

СТІЙКЕ СТЕГАНОПЕРЕТВОРЕННЯ В ПРОСТОРОВІЙ ОБЛАСТІ ЗОБРАЖЕННЯ-КОНТЕЙНЕРА

В.М. Рудницький¹, О.В. Костирка²

¹ Черкаський державний технологічний університет,
бул. Шевченка, 460, Черкаси, 18006, Україна

² Академія пожежної безпеки імені Героїв Чорнобиля ДСНС України,
вул. Онопрієнка, 8, Черкаси, 18034, Україна; e-mail: chaykaov@rambler.ru

У роботі пропонується новий стеганографічний метод, стійкий до збурних дій, який здійснює вбудову додаткової інформації в просторовій області зображення-контейнера. Як збурну дію детально досліджено накладення різних шумів з різними параметрами (гауссівського, мультиплікативного, пуассонівського) на цифрове зображення. В ході дослідження встановлена залежність основного параметра розробленого методу – величини збурення яскравості пікселів блоку контейнера при стеганоперетворенні від розміру блоку.

Ключові слова: стеганографічний метод, цифрове зображення, просторова область зображення, збурна дія, гауссівський шум, мультиплікативний шум, пуассонівський шум

Вступ

Розвиток і вдосконалення комплексної системи захисту інформації сьогодні неможливо без наявності в її складі ефективної стеганографічної системи, що ґрунтується на сучасних стеганографічних алгоритмах [1–3]. Стеганографування може застосовуватися як для прихованої передачі конфіденційних даних, так і для захисту від несанкціонованого використання інформаційного контенту шляхом вбудовування в контейнер цифрових водяних знаків [2]. Найчастіше як контейнер, або основне повідомлення (ОП), сьогодні використовуються цифрові зображення (ЦЗ), файли аудіо й відеоданих [2, 3].

При розробці будь-якого стеганометоду, стеганоалгоритму для прихованої передачі даних до нього висуваються певні вимоги, зокрема:

- 1) стійкості до стеганоаналізу;
- 2) стійкості до різного роду збурних дій,
- 3) забезпечення надійності сприйняття стеганоповідомлення (СП), яке є результатом вбудови додаткової інформації (ДІ) в ОП (ДІ будемо називати результат кодування конфіденційної інформації, що представляє, як правило, бінарну послідовність: $p_1, p_2, \dots, p_t, p_i \in \{0, 1\}, i = \overline{1, t}$);
- 4) забезпечення достатньої прихованої пропускнує спроможності стеганографічного каналу зв'язку, що організується [2];
- 5) малої обчислювальної складності.

У даній роботі як контейнер розглядається ЦЗ.

Вбудова ДІ, або стеганоперетворення (СПР), у загальному випадку може відбуватися як у просторовій області ЦЗ, так і в області перетворення (частотній, області сингулярного розкладання відповідної матриці і т.д.). В [4] показано практично, що просторова область ОП має певні переваги при організації СПР, у порівнянні з областями перетворення контейнера, як з погляду обчислювальної складності

відповідних алгоритмів, так і з погляду обчислювальної похибки, яка впливає на ефективності декодування ДІ. У той же час, в [5, 6] показано, що забезпечення стійкості стеганоалгоритму до збурних дій не залежить безпосередньо від того, у якій області ЦЗ-контейнера відбувається СПР. З врахуванням цього питання розробки стійких до збурних дій стеганометодів і алгоритмів, що працюють у просторовій області ЦЗ-контейнера, є своєчасним і *актуальним*.

Ціль статті й постановка завдань

В [6] отримана достатня умова забезпечення стійкості стеганографічного алгоритму до збурних дій при організації СПР у просторовій області ЦЗ-контейнера, яка зводиться до збурення яскравості пікселів кожного $l \times l$ -блоку B ЦЗ-контейнера, отриманого шляхом стандартної розбивки його матриці на блоки, на значення Δb , при цьому

$$|\Delta b| = \left| \frac{\Delta \sigma_1}{l} \right| > \frac{\|\Delta \bar{B}\|_2}{l}, \quad (1)$$

де

$\Delta \sigma_1$ — збурення максимального сингулярного числа [7] блока B при СПР,
 $\|\Delta \bar{B}\|_2$ — спектральна норма [7] матриці збурення $\Delta \bar{B}$ відповідного блока \bar{B} СП.

Шляхом варіювання величини Δb буде забезпечуватися стійкість стеганоалгоритмів, що розроблятимуться, до різних конкретних збурних дій.

У зв'язку з цим *метою* роботи є розробка нового стійкого до збурних дій стеганометоду, що організує СПР у просторовій області ЦЗ-контейнера на основі отриманої в [6] достатньої умови забезпечення стійкості.

Як збурна дія для конкретного визначення Δb нижче буде розглядатися накладання різних шумів з різними параметрами на ЦЗ.

Для досягнення поставленої мети необхідно розв'язати наступні *задачі*:

1) Отримати оцінки значень $\|\Delta \bar{B}\|_2$ матриці збурення блоку зображення при накладанні різних найбільш часто використовуваних шумів на ЦЗ: гауссівського, мультиплікативного, пуассонівського;

2) Дослідити залежність $\|\Delta \bar{B}\|_2$ від розміру блоку l ;

3) З урахуванням рішень задач 1, 2 визначити можливі значення Δb коректування яскравості пікселів блоку при СПР для різних l ;

4) Отримати рекомендації для розмірів блоку при організації СПР відповідно до отриманої в [6] достатньої умови забезпечення стійкості стеганометоду до збурних дій.

Основна частина

Нехай F, \bar{F} — $m \times m$ -матриці ОП, СП відповідно, p_1, p_2, \dots, p_t — ДІ, $p_i \in \{0, 1\}$, $i = \overline{1, t}$. Декодовану ДІ будемо позначати: $\bar{p}_1, \bar{p}_2, \dots, \bar{p}_t$, де $\bar{p}_i \in \{0, 1\}$, $i = \overline{1, t}$. Для кольорового зображення його формальним представленням буде не одна, а три (чотири) матриці. Однак, з врахуванням того, що вбудова ДІ часто відбувається лише в одну матрицю ЦЗ (при моделі RGB – у синю складову, як правило [2]), представлення ОП, СП у вигляді однієї матриці ніяк не обмежує область застосування запропонованого нижче стеганометоду.

Припустимо, що оцінка $\|\Delta\bar{B}\|_2$ результату передбачуваної збурної дії на блок СП відома. Основні кроки стеганометоду наступні.

Вбудова ДІ.

Крок 1. Матриця F ОП розбивається на $l \times l$ -блоки. Кожний блок контейнера використовується для вбудови $k+1$ ($k \geq 0$) біт ДІ.

Крок 2. (Вбудова ДІ в черговий блок контейнера). Нехай B — черговий блок ОП, що використовується для СПР, а p_i, \dots, p_{i+k} — чергові біти ДІ. Вбудова ДІ проводиться шляхом збурення значень яскравості пікселів блоку B на Δb , що задовольняє (1). Кількість різних варіантів коректування яскравості визначається кількістю S різних варіантів упорядкованих бінарних послідовностей p_i, \dots, p_{i+k} :

$$S = 2^{k+1}. \quad (2)$$

(Наприклад, якщо в блок B контейнера вбудовується один біт ДІ p_i ($k=0$), то кількість різних варіантів бінарної послідовності, яка містить один елемент p_i , відповідно до (2) дорівнює 2. Таким чином, при СПР необхідно забезпечити два можливі варіанти коректування значень яскравості пікселів блоку B . Це можна зробити, наприклад, використовуючи як величини збурення $+\Delta b$, $-\Delta b$). Результат — блок \bar{B} СП \bar{F} .

У результаті пересилання й/або зберігання СП може зазнати збурень, після яких його матриця, у загальному випадку, буде відрізнитися від \bar{F} , а тому далі позначається $\overline{\bar{F}}$.

Декодування ДІ.

Крок 1. Матриці F контейнера в $\overline{\bar{F}}$ можливо збуреного СП розбиваються на $l \times l$ -блоки. Кожний блок СП використовується для декодування $k+1$ ($k \geq 0$) біт ДІ.

Крок 2. Нехай \bar{B} — черговий блок СП, з якого декодуються біти p_i, \dots, p_{i+k} ДІ, а B — відповідний йому блок ОП.

2.1. Визначити:

$$\Delta B = \bar{B} - B.$$

2.2. Визначити по матриці ΔB значення Δb , відповідно до якого цілком декодувати бінарну послідовність p_i, \dots, p_{i+k} .

Конкретний спосіб реалізації кроків 2 при вбудові й декодуванні ДІ буде визначати конкретний стеганоалгоритм, що реалізує метод.

Ключовим моментом у запропонованому стеганометоді є оцінка значення $\|\Delta\bar{B}\|_2$ передбачуваної збурної дії, у якості якої в даній роботі розглядається накладання шуму.

Для рішення цієї задачі в середовищі *MathWorks* MATLAB був проведений обчислювальний експеримент, у якому було задіяно 200 кольорових ЦЗ (модель RGB) у форматах як з втратами (JPEG), так і без втрат (TIF) з бази NRCS [8], а також отримані непрофесійними фотографами. В ході експерименту на ЦЗ накладалися різні шуми (гауссівський, мультиплікативний, пуассонівський) з різними параметрами (варіанти значень параметрів шумів підбиралися, по можливості, так, щоб накладання шуму зберігало/не зберігало надійність сприйняття ЦЗ), після чого зображення аналізувалося. Для цього одна з кольорних матриць зашумленого ЦЗ й відповідна матриця вхідного зображення аналогічним чином розбивалися на $l \times l$ -блоки ($l \in \{4, 8, 10, 12\}$), для кожного з яких визначалася спектральна норма матриці збурення

$\|\Delta\bar{B}\|_2$, що відбулося в результаті накладання шуму. Для кожного i -го ЦЗ, $i = \overline{1, 200}$, для аналізованої колірної матриці обчислювалися: максимальне $M^{(i)}$, мінімальне $m^{(i)}$, середнє $S^{(i)}$ значення $\|\Delta\bar{B}\|_2$ по всіх блоках, а також $PSNR$ — пікове відношення «сигнал-шум», що отримується в децибелах (dB) і є традиційним при оцінці спотворень ЦЗ [9]:

$$PSNR = 10 \cdot \log_{10} \left(255^2 / \left(\frac{1}{m^2} \sum_{i,j} (F(i,j) - (F + \Delta F)(i,j))^2 \right) \right),$$

де $F(i,j), (F + \Delta F)(i,j), i, j = \overline{1, n}$, — значення яскравості пікселів вхідного зображення з матрицею F і зашумленого з матрицею $F + \Delta F$ відповідно. Потім по всіх ЦЗ обчислювалися середні значення $M^{(i)}, m^{(i)}, S^{(i)}$ і $PSNR$. Результати експерименту відображені в табл. 1–3 для гауссівського, мультиплікативного й пуассонівського шумів відповідно.

Необхідно відмітити, що оцінка візуального спотворення ЦЗ за допомогою $PSNR$ в загальному випадку не є придатною для оцінки надійності сприйняття СП у стеганографії, яка носить суб'єктивний характер [10]. Оскільки основною задачею будь-якого стеганометоду є збереження в секреті наявності таємного каналу передачі інформації, що досягається, у тому числі, і за рахунок забезпечення надійності сприйняття СП, у систему стеганографічної передачі даних включається людина, що вносить додаткові, неподоланні до цього моменту труднощі у процес математичної формалізації забезпечення розглянутої вимоги. У силу цього поряд з $PSNR$ оцінка спотворень ЦЗ в роботі проводиться також шляхом суб'єктивного ранжирування, відображенням якого є останні стовпці таблиць 1–3.

Таблиця 1.

Результати накладання на ЦЗ гауссівського шуму з нульовим математичним сподіванням

Дисперсія	l	Середні знач-я по всіх протестованих ЦЗ				Збереження надійності сприйняття
		$M^{(i)}$	$m^{(i)}$	$S^{(i)}$	$PSNR$ (dB)	
0.001	4	46	4	24	30	–
	8	58	21	39		
	10	63	23	44		
	12	67	32	49		
0.0001	4	15	2	8	40	+
	8	19	7	13		
	10	20	8	14		
	12	22	11	16		
0.0005	4	35	3	18	33	±
	8	41	15	27		
	10	45	18	31		
	12	48	23	35		

Таблиця 2.

Результати накладання на ЦЗ мультиплікативного шуму

Дисперсія	l	Середні знач-я по всім протестованим ЦЗ				Збереження надійності сприйняття
		$M^{(i)}$	$m^{(i)}$	$S^{(i)}$	$PSNR$ (dB)	
0.00005	4	8	1	2	49	+
	8	10	1	4		
	10	12	2	5		
	12	13	3	6		
0.0001	4	11	1	3	46	±
	8	15	2	6		
	10	17	2	7		
	12	18	3	8		
0.001	4	35	2	9	37	-
	8	42	4	15		
	10	53	4	17		
	12	57	5	21		

Таблиця 3.

Результати накладання на ЦЗ пуассонівського шуму

l	Середні знач-я по всім протестованим ЦЗ				Збереження надійності сприйняття
	$M^{(i)}$	$m^{(i)}$	$S^{(i)}$	$PSNR$ (dB)	
4	78	4	26	28	-
8	95	14	42		
10	102	16	47		
12	111	19	54		

У ході обчислювального експерименту фіксувалися максимальні значення $\|\Delta\bar{B}\|_2$ при кожному розмірі l блоку для кожного виду розглянутого шуму. Результати знайшли своє відображення на графіках, представлених на рис. 1(а).

Аналіз отриманих результатів (табл. 1–3, рис. 1(а)), на перший погляд, говорять про перевагу блоків малого розміру l для організації СПР відповідно до згаданої вище достатньої умови стійкості стеганометоду, оскільки $\|\Delta\bar{B}\|_2$ для таких блоків має найменше значення. Однак, з врахуванням (1), для стійкості запропонованого стеганометоду до накладання гауссівського/мультиплікативного/пуассонівського шуму з розглянутими варіантами параметрів при $l=4$ має сенс брати $|\Delta b| > \frac{50}{4} / |\Delta b| > \frac{37}{4} / |\Delta b| > \frac{90}{4}$; при $l=8$ – $|\Delta b| > \frac{65}{8} / |\Delta b| > \frac{49}{8} / |\Delta b| > \frac{111}{8}$; при $l=10$ – $|\Delta b| > \frac{69}{10} / |\Delta b| > \frac{56}{10} / |\Delta b| > \frac{116}{10}$; при $l=12$ – $|\Delta b| > \frac{71}{12} / |\Delta b| > \frac{60}{12} / |\Delta b| > \frac{125}{12}$, тобто, наприклад, ті значення, які відображені на рис. 1(б), що, враховуючи необхідність збереження надійності сприйняття СП, надає переваги блокам більшого розміру. Однак, збільшення розміру блоку приведе до зменшення прихованої пропускну здатності стегаграфічного каналу зв'язку, що відповідно з вимогою 4 до стегаалгоритму є небажаним. Таким чином, з врахуванням усього вищесказаного, компромісними варіантами розміру блоку l є величини 8,10.

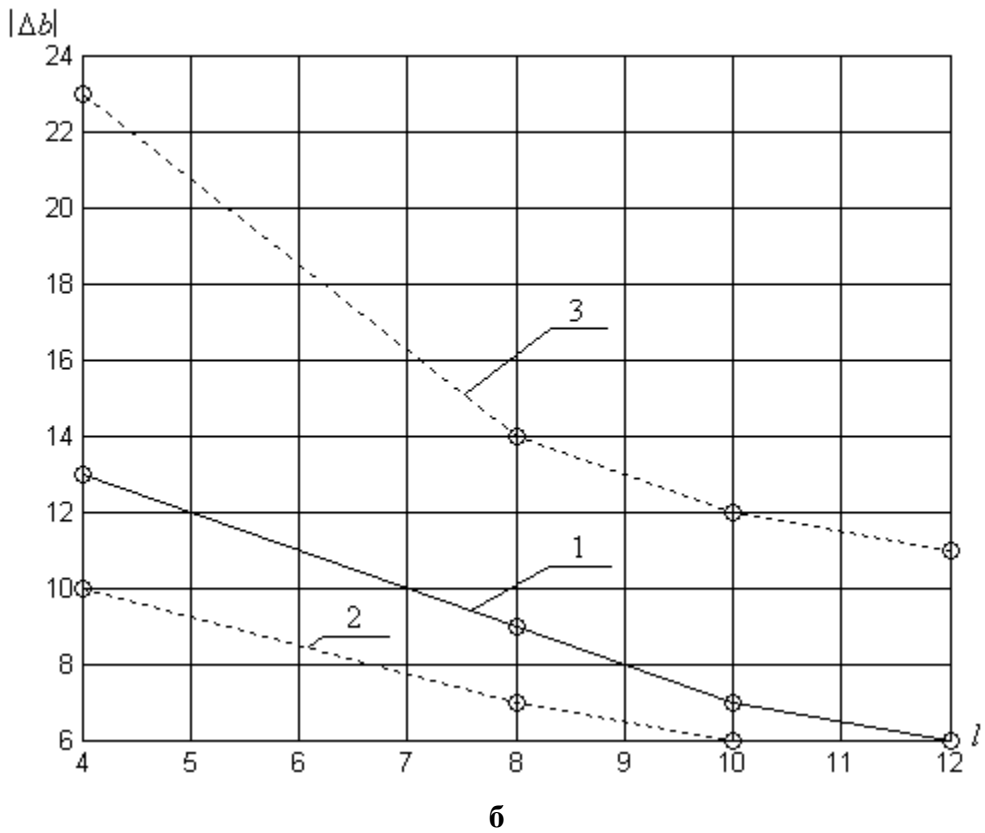
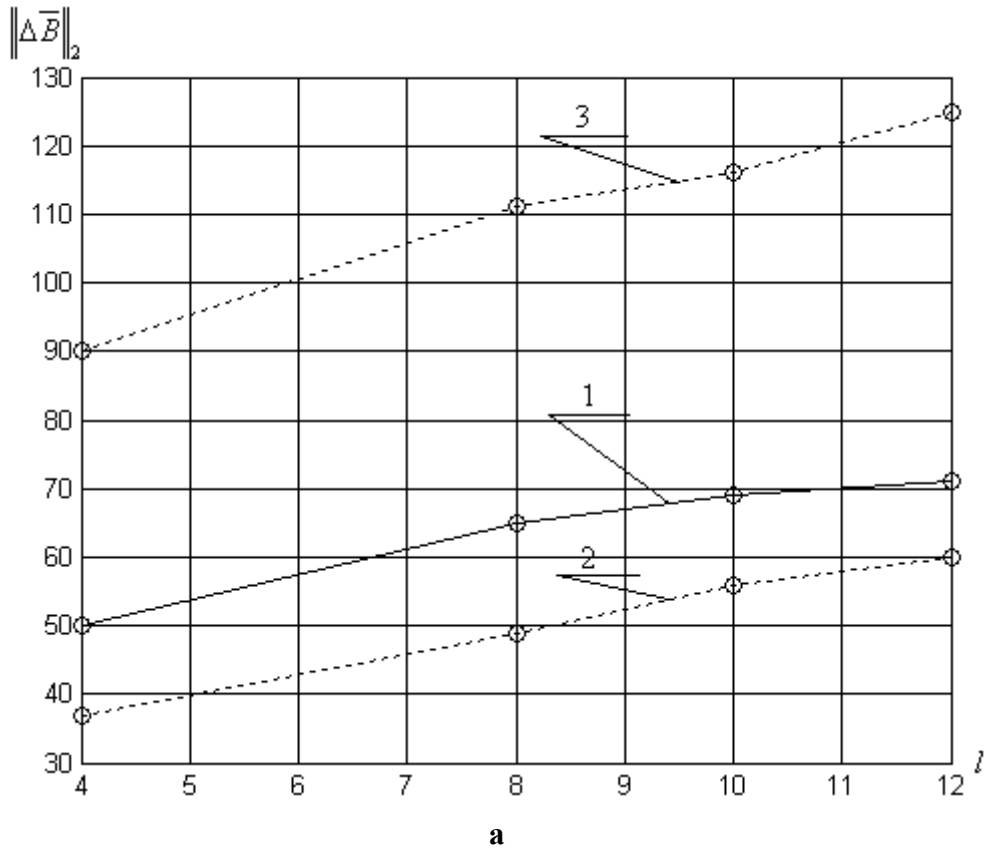


Рис. 1. Залежність від величини l при різних шумах: а – максимального значення, що мало місце в експерименті $\|\Delta \bar{B}\|_2$; б – Δb : 1 – гауссівський; 2 – мультиплікативний; 3 – пуассонівський шум

Висновки

На основі отриманої раніше достатньої умови стійкості в роботі розроблений новий стеганографічний метод, стійкий до збурних дій, що здійснює вбудову додаткової інформації в просторовій області зображення-контейнера шляхом збурення значень яскравості пікселів блоків матриці основного повідомлення.

Як збурна дія, детально досліджене накладення різних шумів з різними параметрами: гауссівського, мультиплікативного, пуассонівського. У ході дослідження встановлена залежність основного параметра розробленого методу – величини Δb збурення яскравості пікселів блоку контейнера при стеганоперетворенні, від розміру l блока.

Отримані рекомендації для величини розміру блоку l , що дозволяють забезпечити: стійкість стеганометоду до накладання шуму; надійність сприйняття формованого стеганоповідомлення; уникнути зменшення прихованої пропускної спроможності стеганографічного каналу зв'язку, що організується, за рахунок величини l .

Список літератури

1. Ленков, С.В. Методы и средства защиты информации: в 2 т. / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. — К.: Арий, 2008 — . — Т.2: Информационная безопасность. — 2008. — 344 с.
2. Грибунин, В.Г. Цифровая стеганография [Текст] : монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М. : СОЛОН-Пресс, 2002. — 272 с.
3. Стеганография, цифровые водяные знаки и стеганоанализ : [монография] / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. — М.: Вузовская книга, 2009. — 220 с.
4. Костырка, О.В. Анализ преимуществ пространственной области цифрового изображения-контейнера для стеганопреобразования / О.В. Костырка // Информатика та математичні методи в моделюванні. — 2013. — Т. 3, № 3. — С. 275–282.
5. Кобозева, А.А. Загальний підхід до оцінки властивостей стеганографічного алгоритму, заснований на теорії збурень / А.А. Кобозева // Інформаційні технології та комп'ютерна інженерія. — 2008. — № 1(11). — С. 164–171.
6. Кобозева, А.А. Условия обеспечения устойчивости стеганоалгоритма при организации стеганопреобразования в пространственной области контейнера-изображения / А.А. Кобозева, О.В. Костырка // Інформаційна безпека. — 2013. — № 4.
7. Деммель, Д. Вычислительная линейная алгебра [Текст] : теория и приложения / Д. Деммель; Пер. с англ. Х.Д. Икрамова. — М. : Мир, 2001. — 430 с.
8. NRCS Photo Gallery : [Електронний ресурс] // United States Department of Agriculture. Washington, USA. Режим доступа: <http://photogallery.nrcs.usda.gov> (Дата зверення: 26.07.2012).
9. Коначович, Г.Ф. Компьютерная стеганография [Текст]: теория и практика / Г.Ф. Коначович, А.Ю. Пузыренко. — Киев : МК-Пресс, 2006. — 288 с.
10. Кобозева, А.А. Учет свойств нормального спектрального разложения матрицы контейнера при обеспечении надежности восприятия стегосообщения / А.А. Кобозева, Е.А. Трифонова // Вестник НТУ «ХПИ». — 2007. — № 18. — С. 81–93.

УСТОЙЧИВОЕ СТЕГАНОПРЕОБРАЗОВАНИЕ В ПРОСТРАНСТВЕННОЙ ОБЛАСТИ ИЗОБРАЖЕНИЯ-КОНТЕЙНЕРА

В.Н. Рудницький¹, О.В. Костырка²

¹ Черкасский государственный технологический университет,
бул. Шевченко, 460, Черкассы, 18006, Украина

² Академия пожарной безопасности имени Героев Чернобыля ГСЧС Украины,
ул. Оноприенко, 8, Черкассы, 18034, Украина; e-mail: chaykaov@rambler.ru

В работе предлагается новый стеганографический метод, устойчивый к возмущающим воздействиям, осуществляющий погружение дополнительной информации в пространственной области изображения-контейнера. В качестве возмущающего воздействия детально исследовано наложение различных шумов с различными параметрами (гауссовского, мультипликативного, пуассоновского) на цифровое изображение, в ходе которого установлена зависимость основного параметра разработанного метода – величины возмущения яркости пикселей блока контейнера при стеганопреобразовании, от размера блока.

Ключевые слова: стеганографический метод, цифровое изображение, пространственная область изображения, возмущающее воздействие, гауссовский шум, мультипликативный шум, пуассоновский шум

ROBUST STEGANO TRANSFORMATION IN SPATIAL DOMAIN OF COVER IMAGE

Volodymyr M. Rudnitsky¹, Olesya V. Kostyrka²

¹ Cherkasy State Technological University,
460 Shevchenko Ave., Cherkasy, 18006, Ukraine

² Academy of Fire Safety named after Chernobyl Heroes,
8 Onoprienko str., Cherkasy, 18034, Ukraine; e-mail: chaykaov@rambler.ru

In this work, a new robust-to-distortion steganography technique ensuring embedding of additional data into the spatial domain of cover image is proposed. As a distortion, investigated was addition of various (Gaussian, multiplicative and Poisson) noises with different parameter values to digital image. Within this investigation, a relationship between the main parameter of the technique developed, the value of brightness distortion of cover block pixel during stego transformation, and the block size, was established.

Keywords: steganographic method, digital image, spatial domain, disturbance, Gaussian noise, speckle noise, Poisson noise