УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 6 (2016), No. 1, pp. 85-93

МОДИФІКАЦІЯ СТІЙКОГО ДО ЗБУРНИХ ДІЙ СТЕГАНОПЕРЕТВОРЕННЯ ПРОСТОРОВОЇ ОБЛАСТІ ЗОБРАЖЕННЯ-КОНТЕЙНЕРА

О.В. Костирка

Черкаський інститут пожежної безпеки ім. Героїв Чорнобиля Національного університету цивільного захисту України,
вул. Онопрієнка, 8, Черкаси, 18034, Україна; e-mail: chaykaov@rambler.ru

В роботі запропоновано модифікацію стійкого до атак проти вбудованого повідомлення стеганографічного методу, розробленого автором раніше, який здійснює стеганоперетворення в просторовій області контейнера-зображення, але має обмеження області застосування завдяки можливості порушення надійності сприйняття зображення в результаті вбудови додаткової інформації. Результатом модифікації є усунення будь-яких обмежень на область застосування відповідного алгоритму шляхом забезпечення надійності сприйняття формованого стеганоповідомлення незалежно від специфіки зображення-контейнера. Стійкість алгоритму, що реалізує модифікований метод, до атак проти вбудованого повідомлення при цьому знижується незначно. Як збурні дії розглянуто: накладання на стеганоповідомлення різних шумів з різними параметрами, фільтрація, стиск стеганоповідомлення з втратами з різними коефіцієнтами якості (збереження в формати Jpeg, Jpeg2000). Наведені результати обчислювального експерименту.

Ключові слова: стеганографічний алгоритм, цифрове зображення, просторова область контейнера, надійність сприйняття стеганоповідомлення, стійкість до атак проти вбудованого повідомлення

Вступ

При розробці нових і вдосконаленні існуючих стеганографічних алгоритмів (СА), що використовуються при організації прихованого каналу зв'язку, гостро встають питання забезпечення ними різних вимог, серед яких одною з основних, але не вирішених до кінця залишається задача забезпечення стійкості алгоритму до різних збурних дій — атак проти вбудованого повідомлення [1,2]. До таких атак відносяться, зокрема, накладання різних шумів на стеганоповідомлення (СП), що є результатом вбудови додаткової інформації (ДІ) в контейнер, фільтрація, стиск СП із втратами та ін.

Протягом привалого часу вважалося, що для забезпечення стійкості СА кращою для вбудови ДІ є область перетворення контейнера, в якості якого далі розглядається цифрове зображення (ЦЗ), зокрема, частотна область [3,4]. Завдяки цьому розробки стійких стеганоалгоритмів у просторовій області (ПО) ЦЗ були нечисленними, безсистемними, не мали потрібного математичного фундаменту [5,6].

У результаті сучасних наукових досліджень було показано, що забезпечення стійкості СА не залежить прямо від того, у якій області контейнера — просторовій або перетворення відбувається вбудова ДІ [7,8]. При цьому просторова область ЦЗ має значні переваги перед областями перетворень для організації стеганоперетворення [9]. В [8,10,11] був розроблений стеганографічний метод і реалізуючий його поліноміальний СА, стійкість до атак проти вбудованого повідомлення якого перевищує стійкість сучасних аналогів. Однак недоліком методу і відповідного

алгоритму є можливість порушення надійності сприйняття формованого СП в тому випадку, коли ЦЗ-контейнер має значні по розмірі фонові області, що звужує область його застосування.

Мета статті і постановка досліджень

Метою роботи є модифікація розробленого в [8,10,11] стійкого стеганографічного методу, що здійснює стеганоперетворення в просторовій області контейнера, яка дозволить усунути будь-які обмеження на область застосування модифікованого методу шляхом забезпечення надійність сприйняття формованого їм стеганоповідомлення незалежно від специфіки зображення-контейнера, не знижуючи при цьому значимо його стійкість до атак проти вбудованого повідомлення.

Для досягнення поставленої мети в роботі потрібно вирішити наступні *задачі*:

1. Забезпечити зменшення стрибка функції яскравості пікселів на границі блоків матриці ЦЗ-контейнера при вбудові ДІ за рахунок зміни виду матриці збурення блоку контейнера при стеганоперетворенні;
2. Визначити розміри складових частин матриці збурення блоку контейнера при стеганоперетворенні таким чином, щоб вона забезпечувала найкраще співвідношення між кількісними показниками спотворення контейнера в результаті вбудови ДІ й стійкості відповідного алгоритму до збурних дій;
3. Провести порівняльний аналіз властивостей стеганоалгоритмів, що реалізують модифікований метод, і базового алгоритму.

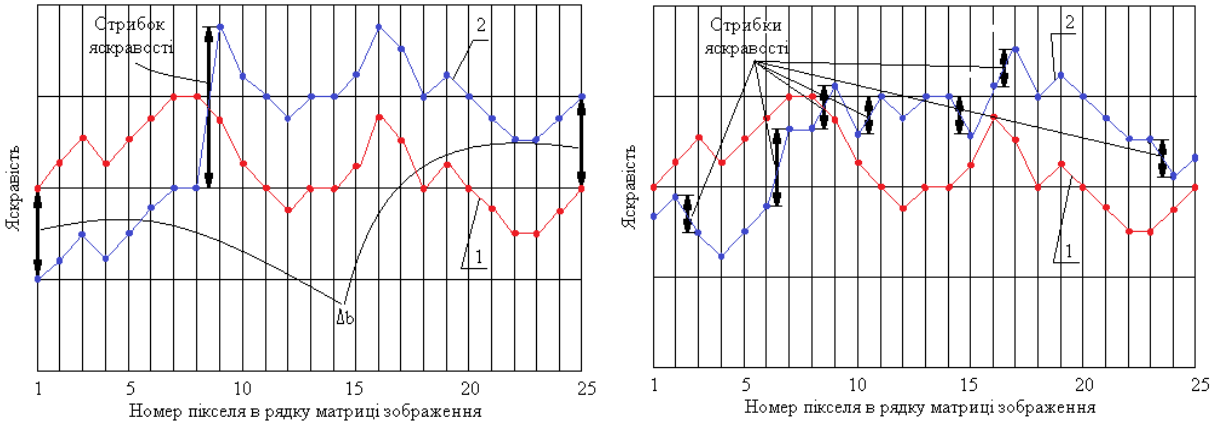
Основна частина

Нехай F, $\overline{F}$ — $m\times m-$матриці контейнера, СП відповідно, $p_1, p_2,..., p_t$, $p_i \in \{0,1\}, i=\overline{1,t}$, - бінарна послідовність, яка є результатом кодування пересилаємої інформації, що розглядається як ДІ. Зауважимо, що хоча для кольорового ЦЗ його формальним представленням в різних схемах буде 3 або 4 двовимірні матриці, запропонована формалізація у вигляді одної матриці не обмежує спільність подальших міркувань, оскільки, по-перше, всі ці міркування можуть бути застосовані для кожної з матриць, по-друге, для збільшення ймовірності збереження прихованості стеганографічного каналу звязку при стеганоперетворенні кольорового зображення-контейнера часто використовується лише одна його кольорова складова.

Основним недоліком розробленого автором раніше стійкого стеганографічного методу SA_B [10], що використовується для організації прихованого каналу зв'язку, є обмеження області його застосовності: на фонових ділянках, при їх наявності в зображенні-контейнері, завдяки перепаду значень яскравості пікселів на границі блоків, що використовуються при стеганоперетворенні за допомогою SA_B, виникають артефакти. Звичайно такі області контейнера можна не задіювати в процесі вбудови ДІ, що дасть можливість уникнути порушення надійності сприйняття зображення-стеганоповідомлення, але приведе до зменшення пропускної спроможності прихованого каналу зв'язку, що організується за допомогою даного стеганометода, що є вкрай небажаним.

В ході стеганоперетворення методом SA_B $m\times m-$матриця F ЦЗ розбивається стандартним чином [12] на $l\times l-$блоки B (в алгоритмічній реалізації SA_B $l=8$, що обгрунтовано в [10,11]). В один блок відбувається вбудова одного біта ДІ шляхом збільшення/зменшення всіх значень яскравості пікселів блоку на одне й те саме значення Δb (в алгоритмічній реалізації SA_B $\Delta b=9$ [10]), що може бути представлене

в матричному виді наступним чином: $\overline{B} = B \pm \Delta B$, де $\overline{B}$ - відповідний блок СП, а ΔB - $l \times l$ – матриця, всі елементи якої дорівнюють Δb. В результаті можливий значний перепад яскравості на спільній границі блоків, що знаходяться поряд і використовуються в процесі стеганоперетворення. Це відбувається тоді, коли в них вбудовуються різні за значенням біти ДІ (див. рис.1(а)). Стрибок функції яскравості пікселів, що відбувається, за значенням порівнянний з $2\Delta b$, і викликає появу артефактів на ЦЗ-стеганоповідомленні, що формується SA_B. Щоб запобігти можливості виникнення таких артефактів, треба зменшити цей перепад значень функції яскравості.



а **б**

Рис. 1. Графіки залежності значення яскравості пікселя від його номера в рядку ЦЗ: 1 – для ЦЗ-контейнера; 2 – для СП; а – СП, яке сформоване базовим стеганометодом SA_B; б – СП, яке сформоване з використанням ΔB^M

Для цього змінимо вид $l \times l$ – матриці ΔB наступним чином. Розіб'ємо ΔB на 2 ділянки, як пропонує рис.2. Модифіковану матрицю будемо позначати ΔB^M. При цьому елементи внутрішньої частини матриці збурення блоку контейнера при стеганоперетворенні, що позначимо ΔB_h, будуть залишатися рівними Δb, а елементи зовнішньої області будуть визначатися як $\Delta b/3$ (чи $[\Delta b/3]$ в випадку, коли Δb не є кратним трьом). Таке рішення приймається в силу наступних обставин. При запропонованих змінах матриці ΔB хоча стрибків функції яскравості буде більше, але всі вони не будуть перевищувати Δb (рис.1(б)). Це буде сприяти зменшенню спотворення ЦЗ в процесі стеганоперетворення.

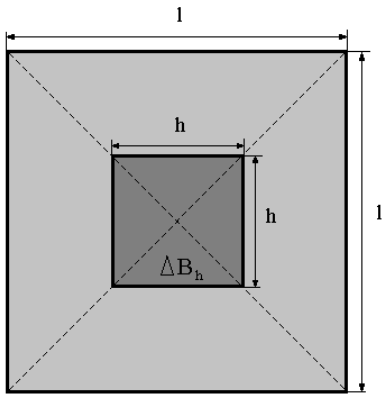


Рис. 2. Розбиття $l \times l$ – матриці збурення блоку ΔB при стеганоперетворенні на 2 ділянки

Основні кроки пропонуємої модифікації стеганографічного методу SA_B, яка далі позначається $SA_B^{(M)}$, виглядають наступним чином.

Вбудова ДІ.

1. Матрицю F ЦЗ-контейнера розбити стандартним чином на $l \times l$ – блоки.

2. Побудувати матрицю ΔB^M.

3. Нехай B — черговий блок контейнеру, що використовується для стеганоперетворення, а p_i — черговий біт ДІ, $\overline{B}$ — відповідний блок СП.

Якщо $p_i = 1$

то $\overline{B} = B + \Delta B^M$

інакше $\overline{B} = B - \Delta B^M$.

Результат – матриця $\overline{F}$ стеганоповідомлення.

Декодування ДІ

1. Матриці F контейнера і $\overline{\overline{F}}$ можливо зміненого в процесі пересилання стеганоповідомлення розбиваються стандартним чином на непересічні $l \times l$ – блоки.

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

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

2.2. Визначити кількості додатних k_p і від'ємних k_n елементів в $\Delta\overline{\overline{B}}$.

Якщо $k_p > k_n$,

то $\overline{p}_i = 1$,

інакше $\overline{p}_i = 0$.

Конкретна алгоритмічна реалізація методу $SA_B^{(M)}$ буде визначатися конкретними значеннями параметрів l, h.

Для практичного підтвердження зменшення спотворення ЦЗ в процесі стеганоперетворення $SA_B^{(M)}$ в порівнянні з SA_B був проведений обчислювальний експеримент, у якому були задіяні 400 ЦЗ з бази NRCS [13], що є традиційною для тестування алгоритмів, які працюють з ЦЗ. Далі ця множина зображень називається тестовою множиною (ТМ). Оскільки для алгоритмічної реалізації SA_B в [10,11] обгрунтована доцільність значення $l = 8$, далі розглядається саме це значення для розміру блоків, що використовуються при вбудові ДІ.

В ході експерименту в ЦЗ-контейнери із ТМ вбудовувалася ДІ, що представляла із себе бінарну послідовність, методом $SA_B^{(M)}$ з різними значеннями $h \in \{2,4,6,8\}$ (відповідні алгоритми далі позначаються $SA_B^{(M,h)}$). Після цього отримане стеганоповідомлення зберігалося у форматі без втрат. Кількісна оцінка спотворення контейнера за рахунок стеганоперетворення проводилася за допомогою різницевого показника PSNR – пікового відношення «сигнал-шум»:

$$PSNR = 10 \cdot lg\left(255^2 \Big/ \left(\frac{1}{m^2} \sum_{i,j} \left(f_{ij} - \overline{f}_{ij} \right)^2 \right) \right).$$

Результати цієї частини експерименту наведені на рис.3 (при цьому $h = 8$ відповідає алгоритмічній реалізації базового методу SA_B). Необхідно зазначити, що й

для SA_B середнє значення PSNR>40dB, що розглядається в літературних джерелах як значення, яке характеризує прийнятну якість ЦЗ при стеганоперетворенні [3], хоча порушення надійності сприйняття стеганопвідомлення, як було зазначено вище, можливо, що в черговий раз підтверджує недосконаліть існуючих кількісних різницевих показників у випадку оцінки візуального сприйняття зміненого ЦЗ.

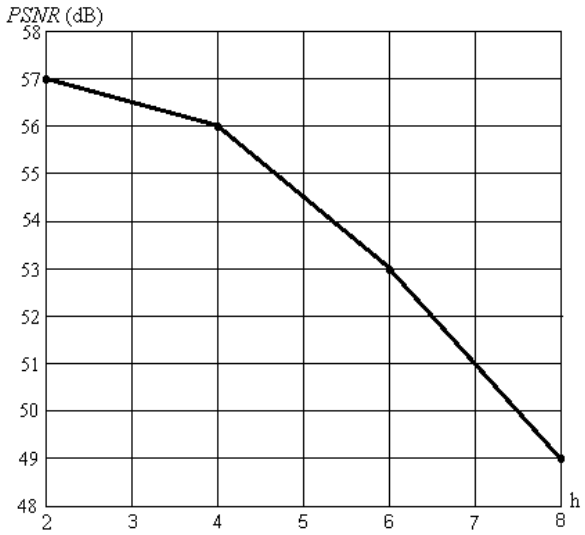


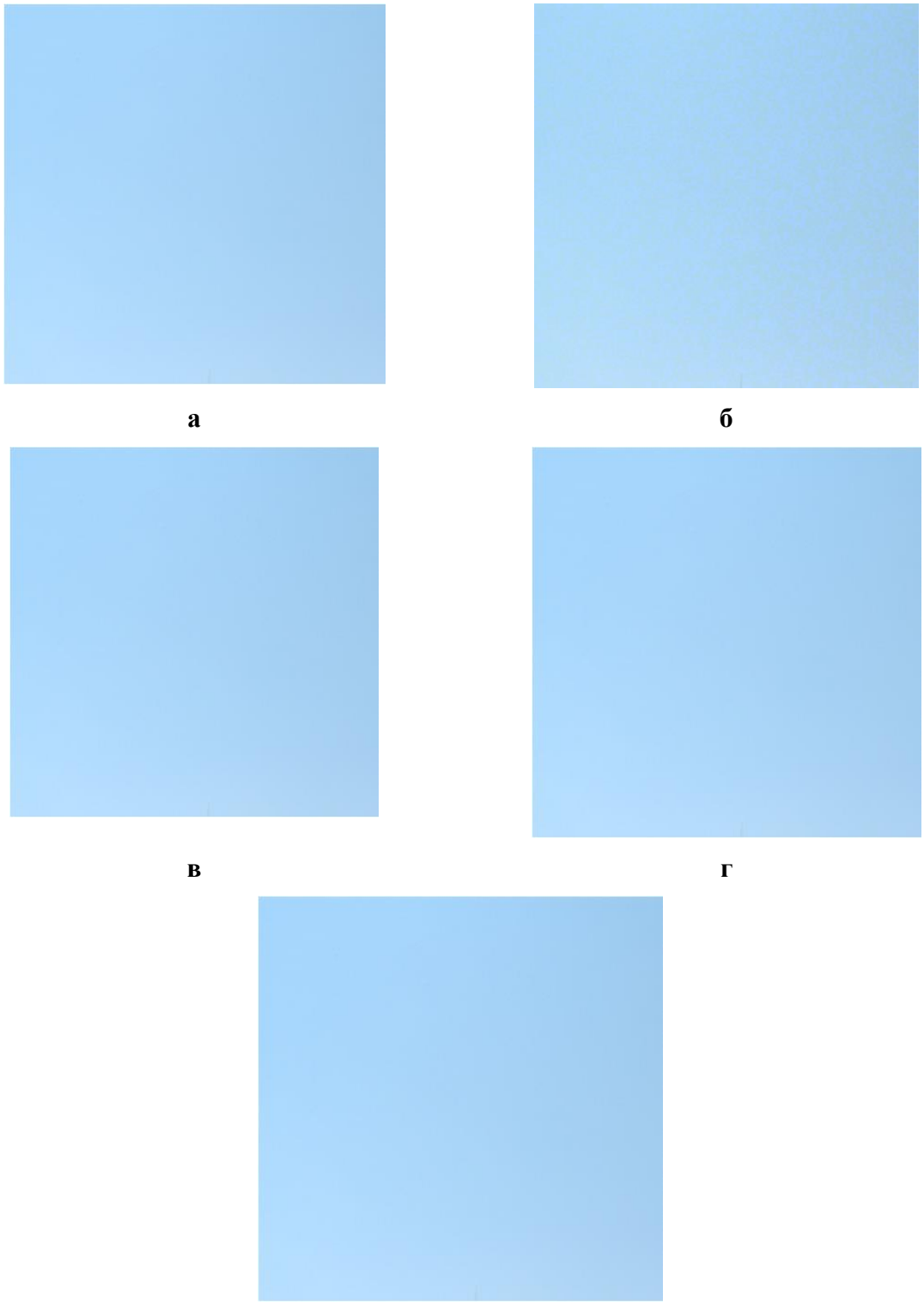
Рис. 3. Залежність значення PSNR, що відображає спотворення контейнера в результаті стеганоперетворення за допомогою $SA_B^{(M,h)}$, від величини h

Виходячи з отриманих результатів для забезпечення візуальної стійкості СП найкращим з погляду значення PSNR після стеганоперетворення є $h=2$, однак експертна оцінка, отримана шляхом суб'єктивного ранжирування, є задовільною вже для $h=6$, в тому числі, для абсолютної більшості тих ЦЗ-контейнерів, для яких для SA_B спостерігалося виникнення артефактів (рис. 4). Однак, з урахуванням мети роботи, вибір h повинен забезпечити відсутність артефактів на СП при незначному зменшенні стійкості модифікованого алгоритму в порівнянні з базовим, яке очевидно відбудеться. Рішенню цієї задачі була присвячена друга частина обчислювального експерименту, у ході якої отримані раніше й збережені без втрат (у відсутності будь-яких збурних дій) стеганоповідомлення піддавалися різним атакам проти вбудованого повідомлення, після чого відбувалося декодування ДІ. Кількісна оцінка ефективності декодування визначалася коефіцієнтом кореляції NC для ДІ [10]:

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

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 $p_i=0,\ \overline{p}_i=0$.

Як атаки використовувалися: накладання різних шумів, фільтрація, збереження СП із втратами (формати Jpeg, Jpeg2000). Результати експерименту наведені в табл.1.



а **б** **в** **г** **д**

Рис. 4. Результати стеганоперетворення зображення за допомогою SA_B та стеганоалгоритмами, що реалізують $SA_B^{(M)}$: а – контейнер; б – СП, сформоване SA_B; в – СП, сформоване $SA_B^{(M,6)}$; г – СП, сформоване $SA_B^{(M,4)}$; д – СП, сформоване $SA_B^{(M,2)}$

Таблиця 1.

Кількісні оцінки стійкості до атак проти вбудованого повідмлення алгоритмічних реалізацій методів SA_B та $SA_B^{(M)}$

Збурні дії та їх параметри		Значення NC			
		SA_B	$SA_B^{(6)}$	$SA_B^{(4)}$	$SA_B^{(2)}$
Гауссівський шум з нульовим маточікуванням	$D=0.0005$	0.994	0.994	0.920	0.834
	$D=0.001$	0.993	0.992	0.891	0.811
	$D=0.005$	0.988	0.979	0.874	0.791
	$D=0.01$	0.962	0.951	0.823	0.715
	$D=0.1$	0.524	0.508	0.505	0.491
Мультиплікативний шум	$D=0.0001$	0.995	0.995	0.941	0.854
	$D=0.001$	0.993	0.993	0.903	0.802
	$D=0.01$	0.977	0.967	0.873	0.779
	$D=0.08$	0.822	0.810	0.806	0.721
	$D=0.5$	0.548	0.533	0.505	0.496
Пуассонівський шум		0.9977	0.9953	0.9211	0.8454
Усереднюючий фільтр розміру $p\times p$	p=3	0.994	0.989	0.922	0.834
	p=5	0.962	0.943	0.881	0.794
	p=7	0.881	0.839	0.709	0.678
Гауссов фільтр розміру $p\times p\,(sig=0.5)$	p=3	0.997	0.982	0.912	0.833
	p=5	0.997	0.982	0.912	0.833
	p=7	0.997	0.983	0.912	0.833
Медіанний фільтр 3×3		0.997	0.985	0.913	0.836
Збереження СП в форматі Jpeg з коефіцієнтом якості QF	QF=40	0.969	0.920	0.808	0.703
	QF=60	0.987	0.966	0.845	0.737
	QF=70	0.988	0.974	0.890	0.765
	QF=80	0.989	0.980	0.911	0.834
	QF=90	0.991	0.990	0.951	0.884
Збереження СП в форматі Jpeg2000 з коефіцієнтом якості QF	QF=40	0.782	0.739	0.648	0.549
	QF=60	0.947	0.934	0.723	0.623
	QF=70	0.980	0.963	0.867	0.711
	QF=80	0.990	0.972	0.912	0.799
	QF=90	0.992	0.989	0.954	0.888

Виходячи з результатів порівняльного аналізу стійкості алгоритму, що реалізує базовий стеганометод, і його модифікацій, що визначаються значеннями параметра h, і беручи до уваги оцінки спотворень контейнера в результаті стеганоперетворення, можна зробити висновок, що співвідношення між NC и $PSNR$, яке найбільш підходе, досягається для $h=6$, яке й рекомендується використовувати для розробленої модифікації $SA_B^{(M)}$ методу SA_B. Рекомендоване значення параметра знижує стійкість алгоритму до атак проти вбудованого повідомлення незначно - не більше, ніж на 5.5% (див. табл.1).

Висновки

В роботі запропонована модифікація стійкого до атак проти вбудованого повідомлення стеганометода, що здійснює вбудову ДІ в просторовій області зображення-контейнера, яка дозволяє усунути будь-які обмеження на область

застосування, забезпечуючи надійність сприйняття відповідного стеганоповідомлення незалежно від специфіки зображення-контейнера, що не було притаманне базовому стеганометоду і відповідному алгоритму, область застосовності якого обмежувалася зображеннями, що не мали значних за розміром фонових ділянок. Результат модифікації досягається за рахунок зменшення стрибка функції яскравості пікселів на границі блоків матриці ЦЗ-контейнера при вбудові ДІ шляхом зміни виду матриці збурення блоку контейнера при стеганоперетворенні.

Алгоритмічна реалізація побудованої модифікації не знижує значно стійкість модифікованого алгоритму, у порівнянні з базовим, при рекомендованому значенні параметра $h=6$, який визначає вид матриці збурення блоку контейнера при стеганоперетворенні. Максимальне зниження стійкості стеганоалгоритму, яка кількісно оцінювалася коефіцієнтом кореляції для переданої інформації, досягало 5.5%.

Обчислювальна складність запропонованої алгоритмічної реалізації визначається кількістю блоків в $m\times m-$ матриці ЦЗ і складає $\underline{O}\left(m^2\right)$ операцій.

Література

1. Qin, C. A Novel Digital Watermarking Algorithm in Contourlet Domain / C. Qin, X. Wen // Journal of Information & Computational Science. — 2014. — 11(2). — P. 519 – 526;
2. Fang, H. Robust Watermarking Scheme for Multispectral Images Using Discrete Wavelet Transform and Tucker Decomposition / H. Fang, Q. Zhou, K. Li // Journal of Computers. — 2013. — Vol.8. — No.11. — P. 2844 – 2850.
3. Lin, W.H. A blind watermarking method using maximum wavelet coefficient quantization / W.H. Lin, Y.R.Wang, S.J. Horng *et al*. // Expert Systems with Applications. — 2009. — No.36. — P. 11509 – 11516.
4. Doncel, V.R. An Optimal Detector Structure for the Fourier Descriptors Domain Watermarking of 2D Vector Graphics / V.R. Doncel, N. Nikolaidis, I. Pitas // IEEE Transactions on Visualization and Computer Graghics. — 2007. — 13(5). — P. 851 – 863.
5. Nasir, I. A New Robust Watermarking Scheme for Color Image in Spatial Domain / I. Nasir, Y. Weng, J. Jiang // In Proceedings of the 3rd International IEEE Conference on Signal-Image Technologies and Internet-Based System (SITIS'07), 16–18 Dec. 2007, Shanghai. — 2007. — P. 942 – 947.
6. Viswanatham, V.M. Novel Technique for Embedding Data in Spatial Domain / V.M. Viswanatham, J. Manikonda // International Journal on Computer Science and Engineering. — 2010. — Vol.2. — P. 233 – 236.
7. Кобозева, А.А. Связь свойств стеганографического алгоритма и используемой им области контейнера для погружения секретной информации / А.А. Кобозева // Искусственный интеллект. — 2007. — № 4. — С. 531 – 538.
8. Кобозева, А.А. Условия обеспечения устойчивости стеганоалгоритма при организации стеганопреобразования в пространственной области контейнера-изображения / А.А. Кобозева, О.В. Костырка // Інформаційна безпека. — 2013. — №3(11). – С. 29 – 35.
9. 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.
10. Костирка, О.В. Стеганографічний алгоритм, стійкий до накладання шуму / О.В. Костирка // Безпека інформації. – 2014. – Т.20. – №1. – С. 71 – 75.
11. Кобозева, А.А. Стеганопреобразование пространственной области изображения-контейнера, устойчивое к атакам против встроенного сообщения Проблемы региональной энергетики. / А.А. Кобозева, О.В. Костырка, Е.Ю. Лебедева // Электронный журнал Академии наук республики Молдова. – 2014. – №1(24). – С. 1 – 12.
12. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. П.А. Чочиа. — М. : Техносфера, 2006. — 1070 с.
13. NRCS Photo Gallery: *[Електронний ресурс]* // United States Department of Agriculture. Washington, USA. Режим доступу: http://photogallery.nrcs.usda.gov (Дата звернення: 26.07.2012).

МОДИФИКАЦИЯ УСТОЙЧИВОГО К ВОЗМУЩАЮЩИМ ВОЗДЕЙСТВИЯМ СТЕГАНОПРЕОБРАЗОВАНИЯ ПРОСТРАНСТВЕНОЙ ОБЛАСТИ ИЗОБРАЖЕНИЯ-КОНТЕЙНЕРА

А.В Костырка

Черкасский институт пожарной безопасности им. Героев Чернобыля Национального университета гражданской защиты Украины,
ул. Оноприенко, 8, Черкассы, 18034, Украина; e-mail: chaykaov@rambler.ru

В работе предложена модификация устойчивого к атакам против встроенного сообщения стеганографического метода, разработанного автором ранее, осуществляющего стеганопреобразование в пространственной области контейнера-изображения, имеющего ограничение области применения в силу возможности нарушения надежности восприятия изображения в результате внедрения дополнительной информации. Результатом модификации является устранение любых ограничений на область применения соответствующего алгоритма путем обеспечения надежности восприятия формируемого стеганосообщения независимо от специфики изображения-контейнера. Устойчивость алгоритма, который реализует модифицированный метод, к атакам против встроенного сообщения при этом снижается незначительно. В качестве возмущающих воздействий рассмотрены: наложение на стеганосообщение различных шумов с различными параметрами, фильтрация, сжатие стеганосообщения с потерями с различными коэффициентами качества (сохранение в форматы Jpeg, Jpeg2000). Приведены результаты вычислительного эксперимента.

Ключевые слова: стеганографический алгоритм, цифровое изображение, пространственная область контейнера, надежность восприятия стеганосообщения, устойчивость к атакам против встроенного сообщения

MODIFICATION OF RESISTANCE TO DISTURBANCE QUILTED TRANSFORMATION OF SPATIAL IMAGE CONTAINER

O.V Kostyrka

Cherkassy Institute of Fire Safety named. Heroes of Chernobyl National University of Civil Defense of Ukraine,
8, Onoprienko st., Cherkasy, 18034, Ukraine; e-mail: chaykaov@rambler.ru

The paper presents a modification resistant to attacks against embedded message steganographic method developed earlier by the author, which provides a spatial region stehanoperetvorennya container image, but is limited to applications with the ability to breach the reliability of the image due to embed additional information. The result of the modification is to eliminate any restriction on the scope of the relevant algorithm by ensuring the reliability of perception formed stehanopovidomlennya regardless of the specific image container. Resistance algorithm that implements a modified method to attacks against embedded message in this case is reduced slightly. As discussed zburni steps: overlay stehanopovidomlennya different noises with different parameters, filtering, compression lossy stehanopovidomlennya with different coefficients of quality (saving in format Jpeg, Jpeg2000). The results of computational experiments.

Keywords: steganography algorithm, digital images, spatial region container perception stehanopovidomlennya reliability, resistance to attacks against embedded message