : дис. … канд. тех. наук: 05.13.18. – Самара, 2009. – 142 с.