

¹Магістр, аспірант кафедри фізико-технічних засобів захисту інформації, Фізико-технічний інститут, Національний технічний університет України «Київський політехнічний інститут», Київ, Україна
²Канд. техн. наук, доцент, доцент кафедри фізико-технічних засобів захисту інформації, Фізико-технічний інститут, Національний технічний університет України «Київський політехнічний інститут», Київ, Україна

СПЕКТРАЛЬНЫЙ АНАЛИЗ СТЕГАНОГРАММ

Для повышения стойкости стеганоалгоритмов к известным методам стегоанализа широко применяются методы скрытия сообщений в области преобразования цифровых изображений. Использование при формировании стеганограмм стандартных методов обработки изображений-контейнеров и стегоданных – двумерных дискретных косинусного и вейвлет преобразований – позволяет минимизировать искажения скрытых сообщений при компрессии изображений.

В работе для выявления факта встраивания стегоданных с применением стандартных преобразований контейнера и стегоданных предложено использовать методы спектрального анализа изображений: анализ спектра сингулярностей и мультифрактальный анализ. Преимуществом данного подхода, по сравнению со статистическими методами стегоанализа, является возможность исследования одновременно нескольких компонент изображения-контейнера, что позволяет локализовать область встраивания.

Анализ эффективности применения методов спектрального анализа был проведен для случая использования одноэтапных и двухэтапных методов формирования стеганограмм. Показано, что скрытие данных приводит к изменениям всех компонент сингулярного разложения изображения-контейнера, а также появлению характерных искажений мультифрактальных характеристик стеганограмм – увеличения мощности множества монофрактальных компонент изображений. Выявленные демаскирующие признаки наличия встроенных сообщений являются устойчивыми в широком диапазоне степеней заполнения контейнера стегоданными, что упрощает задачу обнаружения сообщений, скрытых в области преобразования изображений.

Ключевые слова: цифровые изображения, пассивный стегоанализ, анализ спектра сингулярностей, мультифрактальный анализ.

НОМЕНКЛАТУРА

J+SRM – JPEG & Spatial Rich Model;
PSRM – Projection Spatial Rich Model;
RGB – аддитивная цветовая модель цифровых изображений (Red/Green/Blue);
UHD – Ultra High Definition;
YCbCr – цветоразностная цветовая модель цифрового изображения (Y – компонента яркости; Cb/Cr – синяя/красная цветоразностные компоненты);
YIQ – цветоразностная цветовая модель цифрового изображения (Y – компонента яркости; I/Q – синфазная/квадратурная цветоразностные компоненты);
AMBC – адаптивные методы встраивания стегоданных;
АСС – анализ спектра сингулярностей;
ДДВП – двумерное дискретное вейвлет-преобразование;
ДКП – дискретное косинусное преобразование;
КМ – корреляционная матрица;
МФА – мультифрактальный анализ;
МФС – мультифрактальный спектр;
ПА – преобразование Арнольда;
СОФР – спектр обобщенных фрактальных размерностей;
ЦИ – цифровое изображение;
 a – средняя «шероховатость» текстуры цифрового изображения;
 C – корреляционная матрица;
 D_1 – информационная размерность мультифрактала;
 D_2 – корреляционная размерность мультифрактала;
 $D_{+\infty}(D_{-\infty})$ – граничная обобщенная фрактальная размерность мультифрактала;
 D_q – обобщенная фрактальная размерность мультифрактала;

$D_{x,y}$ – стегоданные (полутонное цифровое изображение);
 $D[\cdot]$ – дисперсия значений;
 $E[\cdot]$ – среднее значение;
 $f(\alpha)$ – функция мультифрактального спектра;
 $F_g(\cdot)$ – преобразование цифрового изображения в базисе функций $\{\vartheta_i\}_{i=1}^{N_g}$;
 G – весовой коэффициент для коэффициентов разложения стегоданных в заданном базисе;
 $H^{\mathbb{R}^{x \times y}}$ – оператор приведения квадратной матрицы к ганкелевому виду (обработка блоками $x \times y$ (элементов));
 $I_{x,y}$ – изображение-контейнер;
 IQR – интерквартильный размах;
 $J(D_{x,y})$ – преобразование стегоданных $D_{x,y}$ перед встраиванием в контейнер;
 k_{st} – стегоключ, используемый при скрытии данных в изображении-контейнере;
 K_{steg} – коэффициенты преобразования стеганограммы;
 M_{BH} – блочно-ганкелева матрица M ;
 M_i – i -я тройка сингулярного разложения;
 M^T – транспонированная матрица M ;
 n_s – относительная высота отдельного блока разбиения матрицы (размер блока – $s \times s$ пикселей);
 N_A – количество итераций преобразования Арнольда;
 $N(s)$ – количество блоков разбиения матрицы (размер блока – $s \times s$ пикселей);

P – количество ненулевых элементов вектора собственных чисел;

$p(n_s)$ – распределение вероятностей значений относительных высот отдельных блоков разбиения матрицы (размер блока – $S \times S$ пикселей);

q – масштабирующий показатель степени обобщенной статистической суммы $Z(q, s)$;

$Q_1(Q_3)$ – первый (третий) квартили распределения значений;

$R_{x,y}$ – скользящее окно обработки цифрового изображения;

$S_{x,y}$ – стеганограмма;

$T_C^i(T_S^i)$ – i -я спектральная характеристика контейнера (стеганограммы);

U – ортонормированная система факторных векторов сингулярного разложения матрицы $M_{BH} M_{BH}^T$;

V – ортонормированная система собственных векторов сингулярного разложения матрицы $M_{BH} M_{BH}^T$;

$Z(q, s)$ – обобщенная статистическая сумма;

$\alpha(q)$ – вероятность заполнения ячеек разбиения монофрактального подмножества мультифрактала при фиксированном значении масштабирующего показателя степени q обобщенной статистической суммы $Z(q, s)$;

λ_i – i -е собственное число матрицы $M_{BH} M_{BH}^T$;

σ – среднее квадратическое отклонение значений яркости пикселей полутонового цифрового изображения;

$\tau(q)$ – функция распределения масштабирующих показателей степени q обобщенной статистической суммы $Z(q, s)$;

Δ_α – ширина мультифрактального спектра;

Δ_b – шаг выборки блоков цифрового изображения;

Δ_f – размах мультифрактального спектра;

Δ_q – шаг выборки значений параметра q ;

Λ – подмножество спектральных характеристик ЦИ, значения которых наиболее изменяются при встраивании стегоданных.

ВВЕДЕНИЕ

В современных методах стеганографии ЦИ широко используются АМВС, особенностью которых является локализация области встраивания – скрытие сообщений производится в шумоподобных текстурах изображения-контейнера, что позволяет существенно повысить стойкость получаемых стеганограмм к известным методам пассивного стегоанализа.

Наиболее часто АМВС применяются для встраивания стегоданных в ЦИ, представленные в графических форматах сжатия без потерь. Повышение устойчивости стеганоалгоритмов на основе АМВС, при компрессии или фильтрации изображений-контейнеров, обеспечивается за счет использования при формировании стеганограмм стандартных преобразований, как изображения-контейнера, так и стегоданных – ДКП и ДДВП.

Для обнаружения стеганограмм, сформированных с использованием ДКП, в работе [1] был предложен эффективный метод статистического стегоанализа. На основе данного метода в работе [2] был построен универсальный стегодетектор, позволяющий выявлять стегоданные, встроенные, как в пространственной, так и частотной областях изображений. Существенным ограничением практического применения предложенного стегодетектора является чрезвычайно высокая размерность используемого пространства признаков – 35263 характеристики ЦИ, по совокупности которых, с высокой вероятностью можно определить наличие встроенных в контейнер данных.

Поэтому актуальной является задача поиска новых методов обнаружения стеганограмм, сформированных на основе АМВС, обеспечивающих высокую вероятность распознавания независимо от области скрытия сообщений при использовании пространства признаков сравнительно небольшой размерности.

Одним из подходов к стегоанализу стеганограмм, сформированных на основе АМВС является использование методов структурного и спектрального анализов ЦИ. Необходимо отметить, что локализация области встраивания стегоданных при использовании АМВС существенно ограничивает эффективность применения классических методов спектрального анализа, например, преобразования Фурье. Поэтому, для выявления характерных изменений спектральных компонент стеганограмм, обусловленных встраиванием стегоданных в контейнер, представляет интерес использование комплексных методов спектрального анализа.

Объектом исследований является пассивный стегоанализ стеганограмм, сформированных путем встраивания исходных, либо предварительно обработанных сообщений в области преобразования ЦИ для общего случая применения одно- и многоэтапных АМВС.

Предметом исследований являются структурные и спектральные методы пассивного стегоанализа, включая АСС и МФА цифровых изображений.

Целью работы является исследование возможностей использования методов АСС и МФА для выявления факта скрытия сообщений для общего случая проведения преобразований, как изображения-контейнера, так и стегоданных.

1 ПОСТАНОВКА ЗАДАЧИ

Пусть мы имеем стеганографическую систему скрытой передачи сообщений, основанную на встраивании изображений-стегоданных $D_{x,y}$ в области преобразования полноцветного изображения-контейнера $I_{x,y}$. При формировании стеганограмм проведены преобразования, как изображения-контейнера, так и скрываемого сообщения. Коэффициенты разложения стеганограмм в базисе преобразования $\{\psi_i\}_{i=1}^{N_\psi}$ определены как сумма соответствующих коэффициентов разложения контейнера $K_{\text{cont}} = F_\psi(I_{x,y}, k_{st})$ и, взятых с весовым коэффициентом G , скрываемого сообщения $K_{\text{data}} = F_\psi(D_{x,y}, k_{st})$:

$$K_{\text{steg}} = K_{\text{cont}} + G \cdot K_{\text{data}}. \quad (1)$$

Рассматривается наиболее сложный для проведения стегоанализа случай, когда в качестве стегоключа k_{st} выбраны позиции коэффициентов K_{cont} , измененных при скрытии сообщений, а также параметры преобразования стегоданных $J(D_{x,y})$.

Тогда для выявления стеганограмм необходимо выделить подмножество спектральных характеристик ЦИ, которые наиболее сильно изменяются при встраивании стегоданных в области преобразования изображений-контейнеров согласно АМВС. Данная задача сводится к задаче минимизации целевой функции:

$$\frac{1}{\sum_{i \in \Lambda} |T_C^i - T_S^i|} \rightarrow \min.$$

2 ОБЗОР ЛИТЕРАТУРЫ

Локальный характер изменений параметров ЦИ, в случае применения адаптивных методов скрытия сообщений, существенно усложняет проведение стегоанализа с использованием стандартных методов, основанных на использовании простых статистических моделей ЦИ, например, χ^2 -теста, RS-анализа.

Для повышения эффективности пассивного стегоанализа стеганограмм в случае применения АМВС был предложен метод, основанный на использовании статистических моделей ЦИ [3], включающих наборы (кластеры) статистических характеристик изображений. При формировании кластеров использовались наиболее общие параметры ЦИ, в частности, гистограммы распределений и матрицы сочетаемости яркости пикселей. Дальнейшее увеличение точности распознавания АМВС было достигнуто путем объединения нескольких кластеров характеристик ЦИ (например, J+SRM-модель [2]), и анализа результатов свертки шумовых компонент ЦИ со случайно выбранными векторами в PSRM-модели [4]. Платой за высокую точность обнаружения стеганограмм являлось существенное возрастание требований к объему тестовой выборки ЦИ и времени настройки стегодетектора.

В работах [5, 6] для исследования изменений параметров ЦИ, обусловленных встраиванием стегоданных с применением ДКП и ДДВП, было предложено использовать специальные методы структурного анализа ЦИ. Было показано, что скрытие сообщений в контейнерах приводит к существенным изменениям мультифракталь-

ных характеристик шумовых компонент ЦИ [5], вид которых зависит от типа использованных преобразований контейнера и наличия/отсутствия этапа предварительной обработки стегоданных [7]. В ряде случаев практическое использование данных методов ограничивает их высокая вычислительная сложность и возможность анализа только шумовых компонент ЦИ. Поэтому представляет интерес использование методов спектрального анализа, позволяющих проводить комплексное исследование изменений параметров ЦИ, для определения факта встраивания стегоданных с применением ДКП и ДДВП.

В работах [5, 6] для исследования изменений параметров ЦИ, обусловленных встраиванием стегоданных с применением ДКП и ДДВП, было предложено использовать специальные методы структурного анализа ЦИ. Было показано, что скрытие сообщений в контейнерах приводит к существенным изменениям мультифрактальных характеристик шумовых компонент ЦИ [5], вид которых зависит от типа использованных преобразований контейнера и наличия/отсутствия этапа предварительной обработки стегоданных [7]. В ряде случаев практическое использование данных методов ограничивает их высокая вычислительная сложность и возможность анализа только шумовых компонент ЦИ. Поэтому представляет интерес использование методов спектрального анализа, позволяющих проводить комплексное исследование изменений параметров ЦИ, для определения факта встраивания стегоданных с применением ДКП и ДДВП.

3 МАТЕРИАЛЫ И МЕТОДЫ

В работе исследованы одноэтапные и двухэтапные стеганографические методы, использующие преобразования, как контейнеров, так и стегоданных. Этапы обработки контейнеров и стегоданных согласно методам Дея [9], Элайона [8] и Гунджаля [10] представлены в табл. 1.

На предварительном этапе обработки ЦИ, согласно методам Элайона и Гунджаля, производилось изменение системы цвета изображения-контейнера (табл. 1): с RGB на YCbCr/YIQ, что позволило минимизировать искажения цвета изображения-контейнера при встраивании стегоданных.

Формирование стеганограмм согласно методам Дея и Элайона производилось согласно формуле (1) с выборок в качестве базисных функций ДДВП вейвлета Хаара и соответствующей ему скейлинг-функции. Минимальное и максимальное значения параметра G были опре-

Таблица 1 – Этапы обработки контейнера и стегоданных при формировании стеганограмм согласно рассмотренным стеганографическим методам

Метод	Обработка контейнера			Обработка стегоданных		Весовой коэффициент G
	Изменение системы цвета	Первый этап	Второй этап	Первый этап	Второй этап	
Дея	–	ДДВП	–	ДДВП	–	0,02; 0,04; 0,06; 0,08
Элайона	RGB → YCbCr (скрытие в Y-канале)	ДДВП	–	Преобразование Арнольда	ДДВП	1; 4; 8; 12
Гунджаля	RGB → YIQ (скрытие в I-канале)	ДДВП	ДКП	Преобразование Арнольда	ДКП	$G_0 = 3$; $G_1 \in \{5, 8, 11, 14\}$

делены из условий возможности извлечения стегоданных без искажений и появления видимых изменений изображения-контейнера при встраивании сообщений.

Для дополнительного уменьшения вероятности выявления стеганограмм, при их формировании, к стегоданным, представленным в виде полутонового изображения $D_{x,y}$ с размерами $W_x \times W_y$ ($W_x = W_y$) (пикселей), применялись N_A итераций ПА [11]. Особенностью ПА является периодичность – после конечного количества итераций исходное и полученное изображения совпадают. Для предотвращения такой ситуации в работе количество итераций ПА было выбрано равным $N_A = 23$, которое не является делителем размеров встраиваемых стегоданных.

В случае двухэтапного метода Гунджаля, к детализирующим коэффициентам ДДВП, полученным на первом этапе обработки изображения-контейнера, применялось ДКП. Встраивание сообщений, полученных после ПА, производилось аналогично формуле (1) – путем суммирования коэффициентов ДКП контейнера и стегоданных. Отметим, что величина весового параметра G изменялись в зависимости от значения скрываемого бита (табл. 1) – единицы ($G = G_1$) либо нуля ($G = G_0$).

АСС ЦИ является двумерным расширением известного метода исследований временных рядов Singular Spectrum Analysis [12]. Особенностью данного метода является использование сингулярного разложения для разделения информативных и шумовых компонент рассматриваемого сигнала.

АСС изображений проводился в четыре этапа [12]. На первом этапе, путем обработки заданного полутонового изображения $I_{x,y}$ ($N_x \times N_y$ пикселей) с использованием скользящего окна $R_{x,y}$ ($L_x \times L_y$ пикселей), была сформирована блочно-ганкелева матрица M_{BH} :

$$M_{BH} = \begin{pmatrix} B_1 & B_2 & B_3 & \cdots & B_{K_y} \\ B_2 & B_3 & B_4 & \cdots & B_{K_y+1} \\ B_3 & B_4 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ B_{L_y} & B_{L_y+1} & \cdots & \cdots & B_{N_y} \end{pmatrix},$$

$$B_j = \begin{pmatrix} I_{1,j} & I_{2,j} & \cdots & I_{K_x,j} \\ I_{2,j} & I_{3,j} & \cdots & I_{K_x+1,j} \\ \vdots & \vdots & \ddots & \vdots \\ I_{L_x,j} & I_{L_x+1,j} & \cdots & I_{N_x,j} \end{pmatrix}. \quad (2)$$

где $K_x = N_x - L_x + 1$, $K_y = N_y - L_y + 1$.

На втором этапе было выполнено сингулярное разложение матрицы M_{BH} :

$$M_{BH} = \sum_{i=1}^P M_i = \sum_{i=1}^P \sqrt{\lambda_i} U_i V_i^T. \quad (3)$$

На третьем этапе анализа производилась группировка троек M_i (3) в L групп:

$$M_{BH} = \sum_{i=1}^P M_i = \sum_{j=1}^L \left(\sum_{q=1}^{L_j} M_q \right), \quad \sum_j L_j = P. \quad (4)$$

На последнем этапе АСС для восстановления исходного ЦИ в пространственной области проводилась нормировка групп собственных троек (4) по норме Фробениуса и проектирование их на множество блочно-ганкелевых матриц вида (2), используя операторы $H_{\omega}^{1 \times 1}$ и $H_{\omega}^{L_x \times K_x}$ [12], усредняющие элементы внутри блоков матрицы M :

$$\tilde{M} = H_{\omega}^{L_x \times K_x} \circ H_{\omega}^{1 \times 1} (M) = H_{\omega}^{1 \times 1} \circ H_{\omega}^{L_x \times K_x} (M).$$

Обычно порядок группировки троек M_i для чистого изображения-контейнера неизвестен. Поэтому анализ интегральных изменений компонент АСС-разложения ЦИ (групп собственных троек) был проведен на основе исследования параметров КМ (табл. 2), элементы которой рассчитывались согласно формуле:

$$C_{ij} = \frac{E \left[(M_i - E[M_i]) (M_j - E[M_j]) \right]}{\sqrt{D[M_i]} \sqrt{D[M_j]}}, \quad i \leq P, j \leq P.$$

Однородность значений элементов КМ (табл. 2) является мерой близости положения элементов с большими значениями к главной диагонали КМ, а энтропия позволяет оценить степень «хаотичности» значений элементов корреляционной матрицы C .

Для выявления и исследования фрактальных свойств временных рядов широко используется МФА [13]. Отличие МФА от известных методов оценки показателя Херста, например, R/S-анализа, состоит в представлении исследуемого сигнала в виде суперпозиции набора фракталов с единственным значением фрактальной размерности (монофракталов), что позволяет исследовать мультифрактальные свойства отдельных компонент сигнала.

Таблица 2 – Исследованные параметры корреляционной матрицы компонент АСС-разложения стеганограмм

Параметр корреляционной матрицы	Формула для расчета
Равномерность значений элементов	$R_1 = \sum_{i=1}^P \sum_{j=1}^P C_{ij}^2$
Однородность значений элементов КМ	$R_2 = \sum_{i=1}^P \sum_{j=1}^P [C_{ij} / (1 + i - j)]$
Средние значения элементов КМ	$R_3 = (1/P^2) \sum_{i=1}^P \sum_{j=1}^P C_{ij}$
Параметр корреляционной матрицы	Формула для расчета
Энтропия значений элементов КМ	$R_4 = -\sum_{i=1}^P \sum_{j=1}^P (p_{ij} \times \log_2 p_{ij}),$ $p_{ij} = C_{ij} / \sum_{i=1}^P \sum_{j=1}^P (C_{ij})$

Классические методы МФА позволяют проводить анализ только бинарных ЦИ и дают существенную погрешность при оценке мультифрактальных параметров, обусловленную наличием краевых эффектов [14]. Поэтому в работе был использован усовершенствованный метод оценки мультифрактальных характеристик ЦИ [15], который выдержал следующие этапы:

1. Фрагментирование исходного ЦИ $I_{x,y}$, представленного в градациях серого цвета, на перекрывающиеся блоки размером $s \times s$ пикселей. Область пересечения блоков по горизонтали (вертикали) составляла одну строку (столбец).

2. Вычисление относительной высоты n_s каждого блока разбиения ЦИ:

$$n_s = \begin{cases} \lceil (z_{\max} - z_{\min}) \cdot (1 + 2a\sigma) / (s - 1) \rceil, & \text{если } z_{\max} \neq z_{\min} \\ 1, & \text{если } z_{\max} = z_{\min} \end{cases}$$

Согласно рекомендациям [15], значение параметра a было выбрано равным 3, что позволило минимизировать погрешность оценки мультифрактальных параметров ЦИ при анализе шумоподобных текстов.

3. Вычисление распределения вероятностей $p(n_s) = n_s / \sum_s n_s$ для высот n_s отдельных блоков разбиения $I_{x,y}$ и заданного размера блока s .

4. Вычисление обобщенной статистической суммы $Z(q, s)$ и спектра обобщенных фрактальных размерностей D_q :

$$Z(q, s) = \begin{cases} \sum_{i=1}^{N(s)} p_i^q(s), & \text{если } q \in \mathbb{R} \setminus \{0\}; \\ \sum_{i=1}^{N(s)} [-p_i(s) \times \log(p_i(s))], & \text{если } q = 0, \end{cases}$$

$$D_q = \frac{\tau(q)}{q-1}, \tau(q) = \lim_{r \rightarrow 0} \frac{\ln Z(q, r)}{\ln(r)}.$$

5. Вычисление мультифрактального спектра:

$$\alpha(q) = \frac{d}{dq} [(q-1) \cdot D_q], f(\alpha) = q \cdot \alpha(q) - \tau(q).$$

Для повышения точности оценки значений обобщенных фрактальных размерностей этапы № 1–3 повторялись не менее трех раз при разных значениях размера блока разбиения s . При проведении исследований мультифрактальных параметров стеганограмм были использованы следующие характеристики СОФР и МФС [13]: информационная (D_1), корреляционная (D_2) и граничные обобщенные фрактальные размерности ($D_{-\infty}, D_{+\infty}$); ширина ($\Delta_\alpha = \alpha_{\max} - \alpha_{\min}$) и размах ($\Delta_f = f_{\max} - f_{\min}$) МФС.

4 ЭКСПЕРИМЕНТЫ

Исследование было проведено с использованием тестового пакета из ста полноцветных ЦИ с разрешением UHD-4K. В качестве стегоданных были выбраны три полноцветных изображения с различной степенью детализации: портрет, чертеж и карта. Характеристики тестовых изображений и скрываемых сообщений представлены в табл. 3.

Анализ стеганограмм проводился при изменении степени заполнения контейнера стегоданными (отношения измененных коэффициентов разложения ЦИ к общему количеству коэффициентов разложения изображения-контейнера) от 5% до 25%, с шагом 5%, и от 25% до 95%, с шагом 10%.

В работе приведены результаты исследования АСС стеганограмм, сформированных согласно методу Дея при размерах скользящего окна $R_{x,y}$ равных 50×50 (пикселей) и шаге выборки блоков ЦИ по строкам/столбцам $\Delta_b = 500$ пикселей. Отметим, что АСС характеризуется высокой вычислительной сложностью и для его реализации необходим большой объем памяти. Это связано с тем, что размеры матрицы $M_{BH}(2)$ нелинейно зависят от размеров анализируемого ЦИ и скользящего окна $R_{x,y}$:

$$M_{(L_x L_y) \times (K_x K_y)} = M_{(L_x L_y) \times [(N_x - L_x + 1)(N_y - L_y + 1)]}.$$

По результатам предварительных исследований было установлено, что заданная точность определения характеристик МФА ЦИ при минимальном времени расчета достигается при выборе диапазона значений параметра $q \in [-20; 20]$ и шаге выборки $\Delta_q = 0,5$. Зависимости D_q , $\alpha(q)$ и $f(\alpha)$ получены при использовании сплайн-интерполяции данных.

5 РЕЗУЛЬТАТЫ

Результаты АСС стеганограмм, сформированных согласно методу Дея, представлены на рис. 1–2 в виде графика «ящик с усами». Линией в «ящике» и кружком отображаются, соответственно, медиана и среднее значение параметров КМ; концы «усов» рассчитывались согласно следующим выражениям: $L_{up} = Q_3 + 1,5 \cdot (Q_3 - Q_1)$, $L_{down} = Q_1 - 1,5 \cdot (Q_3 - Q_1)$, где первый (Q_1) и третий (Q_3) квартили распределения значений параметров КМ соответствуют нижней /верхней границе «ящика».

Скрытие стегоданных согласно методу Дея приводит к существенным изменениям медиан значений равномерности (рис. 1а) и энтропии (рис. 2) элементов КМ, что дает возможность распознавать наличие скрытых сообщений в ЦИ. Одновременное уменьшение интерквартильного размаха $IQR = Q_3 - Q_1$ значений анализируемых параметров свидетельствует об устойчивости данного демаскирующего признака.

Таблица 3 – Характеристики тестовых изображений и стегоданных

Параметр	Тестовые изображения	Стегоданные		
		Портрет	Чертеж	Карта
Разрешение, пикселей	3840×2160	565×850	567×463	800×800
Формат представления	JPEG	BMP	BMP	BMP
Система цвета	RGB	RGB	RGB	RGB
Глубина цвета, [бит/(пиксель×канал)]	8	8	8	8

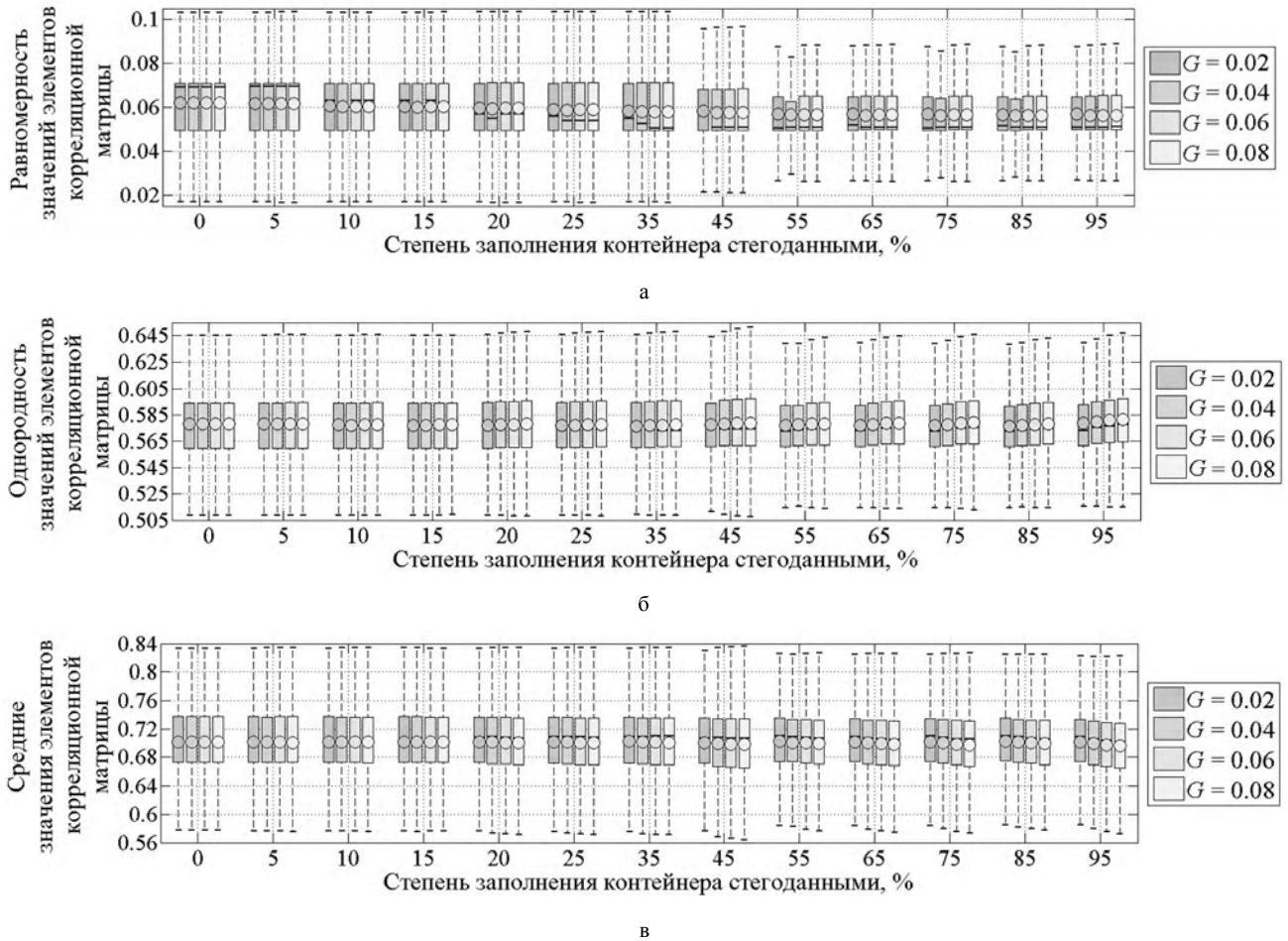


Рисунок 1 – Результаты АСС стеганограм, сформированных согласно методу Дея: а – равномерность значений элементов КМ; б – однородность значений элементов КМ; в – средние значения элементов КМ

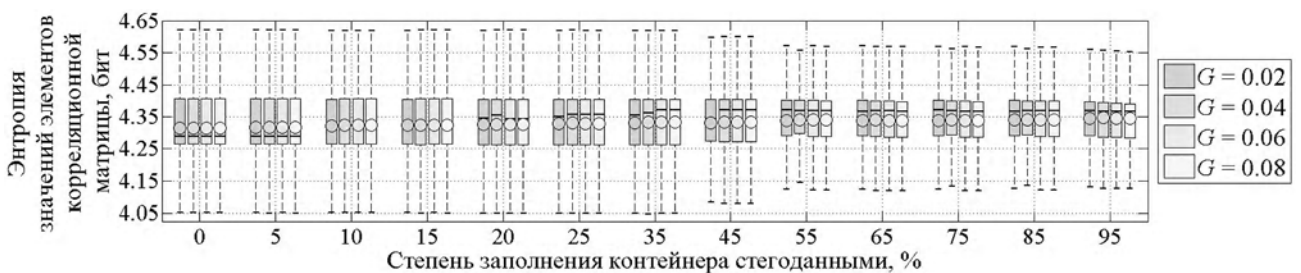


Рисунок 2 – Результаты АСС стеганограм, сформированных согласно методу Дея – энтропия значений элементов КМ

Для оценки изменений мультифрактальных параметров компонент ЦИ при встраивании стегоданных был проведен МФА стеганограм. Результаты МФА представлены на рис. 3–4, где минимальные значения параметров получены при $G = G_{\min}$, а максимальные – при $G = G_{\max}$ (табл. 1).

Изменения информационной (рис. 3а), корреляционной (рис. 3б) и граничной обобщенной фрактальной размерности $D_{+\infty}$ (рис. 4б) для одноэтапных методов встраивания стегоданных близки к нулю. Это свидетель-

ствует о незначительных изменениях энтропии яркости пикселей всего изображения и корреляции значений яркости соседних пикселей при формировании стеганограм согласно методам Дея и Элайона.

Изменения параметров СОФР и МФС ЦИ (рис. 3–4) в случае применения двухэтапного метода Гунджала существенно больше изменений соответствующих параметров для одноэтапных методов Дея и Элайона, что позволяет распознавать применение одно- и двухэтапных методов скрытия сообщений при проведении стегоанализа ЦИ.

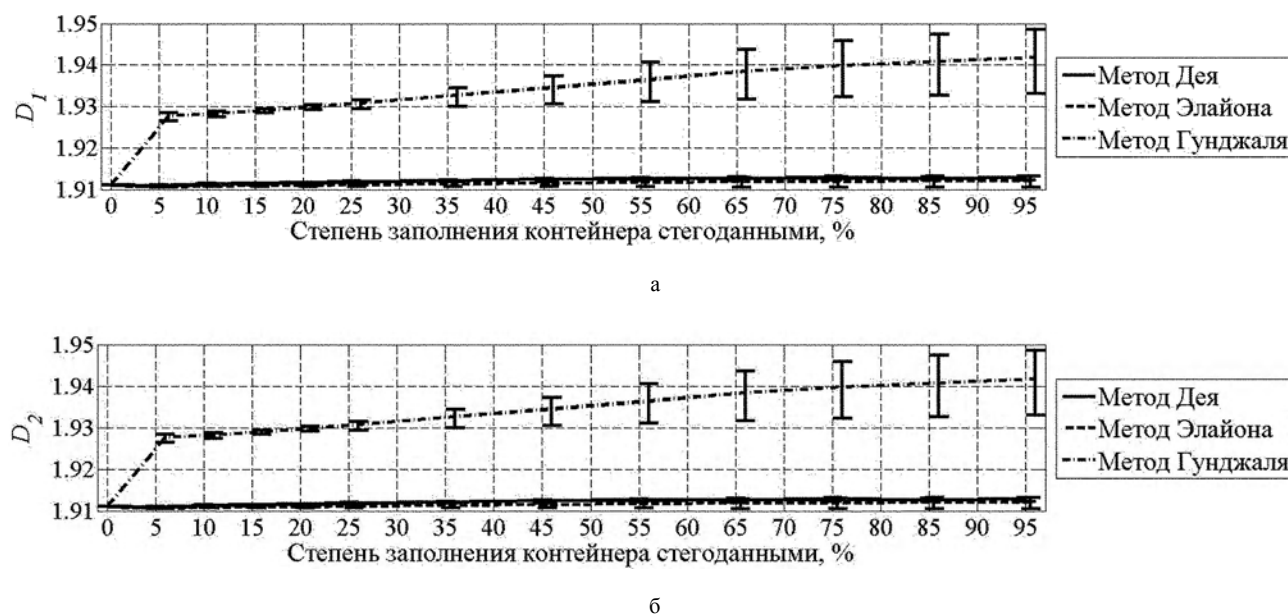


Рисунок 3 – Результаты МФА стеганограмм: а – информационная размерность D_1 ; б – корреляционная размерность D_2 ; в – граничная обобщенная фрактальная размерность $D_{-\infty}$

6 ОБСУЖДЕНИЕ

Предложенный метод пассивного стегоанализа, по сравнению с методами, рассмотренными в работах [2–4], при заданной вероятности распознавания стеганограмм, требует существенно меньших затрат времени и ресурсов памяти, даже для случая многоэтапного формирования стеганосистемы.

Формирование стеганограмм согласно методу Дея практически не изменяет усредненных значений элементов КМ (рис. 1в), но приводит к возрастанию энтропии их значений (рис. 2), что соответствует росту дисперсии значений элементов КМ. С другой стороны, однородность значений элементов КМ остается практически неизменной (рис. 1б), что свидетельствует об одинаковом уровне искажений, внесенных в компоненты АСС-разложения ЦИ при скрытии стегоданных.

К недостаткам предложенного метода пассивного стегоанализа можно отнести то, что диапазон изменений характеристик АСС-разложения стеганограмм сравнительно мал (порядка 10^{-3}). Вследствие этого (существенно) усложняется алгоритм настройки стегодетектора, однако использование интегральных характеристик АСС-разложения стеганограмм позволяет достичь вероятности распознавания стеганограмм сопоставимой со случаем применения J+SRM-модели [2] при существенном сокращении размерности используемого пространства признаков.

Отметим, что при проведении МФА был получен а priori неочевидный результат. Двухэтапный метод Гунджала встраивания стегоданных, который за счет уменьшения уровня демаскирующих признаков показал высокую робастность к стандартным методам стегоанализа, в случае применения МФА оказался менее

устойчивым, чем одноэтапные методы. Существенное увеличение значений обобщенных фрактальных размерностей $D_{-\infty}$ ($D_{+\infty}$) для данного метода (рис. 4а–4б), может быть интерпретировано, как соответствующее увеличение фрактальных размерностей шумовых и детерминированных, например, контуров объектов, компонент ЦИ. Возрастание ширины Δ_α и уменьшение размаха Δ_f МФС (рис. 4в–4г) свидетельствует об увеличении мощности множества монофрактальных компонент ЦИ при сужении диапазона значений фрактальных размерностей данных компонент.

Также было выявлено, что предварительная обработка стегоданных в случае одноэтапных методов (метод Элайона) позволяет минимизировать искажения мультифрактальных параметров ЦИ (рис. 3–4) в широком диапазоне значений степени заполнения контейнера.

ВЫВОДЫ

В работе решена задача выявления характерных искажений спектральных характеристик стеганограмм, сформированных согласно АМВС, с использованием АСС и МФА для общего случая обработки, как изображения-контейнера, так и скрываемых сообщений.

Научная новизна результатов, полученных в статье, состоит в том, что впервые выдвинута и экспериментально подтверждена гипотеза о возможности использования спектральных методов анализа ЦИ для распознавания факта скрытия сообщений в области преобразования контейнера.

В результате проведенных исследований спектральных характеристик стеганограмм, сформированных согласно одно- и двухэтапным методам встраивания стегоданных, установлено следующее.

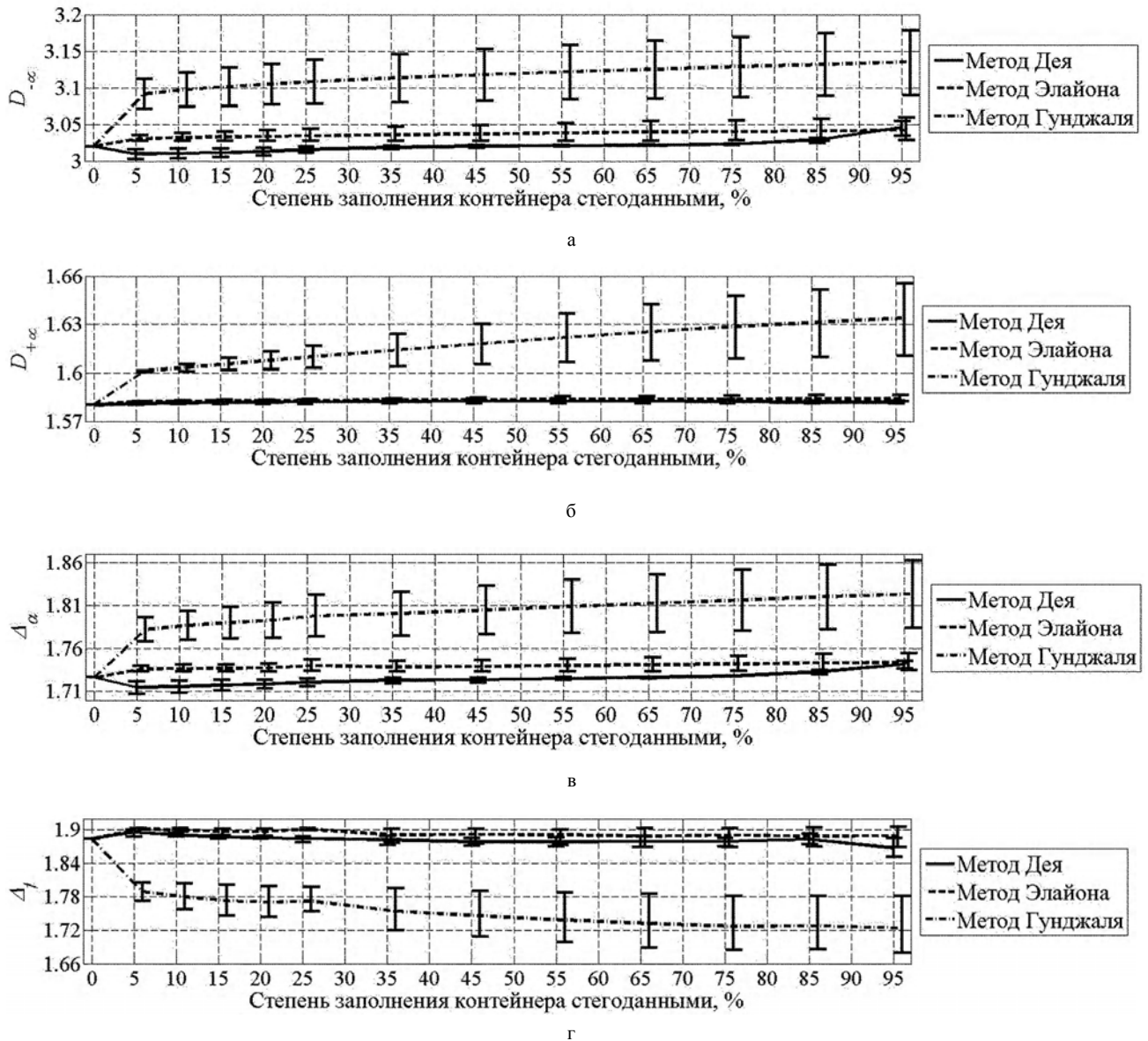


Рисунок 4 – Результаты МФА стеганогамм: а – граничная обобщенная фрактальная размерность $D_{-\infty}$; б – граничная обобщенная фрактальная размерность $D_{+\infty}$; в – ширина МФС Δ_{α} ; г – размах МФС Δ_f

1. Встраивание стегоданных в контейнеры с применением одноэтапных методов приводит к значительным изменениям энтропии значений элементов КМ компонент АСС-разложения ЦИ. Данный демаскирующий признак является устойчивым в широком диапазоне значений степени заполнения контейнера стегоданными, что представляет особый интерес в связи с постоянным увеличением объемов контейнеров, например от Full HD к UHD-4K и UHD-8K.

2. Характерные изменения результатов МФА стеганогамм, сформированных двухэтапными методами – возрастание мощности множества монофрактальных компонентов ЦИ и уменьшение диапазона изменений фрактальных размерностей данных компонент, позволяет обнаруживать факт использования данных стеганографических методов с высокой точностью.

3. Не смотря на то, что при формировании стеганогамм на основе одно и двухэтапных методов используются преобразования одного вида, для повышения эффективности пассивного стегоанализа, для каждого метода необходима разработка специализированного стегодетектора.

Практическая значимость работы состоит в том, что:

- разработан программный комплекс, позволяющий проводить пассивный стегоанализ стеганогамм, сформированных на основе одно- и многоэтапных АМВС;
- применение выявленных характерных изменений спектральных характеристик ЦИ при скрытии сообщений согласно АМВС позволило существенно уменьшить время и вычислительную сложность процедуры настройки стегодетектора;

Полученные результаты могут быть использованы для повышения точности современных стегодетекторов и разработки целевых методов активного стегоанализа двухэтапных комплексных методов скрытия сообщений в ЦИ.

Дальнейший интерес представляет исследование возможности применения МФА в случае использования статистических АМБС (например, методов HUGO, S-UNIWARD).

БЛАГОДАРНОСТИ

Статья написана по материалам, полученным в рамках выполнения научно-исследовательской темы «Стеганография многомерных сигналов кафедры физико-технических средств защиты информации Физико-технического института Национального технического университета Украины «Киевский политехнический институт».

СПИСОК ЛИТЕРАТУРЫ

1. Kodovsky J. Calibration revisited / J. Kodovsky, J. Fridrich // 11th Multimedia and Security Workshop, New York, 2009 : proceedings. – New York : ACM Press, 2009. DOI 10.1145/1597817.1597830.
2. Fridrich J. Rich models for steganalysis of digital images / J. Fridrich, J. Kodovsky // Transactions on Information Forensics and Security. – 2012. – Vol. 7, Issue 3. – P. 868–882. DOI 10.1109/tifs.2012.2190402.
3. Liu Q. Steganalysis of DCT-embedding based adaptive steganography and YASS / Q. Liu // 13th Multimedia & Security Workshop, New York, 2011 : proceedings. – New York : ACM Press, 2011. – P. 77–86. DOI 10.1145/2037252.2037267.
4. Holub V. Random Projections of Residuals for Digital Image Steganalysis / V. Holub, J. Fridrich // Transactions on Information Forensics and Security. – 2013. – Vol. 8, Issue 12. – P. 1996–2006. DOI 10.1109/tifs.2013.2286682.
5. Прогонов Д. О. Виявлення стеганогам з даними, прихованими в області перетворення цифрових зображень / Д. О. Прогонов, С. М. Куш // Вісник Національного технічного університету України «Київський політехнічний інститут». Серія «Радіотехніка. Радіоапаратування». – 2014. – № 57. – С. 128–142.
6. Прогонов Д. Вариограмний аналіз стеганогам / Д. Прогонов, С. Куш // Захист інформації і безпека інформаційних систем: III Міжнародна науково-технічна конференція, Львів, 5–6 червня 2014 р.: матеріали конференції. – Львів : Українська академія друкарства, 2014. – С. 84–85.
7. Прогонов Д. А. Определение типа преобразований, использованных для скрытия данных в цифровых изображениях / Д. А. Прогонов, С. Н. Куш // System analysis and information technologies : 16-я Международная научно-практическая конференция, Киев, 26–30 мая 2014 г. : материалы конференции. – К. : УНК «ИПСА» НТУУ «КПИ», 2014. – С. 435–436.
8. Elahian A. Improved robust DWT-watermarking in YCbCr color space / A. Elahian, M. Khalili, S. B. Shokouhi // Global journal of computer application and technology. – 2011. – Vol. 1, Issue 3. – P. 300–304.
9. Dey N. A novel approach of color image hiding using RGB color planes and DWT / N. Dey, A. B. Roy, S. Dey // International journal of computer application. – 2011. – Vol. 36, Issue 5. – P. 19–24.
10. Gunjal B. L. Secured color image watermarking technique in DWT-DCT domain / B. L. Gunjal, S. N. Mali // International Journal of Computer Science, Engineering and Information Technology (IJCEIT). – 2011. – Vol. 1, Issue 3. – P. 36–44.
11. Nance J. Periods of discretized Arnold Cat Map and its extension to dimensions [Electronic resource] / J. Nance. – Cornell University Library, e-print archive. – Access mode: <http://arxiv.org/abs/1111.2984>.
12. Golyandina N. E. 2D-extension of singular spectrum analysis: algorithm and elements of theory / N. E. Golyandina, K. D. Usevich // World scientific. – P. 449–473. – DOI 10.1142/9789812836021_0029.
13. Божокін С.В. Фрактали і мультифрактали: монографія / С. В. Божокін, Д. А. Паршин. – Іжевск : НИЦ. Регулярна і хаотическа динаміка, 2001. – 128 с.
14. Lopes R. Fractal and multifractal analysis: A review / R. Lopes, N. Betrouni // Medical Image Analysis. – 2009. – Vol. 13, Issue 4. – P. 634–649. DOI 10.1016/j.media.2009.05.003.
15. Li J. An improved box-counting method for image fractal dimension estimation / J. Li, Q. Du, C. Sun // Pattern Recognition. – 2009. – Vol. 42, Issue 11. – P. 2460–2469. DOI 10.1016/j.patcog.2009.03.001.

Статья поступила в редакцию 09.12.2014.

После доработки 12.12.2014.

Прогонов Д. О.¹, Куш С. М.²

¹Магістр, аспірант кафедри фізико-технічних засобів захисту інформації, Фізико-технічний інститут, Національний технічний університет України «Київський політехнічний інститут», Київ, Україна

²Канд. техн. наук, доцент, доцент кафедри фізико-технічних засобів захисту інформації, Фізико-технічний інститут, Національний технічний університет України «Київський політехнічний інститут», Київ, Україна

СПЕКТРАЛЬНИЙ АНАЛІЗ СТЕГАНОГРАМ

Для підвищення стійкості стеганоалгоритмів до відомих методів стегоаналізу широко використовуються методи приховання повідомлень в області перетворення цифрових зображень. Використання при формуванні стеганогам стандартних методів обробки зображень-контейнерів та стегоданих – двовимірних дискретних косинусного та вейвлет перетворень – дозволяє мінімізувати спотворення вбудованих повідомлень при стисненні зображень.

В роботі для виявлення факту вбудовування стегоданих з використанням стандартних перетворень контейнеру та стегоданих запропоновано використовувати методи спектрального аналізу зображень: аналіз спектру сингулярностей та мультифрактальний аналіз. Перевагою даного підходу у порівнянні зі статистичними методами стегоаналізу є можливість дослідження одночасно декількох компонент зображення-контейнеру, що дозволяло локалізувати область приховання повідомлень.

Аналіз ефективності застосування методів спектрального аналізу був проведений для випадку використання одноетапних та багатоетапних методів формування стеганогам. Показано, що вбудовування повідомлень призводить до змін усіх компонент сингулярного розкладу зображення-контейнеру, а також появі характерних спотворень мультифрактальних характеристик стеганогам – підвищення потужності множини монофрактальних компонент зображень. Виявлені демаскуючі ознаки наявності прихованих повідомлень є стійкими в широкому діапазоні змін ступеня заповнення контейнеру стегоданими, що спрощує задачу виявлення повідомлень, прихованих в області перетворення зображень.

Ключові слова: цифрові зображення, пасивний стегоаналіз, аналіз спектру сингулярностей, мультифрактальний аналіз.

Progonov D. O.¹, Kushch S. M.²

¹M.Sc., post-graduate student of Faculty of Information Security, The Institute of Physics and Technology, National technical University of Ukraine «Kyiv Polytechnic Institute», Kyiv, Ukraine

²Ph.D, Associate Professor, Associate Professor of Faculty of Information Security, The Institute of Physics and Technology, National technical University of Ukraine «Kyiv Polytechnic Institute», Kyiv, Ukraine

SPECTRAL ANALYSIS OF STEGANOGRAMS

The data embedding algorithms in transformation domain of digital images are widely used for increasing the robustness of stegoalgorithms to known steganalysis methods. Applying of standard transformations the digital images by steganograms forming – two-dimensional discrete cosine and wavelet transforms – allows minimizing the garbling the hidden messages by image compression.

We propose to use the spectral analysis methods – singular spectrum analysis and multifractal analysis – for revealing the fact of message embedding with usage of standard transform of cover image and stegodata. The advantage of such approach in comparison with statistical steganalysis methods is possibility to simultaneously investigation of several components the cover image, which allows localizing the domain of data hiding.

Research of effectiveness of the spectral analysis methods was provided for the case of usage the one-stage and multi-stage embedding methods. It is shown that stegodata embedding leads to alteration the all components of singular value decomposition of cover images as well as appearance the peculiar alteration of multifractal features the steganograms – increasing the cardinality of monofractal components the image. Revealed distinctive features of steganograms are stable in wide range of cover image payloads, which is simplifying of task of stegodata revealing, hidden in transformation domain of digital images.

Keywords: digital images, passive steganalysis, singular spectrum analysis, multifractal analysis.

REFERENCES

- Kodovsky J., Fridrich J. Calibration revisited, *11th Multimedia and Security Workshop, New York, 2009: proceedings*. New York, ACM Press, 2009. DOI 10.1145/1597817.1597830.
- Fridrich J., Kodovsky J. Rich models for steganalysis of digital images, *Transactions on Information Forensics and Security*, 2012, Vol. 7, Issue 3, pp. 868–882. DOI 10.1109/tifs.2012.2190402.
- Liu Q., Steganalysis of DCT-embedding based adaptive steganography and YASS, *13th Multimedia & Security Workshop, New York, 2011, proceedings*. New York, ACM Press, 2011, p. 77–86. DOI 10.1145/2037252.2037267.
- Holub V., Fridrich J. Random Projections of Residuals for Digital Image Steganalysis, *Transactions on Information Forensics and Security*, 2013, Vol. 8, Issue 12, pp. 1996–2006. DOI 10.1109/tifs.2013.2286682.
- Progonov D. O., Kushch S. M. Vyjavlennja steghanogram z danymy, prykhovanymy v oblasti peretvorennja cyfrovykh zobrazenj, *Visnyk Nacionalnogo tekhnichnogho universytetu Ukrainy «Kyivskij politekhnichnyj instytut»*. Serija – Radiotekhnika. Radioaparotobuduvannja, 2014, Vol. 57, pp.128–142.
- Progonov D., Kushch S. Variogramnyj analiz steganogram, *Zahyst informacii i bezpeka informacijnyh system: III Mizhnarodna naukovo-tehnichna konferencija, L'viv, 5–6 chervnja 2014 r.: materialy konferencii*. L'viv, Ukraïns'ka akademija drukarstva, 2014, pp. 84–85.
- Progonov D. A., Kushch S. N. Opredelenie tipa preobrazovanij, ispol'zovannyh dlja skrytija dannyh v cifrovych izobrazhenijah, *System analysis and information technologies: 16-taja Mezhdunarodnaja nauchno-prakticheskaja konferencija*, Kiev, 26–30 maja 2014 g.: materialy konferencii. Kiev, UNK «IPSA» NTUU «KPI», 2014, pp. 435–436.
- Elahian A., Khalili M., Shokouhi S. B. Improved robust DWT-watermarking in YCbCr color space, *Global journal of computer application and technology*, 2011, Vol. 1, Issue 3, pp. 300–304.
- Dey N., Roy A. B., Dey S. A novel approach of color image hiding using RGB color planes and DWT, *International journal of computer application*, 2011, Vol. 36, Issue 5, pp. 19–24.
- Gunjal B. L., Mali S. N. Secured color image watermarking technique in DWT-DCT domain, *International Journal of Computer Science, Engineering and Information Technology (IJCEIT)*, 2011, Vol. 1, Issue 3, pp. 36–44.
- Nance J. Periods of discretized Arnold Cat Map and its extension to dimensions [Jelettronnyj resurs]. Cornell University Library, e-print archive. Rezhim dostupa <http://arxiv.org/abs/1111.2984>. Zagl. s jekrana
- Golyandina N. E., Usevich K. D. 2D-extention of singular spectrum analysis: algorithm and elements of theory, *WORLD SCIENTIFIC*, pp. 449–473. DOI 10.1142/9789812836021_0029
- Bozhokin S. V., Parshin D. A. Fraktaly i mul'tifraktaly: monografija. Izhevsk, NIC, Reguljarnaja i haoticheskaja dinamika, 2001, 128 p.
- Lopes R., Betrouni N. Fractal and multifractal analysis: A review, *Medical Image Analysis*, 2009, Vol. 13, Issue 4, pp. 634–649. DOI 10.1016/j.media.2009.05.003.
- Li J., Du Q., Sun C. An improved box-counting method for image fractal dimension estimation, *Pattern Recognition*, 2009, Vol. 42, Issue 11, pp. 2460–2469. DOI 10.1016/j.patcog.2009.03.001.