© Kostyrka O. Steganographic algorithm robust against noise imposition // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 1, p. 71-75.

СТЕГАНОГРАФІЧНИЙ АЛГОРИТМ, СТІЙКИЙ ДО НАКЛАДАННЯ ШУМУ

Олеся Костирка

Академія пожежної безпеки ім. Героїв Чорнобиля, Україна

КОСТИРКА Олеся Вікторівна

Рік та місце народження: 1990 рік, м. Черкаси, Україна.
Освіта: Академія пожежної безпеки ім. Героїв Чорнобиля, 2012 рік.
Посада: аспірант.
Наукові інтереси: інформаційна безпека, стеганографія.
Публікації: 6 наукових публікацій.
E-mail: chaykaov@rambler.ru

Анотація. *У роботі розроблений новий стеганографічний алгоритм, що здійснює вбудову додаткової інформації в просторовій області контейнера-зображення. Алгоритм є стійким до накладання різних шумів, найчастіше використовуваних при моделюванні активних атакуючих дій; він забезпечує надійність сприйняття стеганоповідомлення, є поліноміальним ступеня 2. Показано, що характеристика стійкості алгоритму (яка оцінюється нормованим коефіцієнтом кореляції для вбудованої додаткової інформації) не залежить від виду шуму, що накладається на стеганоповідомлення, а визначається величиною збурної дії, що зазнає матриця стеганоповідомлення під час атаки. В роботі наведено результати обчислювальних експериментів, рекомендації з області застосування розробленого алгоритму; проведено порівняльний аналіз ефективності нового алгоритму з сучасними аналогами.*

Ключові слова: *стеганоалгоритм, просторова область стеганоперетворення, зображення-контейнер, накладання шуму, надійність сприйняття, стійкість до збурних дій.*

Вступ

Захист інформації в сучасних умовах стає все більш актуальною проблемою, що обумовлено рядом обставин, основними з яких є [1]:

– масове поширення засобів електронної обчислювальної техніки;

– стрімке проникнення інформаційних технологій в усі сфери діяльності людини;

– з'явлення нових каналів передачі й, як наслідок, витоку інформації;

– поширення можливостей несанкціонованих дій над інформацією.

Етап свого ефективного розвитку сьогодні переживає стеганографія, методи якої є обов'язковою складовою частиною будь-якої комплексної системи захисту інформації [1].

Розробка стеганографічних алгоритмів завжди проводиться з врахуванням основних вимог, серед яких важливу роль відіграє вимога стійкості алгоритму до збурних дій. Така стійкість необхідно повинна супроводжуватися забезпеченням надійності сприйняття відповідного стеганоповідомлення (СП). Враховуючи те, що особливістю сьогоднішньої стеганографії є її «комп'ютерний характер», велике значення набуває забезпечення малої обчислювальної складності стеганоалгоритмів, а також контроль нагромадження обчислювальної похибки при організації вбудови/декодування додаткової інформації (ДІ).

Як контейнер, або основне повідомлення (ОП), завдяки об'єктивним причинам [2,3] часто використовуються цифрові зображення (ЦЗ) (що робиться й у даній роботі), цифрові відео, аудіо.

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.). Однак, враховуючи вищесказане, а також результати, отримані в [4], де показано, що просторова область ОП має ряд переваг при організації СПр, у порівнянні з областями перетворення контейнера, як з погляду обчислювальної складності відповідних алгоритмів, так і з погляду обчислювальної похибки, можна стверджувати, що питання розробки стійких стеганометодів і алгоритмів, що працюють у просторовій області ЦЗ-контейнера, є *актуальним*.

Аналіз існуючих досліджень

В [5] розроблений новий стеганографічний метод, стійкий до збурних дій, що здійснює вбудову ДІ в просторовій області зображення-контейнера. Як збурна дія детально досліджене накладання різних шумів з різними параметрами: гауссівського, мультиплікативного, пуассонівського.

Метою роботи є розробка поліноміального стеганоалгоритму, що реалізує запропонований в [5] метод, стійкого до накладання шуму, що забезпечує надійність сприйняття СП.

Стеганометод, розроблений в [5], базується на отриманій в [6] достатній умові забезпечення стійкості стеганографічного алгоритму до збурних дій при організації СПр у просторовій області ЦЗ-контейнера, яке зводиться до коректування яскравості пікселів на значення Δb кожного $l \times l -$ блоку B ЦЗ-контейнера, після стандартної розбивки його матриці. При цьому

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

де $\Delta\sigma_1$ - збурення максимального сингулярного числа блоку B при СПр, а $\left\|\Delta\overline{B}\right\|_2$ - спектральна норма матриці збурення блоку СП. З врахуванням цього для досягнення поставленої мети роботи необхідно розв'язати наступні *задачі*:

1. Визначити розмір блоків l, на які розбивається матриця ОП при СПр, що дозволяє забезпечити: стійкість стеганоалгоритму до накладання шуму; надійність сприйняття стеганоповідомлення; уникнути зменшення прихованої пропускної спроможності відповідного стеганографічного каналу зв'язку за рахунок величини l;

2. Визначити конкретне значення Δb з урахуванням обраного розміру блоку l і отриманої оцінки збурення блоку СП $\left\|\Delta\overline{B}\right\|_2$;

3. Розробити стеганоалгоритм, що реалізує метод з [5];

4. Оцінити обчислювальну складність розробленого стеганоалгоритму;

5. Дослідити ефективність розробленого стеганоалгоритму в умовах накладання шуму;

6. Провести порівняння ефективності розробленого методу із сучасними аналогами.

Основна частина дослідження

Величина розміру блоку l є суттєвою при організації СПр розглянутим методом. Аналіз отриманих в [5] результатів, на перший погляд, говорить про перевагу блоків малого розміру l, оскільки $\left\|\Delta\overline{B}\right\|_2$ для таких блоків має найменше значення [5]. З врахуванням (1), для стійкості стеганометоду до накладання гауссівського/ мультиплікативного/пуассонівського шуму при $l = 4$ пропонується брати $|\Delta b| = 13$ / $|\Delta b| = 10$ / $|\Delta b| = 23$; при $l = 8$ - $|\Delta b| = 9$ / $|\Delta b| = 7$ / $|\Delta b| = 14$; при $l = 10$ - $|\Delta b| = 7$ / $|\Delta b| = 6$ / $|\Delta b| = 12$; при $l = 12$ - $|\Delta b| = 6$ / $|\Delta b| = 6$ / $|\Delta b| = 11$. Це, враховуючи необхідність забезпечення надійності сприйняття СП, надає перевагу блокам більшого розміру. Однак, збільшення розміру блоку приведе до зменшення прихованої пропускної спроможності [2] відповідного стеганографічного каналу зв'язку, що є небажаним. Таким чином, з врахуванням усього вищесказаного, компромісними варіантами розміру блоку l є величини 8,10. Беручи до уваги розміри блоків при стандартній розбивці матриці ЦЗ [7], а також перспективи адаптації розробленого алгоритму для задовільнення умові стійкості до стиску, покладемо скрізь нижче $l = 8$.

Нехай F, $\overline{F}$ - $m \times m -$ матриці ОП, СП відповідно, $p_1, p_2, ..., p_t$ - ДІ, $p_i \in \{0,1\}, i = \overline{1,t}$. Декодовану ДІ будемо позначати: $\overline{p}_1, \overline{p}_2, ..., \overline{p}_t$, де $\overline{p}_i \in \{0,1\}, i = \overline{1,t}$.

Для оцінки $\left\|\Delta\overline{B}\right\|_2$ результату передбачуваної збурної дії на блок СП будемо, в основному, орієнтуватися на дослідження результатів [5] накладання гауссівського шуму, оскільки найчастіше моделювання різних активних дій на СП відбувається шляхом накладання саме цього шуму [8]. У зв'язку із цим покладемо $\Delta b = 9$.

Основні кроки алгоритму, що називається далі SS_noise, виглядають наступним чином.

Вбудова ДІ.

1. Матриця F ЦЗ-контейнера розбивається стандартним чином на $8 \times 8 -$ блоки.

2. (*Вбудова ДІ – реалізація двох різних варіантів коректування значень яскравості пікселів блоку* B). Нехай B – черговий блок ОП, що використовується для СПр, а p_i – черговий біт ДІ, $\overline{B}$ - відповідний блок стеганоповідомлення.

Якщо $p_i = 1$
то $\overline{B} = B + \Delta b \cdot \overline{E}$
інакше $\overline{B} = B - \Delta b \cdot \overline{E}$,

де $\overline{E}$ - $8 \times 8 -$ матриця, всі елементи якої дорівнюють 1.

Декодування ДІ

1. Матриці F контейнера і $\overline{\overline{F}}$ можливо збуреного СП розбиваються на $8 \times 8 -$ блоки. Кожний блок СП використовується для декодування 1 біта ДІ.

2. Нехай $\overline{\overline{B}}$ – черговий блок СП, з якого декодується біт $\overline{p}_i$ ДІ, а B - відповідний йому блок ОП.

2.1. Визначити: $\Delta B = \overline{\overline{B}} - B$.

2.2. Визначити кількості додатних k_p і від'ємних k_n елементів в матриці ΔB.

Якщо $k_p > k_n$,
то $\overline{p}_i = 1$,
інакше $\overline{p}_i = 0$.

Зауваження 1. Реалізація процесів СПр і декодування в SS_noise відбувається в припущенні, що формальним представленням ЦЗ-контейнера є одна матриця (що має місце в випадку зображення в градаціях сірого). Це ніяк не обмежує область застосування розробленого алгоритму: якщо як ОП використовується кольорове зображення, то алгоритм, по-перше, може застосовуватися для вбудови ДІ лише в одну із множини матриць, що

використовуються для представлення ЦЗ; по-друге, він може застосовуватися для кожної з матриць окремо.

Зауваження 2. При розробці стеганоалгоритму реалізація двох різних варіантів коректування значень яскравості пікселів блоку B при СПр може бути реалізована шляхом тільки збільшення/зменшення значень яскравості. У цьому випадку для організації ефективного декодування ДІ значення Δb_1 і Δb_2 - двох варіантів коректування повинні задовольняти співвідношенням:

$$\begin{cases} |\Delta b_1| \geq |\Delta b|, \\ |\Delta b_1 - \Delta b_2| \geq |\Delta b|' \end{cases}$$

де Δb визначається відповідно до (10).

Зауваження 3. Обчислювальна складність стеганоалгоритму SS_noise визначається кількістю блоків, на які розбивається матриця контейнера/стеганоновідомлення, і становить

$$\left[\frac{m}{8}\right]\left[\frac{m}{8}\right] = \underline{O}\left(m^2\right) \qquad (2)$$

операцій, де $[\bullet]$ - ціла частина аргументу.

Для перевірки ефективності розробленого стеганоалгоритму в середовищі Matlab був проведений обчислювальний експеримент, у якому було задіяні 200 ЦЗ-контейнерів розміром 1000×1000 пікселів (колірна схема RGB) у форматах як з втратами (Jpeg), так і без втрат (Tif) з бази NRCS [9] (яка є традиційною для тестування алгоритмів, що працюють із ЦЗ), а також зображення, отримані непрофесійними фотографами.

Традиційним при оцінці спотворень ЦЗ при різних збуреннях є значення пікового відношення «сигнал-шум» ($PSNR$), що отримується в децибелах (dB) [10]:

$$PSNR = 10 \cdot \log_{10}\left(255^2 \Big/ \left(\frac{1}{m^2}\sum_{i,j}\left(F(i,j) - (F+\Delta F)(i,j)\right)^2\right)\right), \qquad (3)$$

де $F(i,j), (F+\Delta F)(i,j),\ i,j = \overline{1,m}$, – значення яскравості пікселів вхідного зображення з матрицею F і збуреного з матрицею $F + \Delta F$ відповідно. У випадку кольорового ЦЗ для обчислення $PSNR$ зображення переводиться в колірну схему YCbCr, де аналізується одна матриця Y – матриця яскравості [11].

Однак (3) не завжди є придатною для оцінки надійності сприйняття СП у стеганографії, яка носить суб'єктивний характер [12]. Оскільки основною задачею будь-якого стеганоалгоритму є збереження в секреті наявності таємного каналу передачі інформації, що досягається, у тому числі, і за рахунок забезпечення надійності сприйняття стеганоповідомлення, у систему стеганографічної передачі даних включається людина, що вносить додаткові, неподоланні до цього моменту труднощі у процес математичної формалізації забезпечення розглянутої вимоги, хоча робота в цьому напрямку ведеться дуже активно, із залученням великого математичного апарата [12]. Тому ступінь забезпечення надійності сприйняття СП у стеганографії часто оцінюється разом з $PSNR$ також і за допомогою суб'єктивного ранжирування, що робиться і в даній роботі.

У ході обчислювального експерименту в синю складову ЦЗ вбудовувалася ДІ, після чого СП зберігалося у форматі без втрат (Tif). $PSNR$, що відображає спотворення ОП у процесі СПр, дорівнював тут у середньому 49 dB незалежно від формату контейнера, що розглядається в літературних джерелах як значення, яке характеризує прийнятну якість ЦЗ [10]. Суб'єктивним ранжируванням було встановлено дотримання надійності сприйняття СП, сформованих розробленим алгоритмом для 98.3% ЦЗ, підданих тестуванню. В 1.7% ЦЗ (ці зображення мали значні фонові області) спостерігалося виникнення артефактів на фонових областях, хоча $PSNR$ для них також мав прийнятне значення. Таким чином, рекомендується не використовувати подібні ЦЗ як контейнери для SS_noise.

Збурні дії на СП моделювалися в середовищі Matlab шляхом накладання на них різних шумів: гауссівського, мультиплікативного, пуассонівського з різними параметрами. Збурене СП зберігалося у форматі без втрат (Tif). Необхідно відзначити, що хоча для повноти експерименту шуми бралися різні, але, виходячи з основної ідеї організації СПр, ще на етапі теоретичної розробки можна було припустити, що ефективність алгоритму не буде залежати від характеру шуму, а буде визначатися, головним чином, величиною збурної дії, оцінюваної значенням $PSNR$, що й буде практично підтверджене нижче.

Результати декодування ДІ, що говорять про високу абсолютну ефективність розробленого алгоритму незалежно від формату контейнера (із втратами, без втрат), представлені в табл.1-3 ($PSNR$ тут відображає спотворення СП при накладанні шуму). Ефективність роботи стеганоалгоритму оцінювалася стандартним чином за значенням коефіцієнта кореляції (NC) для ДІ [13]:

$$NC = \left(\sum_{i=1}^{t} p_i' \times \overline{p}_i'\right) \Big/ t,$$

де $p_i' = 1, \overline{p}_i' = 1$, якщо $p_i = 1, \overline{p}_i = 1$, і $p_i' = -1, \overline{p}_i' = -1$, якщо $p_i = 0, \overline{p}_i = 0$.

Таблиця 1

Результати декодування ДІ при накладанні на СП гауссівського шуму з нульовим математичним очікуванням і дисперсією D

Дисперсія	$D = 0.0005$	$D = 0.001$	$D = 0.005$	$D = 0.01$	$D = 0.1$
NC	0.994	0.993	0.988	0.962	0.524
$PSNR$ (dB)	38	35	28	25	16

Результати декодування ДІ при накладанні на СП мультиплікативного шуму Таблиця 2

Дисперсія	$D = 0.0001$	$D = 0.001$	$D = 0.01$	$D = 0.08$	$D = 0.5$
NC	0.995	0.993	0.977	0.822	0.548
PSNR (dB)	49	41	25	24	15

Таблиця 3

Результати декодування ДІ при накладанні на СП пуассонівського шуму

NC	*PSNR* (dB)
0.992	32

Представлення результатів експерименту у вигляді графіків залежності *NC* від *PSNR* (рис.2) для різних шумів наочно підтверджує, що ефективність *SS_noise*, як і передбачалося вище, визначається величиною спотворення ЦЗ, а не характером накладеного на СП шуму (зауважимо, що для пуассонівського шуму значення $NC = 0.992$ для $PSNR = 32\ dB$ (табл.3) також знаходиться у відповідній області графіків на рис.2).

Для порівняльної оцінки ефективності розробленого алгоритму був обраний один з найбільш ефективних сучасних аналогів, представлений в [14] (відзначимо, що він здійснює вбудову ДІ в області перетворення контейнера). Результати порівняння, відображені на рис.3, показують, що розроблений алгоритм *SS_noise* незначно уступає аналогу лише для мультиплікативного шуму з дисперсією $D = 0.08$, при цьому значно перевершуючи у всіх інших випадках (особливо для гауссівського шуму). Крім того, автори [14] взагалі не аналізували свій продукт для значущих дисперсій шуму, що змушує припустити, що для цих випадків їх алгоритм є неспроможним, чого не можна сказати про *SS_noise*.

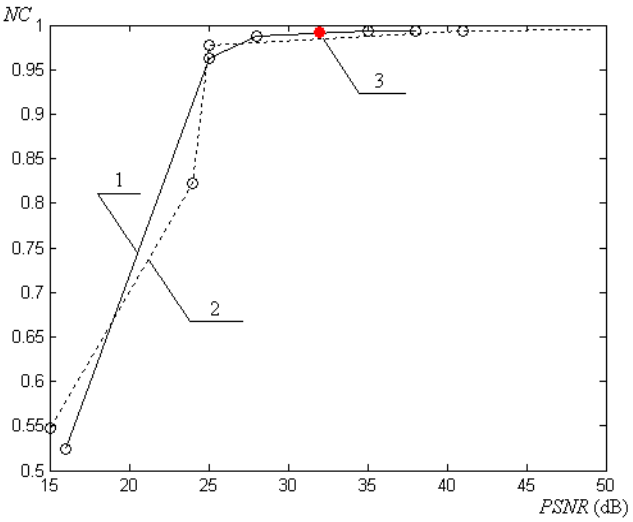

Рис.2. Залежність *NC* від величини *PSNR* спотворення СП, сформованого *SS_noise*, при накладанні шуму: 1 – гауссівського; 2 – мультиплікативного; 3 – пуассонівського

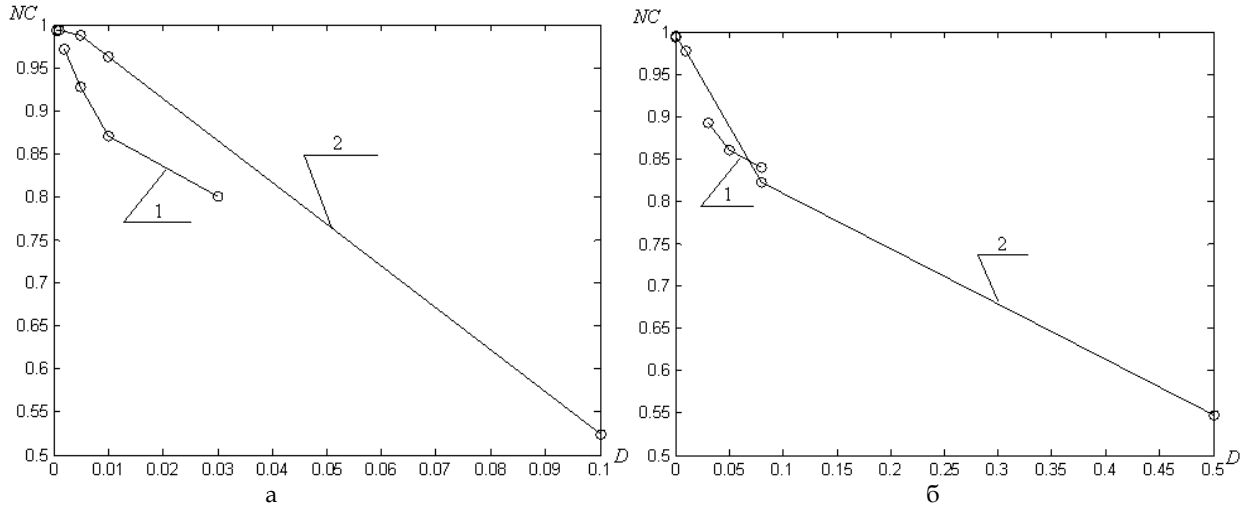

Рис.3. Залежність *NC* від дисперсії шуму, що накладається на СП: а - гауссівського; б - мультиплікативного: 1 – стеганоалгоритм з [14]; 2 – *SS_noise*

Таким чином, проведений обчислювальний експеримент практично підтверджує високу ефективність розробленого стеганоалгоритму, як абсолютну, так і відносну.

Висновки

У роботі розроблений новий стеганографічний алгоритм *SS_noise*, що реалізує стеганометод, запропонований в [5]. Розроблений алгоритм задовольняє усім висунутим до нього вимогам:

– здійснює вбудову ДІ в просторовій області контейнера;

– є стійким до накладання шуму, до того ж характеристика цієї стійкості (значення *NC*) не залежить від виду шуму, а залежить, головним чином, від величини збурної дії, викликаної його накладанням (і вимірюваної за допомогою *PSNR*);

– забезпечує прийнятну якість СП (у результаті СПр $PSNR \approx 49\ dB$ незалежно від формату контейнера);

– є поліноміальним ступеня 2 (див. (2)).

Виходячи з результатів обчислювального експерименту, не рекомендується використовувати як контейнер ЦЗ з великими фоновими областями, оскільки в цьому випадку можливе виникнення артефактів у результаті стеганоперетворення.

Література

[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 // Інформатика та математичні методи в моделюванні. — 2013. — Т. 3, № 3. — С. 275-282.

[5] Рудницький В.М. Стійке стеганоперетворення в просторовій області зображення-контейнера / В.М.Рудницький, О.В.Костирка // Інформатика та математичні методи в моделюванні. — 2013. — Т.3, №4. — С. 320-327.

[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. — С. 57-65.

[7] Гонсалес Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. П.А. Чочиа. — М.: Техносфера, 2006. — 1070 с.

[8] Gkizeli M. Optimal Signature Design for Spread-Spectrum Steganography / M. Gkizeli, D.A. Pados, M.J. Medley // IEEE Trans. On Image Processing. — 2007. — Vol.16, № 2. — P. 1021-1031.

[9] NRCS Photo Gallery: [Електронний ресурс] // US Department of Agriculture. Washington, USA. Режим доступу: http://photogallery.nrcs.usda.gov (Дата звернення: 26.07.2012).

[10] Конахович Г.Ф. Компьютерная стеганография [Текст]: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. — К.: МК-Пресс, 2006. — 288 с.

[11] PSNR: [Електронний ресурс] // Math Works. Docum. Center. The MathWorks, Inc. USA. Режим доступу: http://www.mathworks.com/help/vision/ref/psnr.html (Дата звернення: 26.07.2012).

[12] 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.

[13] Lin W.-H. A blind watermarking method using maximum wavelet coefficient quantization / W.-H. Lin et al // Expert Systems with Applications. — 2009. — Vol. 36, Iss. 9. — PP. 11509-11516.

[14] Perwej Y. Copyright protection of digital images using robust watermarking based on joint DLT and DWT / Y. Perwej, F. Perwej, A. Perwej // International Journal of Scientific & Engineering Research. — 2012. — Vol. 3, Iss. 6. — PP. 1–9.

УДК 004.056.5 (045)

Костырка О.В. Стеганографический алгоритм, устойчивый к наложению шума

Аннотация. *В работе разработан новый стеганографический алгоритм, осуществляющий погружение дополнительной информации в пространственной области контейнера-изображения. Алгоритм является устойчивым к наложению различных шумов, наиболее часто используемых при моделировании активных атакующих действий; он обеспечивает соблюдение надежности восприятия стеганосообщения, является полиномиальным степени 2. Показано, что характеристика устойчивости алгоритма (нормированный коэффициент корреляции для погруженной дополнительной информации) не зависит от вида накладываемого на стеганосообщение шума, а определяется только величиной возмущающего воздействия. Даны рекомендации по области применения разработанного алгоритма.*

Ключевые слова: *стеганоалгоритм, пространственная область стеганопреобразования, изображение-контейнер, наложение шума, надежность восприятия, устойчивость к возмущающим воздействиям.*

Kostyrka O. Steganographic algorithm robust against noise imposition

Abstract. *The works devoted to development of new steganographic algorithm that worked in spatial domain of cover-image. Proposed algorithm is robust to noise such as Gaussian, Poisson and Speckle. Proposed algorithm enforces reliability perception of stegomessage, and is a polynomial of degree 2. It is shown that the stability characteristics of the algorithm (normalized correlation coefficient for embedded information) does not depend on the type of noise and is determined only by the disturbing effect, which is evaluated in the standard way with a peak signal-to-noise ratio. Characteristics of the algorithm does not depend on the image format. Recommendations on the application of the algorithm are given.*

Key words: *steganographic algorithm, spatial domain, cover-image, noise, reliability of perception, robustness to disturbing.*

Отримано *20 лютого 2014 року*, затверджено редколегією *17 березня 2014 року*