УДК 681.3

И. С. Вершинин

СТОЙКОСТЬ АССОЦИАТИВНОЙ ЗАЩИТЫ К АТАКЕ СО ЗНАНИЕМ ОТКРЫТОГО ТЕКСТА

Ключевые слова: двумерно-ассоциативное маскирование, стеганография.

Рассматриваются вопросы стойкости двумерно-ассоциативного механизма маскирования, применяемого для сокрытия информации, к атаке со знанием открытого текста. Предлагается алгоритм оценки стойкости. Приводятся результаты эксперимента.

Keywords: two-dimensionalassociativemasking, steganography.

Considers issues of strength of two-dimensional associative mechanism masking to attack with knowledge of plain text. Provides an algorithm for estimating strength and experimental results.

Введение

Подсистемазащиты информации является важной составляющей системы безопасности предприятий [1]. В состав указанной подсистемы входят, в частности, различные криптографические средства. Используемые в них криптоалгоритмы подразделяются на симметричные, например AES, и асимметричные, например RSA [2]. Однако в ряде случаев разумной альтернативой криптографии является *стеганография* [3].

В работе [4] предложен базовый АЛГОРИТМ маскирования, применяемый для *стегозащиты* стилизованных бинарных изображений – описаний картографических сцен в терминах «объекты – координаты». Имена объектов и их координаты кодируются десятичными цифрами почтового алфавита. В результате бинаризации все 10 символов кода представляются двоичными матрицами-эталонами одинаковых размеров. Для них по АЛГОРИТМу случайно генерируется набор масок.

Бинаризованные коды объектов и их координат погружаются по маскам в т.н. стегоконтейнеры, первоначально заполненные отрезками практически случайных последовательностей двоичных бит. При этом значения незамаскированных бит исходных матриц сохраняются. Тем самым осуществляется необходимая рандомизация. Известный набор масок является ключом распознавания.

Оценка стойкости АЛГОРИТМа проводилась в работах [5, 6]. Рассматривались следующие виды атак:

– атака путем полного перебора ключей;
– атака с позиций точного знания некоторых типов объектов и их координат на карте;
– ассоциации с картой местности;
– атака на гамму.

Была доказана вычислительная стойкость, связанная с невозможностью перебора ключей в приемлемое время.

Вопросы помехоустойчивости. Для борьбы со случайными помехами и преднамеренными помехами дезинформации в работах [7, 8] были предложены:

– модификация АЛГОРИТМА, заключающаяся в запрете использования в качестве дихотомизирующих битов эталонов, находящихся в узловых точках;
– внедрение избыточности для обнаружения и возможной коррекции ошибок.

При этом стойкость к атаке со знанием открытого текста не исследовалась. В этом случае аналитик имеет доступ не только к стеготекстам одного или нескольких сообщений, но и знает их открытые тексты. От него требуется найти ключ, который использовался для сокрытия этих сообщений.

Постановка задачи

Пусть в качестве открытого текста выступает последовательность

1 2 3 4 5 6 7 8 9 0,

представленная в алфавите почтовых индексов. Противнику известен стеготекст данного сообщения, полученный с использованием АЛГОРИТМа двумерно-ассоциативного маскирования и процедуры рандомизации.

Требуется оценить возможность нахождения секретного ключа (истинного набора масок), использованного при рандомизации.

Поиск ключа осуществляется путем нахождения потенциальных битов дихотомизации, по которым формировался ключ (набор масок). Для этого проводится сравнение по каждому биту совокупности эталонов исходного сообщения и соответствующего ему стегосообщения. По каждому совпадающему биту проводится дихотомизация исходного и стегосообщений на подмножества и далее процесс повторяется для полученных подмножеств.

Результатом поиска будет являться множество ключей (наборов масок), по которым из исходного текста мог быть получен соответствующий стеготекст.

Приведем *алгоритм* поиска.

D_0 и B_0 содержат полное множество эталонов и соответствующих им рандомизированных объектов.

1. $l = 0$. $\lambda_0 = 10$.
2. $A_1 = \sum_{i=1}^{\lambda_l} Э_i$ (побитно). $Э_i$ – элементы множества D_l (эталоны).
3. $A_2 = \sum_{i=1}^{\lambda_l} O_i$ (побитно). O_i – элементы множества B_l (рандомизированные объекты).
4. Провести побитное сравнение матриц A_1 и A_2. Определить количество совпадений k_l при условии побитного равенства эталонов и соответствующих им рандоимзированных объектов по

координатам совпадений. Сформировать список C_{l+1} совпадающих координат. Если $\lambda_l \neq 2$, идти к п.5. Иначе – к п. 11 (при $flag_l = 1$) либо к п. 16 (при $flag_l = 0$).

5. $kol1_l := 0$, $kol0_l := 0$. $l := l + 1$.
6. $j_l := 1$.
7. Для j_l-координаты списка C_l сформировать два подмножества D_l и B_l из соответствующих элементов множества D_{l-1} и B_{l-1}, содержащих *единицу* по данной координате. Мощность сформированных подмножеств определяет величину λ_l.
8. Если D_l и B_l – единичные множества, идти к п.10. Иначе – к п.9.
9. $flag_l := 1$. Переход к п.2.
10. $kol1_l := 1$.
11. $kol1_l := k_l$.
12. Для j_l-координаты списка C_l сформировать два подмножества D_l и B_l из соответствующих элементов множества D_{l-1} и B_{l-1}, содержащих ***ноль*** по данной координате. Мощность сформированных подмножеств определяет величину λ_l.
13. Если D_l и B_l – единичные множества, идти к п.15. Иначе – к п.14.
14. $flag_l := 0$. Переход к п.2.
15. $kol0_l := 1$.
16. $kol0_l := k_l$.
17. Если $flag_{l-1} := 1$, то $kol1_{l-1} := kol1_{l-1} + kol1_l \cdot kol0_l$.
    Иначе $kol0_{l-1} := kol0_{l-1} + kol1_l \cdot kol0_l$.
18. $j_l := j_l + 1$.
19. Если $j_l < k_{l-1}$, переход к п.7. Иначе – к п. 20.
20. $l := l + 1$.
21. Если $l > 0$, переход к п. 7 (при $flag_l = 0$) либо к п. 13 (при $flag_l = 1$).Иначе переход к п. 22.
22. Подсчет числа ключей считать законченным. Общее число ключей равно $kol1_0 \cdot kol0_0$.
23. КОНЕЦ.

Приведем пример работы представленного алгоритма для случая трех эталонов в множестве D_0 в алфавите почтовых индексов (0, 1, 2).

На рис. 1 сверху представлены двоичные матрицы для трех почтовых индексов 0, 1 и 2 размером 5×3. На этом же рис. снизу приведены те же эталоны, погруженные по маске в стегоконтейнер (т.е. рандомизированные объекты). Выделены местоположения возможных дихотомизирующих битов, совпадающих для соответствующих эталонов и их рандомизированных представлений.

По первой координате эталон 0 противопоставляется эталонам 1 и 2. Определим дихотомизирующие биты этих двух эталонов. Их количество равно двум (см. рис. 2, а).

По второй координате эталон 2 противопоставляется эталонам 0 и 1. Определим дихотомизирующие биты этих двух эталонов. Их количество равно четырем (см. рис. 2, б).

Таким образом, общее число возможных ключей равно 6.

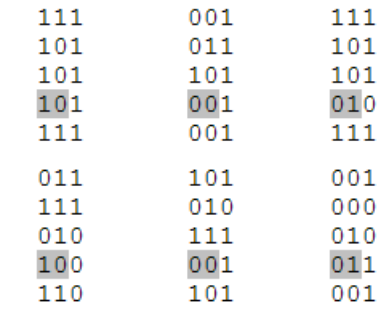
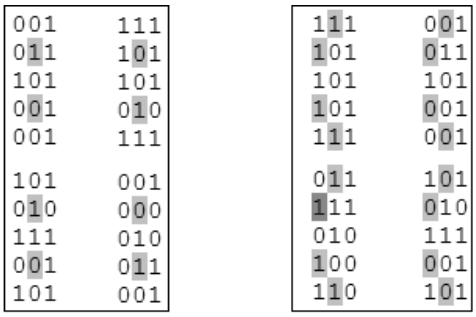


Рис. 1 - Дихотомизирующие биты для трех эталонов



а б

Рис. 2 - Дихотомизирующие биты для двух эталонов

Экспериментальные исследования

Поиск ключей проводился для двух размеров эталонов m = 3 и m = 60 для трех случаев: базового АЛГОРИТМА маскирования, модифицированного АЛГОРИТМА и при внедрении избыточности.

Результаты эксперимента представлены в табл. 1.

Таблица 1 - Результаты эксперимента

Размер эталонов m	3	60
Полное множество ключей	10^{13}	10^{29}
Базовый АЛГОРИТМ	10^{3}	10^{14}
Модифицированный АЛГОРИТМ	10^{3}	10^{14}

В табл. 1 приведены усредненные значения для 10^5 «прогонов» алгоритма поиска ключей для каждого из рассматриваемых случаев.

Для всех рассмотренных случаев количество ключей при соответствующих значениях m одинаково, т.е. *не зависит* от модификации алгоритма и внедрения избыточности.

Обсуждение

Для m = 3 число полученных ключей составило всего 10^3. При этом по ранее проведенным исследованиям [6] полное множество ключей для этого случая – 10^{13}. Таким образом, при m = 3 имеем потерю вычислительной стойкости.

При m = 60 число полученных ключей составило 10^{14} при полном множестве ключей в 10^{29}.

Если принять время испытания одного ключа равным 1 секунде, то при условии одновременный работы 10^5 процессоров полный перебор займет около 30 лет.

Полученные результаты свидетельствуют о возможности проведения потенциально успешной атаки со знанием открытого текста. Для сохранения вычислительной стойкости необходимо увеличение значения m. Однако увеличение m может привести к чрезмерному размеру ключа.

Альтернативой является случай, когда изменение m не осуществляется, при этом, следуя общепринятой практике, проводится регулярная смена ключей с периодичностью один раз в сутки/неделю/месяц.

Литература

1. Патракова Г.Р. *Политика в области управления персоналом и система безопасности на предприятии на примере ОАО «Нижнекамскнефтехим»*//Вестник Казан. технол. ун-та. – 2013. – № 2. – С. 182-184.
2. Кирпичников А.П., Кутепова И.А. *Статистические характеристики криптосистемы RSA*//Вестник Казан. технол. ун-та. – 2013. – № 24 – С. 163-167.
3. Грибунин В.Г., Оков И.Н., Туринцев И.В. *Цифровая стеганография*–М.: СОЛОН-ПРЕСС, 2009. –265 С.
4. 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.
5. Райхлин В.А., Вершинин И.С. *Элементы криптоанализа двумерного карто-графического шифра* //Вестник КГТУ им. А.Н. Туполева. –2002. –№4–С.48-55.
6. Вершинин И.С. *Стойкость ассоциативной защиты распределенных объектов картографии* //Нелинейный мир. Том 9. № 12. –2011. –С. 822-825.
7. Вершинин И.С., Гибадуллин Р.Ф. *Изменение результатов распознавания на множестве замаскированных бинарных матриц при действии аддитивных помех* //Вестник КГТУ им. А.Н. Туполева. –2012. –№4. Вып. 1. –С.198-206.
8. 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.
9. Вершини И.С. *Верхняя оценка числа ключей двумерно-ассоциативной защиты объектов картографии* //Методы моделирования /Под ред. В.А. Райхлина. Труды республиканского научного семинара АН РТ «Методы моделирования». Вып. 4 – Казань: Изд-во «Фэн» («Наука»), –2010.– С. 96-100.

© **И. С. Вершинин -** канд. техн. наук, доц. каф. САУТП КНИТУ, Vershinin_Igor@rambler.ru.

© **I. S. Vershinin -** associate professor, KNRTU, Vershinin_Igor@rambler.ru.