Числовое значение мощности СДР порождающего П(12)-класса порядка $N=12$, созданных по предложенному конструктивному методу, после подстановки в (12) значения выражений (10), (11)

$$\Psi = 2\cdot 3\cdot 36\cdot \Psi_{A(6)B(6)}\cdot 6\cdot \Psi_{C(6)}\cdot \Psi_{D(6)} = 2\cdot 3\cdot 36\cdot 18\cdot 6\cdot 36\cdot 36 = 2^9 3^{10} = 30\,233\,088$$

матриц.

Заключение

Такие огромные мощности класса порождающих СДР порядка $N=12$ привлекательны для криптографической передачи данных, так как позволяют передать большой объем информации. Так произведение Л.Н. Толстого «Война и мир» содержит 3 198 976 символов и это произведение, без смены ключа, описанным криптографическим методом, можно передать 9,45 раз. В дальнейшем предстоит разработать алгоритмы построения порождающих классов больших порядков.

Список литературы

1. Chan, W.K. Summary of perfect $s\times t$ arrays, $1\le s\le t\le 100$ / W.K. Chan, M.K. Siu // Electronics letters. — 1991. — Vol. 27 № 9. — P. 709—710.

2. Мазурков, М.И. Классы эквивалентных и порождающих совершенных двоичных решеток для CDMA-технологий / М.И. Мазурков, В.Я. Чечельницкий // Изв. вузов Радиоэлектроника. — 2003. — № 5. — С. 54—63.

3. Мазурков, М.И. Метод защиты информации на основе совершенных двоичных решеток / М.И. Мазурков, В.Я. Чечельницкий, П. Мурр // Изв. вузов Радиоэлектроника. — 2008. — № 11. — С. 53—57.

4. Чечельницкий, В.Я. Метод криптографической передачи данных на основе совершенных двоичных решеток / В.Я. Чечельницкий, П. Мурр // Защита информации. — 2008. — № 2(38). — С. 32—38.

5. Мазурков, М.И Свойства полного класса совершенных двоичных решеток на 36 элементов / М.И. Мазурков, В.Я. Чечельницкий // Изв. вузов Радиоэлектроника. — 2004. — № 6. — С. 56—64.

Предложен конструктивный метод построения порождающего класса совершенных двоичных решеток размера 12x12 для криптографической передачи информации и получена оценка его мощности.
Ключевые слова: совершенные двоичные решетки, порождающий класс, криптография.

Запропоновано конструктивний метод побудови породжуючого класу досконалих двійкових решіток розміру 12x12 для криптографічного передачі інформації та знайдено оцінку його потужності.

A constructive method which generates a class of perfect binary arrays size 12x12 for cryptographic information transfer and obtain an estimate of its power.

Рецензент: Хорошко В.О.
Надійшла 27.05.2010

УДК 004.056.5

Борисенко И.И. (ОНПУ)

МОДЕЛИ ПРЕДСТАВЛЕНИЯ ИНФОРМАЦИОННОГО КОНТЕЙНЕРА И АНАЛИЗ СОСТОЯНИЯ ЕГО ЗАЩИЩЕННОСТИ

Введение

В настоящее время количество областей, в которых средства электронной связи заменяют бумажную переписку, быстро увеличивается. В результате увеличивается и доступный для перехвата объем информации (носящий конфиденциальный характер), а сам перехват становится более легким [1]. Надежная защита информации от несанкционированного доступа является актуальной, но не решенной в полном объеме проблемой. Одно из перспективных направлений защиты информации сформировали современные методы стеганографии, которые обеспечивают сокрытие самого факта существования секретной информации в той или иной среде и представляют собой

самостоятельное научное направление информационной безопасности. В настоящее время в рамках вычислительных сетей возникли достаточно широкие возможности по оперативному обмену различной информацией в виде текстов, программ, звука, изображений между участниками сетевых сеансов независимо от их территориального размещения, поэтому такие информационные потоки могут быть использованы в качестве *контейнеров* для пересылки *секретной информации* в открытой информационной среде.

В качестве *незаполненного контейнера* (НК) будем рассматривать изображение в градациях серого, т.е. НК – это исходное изображение без какой-либо дополнительной информации. *Секретная информация* - это та дополнительная информация (ДИ), которая каким-либо стеганографическим методом (СМ) встраивается в НК. Процесс встраивания ДИ называется стеганопреобразованием (СП), а результат СП будем называть *информационным контейнером* (ИК).

В основе того или иного СМ лежат различные принципы погружения ДИ, но любой из них должен обеспечить: *надежность восприятия* – ИК не должен зрительно отличаться от НК, достаточную *пропускную способность* (определяется степенью секретности информации) – объем пересылаемой ДИ, *надежность декодирования* – объем правильно восстановленной информации.

При пересылке или хранении ИК может подвергнуться атакам непреднамеренным (шумы в канале связи) или преднамеренным (атаки конкурентов, заинтересованных лиц). В любом случае в дальнейшем объекты, субъекты, события, ставшие причиной нарушения целостности ИК, будем называть – *противник*. Понятно, что чем больше атакующее воздействие, тем большая степень разрушения ИК вплоть до его уничтожения. Будем считать, что, атакуя ИК, противник не намерен себя обнаружить, т.е. атакующее воздействие должно быть таким, при котором обеспечивается надежность восприятия – атака зрительно не заметна.

Универсальных систем и средств защиты на все случаи не существует, т.к. каждая защита создается для конкретной информационной системы, ее окружения и внешней среды, под конкретные угрозы, функциональные требования и требования гарантии защиты [1]. При их изменении защита должна быть способной непрерывно адаптироваться к ним. В связи с этим очень важным становиться вопрос, к каким атакам ИК будет устойчивым, а к каким нет, другими словами, достаточным ли будет объем правильно восстановленной информации из атакованного ИК для адекватного ее восприятия.

Целью данной работы является разработка моделей ИК, дающих возможность учета различий в результатах воздействия атаки на ИК, сформированных различными СМ, что обеспечит решение задачи по установлению устойчивости ИК к предполагаемым атакам.
Для достижения поставленной цели необходимо решить следующие *задачи*:

- Разработать иерархию ИК для его графового представления;
- Определить математический параметр матрицы смежности графа-модели, являющийся формальным представлением хранимой информации ИК;
- Определить способ определения весовых коэффициентов графовой модели ;
- Выбрать способ представления атаки на ИК;
- Разработать совокупную матричную модель «ИК-противник»;
- Разработать метод оценки устойчивости ИК по отношению к предполагаемым атакам;
- Выбрать математический объект, который может быть поставлен в соответствие ИК для построения его геометрической модели;

Построение графовой модели информационного контейнера

Каким бы образом не выполнялось СП – пространственной области, частотной или спектра матрицы контейнера, оно неминуемо приведет к изменению яркости некоторых (всех) его пикселей, что свидетельствует о том, что именно они являются носителями

встроенной ДИ. Пиксели, которые изменили свои значения в результате СП, назовем *информационными элементами* (ИЭ).

Проведем адаптацию графово-матричной модели произвольной информационной системы, построенной в [2], для ИК.

Перейдем непосредственно к построению взвешенного графа-модели ИК, представляющего дерево [3].

Рис.1. Первоначальный вид графа

Этап 1. ИК в целом (корень графа-дерева) рассматривается как изолированная вершина (рис.1), подграф, отвечающий контейнеру, существует изолированно, еще не имея связи с циркулирующей в системе-ИК информацией. Каждый последующий уровень корневой структуры, кроме последнего, представляет собой следующий уровень детализации. В общем случае рациональная степень детальности определяется используемым стегопреобразованием. Последний уровень первоначального графа представлен пикселями, которые составляют подмножества Пі предыдущего уровня и являються листьями корневой структуры. Значения весовых коэффициентов (ВК) графа, вычисление которых рассматривается ниже, отражают реальную защищенность ИЭ. Конкретные значения коэффициентов определяются исходя из СП, которое лежит в основе того или иного СМ и обеспечивают положительную полуопределенность (положительную определенность) матрицы смежности графа.

Этап 2. Построение матрицы смежности *MS* взвешенного графа-модели, которая в силу его неориентированности является симметричной. При помощи нормального спектрального разложения (СР) [4] однозначно определяются спектр (собственные значения – СЗ) и собственные векторы (СВ) *MS* .

Этап 3. Введение связи <1,2> (рис. 2) — информация, подлежащая защите, распределяется в контейнере. Это возмутит *MS* (в результате получается матрица $\overline{MS}$), а значит и ее СЗ и СВ. Совокупность этих возмущений является математическим представлением для имеющейся в ИК информации подлежащей защите. В общем случае информация представляется некоторым подмножеством множества возмущений СЗ и СВ матрицы *MS* .

Рис.2. Корневая структура уровней графа ИК

Будем считать, что все атаки на ИК выражаются в воздействии на листья. Вес вершины на каждом уровне, кроме последнего, определяется как положительное число, большее или равное сумме весов смежных с ней вершин, находящихся на следующем по порядку уровне корневой структуры. Пример взвешенного графа-модели ИК, иллюстрирующий возможное соотношение между весовыми коэффициентами вершин разных уровней, представлен на рис.3 (рядом с узлом – его номер, внутри узла –его вес). Говоря о произвольном ИК, следует заметить, что размерность соответствующего ему графа может быть достаточно большой. Очевидно, основной операцией будет выявление отношений смежности между узлами, поэтому следует выбирать такой способ представления графа, который бы минимизировал время его обработки и объемы памяти для хранения. Наиболее распространенные схемы хранения можно найти в [5] а их анализ - в [2].

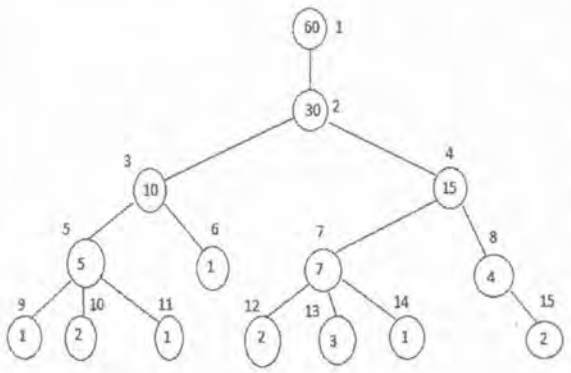

Рис.3. Пример взвешенного графа

Определение математических параметров графово-матричной модели ИК

Поскольку матрица $\overline{MS}$ симметрична, то ее *спектр* содержит лишь хорошо обусловленные СЗ. Хорошая обусловленность СЗ приводит к нечувствительности всего спектра симметричной матрицы $\overline{MS}$ к возмущающим воздействиям или, иначе говоря, к тому, что возмущения СЗ по абсолютной величине сравнимы с самим возмущающим воздействием, чего нельзя в общем случае сказать о СВ (их чувствительность в пределах матрицы зависит от абсолютной отделенности соответствующих СЗ) [4]. Чувствительные СВ могут отклониться на большой угол при малом возмущающем воздействии (даже по причине округлений, происходящих при вычислениях), и тем самым их возмущение не дает истинной информации о величине возмущающего воздействия - о серьезности атаки. Таким образом, об устойчивости ИК предполагаемой атаке будем судить по величине возмущений СЗ.

Количественная оценка устойчивости ИК предполагаемой атаке

Для наглядности изложения рассмотрим одну ветвь корневой структуры (рис. 2), отвечающей одному блоку ИК. Пусть этот блок имеет восемь ИЭ, которые определят подмножество из восьми пикселей, обозначим его П1, в которых находится ДИ, и пусть весовые коэффициенты защищенности ИЭ в этих пикселях имеют такие значения: 3, 1, 1, 5, 1, 5, 1, 1. Сумма этих значений определит вес вершины предыдущего уровня, которая соответствует П1. Неинформационные пиксели блока (они также имеют весовые коэффициенты) определят подмножества П2, П3 и т.д. Сумма весов всех $П_i$ определит вес блока. Поскольку пиксели, в которых нет ДИ, нас пока интересовать не будут, то построим взвешенную ветвь графа-дерева (Рис. 4), обозначим ее $\overline{G}$, без уровня вершин, соответствующих подмножествам $П_i$, что не нарушит общности рассуждений, поскольку вес вершин этого уровня будет учтен в весе блока. Следует заметить, что хотя листья графа и не смежны между собой их нумерация четко определяет последовательное расположение битов ДИ.

Атаку будем моделировать в виде аддитивного гауссовского шума (таким образом в роли противника выступает шум в канале связи) с нулевым средним и $\sigma = 0.0003$: -3, 3, 3, 4, 1, -5, -3, 3- один из возможных вариантов. Такой уровень шума еще не нарушает надежность восприятия ИК, но каждый лист графа подвергается атаке. Будем полагать, что каждый лист

графа может подвергаться атаке с равной долей вероятности и независимо друг от друга, поэтому граф противника будет несвязным, т.е. представляет собой восемь изолированных вершин, а вес каждой вершины определяется одним и тем же положительным числом z. Матрица такого графа, обозначим ее $ATAK$, будет диагональной, а ее диагональные элементы равны z. Анализ результата атаки будет проводиться, используя спектр совокупной графово-матричной модели ИК и противника, поэтому важно, чтобы СЗ ИК хорошо были отделены от СЗ противника. С этой целью значение z выбирается так, чтобы оно удовлетворяло двум условиям: во-первых, z должно быть меньше веса блока, а во-вторых, - больше веса листьев, для определенности положим z =20.

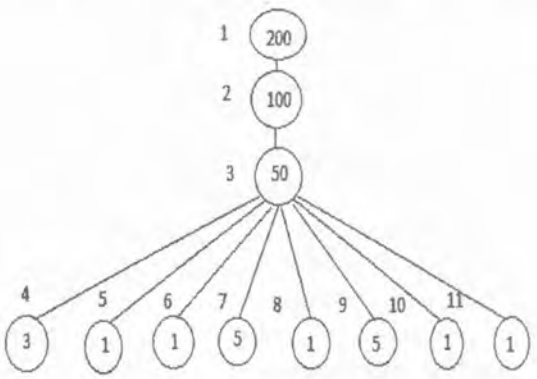

Рис. 4. Взвешенная ветвь графа-дерева ИК

$$\overline{G} = \begin{bmatrix} 200 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 100 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 50 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Рис. 5. Матрица смежности $\overline{G}$

Построим совокупную графово-матричную модель ИК и противника. Матрица смежности C такой модели является блочно-диагональной:

$$C = \begin{pmatrix} \overline{G} & 0 \\ 0 & ATAK \end{pmatrix}.$$

Пока противник не оказывает атакующее воздействие на ИК, связи между блоками $\overline{G}$ и $ATAK$ отсутствуют (наличие нулевых блоков). Спектр блочно-диагональной матрицы является объединением СЗ блоков. Спектр матрицы C для рассматриваемого примера состоит из следующих значений:

200.0200 100.0216 50.1485 20.0000 20.0000 20.0000 20.0000 20.0000 20.0000 20.0000 20.0000 **5.0005 5.0000 3.0002 1.0010 1.0000 1.0000 1.0000 1.0000**

Жирным шрифтом выделены СЗ, которые соответствуют вершинам-листьям, т.е. пикселям, которые осуществляют защиту ДИ. Нас будет интересовать вопрос устойчивости этой защиты предполагаемой атаке.

Проведение атаки будет осуществляться вводом новой связи между диагональными элементами блока $ATAK$ и элементами блока $\overline{G}$, которые соответствуют листьям. Связь будет определяться ребрами, вес которых определяется гауссовским шумом с параметрами, описанными выше. Результатом атаки будет разрушение блочно-диагональной структуры C, итогом которого является матрица $\overline{C}$ (рис. 6), и возмущение СЗ, соответствующих блоку $\overline{G}$. СЗ матрицы $\overline{C}$ выглядят следующим образом:

200.0200 100.0216 50.1485 21.5110 20.9980 20.5130 20.4624 20.4624 20.4624 20.4593 20.0524 **3.9812 3.4668 2.4662 0.9302 0.5376 0.5376 0.5376 0.4535**

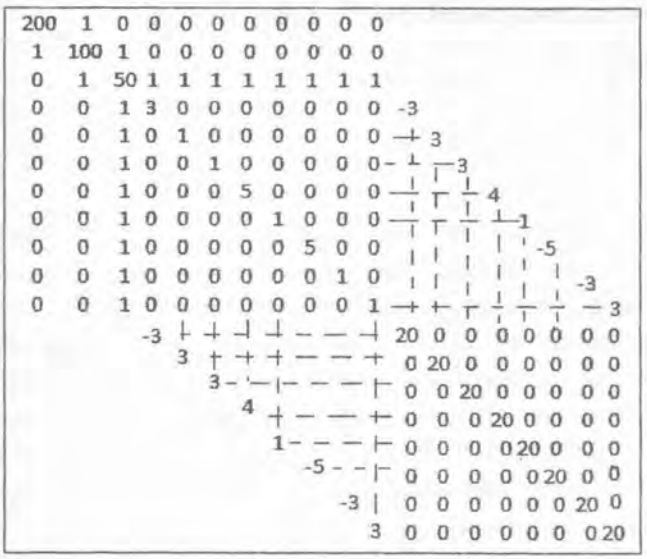

Рис.6. Матричная модель атакованного ИК

Чтобы количественно оценить результат атаки воспользуемся соотношением

$$\delta = \frac{СЗ_и - СЗ_а}{СЗ_а},$$

где δ - относительная погрешность, $СЗ_и$ - СЗ до атаки, $СЗ_а$ - СЗ после атаки. Вычислим δ для СЗ, выделенных жирным шрифтом, т. е. для СЗ, отвечающих листьям.

δ: 0.2560 0.4423 0.2165 0.0761 0.8601 0.8601 0.8601 1.2051

Последние δ, которые отвечают листьям с весовыми коэффициентами равными единице, имеют большие значения (в отличие от листьев с весовыми коэффициентами 3 и 5), что и следовало ожидать, поскольку, естественно полагать, что, чтобы разрушить защиту листа, имеющего весовой коэффициент равный κ, достаточно применить атаку, математическим выражением которой является ребро с весом κ. Для рассматриваемого примера атака, разрушающая защиту всех листьев, выражается реберными коэффициентами: 3 1 1 5 1 5 1 1 (знак коэффициента не имеет значения, поскольку на возмущение СЗ влияет абсолютная величина коэффициента (Лемма Гершгорина [6] о локализации СЗ)). Спектр матрицы $\overline{C}$ после такой атаки выглядит следующим образом:

200.0100 100.0200 50.1482 21.5139 21.5081 20.5129 20.0525 20.0525 20.0525 20.0525 20.0520 **3.4861 3.4491 2.4663 0.9475 0.9475 0.9475 0.9475 0.8433,** а относительная погрешность δ: 0.4448 0.4498 0.2165 0.0554 0.0554 0.0554 0.0554 0.1858, т.е. относительная погрешность между $СЗ_и$ и $СЗ_а$ порядка 0.0554 и выше свидетельствует о том, что защита листа с единичным весом разрушена. Понятно, что при выборе пикселей для встраивания ДИ, нужно стремится к тому, чтобы их защищенность была как можно выше. Допустим, в блоке есть другое подмножество пикселей, с весовыми коэффициентами их защищенности: 1, 2, 5, 6, 2, 5, 5, 1, обозначим его П2. Предпримем ту же атаку. Для построения матричной модели не атакованного и атакованного ИК выполним действия, изложенные выше. Получим матрицу C и матрицу $\overline{C}$ аналогичные тем, которые были построены для П1, но вместо диагональных элементов 3, 1, 1, 5, 1, 5, 1, 1 выполним подстановку 1, 2, 5, 6, 2, 5, 5, 1 соответственно.

Спектр матрицы C:

200.0200 100.0216 50.1513 20.0000 20.0000 20.0000 20.0000 20.0000 20.0000 20.0000 20.0000 **5.9792 5.0000 5.0000 4.9338 2.0000 1.9591 1.0000 0.9567**

Спектр матрицы $\overline{C}$:

200.0200 100.0200 50.1526 21.5110 21.0600 20.5777 20.5754 20.4860 20.4624 20.4608 20.0553 **4.9193 4.4223 4.3805 3.4661 1.9247 1.4924 0.5376 0.4959**

δ: 0.2155 0.1306 0.1414 0.4234 0.0391 0.3127 0.8601 0.9292

Сравнивая δ для листьев последовательности П1 и листьев последовательности П2 замечаем, что возмущения для первых трех выделенных собственных значений и пятого СЗ

меньше для П2. Полученный результат объясняется тем, что эти собственные значения соответствуют листьям подмножества П2 с бóльшими весовыми коэффициентами:

№ листа:	4	5	6	7	8	9	10	11
ВК П1:	3	1	**1**	**5**	**1**	5	**1**	1
ВК П2:	1	2	**5**	**6**	**2**	5	**5**	1
атака:	3	3	3	4	1	5	3	3

Т.о П2 более предпочтительно для погружения ДИ, поскольку уже четыре листа (с номерами 6, 7, 8, 10) будут устойчивы к предполагаемой атаке вместо одного, как в случае с П1 (лист с номером 7), но остальные листья по-прежнему не обеспечивают защиту ИЭ.

Пусть $\pm\theta$ - максимально возможная атака на ИЭ (такое ограничение мы всегда можем допустить, поскольку должно выполняться требование надежности восприятия ИК, в противном случае противник себя обнаружит), тогда, чтобы обеспечить защищенность всех ИЭ, весовые коэффициенты листьев, которые выполняют роль их защиты, должны быть не меньше θ. Назовем такое подмножество листьев оптимальным и обозначим его $\Pi_{опт}$. Положим для определенности $\theta = 7$. Построим матрицы C и $\overline{C}$ для $\Pi_{опт}$.

Спектр матрицы C:

200.0200 100.0200 50.1653 20.0000 20.0000 20.0000 20.0000 20.0000 20.0000 20.0000
20.0000 **7.000 7.000 7.000 7.000 7.000 7.000 7.000 6.8147**

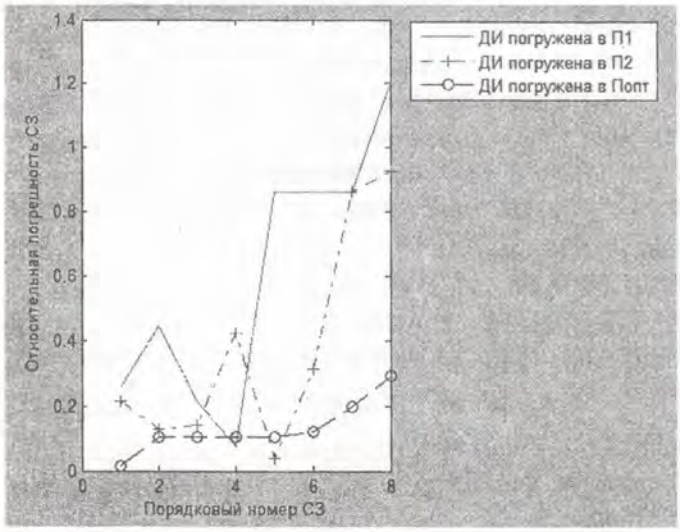

Рис. 7. Представление атакованного ИК относительными погрешностями СЗ

Спектр матрицы $\overline{C}$:

200.0200 100.0200 50.1668 21.6971
21.1297 20.6589 20.6589 20.6589
20.6589 20.6511 20.0763 **6.9048**
6.3411 6.3411 6.3411 6.3411 6.2368
5.8416 5.2758

δ: 0.0138 0.1039 0.1039 0.1039
0.1039 0.1224 0.1983 0.2917

Понятно, что в этом случае защищены будут все ИЭ в полной мере, более того, $\Pi_{опт}$ обеспечит защиту и при увеличении значений атаки до ± 7 на каждый информационный элемент.

Сравнение возмущений спектров матриц, построенных для различных локализаций ДИ, но в условиях одной и той же предполагаемой атаки дан на рис. 7. Из полученных результатов (Рис.7) следует, что минимальные возмущения получают листья подмножества $\Pi_{опт}$, а значит листья, составляющие эту последовательность обеспечивают защиту ИК и должны использоваться для погружения ДИ. Поиск оптимальной (в смысле защищенности) последовательности пикселей в блоке для погружения ДИ не является тривиальной задачей не только в вычислительном смысле, но такой последовательности, как правило, в блоках реальных изображений не существует. Поэтому обеспечение максимально возможной защиты ДИ должно обеспечиваться СМ при СП.

Определение весовых коэффициентов ИЭ

Пусть в результате некоторого СП сгенерирован ИК. Чтобы после декодирования получить правильно восстановленную информацию в полном объеме значения яркостей

пикселей, в которые она была погружена, т.е. ИЭ должны находиться в заданных пределах. Не сужая общности рассуждений, рассмотрим один ИЭ со значением m равным $m = 200$, который должен сохранить это значение при пересылке в пределах от 214 до 199, т.е. $m \in [214;199)$. Изменение значения m на -1 или +15 при пересылке выведет данный ИЭ из заданного полуинтервала, что будет соответствовать уничтожению в нем ДИ. Таким образом, весовой коэффициент, определяющий защищенность данного ИЭ, может быть либо 1 либо 15. В зависимости от конкретного вида предполагаемой атаки выбирается одно из двух значений.

Модель информационного контейнера, основанная на знаковой чувствительности

Наряду с оценкой классической чувствительности для всестороннего анализа результата некоторых задач из области информационной безопасности значимой также будет оценка знаковой чувствительности (*sign-чувствительности)* [2].

Sign-чувствительность ИК определяется как sign-чувствительность соответствующего ему математического объекта P.

Очевидно, что sign-чувствительность (ЗЧ) (sign-нечувствительность (ЗНЧ)) любого объекта P сведется к ЗЧ (ЗНЧ) скалярных элементов, которые его составляют. Естественно полагать, что чем больше sign-чувствительных скалярных элементов в составе объекта, тем более этот математический объект sign-чувствительный в целом, тем более sign-чувствительным окажется соответствующий ИК. Если математическим объектом является вектор $x \in R^n$, то *достаточным условием* его sign-чувствительности является малость $\|x\|_1$, где $\|\bullet\|_1$ — векторная 1-норма [7], чем меньше $\|x\|_1$, тем более sign-чувствительным будет x (выбор нормы не существенен).

Очень часто при работе с векторами, когда они используются в качестве математического инструмента для анализа свойств реальных объектов, прибегают к их нормированию. Результатом произвольного возмущающего воздействия для нормированного вектора является его поворот на некоторый угол, а ЗЧ геометрически означает, что он составляет малый угол (углы) с координатной плоскостью (плоскостями), о чем свидетельствует малость модулей его некоторых координат по сравнению с другими координатами. *Достаточным условием* нормальной знаковой нечувствительности - nsign-нечувствительности (НЗНЧ) вектора $x \in R^n$ является сравнимость между собой значений модулей всех его координат (малый разброс этих значений в сегменте [0,1]), что геометрически соответствует сравнимости всех углов между вектором и координатными плоскостями. Наименьшей nsign-чувствительности отвечает равенство всех координат вектора (равенство всех углов между вектором и его проекциями на координатные плоскости).

Нормированный вектор $\bar{x} = \left(\frac{1}{\sqrt{n}}, \frac{1}{\sqrt{n}}, ..., \frac{1}{\sqrt{n}}\right)^T$, обладающий наименьшей НЗЧ, называется *n-оптимальным.*

Для исследования связи между ЗЧ и НЗЧ вектора будем использовать ВК для П1 и П2 из п. 2.2, представив эти последовательности в виде 8-компонентных векторов x_1 и x_2: $x_1 = (3,1,1,5,1,5,1,1)^T$, $x_2 = (1,2,5,6,2,5,5,1)^T$. Значения координат вектора x_1 малы, поэтому этот вектор является sign-чувствительным, уменьшив значения четвертой и шестой координаты мы можем получить nsign-нечувствительный и sign-чувствительный вектор одновременно. Если значения всех координат будут равны единице, то получим n-оптимальный вектор. Рассмотрим x_2 sign-чувствительность этого вектора меньше, поскольку пять его координат из восьми имеют бóльшие значения, чем соответствующие координаты вектора x_1, а следовательно, и $\|x\|_1 < \|x\|_2$, это дает некоторое преимущество x_2

перед x_1. С другой стороны координаты вектора x_2 не являются сравнимыми между собой и при его нормировании это приведет к значительному разбросу значений координат в сегменте [0,1]. Например, нормированное значение первой координаты равно 0.09, а четвертой 0.545, поэтому x_2 является nsign-чувствительным. Таким образом, знаковая чувствительность — это математический параметр, качественное изменение которого различно в зависимости от характера возмущающего воздействия.

Координаты векторов x_1 и x_2 представляют собой весовые коэффициенты защищенности ИЭ, поэтому сами x_1 и x_2 являются тем математическим объектом, который может быть поставлен в соответствие системе защиты ИК. Основываясь на знаковой чувствительности обоих векторов, заключаем, что ни один из них не может обеспечить безопасность ИЭ.

Построение геометрической модели ИК

Рассмотрим некоторый блок реального изображения размерности 8x8. Пусть ДИ погружено в некоторый столбец. После СП пиксели приняли такие значения яркости в градации серого: 200 186 164 175 186 204 210 199, как и раннее, будем называть эти пиксели ИЭ. Значения яркости пикселей, которые для реального изображения могут принимать от 0 до 255, нанесем на окружность единичного радиуса с центром в точке M. Каждому ИЭ поставим в соответствие вектор с началом в точке M и концом на окружности в точке, которая соответствует яркости пикселя, который является информационным элементом. Для каждого вектора определим сектор окружности, в котором он принимает свое первоначальное положение. Сектор будет определяться некоторым подмножеством значений яркости, нанесенных на окружность, причем, только одна граница сектора, определяемая бóльшим числом, будет ему принадлежать. Поскольку все вектора, отвечающие ИЭ, нормированы, то в основу построения геометрической модели положим нормальную знаковую чувствительность. Моделирование атаки будем проводить при помощи поворота векторов на угол, который будет определяться атакой. Атаку, как и прежде, моделируем при помощи гауссовского шума и конкретное ее выражение задается той же последовательностью, что и в п. 2.2, т.е.: -3 3 3 4 1 -5 -3 3. Переход вектора в другой сектор или на границу, которая не принадлежит сектору, в котором вектор занимал свое исходное положение (до атаки), будет сигнализировать о разрушении ИЭ. Геометрическая модель, соответствующая первым трем ИЭ из восьми, что не сужает общности построения, изображена на рис. 8. Проанализируем результат атаки. Вектор x_1 повернулся на угол, который перевел его в соседний сектор, что соответствует тому, что ИЭ разрушен. Вектора x_2 и x_3 остались в своих секторах, следовательно, предпринятая атака безопасна для ИЭ, которые соответствуют этим векторам.

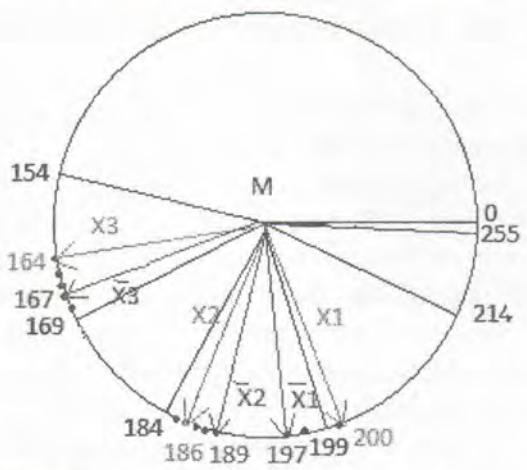

Рис.8. Геометрическая модель ИК, основанная на *nsign*-чувствительности

В отличие от классической чувствительности, sign-чувствительный (nsign-чувствительный) вектор может не проявить свою знаковую чувствительность, даже претерпев большое возмущение (конец вектора x_2 отстоит от границы со значением 184 всего на две единицы, что определяет малый угол между ними (рис. 8)). Для реакции sign-чувствительного вектора на возмущение важно геометрическое направление этого возмущения при его математическом представлении, т.е. проявление или не проявление

последствий ЗЧ, НЗЧ в виде изменения знака координат будет зависеть от конкретики возмущающего воздействия. Однако, если вектор $x \in R^n$ является нечувствительным в обычном смысле, т.е. угол его отклонения при малом возмущающем воздействии мал, то вероятность проявления последствий НЗЧ при ее наличии у такого вектора, т.е. вероятность того, что этот малый угол все же выведет исходный вектор за пределы исходного ортанта, будет очевидно меньше, чем у чувствительного в обычном смысле. Таким образом чувствительность (нечувствительность) вектора в обычном смысле и НЗЧ (НЗНЧ) в общем случае никак не определяют одна другую, однако, чем менее (более) чувствительным будет вектор в обычном смысле, тем менее (более) вероятным будет проявление его НЗЧ (при наличии таковой) в виде изменения знаков (знака) координат. Вернемся к анализу геометрической модели (рис. 8). Изменим геометрическое направление возмущения рассматриваемой системы векторов, т.е. предпримем атаку вида: 13 10 -9. В результате такой атаки концы векторов x_1 ,x_2 и x_3 переместятся в точки со значениями 213 196 и 155 соответственно, но все три вектора останутся в секторах, в которых они находились до атаки, т.е. атака оказалась безопасной, не смотря на то, что сила возмущающего воздействия гораздо больше, по сравнению с атакой вида: -3 3 3. Понятно, что если исходное положение вектора будет соответствовать биссектрисе угла, который определяет сектор (т.е. составит равные углы с границами сектора), то такой вектор будет одинаково реагировать как на положительные так и на отрицательные возмущения одинаковые по абсолютной величине, т.е такой вектор становится nsign-нечувствительным (более того, он n-оптимальный). Если все вектора, которые соответствуют всем ИЭ ИК перевести в положение биссектрисы сектора, которому они первоначально принадлежат, то таким образом будет построен nsign-нечувствительный ИК (n-оптимальный ИК). Если границы каждого сектора достаточно отстоят друг от друга, т.е. составляют достаточно большой угол, то такой ИК также будет и sign-нечувствительным. На практике построение такого идеального ИК достаточно проблематично, одной из причин, например, является обеспечение надежности восприятия, т.е. незаметности результата стегопреобразования. Различные СМ используют уникальную, присущую только данному СМ, методику встраивания ДИ в контейнер. В результате СП формируются ИЭ, вектора которых далеко не всегда являются n-оптимальными. Для сравнения эффективности различных СМ с точки зрения их устойчивости можно использовать степень отличия векторов x, отвечающих ИЭ, от n-оптимального. В качестве меры такого отличия логично использовать угол между векторами x и n-оптимальным. Пример такого сравнения можно найти в [2].

Заключение

В работе представлена разработка графовой и геометрической моделей ИК. В основе геометрического представления ИК лежит знаковая чувствительность объекта его представляющая, т.е. вектора, компонентами которого являются ИЭ, что позволяет учесть качественную и количественную реакцию ИК на атаку в зависимости от ее конкретного (в зависимости от направленности) выражения.

Предложенная графовая модель ИК, которая отражает его иерархию, позволяет точно локализовать возмущения СЗ спектра, отвечающим ИЭ, - эти СЗ являются формальным представлением дополнительной информации в ИК.

В независимости от способа построения модели ИК получены одинаковые результаты, которые обосновывают вывод о том, что если ДИ после погружения в контейнер математически можно представить как оптимальный вектор, то такой ИК будет устойчив к атакам, при которых соблюдается надежность восприятия. Пример получения такого оптимального вектора для конкретного алгоритма можно посмотреть, например, в [8]. Следует отметить, что конкретную реализацию геометрической и графовой модели будет определять СП, которое лежит в основе любого СМ.

Построенные модели ИК просты, наглядны и могут использоваться непосредственно с целью учета различий в результатах воздействия атаки на различные ИЭ при разработке новых СМ и повышения устойчивости уже существующих.

Список литературы

1. Ленков С.В. Методы и средства защиты информации: в 2 т. / С.В.Ленков, Д.А.Перегудов, В.А.Хорошко. — К.: Арий, 2008 — . —Т.2: Информационная безопасность. — 2008. — 344 с.

2. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности.-К.:ДУИКТ, 2009.-250 с.

3. Ф. Харари. Теория графов.-М.:Мир,1973.-300 с.

4. Кобозєва А.А. Загальний підхід до оцінки властивостей стеганографічного алгоритму, заснованого на теорії збурень. - Информационные технологи и компьютерная инженерия, №1(11), 2008, с.164-171.

5. Джордж А. Численное решение больших разреженных систем уравнений / А.Джордж, Дж.Лю; пер. с англ. Х.Д.Икрамова. — М., Мир, 1984. — 333 с.

6. Гантмахер Ф.Р. Теория матриц / Ф.Р.Гантмахер. — М.: Наука, 1988. — 552 с.

7. Деммель Дж. Вычислительная линейная алгебра / Дж.Деммель; пер.с англ. Х.Д.Икрамова. — М.: Мир, 2001. — 430 с.

8. Борисенко И.И. Повышение помехоустойчивости стеганографического алгоритма – Сучасний захист інформації, №1, 2010, с.36-42.

Представлены две математические модели информационного контейнера (ИК), которые дают возможность оценить его устойчивость к предполагаемой атаке. В качестве инструмента для анализа реакции ИК на атаку в графовой модели используется спектр матрицы смежности графа «ИК-противник», а в геометрической модели – знаковая чувствительность векторов, которые являються математическим объектом ИК.

Запропоновані дві моделі інформаційного контейнера (ІК), які дають можливість оцінити його стійкість до ймовірного нападу. В якості інструмента для аналізу реакції ІК на напад в графовій моделі використовується спектр матриці суміжності графа «ІК - супротивник», а в геометричній моделі – знакова чутливість векторів, які є математичними об'єктами ІК.

Two mathematical models of information cove image (ICI) for estimate noise stability it to the assumption attack are presented in this paper. In the graph model is used spectrum of adjacency matrix of graph "ICI – adversary" for analysis a reaction ICI on the attack, but in the geometrical model is used sign sensibility of vectors that are mathematical object ICI.

Рецензент: Єрохін В.Ф.
Надіслано 04.11.2010

УДК 681.3:004.681

Опірський І.Р. (НУ «Львівська політехніка»)

ЕНТРОПІЯ ВОЛЗ ПРИ ВРАХУВАННІ ЗАВАД В ІНФОРМАЦІЇ, ЩО ПЕРЕДАЄТЬСЯ

Вступ

Зупинившись на понятті інформація в оптико-волокнній системі звязку, неможливо не торкнутися іншого суміжного поняття - ентропія. Вперше поняття ентропія і інформація зв'язав К.Шеннон в 1948р. З його подачі ентропія почала використовуватися як міра кількості інформації в процесах передачі сигналів по проводах. Слід підкреслити, що під інформацією Шеннон розумів сигнали потрібні, корисні для одержувача. Некорисні сигнали, з погляду Шеннона,- це шум і завади. Якщо сигнал на виході каналу зв'язку є точною копією сигналу на вході то, з погляду теорії інформації, це означає відсутність ентропії.

Питання визначення ентропії сигналу в оптичному волокні є досить важливим. При проходженні сигналу на великих відстання по волоконно-оптичній системі ми обовя'зково будемо мати деяку втрату сигналу саме через ентропію. Поняття ентропії вперше було введене в термодинаміці для визначення міри необоротного розсіювання енергії. При