STEGANOGRAPHIC METHOD VERIFYING THE INTEGRITY AND AUTHENTICITY OF EMBEDDED INFORMATION

Kobozeva A.A., Kozina M.A.
Odessa National Polytechnic University, Ukraine

Abstract. The paper focuses on the steganographic method that carries out simultaneous effective solution for creation of covert communication channel within the channel for public use, check of the integrity and authenticity of the transmitted additional information. These tasks define the so-called three-pronged task (TT) that is of current interest, but today, according to the data available from the open press, has no satisfactory solution. This is connected with the complexity of TT and moreover a covert communication channel itself requires additional guaranteeing the reliability of perception and insensitivity of formed steganomessage against disturbing influences. The digital image stands as a container. The additional embedded information that is the result of pre-primary encoding of confidential information and the subsequent secondary coding using a secret key for authentication is represented as a binary sequence. Developed steganomethod for solving TT, ensures the reliability of perception of formed steganomessage, is resistant to attacks against embedded messages and allows to effectively decode the transmitted information even in the event of a breach of its integrity, that is evidenced by the results of a computational experiment.
Keywords: steganography method, integrity, authenticity, discrete Fourier transform, a digital image.

METODA STEGANOGRAFICĂ DE VERIFICARE A INTEGRITĂŢII ŞI AUTENTITĂŢII INFORMAŢIEI TRANSMISE

Kobozeva A.A., Kozina M.A.
Universitatea Naţională Politehnică din Odesa, Ucraina

Rezumat. Lucrarea prezintă o metodă steganografică, care realizează simultan şi eficient procedura de crearea canalului protejat de comunicare în cadrul canalului de uz public; verificarea integrităţii şi autenticităţii informaţiei suplimentare transmise. Problema aceasta defineşte aşa-numita sarcină cu trei componente (TK), care este relevantă, dar până în prezent, conform datelor disponibile din presa deschisă, nu are o soluţie satisfăcătoare. Acest lucru se explică prin faptul complexităţii TK, de asemenea, crearea unui canal protejat de comunicare necesită, asigurarea siguranţei percepерii şi insensibilităţii steganocomunicării formate la perturbaţii stohastice. În calitate de container serveşte imaginea digitală. Informaţia suplimentară, care rezultă din codificarea preliminară a informaţiilor confidenţiale cu codificarea ei ulterioară, folosind un cod secret pentru a asigura autentificarea se prezintă ca o secvenţă binară. Steganometoda elaborată, rezolvând problema TK, asigură siguranţa perceperii steganocomunicării formate, este rezistent la atacurile împotriva mesajelor integrate şi permite să se decodeze eficient informaţia transmisă, chiar şi în caz de pierderi parţiale a integrităţii sale. Aceste sugestii sunt confirmate de rezultatele testărilor la calculator.
Cuvinte-cheie: metoda steganografică, integritatea, authentitatea, transforamrea Fourier discretă, o imagine digitală.

СТЕГАНОГРАФИЧЕСКИЙ МЕТОД, ОБЕСПЕЧИВАЮЩИЙ ПРОВЕРКУ ЦЕЛОСТНОСТИ И АУТЕНТИЧНОСТИ ПЕРЕДАВАЕМЫХ ДАННЫХ

А.А. Кобозева, М. А. Козина
Одесский национальный политехнический университет, Украина

Аннотация. В работе предложен стеганографический метод, осуществляющий одновременное эффективное решение задач организации скрытого канала связи внутри канала общего пользования; проверку целостности и аутентичности передаваемой дополнительной информации. Перечисленные задачи определяют так называемую триединую задачу (ТЗ), которая является актуальной, но на сегодняшний день по данным, доступным из открытой печати, не имеет удовлетворительного решения. Это объясняется сложностью ТЗ, кроме того организация скрытого канала связи сама по себе требует дополнительно обеспечения надежности восприятия и нечувствительности формируемого стеганосообщения к возмущающим воздействиям. В качестве контейнера выступает цифровое изображение. Дополнительная информация, являющаяся результатом предварительного первичного кодирования конфиденциальной информации и последующего вторичного кодирования с

использованием секретного ключа для обеспечения аутентификации, представляется в виде бинарной последовательности. Разработанный стеганометод, решая ТЗ, обеспечивает надежность восприятия формируемого стеганосообщения, является устойчивым к атакам против встроенного сообщения и позволяет эффективно декодировать передаваемую информацию даже в случае нарушения ее целостности, что подтверждается результатами вычислительного эксперимента.
Ключевые слова: стеганографический метод, целостность, аутентичность, дискретное преобразование Фурье, цифровое изображение.

Введение

Элементы, цепи, тракты, соединительные провода и линии связи любых электронных систем и схем постоянно находятся под воздействием собственных (внутренних) и сторонних (внешних) электромагнитных полей различного происхождения, индуцирующих или наводящих в них значительные напряжения. В подобных случаях возникают паразитные связи и наводки, которые приводят к образованию электрических каналов утечки информации [1]. В силу этого необходимым является обеспечение дополнительной защищенности информации в условиях ее возможной утечки, для чего эффективными являются стеганографические методы.

Стеганография была и остается одной из самых важных составляющих частей любой комплексной системы защиты информации [1]. При организации стеганографического канала связи в некоторый объект-контейнер, который не привлекает внимания, погружается дополнительная информация (ДИ), являющаяся результатом кодирования конфиденциальной информации и представляющая из себя бинарную последовательность $p_1, p_2, ..., p_t,\ p_i \in \{0,1\}$. Результат погружения ДИ в контейнер называется стеганосообщением (СС). СС пересылается открыто по каналу связи или хранится в полученном виде.

Можно выделить две причины широкого распространения научных исследований современности в сфере стеганографии:

— необходимость обеспечения защиты прав собственности на информацию, которая представлена в цифровом формате;
— запрещение/ограничение на использование криптосредств в ряде стран мира.

Первая причина послужила толчком для развития направления стеганографии, связанного с внедрением в информационные контенты цифровых водяных знаков (ЦВЗ) [2-4] для обеспечения решения задачи аутентификации контента, вторая привела к углублению и расширению исследований в области организации скрытого канала связи [5-6], требующей наличие возможности для проверки целостности информации после ее декодирования, а также обеспечения нечувствительности формируемого стеганосообщения (устойчивости соответствующего стеганоалгоритма) к возмущающим воздействиям – атакам против встроенного сообщения.

Очевидно, что наиболее желательным при построении комплексной системы защиты информации является комплексное одновременное решение рассмотренных выше задач, что является чрезвычайно *актуальным* на сегодняшний день с учетом возможностей современных IT-технологий, позволяющих легко осуществлять несанкционированные действия над информационными контентами.

Комплексное решение упомянутых выше задач является принципиально возможным. Действительно, дополнительное использование ЦВЗ при организации стеганографического канала связи может обеспечивать проверку аутентичности, целостности передаваемой информации, а ЦВЗ (при обеспечении аутентичности контента, в который он внедрен) может нести в себе и какую-то дополнительную информацию (например, об авторе).

Необходимо заметить, что в открытых научных источниках авторами не обнаружены разработанные стеганографические методы/алгоритмы, которые бы позволяли одновременно:

1. Организовывать скрытый канал связи, необходимо обеспечивающий надежность восприятия и нечувствительность формируемого стеганосообщения к возмущающим воздействиям;
2. Обеспечивать поверку целостности декодированной ДИ;
3. Обеспечивать поверку аутентичности переданной информации.

Такая комплексная задача далее в работе называется триединой (ТЗ).

Отсутствие удовлетворительного решения ТЗ очевидно обусловлено ее значительной сложностью.

Попытки одновременного решения нескольких задач, в частности, организации скрытого канала связи с проверкой целостности передаваемой информации, уже предпринимались, например, в [7-9]. Однако предложенные решения нельзя назвать удовлетворительными. Так алгоритм в [8], осуществляющий проверку целостности декодированной ДИ при организации стеганографического канала связи принципиально не может, если руководствоваться указанными в работе формулами для погружения ДИ, обеспечить надежность восприятия СС для произвольного ЦИ-контейнера; также требует уточнений и обязательной корректировки предложенный авторами алгоритм декодирования ДИ. Стеганоалгоритм, предложенный в [9] для аутентификации и скрытой передачи данных, основанный на дискретном преобразовании Фурье, является неустойчивым к атакам против встроенного сообщения, что в современных условиях бурного развития IT-технологий является недопустимым при организации стеганографического канала связи. Кроме того, предложенный подход позволяет проводить аутентификацию изображений только в градациях серого, хранимых в форматах TIFF и PNG, а передаваемое скрытое сообщение ограничено в размере, что сужает область применения алгоритма. Недостаточно устойчивым к атакам против встроенного сообщения при обеспечении надежности восприятия формируемого стеганосообщения является алгоритм, предложенный в [7], решающий задачу организации скрытого канала связи с одновременной проверкой целостности ДИ.

Таким образом, разработка стеганографических методов и реализующих их алгоритмов, одновременно решающих несколько из перечисленных выше задач 1-3, остается актуальной как для развития современной стеганографии в частности, так и для организации защиты информации в целом.

Цель статьи и постановка исследований

В качестве контейнера с учетом частоты и удобства использования [2] в работе выступает цветное цифровое изображение (ЦИ).

Целью работы является разработка стеганографического метода (СМ) *SM*З, эффективно решающего ТЗ стеганографии.

Поскольку, как указано выше, при организации скрытого канала связи необходимо обеспечить устойчивость используемого СМ (реализующего его алгоритма) к атакам против встроенного сообщения, погружение ДИ в разрабатываемом методе будет проводиться в частотной области ЦИ-контейнера [2] – в коэффициенты дискретного преобразования Фурье.

Для достижения поставленной цели в работе решаются следующие *задачи*:

1. Выбор размера блока разбиения матрицы ЦИ, используемого при погружении ДИ, который позволяет получить целые коэффициенты дискретного преобразования Фурье (ДПФ);

2. Обеспечение решения задачи проверки целостности ДИ с учетом специфики полученных коэффициентов ДПФ;
3. Выбор способа формирования непосредственно погружаемой в контейнер информации таким образом, чтобы скрываемое сообщение несло в себе наряду с передаваемой конфиденциальной информацией информацию для решения задачи аутентификации;
4. Выбор размера секретного ключа, используемого для предварительного кодирования ДИ с целью обеспечения возможности проверки ее аутентичности;
5. Обеспечение аутентификации передаваемой скрытой информации;
6. Обеспечение устойчивости разработанного СМ к возмущающим воздействиям в канале связи;
7. Соблюдение надежности восприятия стеганосообщения.

Эффективность СМ при решении ТЗ в работе будет оцениваться по следующим параметрам:

1. Эффективность декодирования ДИ в условиях атак против встроенного сообщения, количественно оцениваемая стандартным образом при помощи коэффициента корреляции NC для декодированной информации [10];
2. Обеспечение надежности восприятия СС, количественно оцениваемой при помощи $PSNR$ - пикового отношения «сигнал-шум», традиционно используемого при оценке искажений ЦИ [11];
3. Количеством ошибок при проверке целостности декодированной ДИ первого рода – пропуск имеющего место нарушения целостности; второго рода – констатация нарушения целостности в невозмущенном СС;
4. Количеством ошибок при проверке аутентичности передаваемой информации первого рода – пропуск имеющего место нарушения аутентичности; второго рода – ложная констатация нарушения аутентичности.

Основная часть

Пусть $M \times N$-матрица R — одна из цветовых составляющих цветного ЦИ-контейнера произвольного формата, для хранения которого использована схема RGB. Не ограничивая общности рассуждений, все последующие преобразования ЦИ формально будут представляться как преобразования R.

Опишем базовые принципиальные моменты процесса стеганопреобразования, используемого ниже при разработке СМ $SM3$.

Разобьем матрицу R на непересекающиеся блоки f, размером 2×2 с элементами f_{ij}. Обеспечим в пространственной области очередного используемого для стеганопреобразования блока f путем корректировки значения одного (произвольного) элемента этого блока на 1 (если это необходимо) четность количества четных/нечетных элементов. Благодаря указанному размеру блока, а также (возможно) проделанной корректировке элементы $F(u,v),\ u,v = \overline{0,1}$, матрицы F коэффициентов ДПФ блока f принадлежат множеству целых чисел [12]. Обеспечение этого свойства является основой при проверке целостности декодированной ДИ в разработанном СМ.

Погружение бита p_i ДИ (или бита результата предварительного кодирования ДИ) производится в коэффициенты ДПФ путем замены бита в двоичном представлении каждого частотного коэффициента $F(u,v),\ u,v = \overline{0,1}$, очередного используемого для стеганопреобразования блока, стоящего в позиции pos от правого конца, где $pos \in \{2,3,4\}$, на значение погружаемого бита p_i. Результатом является блок FF возмущенных частотных коэффициентов с элементами $FF(u,v),\ u,v = \overline{0,1}$. Выбор

значения pos очевидно напрямую влияет на устойчивость соответствующего стеганопреобразования к возмущающим воздействиям: чем больше pos, тем менее чувствительным окажется СС. Значимым моментом здесь является то, что неиспользование наименьшего бита $F(u,v)$, $u,v=\overline{0,1}$, в процессе внедрения ДИ обеспечивает неизменность четности/нечетности коэффициентов ДПФ после стеганопреобразования, по сравнению с их значениями в блоке контейнера, что, в свою очередь, исключит наличие округлений при возвращении ЦИ в пространственную область путем обратного ДПФ для каждого блока FF (если не учитывать принципиально возможный выход значений яркости пикселей за границы диапазона $[0,255]$, что, как показывает вычислительный эксперимент, происходит крайне редко), результатом чего является блок ff СС [12].

Предложенный способ стеганопреобразования обеспечивает надежность восприятия получаемого СС, которая устанавливалась путем субъективного ранжирования, а также при помощи оценки величины пикового отношения «сигнал-шум» $PSNR$ [11]. Подтверждением вышесказанного являются результаты вычислительного эксперимента, представленные в табл.1, проведенного в среде Matlab, в котором в качестве ДИ выступала сформированная случайным образом бинарная последовательность.

Таблица 1 – Оценка возмущения ЦИ-контейнера в результате стеганопреобразования в зависимости от номера позиции pos, используемой в коэффициентах ДПФ для внедрения ДИ

pos	Среднее значение PSNR по 500 цифровым изображениям (dB)
2	54.05
3	50.10
4	44.33

В ходе эксперимента стеганопреобразованию подвергались 500 цветных ЦИ, разных по жанру, контрастности, цветности, яркости, полученных непрофессиональными фотографами, а также взятых из традиционной при тестировании алгоритмов, работающих с ЦИ, базы NRCS [13]. Артефакты на изображениях-стеганосообщениях при визуальном анализе обнаружены не были (типичный пример, подтверждающий сказанное, представлен на рис.1). Средние значения $PSNR$ при использовании разных значений $pos\in\{2,3,4\}$ при внедрении ДИ превысили 44 dB, что считается приемлемым с точки зрения оценки визуального качества стеганосообщения [11].

Рис. 1. *Результаты стеганопреобразования: а – ЦИ-контейнер; СС, сформированное для б – pos = 2 ; в – pos = 3 ; г – pos = 4*

Основная идея организации проверки целостности ДИ основана на учете свойств коэффициентов ДПФ, упомянутых выше. Проверка целостности декодированной ДИ проводится в два этапа. Предварительно матрица возможно возмущенного СС разбивается на 2×2 – блоки $\overline{ff}$ аналогично тому, как это происходило для матрицы контейнера при стеганопреобразовании.

Первый этап заключается в проверке для каждого блока $\overline{ff}$, в который происходило погружение ДИ, равенства:

$$bitget(\lfloor \overline{F}(0,0) \rfloor, pos) = bitget(\lfloor \overline{F}(1,0) \rfloor, pos) = bitget(\lfloor \overline{F}(0,1) \rfloor, pos) = bitget(\lfloor \overline{F}(1,1) \rfloor, pos) \quad (1)$$

где $bitget$ - операция, которая выдает значение, стоящее в указанной позиции pos для $\left\lfloor \overline{F}(u,v) \right\rfloor$, где $\overline{F}(u,v),\ u,v=\overline{0,1}$, - элементы блока $\overline{F}$ коэффициентов ДПФ блока $\overline{ff}$ матрицы возможно возмущенного СС, а $[\bullet]$ - операция выделения целой части аргумента.

В случае невыполнения (1) делается вывод о нарушении целостности ДИ. Для обеспечения наименьшей из возможных в условиях рассматриваемой задачи чувствительности формируемого СС к возмущающим воздействиям при организации стеганопреобразования целесообразно задействовать позиции в двоичных представлениях коэффициентов ДПФ, отвечающие $pos=4$, что подтверждается ниже в ходе вычислительного эксперимента. В этом случае нарушение целостности погруженной информации на первом этапе проверки принципиально может быть выявлено при возмущении значений коэффициентов ДПФ блока более чем на 2^3.

Более чувствительным является второй этап, который проводится в случае, когда первый не выявил нарушений целостности ДИ. На втором этапе для каждого $2\times 2-$блока $\overline{ff}$ СС происходит проверка на принадлежность множеству целых чисел всех коэффициентов ДПФ. Если хотя бы в одном блоке хотя бы один частотный коэффициент не является целым, делается вывод о нарушении целостности ДИ (при условии игнорирования возможного выхода значений яркости пикселей за пределы $[0,255]$ при возвращении блоков в пространственную область изображения после погружения ДИ). Заметим, что здесь выявление нарушения целостности будет происходить, если значение яркости пикселя изменится, хотя бы на 1 градацию.

Описанные выше базовые моменты стеганопреобразования имеют упрощенную форму по сравнению с их непосредственной реализацией в разработанном алгоритме $SM3$, поскольку не несут в себе возможности обеспечения проверки аутентичности пересылаемой информации. Это делается намеренно для упрощения восприятия излагаемого материала.

Проверка аутентичности пересылаемых сообщений происходит следующим образом [2]. Каждому значению сформированного определенным образом секретного ключа ставится в соответствие некоторое свое подмножество допустимых контейнеров. Для этого множество всех возможных контейнеров разбивается на T непересекающихся подмножеств $R_1, R_2, \ldots, R_T$. При действующем ключе K_i отправитель выбирает подмножество контейнеров R_i. Скрываемое сообщение M_j встраивается в контейнер этого подмножества, образуя СС $S_{i,j}$. Получатель СС проверяет его соответствие действующему ключу K_j: если СС $S_{i,j}$ принадлежит подмножеству R_j, то декодированное (возможно возмущенное) сообщение $\overline{M}_j$ подлинно, в противном случае принятое сообщение отвергается как ложное. В частности, при организации аутентификации возможен вариант, когда $K_i=K_j$, который и используется ниже при разработке СМ $SM3$.

Для обеспечения аутентификации скрываемой информации в $SM3$ в качестве секретного ключа K_i, отвечающего подмножеству контейнеров R_i, используется случайно сформированная бинарная $L\times L-$матрица с элементами $K_{nm}^{(i)},\ n,m=\overline{1,L}$, при помощи которой происходит предварительное побитовое кодирование ДИ перед ее непосредственным погружением в контейнер, в результате которого каждому биту p_j ставится в соответствие бинарная $L\times L-$матрица $P^{j(K)}$, получаемая по формуле:

$$p_j \otimes K_i = \begin{pmatrix} p_j \otimes K_{1,1}^{(i)} & p_j \otimes K_{1,2}^{(i)} & \dots & p_j \otimes K_{1,L}^{(i)} \\ p_j \otimes K_{2,1}^{(i)} & p_j \otimes K_{2,2}^{(i)} & \dots & p_j \otimes K_{2,L}^{(i)} \\ \dots & \dots & \dots & \dots \\ p_j \otimes K_{L,1}^{(i)} & p_j \otimes K_{L,2}^{(i)} & \dots & p_j \otimes K_{L,L}^{(i)} \end{pmatrix} = \begin{pmatrix} P_{1,1}^{j(K)} & P_{1,2}^{j(K)} & \dots & P_{1,L}^{j(K)} \\ P_{2,1}^{j(K)} & P_{2,2}^{j(K)} & \dots & P_{2,L}^{j(K)} \\ \dots & \dots & \dots & \dots \\ P_{L,1}^{j(K)} & P_{L,2}^{j(K)} & \dots & P_{L,L}^{j(K)} \end{pmatrix} = P^{j(K)} \quad (2)$$

где $\otimes$ - логическая операция «исключающего ИЛИ». В итоге процесс погружения p_j будет происходить в блок B матрицы контейнера размером $2L \times 2L$ путем внедрения описанным выше способом элементов $P_{nm}^{j(B)} = p_j \otimes K_{nm}^{(i)}$, $n, m = \overline{1, L}$ матрицы $P^{j(K)}$ в непересекающиеся $2 \times 2 -$ блоки $f_{nm}{}^{(B)}$, $n, m = \overline{1, L}$, полученные при соответствующем разбиении B (рис.2).

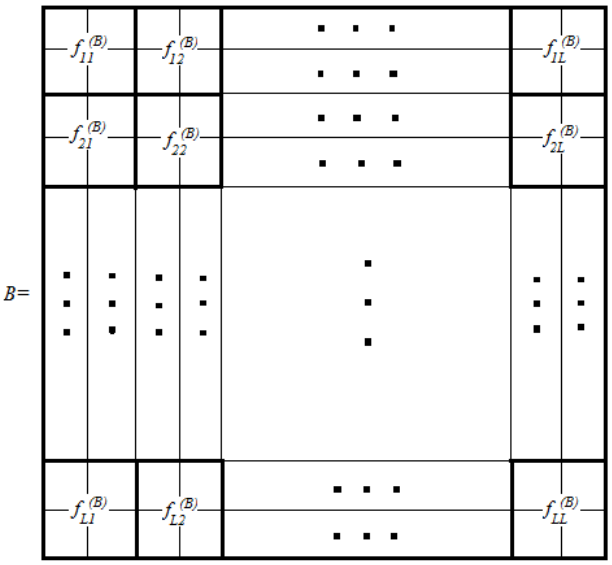

Рис.2. *Разбиение $2L \times 2L$-блока B контейнера на $2 \times 2 -$ блоки, используемые для стеганопреобразования*

Для обеспечения аутентификации скрываемой информации должно быть вычислительно сложно определить, к какому подмножеству R_i принадлежит любое СС [2]. Рекомендованным способом достижения этого является случайное равновероятное разбиение множества контейнеров на подмножества $R_1, R_2, \dots, R_T$, что и делается в *SM*З. Результат этого разбиения является частью секретного ключа, используемого в процессе аутентификации [2].

Заметим, что понятия аутентичности и целостности информации не связаны между собой непосредственно: нарушение одной из этих категорий в общем случае не влечет за собой нарушение другой. При организации стеганографического канала связи необходимо обеспечить, чтобы нарушение целостности не вело напрямую к выводу о нарушении аутентичности, что часто происходит, например, при использовании цифровой подписи [2] и не только [8,9].

С учетом всего вышесказанного основные шаги СМ *SM*З выглядят следующим образом.

Погружение ДИ:

1. Построить случайное равновероятное разбиение конечного множества цветных ЦИ-контейнеров на непересекающиеся подмножества $R_1, R_2, \dots, R_T$.

2. Для каждого из подмножеств $R_1, R_2, \ldots, R_T$ случайным образом сформировать ключ K_i - бинарную $L \times L$ – матрицу.

3. Выбрать ЦИ-контейнер из подмножества R_i и соответствующий ключ K_i, а также конкретную цветовую составляющую контейнера (при схеме хранения RGB) или матрицу яркости (при схеме хранения YUV) для стеганопреобразования — $N \times M$-матрицу R. Матрицу R стандартным образом разбить на непересекающиеся $2L \times 2L$-блоки B.

4. *(Предобработка блока контейнера в пространственной области*). Для каждого блока B ЦИ-контейнера, используемого в процессе стеганопреобразования:

4.1. Разбить блок B стандартным образом на 2×2 – блоки $f_{nm}^{(B)}$, $n, m = \overline{1, L}$.

4.2. Для каждого блока $f_{nm}^{(B)}$, $n, m = \overline{1, L}$, определить количество четных/нечетных элементов:

Если

количество четных/нечетных элементов в $f_{nm}^{(B)}$ равно 1,

то

произвольный элемент блока $f_{nm}^{(B)}$ изменить на 1.

5. *(Погружение очередного бита p_j ДИ)*. Очередной бит p_j погружается в очередной $2L \times 2L$-блок B контейнера, используемый для стеганопреобразования (расположение и выбор таких блоков является частью секретного ключа).

5.1. Сформировать $L \times L$-матрицу $P^{j(K)}$ в соответствии с (2).

5.2. Разбить блок B стандартным образом на 2×2 – блоки $f_{nm}^{(B)}$, $n, m = \overline{1, L}$.

5.3. Для каждого блока $f_{nm}^{(B)}$, $n, m = \overline{1, L}$:

5.3.1. Построить ДПФ. Результат – 2×2 – блок $F_{nm}^{(B)}$ с элементами $F_{nm}^{(B)}(u, v)$, $u, v = \overline{0,1}$, для которых

$$F_{nm}^{(B)}(u, v) = \frac{1}{2} \sum_{x=0}^{1} \sum_{y=0}^{1} f_{nm}^{(B)}(x, y) e^{-i2\pi\left(\frac{ux}{2} + \frac{vy}{2}\right)},$$

где $f_{nm}^{(B)}(x, y)$, $x, y = \overline{0,1}$, - элементы $f_{nm}^{(B)}$.

5.3.2. В элементы блока $F_{nm}^{(B)}$ происходит погружение бита $P_{nm}^{j(K)}$ матрицы (2). Результат – блок $FF_{nm}^{(B)}$ с элементами:

$$FF_{nm}^{(B)}(u, v) = bitset\left(F_{nm}^{(B)}(u, v), pos, P_{nm}^{j(K)}\right), \quad u, v = \overline{0,1},$$

где *bitset* - операция, реализованная в среде в Matlab (2009), которая устанавливает значение $P_{nm}^{j(K)}$ в указанной позиции *pos* двоичного представления значения $F_{nm}^{(B)}(u, v)$, $pos \in \{2, 3, 4\}$.

5.3.3. Построить обратное ДПФ для блока $FF_{nm}^{(B)}$. Результат – блок $ff_{nm}^{(B)}$ с элементами $ff_{nm}^{(B)}(x, y)$, $x, y = \overline{0,1}$:

$$ff_{nm}^{(B)}(x, y) = \frac{1}{2} \sum_{u=0}^{1} \sum_{v=0}^{1} FF_{nm}^{(B)}(u, v) e^{2\pi i\left(\frac{ux}{2} + \frac{vy}{2}\right)}.$$

5.4. Из блоков $\overline{ff}_{nm}^{(B)},\ n,m=\overline{1,L}$ соответствующим образом сформировать $2L\times 2L-$ блок $\overline{B}$ СС.

6. Сформировать матрицу $\overline{R}$ - результат стеганопреобразования матрицы R с учетом полученных в результате стеганопреобразования $2L\times 2L-$ блоков $\overline{B}$.

7. Сформировать цветное ЦИ-стеганосообщение, заменяя матрицу R контейнера на полученную на шаге 6 матрицу $\overline{R}$.

Декодирование ДИ:

1. Для ЦИ-стеганосообщения определяется подмножество R_i, содержащее это ЦИ, и соответствующий ключ K_i.

2. Из полученного цветного возможно возмущенного ЦИ-стеганосообщения выделяется матрица $\overline{\overline{R}}$, использованная в процессе стеганопреобразования (в общем случае $\overline{\overline{R}}\neq\overline{R}$ в силу предполагаемого наличия атак против встроенного сообщения). Блокам B, задействованным в процессе стеганопреобразования, матрицы R контейнера соответствуют в матрице $\overline{\overline{R}}$ блоки $\overline{\overline{B}}$ (в общем случае $\overline{\overline{B}}\neq\overline{B}$).

3. *(Проверка аутентичности переданной информации)*. Для каждого блока $\overline{\overline{B}}$:

3.1. Разбить блок $\overline{\overline{B}}$ стандартным образом на $2\times 2-$блоки $\overline{ff}_{nm}^{(B)},\ n,m=\overline{1,L}$.

3.2. Для каждого блока $\overline{ff}_{nm}^{(B)},\ n,m=\overline{1,L}$:

3.2.1. Построить ДПФ. Результат – $2\times 2-$блок $\overline{F}_{nm}^{(B)}$ с элементами $\overline{F}_{nm}^{(B)}(u,v),\ u,v=\overline{0,1}$

3.2.2. Из элементов блока $\overline{F}_{nm}^{(B)}$ происходит извлечение бита $\overline{P}_{nm}^{j(K)}$ возможно возмущенной матрицы (2) - $\overline{P}^{j(K)}$: пусть k_0, k_1 - количество нулей и единиц соответственно, выделенных из позиции pos двоичных представлений целых частей значений всех четырех коэффициентов ДПФ блока $\overline{F}_{nm}^{(B)}$. Тогда

$$\overline{P}_{nm}^{\ j(K)}=\begin{cases}bitget\left(\left[\overline{F}_{nm}^{(B)}(1,1)\right],pos\right),\ \textit{если } k_0=0\vee k_1=0,\\ 0,\ \textit{если } k_0>k_1,\\ 1,\ \textit{если } k_0\le k_1\end{cases}$$

где *bitget* - операция, реализованная в среде Matlab (2009), которая выдает значение, стоящее в указанной позиции pos для $\left[\overline{F}_{nm}^{(B)}(1,1)\right]$

3.3. Из элементов $\overline{P}_{nm}^{\ j(K)}$, $n,m=\overline{1,L}$, построить матрицу $\overline{P}^{j(K)}$.

Если

$$\overline{P}^{j(K)}=K_i\ \vee\ \overline{P}^{j(K)}=\overline{K_i},\ \text{где } \overline{K_i}\ \text{- инверсия матрицы } K_i$$

то

аутентичность блока $\overline{B}$ не нарушена

4. Определить K_a (%) – часть от общего количества блоков $\overline{\overline{R}}$, для которых аутентичность в результате проверки считается ненарушенной:

если

$K_a > A$, где A - пороговое значение

то

аутентичность переданной информации не нарушена

иначе

переданная информация не является аутентичной. Выход.

5. (*Проверка целостности переданной информации*).

Если

на шаге 3.2.2 хотя бы для одного $\overline{\overline{B}}$ существовал блок $\overline{F}_{nm}^{(B)}$, для которого наблюдалась ситуация: $k_0 \in \{1,2,3\}$,

то

целостность передаваемой информации нарушена

иначе

дополнительная проверка целостности:

если

на шаге 3.2.2 хотя бы для одного $\overline{\overline{B}}$ существовал блок $\overline{F}_{nm}^{(B)}$, для которого среди его элементов $\overline{F}_{nm}^{(B)}(i, j), i, j = \overline{0,1},$ существовал $\overline{F}_{nm}^{(B)}(i, j) \notin Z$, где Z -множество целых чисел,

то

целостность передаваемой информации нарушена;

иначе

целостность передаваемой информации не нарушена.

6. *(Декодирование очередного возможно возмущенного бита $\overline{p}_j$ ДИ из очередного блока $\overline{\overline{B}}$ СС).*

Если

Для блока $\overline{\overline{B}}$ матрица $\overline{P}^{j(K)}$, полученная на шаге 3.3, удовлетворяет: $\overline{P}^{j(K)} = K_i$,

то

$$\overline{p}_j = 0.$$

Если

Для блока $\overline{\overline{B}}$ матрица $\overline{P}^{j(K)}$, полученная на шаге 3.3, удовлетворяет: $\overline{P}^{j(K)} = \overline{K_i}$,

то

$$\overline{p}_j = 1,$$

иначе

пусть t_0 - количества совпадений между значениями соответствующих элементов матриц $\overline{P}^{j(K)}$ и K_i, а t_1 - количества совпадений между значениями соответствующих элементов матриц $\overline{P}^{j(K)}$ и $\overline{K_i}$

если

$$t_0 > t_1,$$

то

$$\overline{p}_j = 0,$$

иначе

$$\overline{p}_j = 1.$$

Для реализации предложенного метода ключевую роль играет определение порогового значения A, используемого при проверке аутентичности передаваемой

информации. Проверка аутентичности должна давать правильный результат и в случае нарушения целостности погруженной информации. Поэтому для определения A необходимо оценить возможные ошибки, возникающие при декодировании ДИ в условиях атак против встроенного сообщения. В качестве таких атак в работе рассмотрено наложение различных шумов (с различными параметрами) на СС.

Для решения возникшей задачи первоначально СМ $SM3$ был реализован в виде стеганоалгоритма, где отсутствовал блок, осуществляющий проверку аутентичности информации: погружение очередного бита p_j ДИ проводилось в $2\times 2-$блок матрицы ЦИ-контейнера без предварительного кодирования p_j с использованием ключа K_i. После формирования СС на него накладывался шум, параметры которого обеспечивали надежность восприятия возмущенного СС, после чего происходило декодирование ДИ. Результаты вычислительного эксперимента, проведенного в среде Matlab с 750 ЦИ, представлены в табл.2,3, где P и $P_{\max}$ определяют соответственно среднее и максимальное по всем тестированным ЦИ количества ошибочно декодированных бит ДИ относительно общего количества погруженных, выраженное в процентах; NC-коэффициент корреляции для погруженной ДИ, который определяется в соответствии с формулой [10]: $NC=\sum_{i=1}^{t} p_i'\times \overline{p}_i' \Big/ t$, где $p_1, p_2,..., p_t$ — ДИ, погруженная в контейнер, $p_i\in\{0,1\}, i=\overline{1,t}$; $\overline{p}_1, \overline{p}_2,..., \overline{p}_t$ — декодированная ДИ, где $\overline{p}_i\in\{0,1\}, i=\overline{1,t}$; $p_i'=1, \overline{p}_i'=1$, если $p_i=1, \overline{p}_i=1$; $p_i'=-1, \overline{p}_i'=-1$, если $p_i=0, \overline{p}_i=0$.

Полученные результаты (табл.2) дают возможность говорить об устойчивости разработанного метода к атакам, осуществляемым при помощи наложения шума на СС, при $pos=4$. Именно этот вариант ($pos=4$), с учетом соблюдения для него надежности восприятия формируемого СС, что было отмечено выше, и предлагается использовать при непосредственной реализации СМ $SM3$ в виде алгоритмов. Кроме этого, поскольку максимальное количество ошибочно декодированных бит ДИ в проведенном эксперименте (табл.3) не превосходит при всех вариантах параметров шумов для $pos=4$ 21%, то при нарушении целостности пересылаемой информации за счет наложения шума не более 21% декодированных матриц $\overline{P}^{j(K)}$ могут отличаться от K_i или $\overline{K_i}$. Таким образом полагаем здесь $A=79$.

Таблица 2. Средние значения P (%), NC в зависимости от позиции внедрения (pos) в условиях наложения на СС шума с дисперсией σ^2

Шум	Гауссовский (с нулевым мат.ожиданием)				Мультипликативный			
σ^2	0.0001		0.00001		0.0001		0.00001	
pos	P	NC	P	NC	P	NC	P	NC
2	49	0.02	24.5	0.51	44	0.12	17	0.66
3	30	0.4	3	0.94	15	0.7	1.5	0.97
4	10	0.8	1.1	0.98	8	0.84	1	0.98

Таблица 3. Значение $P_{\max}$ в условиях наложения на СС шума с дисперсией σ^2 (%)

Шум	Гауссовский (с нулевым мат.ожиданием)		Мультипликативный	
σ^2 / *pos*	0.0001	0.00001	0.0001	0.00001
4	20.2	3.1	19.4	2.2

Замечание. Для окончательной разработки алгоритмов, реализующих метод *SM*З, для определения порога A необходимо в качестве атак против встроенного сообщения, приводящих к нарушению целостности ДИ, рассмотреть не только наложение шума, а и атаки фильтрацией (линейными и нелинейными фильтрами), атаки сжатием и т.д., а значение A определить после комплексного учета ошибок, возникающих при декодировании ДИ в условиях возмущающих воздействий, над чем сейчас работают авторы.

Реализация СМ *SM*З в виде алгоритма при значениях параметров $T=10$, $L=4$, $A=79$ и его тестирование, когда в качестве атак против встроенного сообщения рассматривались атаки наложением различных шумов на СС, а погружение ДИ происходило в синюю составляющую цветного ЦИ-контейнера (цветовая схема RGB), привели к следующим результатам, являющимся результатами вычислительного эксперимента, проведенного в среде Matlab более, чем с 700 ЦИ:

— Ошибки первого и второго рода при проверке аутентичности информации составили 0 и 0.004% соответственно;
— Ошибки первого и второго рода при проверке целостности декодированной информации составили 0 и 0.01% соответственно.

Полученные результаты говорят о высокой эффективности разработанного СМ при проверке целостности и аутентичности декодированной ДИ.

Выводы.

Разработан стеганографический метод *SM*З скрытой передачи данных, осуществляющий одновременное эффективное решение задач проверки целостности и аутентичности передаваемой дополнительной информации.

Предложенный стеганометод обеспечивает надежность восприятия формируемого стеганосообщения, является устойчивым к наложению шумов на стеганосообщение с параметрами, обеспечивающими надежность восприятия возмущенного стеганосообщения, позволяет эффективно декодировать передаваемую информацию даже в случае нарушения ее целостности, что подтверждается результатами вычислительного эксперимента.

В настоящий момент усилия авторов направлены на уточнение порогового значения A, используемого в процессе проверки аутентичности информации, а также на повышение устойчивости стеганоалгоритмов, реализующих *SM*З к возмущающим воздействиям, отличным от наложения шума.

Литература

[1] Horoshko, V.A. Metody i sredstva zaschity informatsii [Text] : nauchnoe izdanie / V.A. Horoshko, A. A. Chekatkov; Red. Iu.S. Kovtaniuk. — K.: IUNIOR, 2003. — 505 s. (in Russian)

[2] Gribunin, V.G. Tsifrovaia steganografia [Text]: monografia / V.G. Gribunin, I.N. Okov, I.V. Turintsev. — M. : SOLON-Press, 2002. — 272 s. (in Russian)

[3] Vafaei, M. A Novel Digital Watermarking Scheme Using Neural Networks with Tamper Detection Capability/ M.Vafaei, H.Mahdavi-Nasab // J. Basic. Appl. Sci. Res. — 2013. — 3(4). — pp. 577-587.
[4] Surachat, K. Pixel-wise based Digital Watermarking Using a Multiple Sections Embedding Technique / K.Surachat // International Journal of Future Computer and Communication. — 2012. — Vol. 1, No. 2. — pp.124-127.
[5] Li, B. A Survey on Image Steganography and Steganalysis / B. Li *et al.* // Journal of Information Hiding and Multimedia Signal Processing. — 2011. — Vol.2, No.2. — pp.142–172.
[6] Subhashini, D. Comparison analysis of spatial Domain and compressed Domain steganographic techniques / D. Subhashini, P. Nalini, G. Chandrasekhar // International Journal of Engineering Research and Technology. — 2012. — Vol. 1, Iss. 4. — pp. 1–6.
[7] Kobozeva A. A. Steganograficheskii algoritm skrytoi peredachi informatsii, obespechivaiuschii autentifikatsiu konteinera / Kobozeva A. A., Shovkun A.D. - Naukovii visnik Mijnarodnogo gumanitarnogo universitetu. – 2012. – N.4. – s. 21-28.
[8] Glumiv N.I. Algoritm vstraivania poluhrupkih tsifrovyh vodeanyh znakov dlea zadach autentifikatsii izobrajenii i skrytoi peredachi informatsii / N.I. Glumov, V.A. Mitekin. – Kompiuternaia optika – 2011. – Nr.2, t.35. – s.262-267. (in Russian)
[9] D. Bhattacharyya, J. Dutta, P. Das, S.K. Bandyopadhyay, T. Kim. Authentication and Secret Message Transmission / Int. J. Communications, Network and System Sciences. – 2009. - № 5. – pp. 363-370.
[10] Lin, W.-H. A blind watermarking method using maximum wavelet coefficient quantization / W.-H.Lin, Y.-R.Wang, S.-J.Horng *et al.* // Expert Systems with Applications. — 2009. — No.36. — pp.11509–11516.
[11] Surekha, B. A Spatial Domain Public Image Watermarking / B.Surekha, G.N.Swamy // International Journal of Security and Its Applications. – 2011. - Vol. 5 No. 1. – pp.1-12.
[12] Kozina M.O. Discrete Fourier transform as a basis for steganography method / M. O. Kozina // Pratsi Odesikogo politehnichnogo universitetu. – 2014. – Vip.2(44). – s.118-126. (in Ukrainian)
[13] NRCS Photo Gallery: //United States Department of Agriculture. Washington, USA. http:// http://photogallery.nrcs.usda.gov (date of visit to the sait: 10.09.2014).

Сведения об авторах:

Кобозева Алла Анатольевна – д.т.н., проф., зав.каф. информатики и управления защитой информационных систем Одесского национального политехнического университета.
Email: alla_kobozeva@ukr.net

Козина Мария Александровна – аспирант кафедры информатики и управления защитой информационных систем Одесского национального политехнического университета.
Email: masha_1991@rambler.ru