УДК 004.056.5: 518: 512.624.3

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 2, pp. 99-104

ОБЩИЙ ПОДХОД К АНАЛИЗУ СОСТОЯНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ КАК ТЕОРЕТИЧЕСКИЙ БАЗИС ДЛЯ СТЕГАНОАЛГОРИТМОВ, УСТОЙЧИВЫХ К АТАКЕ СЖАТИЕМ

А.А. Кобозева, М.А. Мельник, П.Е. Баранов

Одесский национальный политехнический университет
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: ritochek@yandex.ua

В работе выявлены и обоснованы недостатки при обеспечении устойчивости стеганоалгоритмов к атаке сжатием в случае организации стеганопреобразования в частотной, пространственной/временной области контейнера, в качестве которого выступают цифровые изображения, аудио и видео последовательности. Показано, что одной из основных причин отсутствия окончательного решения обсуждаемой задачи является отсутствие единого теоретического базиса, общего математического подхода к ее решению. Обосновано, что перспективным, с точки зрения построения на его основе стеганоалгоритмов, устойчивых к сжатию, в том числе со значительными коэффициентами, является общий подход к анализу состояния и технологии функционирования информационных систем, основанный на теории возмущений и матричном анализе.

Ключевые слова: стеганоалгоритм, атака против встроенного сообщения, устойчивость к сжатию, общий подход к анализу состояния и технологии функционирования информационных систем

Введение

Стеганографическая система сегодня является одной из наиболее значимых составных частей комплексной системы защиты информации [1]. Компьютерный характер современной стеганографии обусловил широкое использование в качестве контейнеров (в том числе, и в настоящей работе) цифровых изображений, видео, аудио.

При разработке стеганографической системы необходимо учитывать требование устойчивости этой системы к активным атакующим действиям. Одними из наиболее пагубных атак являются атаки против встроенного сообщения [2], имеющие своей целью разрушение конфиденциальной информации, передающейся посредством организации скрытого канала внутри канала общего пользования. К атакам против встроенного сообщения относятся: наложение шума на стеганосообщение (СС), его фильтрация, сжатие с потерями. Последняя из перечисленных атак является сегодня чрезвычайно распространенной благодаря популярности и необходимости использования форматов с потерями для хранения и передачи цифровых сигналов (в частности, цифровых изображений (ЦИ)). По этой же причине действия атакующего, связанные с пересохранением СС в формат с потерями, не привлекают к себе внимание адресатов и могут остаться незамеченными. Организаторы скрытого канала заинтересованы в том, чтобы результат таких действий не привел к разрушению передаваемой информации. Кроме того, учитывая реалии сегодняшнего дня, необходимо отметить, что пересылка ЦИ, аудио, цифрового видео в формате без потерь сама по себе привлекает внимание и вызывает подозрение. Поэтому при организации

стеганографического канала связи для передающей стороны целесообразно использовать форматы с потерями еще на этапе формирования СС.

Из всего вышесказанного очевидным является вывод: при организации скрытого (стеганографического) канала связи необходимо использовать стеганоалгоритмы, устойчивые к сжатию, что даст возможность еще до пересылки сохранять СС в привычном сегодня формате с потерями, не привлекающем внимания (например, Jpeg для ЦИ), а также извлекать дополнительную информацию (ДИ) в случае, если СС подверглось соответствующей атаке.

На сегодняшний день существует значительное количество различных стеганографических алгоритмов (СА), которые позиционируются авторами как устойчивые к сжатию [3-5], однако все эти алгоритмы не лишены значительных недостатков: многие из них не обеспечивают устойчивость к сжатию со значительными коэффициентами, многие не обеспечивают надежность восприятия формируемого СС. Необходимо отметить, что при рассмотрении данной проблемы в современной научной литературе большое внимание уделяется устойчивости к сжатию СА, реализующих погружение цифровых водяных знаков (где надежность восприятия СС часто не требуется), а вот алгоритмы организации скрытого канала связи рассматриваются гораздо реже. Причина этому ясна: сложность одновременного обеспечения устойчивости к сжатию (со значительными коэффициентами) и надежности восприятия СС, обусловленная отсутствием единого теоретического базиса, общего математического подхода для решения рассматриваемых задач. Развитие стеганографии в направлении создания устойчивых к сжатию стеганометодов сегодня идет по экстенсивному пути, при помощи накопления все большего количества различных СА, которые не отличаются друг от друга принципиально, а лишь незначительно улучшают параметры своей работы относительно «предшественников».

Таким образом, *цель* настоящей работы, заключающаяся в выборе математических основ для построения теоретического базиса для разработки стеганографических методов и алгоритмов, гарантированно устойчивых к сжатию, в том числе, со значительными коэффициентами, обеспечивающих надежность восприятия СС, для повышения эффективности работы стеганосистемы, и, как следствие, комплексной системы защиты информации, является *актуальной*.

Основная часть

Анализ современных научных публикаций, касающихся разработки стеганометодов и алгоритмов, устойчивых к атаке сжатием, в том числе, со значительными коэффициентами, приводит к следующим выводам.

Подавляющее большинство СА, позиционируемых как устойчивые к сжатию, производит стеганопреобразование в частотной области контейнера, или основного сообщения (ОС) [4,5], основываясь на спорном в свете [1,6] утверждении, что более устойчивыми к разнообразным искажениям, в том числе, к сжатию, являются СА, использующие для стеганопреобразования именно частотную область. Такие алгоритмы, основываются на компромиссе между требованиями надежности восприятия формируемого СС и устойчивости к сжатию, достигаемом в большинстве случаев за счет использования в процессе стеганопреобразования, главным образом, среднечастотных коэффициентов. Однако этот компромисс не позволяет достичь эффективного декодирования ДИ при значительном сжатии СС, он является определенным ограничителем на повышение эффективности стеганосистемы. Оставаясь в рамках такого подхода, невозможно повышение устойчивости к сжатию разрабатываемых стеганометодов, СА и соответствующих стеганосистем.

В связи с этим интерес вызывают попытки ученых выйти за границы среднечастотной области при организации внедрения ДИ. Но хотя эти попытки и

предпринимаются, они не содержат ничего принципиально нового в подходе к решению рассматриваемой задачи [7-9]. Основными недостатками существующих СА, использующих значимые частотные коэффициенты в процессе организации стеганопреобразования, являются:

- негарантированность обеспечения надежности восприятия СС за счет значительного возмущения матрицы ЦИ при возмущениях низкочастотных коэффициентов;
- для соблюдения надежности восприятия СС при организации стеганопреобразования за счет возмущения низкочастотных коэффициентов ОС эти возмущения необходимо настолько малы, что для декодирования ДИ требуется наличие контейнера, что на практике часто не имеет места.

Подлежит сомнению не только мнение о преимуществе частотной области стеганопреобразования в свете устойчивости стеганосистемы к сжатию. Авторы [10] утверждают, что СА может быть устойчивым к сжатию только тогда, когда он будет учитывать особенности реализации алгоритма перспективного сжатия: алгоритм, устойчивый к сжатию, основанному на вейвлет-преобразовании (Jpeg2000), может оказаться неустойчивым к сжатию, основанному на дискретном косинусном преобразовании (Jpeg). С учетом того, что сжатие является лишь одним из возмущающих воздействий на СС [1], специфика которого – это обнуление высокочастотных составляющих сигнала, такое мнение в общем случае является ошибочным, оно ограничивает возможности для построения СА, устойчивых к компрессии.

Таким образом, в рамках частотной области, используемой для организации стеганопреобразования, обеспечение одновременной устойчивости СА к сжатию со значительными коэффициентами, надежности восприятия СС, организации процесса декодирования без наличия контейнера вызывает непреодолимые трудности. Использование частотной области принципиально не позволяет проводить дальнейшее увеличение устойчивости разрабатываемых стеганоалгоритмов к сжатию.

Организация стеганопреобразования в рамках пространственной/временной области контейнера [3] в общем случае также не может гарантировать устойчивости СА: все пиксели матрицы ЦИ, кадра видеопоследовательности, отсчеты цифрового аудио равноправны; изменения каких-либо из них (например, максимальных, минимальных, стоящих на определенных местах и т.д.) не отвечают, в общем случае, каким-либо определенным частотным характеристикам. Крайне затруднительно в пространственной/временной области управлять процессом, связанным с необходимостью изменений конкретных частотных составляющих сигнала.

Таким образом, для интенсификации процесса решения рассматриваемой задачи требуется выход за пределы частотной, пространственной/временной областей контейнера для организации стеганопреобразования, использование новых математических инструментов и подходов.

Перспективным с точки зрения построения на его основе стеганоалгоритмов, устойчивых к сжатию, в том числе, со значительными коэффициентами, является общий подход к анализу состояния и технологии функционирования информационных систем (ОПАИС), основанный на теории возмущений и матричном анализе [1].

Основная идея этого подхода заключается в следующем. ЦИ, видео, а также аудио последовательность формально можно представить в виде одной или конечного множества двумерных матриц. В силу этого в качестве ОС, не ограничивая общности рассуждений, для простоты изложения рассматривается ЦИ в градациях серого с матрицей F. Результат стеганопреобразования, независимо от способа и области погружения ДИ, формально представляется в виде совокупности возмущений полного набора параметров [1], определяющих матрицу ОС (или матрицы блоков ОС). При этом последующие изменения СС, в том числе и в результате активных атакующих действий

(в частности, атаки сжатием), формализуются в виде дополнительных возмущений полного набора параметров. В качестве такого набора может использоваться набор сингулярных чисел (СНЧ) и ортонормированных лексикографически положительных сингулярных векторов (СНВ) соответствующих матриц, однозначно определяемых их нормальным сингулярным разложением, целесообразность использования которого подробно обоснована в [1] (везде ниже, если не оговорено особо, сингулярные векторы рассматриваются в ортонормированном лексикографически положительном виде). Таким образом, результат сжатия СС с потерями формально представляется как совокупность возмущений СНЧ и СНВ соответствующей матрицы (матриц) СС.

В [1,6] показано, что свойства СА, в том числе, их устойчивость к активным атакующим действиям, определяются величинами и локализацией возмущений СНЧ и СНВ матриц, отвечающих контейнеру, произошедших в ходе стеганопреобразования, а не областью, используемой для стеганопреобразования.

Все вышесказанное и результаты, изложенные в [1,6], приводит к следующим значимым для рассматриваемой задачи выводам, говорящим о преимуществах ОПАИС перед используемыми до настоящего момента подходами как основы для разработки устойчивых стеганоалгоритмов:

1. СНЧ и СНВ принципиально отличаются по своим свойствам от совокупности частотных коэффициентов, которые также однозначно определяют матрицу ЦИ и использование которых традиционного при организации стеганопреобразования, в частности, коэффициентов дискретного косинусного преобразования. Если

$$F = U_F \Sigma_F V_F^{\ T}$$

— нормальное сингулярное разложение матрицы F [1], где U_F, V_F — ортогональные матрицы левых и правых СНВ F соответственно, столбцы U_F — лексикографически положительны, а $\Sigma_F = diag\left(\sigma_1(F),...,\sigma_n(F)\right)$ — матрица СНЧ, то каждая сингулярная тройка

$$\left(\sigma_i(F), u_i(F), v_i(F)\right),$$

где $u_i(F), v_i(F)$ — левый и правый СНВ, соответствующие $\sigma_i(F)$, несет в себе в той или иной мере информацию обо всех частотных составляющих сигнала-изображения (при этом максимальные СНЧ — главным образом, о низкочастотных составляющих, а минимальные — о высокочастотных) [1,6]. А это значит, что возмущение даже одного СНЧ/СНВ в процессе стеганопреобразования в той или иной мере «растворит» погруженную информацию во всех частотных составляющих контейнера; возмущение максимальных СНЧ при погружении ДИ затронет не только низкочастотные коэффициенты дискретного косинусного преобразования матрицы ЦИ-контейнера (хотя именно они возмутятся в этом случае больше всего, по сравнению с другими [1,6], что и будет обеспечивать нечувствительность СС к сжатию со значительными коэффициентами [1]), но и все остальные, что уменьшит «удар» на низкие частоты, повышая при этом вероятность обеспечения надежности восприятия СС. Такой принципиально новый подход опосредованного «размазывания» дополнительной информации по всем частотным составляющим при организации стеганопреобразования должен позволить получить более устойчивые к сжатию СА, обеспечивающие надежность восприятия соответствующего СС, по сравнению с теми СА, которые основывались на возмущениях исключительно в частотной области ОС.

2. С учетом того, что анализ свойств СА в свете ОПАИС часто сводится к анализу возмущений СНЧ матрицы (блоков матрицы) ЦИ [1], важно отметить, что

такой анализ является более предпочтительным в вычислительном смысле по сравнению с анализом возмущений яркости пикселей в пространственной области или частотных коэффициентов изображения, что имеет большое значение, особенно при работе с видео последовательностями. Действительно, для $n \times n$-матрицы изображения количество пикселей, как и частотных коэффициентов равно n^2, в то время как сингулярных чисел на порядок меньше - n.

Таким образом, использование общего подхода к анализу состояния и технологии функционирования информационных систем является на сегодняшний день наиболее перспективным для разработки на его основе стеганоалгоритмов, устойчивость которых к сжатию превысит этот параметр для существующих аналогов.

Выводы

В работе обосновано, что при организации скрытого канала связи внутри канала общего пользования на современном этапе развития инфокоммуникационных технологий целесообразно использовать стеганоалгоритмы, необходимо устойчивые к атаке сжатием.

В работе выявлены и обоснованы недостатки при обеспечении устойчивости стеганоалгоритмов к сжатию с потерями в случае организации стеганопреобразования в частотной, пространственной/временной области контейнера, в качестве которого выступают цифровые изображения, аудио или видео последовательности.

Показано, что одной из основных причин отсутствия окончательного решения обсуждаемой задачи является отсутствие единого теоретического базиса, общего математического подхода к ее решению.

Обосновано, что перспективным с точки зрения построения на его основе стеганоалгоритмов, устойчивых к сжатию, в том числе, со значительными коэффициентами, является общий подход к анализу состояния и технологии функционирования информационных систем, основанный на теории возмущений и матричном анализе, принципиально позволяющий организовать процесс стеганопреобразования таким образом, чтобы, наряду с устойчивостью, повысить вероятность обеспечения надежности восприятия стеганосообщения по сравнению с существующими аналогами.

Список литературы

1. Кобозєва, А.А. Аналіз захищеності інформаційних систем [Текст] : підруч. для студ. вищ. навч. закл., які навч. за напр. «Інформаційна безпека» та «Системні науки та кібернетика» / А.А. Кобозєва, І.О. Мачалін, В.О. Хорошко ; М-во трансп. та зв'язку України, Держ. ун-т інформ.-комунікац. технологій. — К. : ДУІКТ, 2010. — 316 с.
2. Грибунин, В.Г. Цифровая стеганография [Текст] : монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М. : СОЛОН-Пресс, 2002. — 272 с.
3. Lancini, R. A robust video watermarking technique in the spatial domain / R. Lancini, F. Mapelli, S. Tubaro // Proceedings of Video/Image Processing and Multimedia Communications 4th EURASIP-IEEE Region 8 International Symposium on VIPromCom, Zadar, Croatia, 16–19 June 2002. — 2002. — PP. 251–256.
4. Shih, F.Y. Combinational image watermarking in the spatial and frequency domains / F.Y. Shih, S.Y.T. Wu // Pattern Recognition. — 2003. — Vol. 36, Iss. 4. — PP. 969–975.
5. Suhail, M.A. Digital watermarking based DCT and JPEG model / M.A. Suhail, M.S. Obaidat // IEEE Transactions on Instrumentation and Measurement. — 2003. — Vol. 52, Iss. 5. — PP. 1640–1647.
6. Кобозева, А.А. Связь свойств стеганографического алгоритма и используемой им области контейнера для погружения секретной информации // Искусственный интеллект. — 2007. — № 4. — С. 531–538.

7. Fridrich, J. Combining Low-Frequency and Spread Spectrum Watermarking / J. Fridrich // Proceedings of the SPIE Conference on Mathematics of Data/Image Coding, Compression and Encryption, July 19, 1998, San-Diego, USA. — 1998. — Vol.3456. — PP. 2–12.
8. Huang, J. Image digital watermarking algorithm using multiresolution wavelet transform // J. Huang, C. Yang // Proceeding of the IEEE International Conference on Systems, Man and Cybernetics, 10–13 Oct. 2004. — 2004. — Vol. 3. — PP. 2977–2982.
9. Lin, W.-H. A blind watermarking method using maximum wavelet coefficient quantization / W.-H. Lin et al. // Expert Systems with Applications. — 2009. — Vol. 36, Iss. 9. — PP. 11509–11516.
10. Конахович, Г.Ф. Компьютерная стеганография [Текст]: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. — Киев : МК-Пресс, 2006. — 288 с.

ЗАГАЛЬНИЙ ПІДХІД ДО АНАЛІЗУ СТАНУ ІНФОРМАЦІЙНИХ СИСТЕМ ЯК ТЕОРЕТИЧНИЙ БАЗИС ДЛЯ СТЕГАНОАЛГОРИТМІВ, СТІЙКИХ ДО АТАКИ СТИСКОМ

А.А. Кобозєва, М.О. Мельник, П.Є. Баранов

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: ritochek@yandex.ua

У роботі виявлені й обґрунтовані недоліки при забезпеченні стійкості стеганоалгоритмів до атаки стиском у випадку організації стеганоперетворення в частотній, просторовій/часовій області контейнера, у якості якого виступають цифрові зображення, аудіо й відео послідовності. Показано, що однією з основних причин відсутності остаточного рішення обговорюваної задачі є відсутність єдиного теоретичного базису, загального математичного підходу до її рішення. Обґрунтовано, що перспективним з погляду побудови на його основі стеганоалгоритмів, стійких до стиску, у тому числі, зі значними коефіцієнтами, є загальний підхід до аналізу стану й технології функціонування інформаційних систем, заснований на теорії збурень і матричному аналізі.
Ключові слова: стеганоалгоритм, атака проти вбудованого повідомлення, стійкість до стиску, загальний підхід до аналізу стану й технології функціонування інформаційних систем.

GENERAL APPROACH TO INFORMATION SYSTEM STATE ANALYSIS AS THEORETICAL BASIS FOR STEGO ALGORITHMS ROBUST AGAINST COMPRESSION ATTACKS

A.A. Kobozeva, M.A. Melnik, P.E. Baranov

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: ritochek@yandex.ua

Shortcomings in the process of provision of stegoalgorithms with robustness to compression attacks were identified and proved for the case of stegotransformation in frequency, spatial/time domain of a cover object, with digital images, audio and video series used as cover objects. It was shown that lack of a comprehensive theoretical basis and general mathematical approach to the solution process for the problem discussed is one of the basic reasons for absence of the final solution. It was justified that general approach to information system state and functioning analysis based on perturbation theory and matrix analysis is a promising one for the development of robust to compression attacks stegoalgorithms, including those with significant coefficients.
Keywords: stegoalgorithm, attack against the embedded message, robustness against compression, general approach to information system state and functioning analysis