Список літератури

1. Криптография и защита сетей: принципы и практик, 2-е издание.: Пер. с англ. – М.: Издательский дом «Вильямс», 2001. – 672 с.

Надійшла 30.03.2007 р.

УДК 519.688 **Ерохин В.Ф.**

СТРУКТУРНАЯ СХЕМА И МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ПОТОКОВОЙ ЭЛЕКТРОМАГНИТНОЙ СТЕГАНОСИСТЕМЫ

В работе [1] предложено следующее определение цифровой стеганографии: "… наука о незаметном и надежном скрытии одних битовых последовательностей в других, имеющих аналоговую природу." Такое определение позволяет расширить область правомерности понятия "цифровая стеганография" на случай, когда скрываемое сообщение встраивается в контейнер не внутри некоторого устройства, а непосредственно в канале связи, аддитивно. Область применения стеганографических методов, когда скрываемое сообщение (СС) встраивается в основное сообщение (ОС) без ограничения на его длину непосредственно в пространстве, назовем потоковой электромагнитной стеганографией.

Цель статьи – формализованное описание стеганографической системы, в которой контейнер представляет собой электромагнитное поле, являющееся цифровым радиосигналом, а физическое встраивание скрываемого сообщения происходит аддитивно, в пространстве.

Для компьютерной стеганографии характерно, что СС обычно встраивается в места расположения младших значащих битов ОС (изображения, аудио-видеофайла) или в биты, замена которых не приводит к заметному для человека изменению результата – например, в биты, определяющие градации синего цвета в изображении. Выбор стеганопути такого типа обусловлен, в частности, особенностями восприятия органов чувств человека [1, 2]. Относительно же электромагнитной стеганографии вопрос оказывается сложнее – мы непосредственно воспринимаем лишь видимое электромагнитное излучение. Поэтому в таком случае выбор стеганопути в первую очередь будет определяться возможностями аппаратуры анализа электромагнитного спектра и соответствующих демодуляторов, а уже потом – возможностями человеческого глаза (уха) обнаружить возможное изменение.

Очевидно одно – при аддитивном встраивании электромагнитного излучения (ЭМИ) СС в ЭМИ ОС необходимо будет позаботиться о том, чтобы напряженность поля в используемой полосе частот, создаваемая передатчиком ОС, на некоторую требуемую величину превышала напряженность поля, создаваемую в той же полосе передатчиком СС, и чтобы это превышение соблюдалось в любой точке пространства, в которой может находиться нарушитель. Такое превышение определяется рядом факторов: требованиями к энергетической и временной скрытности [3] передатчика СС, которая, в свою очередь определяется уровнем априорных знаний нарушителя о неинформационных параметрах несущего излучения СС, а также о прекодере и стеганокодере передающей части стеганосистемы.

Если мы имеем дело с длительно работающим передатчиком ОС, то можно говорить о потоковом электромагнитном контейнере (ПЭК). В общем виде структурная схема потоковой электромагнитной стеганосистемы (ПЭС) представлена на рис.1.

Передатчик маскирующего излучения (цифрового радиосигнала ОС) создает пустой ПЭК, параметры которого оцениваются (фильтруются) в блоке оценки параметров (БОП) пустого ПЭК на передающей стороне электромагнитного стеганоканала (ЭС) и в блоке оценки неинформационных параметров (БОНП) на приемной стороне ЭС. Особенностями

функционирования БОП передающей стороны являются его переход в режим экстраполяции в интервалах электромагнитного излучения, содержащего СС (ЭСС), а также отсутствие необходимости в оценке энергетических параметров ПЭК. Особенностями функционирования БОНП приемной стороны является наличие двух режимов работы – в отсутствие ЭСС выполняется оценка параметров ПЭК (включая энергетические), а при появлении ЭСС по команде со стеганодетектора дополнительно выполняется дооценка тех неинформационных неэнергетических параметров ЭСС, которые не совпадают с параметрами ПЭК, уже оцененными и экстраполируемыми в интервалах излучения ЭСС.

В целом вышеизложенные наиболее общие особенности функционирования БОП и БОНП диктуются результатами синтеза алгоритмов некогерентного и квазикогерентного разделения взаимнонеортогональных цифровых сигналов, получаемыми путем совместного взаимодополняющего применения так называемой статистической теории разделения цифровых сигналов [4, 5] и методов теории фильтрации [6 и др.]. Отметим здесь, что при решении задач электромагнитной стеганографии следует стремится не только к обеспечению необходимого отношения напряженностей полей, создаваемых источниками ПЭК и ЭСС, но и к максимально достижимому количеству их неэнергетических неинформационных параметров, которые совпадают (например, несущие частоты, тактовые точки, вид модуляции, форма огибающих). Можно также утверждать, что если нарушителю известен алгоритм работы демодулятора СС на приемной стороне ЭС и он обнаруживает факт наличия ЭСС, то относительно мощный источник ПЭК все равно усложнит или даже сделает невозможной пеленгацию ЭСС с требуемой точностью.

Выше изложены основные принципиальные отличия ПЭС от классической [1, 2 и др.]. В остальном базовые принципы ее функционирования и функции составных элементов остаются такими же, как и в других известных случаях, включая компьютерную стеганографию [1, 2].

Запишем математическую модель ПЭС, соответствующую структурной схеме рис.1.

Эта система представляет собой систему связи, использующую в качестве носителя информации электромагнитное поле.

Алгоритм передачи СС состоит из трех основных этапов: 1) формирования ЭСС, 2) аддитивного сложения ЭСС с ПЭК в пространстве, 3) демодуляции суммарного сигнала с последующим выделением СС.

1. Процесс формирования ЭСС включает в себя процедуры криптографического шифрования (при необходимости), избыточного помехоустойчивого кодирования, стеганографического кодирования (определяющего закон встраивания СС в ЭСС) и переноса результата в полосу частот излучения.

Пусть W*, K*, I*, B* есть множества возможных ЭСС, ключей, фрагментов ПЭК (на интервалах существования ЭСС), и СС соответственно. Тогда генерация ЭСС с учетом переноса в полосу частот излучения может быть формализована в виде:

$$M\circ(K^* \times B^*) \rightarrow W^* ; W = M\circ[F(K, B)], \quad (1)$$

где K, B – представители соответствующих множеств, F(·) – функция, описывающая процедуры шифрования сообщения B, избыточного кодирования и распределения результата на временном интервале существования фрагмента I ПЭК, в который будет встроено (спроецировано) ЭСС; M○(·) – оператор модуляции. Очевидно, с целью достижения максимально возможной энергетической скрытности [3] ЭСС огибающие энергетических спектров ЭСС и ПЭК должны по форме совпадать. А для этого все неинформационные параметры ПЭК (частота, форма огибающей несущего колебания, закон и скорость манипуляции и др.), оцениваемые в БОП пустого ПЭК, должны быть параметрами оператора M. В этом смысле между неинформационными параметрами ЭСС и ПЭК должна соблюдаться жесткая взаимосвязь, вплоть до равенства ряда из них (например, несущих частот и скоростей манипуляции). С другой стороны, как видно из (1) функция F(·) от I не

зависит, т.е. алгоритм работы стеганокодера в структурной схеме рис.1 инвариантен к текущим состояниям дискретного представляющего параметра (например, к скачкам фазы при фазовой манипуляции) ПЭК.

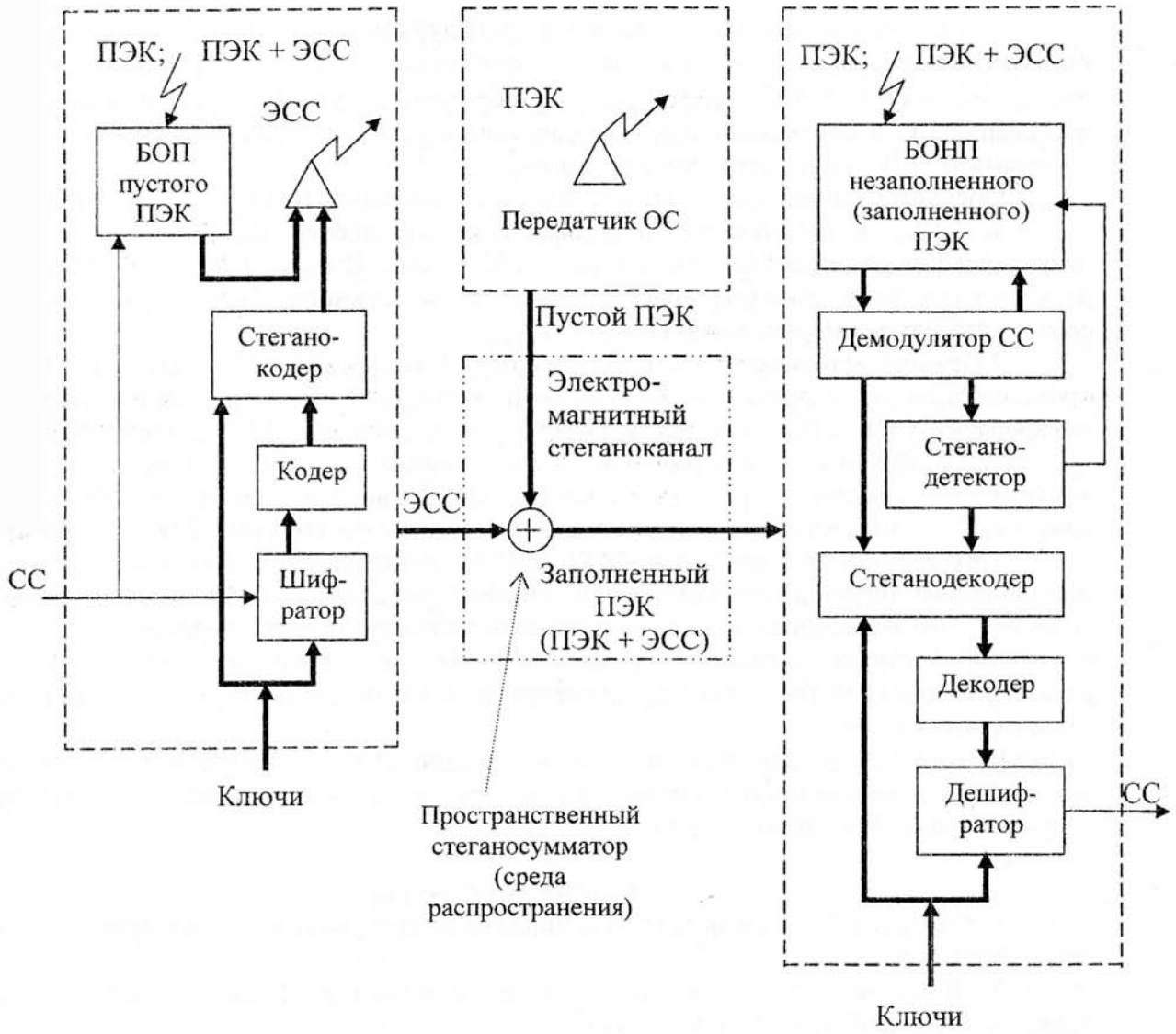

Рис.1 Структурная схема потоковой электромагнитной стеганосистемы

2. Процесс встраивания ЭСС в ПЭК, является, очевидно, сложением в пространстве:

$$\varphi \circ I^* + \psi \circ W^* \rightarrow I^*_W; \qquad (2)$$

$$I_W(x, y, z) = \varphi(x_k, y_k, z_k, x, y, z) \circ I + \psi(x_c, y_c, z_c, x, y, z) \circ W.$$

Здесь $\varphi(x_k, y_k, z_k, x, y, z) \circ (\cdot)$ – оператор излучения ПЭК, порождаемого в точке (x, y, z) передатчиком ОС, находящимся в точке (x_k, y_k, z_k); $\psi(x_c, y_c, z_c) \circ (\cdot)$ – оператор излучения ЭСС от соответствующего передатчика, находящегося в точке (x_c, y_c, z_c). Данные операторы определяются параметрами соответствующих передатчиков, антенн и свойствами среды распространения.

3. Процесс обработки заполненного ПЭК $I_W(x, y, z)$ может быть представлен в виде:

$$D \circ I^{*}_{W} \quad \rightarrow K^{*} \times B^{*\prime};$$
$$F(K, B') = D \circ I_{W}(x, y, z); \qquad (3)$$
$$B = F^{-1}(K, B').$$

Здесь оператор $D \circ (\cdot)$ определяется процедурами обработки в приемном устройстве, включая демодуляцию – разделение сигналов [4,5], одновременно излучаемых передатчиками ОС и СС. Оператор $F^{-1}(\cdot)$, обратный оператору $F(\cdot)$, описывает процессы извлечения СС в стеганодекодере, декодирования и дешифрования. Очевидно, в канале с помехами $B' \neq B$ в силу возникновения ошибок.

Обсудим отличия предложенной модели от известных ранее [1, 2 и др.].

1. ЭСС, в отличие от цифровых водяных знаков, инвариантен к поведению дискретного параметра ПЭК (основного сообщения). Вместе с тем неинформационные неэнергетические параметры ЭСС должны по возможности максимально совпадать с соответствующими параметрами ПЭК.

2.Процесс встраивания СС в ОС содержит 2 четко разграниченных этапа. На первом, происходящем в аппаратно – программной части, стеганокодер (после шифрования и кодирования СС) определяет места (закон) размещения бит СС на временной оси. Эта процедура в общем случае может быть также криптографически защищенной. На втором этапе, происходящем в среде распространения, происходит сложение ЭСС (имеющего конечную длительность во времени) с соответствующим фрагментом ПЭК.

3.Выделение СС из смеси ЭСС и ПЭК реализуется в приемном устройстве, с применением методов статистической теории разделения цифровых сигналов [4,5]. Известно, что совпадение неинформационных неэнергетических параметров ПЭК и ЭСС облегчает задачу демодуляции – разделения, так как предположительно энергетические характеристики ПЭК (постоянно присутствующего в наблюдении) существенно превышают характеристики ЭСС.

В заключение отметим, что использование ПЭК в качестве маскирующего не исключает одновременного применения и других методов повышения скрытности – например, кодового зашумления [7].

Список литературы

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.: Солон-пресс, 2002. – 272 с.

2. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. – К.:"МК Пресс", 2006. – 288 с.

3. Каневский З.М., Литвиненко В.П. Теория скрытности. – Воронеж: Изд-во ВГУ, 1991. – 144 с.

4. Бураченко Д.Л. Оптимальное разделение цифровых сигналов многих пользователей в линиях и сетях связи в условиях помех. – Л.: ВАС, 1990. – 302 с.

5. Ерохин В.Ф. Демодуляция конфликтующих цифровых сигналов. – К.: ИК. АН Украины им. В.М. Глушкова, 1993. – 130 с.

6. Тихонов В.И., Харисов В.И. Статистический анализ и синтез радиотехнических устройств и систем. – М.: Радио и связь, 1991. – 608 с.

7. Защита информации на основе кодового зашумления. Ч 1. Теория кодового зашумления. / Под ред В.И. Коржика – СПб.: ВАС, 1993 – 245 с.

Поступила 6.04.2007 г.