УНИФИЦИРОВАННАЯ МОДЕЛЬ СИСТЕМ ВСТРАИВАНИЯ ИНФОРМАЦИИ В ЦИФРОВЫЕ СИГНАЛЫ

В.А. Федосеев

Самарский государственный аэрокосмический университет имени академика С.П. Королёва (национальный исследовательский университет) (СГАУ), Самара, Россия,
Институт систем обработки изображений РАН, Самара, Россия

Аннотация

В работе предложена модель унифицированного описания стеганографических систем и систем встраивания цифровых водяных знаков, основанная на разделении форм информации, переносимой внутри цифрового сигнала-контейнера. Показана применимость модели для описания ряда систем.

Ключевые слова: цифровые водяные знаки, ЦВЗ, система встраивания цифровых водяных знаков, стеганография, стеганографическая система.

Цитирование: **Федосеев, В.А.** Унифицированная модель систем встраивания информации в цифровые сигналы / В.А. Федосеев // Компьютерная оптика. – 2016. – Т. 40, № 1. – С. 87-98. – DOI: 10.18287/2412-6179-2016-40-1-87-98.

Введение

Настоящая работа посвящена разработке модели для унифицированного описания систем защиты информации, предполагающих встраивание каких-либо данных (двоичной или текстовой последовательности, цифрового изображения или звукового сигнала) в цифровой сигнал (изображение, видео, аудио). Методы и алгоритмы, реализующие подобное встраивание, относятся к области знаний, именуемой в англоязычной литературе “Information Hiding” или “Data Hiding”. В рамках данной работы мы будем переводить “Information Hiding” как «*встраивание информации*» (это обусловлено тем, что общепринятый русскоязычный аналог данного понятия в настоящее время отсутствует, а использование точного перевода «сокрытие информации» может вызвать ложные ассоциации с другими областями защиты информации). Рассматриваемое направление информатики сформировалось к середине 90-х годов XX века, а первые крупные монографии появились лишь на рубеже тысячелетий. Наиболее серьёзный вклад в его развитие внесли Ingemar Cox [1–3], Jessica Fridrich [3, 4], Mauro Barni, Franco Bartolini [5], Fabien Petitcolas [6, 7], Stefan Katzenbeisser [6], Eric Cole [8], Birgit Pfitzmann [9].

Итак, под *встраиванием информации* мы будем понимать область знаний, занимающуюся вопросами внедрения секретной или защитной информации (называемой в зависимости от задачи *встраиваемой информацией*, *секретным сообщением* или *цифровым водяным знаком*, ЦВЗ) в содержимое другого информационного объекта (называемого *открыто передаваемой информацией* или *контейнером*).

Совокупность методов и средств, образующих единое решение для встраивания в цифровой сигнал информации, будем называть *системой встраивания информации* (СВИ). Существует два важных случая СВИ: это *стеганографические системы* и *системы встраивания ЦВЗ* (среди последних также иногда выделяют системы цифровых отпечатков пальцев [5]). Целью первых является организация канала защищённой передачи информации, осуществляющейся путём сокрытия самого факта передачи информации; целью вторых служит защита цифровых сигналов (от модификации, от несанкционированного распространения и пр.) посредством внедрения в них ЦВЗ.

В настоящее время в области встраивания информации существует сложившаяся и используемая большинством исследователей терминология, касающаяся крупных структурных компонент и свойств СВИ. Однако в то же время можно говорить об отсутствии общепринятой модели для их унифицированного описания, что несколько затрудняет сравнение систем, различающихся по специфике использования или составным частям.

Вышесказанное указывает на актуальность разработки достаточно универсальной математической модели, формально определяющей все возможные компоненты систем встраивания информации, учитывающей многообразие существующих алгоритмических решений, а также предоставляющей возможность унификации сложившейся терминологии. В настоящей работе предлагается такая модель, получившая название «модель системы встраивания информации» (МСВИ), определяются её основные параметры, а также показывается, как осуществляется структурное описание известных систем при помощи данной модели. Помимо внутреннего описания, данная модель позволяет охарактеризовать внешние свойства систем, их стойкость к различным атакам, а также может быть весьма полезной при синтезе новых СВИ. Однако ввиду ограничений на допустимый объём статей эти вопросы будут рассмотрены в отдельной работе.

1. Модели систем встраивания информации: анализ текущего положения дел

1.1. Основные требования

Основными трудностями, возникающими при построении обобщённой модели СВИ, являются:

- объединение стеганографических систем и систем встраивания ЦВЗ в одной модели;
- унификация типа контейнера (аудио, изображение, видео и пр.);
- формальное однозначное определение всех элементов, которые могут присутствовать в каждой отдельной системе.

Если второе и третье требования интуитивно понятны и логичны, то первое на первый взгляд не является очевидным и требует некоторых разъяснений. Зачем нужна единая модель для систем, используемых на практике для решения разных задач? Действительно, подавляющее большинство известных моделей предназначено только для систем ЦВЗ [3, 5, 10–13] или только для стеганографических систем [14–15].

Пожалуй, наиболее чётко различия и общность ЦВЗ и стеганографии разъясняются в книге [3], являющейся на данный момент одной из наиболее авторитетных монографий в области встраивания информации. В числе прочего в этой книге приводится простая классификация методов встраивания информации на 4 типа (см. табл. 1). Первая строка данной таблицы отражает принадлежность к стеганографии, а первый столбец – к ЦВЗ. Как следует из таблицы, принадлежность какой-либо системы к системам встраивания ЦВЗ не означает, что эта система не является стеганографической. Типичным примером систем, относящихся к обоим классам, являются системы цифровых отпечатков пальцев, в которых осуществляется распространение цифровых данных, снабжённых скрытыми метками адресата, предназначенными для защиты информации от несанкционированного распространения.

Табл. 1. Классификация методов встраивания информации [3]

	Сообщение связано с контейнером	Сообщение не связано с контейнером
Факт наличия сообщения сокрыт	Стеганографическое встраивание ЦВЗ	Скрытая (стеганографическая) передача информации
Факт наличия сообщения известен	Нестеганографическое встраивание ЦВЗ	Открытая опосредованная передача информации

Существуют и иные мотивы совместного рассмотрения двух типов систем. Дело в том, что с ними связано множество общих понятий, а кроме того, многие алгоритмы встраивания и извлечения информации используются в системах двух данных типов (простейшим таким примером является встраивание информации в наименее значимые биты, применяемое как для защиты контейнера, так и для скрытой передачи информации).

Чтобы проиллюстрировать трудности, возникающие при описании различных по внутреннему содержанию систем, рассмотрим два простых примера.

Пример 1. Система стеганографического встраивания в наименее значимые биты аудиосигнала. На вход данной системе подаются аудиосигнал и двоичный вектор, элементы которого заменяют младшие биты отсчётов сигнала в порядке, определённом ключом системы. Для извлечения осуществляется считывание младших битов принятого сигнала в заданных позициях.

Пример 2. Простейшее встраивание ЦВЗ в фазу спектра изображения. Входными данными являются полутоновое изображение-контейнер, а также ЦВЗ, представляющий собой изображение того же размера. Далее контейнер подвергается дискретному преобразованию Фурье (ДПФ) с последующим расчётом фазы спектра, представляемой в виде матрицы значений. Далее происходит замена компонент данной матрицы ненулевыми отсчётами маски ЦВЗ, предварительно подвергшейся хаотичному перемешиванию в соответствии с ключом, после чего производится обратное преобразование Фурье. При извлечении информации производятся те же действия по отысканию фазы спектра, из которой формируется оценённая маска ЦВЗ, которая затем сравнивается с оригиналом для формирования итогового ответа на вопрос о наличии конкретного встроенного ЦВЗ в анализируемом изображении.

Две эти системы отличаются практически всем: типом сигнала-контейнера, формой встраиваемой информации, областью, в которой осуществляется встраивание информации, результатом работы системы. И единообразное описание этих систем на первый взгляд представляется затруднительным.

1.2. Анализ существующих моделей

Известно более двух десятков работ, в которых осуществляются попытки обобщения некоторого множества систем встраивания информации при помощи единой модели. Большая часть таких работ издана в период наиболее бурного стартового развития области встраивания информации – с 1998 по 2005 гг. [1, 3, 5, 6, 10–17] (монографии [3] и [10] изданы позднее, однако развивают более ранние работы тех же авторов). Впоследствии авторы этих моделей, стоявшие у истоков ЦВЗ и стеганографии, сосредоточились на разработке конкретных систем и алгоритмов, а также частично сместили свои интересы в область ставшей популярной цифровой криминалистики (digital forensics). Пришедшие же им на смену исследователи долгие годы не могли предложить ничего нового. Лишь в 2010-х годах. группой авторов Nyeem, Boles, Boyd были опубликованы две весьма качественные работы [18–19], в которых приводится очень содержательный критический обзор известных схем, а также вводится собственная модель, хорошо продуманная, однако тоже, увы, не лишённая некоторых недостатков.

Перечислим наиболее существенные ограничения существующих моделей СВИ.

1. Все упомянутые модели, кроме [16, 17], предназначены для описания или стеганографических систем, или систем встраивания ЦВЗ; более общий случай произвольной системы встраивания информации не рассматривается.

2. В моделях [1, 3, 6, 10–16, 18–19] не формализованы такие детали подсистем встраивания и извлечения информации, как анализ контейнера, кодирование и декодирование встраиваемой и извлекаемой информации и пр.

3. Не рассматривается весь спектр вариантов функционирования СВИ, определяемых свойствами СВИ. Вместо этого в моделях [1, 3, 5, 10, 11, 12, 13,

14, 15, 17] рассматриваются лишь несколько наиболее часто используемых вариантов.

4. Модели [6, 10, 11, 15] ограничиваются описанием процессов, составляющих СВИ, и не позволяют перейти от описания внутренней структуры к описанию внешних свойств.

5. Некоторые модели (в частности, [11, 18–20]) предназначены только для контейнеров определённого типа (обычно звуковых сигналов или изображений).

6. Ни одна из существующих моделей не получила повсеместного распространения и не является принятым математическим фундаментом, на котором строились бы новые достижения в области встраивания данных. Также можно добавить, что при описании новых систем встраивания информации авторы чаще всего используют свою модель и свои обозначения.

В результате ни одна из упомянутых моделей не позволяет единообразно описать обе системы, приведённые в качестве примера в подпункте 1.1. Однако модель, предлагаемая в данной статье, позволяет это сделать, что будет показано в пункте 4.

2. Описание предлагаемой модели системы встраивания информации

Предлагаемая *модель системы встраивания информации (МСВИ)* представляет собой совокупность данных и процессов (функций) их обработки. Одним из важнейших понятий, использованных при создании данной модели, является *внутренняя информация* (ВИ), под которой понимается встраиваемая в контейнер (и впоследствии извлекаемая из него) информация. Внутренней она является по отношению к контейнеру, поскольку передаётся внутри него.

Ключевая идея, на которой построена данная модель, заключается во введении трёх эквивалентных друг другу форм представления внутренней информации: двоичный вектор, цифровой сигнал и матрица признаков. Первая форма соответствует, например, сообщению, передаваемому внутри стеганографического контейнера, или цифровому коду защитного ЦВЗ. Вторая форма соответствует традиционной форме контейнера, в который встраивается информация, то есть это может быть цифровое аудио, изображение, видео и пр. Третья форма индивидуальна для каждой системы и является представлением, в котором непосредственно происходит встраивание информации, то есть модификация данных контейнера. То есть признаками являются некоторые производные компоненты, которые подвергаются модификации и по которым впоследствии определяется наличие в сигнале встроенной информации и/или её содержание. Термин «признак» используется для определения близкого понятия в книге [5], кроме того, это понятие перекликается с ключевым термином машинного обучения (но не эквивалентен ему). В процессе работы системы осуществляется преобразование внутренней информации и некоторых других данных из одной формы в другую.

При описании модели будут использоваться следующие обозначения:

- $\mathbb{B}^n = \mathbb{N}_0 \cap [0, 2^n - 1]$ – множество целых неотрицательных чисел, для хранения которых достаточно n бит. Частным случаем является множество $\mathbb{B} = \mathbb{B}^1$, состоящее из нуля и единицы;
- $\mathbb{S}^m_{[N_1 \times N_2 \times .. \times N_m]}$ – m-мерная матрица размерами $N_1 \times N_2 \times \ldots \times N_m$ из элементов некоторого числового множества $\mathbb{S}$;
- $\mathbb{S}^m_{[]}$ – m-мерная матрица неопределёных размеров из элементов некоторого числового множества $\mathbb{S}$ (употребляется, когда размеры матрицы не важны в рассматриваемом контексте).

Введённые обозначения позволяют определить множества, соответствующие трём вышеупомянутым формам внутренней информации. Так, первой форме двоичного вектора соответствует множество $\mathbb{B}^1_{[N_b]}$, где N_b – длина вектора. Под *m-мерным цифровым сигналом* будем понимать величину $X \in \mathbb{X}^m_{[]}$, представляющую собой m-мерную матрицу, элементы которой определены на множестве $\mathbb{X} \subseteq \mathbb{R}$. Само множество $\mathbb{X}^m_{[]}$ будем называть *множеством цифровых сигналов*. Наконец, под *матрицей признаков* $y \in \mathbb{Y}^l_{[]}$ будем понимать l-мерную матрицу, элементы которой определены на множестве $\mathbb{Y} \subseteq \mathbb{C}$. Само множество $\mathbb{Y}^l_{[]}$ мы будем называть *множеством признаков*.

2.1. Описание основных элементов модели

Цифровой сигнал до встраивания в него внутренней информации будем называть *контейнером* (обозначение $C \in \mathbb{X}^m_{[]}$), после встраивания – *носителем информации* (обозначение $C^W \in \mathbb{X}^m_{[]}$). На этапе извлечения информации используется *принятый носитель информации* $\widetilde{C^W} \in \mathbb{X}^m_{[]}$, который может отличаться от C^W вследствие искажений при передаче данных.

Важным элементом любой системы является *составной ключ СВИ* $\mathbf{k} = (k^s, k^p) \in K = K^s \times K^p$, включающий в себя как *секретный ключ* $k^s \in K^s \subseteq \mathbb{B}^1_{[N_k]}$ (secret key), обеспечивающий защищённость СВИ, так и *открытые параметры* $k^p \in K^p$ (public parameters) функций и алгоритмов, входящих в её состав. Структура множества K^p не конкретизируется на уровне модели, а определяется для отдельных систем.

Внутреннюю информацию на схемах характеризуют следующие обозначения: $\mathbf{b}, \mathbf{b}^R \in \mathbb{B}^1_{[N_b]}$ (в форме двоичного вектора); $W, W^R \in \mathbb{X}^m_{[]}$ (в форме сигнала); $\Omega, \widetilde{\Omega} \in \mathbb{Y}^l_{[]}$ (в форме матрицы признаков). Названия, соответствующие этим и другим обозначениям, приведены в табл. 2.

Как уже было показано в рассмотренных выше примерах, в некоторых системах внутренняя информация изначально представляется в виде вектора **b**, а в некоторых – сразу в виде сигнала *W*. Это обусловливает необходимость введения понятия *начальной формы внутренней информации*, под которым понимается одно из множеств: $\mathbb{B}^1_{[N_b]}$ (если внутренняя информация изначально представлена в виде вектора $\mathbf{b}\in\mathbb{B}^1_{[N_b]}$) или $\mathbb{X}^m_{[]}$ (если она изначально имеет вид $W\in\mathbb{X}^m_{[]}$).

Табл. 2. Список обозначений данных в МСВИ

Обозначение	Название	Аналоги в англоязычной литературе
$C\in\mathbb{X}^m_{[]}$	Контейнер	Host asset [5], cover work [3], cover object [4]
$\mathbf{b}\in\mathbb{B}^1_{[N_b]}$	Встраиваемая информация	Information message [5], secret message [3]
$\mathbf{b}^{\mathbf{R}}\in\mathbb{B}^1_{[N_b]}$	Извлечённая информация	Recovered {название **b** }
$W\in\mathbb{X}^m_{[]}$	Встраиваемый сигнал	Watermarking signal [5], encoded message
$C^W\in\mathbb{X}^m_{[]}$	Носитель информации	Watermarked asset [5], watermarked work [3], stego work [3], stego object [4]
$\widetilde{C^W}\in\mathbb{X}^m_{[]}$	Принятый носитель информации	Transformed (received) watermarked asset [5]
$W^R\in\mathbb{X}^m_{[]}$	Извлечённый сигнал	Recovered {название *W*}
$k^s\in K^s\subseteq\mathbb{B}^1_{[N_k]}$	Секретный ключ СВИ	Watermarking key, secret key, key, stego key
$k^p\in K^p$	Открытые параметры СВИ	Public parameters
$\mathbf{k}\in K$	Составной ключ СВИ	–
$\xi\in\mathbb{B}$	Результат обнаружения	Detection result [5]
$\lambda\in\Lambda$	Параметры контейнера	–
$\widetilde{\lambda}\in\Lambda$	Оценённые параметры контейнера	–
$\Omega\in\mathbb{Y}^l_{[]}$	Матрица признаков встраиваемой информации	–
$\widetilde{\Omega}\in\mathbb{Y}^l_{[]}$	Матрица признаков извлечённой информации	–
$f\in\mathbb{Y}^l_{[]}$	Матрица признаков контейнера	Host feature set [5]
$f^W\in\mathbb{Y}^l_{[]}$	Матрица признаков носителя информации	–
$\widetilde{f^W}\in\mathbb{Y}^l_{[]}$	Матрица признаков принятого носителя информации	–
$\psi\in\Psi$	Дополнение матрицы признаков контейнера	–

Преобразование внутренней информации из одной формы в другую осуществляется при помощи следующих функций:

– функции кодирования информации в виде цифрового сигнала

$$\mathcal{P}:\mathbb{B}^1_{[N_b]}\times K\mapsto\mathbb{X}^m_{[]}; \quad (1)$$

– функции кодирования информации в виде матрицы признаков

$$\mathcal{P}_f:\mathbb{B}^1_{[N_b]}\times K\mapsto\mathbb{Y}^l_{[]}; \quad (2)$$

– функции преобразования сигнала в матрицу признаков, которая чаще всего имеет вид

$$\mathcal{F}:\mathbb{X}^m_{[]}\mapsto\mathbb{Y}^l_{[]} \quad (3)$$

и реже

$$\mathcal{F}:\mathbb{X}^m_{[]}\mapsto\mathbb{Y}^l_{[]}\times\Psi, \quad (4)$$

а также обратных им функций $\mathcal{P}^{-1},\mathcal{P}_f^{-1},\mathcal{F}^{-1}$.

Связь различных форм представления внутренней информации проиллюстрирована на рис. 1.

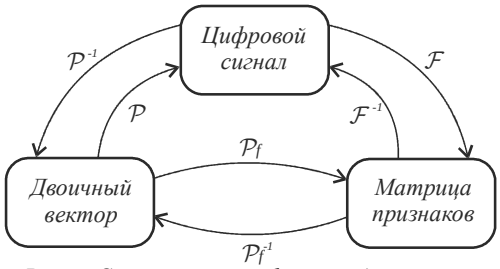

Рис. 1. Связь различных форм представления внутренней информации

В табл. 3 показано, какие формы внутренней информации используются на различных стадиях функционирования СВИ. Наличие различных вариантов в одной строке табл. 3 обусловлено отличиями разных систем. Для одной конкретной системы на каждой из стадий всегда используется только одна форма. Следует отметить, что результатом работы всей системы помимо внутренней информации (в двух формах, отмеченных в таблице) может являться величина $\xi\in\mathbb{B}$ – *результат обнаружения наличия встроенной информации*. Более подробно она будет рассмотрена ниже.

Как уже отмечалось ранее, форма матрицы признаков существует для всех СВИ, поскольку именно в этой форме осуществляется собственно встраивание и извлечение информации; в то время как одна из двух других форм в ряде систем не используется.

Состав используемых в конкретной системе форм внутренней информации определяется на основе двух показателей, которые будем называть *предикатом начальной формы внутренней информации:*

$$\pi_{bw}=\begin{cases}true, & \text{если начальная форма ВИ}-\mathbb{B}^1_{[N_b]},\\ false, & \text{если начальная форма ВИ}-\mathbb{X}^m_{[]}\end{cases}$$

и *предикатом способа кодирования информации*:

$$\pi_{\mathcal{P}}=\begin{cases}true, & \text{если информация кодируется в }\mathbb{X}^m_{[]},\\ false, & \text{если информация кодируется в }\mathbb{Y}^l_{[]}.\end{cases} \quad (5)$$

На рис. 2 представлена общая схема обработки информации в СВИ согласно предлагаемой модели.

Табл. 3. Формы внутренней информации, используемые на различных стадиях обработки данных в СВИ

		Форма внутренней информации		
		Бинарный вектор	Цифровой сигнал	Матрица признаков
Стадия обработки данных в СВИ	Инициализация	✓	✓	
	Встраивание информации			✓
	Передача контейнера		✓	
	Обнаружение информации	✓	✓	✓
	Формирование результата	✓	✓	

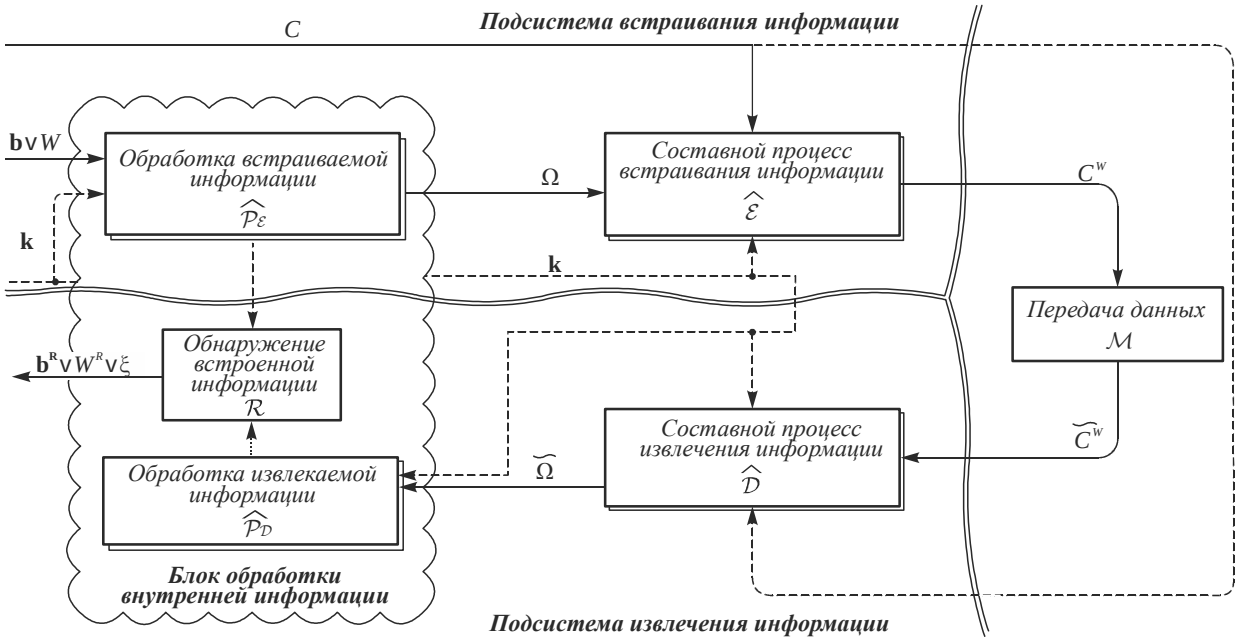

Рис. 2. Общая схема обработки данных согласно МСВИ

На схеме выделены подсистемы встраивания и извлечения информации, а также канал передачи данных. На этой и последующих схемах СВИ (рис. 3–5) стрелками обозначаются потоки данных, а прямоугольниками – процессы обработки данных. Сплошными стрелками обозначаются обязательные потоки данных, существующие во всех системах, а штриховыми – опциональные, которые могут существовать в одних системах и отсутствовать в других. Кружком на рис. 4–5 отмечены объединяющиеся потоки данных, а ромбом на рис. 5 – разветвляющиеся (в зависимости от условия, согласованного с предикатами (4)-(5)). Двойные линии на рис. 2 разделяют подсистемы встраивания и извлечения информации, а также процесс передачи данных, не входящих ни в одну из них. Волнистой рамкой на том же рисунке выделен блок процессов обработки внутренней информации, раскрываемый подробнее на рис. 5. Двойными рамками на рис. 2 помечаются составные процессы, раскрываемые на последующих рисунках. Так, схема на рис. 3 описывает атомарные процессы обработки данных, входящие в состав выделенного на общей схеме составного процесса встраивания информации, а рис. 4 – содержимое составного процесса извлечения информации.

Введённых на данный момент понятий достаточно, чтобы прокомментировать общую схему СВИ (рис. 2). Итак, на вход любой системы подаются контейнер C, внутренняя информация в форме $\mathbf{b}$ или W, а также ключ $\mathbf{k}$, который теоретически может отсутствовать, но для практически значимых систем, разумеется, является обязательным элементом. Далее на предварительном этапе (до встраивания) происходит преобразование внутренней информации в форму матрицы признаков Ω, которое может осуществляться с использованием ключа $\mathbf{k}$. Полученная матрица признаков Ω вместе с контейнером подаются на вход составного процесса встраивания информации, результатом работы которого является носитель информации C^W. Далее происходит его передача подсистеме извлечения, в результате которой могут произойти непреднамеренные искажения или преднамеренные атаки. Далее принятый носитель информации $\widetilde{C^W}$ попадает на вход составного процесса извлечения информации (наряду с ним в этом блоке может также использоваться и исходный контейнер, переданный по закрытым каналам до начала работы системы). Результатом работы последнего является *оценённая матрица признаков встроенной информации* $\widetilde{\Omega}$. Далее с её помощью осуществляется формирование результата всей системы, которым может являться *извлечённая информация* $\mathbf{b}^R$ (верхний индекс R является сокращением от англ. “recovered” – восстановленная, проявленная) или *извлечённый сигнал* W^R (в зависимости от начальной

формы внутренней информации), либо результат обнаружения внутренней информации – величина $\xi \in \mathbb{B}$, принимающая значения

$$\xi = \begin{cases} 1, & \text{если } \widetilde{C^W} \text{ содержит } \mathbf{b} \left(\text{или } W\right), \\ 0, & \text{если } \widetilde{C^W} \text{ не содержит } \mathbf{b} \left(\text{или } W\right). \end{cases} \quad (6)$$

Формирование величины ξ рассматривается в следующем разделе.

Схемы на рис. 2–5 позволяют легко определить вид функций, соответствующих отдельным процессам. Так, согласно общей схеме составной процесс встраивания информации может описываться функциями следующего вида (в зависимости от использования ключа **k**):

$$\hat{\mathcal{E}} : \mathbb{X}_{[]}^m \times \mathbb{Y}_{[]}^l \times K \mapsto \mathbb{X}_{[]}^m, \; C^W = \hat{\mathcal{E}}\left(C, \Omega, \mathbf{k}\right),$$

$$\hat{\mathcal{E}} : \mathbb{X}_{[]}^m \times \mathbb{Y}_{[]}^l \mapsto \mathbb{X}_{[]}^m, \; C^W = \hat{\mathcal{E}}\left(C, \Omega\right).$$

Аналогичным образом существуют четыре варианта составного процесса извлечения информации:

$$\hat{\mathcal{D}} : \mathbb{X}_{[]}^m \times \mathbb{X}_{[]}^m \times K \mapsto \mathbb{Y}_{[]}^l, \; \widetilde{\Omega} = \hat{\mathcal{D}}\left(\widetilde{C^W}, C, \boldsymbol{k}\right),$$

$$\hat{\mathcal{D}} : \mathbb{X}_{[]}^m \times \mathbb{X}_{[]}^m \mapsto \mathbb{Y}_{[]}^l, \; \widetilde{\Omega} = \hat{\mathcal{D}}\left(\widetilde{C^W}, C\right),$$

$$\hat{\mathcal{D}} : \mathbb{X}_{[]}^m \times K \mapsto \mathbb{Y}_{[]}^l, \; \widetilde{\Omega} = \hat{\mathcal{D}}\left(\widetilde{C^W}, \boldsymbol{k}\right),$$

$$\hat{\mathcal{D}} : \mathbb{X}_{[]}^m \mapsto \mathbb{Y}_{[]}^l, \; \widetilde{\Omega} = \hat{\mathcal{D}}\left(\widetilde{C^W}\right).$$

2.2. Детализация составных процессов МСВИ

Как показывает рис. 3, составной процесс встраивания информации включает в себя следующие атомарные процессы:

- анализ сигнала (контейнера) $\mathcal{A}$,
- преобразование сигнала в матрицу признаков $\mathcal{F}$ и обратное ему $\mathcal{F}^{-1}$,
- встраивание информации на множестве признаков $\mathcal{E}$.

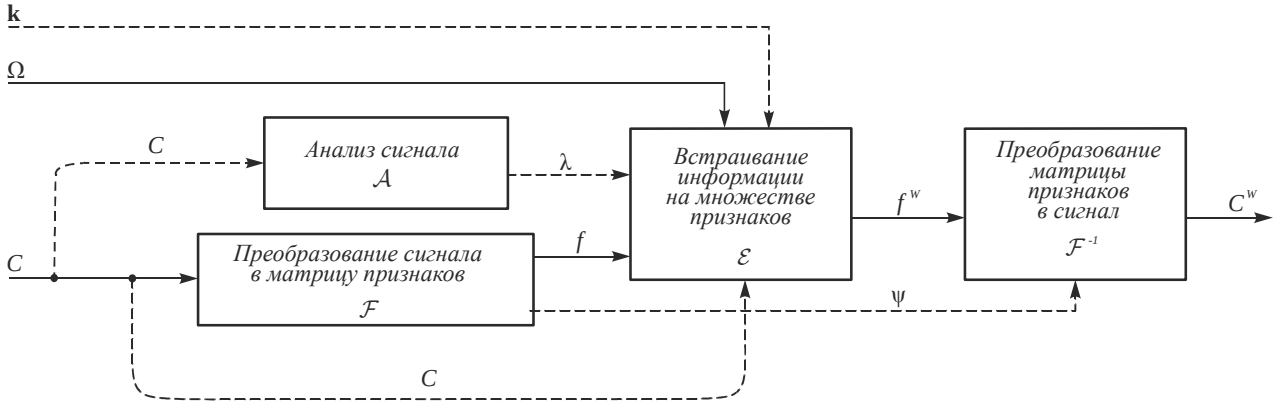

Рис. 3. Детализация составного процесса встраивания информации

Под анализом сигнала понимается процесс оценивания числовых характеристик этого сигнала, которые составляют множество Λ, определяемое индивидуально для каждой СВИ. Например, анализ контейнера-изображения может состоять в отыскании координат его характеристических точек, осуществляемом при помощи уголкового детектора. Процесс анализа сигнала является опциональным и присутствует далеко не у всех систем.

Процессы $\mathcal{F}$ и $\mathcal{F}^{-1}$, уже упомянутые выше, предназначены соответственно для преобразования сигнала в матрицу признаков и обратного преобразования. Особенностью этих процессов является возможное использование величины $\psi \in \Psi$, являющейся частью результата функции $\mathcal{F}$ и дополнительным аргументом функции $\mathcal{F}^{-1}$. Эту величину мы назовём *дополнением матрицы признаков контейнера*, которое в совокупности с f позволяет безошибочно восстановить исходный преобразованный сигнал. В ряде систем в качестве матрицы признаков используется полный набор данных, необходимых для восстановления сигнала (например, все пространственные отсчёты изображения или все компоненты какого-либо обратимого спектрального преобразования). Для таких систем величина ψ не определена.

Процесс $\mathcal{E}$ заключает в себе собственно встраивание информации, то есть слияние матриц признаков контейнера f и внутренней информации Ω в единой матрице f^W.

Схема на рис. 3 показывает, что для встраивания информации необходимо преобразовать контейнер C в матрицу признаков f. В некоторых системах также осуществляется анализ *параметров контейнера* λ. Полученные величины вместе с Ω и **k** используются при встраивании информации на множестве признаков, результат которого на заключительном этапе преобразуется в форму цифрового сигнала для передачи принимающей стороне.

Содержание составного процесса извлечения информации легко понять по схеме на рис. 4.

Отметим лишь, что анализ сигнала на этапе извлечения может выполняться либо по исходному контейнеру (в случае его предварительной передачи подсистеме извлечения информации), либо по принятому носителю информации.

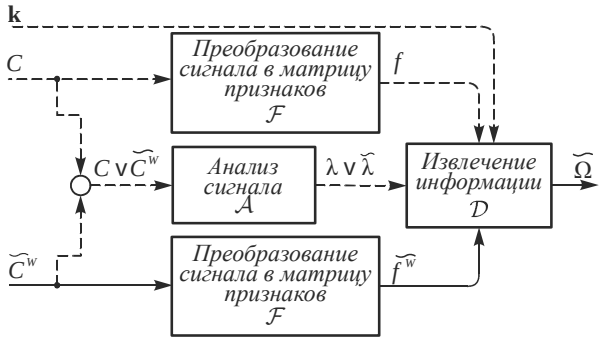

Рис. 4. Детализация составного процесса извлечения информации

В последнем случае результатом будут являться оценённые параметры контейнера $\widetilde{\lambda}$, в общем случае не совпадающие с λ.

Собственно извлечение информации реализуется в процессе $\mathcal{D}$, результатом которого является оценённая матрица признаков встроенной информации $\widetilde{\Omega}$. Следует отметить, что в результате двух функций $\mathcal{F}$, используемых в составе рассматриваемого составного процесса, не рассчитываются соответствующие дополнения, поскольку они впоследствии не требуются. Наконец, блок обработки внутренней информации, изображённый на рис. 5, включает в себя процессы её преобразования из одной формы в другую в обеих подсистемах. Для этого используются ранее введённые функции кодирования-декодирования $\mathcal{P}, \mathcal{P}_f, \mathcal{P}^{-1}, \mathcal{P}_f^{-1}$, состав которых определяется двумя предикатами, также упоминавшимися ранее, а также функции $\mathcal{F}$ и $\mathcal{F}^{-1}$.

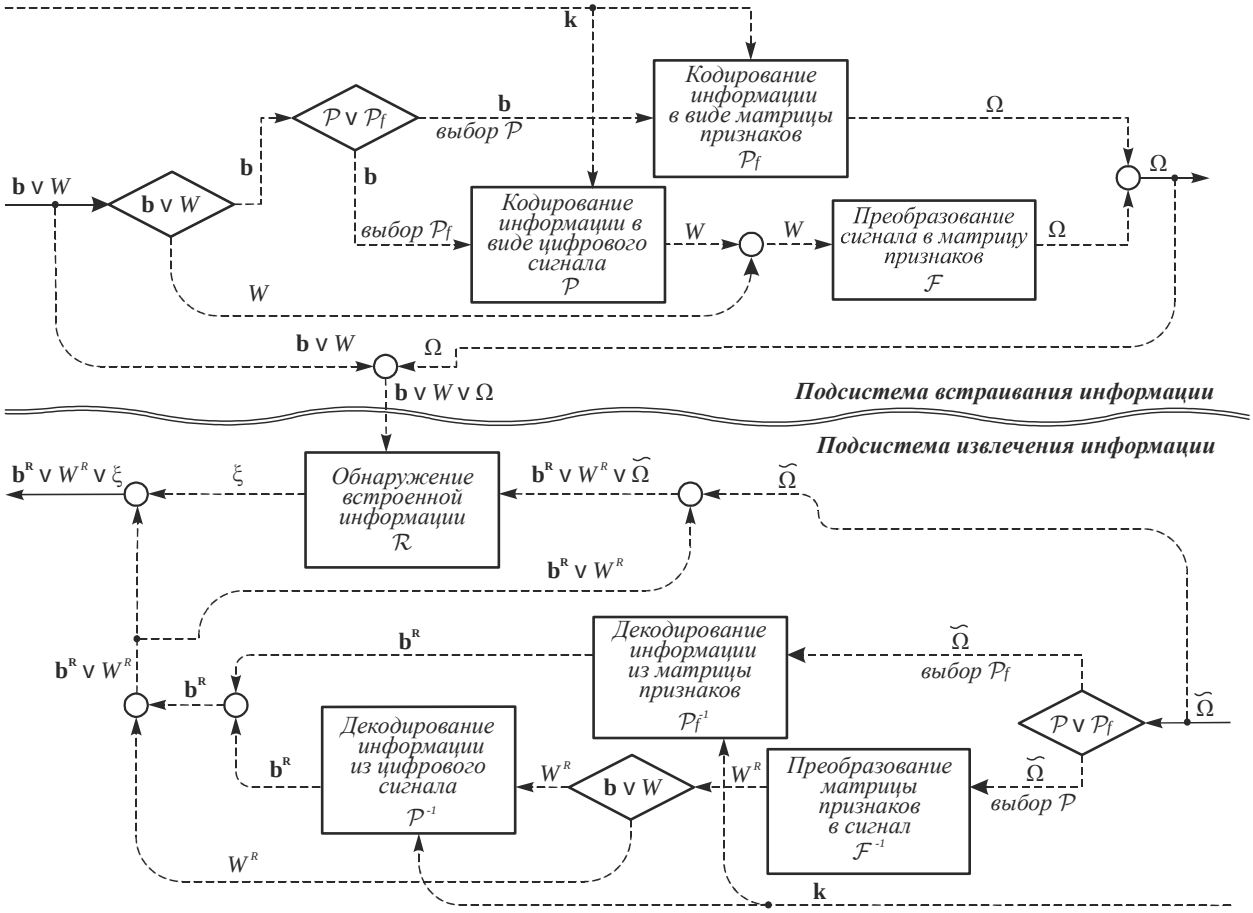

Рис. 5. Блок обработки внутренней информации

Помимо этих процессов, в данный блок может также входить функция *обнаружения встроенной информации* $\mathcal{R}$ (действующая в подсистеме извлечения), которая в зависимости от *формы* внутренней информации, *используемой при детектировании*, может иметь одну из следующих форм:

$$\mathcal{R}: \mathbb{B}^1_{[N_b]} \times \mathbb{B}^1_{[N_b]} \mapsto \mathbb{B},\ \xi = \mathcal{R}\left(\mathbf{b}, \mathbf{b}^{\mathbf{R}}\right), \tag{7}$$

$$\mathcal{R}: \mathbb{X}^m_{[]} \times \mathbb{X}^m_{[]} \mapsto \mathbb{B},\ \xi = \mathcal{R}\left(W, W^R\right), \tag{8}$$

$$\mathcal{R}: \mathbb{Y}^l_{[]} \times \mathbb{Y}^l_{[]} \mapsto \mathbb{B},\ \xi = \mathcal{R}\left(\Omega, \widetilde{\Omega}\right). \tag{9}$$

В каждом из этих случаев функция $\mathcal{R}$ имеет вид пороговой обработки

$$\mathcal{R}\left(x, x^R\right) = \begin{cases} 1, & \rho\left(x, x^R\right) \geq T_\rho, \\ 0, & \rho\left(x, x^R\right) < T_\rho, \end{cases} \tag{10}$$

где x и x^R – встроенная и извлечённая информации в форме, используемой при детектировании, $T_\rho \in \mathbb{R}$ – порог, а $\rho(x, x^R)$ – некоторая функция близости величин x и x^R, определяемая индивидуально для каждой конкретной системы.

Функция ρ и порог T_ρ определяются при проектировании конкретной системы, однако можно выделить некоторые общие закономерности:

1. Для СВИ, результатом работы которых является $\mathbf{b}^{\mathrm{R}}$ или W^R, формой детектирования является начальная форма внутренней информации.

2. Для СВИ с формой детектирования $\mathbb{B}^1_{[N_b]}$ зачастую используется функция ρ, равная доле правильно извлечённых бит:

$$\rho\left(\mathbf{b},\mathbf{b}^{\mathbf{R}}\right)=\frac{1}{N_b}\sum_{i=0}^{N_b-1}\left(1-b_i\oplus b_i^R\right). \qquad (11)$$

3. Для СВИ с формой детектирования $\mathbb{X}^m_{[]}$ функция ρ может быть задана как один из стандартных показателей качества, используемых для m-мерных сигналов. К примеру, для полутоновых изображений, принадлежащих множеству $\mathbb{X}^m_{[]}=\left(\mathbb{B}^8\right)^2_{[N_1\times N_2]}$ (то есть множеству двумерных матриц размерами $N_1\times N_2$ из целых чисел в диапазоне от 0 до 255), в качестве функции близости можно использовать *PSNR* двух сигналов [21]:

$$\rho\left(W,W^R\right)=PSNR\left(W,W^R\right)=10lg\frac{255^2}{\varepsilon^2_{кв}\left(W,W^R\right)}, \qquad (12)$$

где $\varepsilon^2_{кв}\left(W,W^R\right)$ – среднеквадратичная ошибка.

4. Для систем, в которых формой детектирования является $\mathbb{Y}^l_{[]}$, вид функции ρ существенно зависит от структуры самого множества $\mathbb{Y}^l_{[]}$. Так, зачастую признаки отражают энергетические характеристики сигнала, а значит, отсчёты матрицы признаков с различными индексами могут иметь разную значимость в отличие от отсчётов цифровых сигналов.

В заключение необходимо привести два важных замечания. Во-первых, как видно из схемы на рис. 5, функция обнаружения встроенной информации не является обязательным элементом СВИ и в ряде конкретных систем может отсутствовать. В этом случае результатом работы является извлечённая внутренняя информация в форме $\mathbf{b}^{\mathrm{R}}$ или W^R. Во-вторых, как показано на схеме, преобразование $\mathcal{F}^{-1}$ осуществляется без использования дополнения. Дело в том, что ветвь схемы, использующая $\mathcal{F}^{-1}$, существует только в тех системах, где матрица признаков является достаточной для обратного преобразования (и дополнение не определено). В противном случае это дополнение было бы неоткуда получить подсистеме извлечения информации.

3. Параметрическое описание СВИ с использованием предложенной модели

МСВИ, проиллюстрированная на рис. 2–5, содержит ряд опциональных потоков данных, которые должны быть конкретизированы при описании конкретной системы. Однозначным образом схему конкретной системы определяют следующие признаки:

1) значение предиката π_{bW};
2) значение предиката $\pi_{\mathcal{P}}$ (в случае, если если $\pi_{\mathrm{bw}}=true$);
3) факт использования секретного ключа; и если он имеет место, то в каких из трёх возможных процессов: $\mathcal{E}$, $\mathcal{D}$, $\mathcal{P}$ (или $\mathcal{P}_f$);
4) наличие процесса анализа сигнала;
5) достаточность матрицы признаков для восстановления соответствующего ей сигнала;
6) факт использования контейнера C при извлечении информации (в обобщённом процессе $\widehat{\mathcal{D}}$);
7) тип подсистемы извлечения информации – детектор или декодер;
8) форма детектирования (если подсистема извлечения информации типа детектор);
9) наличие дополнения матрицы признаков.

Схема СВИ, для которой определены вышеуказанные признаки, не содержит опциональных потоков данных. Однако нельзя сказать, что они полностью характеризуют систему, поскольку неопределёнными остаются многие процессы и множества, на которых определены используемые в системе данные.

Ниже представлен перечень процессов, множеств, значений предикатов МСВИ, уточнение которых полностью определяет модель *конкретной* системы встраивания информации. Мы будем называть элементы данного списка *параметрами МСВИ.*

1. Тип сигнала, в который встраивается внутренняя информация – множество $\mathbb{X}^m_{[]}$.
2. Значение предиката π_{bw}.
3. Длина встраиваемого битового вектора N_b (если $\pi_{\mathrm{bw}}=true$).
4. Состав полного ключа СВИ – множество $K=K^s\times K^p$.
5. Пара функций преобразования между сигналом и матрицей признаков: $\mathcal{F}$ и $\mathcal{F}^{-1}$, а также множества признаков $\mathbb{Y}^l_{[]}$ и дополнений Ψ.
6. Наличие функции анализа сигнала $\mathcal{A}$ и её вид.
7. Функция $\mathcal{E}$ встраивания информации в матрицу признаков.
8. Функция $\mathcal{D}$ извлечения информации из матрицы признаков.
9. Значение предиката способа кодирования информации $\pi_{\mathcal{P}}$ (если $\pi_{\mathrm{bw}}=true$).
10. Вид функции кодирования информации $\mathcal{P}$ (или $\mathcal{P}_f$ – зависит от $\pi_{\mathcal{P}}$) (если $\pi_{\mathrm{bw}}=true$).
11. Тип данных, являющихся результатом работы подсистемы извлечения: извлечённая внутренняя информация в форме $\mathbf{b}^{\mathbf{R}}$ (или W^R в зависимости от π_{bw}) или результат обнаружения ξ.
12. Форма детектирования: $\mathbb{B}^1_{[\mathrm{N_b}]}$, $\mathbb{X}^m_{[]}$ или $\mathbb{Y}^l_{[]}$.

13. Функция $\mathcal{P}^{-1}$ (или $\mathcal{P}_f^{-1}$ в зависимости от $\pi_{\mathcal{P}}$) (если форма детектирования – $\mathbb{B}^1_{[\mathrm{N_b}]}$ и/или результатом работы подсистемы извлечения является $\mathbf{b}^{\mathbf{R}} \in \mathbb{B}^1_{[\mathrm{N_b}]}$).
14. Функция обнаружения наличия встроенной информации $\mathcal{R}$.

Данный перечень можно рассматривать и как стандартизованное описание СВИ (которое мы будем называть *параметрическим описанием*), и как пошаговое руководство при проектировании новой СВИ.

4. Примеры описания систем встраивания информации при помощи предложенной модели

Рассмотрим три примера описаний различных СВИ при помощи разработанной модели. Первые две системы кратко рассматривались в пункте 1, поэтому для них приведём только параметрические описания.

4.1. Стеганографическое НЗБ-встраивание

1. $\mathbb{X}^m_{[]} = \left(\mathbb{B}^{16}\right)^1_{[N]}$ – множество одномерных векторов из N 16-битных целых чисел (для хранения одноканального аудиосигнала, как правило, используется 16 бит на отсчёт).
2. $\pi_{\mathrm{bw}} = true$.
3. $N_b \le N$.
4. $K = \mathbb{R}^1_{[N_k]}$, то есть сам ключ имеет вид $\mathbf{k} = \{k_i\}_{i=0}^{N_k-1}$.
5. $\mathcal{F}(\mathrm{x}) = x$, $\mathbb{Y}^l_{[]} = \left(\mathbb{B}^{16}\right)^1_{[N]}$, дополнения нет.
6. –
7. $$f^W(n) = \begin{cases} f(n), & n \ne k_i, i = 0..N_k - 1, \\ 2\left\lfloor \dfrac{f(n)}{2} \right\rfloor + \Omega(n), & n = k_i, \end{cases}$$
8. $\widetilde{\Omega}(n) = \widetilde{f^W}(n) (\mathrm{mod}\, 2)$.
9. $\pi_{\mathcal{P}} = true$. (на самом деле его значение не важно, поскольку $\mathbb{X}^m_{[]} = \mathbb{Y}^l_{[]}$).
10. $$\Omega(n) = \begin{cases} 0, & n \ne k_i, i = 0..N_k - 1, \\ b_i, & n = k_i. \end{cases}$$
11. $\mathbf{b}^{\mathbf{R}}$.
12. $\mathbb{B}^1_{[\mathrm{N_b}]}$.
13. $b_i^R = \widetilde{\Omega}(k_i)$ /
14. (10)–(11).

4.2. Простейший ЦВЗ в спектральной области

Для простоты описания данной системы примем в качестве способа перемешивания отсчётов маски ЦВЗ циклический сдвиг на вектор $\mathbf{k} = (k_1, k_2)$, а также ограничимся множеством значений $\{0, 1, 2\}$ для отсчётов встраиваемого сигнала, причём будем считать, что в случае нуля встраивания не производится, а в случае значения 2 встраивается значение –1.

1. $\mathbb{X}^m_{[]} = \left(\mathbb{B}^8\right)^2_{[N_1 \times N_2]}$.
2. $\pi_{\mathrm{bw}} = false$.
3. –
4. $K = \mathbb{Z} \cap [0, N_1 - 1] \times \mathbb{Z} \cap [0, N_2 - 1]$; $\mathbf{k} = (k_1, k_2)$.
5. $\mathbb{Y}^l_{[]} = \Psi = \mathbb{R}^2_{[N_1 \times N_2]}$,

   $\mathcal{F}(x) = DFT(x)$, $\mathcal{F}^{-1}(x) = DFT^{-1}(x)$,

   где $DFT(x)$ – ДПФ сигнала x;

   $f_x = \arg \mathcal{F}(x)$, $\psi_x = \arg \mathcal{F}(x)$,

   где f_x, ψ_x – соответственно матрица признаков сигнала x и её дополнение.
6. –
7. $$f^W(n_1, n_2) = \begin{cases} \mathrm{sign}\, f(n_1, n_2) \times \\ \times \max\left(1 + \varepsilon, \left| f(n_1, n_2) \right|\right), & \Omega(n_1, n_2) = 0, \\ \Omega(n_1, n_2), & \Omega(n_1, n_2) \ne 0. \end{cases}$$

   где ε – небольшая положительная константа.
8. $$\Omega(n_1, n_2) = \begin{cases} 0, & \left| f^W(n_1, n_2) \right| > 1, \\ f^W(n_1, n_2) & \left| f^W(n_1, n_2) \right| \le 1. \end{cases}$$
9. –
10. $$\Omega_1(n_1, n_2) = \begin{cases} -1, & W(n_1, n_2) = 2, \\ W(n_1, n_2), & \textit{иначе}; \end{cases}$$

    $\Omega(n_1, n_2) = \mathrm{shift}(\Omega_1(n_1, n_2), \mathbf{k})$,

    где $\mathrm{shift}(x, \mathbf{a})$ – циклический сдвиг матрицы x на вектор $\mathbf{a}$.
11. ξ.
12. $\mathbb{Y}^l_{[]}$.
13. Декодирование не производится.
14. (10), с функцией близости

$$\rho(\Omega, \widetilde{\Omega}) = \frac{1}{N_1 N_2} \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} \eta\left(\Omega(n_1, n_2), \widetilde{\Omega}(n_1, n_2)\right), \quad (13)$$

где

$$\eta(x, y) = \begin{cases} 1, & x = y, \\ 0, & x \ne y. \end{cases}$$

4.3. Система встраивания информации в изображения с расширением спектра

Третьей системой, которую мы опишем в терминах МСВИ, является широко известная система встраивания информации в изображения с расширением спектра (Cox et al., [22]).

Эта система предназначена для защиты изображений цифровыми водяными знаками, встраиваемыми в области дискретного косинусного преобразования (ДКП). Несомненным достоинством системы является её стойкость к широкому кругу искажений, однако достигается это во многом за счёт использования оригинального контейнера на этапе извлечения информации.

Длина встраиваемой информации N_b строго не задана, но она должна кодироваться матрицей признаков $\Omega \in \mathbb{R}^1_{[N_\Omega]}$, где $N_\Omega = 1000$. Функция кодирования тоже может быть произвольной:

$$\Omega = \mathcal{P}_f(\mathbf{b}, \mathbf{k}). \quad (14)$$

Элементы Ω представляют собой псевдослучайные числа, распределенные по гауссовскому закону.

Для модификации отбираются 1000 самых больших по модулю коэффициентов глобального дискретного косинусного преобразования (ДКП) контейнера $C_{DCT}(m_1, m_2)$ в змеевидной развёртке, как показано на рис. 6 (при этом отсчёт $C_{DCT}(0,0)$ не изменяется). Результатом данного отбора является матрица признаков контейнера $f \in \mathbb{R}^1_{[N_\Omega]}$. Не будем конкретизировать точную формулу расчёта f, поскольку она окажется весьма громоздкой.

Встраивание информации в пространстве признаков осуществляется по формуле

$$f^W(n) = f(n)\left(1 + \alpha \cdot \Omega(n)\right), \quad (15)$$

где $\alpha > 0$ – коэффициент усиления ЦВЗ.

Извлечение матрицы признаков встроенной информации осуществляется по формуле

$$\widetilde{\Omega}(n) = \frac{\widetilde{f^W}(n) - f(n)}{\alpha \cdot f(n)}. \quad (16)$$

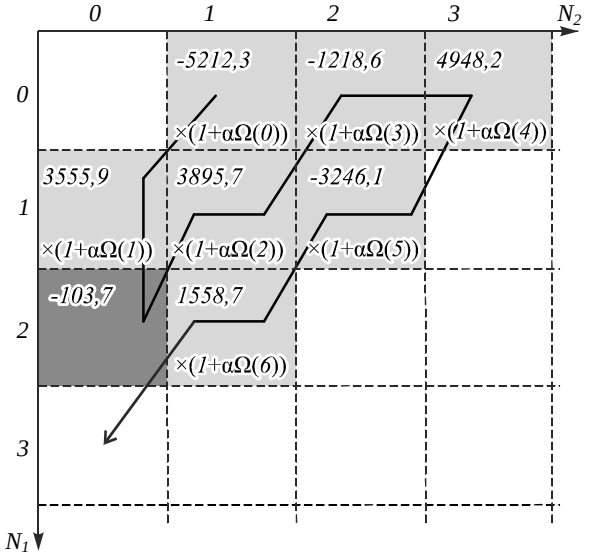

Рис. 6. Схема отбора коэффициентов ДКП при встраивании ЦВЗ системой Cox et al. В левом углу каждой ячейки отмечено значение соответствующей спектральной компоненты. Тёмной заливкой отмечен пропускаемый отсчёт

Результатом работы системы является обнаружение встроенного сигнала, которое осуществляется по формуле (10) с функцией близости вида

$$\rho\left(\Omega, \widetilde{\Omega}\right) = \frac{\sum_{n=0}^{N-1} \Omega(n)\widetilde{\Omega}(n)}{\sqrt{\sum_{n=0}^{N-1} \widetilde{\Omega}^2(n)}}. \quad (17)$$

Таким образом, данная система будет иметь следующее параметрическое описание:

1. $\mathbb{X}^m_{[]} = \left(\mathbb{B}^8\right)^2_{[N_1 \times N_2]}$.
2. $\pi_{\text{bw}} = true$.
3. N_b определяется функцией $\mathcal{P}_f$.
4. Формат ключа **k** явно не задан, используется он в функции $\mathcal{P}_f$.
5. $\mathbb{Y}^1_{[]} = \mathbb{R}^1_{[N_\Omega]}$, $\Psi = \mathbb{R}^1_{[N_1 N_2 - N_\Omega]}$,

   $\mathcal{F}(x) = DCT(x)$, $\mathcal{F}^{-1}(x) = DCT^{-1}(x)$, ,

   где $DCT(x)$ – ДКП сигнала x. Далее f_x формируется из отсчётов $DCT(x)$ в соответствии с рис. 6, а ψ_x содержит оставшиеся отсчёты.
6. –.
7. Формула (15).
8. Формула (16).
9. $\pi_{\mathcal{P}} = falce$.
10. Функция вида (14), строго не определена.
11. Результатом работы подсистемы извлечения является $\xi \in \mathbb{B}$.
12. $\mathbb{Y}^1_{[]}$.
13. Отсутствует.
14. (10), (17).

Заключение

В работе предложена модель, предназначенная для унифицированного описания произвольных систем встраивания информации, к которым относятся стеганографические системы и системы встраивания цифровых водяных знаков. В основе её лежит разделение форм информации, переносимой внутри цифрового сигнала-контейнера. Структурированы внутренние процессы СВИ, в также введено параметрическое описание СВИ, полностью определяющее алгоритмы её функционирования, а также облегчающее синтез новых систем. Показана применимость данной модели для описания трёх различных по своей структуре и назначению систем встраивания информации.

За рамками работы остались вопросы использования разработанной модели для формализации внешних свойств СВИ, их стойкости к различным атакам, а также для синтеза новых систем. Автор планирует рассмотреть эти вопросы в отдельной статье.

Благодарности

Работа выполнена при поддержке Минобрнауки РФ в рамках гранта президента РФ МК-4506.2015.9, государственного задания вузу №2014/198 (код проекта 2298) и Программы повышения конкурентоспособности СГАУ среди ведущих мировых научно-образовательных центров на 2013–2020 годы.

Литература

1. **Miller, M.L.** A review of watermarking, principles and practices / M.L. Miller, I.J. Cox, J.-P.M.G. Linnartz, T. Kal-

ker // Digital Signal Processing in Multimedia Systems. – 1999. – P. 461-485.
2. **Cox, I.J.** Digital watermarking / I.J. Cox, M.L. Miller, J.A. Bloom. – Morgan Kaufmann Publishers, 2002. – 568 p.
3. **Cox, I.J.** Digital watermarking and steganography / I.J. Cox, M.L. Miller, J.A. Bloom, J. Fridrich, T. Kalker. – 2nd ed. – Elsevier, 2008. – 587 p.
4. **Fridrich, J.** Steganography in digital media: principles, algorithms, and applications / J. Fridrich. – Cambridge University Press, 2010. – 450 p.
5. **Barni, M.** Watermarking systems engineering / M. Barni, F. Bartolini. – New-York: Marcel Dekker, 2004. – 485 p.
6. **Katzenbeisser, S.** Information hiding techniques for steganography and digital watermarking / S. Katzenbeisser, F.A.P. Petitcolas. – Boston, London: Artech House, 2000. – 237 p.
7. **Petitcolas, F.A.P.** Information hiding – a survey / F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn // Proceedings of the IEEE. – 1999. – Vol. 87(7). – P. 1062-1078.
8. **Cole, E.** Hiding in plain sight: steganography and the art of covert communication / E. Cole. – Wiley Publishing, 2003. – 362 p.
9. **Pfitzmann, B.** Information hiding terminology: results of an informal plenary meeting and additional / B. Pfitzmann // Lecture Notes in Computer Science. – 1996. – Vol. 1174. – P. 347-350.
10. **Furht, B.** Multimedia encryption and watermarking / B. Furht, E. Muharemagic, D. Socek. – Springer, 2006. – 331 p.
11. **Mohanty, S.P.** Digital watermarking: a tutorial review / S.P. Mohanty. – Bangalore, 1999.
12. **Cohen, A.S.** The gaussian watermarking game / A.S. Cohen, A. Lapidoth // IEEE Transactions on Information Theory. – 2002. – Vol. 48(6). – P. 1639-1667.
13. **Zhao, J.** A generic digital watermarking model / J. Zhao, E. Koch // Computers and Graphics. – 1998. – Vol. 22(4). – P. 397-403.
14. **Cachin, C.** An information-theoretic model for steganography / C. Cachin // Information and Computation. – 2004. – Vol. 192(1). – P. 41-56.
15. **Грибунин, В.Г.** Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: Солон-Пресс, 2002. – 272 с.
16. **Moulin, P.** Information-theoretic analysis of information hiding / P. Moulin, J.A. O'Sullivan // IEEE Transactions on Information Theory. – 2003. – Vol. 49(3). – P. 563-593.
17. **Mittelholzer, T.** An information-theoretic approach to steganography and watermarking / T. Mittelholzer // Lecture Notes in Computer Science. – 1999. – Vol. 1768. – P. 1-16.
18. **Nyeem, H.** Developing a digital image watermarking model / H. Nyeem, W. Boles, C. Boyd // 2011 International Conference on Digital Image Computing Techniques and Applications. – 2011. – P. 468-473.
19. **Nyeem, H.** Digital image watermarking: its formal model, fundamental properties and possible attacks / H. Nyeem, W. Boles, C. Boyd // EURASIP Journal on Advances in Signal Processing. – 2014. – Vol. 2014(1). – P. 1-22.
20. **Ma, L.** An Information-hiding model for secure communication / L. Ma, Z. Wu, Y. Hu, W. Yang // Advanced Intelligent Computing Theories and Applications. With Aspects of Theoretical and Methodological Issues. – 2007. – Vol. 4681. – P. 1305-1314.
21. **Гонсалес, Р.** Цифровая обработка изображений / Р. Гонсалес, Р. Вудс. – М.: Техносфера, 2012. – 1104 с.
22. **Cox, I.J.** Secure spread spectrum watermarking for multimedia / I.J. Cox, J. Kilian, F.T. Leighton, T. Shamoon // IEEE Transactions on Image Processing. – 1997. – Vol. 6(12). – P. 1673-1687.

Сведения об авторе

Федосеев Виктор Андреевич, 1986 года рождения, в 2009 году окончил Самарский государственный аэрокосмический университет имени академика С.П. Королёва (СГАУ) по специальности «Прикладная математика и информатика», кандидат физико-математических наук (2012). В настоящее время работает старшим научным сотрудником Лаборатории прорывных технологий дистанционного зондирования Земли СГАУ и научным сотрудником Института систем обработки изображений РАН. Области научных интересов: обработка и анализ изображений, компьютерное зрение, цифровые водяные знаки, стеганография. E-mail: *vicanfed@gmail.com* .

Поступила в редакцию 28 января 2016 г.
Окончательный вариант – 22 февраля 2016 г.

A UNIFIED MODEL FOR INFORMATION HIDING SYSTEMS

V.A. Fedoseev
Samara State Aerospace University,
Image Processing Systems Institute, Russian Academy of Sciences

Abstract

The paper presents a new model for a unified description of information hiding systems including both steganographic and watermarking systems. The model is based on considering three possible representations of the information being embedded: a binary vector, a digital signal, and a feature matrix. Some examples of the model usage are discussed.

Keywords: information hiding, data hiding, digital watermarking, watermarking system, steganography, steganographic system.

Citation: Fedoseev VA. A unified model for information hiding systems. Computer Optics 2016; 40(1): 87-98. DOI: 10.18287/2412-6179-2016-40-1-87-98.

Acknowledgements: The work was partially funded by the RF President's grant MK-4506.2015.9, the University state contract # 2014/198 (code 2298), and the RF Ministry of Education and Science as part of the SSAU's global competitiveness enhancement program for 2013-2020.

References

[1] Miller ML, Cox IJ, Linnartz J-PMG, Kalker T. A review of watermarking, principles and practices. Digital Signal Processing in Multimedia Systems 1999: 461-485.
[2] Cox IJ, Miller ML, Bloom JA. Digital Watermarking. San Francisco: Morgan Kaufmann Publishers; 2002.
[3] Cox IJ, Miller ML, Bloom JA, Fridrich J, Kalker T. Digital Watermarking and Steganography. 2nd ed. Elsevier; 2008.
[4] Fridrich J. Steganography in digital media: principles, algorithms, and applications. Cambridge University Press; 2010.
[5] Barni M, Bartolini F. Watermarking Systems Engineering. NY: Marcel Dekker; 2004.
[6] Katzenbeisser S, Petitcolas FAP. Information Hiding Techniques for Steganography and Digital Watermarking. Boston, London: Artech House; 2000.
[7] Petitcolas FAP, Anderson RJ, Kuhn MG. Information Hiding – A Survey. Proceedings of the IEEE 1999; 87(7): 1062-1078.
[8] Cole E. Hiding in Plain Sight: Steganography and the Art of Covert Communication. Wiley Publishing; 2003.
[9] Pfitzmann B. Information hiding terminology: results of an informal plenary meeting and additional proposals. LNCS 1996; 1174: 347-350.
[10] Furht B, Muharemagic E, Socek D. Multimedia encryption and watermarking. Springer; 2006.
[11] Mohanty SP. Digital Watermarking: A Tutorial Review. Bangalore: 1999.
[12] Cohen AS, Lapidoth A. The Gaussian watermarking game. IEEE Transactions on Information Theory 2002; 48(6): 1639-1667. doi:10.1109/TIT.2002.1003844.
[13] Zhao J, Koch E. A generic digital watermarking model. Computers & Graphics 1998; 22(4): 397-403. doi:10.1016/S0097-8493(98)00029-6.
[14] Cachin C. An information-theoretic model for steganography. Information and Computation 2004; 192(1): 41-56. doi:10.1016/j.ic.2004.02.003.
[15] Gribunin VG, Okov IN, Turintsev IV. Digital steganography [In Russian]. Moscow: Solon-Press; 2002.
[16] Moulin P, O'Sullivan JA. Information-theoretic analysis of information hiding. IEEE Transactions on Information Theory 2003; 49(3): 563-593. doi:10.1109/TIT.2002.808134.
[17] Mittelholzer T. An Information-Theoretic Approach to Steganography and Watermarking. LNCS 1999; 1768: 1-16.
[18] Nyeem H, Boles W, Boyd C. Developing a Digital Image Watermarking Model. 2011 International Conference on Digital Image Computing Techniques and Applications (DICTA) 2011: 468-473. doi:10.1109/DICTA.2011.85.
[19] Nyeem H, Boles W, Boyd C. Digital image watermarking: its formal model, fundamental properties and possible attacks. EURASIP J Adv Signal Process 2014; 2014(1): 1-22. doi:10.1186/1687-6180-2014-135.
[20] Ma L, Wu Z, Hu Y, Yang W. An Information-Hiding Model for Secure Communication. Advanced Intelligent Computing Theories and Applications. With Aspects of Theoretical and Methodological Issues. Berlin, Heidelberg: Springer; 2007: 1305-1314.
[21] Gonzalez RC, Woods RE. Digital Image Processing. 3th ed. Upper Saddle River, NJ: Prentice Hall; 2007.
[22] Cox IJ, Kilian J, Leighton FT, Shamoon T. Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing 1997; 6(12): 1673-1687. DOI:10.1109/83.650120.

Authors' information

Victor Andreevich Fedoseev (b. 1986) graduated (2009) from Samara State Aerospace University (SSAU), majoring in Applied Mathematics and Computer Science. PhD in Computer Science (2012). Currently he is a senior researcher scientist at Remote Sensing Lab, SSAU, and a researcher at Image Processing Systems Institute of the Russian Academy of Sciences. His current research interests include image processing and image analysis, computer vision, digital watermarking and steganography. E-mail: *vicanfed@gmail.com* .

Received January 28, 2016. The final version – February 22, 2016.