УДК 621.396

А.А. Кузнецов, проф., докт. техн. наук,
Харьковский университет Воздушных Сил
А.А. Смирнов, доц., канд. техн. наук Е.В.Мелешко, канд. техн. наук
Кировоградский национальный технический университет

Математическая модель и структурная схема стеганографической системы

В данной работе исследуется формальное математическое описание и структурная схема стегранографической системы, и по аналогии с теорией криптографических систем, вводятся основные элементы и математически операторы, абстрактно описывающие стеганографическую систему защиты информации.
стеганография, защита информации, структурная схема, математическая модель

1. Введение. Математические основы современной криптографии заложены в работах известного американского ученого К. Шеннона [1-3], который впервые, используя теоретико-информационный подход, ввел абстрактное математическое определение криптографической системы и формализовал процедуры криптографического преобразования информации. Эти работы дали существенный толчок в развитии отдельных методов теории защиты информации, криптографии и аутентификации, цифровой стеганографии, а также методов цифровой обработки сигналов и помехоустойчивого кодирования [4-12].

В данной работе исследуется формальное математическое описание (в терминах К. Шеннона) и структурная схема стеганографической системы и по аналогии с теорией криптографических систем вводятся основные элементы и математические операторы, абстрактно описывающие стеганографическую систему защиты информации.

Методы стеганографической защиты информации развиваются в последние годы очень интенсивно [1-7]. В их основе лежит сокрытие не только смыслового содержания передаваемой информации, но и самого факта организации передачи данных. Другими словами, основной задачей методов стеганографической защиты информации является организация скрытного канала передачи данных посредством встраивания передаваемых информационных сообщений в объекты (контейнеры), обладающие высокой естественной избыточностью.

Одним из наиболее удобных способов организации цифровых стеганографических каналов скрытной передачи информации является использование в качестве цифровых контейнеров неподвижных изображений [1-7]. Обладая высоким уровнем естественной избыточности подобные контейнеры являются наиболее перспективным направлением исследований в современной стеганографии. В тоже время подавляющее большинство известных методов встраивания информации в неподвижные изображения используют простейшие процедуры кодирования наименее значимых бит и/или особенности форматирования растровых данных изображения [1-3].

2. Структурная схема и формальное математическое определение криптографической системы. Абстрактно криптографическая система определяется

© А.А. Кузнецов, А.А. Смирнов, Е.В.Мелешко, 2012

как некоторое множество отображений одного пространства (множества возможных сообщений) в другое пространство (множество возможных криптограмм) [1-3].

Зафиксируем множество возможных сообщений $M = \{M_1, M_2, ..., M_m\}$ и множество криптограмм $E = \{E_1, E_2, ..., E_n\}$. Зафиксируем также множество отображений:

$$\varphi = \{\varphi_1, \varphi_2, \ldots, \varphi_k\},$$

где:

$$\varphi_i: M \to E,\ i = 1, 2, ..., k.$$

Если множества M и E равномощны, т.е. $n = m$то существует обратное отображение $\varphi_i^{-1}: E \to M$, которое каждому элементу множества E ставит в соответствие элемент множества M. Очевидно, что φ_i и φ_i^{-1} задают взаимно однозначное отображение множеств M и E.

Зафиксируем теперь множество ключей $K = \{K_1, K_2, ..., K_k\}$ так, что для всех $i = 1, 2, ..., k$ отображение $\varphi_i \in \varphi$ однозначно задается ключом K_i, т. е.:

$$\varphi_i : M \xrightarrow{K_i} E.$$

Каждое конкретное отображение φ_i из множества φ соответствует способу шифрования при помощи конкретного ключа K_i. На рис. 1 схематично представлено отображение $\varphi_i \in \varphi$, заданное ключом K_i.

Зафиксируем множество ключей $K^* = \{K_1^*, K_2^*, ..., K_k^*\}$, в общем случае $K \neq K^*$. Все элементы множества обратных отображений:

$$\varphi^{-1} = \{\varphi_1^{-1}, \varphi_2^{-1}, \ldots, \varphi_k^{-1}\},$$

задаются соответствующим ключом:

$$\varphi_i^{-1} : E \xrightarrow{K_i^*} M.$$

Каждое конкретное отображение φ_i^{-1} из множества φ^{-1} соответствует способу расшифрования при помощи ключа K_i^*. Если известен ключ K_i^* то в результате расшифрования возможен лишь единственный ответ – элемент множества M.

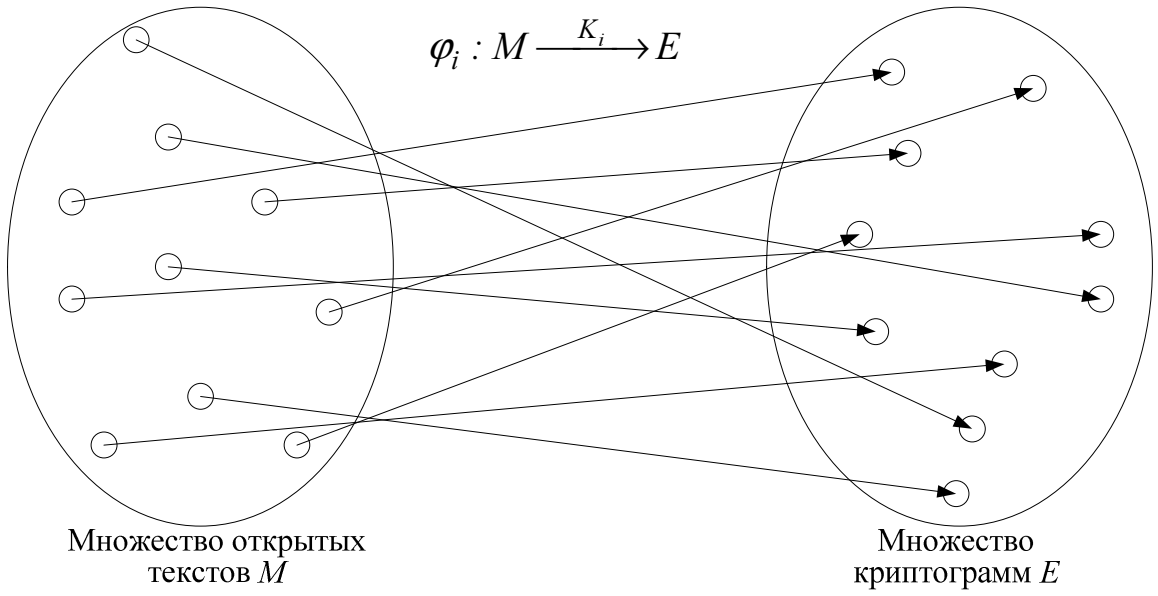

Рисунок 1 – Отображение $\varphi_i : M \xrightarrow{K_i} E$ множества открытых текстов в множество криптограмм

Таким образом, в абстрактное *определение криптографической системы* входят следующие множества M, E, φ, φ^{-1}, K и K^* (множества открытых текстов и криптограмм, множеств прямых и обратных отображений, множества ключей). Если

при этом $K \neq K^*$, то система *асимметрична*. Напротив, если $K = K^*$ – *симметрична*. На рис. 2 представлена структурная схема криптографической системы.

Источник сообщений порождает поток сообщений из множества M. Каждое сообщение представляется конкретной реализацией некоторого случайного процесса, описывающего работу источника сообщений. Каждому сообщению $M_j \in M = \{M_1, M_2, ..., M_m\}$ соответствует вероятность $P(M_j)$. Распределение вероятностей случайного процесса задается совокупным распределением вероятностей случайных величин, т.е. множеством вероятностей:

$$P_M = \{P(M_1), P(M_2), ..., P(M_m)\}. \quad (1)$$

Источник ключей порождает поток ключей из множества K и/или K^*. Каждому ключу $K_i \in K = \{K_1, K_2, ..., K_k\}$ соответствует некоторая вероятность $P(K_i)$, а каждому $K_i^* \in K^* = \{K_1^*, K_2^*, ..., K_k^*\}$ соответствует вероятность $P(K_i^*)$. Случайный процесс выработки ключей задается множествами вероятностей:

$$P_K = \{P(K_1), P(K_2), ..., P(K_k)\}, \quad (2)$$

и

$$P_{K^*} = \left\{P\left(K_1^*\right), P\left(K_2^*\right), ..., P\left(K_k^*\right)\right\}. \quad (3)$$

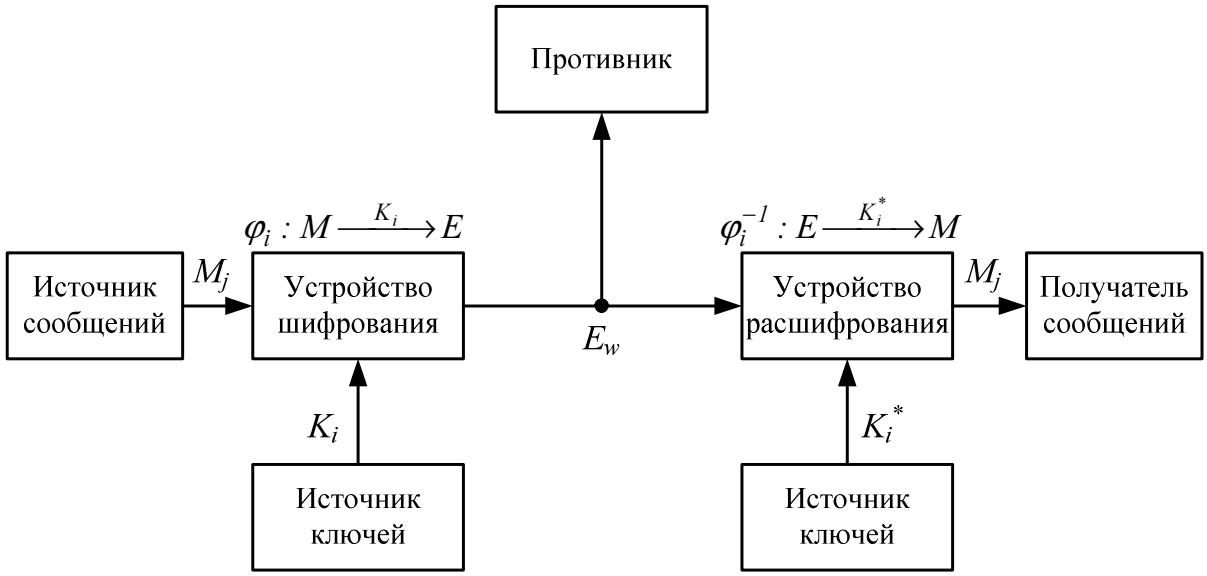

Рисунок 2 – Структурная схема криптографической системы

Множества значений априорных вероятностей (1 – 3) образуют априорные знания злоумышленника об источнике сообщений и источнике ключей, соответственно. Фактически эти множества характеризуют априорные знания злоумышленника относительно возможной «слабости» криптографической системы.

Выбор ключа K_i определяет конкретное отображение φ_i из множества отображений φ. С помощью отображения φ_i, соответствующего выбранному ключу K_i, по поступившему сообщению M_j формируется криптограмма:

$$E_w = \varphi_i(K_i, M_j),$$

$$i \in [1,2,...,k],\ j \in [1,2,...,m],\ w \in [1,2,...,n],\ n \geq m.$$

Криптограмма E_w передается в точку приема по некоторому каналу и может быть перехвачена злоумышленником. На приемном конце с помощью обратного отображения φ_i^{-1} (заданного ключом K_i^*) из криптограммы E_w восстанавливается первоначальное сообщение:

$$M_j = \varphi_i^{-1}(K_i, E_w).$$

Если злоумышленник перехватит криптограмму E_l, он может с ее помощью попытаться вычислить апостериорные вероятности различных возможных сообщений

$$P_{M|E_w} = \{P(M_1|E_w), P(M_2|E_w), ..., P(M_m|E_w)\}, \quad (4)$$

и различных возможных ключей:

$$P_{K|E_w} = \{P(K_1|E_w), P(K_2|E_w), ..., P(K_k|E_w)\}, \quad (5)$$

которые могли быть использованы при формировании криптограммы E_w.

Множества апостериорных вероятностей (4 – 5) образуют апостериорные знания злоумышленника о ключах $K = \{K_1, K_2, ..., K_k\}$ и сообщениях $M = \{M_1, M_2, ..., M_m\}$ после перехвата криптограммы E_l. Фактически, множества $P_{K|E_w}$ и $P_{M|E_w}$ представляют собой множества предположений, которым приписаны соответствующие вероятности.

3. Структурная схема и формальное математическое определение стеганографичной системы. По аналогии с теорией криптографических систем рассмотрим основные функциональные элементы и математически операторы, абстрактно описывающие стеганографическую систему защиты информации.

Зафиксируем множество возможных сообщений $M = \{M_1, M_2, ..., M_m\}$, множество возможных контейнеров $L = \{L_1, L_2, ..., L_l\}$, и множество возможных заполненных контейнеров (стеганограмм) $E = \{E_1, E_2, ..., E_n\}$. Зафиксируем множество отображений:

$$\varphi = \{\varphi_1, \varphi_2, \ldots, \varphi_k\},$$

где

$$\varphi_i: (M, L) \to E, \; i = 1, 2, ..., k.$$

Определим обратное отображение:

$$\varphi_i^{-1}: E \to (M, L),$$

которое каждому элементу множества E ставит в соответствие элемент множества M и элемент множества L.

Зафиксируем множество ключей $K = \{K_1, K_2, ..., K_k\}$ так, что для всех $i = 1, 2, ..., k$ отображение $\varphi_i \in \varphi$ однозначно задается ключом K_i, т. е.:

$$\varphi_i : (M, L) \xrightarrow{K_i} E.$$

Каждое конкретное отображение φ_i из множества φ соответствует способу встраивания сообщения из множества M в контейнер из множества L при помощи конкретного ключа K_i. На рис. 3 схематично представлено отображение $\varphi_i \in \varphi$, заданное ключом K_i.

Зафиксируем множество ключей $K^* = \{K_1^*, K_2^*, ..., K_k^*\}$, в общем случае $K \neq K^*$. Все элементы множества обратных отображений:

$$\varphi^{-1} = \{\varphi_1^{-1}, \varphi_2^{-1}, \ldots, \varphi_k^{-1}\},$$

задаются соответствующим ключом:

$$\varphi_i^{-1} : E \xrightarrow{K_i^*} (M, L).$$

Каждое конкретное отображение φ_i^{-1} из множества φ^{-1} соответствует способу извлечения сообщения из заполненного контейнера (и формирования пустого контейнера) при помощи ключа K_i^*. Если известен ключ K_i^* то в результате выполнения

операции извлечения возможен лишь единственный ответ – элемент множества M и элемент множества L:

$$\left(M_j, L_l\right) = \varphi_i^{-1}\left(E_w, K_i^*\right).$$

Для робастных систем справедливо следующее равенство:

$$\left(M_j, L_l\right) = \varphi_i^{-1}\left(E_w + \varepsilon, K_i^*\right),$$

т.е. незначительное изменение заполненного контейнера (на величину ε) не приведет к неправильному извлечению сообщения.

Хрупкие стаганосистемы характеризуются выполнением неравенства:

$$\left(M_j, L_l\right) \neq \varphi_i^{-1}\left(E_w + \varepsilon, K_i^*\right),$$

для сколь угодно малой величины ε.

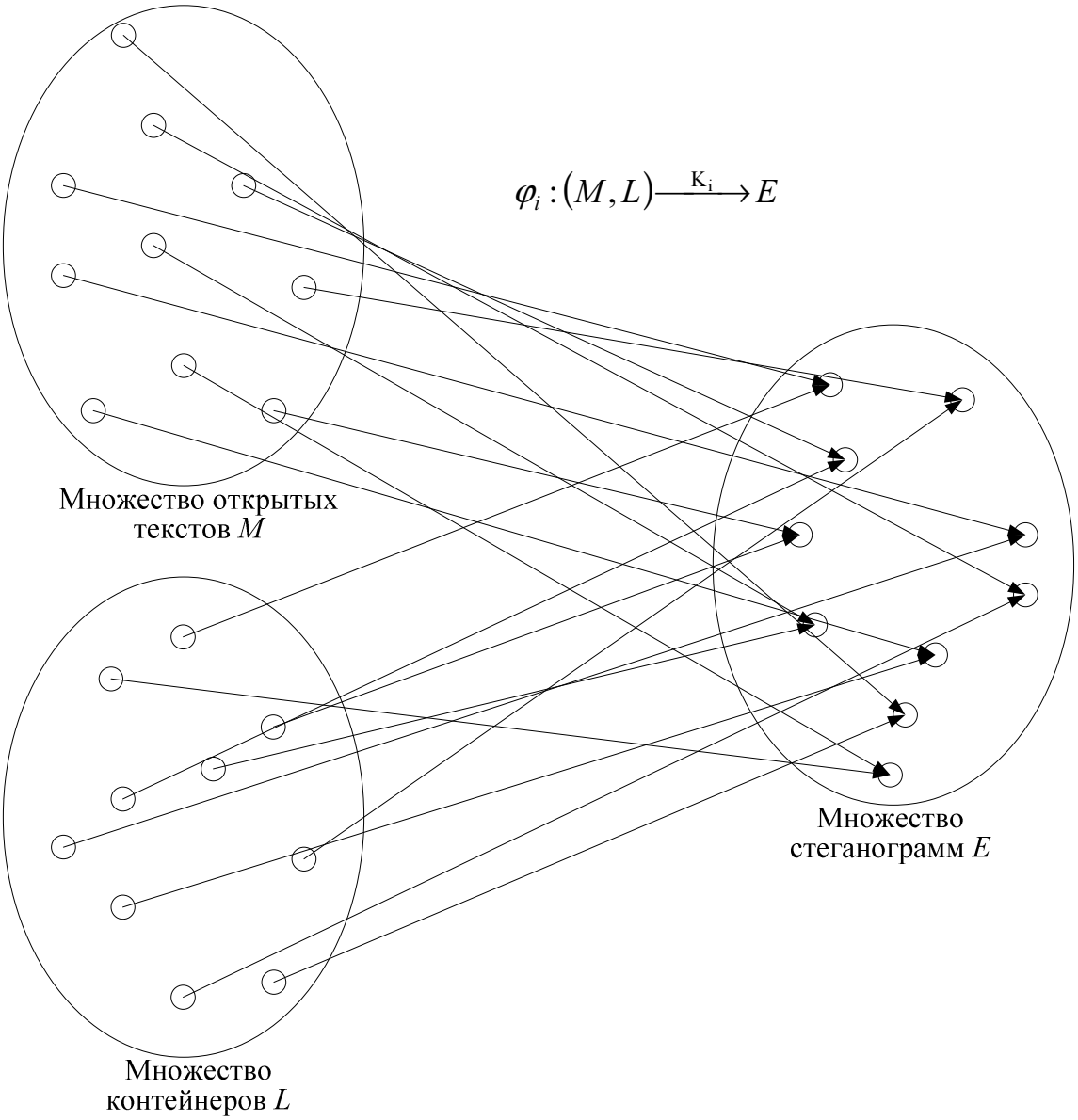

Рисунок 3 – Отображение $\varphi_i : \left(M, L\right) \xrightarrow{K_i} E$ множества открытых текстов в множество криптограмм

Таким образом, в абстрактное *определение стеганографической системы* входят следующие множества *M, L, E,* φ, φ^{-1}, *K* и K^* (множества открытых текстов, пустых

контейнеров и стеганограмм (заполненных контейнеров), множества прямых и обратных отображений и множества соответствующих им ключей).

На рис. 4 представлена структурная схема стеганографической системы.

Источник сообщений порождает поток информационных сообщений I_j из множества $I = \{I_1, I_2, ..., I_m\}$, которое, после предварительного преобразования в прекодере, формируется в виде сообщения M_j из множества M. Прекодер выполняет таким образом функцию предварительной подготовки информационного сообщения к встраиванию в контейнер (например, преобразование информационного сообщения в массив специально отформатированных цифровых данных).

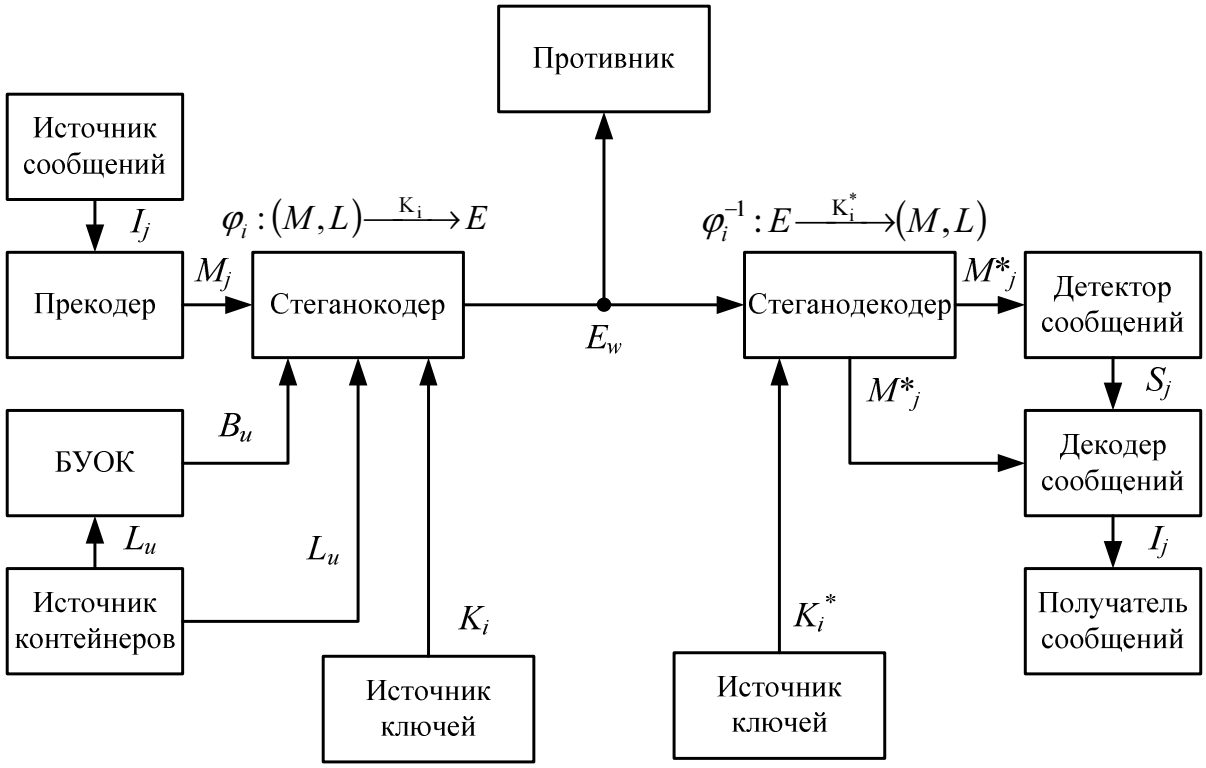

Рисунок 4 – Структурная схема стеганографической системы

Каждому сообщению $M_j \in M = \{M_1, M_2, ..., M_m\}$ соответствует вероятность $P(M_j)$. Распределение вероятностей случайного процесса задается совокупным распределением вероятностей случайных величин, т.е. множеством вероятностей:

$$P_M = \{P(M_1), P(M_2), ..., P(M_m)\}. \quad (6)$$

Источник контейнеров порождает поток пустых контейнеров L_u из множества $L = \{L_1, L_2, ..., L_l\}$. Работа источника контейнеров может так же описываться некоторым случайным процессом, конкретная реализация которого есть контейнер L_u. В этом случае имеем дело со случайными контейнерами, которым могут быть приписаны соответствующие вероятности:

$$P_L = \{P(L_1), P(L_2), ..., P(L_l)\}.$$

Гораздо чаще на практике используется другой тип контейнеров, формирование которых нельзя описать случайным процессом. В этом случае источник контейнеров работает по детерминированному правилу, задаваемому либо уполномоченной (например, передающей) стороной, либо злоумышленником. В первом случае формируются т.н. выбранные контейнеры, т.е. используемый контейнер не сформирован случайно, а выбран уполномоченной стороной по некоторым не

стохастическим признакам. Во втором случае источник контейнеров находится под управлением злоумышленника, а сами контейнеры по детерминированному правилу формируются злоумышленником и навязываются передающей стороне. Таким образом, имеем т.н. навязанный контейнер.

В простейшем случае множество пустых контейнеров содержит всего один элемент, который используется передающей стороной для встраивания сообщения и скрытной передачи его по каналу связи.

Сформированный контейнер L_u обрабатывается блоком учета особенностей контейнеров (БУОК). Основной функцией БУОК является выделение тех признаков (особенностей) B_u поступившего контейнера L_u, которые будут использованы при встраивании в него сообщения M_j .

Источник ключей в стеганографической системе порождает поток ключей из множества K и/или K^*. Каждому ключу $K_i \in K = \{K_1, K_2, ..., K_k\}$ соответствует некоторая вероятность $P(K_i)$, а каждому $K_i^* \in K^* = \{K_1^*, K_2^*, ..., K_k^*\}$ соответствует вероятность $P(K_i^*)$. Случайный процесс выработки ключей задается множествами вероятностей:

$$P_K = \{P(K_1), P(K_2), ..., P(K_k)\}, \quad (7)$$

и

$$P_{K^*} = \{P(K_1^*), P(K_2^*), ..., P(K_k^*)\}. \quad (8)$$

Множества значений априорных вероятностей (6 – 8) образуют априорные знания злоумышленника об источнике сообщений и источнике ключей, соответственно. Фактически эти множества характеризуют априорные знания злоумышленника относительно возможной «слабости» стеганографической системы.

Выбор ключа K_i определяет конкретное отображение φ_i из множества отображений φ. С помощью отображения φ_i, соответствующего выбранному ключу K_i, по поступившему сообщению M_j и поступившему контейнеру L_u с учетом выявленных особенностей B_u контейнера L_u формируется стеганограмма (заполненный контейнер):

$$E_w = \varphi_i(K_i, M_j, L_u),$$

$$i \in [1,2,...,k],\ j \in [1,2,...,m],\ u \in [1,2,...,l],\ w \in [1,2,...,n],\ n \geq m .$$

Стеганограмма E_w передается в точку приема по некоторому каналу и может быть перехвачена злоумышленником. На приемном конце с помощью обратного отображения φ_i^{-1} (заданного ключом K_i^*) из стеганограммы E_w восстанавливается первоначальное сообщение и пустой контейнер:

$$(M_j, L_u) = \varphi_i^{-1}(K_i, E_w).$$

При передаче стеганограммы E_w по каналу связи и возможном воздействии злоумышленником на E_w передаваемая стеганограмма может исказиться. В этом случае на приемной стороне будет принята некоторая смесь переданного заполненного контейнера и результата воздействия на контейнер при передаче по каналу связи: $E_w+\varepsilon$. Выполнение операции обратного отображения φ_i^{-1} (заданного ключом K_i^*) в этом случае приведет к формированию некоторой оценки переданного сообщения и переданного пустого контейнера, т.е. получим:

$$(M_j^*, L_u^*) = \varphi_i^{-1}(K_i, E_w + \varepsilon).$$

Для хрупких стеганографических систем неравенство $M_j^* \neq M_j$ должно приводить к отбраковке сообщения, т.е. при малейшем искажении контейнера ($\varepsilon \neq 0$) извлеченная оценка M_j^* не должна приводить к прочтению встроенного сообщения (сообщение M_j разрушается при $\varepsilon \neq 0$).

Робастные стеганографические системы устойчивы к воздействию на заполненный контейнер. В введенных выше обозначениях это означает, что при $\varepsilon \neq 0$ извлеченная оценка M_j^* должна сопоставляться с одним из возможных сообщений (в идеальном случае, с сообщением M_j). В тоже время, полученный из канала связи контейнер E_w может вовсе не содержать встроенного сообщения, т.е извлеченная из контейнера оценка M_j^* не должна быть сопоставлена ни с одним из допустимых сообщений. Функции детектирования встроенного сообщения на приемной стороне возложены на детектор сообщений, который по поступившей оценке M_j^* принимает решение о наличии или отсутствии встроенного сообщения в принятом контейнере E_w. Таким образом, оценка детектора S_j может быть интерпретирована как двоичное (да/нет) решение помехоустойчивого декодера о наличии или отсутствии неисправляемой ошибки. Само декодирование осуществляется в декодере сообщений, основными функциями которого является сопоставление извлеченной оценки M_j^* с одним из возможных сообщений M_j и преобразования последнего в информационное сообщение I_j, предоставляемое получателю информации.

Злоумышленник может перехватить стеганограмму E_w. В этом случае он может с ее помощью попытаться вычислить апостериорные вероятности различных возможных сообщений:

$$P_{M|E_w} = \{P(M_1|E_w), P(M_2|E_w), ..., P(M_m|E_w)\}, \quad (9)$$

и различных возможных ключей:

$$P_{K|E_w} = \{P(K_1|E_w), P(K_2|E_w), ..., P(K_k|E_w)\}, \quad (10)$$

которые могли быть использованы при формировании стеганограммы E_w.

Множества апостериорных вероятностей (9 – 10) образуют апостериорные знания злоумышленника о ключах $K = \{K_1, K_2, ..., K_k\}$ и сообщениях $M = \{M_1, M_2, ..., M_m\}$ после перехвата стеганограммы E_w. Фактически, множества $P_{K|E_w}$ и $P_{M|E_w}$ представляют собой множества предположений, которым приписаны соответствующие вероятности.

4. Выводы. В данной работе проведен анализ и исследовано формальное математическое описание и структурная схема стеганографической системы. По аналогии с рассмотренной формализацией из теории криптографических систем введены основные элементы и математически операторы, абстрактно описывающие стеганографическую систему защиты информации.

Во введенной формализации получено определение хрупких и робастных стеганосистем, а также введены вероятностные показатели, характеризующие апостериорные знания злоумышленника о криптографических ключах и встраиваемых сообщениях. *Перспективным направлением дальнейших исследований* является анализ и теоретическое обоснование критериев и показателей эффективности стеганографических систем защиты информации, исследование свойств известных примеров стеганосистем по введенным показателям и критериям оценки эффективности.

Список литературы

1. Шеннон К. Работы по теории информации и кибернетике. – М.: ИЛ, 1963. – 829 с.
2. Шеннон К. Связь при наличии шума. // Теория информации и ее приложения. Сборник переводов. – М.:ФИЗМАТГИЗ, 1959.– С. 82-12.

3. Шеннон К. Теория связи в криптографических системах // Шеннон К. Работы по теории информации и кибернетике. – М.: Изд-во иностранной литературы, 1963. – С.333-402.
4. Долгов В.И. Основы статистической теории приема дискретных сигналов. – Х.: ХВВКИУРВ, 1989. – 448 с.
5. Стасєв Ю.В. Основи теорії побудови сигналів. – Х.: ХВУ, 1999. – 87с.
6. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. – М.: Связь, 1979. – 744 с.
7. Науменко М.І., Стасєв Ю.В., Кузнецов О.О. Теоретичні основи та методи побудови алгебраїчних блокових кодів. Монографія. – Х.: ХУ ПС, 2005. – 267 с.
8. Молдовян Н.А., Молдовян А.А., Еремеев М.А. Криптография: от примитивов к синтезу алгоритмов. – СПб.: БХВ-Петербург, 2004. – 448 с.
9. Сидельников В.М. Криптография и теория кодирования. Материалы конференции «Московский университет и развитие криптографии в России», МГУ. – 2002. – 22 с.
10. Саломаа А. Криптография с открытым ключом: Пер. с англ., – М.: Мир, 1995. – 318с.
11. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. – К.: «МК-Пресс»б 2006. - 288 с., ил.
12. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. – М.: Вильямс, 2003. – 1104 с.
13. Кузнецов А.А., Смирнов А.А. Встраивание данных в контейнеры-изображения с использованием сложных дискретных сигналов // Радиотехника: Всеукр. межвед. науч.-техн. сб. – Харьков: ХТУРЭ.–2011. – Вып. 166. – С. 134-141.
14. Kuznetsov A., Serhiienko R., Kovtun V., Botnov A. Use of Complex Discrete Signals for Steganographic Information Security // Statistical Methods of Signal and Data Processing (SMSDP-2010): Proceedings. – Kiev: National Aviation University “NAU-Druk” Publishung House – 2010. – pp. 143 – 146.
15. Стасев Ю.В., Кузнецов А.А., Смирнов А.А. Использование сложных дискретных сигналов для стеганографической защиты информации // Системи управління, навігації та зв’язку. – Київ: Центральний науково-дослідний інститут навігації і управління. – 2011. – Вип. 3 (19). – С. 110-114.

О. Кузнецов, О. Смірнов, Є. Мелешко

Математична модель і структурна схема стеганографічної системи

У даній роботі досліджується формальний математичний опис і структурна схема стеганографичної системи, і за аналогією з теорією криптографических систем, уводяться основні елементи й математично оператори, що абстрактно описують стеганографічну систему захисту інформації.

A. Kuznetsov, A. Smirnov, E. Meleshko

The mathematical model and flow diagram of the steganography system

In this work is probed formal mathematical specification and flow diagram of the steganography system, and by analogy with the theory of the secret systems, basic elements and mathematically operators, abstractly describing the steganography system of priv are entered.

Одержано 27.02.12