УДК 681.3

УТОЧНЕНИЕ КРИТЕРИЯ ИЗБЫТОЧНОСТИ ПОМЕХОУСТОЙЧИВОГО СОКРЫТИЯ ИНФОРМАЦИИ В РАМКАХ АССОЦИАТИВНОЙ СТЕГАНОГРАФИИ

И.С. Вершинин

Рассматриваются вопросы помехоустойчивости ассоциативного метода стеганографии путем введения избыточности на уровне ключей с учетом допустимого уровня искажений при распознавании

Ключевые слова: двумерно-ассоциативное маскирование, ассоциативная стеганография

Рассматриваются вопросы, относящиеся к области, связанной с генерацией и распознаванием замаскированных бинарных изображений с использованием базового алгоритма маскирования, предложенного в работе [1].

Основной задачей является уточнение оценки помехоустойчивости распознавания стилизованных бинарных изображений по дихотомальным троичным эталонам, полученной в работе [2].

В качестве исходной информации, подлежащей хранению или передаче, используется множество стегоконтейнеров (кодовых слов), состоящих из 3 букв в алфавите почтовых индексов, погруженных по маске в случайную последовательность. Размер каждого стегоконтейнера равен 198 байт (при m = 60, где m – количество столбцов любого почтового индекса).

Для повышения помехоустойчивости при проведении маскирования и последующей рандомизации для каждой буквы стегоконтейнера необходимо использовать не один, а **несколько** наборов масок k_m. Их совокупность используется в качестве ключа при распознавании.

Процедура распознавания искаженного сообщения проводится по всем наборам масок. Для каждой стегобуквы за результат распознавания принимается эталон, число распознаваний которого

$$k_r \geq (k_m + 1)/2. \qquad (1)$$

Если данное условие по результатам распознавания некоторой стегобуквы не выполняется, фиксируется факт ее искажения (отказ от распознавания). Были получены экспериментальные оценки помехоустойчивости с учетом вводимой избыточности для $k_m = 3, 5, 7, 9$.

Эксперимент проводился следующим образом.

1. Генерируется множество стегоконтейнеров (10^6) с использованием k_m наборов масок.
2. Случайным образом выбирается 16 (32, 64, 128) байтов для каждого стегоконтейнера, в пределах которых будет действовать помеха.
3. В каждом из 16 вышеуказанных байтов всех стегоконтейнеров случайным образом выбирается один искажаемый (инвертируемый) бит.
4. Проводится распознавание искаженного множества стегоконтейнеров по k_m наборам масок.
5. Определяется количество неверных распознаваний и отказов от распознавания.
6. Пункты 3-5 повторяются 8 раз (до полной инверсии всех битов в шестнадцати байтах каждого стегоконтейнера).

По результатам проведенных экспериментов установлено, что уже при $k_m = 5$ число *неверных* распознаваний при любых значениях искажаемых битов в байте не превышает 2%. Всё остальное – либо верное распознавание, либо отказ от распознавания [2].

Оценим возможности рассматриваемого способа по ***коррекции*** ошибок. На рис. 1-4 проведена оценка стопроцентно верного распознавания в зависимости от количества

Вершинин Игорь Сергеевич – КНИТУ-КАИ, канд. техн. наук, доцент, e-mail: ISVershinin@kai.ru

искажаемых бит в байте (ось Y) и количества ключей (ось X).

Из представленных рисунков видно, что возможности рассматриваемого способа по коррекции ошибок ограничиваются сравнительно малым числом искажений бит в байте.

В противном случае можно говорить только об ***обнаружении*** ошибки, но не ее коррекции.

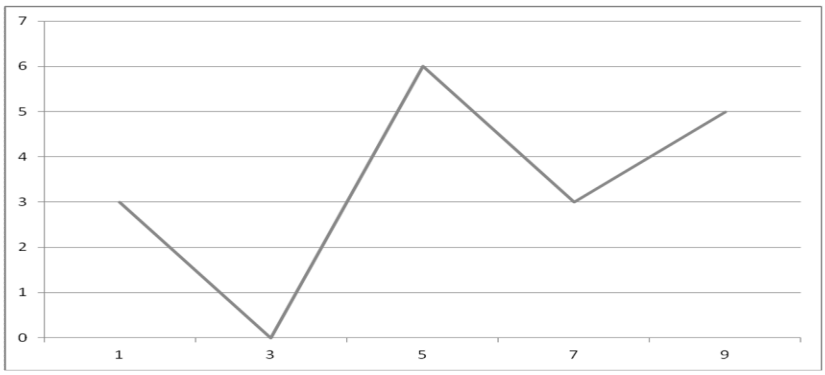

Рис. 1. Случай искажения 16 байт

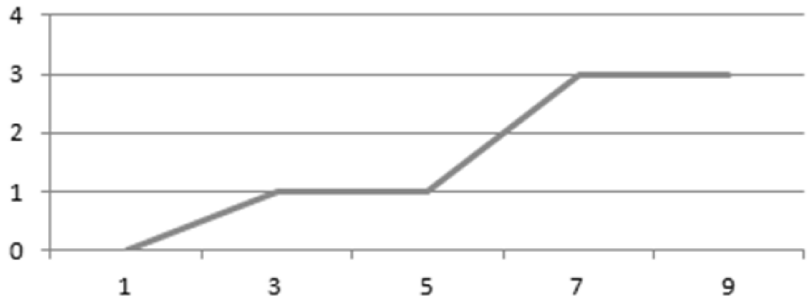

Рис. 2. Случай искажения 32 байт

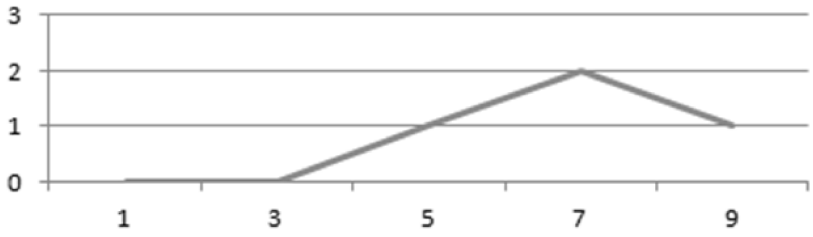

Рис. 3. Случай искажения 64 байт

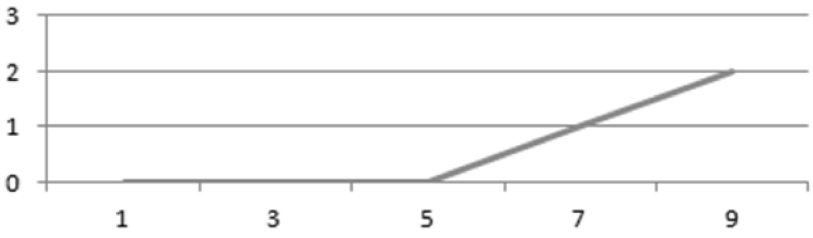

Рис. 4. Случай искажения 128 байт

Для сравнительной оценки эффективности предлагаемого подхода по внедрению избыточности на уровне ключей указанные эксперименты были проведены с использованием менее жесткого критерия – *по большинству*. В этом случае для каждой стегобуквы за результат распознавания принимается эталон, число распознаваний которого

$$k_r \geq (k_m - 1)/2. \quad (2)$$

Если данное условие по результатам распознавания некоторой стегобуквы не выполняется, фиксируется факт ее искажения (отказ от распознавания). Эксперименты проводились по приведенной выше методике.

Результаты представлены на рис. 5-8.

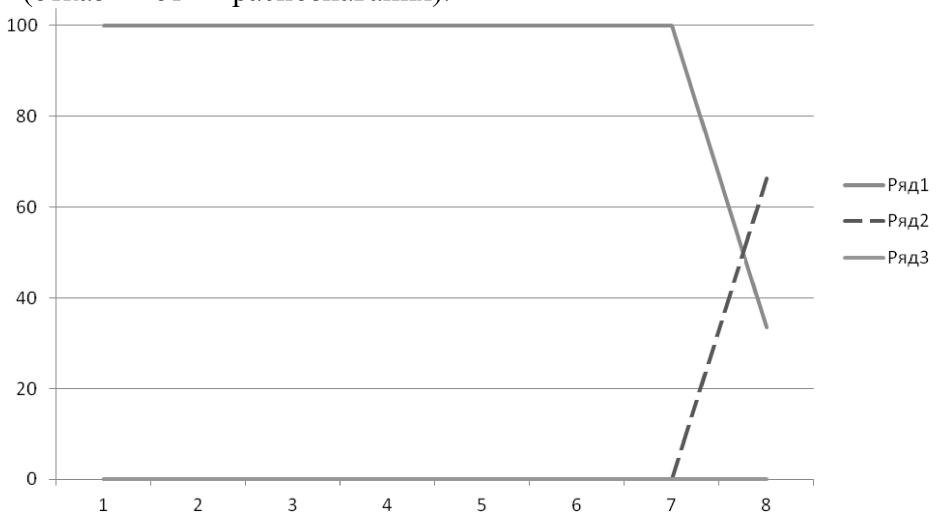

Рис. 5. Искажение 16 байт, $k_m = 3$

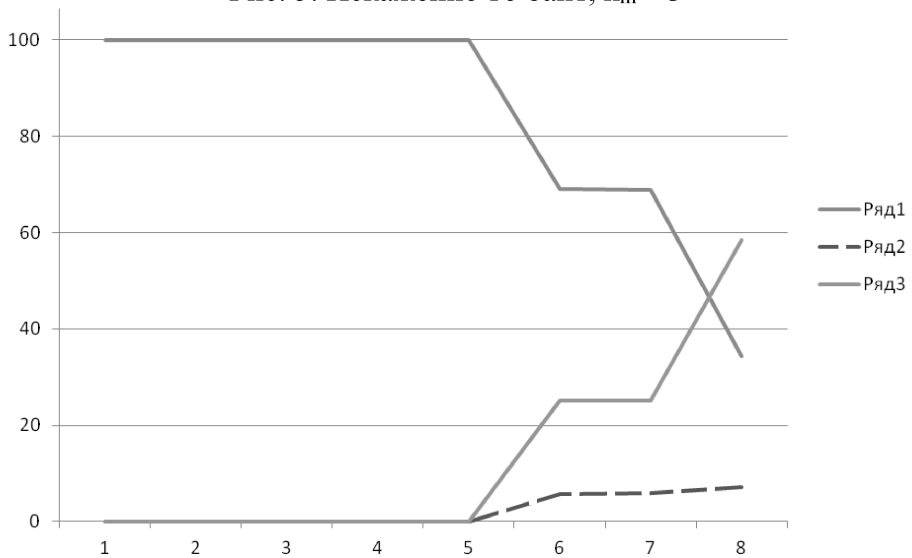

Рис. 6. Искажение 32 байт, $k_m = 7$

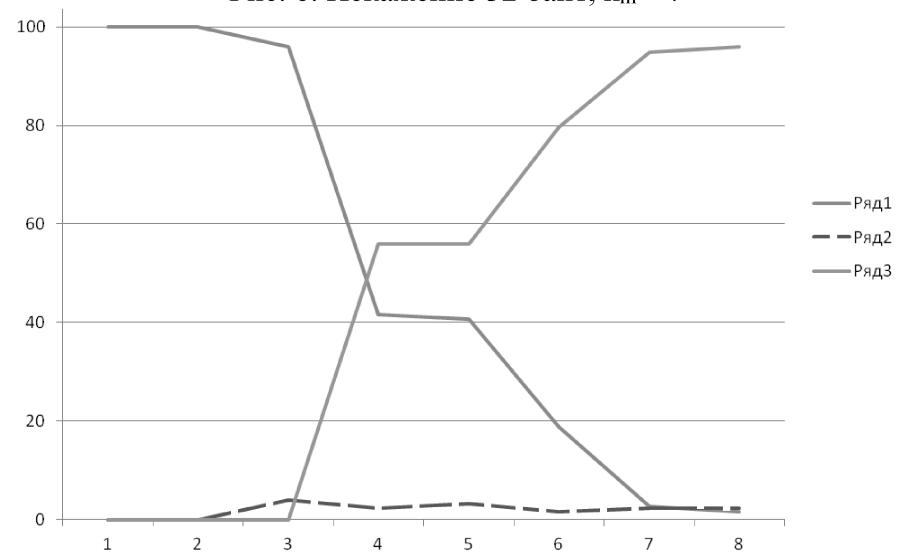

Рис. 7. Искажение 64 байт, $k_m = 7$

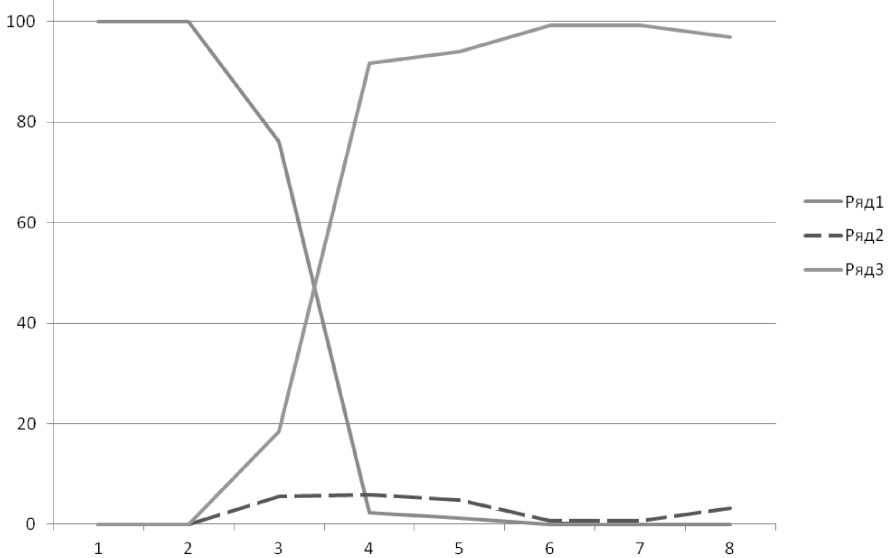

Рис. 8. Искажение 128 байт, $k_m = 7$

Ряд 1 соответствует количеству верных распознаваний (в процентах) в зависимости от количества искажаемых бит в байте, ряд 2 – отказам от распознавания, ряд 3 – неверным распознаваниям.

Для рассмотренного критерия эффективным является случай искажения лишь малого количества байт (16). При этом достаточна минимальная избыточность $k_m = 3$.

Для случаев искажения большего количества байт k_m должен быть равен минимум 7. Однако даже в этом случае число неверных распознаваний достигает 7%. Поэтому для указанных случаев (рис. 6-8) целесообразно использование критерия 1.

Стойкость ассоциативного метода защиты информации при введении избыточности для случая «лобовой» атаки меняется несущественно.

Вопрос стойкости метода при введении избыточности для других видов атак требует проведения отдельных исследований.

Литература

1. Райхлин В.А., Вершинин И.С., Глебов Е.Е. К решению задачи маскирования стилизованных двоичных изображений //Вестник КГТУ им. А.Н. Туполева. 2001. №1. С. 42-47.

2. Вершинин И.С. Помехоустойчивость анализа ассоциативно-защищенных картографических сцен при действии случайных помех //Моделирование систем /под ред. В.А. Райхлина. Труды Республиканского научного семинара «Методы моделирования» – Вып. 5. – Казань: Изд-во «Фэн» («Наука»). 2013. С. 59 – 70.

ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ»
Kazan National Research Technical University

CLARIFICATION OF THE REDUNDANCY ERROR-CORRECTING CRITERION WITHHOLDING INFORMATION WITHIN THE FRAMEWORK OF ASSOCIATIVE STEGANOGRAPHY

I.S. Vershinin

The article deals with the issues of noise immunity of the associative method of steganography by introducing redundancy at the level of the keys given acceptable level of distortion for recognition

Key words: two-dimensional associative masking, associative steganography