УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 5 (2015), No. 1, PP. 57-64

МЕТОД СКРЫТОЙ ПЕРЕДАЧИ ДАННЫХ, ОБЕСПЕЧИВАЮЩИЙ ПРОВЕРКУ ЦЕЛОСТНОСТИ И АУТЕНТИЧНОСТИ ПЕРЕДАВАЕМОЙ ИНФОРМАЦИИ

А.А. Кобозева, М.А. Козина

Одесский национальный политехнический университет
пр. Шевченко, 1, Одесса, 65044, Украина; e-mail: alla_kobozeva@ukr.net

В работе предлагается усовершенствование ранее разработанного авторами стеганографического метода, решающего одновременно актуальную на сегодня триединую задачу стеганографии: скрытой передачи данных, проверки их аутентичности и целостности. В качестве контейнера используется цифровое цветное изображение, а в качестве дополнительной информации выступает произвольным образом сформированная бинарная последовательность. Усовершенствование стеганографического метода включает в себя: уменьшение объема необходимо передаваемой информации по защищенному каналу связи для организации аутентификации данных; обеспечение возможности декодирования переданной информации без наличия контейнера. Приведены результаты вычислительных экспериментов, подтверждающие высокую эффективность предложенного метода.

Ключевые слова: стеганографический метод, скрытый канал связи, целостность, аутентичность, дискретное преобразование Фурье, цифровое изображение.

Введение

Стеганография – наука, которая изучает и обеспечивает сокрытие информации в произвольном носителе-контейнере (например, фото, видео и др.), таким образом, чтобы никто, кроме отправителя и получателя, не подозревал о существовании передаваемой информации [1,2]. Не ограничивая общности рассуждений, далее как контейнер используется цифровое изображение (ЦИ).

Стеганография помогает решать вопросы, связанные с защитой авторских прав, проверкой подлинности, целостности различных информационных контентов.

Существующие стеганографические методы могут осуществлять погружение скрываемой, или дополнительной информации (ДИ), как в пространственной, так и в частотной областях изображения. Традиционно считается [1], что стеганопреобразование, реализуемое в частотной области изображения, более устойчиво к различным видам возмущений (под устойчивостью стеганографического алгоритма, согласно [3], понимается нечувствительность к возмущающим воздействиям сформированного им стеганосообщения (СС) (СС – результат внедрения ДИ в контейнер)).

К современным стеганографическим методам предъявляется ряд требований, одновременное удовлетворение которых является нетривиальной, нерешенной до конца, а потому актуальной на сегодняшний день задачей. Так при организации скрытого канала связи внутри канала общего пользования необходимо обеспечение не только надежности восприятия СС [3], устойчивости стеганоалгоритма к атакам против встроенного сообщения и стеганоанализу, но и возможности проверки целостности передаваемой информации/контейнера, аутентификации информационных контентов.

Необходимо заметить, что последнее требование, которое чаще всего в настоящий момент обеспечивается путем использования цифровой подписи, имеет свои особенности при обеспечении его для мультимедийной информации: сообщение, содержащее цифровую подпись, должно храниться или передаваться абсолютно точно «бит в бит», но данные, которые хранятся в цифровом формате, могут незначительно искажаться как на этапе хранения (например, при сжатии), так и при передаче по каналу связи, не теряя своей аутентичности. Кроме того, значительным недостатком цифровой подписи является то, что ее можно легко удалить и прикрепить новую, отвечающую другому владельцу/автору информации [3]. Все это оставляет на сегодняшний день актуальной задачу организации аутентификации информации саму по себе.

Попытки одновременного решения нескольких задач стеганографии, в частности, организации скрытого канала связи с проверкой аутентичности ЦИ-контейнера уже предпринимались [4-6], однако предлагаемые решения нельзя назвать удовлетворительными. Так стеганографический метод, предложенный в [4], не гарантирует надежность восприятия формируемого СС, что ставит под сомнение принципиальную возможность его использования при организации стеганографического канала связи. Усовершенствование обсуждаемого метода было предложено в [5], однако и здесь вопрос обеспечения надежности восприятия СС не нашел окончательного решения. Не лишен значительных недостатков и метод, разработанный в [6].

В [7] Козиной М.А. был предложен стеганографический метод, обеспечивающий скрытую передачу произвольной бинарной последовательности с одновременной проверкой целостности ДИ, соблюдение надежности восприятия стеганосообщения, устойчивость к возмущающим воздействиям в канале связи, который послужил основой для разработки в [8-9] уникального, как можно судить из открытой печати, метода, обеспечивающего решение триединой задачи стеганографии (ТЗ):

1. Организации скрытого канала связи (с соблюдением надежности восприятия и нечувствительности формируемого СС к возмущающим воздействиям);
2. Проверку целостности ДИ;
3. Проверку аутентичности передаваемой информации.

Цель статьи и постановка заданий

При всей своей уникальности, стеганометод, предложенный в [8,9], не лишен недостатков:

1. Необходимость наличия контейнера для организации декодирования ДИ;
2. Большой объем информации, необходимо передаваемой по защищенному каналу связи.

В связи с этим *целью* данной работы является усовершенствование предложенного в [8,9] стеганографического метода путем уменьшения объема информации, которую необходимо передавать по защищенному каналу связи для организации аутентификации данных; обеспечения возможности декодирования передаваемой информации без наличия контейнера.

Задачи, которые необходимо решить для достижения цели:

1. Выбор информации, которая будет передаваться по защищенному каналу связи для обеспечения возможности декодирования скрываемой информации без наличия контейнера;
2. Выбор способа формирования секретного ключа стеганометода ;
3. Выбор устойчивого к возмущающим воздействиям способа внедрения ключа для организации аутентификации ДИ, обеспечивающего надежность восприятия СС.

Основная часть

В работе в качестве контейнера выступает цифровое цветное изображение произвольного формата, для хранения которого используется схема RGB. Пусть B — $M \times N$ -матрица — одна из цветовых составляющих ЦИ-контейнера.

Рассмотрим основные шаги предлагаемого усовершенствованного стеганографического метода, обозначаемого далее SM_3, и принципиальные его отличия от разработанного в [8,9].

Кодирование. Опираясь на существующие принципы аутентификации передаваемой информации, описанные в [1], разобьем множество имеющихся изображений-контейнеров произвольно на подмножества. Каждому *i*-му подмножеству поставим в соответствие уникальную числовую метку num_i, выбираемую из диапазона [a; b], и уникальный бинарный ключ кодирования K_j – $q \times p$ -матрицу, участвующий в предварительном кодировании дополнительной информации, $j = 1,2,...,2^{q \cdot p}$, которые в совокупности образуют так называемую стеганографическую пару (num_i, K_j), далее обозначаемую *SP*. В общем случае количество сформированных ключей кодирования K_j должно быть не меньше количества меток num_i, чтобы каждое подмножество контейнеров получило свой уникальный ключ кодирования. Соответствие между метками подмножеств контейнеров и ключами кодирования (или их однозначно определяемыми номерами, или однозначно определяемыми метками) устанавливается произвольным образом. Множество полученных стеганографических пар, обозначаемое далее *MSP*, определяет секретный ключ стеганоалгоритма, передается по защищенному каналу связи, в отличие от [8,9] имеет реальные размеры.

Основные шаги при определении ЦИ-контейнера и соответствующих ему параметров в SM_3:

1. Выбрать случайным образом из *MSP* стеганографическую пару *SP* (num_i, K_j).
2. Выбрать подмножество контейнеров, которое отвечает метке num_i.
3. Из полученного на предыдущем шаге подмножества выбрать произвольным образом ЦИ-контейнер для дальнейшего погружения ДИ, с использованием соответствующей *SP* (num_i, K_j).

Опишем основные моменты стеганопреобразования, обеспечивающего надежность восприятия СС, которые были предложены в [7] и используются в SM_3.

Матрица B разбивается стандартным образом на непересекающиеся блоки размером 2×2, которые далее обозначаются $F_{nm}^{(B)}$, $n = \overline{1, \left[\frac{N}{2}\right]}$, $m = \overline{1, \left[\frac{M}{2}\right]}$. Для каждого блока строится дискретное преобразование Фурье (ДПФ). В [10] была обоснована целесообразность выбора упомянутого размера блока, который обеспечивает получение вещественных частотных коэффициентов, а также предложен способ получения целых частотных коэффициентов ДПФ, что явилось основой для организации проверки нарушения целостности ДИ на этапе декодирования.

Дополнительная информация представляет из себя случайным образом сформированную бинарную последовательность $p_1, p_2, ..., p_t$, $p_j \in \{0,1\}$, $j = \overline{1,t}$. С помощью ключа кодирования K_m, для которого $q = p = R$, происходит ее побитовое кодирование:

$$p_j \otimes K_m = \begin{pmatrix} p_j \otimes K_{1,1}^{(m)} & p_j \otimes K_{1,2}^{(m)} & \dots & p_j \otimes K_{1,R}^{(m)} \\ p_j \otimes K_{2,1}^{(m)} & p_j \otimes K_{2,2}^{(m)} & \dots & p_j \otimes K_{2,R}^{(m)} \\ \dots & \dots & \dots & \dots \\ p_j \otimes K_{R,1}^{(m)} & p_j \otimes K_{R,2}^{(m)} & \dots & p_j \otimes K_{R,R}^{(m)} \end{pmatrix} = \begin{pmatrix} P_{1,1}^{j(K)} & P_{1,2}^{j(K)} & \dots & P_{1,R}^{j(K)} \\ P_{2,1}^{j(K)} & P_{2,2}^{j(K)} & \dots & P_{2,R}^{j(K)} \\ \dots & \dots & \dots & \dots \\ P_{R,1}^{j(K)} & P_{R,2}^{j(K)} & \dots & P_{R,R}^{j(K)} \end{pmatrix} = P^{j(K)},$$

где p_j - очередной бит ДИ, $\otimes$ - логическая операция «исключающее ИЛИ»; $K_{k,l}^{(m)}$, $k,l = \overline{1,R}$ - элементы матрицы K_m; $P^{j(K)}$ - $R \times R -$матрица с элементами $P_{k,l}^{j(K)}$, $k,l = \overline{1,R}$, которая отвечает 1 биту p_j ДИ после кодирования.

После этого каждый очередной элемент $P_{k,l}^{j(K)}$ сформированной бинарной матрицы $P^{j(K)}$ внедряется в очередной используемый для стеганопреобразования блок $F_{nm}^{(B)}$. Результат – блок $FF_{nm}^{(B)}$ с элементами:

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

где *bitset* - операция, которая реализована в пакете Matlab (2009), работает следующим образом: значение $P_{k,l}^{j(K)}$ устанавливается в указанной позиции *pos* от правого конца двоичного представления элемента $F_{nm}^{(B)}(u,v)$, где $pos \in \{2,3,4\}$ [7]. Таким образом, погружение 1 бита ДИ происходит в блок матрицы B размером $2R \times 2R$, что с учетом желаемого обеспечения достаточной скрытой пропускной способности, накладывает ограничения сверху на размер R матрицы ключа кодирования.

Внедрение ДИ происходит не во все $2R \times 2R -$блоки матрицы B. Предлагается оставлять P (P – нечетное число) блоков $Bl_k, k = \overline{1,P}$, размером 8×8, расположение которых в пределах B может являться частью секретного ключа стеганоалгоритма, реализующего SM_3, для погружения метки контейнера num_i. Выбор размера блока связан с предлагаемым способом погружения num_i, описанным ниже, и никак не связан с размером матриц, участвующих при кодировании и погружении ДИ.

В каждый из выбранных P блоков погружается num_i при помощи устойчивого к атакам против встроенного сообщения стеганографического алгоритма, основой для которого послужил стеганоалгоритм, описанный в [11]: для каждого $Bl_k, k = \overline{1,P}$, строится сингулярное разложение

$$Bl_k = U \Sigma V^T, \qquad (2)$$

где U, V - ортогональные $8 \times 8 -$матрицы, столбцы которых – левые и правые сингулярные векторы матрицы Bl_k соответственно, $\Sigma = diag(\sigma_1, .., \sigma_8)$, $\sigma_1 \geq \sigma_2 \geq .... \sigma_8 \geq 0$ - сингулярные числа. Погружение num_i происходит в сингулярные числа Bl_k в соответствии с формулой:

$$\sigma_1 = \left[\sigma_1 - \sigma_2 / K\right] \cdot K + num_i + \sigma_2, \quad K = \max_i(num_i) + 10, \;\; K \in N,$$

где N — множество натуральных чисел.

Для обеспечения устойчивости предложенного стеганоалгоритма предлагается использовать числовые метки num_i с шагом 10 (если взять метки с меньшим шагом

обеспечить устойчивость к возмущающим воздействиям будет крайне затруднительно). В практической части работы предлагается формировать метку подмножеств контейнеров из диапазона [0,50].

После внедрения ДИ в частотной области ЦИ-контейнера происходит возвращение в пространственную при помощи обратного дискретного преобразования Фурье (ОДПФ) для дальнейшей передачи изображения по каналу связи. ОДПФ будет происходить без округлений с учетом специфики формирования коэффициентов Фурье для блоков 2×2 благодаря предложенной организации погружения ДИ [7-9].

Декодирование. На этапе декодирования происходит выделение той составляющей $\overline{\overline{B}}$ цветного ЦИ-СС, в которую происходило погружение ДИ. В общем случае $B \neq \overline{\overline{B}}$.

Декодирование ДИ начинается с выделения метки подмножества контейнеров из $\overline{\overline{B}}$, которую обозначим далее $\overline{num_i}$, из P возможно измененных, а потому обозначаемых далее $\overline{Bl}_k$, $k=\overline{1,P}$, блоков, задействованных для пересылки num_i. В ходе этого для каждого блока $\overline{Bl}_k$ строится сингулярное разложение вида (2), в результате которого вычисляются его сингулярные числа $\overline{\sigma_1}^{(k)} \geq \overline{\sigma_2}^{(k)} \geq ....\overline{\sigma_8}^{(k)} \geq 0,\ k=\overline{1,P}$. Для извлечения метки $\overline{\overline{num_i}}^{(k)}$ из блока $\overline{Bl}_k$, $k=\overline{1,P}$, необходимо проделать следующие шаги:

1. Вычислить значение $M=\left\lfloor\left(\overline{\sigma_1}^{(k)}-\overline{\sigma_2}^{(k)}\right)\Big/K\right\rfloor$;
2. Из всех значений меток num_i, задействованных при формировании *MSP*, выбрать ближайшее к M. Положить $\overline{\overline{num_i}}^{(k)}=M$.

В общем случае $\overline{\overline{num_i}}^{(k)} \neq num_i$. В качестве $\overline{\overline{num_i}}$ выбирается тот номер, который повторяется большее количество раз среди $\overline{\overline{num_i}}^{(k)}$, $k=\overline{1,P}$.

Выделение ДИ будет происходить из частотных коэффициентов преобразования Фурье для непересекающихся блоков 2×2, полученных при помощи стандартного разбиения матрицы $\overline{\overline{B}}$. Из матрицы блока частотных коэффициентов ДПФ $\overline{F}_{nm}^{(\overline{\overline{B}})}(u,v),\ u,v=\overline{0,1}$ происходит выделение 1 элемента (возможно) возмущенной матрицы $\overline{P}^{j(K)}$. Для установления аутентичности/неаутентичности переданной ДИ проводится сравнение $\overline{P}^{j(K)}$ с ключом кодирования $\widetilde{K}_j$ или его инверсией, которые получаются по возможно возмущенному выделенному номеру $\overline{\overline{num_i}}$ из множества стеганографических пар *MSP*, имеющихся у получателя. При таком сравнении ведется подсчет количества К1 совпадений матрицы $\overline{P}^{j(K)}$ с ключом кодирования $\widetilde{K}_j$ или его инверсией. С учетом полученного в [9] порогового значения А=87% для К1, проверка аутентичности ДИ в SM_3 проводится следующим образом:

если $K1>87\%$
то аутентичность дополнительной информации не нарушена
иначе аутентичность дополнительной информации нарушена.

В случае, когда аутентичность ДИ не нарушена, в SM_3 проводится двухэтапная проверка ее целостности аналогично тому, как это предложено в [8]. Для этого на первом этапе из бинарного представления каждого частотного коэффициента каждого блока $\overline{F}_{nm}^{(\overline{\overline{B}})}$, использованного при стеганопреобразовании, происходит выделение значения, которое стоит в использованной при погружении позиции *pos* (см. формулу

(1)). Если из различных элементов текущего блока $\overline{F}_{nm}^{(\overline{\overline{B}})}$ выделяются неодинаковые значения, то целостность ДИ нарушена. Второй этап осуществляет проверку принадлежности всех частотных коэффициентов множеству целых чисел:

если для $\overline{\overline{B}}$ существует блок $\overline{F}_{nm}^{(\overline{\overline{B}})}$, для которого среди его элементов $\overline{F}_{nm}^{(B)}(i,j), i,j=\overline{0,1},$ существует $\overline{F}_{nm}^{(B)}(i,j) \notin Z$, где Z -множество целых чисел

то целостность передаваемой информации нарушена;

иначе целостность передаваемой информации не нарушена.

Декодирование очередного возможно возмущенного бита $\overline{p}_j$ ДИ из очередного блока СС осуществляется следующим образом:

если матрица $\overline{P}^{j(K)}$, удовлетворяет: $\overline{P}^{j(K)} = K_j$,

то $\overline{p}_j = 0$.

если матрица $\overline{P}^{j(K)}$, удовлетворяет: $\overline{P}^{j(K)} = \overline{K_j}$,

то $\overline{p}_j = 1,$

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

если $t_0 > t_1$,

то $\overline{p}_j = 0$,

иначе $\overline{p}_j = 1.$

Таким образом, преимуществом предлагаемого стеганографического метода является не только уменьшенный объем информации, который необходимо передавать по защищенному каналу связи, по сравнению с [8-9], но и то, что он является «слепым», не требующим исходного контейнера на этапе декодирования ДИ.

Результаты

Для апробации предложенного метода SM_3 предлагается реализующий его алгоритм, для которой используются следующие значения параметров:

1. Количество подмножеств контейнеров – *Kol*=5;
2. Количество блоков для погружения метки подмножества контейнеров — *P=5*;
3. Метки подмножеств контейнеров выбирались из множества {10,20,30,40,50}. Необходимо отметить, что при увеличении/уменьшении шага между значениями меток повышается/понижается устойчивость к возмущениям стеганоалгоритма, использованного для погружения метки контейнера. Предлагаемое множество используемых значений обеспечивает компромисс между устойчивостью упомянутого стеганоалгоритма и вероятностью обеспечения надежности восприятия формируемого СС;
4. Размер ключа кодирования – $R = 4$.

Погружение метки подмножества контейнеров происходило в пять блоков контейнера размером 8×8, для которых все значения яркости пикселей находились в диапазоне [50;200], что обеспечивало невыход яркости пикселей СС за границы [0;255].

Непосредственное значение *P=5* выбиралось экспериментальным путем. Благодаря устойчивости стеганоалгоритма, использованного для погружения метки,

$P=5$ обеспечивает декодирование num_i даже при наложении возмущений на СС, которые приводят к нарушению его надежности восприятия (что нельзя утверждать для $P<5$). Таким образом, увеличение P, приводящее к уменьшению скрытой пропускной способности организуемого стеганографического канала связи, является нецелесообразным.

Для проверки эффективности реализующего стеганометод SM_3 алгоритма при указанных значениях параметров в среде Matlab был проведен вычислительный эксперимент, в котором задействовалось 300 ЦИ-контейнеров. В результате эксперимента ошибки первого и второго рода выявлены не были.

Выводы

В работе предлагается усовершенствование уникального стеганографического метода, решающего одновременно актуальную на сегодня триединую задачу стеганографии, включающую в себя одновременную организацию передачу конфиденциальных данных, проверку их аутентичности и целостности.

Предложенная модификация имеет ряд преимуществ по сравнению с методом, разработанным в [8-9]: уменьшенный объем информации, необходимо передаваемой по защищенному каналу связи; SM_3 является «слепым» стеганометодом.

Результаты вычислительных экспериментов подтверждают высокую эффективность усовершенствованного метода SM_3.

Список литературы

1. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М. : СОЛОН-Пресс, 2009. – 272 с.
2. Конахович, Г.В. Компьютерная стеганография. Теория и практика / Г.В. Конахович, А.Ю. Пузыренко. – К.: МК-Пресс, 2006. – 288 с.
3. Кобозєва, А. А. Аналіз захищеності інформаційних систем / А.А. Кобозєва, І.О. Мачалін, В.О. Хорошко. – К.: Вид. ДУІКТ, 2010. – 316 с.
4. Глумов, Н.И. Алгоритм встраивания полухрупких цифровых водяных знаков для задач аутентификации изображений и скрытой передачи информации / Н.И. Глумов, В.А. Митекин // Компьютерная оптика. – 2011. – т.35, №2. – С.262-267.
5. Кобозева, А. А. Стеганографический алгоритм скрытой передачи информации, обеспечивающий аутентификацию контейнера / А.А. Кобозева, А.Д. Шовкун // Науковий вісник Міжнародного гуманітарного університету. – 2012. – №4. – С. 21-28.
6. Ghoshal, N. A Novel Technique for Image Authentication in Frequency Domain using Discrete Fourier Transformation Technique (IAFDDFTT) / N. Ghoshal, J.K. Mandal // Malaysian Journal of Computer Science. – 2008/ – Vol. 21, No. 1. – PP. 24-32.
7. Козина, М. А. Стеганографический метод организации скрытого канала связи, осуществляющий проверку целостности передаваемой информации / М.А. Козина // Сучасна спеціальна техніка. – 2014. – №4(39). – С. 98-106.
8. Кобозева, А.А. Стеганографический метод, обеспечивающий проверку целостности и аутентичности передаваемых данных / А.А. Кобозева, М.А. Козина. // Проблемы региональной энергетики. Электронный журнал Академии наук Республики Молдова. – 2014. – №3 (26). – С. 93-106.
9. Козіна, М.О. Метод перевірки автентичності інформації, що передається стеганографічний каналом зв’язку / М.О. Козіна. // Вісник Вінницького політехнічного інституту. – 2015. – №1. – С. 99-104.
10. Kozina, M.O. Discrete Fourier transform as a basis for steganography method / M.O. Kozina // Праці Одеського політехнічного університету. – 2014. – Вип.2(44). – С.118-126.
11. Мельник, М.А. Стеганоалгоритм, устойчивый к сжатию / М.А. Мельник // Інформаційна безпека. – 2012. – No2(8). – С. 99–106.

МЕТОД ПРИХОВАНОЇ ПЕРЕДАЧІ ДАНИХ, ЯКИЙ ЗАБЕЗПЕЧУЄ ПЕРЕВІРКУ ІЛІСНОСТІ ТА АВТЕНТИЧНОСТІ ІНФОРМАЦІЇ, ЩО ПЕРЕДАЄТЬСЯ

А.А. Кобозєва, М.О. Козіна

Одеський національний політехнічний університет
пр. Шевченко, 1, Одеса, 65044, Україна; e-mail: alla_kobozeva@ukr.net

У роботі пропонується вдосконалення раніше розробленого автором стеганографічного методу, який вирішує одночасно актуальну на сьогодні триєдину задачу стеганографії: прихованої передачі даних, перевірки їх автентичності та цілісності. В якості контейнера використовується цифрове кольорове зображення, а в якості додаткової інформації виступає довільним чином сформована бінарна послідовність. Удосконалення стеганографічного методу включає в себе: зменшення обсягу необхідно переданої інформації по захищеному каналу зв'язку для організації автентифікації даних; забезпечення можливості декодування переданої інформації без наявності контейнера. Наведено результати обчислювальних експериментів, що підтверджують високу ефективність запропонованого методу.
Ключові слова: стеганографічний метод, прихований канал зв'язку, цілісність, автентичність, дискретне перетворення Фур'є, цифрове зображення.

HIDDEN DATA TRANSMISSION METHOD THAT PROVIDES VERIFY THE INTEGRITY AND AUTHENTICITY OF TRANSMITTED INFORMATION

A.Kobozeva, M. Kozina

Odessa National Polytechnic University
1 Shevchenko Str., Odessa, 65044, Ukraine; e-mail: alla_kobozeva@ukr.net

In this work it is proposed the previously developed steganographic method, which solves both actual today triune task steganography: to hide data, verify their authenticity and integrity. As a container used digital color image, as an additional information acts randomly generated binary sequence. Improving steganographic method includes: reduction of transmitted information necessary to secure a communication channel for the organization authentication data; to be able to decode the transmitted information without container. The results of computational experiments confirming the high efficiency of the proposed method.
Keywords: steganography method, hidden communication channel, integrity, authenticity, discrete Fourier transform, a digital image.