УДК 004.932

А.О. Коваленко, А.О. Різуненко

Полтавський військовий інститут зв'язку

МЕТОД ПРИХОВУВАННЯ ДАНИХ У ЗОБРАЖЕННЯХ ШЛЯХОМ ЦЕНТРУВАННЯ ЗНАЧЕНЬ КОЛІРНИХ КОМПОНЕНТ

Визначено основні види атак на стегосистеми. Сформульовано способи оцінки прихованості та захищеності стегосистем від пасивних та активних атак. Проаналізовано характер спотворень зображень, які вносяться під час компресії форматом JPEG2000. Розроблено метод приховування даних у зображення шляхом центрування значень колірних компонент. Проведена оцінка синтезованого методу. Доведено залежність стійкості методу від його прихованості

стегосистема, контейнерробастність, стійкість, інтервал впровадження, центрування

Вступ

Аналіз літератури. На сучасному етапі розвитку систем передачі інформації основним методом захисту даних є криптографічне шифрування. Однак, на сьогоднішній день криптографія не може в повній мірі захистити інформацію, представлену у цифровому вигляді. Криптографічні методи дозволяють лише зашифрувати повідомлення, а при застосуванні в якості цифрового підпису захистити лише його цифрове представлення. На відміну від цього стеганографія додатково приховує факт передачі даних, а також дозволяє захистити зміст повідомлення. Перевага застосування стеганографічних методів актуальна при захисті мультимедійних даних [1], тому що цей вид інформації найбільш часто підлягає різноманітним санкціонованим модифікаціям (зміна формату, стиснення, вирізання областей тощо).

При приховуванні інформації виділяють поняття контейнера і стего: контейнер – це повідомлення, в яке приховуються дані, стего – контейнер з прихованим повідомленням [2].

На сьогоднішній день для стеганографічних протоколів характерна боротьба з пасивними та активними атаками [3]. Пасивна атака передбачає спроби зловмисника виявити наявність факту скритої передачі повідомлення, без намагання будь-яким чином модифікувати його. Для боротьби з такими атаками необхідно приховувати повідомлення в області, які несуть в собі найменше інформації (наприклад, молодші значущі біти звукових або графічних файлів), а також застосовувати ключі для визначення місця приховування.

Активна атака більш поширена і передбачає спроби зловмисника прочитати, модифікувати, видалити повідомлення або впровадити хибне. Для боротьби з нею вищезгадані способи недоцільні, тому що будь-які модифікації стего (зміна формату або стиснення з втратами, вирізання областей, додавання шуму і т.д.) призводять до спотворень прихованого повідомлення або його частини. Стійкість стегосистеми до таких атак називають робастністю (від англ. robust – міцний, стійкий). Прикладом активної атаки на стего є стиснення з втратами (наприклад, JPEG2000).

Метою дослідження є розробка квазістійкого (в даному випадку стійкого лише до зміни формату зображення) методу приховування інформації в кольорових сильнонасичених зображеннях.

Способи оцінки прихованості та стійкості стеганографічних методів

Ефективність роботи стегосистеми при дії пасивної атаки оцінюється суб'єктивно (шляхом візуального вивчення утвореного стего) та об'єктивно (статистичне дослідження) [4]. Для об'єктивної оці-

нки найбільш часто застосовують показники середньоквадратичного відхилення σ та пікового співвідношення сигнал-шум PSNR між початковим сигналом-контейнером та утвореним в результаті приховування стего. Математичні вирази для обчислення σ та PSNR, при використанні в якості контейнера зображення, приведені нижче:

$$\sigma = \log_2\left(\sqrt{\frac{1}{n\times m}\sum_{i=0}^{n-1}\sum_{j=0}^{m-1}(x_{i,j}-\tilde{x}_{i,j})^2}\right), \text{ рів.кв.;} \quad (1)$$

$$PSNR = 10\lg\left(\frac{255^2\times n\times m}{\sum_{i=0}^{n-1}\sum_{j=0}^{m-1}(x_{i,j}-\tilde{x}_{i,j})^2}\right), \text{ дБ,} \quad (2)$$

де n і m – висота та ширина зображення; $x_{i,j}$ та $\tilde{x}_{i,j}$ – відповідно відліки початкового та модифікованого зображення.

Якість спотворень зображення вважається допустимою (відсутні візуальні спотворення), якщо $\sigma \le 3$ рівнів квантування та PSNR $\ge$ 28 – 30 дБ [5].

Стійкість до активної атаки оцінюється відносною кількістю правильно прийнятих біт прихованої інформації. З цією метою пропонується застосовувати коефіцієнт помилок $K_{пом}$:

$$K_{пом} = \frac{\sum_{i=0}^{N-1}\left(I_i \oplus \tilde{I}_i\right)}{N}\times 100\%, \quad (3)$$

де I_i та $\tilde{I}_i$ – відповідно біти впровадженого та декодованого повідомлення; N – кількість впроваджених інформаційних біт.

Максимальне допустиме значення коефіцієнту помилок залежить від задач, які вирішує стегосистема та виправляючої можливості завадостійкого коду, який буде застосовуватися на прийомній стороні.

У загальному випадку, на стегосистему будуть діяти комплексні атаки, тому необхідне одночасне виконання умов прихованості та робастності. Складність при цьому полягає в тому, що збільшення стійкості приводить до зменшення прихованості і навпаки [6].

Розробка методу приховування інформаційних повідомлень

Найпростішим методом приховування даних у зображенні є метод молодших бітових площин: заміна молодших значущих біт колірних компонент зображення на інформаційні біти повідомлення, що приховується. Такий метод надає достатню прихованість від візуальних атак, але не дає прихованості від атак методом статистичного дослідження стего (визначення ентропії, зміни частоти колірного перепаду і т.д.), а також абсолютно не захищає від активних атак [7].

Для захисту від активних атак типу стиснення з втратами (наприклад, JPEG2000) необхідне застосування методів, які враховують характер спотворень, які вносяться у зображення при компресії.

Аналіз спотворень компонент зображення показав, що під дією формату JPEG2000 змінюються всі бітові площини зображення (від 0,5 – 1% для 8-ї та 49 – 50% для 1-ї бітових площин). Хоча величина зміни старших бітових площин лежить в межах допустимих норм, приховування в ці площини неможливе через помітність візуальних спотворень зображення.

Інший експеримент показав, що амплітуда 95% значень колірних компонент змінюється не більше ніж на 3 та 5 рівнів градації яскравості (при стиску з коефіцієнтом 5 та 10 відповідно)

Використовуючи одержані результати, було розроблено метод приховування даних шляхом „центрування" значень колірних компонент. Сутність методу зображена на рис. 1 і полягає у наступному:

1. Діапазон значень колірних компонент лежить у межах [0;255]. Даний діапазон розбивається на N інтервалів (значення N залежить від робастності, яку повинен мати метод).

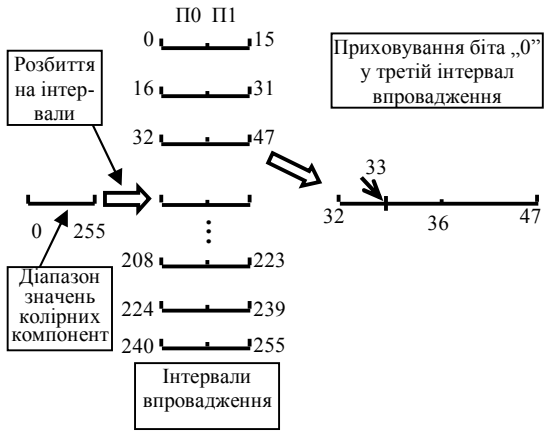

Рис. 1. Схема приховування інформаційного біта „0" методом центрування у другий інтервал впровадження

2. Кожен інтервал має рівні верхній та нижній піддіапазони. Позначимо їх „*піддіапазон одиниці*" (П1) та „*піддіапазон нуля*" (П0) відповідно.

3. Кодування відбувається наступним чином: значення колірної компоненти „розміщуються" в центрі П0 відповідного інтервалу при впровадженні біта „0" (аналогічно при впровадженні біта „1" – в центрі П1).

4. На прийомній стороні декодується біт „0", якщо значення компоненти лежить в межах П0 будь-якого інтервалу (аналогічно при декодуванні „1").

Стійкість розробленого методу полягає у наступному: значення колірних компонент після компресії змінюються не більше ніж на 0–5 рівнів градації яскравості, тому відновлені значення будуть належати тим піддіапазонам, в які вони були переміщені під час кодування.

Аналітично процеси кодування та декодування описуються наступними виразами:

$$x_{i,j} = \begin{cases} w \cdot \left(\dfrac{4 \cdot n + 1}{4} \right), \text{якщо } b_k = 0, \\ w \cdot \left(\dfrac{4 \cdot n + 3}{4} \right), \text{якщо } b_k = 1; \end{cases} \quad (4)$$

$$b_k = \begin{cases} 1, \text{ якщо } \left\{ \dfrac{\tilde{x}_{i,j}}{w} \right\} \geq \dfrac{w}{2}, \\ 0, \text{ якщо } \left\{ \dfrac{\tilde{x}_{i,j}}{w} \right\} < \dfrac{w}{2}; \end{cases} \quad (5)$$

де $x_{i,j}$ – значення колірної компоненти до компресії; $w = 256/N$ – інтервал робастності (інтервал приховування); n – номер інтервалу, якому належить $x_{i,j}$ (нумерація починається з нуля); b_k – біт, що впроваджується; $\tilde{x}_{i,j}$ – значення колірної компоненти після стиснення; $\{\tilde{x}_{i,j}/w\}$ – залишок від ділення $\tilde{x}_{i,j}$ на *w*.

Оцінка розробленого методу

Прихованість стегосистеми залежить від ширини інтервалу впровадження w: при w = 16 середні значення PSNR та СКО дорівнюють 33 дБ та 2,5 рів. кв., а при w = 32 – 27 дБ та 3,5 рів. кв відповідно.

Стійкість методу залежить від частоти колірного перепаду контейнера. Це пояснюється властивістю людського ока зменшувати свою чутливість при спостеріганні висококонтрастних областей (ефект маскування) [4]. Тому в якості контейнера рекомендується застосовувати зображення з частотою колірного перепаду 0,8 і більше.

Іншим обмеженням є використання зеленої колірної компоненти для впровадження біт. Прихованість методу значно зменшується через особливу чутливість зору людини до світлових хвиль в діапазоні зеленого кольору [4]. Колірна модель RGB не враховує цей факт, тому для вирішення цієї проблеми пропонується застосовувати інші моделі представлення зображення (наприклад, YUV, YIQ та ін.).

Залежність значення коефіцієнту помилок від частоти колірного перепаду зображення, ширини інтервалу робастності та коефіцієнту стиснення формату компресії вказана у табл. 1.

Таблиця 1

Залежність значень $K_{пом}$ від інтервалу впровадження, частоти колірного перепаду та коефіцієнту компресії

Частота колірного перепаду	Інтервал впровадження	$K_{пом}$, %	
		$k_{стиску} = 5$	$k_{стиску} = 10$
0,8	w = 16	**5,36**	**28,83**
	w = 32	**1,022**	**19,044**
0,9	w = 16	**13,16**	**30,24**
	w = 32	**4,98**	**28,54**

Таким чином, підтверджується залежність стійкості методу від його прихованості (рис. 2): чим більше прихованість методу (тобто, чим більше частота колірного перепаду зображення та менше інтервал робастності), тим менше його стійкість до активних атак (більший коефіцієнт помилок).

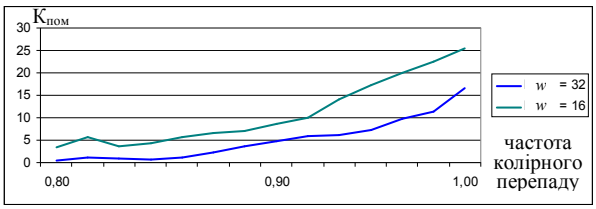

Рис. 2. Графіки залежності коефіцієнту помилок від частоти колірного перепаду контейнера при стисненні з коефіцієнтом компресії 5

Висновки

Розроблено метод приховування даних у зображення, робастний до атак типу стиснення з втратами методом JPEG2000. В залежності від ширини інтервалу впровадження (16 або 32), частоти колірного перепаду (від 0,8 до 0,99) та коефіцієнту стиснення, існує можливість декодування даних з коефіцієнтом помилок від 5% до 30%. Необхідно враховувати, що такі значення отримані при повному заповненні області зображення, куди можливе впровадження даних без візуальних викривлень (наприклад, для зображення 800x600 пікселів це складає близько 58 кбайт на кожну колірну компоненту). Цифрові мітки в області захисту мультимедійної інформації мають невеликий об'єм (десятки – сотні байт), тому додаткове використання виправляючих кодів (наприклад, Ріда-Соломона, БЧХ) надає можливість правильного прийому впроваджених даних.

Підтверджено залежність стійкості стеганографічних методів від їхньої прихованості, а саме: залежність коефіцієнту помилок від ширини інтервалу впровадження та частоти колірного перепаду контейнера.

Подальші дослідження слід направити на вивчення можливості приховування даних в область перетворення зображень (наприклад, при застосуванні вейвлет-перетворення), використання ключів та завадостійких кодів.

Список літератури

1. Kutter M., Voloshynovskiy S., Herrigel A. The Watermark Copy Attack // Proceedings of SPIE: Security and Watermarking of Multimedia Content II. 2000. Vol. 3971.

2. Christian Cachin. An Information-Theoretic Model for Steganography // Proceedings of 2nd Workshop on Information Hiding, Lecture Notes in Computer Science, Springer, 1998.

3. Simmons G. The prisoner`s problem and the subliminal channel // Proc. Workshop on Communications Security, 1984. – P. 51-67.

4. Грибунин В.Г. Цифровая стеганография. – С.-Пб.: ВУС, 2000. – 272 с.

5. Прэтт У. Цифровая обработка изображений: Пер. с англ., кн. 2. – М.: Мир, 1982. – 480 с.

6. Deepa Kundur. Multiresolution Digital Watermarking:Algorithms and Implications for Multimedia. 1999.

7. Fridrich J., Du R., Long M. Steganalysis of LSB encoding in color images // ICME, 2000.

Надійшла до редколегії 29.09.2006

Рецензент: д-р техн. наук, проф. О.О Ємець, Полтавський університет споживчої кооперації України, Полтава

.