УДК 651.326

М.М. ЗАЦЕРКЛЯНИЙ, д-р техн. наук, "ХНУВС" (м. Харків),
Г.С. КИРИЧЕНКО, "ХНУВС" (м. Харків)

ДОСЛІДЖЕННЯ МЕТОДУ RS-СТЕГАНОАНАЛІЗУ

В даній статті стеганографія розглядається як інструмент, за допомогою якого може порушуватись безпека інформаційної системи. Проведено дослідження одного з інструментів протидії певному класу стеганографічних вкладень – метод RS-стеганоаналізу. Докладно проаналізовані процеси, що відбуваються при вкладенні пошуку прихованих даних у типові зображення. Встановлено властивість типових зображень, яка може бути застосована при розробці та модифікації методів стеганоаналізу.

Ключові слова: стеганографія, стеганоаналіз, пошук прихованих даних.

Постановка проблеми. Цифрова стеганографія – це сукупність методів, метою яких є передача секретних повідомлень всередині інших цифрових даних таким чином, що існування вбудовувань складно чи неможливо виявити. Носіями прихованої інформації найчастіше виступають цифрові зображення [1, 2]. Це пов'язано з тим, що особливості деяких класів зображень дозволяють досить легко вносити зміни, не помітні для людського ока. Враховуючи можливість використання стеганографії для реалізації злочинних намірів, досить актуальною є розробка методів стеганоаналізу.

Аналіз літератури. До можливих стеганоаналітичних методів відносяться статистичні методи [3, 4]. Їх особливість полягає у тому, що для певного класу зображень вони дозволяють відшукати "сталі" критерії, за допомогою яких із певною ймовірністю можна зробити висновок про наявність прихованих вкладень [5].

Статистичні методи, які запропоновані в N. Provos [6] та A. Westfeld [7], нехтують важливою інформацією – відношеннями між сусідніми пікселями стеганозображення. Використання просторових зв'язків пікселів зображення дозволяє створювати методи з більш точним виявленням об'єму прихованої інформації.

Одним з таких методів є метод RS-стеганоаналізу [8]. Цей метод дозволяє віднайти та виміряти слабкий зв'язок між найменш значущими пікселями зображення та самим зображенням. Очевидно, що цей зв'язок зміниться після вбудовування прихованої інформації. Отже його можна використовувати як підґрунтя стеганографічного алгоритму.

Мета статті – дослідження методу RS-стеганоаналізу та пошук стеганоаналітичних закономірностей.

Основи методу RS-стеганоаналізу. Розглядаємо зображення розміром $H \times W$ пікселів, де пікселі приймають значення з множини P. Наприклад, для 8-бітових сірих зображень $P = \{0, 1, \ldots, 255\}$. Просторова кореляція

визначається за допомогою функції-дискримінанта *f*, яка ставить у відповідність дійсне число $f(x_1, x_2, ..., x_n) \in R$ групі пікселів $G = (x_1, x_2, ..., x_n)$.

Такою функцією є

$$f(x_1, x_2, ..., x_n) = \sum_{i=1}^{n-1} \left| x_{i+1} - x_i \right|,$$

яка вимірює гладкість *G*.

Більше значення *f* відповідає більшому значенню шуму.

Вкладення в найменш значущі біти (НЗБ) збільшує шумові властивості зображення, що очевидно збільшує значення *f*. Вбудовування в НЗБ зручно описувати, використовуючи функцію-перемикач

$$F_1 : \quad 0 \leftrightarrow 1, 2 \leftrightarrow 3, ..., 254 \leftrightarrow 255 . \tag{1}$$

Зсунута функція-перемикач визначається так:

$$F_{-1} : \ -1 \leftrightarrow 0, 1 \leftrightarrow 2, ..., 255 \leftrightarrow 256$$

або

$$F_{-1} : \ \ (x) = F_1(x+1) - 1 \forall x . \tag{2}$$

Для повноти також визначається

$$F_0(x) = x, \forall x \in P .$$

Функція-дискримінант *f* та функція-перемикач *F* визначають три типи груп пікселів: *R* – "регулярні", *S* – "нерегулярні" та *U* – "незмінні"

$$G \in R \Leftrightarrow f(F(G)) > f(G), \tag{3}$$

$$G \in S \Leftrightarrow f(F(G)) < f(G), \tag{4}$$

$$G \in U \Leftrightarrow f(F(G)) = f(G), \tag{5}$$

де $F(G)$ означає, що функція-перемикач застосована до кожного елементу множини $G = (x_1, x_2, ..., x_n)$.

Аби застосовувати функцію-перемикач до різних пікселів групи введемо поняття маски (рис. 1)

$$M = (m_1, m_2, ..., m_n), \ m_i \in \{-1, 0, 1\}, \ i = 1, 2, \ldots, n .$$

Операція перемикання з використанням маски визначається так:

$$F_M(G) = F_{M(i)}(x_i), \ i = 1, 2, ..., \ n .$$

В типових зображеннях застосування функції-перемикача до групи *G* частіше призведе до збільшення значення функції-дискримінанта. Таким чином, кількість регулярних груп буде більше кількості нерегулярних груп. Позначимо відносну кількість регулярних груп для додатної маски як R_M (у відсотках всіх груп), аналогічно для нерегулярних груп – S_M. Для від'ємної маски кількості регулярних та нерегулярних груп відповідно дорівнюють R_{-M} та S_{-M}. Отже, маємо

$$R_M + S_M \le 1 \ \text{ та } \ R_{-M} + S_{-M} \le 1 . \tag{6}$$

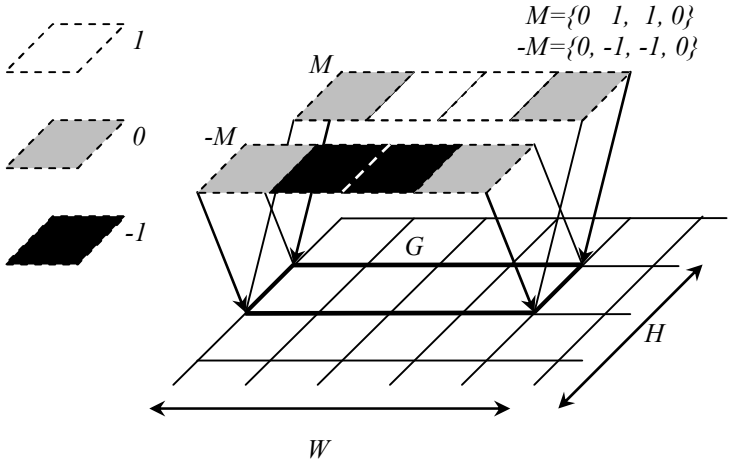

Рис.1. Застосування додатної та від'ємної масок M та $-M$

За нульову гіпотезу описуваного стеганоаналітичного методу приймається рівність кількості регулярних та нерегулярних груп для зображень без вбудовувань

$$R_M \cong R_{-M} \text{ та } S_M \cong S_{-M} . \quad (7)$$

Цю гипотезу легко довести, розглянувши рівняння (2). Використання від'ємної функції-перемикача F_{-1} є застосуванням додатної функції F_1 до зображення, значення кольорів якого зсунуті на одиницю. Оскільки функція-дискримінант f визначає близькість пікселів групи, додавання до всіх пікселів одиниці значно не змінить статистики розподілу регулярних та нерегулярних груп. В роботі [8] заявлено про проведення досліджень, результат яких показує, що зображення, одержані цифровою фотокамерою в JPEG і в нестисненому форматі відповідають виразу (7). Проте вираз (7) порушується в разі зміни площини НЗБ повністю випадковими значеннями.

Наближення розподілу НЗБ до випадкового спрямовує розбіжність R_M та S_M до нуля, тобто зі збільшенням довжини приховуваного зображення кількість регулярних та нерегулярних груп стає для додатної маски однаковою: $R_M \cong S_M$. Проте на R_{-M} та S_{-M} "випадковість" НЗБ зовсім по-іншому впливає. Розбіжність кількості регулярних та нерегулярних груп за умови від'ємної маски – збільшується.

Пошук стеганоаналітичних властивостей. Розглянемо процеси, що відбуваються при застосуванні функції-перемикача та функції-дискримінанта. Для прикладу візьмемо найпростішу маску [0, 1, 0]. Аналогічні процеси можна

відстежити й для більш складних масок. За зображення, що тестується, візьмемо повнокольорове зображення "Lena". Враховуючи розмір маски розіб'ємо зображення на групи пікселів $\{x_i,\ x_{i+1},\ x_{i+2}\}$. Ці групи можна класифікувати за розташуванням елементів на числовій прямій (табл. 1).

Таблиця 1

Класифікація груп пікселів.

	x_i		x_{i+1}		x_{i+2}
1		=		=	
2		=		>	
3		=		<	
4		<		=	
5		<		>	
6		<		<	
7		>		=	
8		>		>	
9		>		<	

Групи пікселів 2 та 4, 3 та 7, а також 6 та 8 є дзеркальним відображенням одна одної. Через те, що інструмент аналізу не має залежати від асиметрії зображення, об'єднаємо відповідні групи (табл. 2). Одержимо 6 множин, до яких можна відносити групи.

Таблиця 2

Класифікація з урахуванням асиметричності деяких груп.

	x_i		x_{i+1}		x_{i+2}
1		=		=	
2		=		>	
3		=		<	
4		<		<	
5		>		<	
6		<		>	

Сформувавши правила віднесення пікселів до тієї чи іншої множини, розглянемо розподіл у них *R*, *S* та *U* типів груп для зображення без вбудовування (табл. 3).

Групи першої множини можуть бути лише *R* типу. Застосування функції перемикача до центрального пікселя завжди змінить його в більшу чи меншу сторону. Збільшення чи зменшення значення пікселя залежить від парності значення пікселя, та типу функції-перемикача. Зміна центрального пікселя

збільшить відстань від нього до його (до того однакових) сусідів. Відповідно виразу (3) ця група є групою *R* типу.

Таблиця 3

Розподіл груп пікселів за множинами для зображення без вбудовувань

	0% *F*+				0% *F*–			
	R	*S*	*U*	SUM	*R*	*S*	*U*	SUM
1	1,37	0,00	0,00	1,37	1,37	0,00	0,00	1,37
2	4,37	0,00	4,52	8,89	4,52	0,00	4,37	8,89
3	4,12	0,00	3,96	8,09	3,96	0,00	4,12	8,09
4	0,00	0,00	41,39	41,39	0,00	0,00	41,39	41,39
5	10,00	9,88	0,00	19,88	9,88	10,00	0,00	19,88
6	10,09	10,29	0,00	20,38	10,29	10,09	0,00	20,38
All	29,95	20,17	49,87	100,00	30,03	20,09	49,88	100,00

Групи другої множини можуть бути *R* та *U* типів. Особливість цієї групи полягає в тому, що центральний піксель більший від одного зі своїх сусідів і дорівнює другому сусіду. Розглянемо випадок застосування додатної функції-перемикача (1).

У випадку парного центрального пікселя застосування функції (1) збільшить його значення на одиницю. Це призведе до того, що він стане більшим за сусідній рівний піксель на одиницю і збільшить свою відстань до сусіднього меншого пікселя також на одиницю, отже відстань між пікселями групи збільшиться. За формулою (3) це буде група *R* типу.

У випадку непарного центрального пікселя застосування функції (1) зменшить його значення на одиницю. Це призведе до того, що він стане меншим від сусіднього рівного пікселя на одиницю і наблизиться до сусіднього меншого пікселя також на одиницю, тобто відстань між пікселями залишиться незмінною. За формулою (5) це буде група *U* типу.

Аналогічні міркування дозволяють пояснити розподіл типів груп у всіх шести множинах.

Аналіз табл. 3 дозволяє краще зрозуміти вирази (6) та (7) для зображень без вбудовувань.

Загальне перевищення кількості регулярних *R* груп над нерегулярними *S* забезпечуються першою, другою та третьою множинами. До четвертої множини, належать лише групи *U* типу. Кількості груп *R* та *S* типів в п’ятій, як і в шостій множинах приблизно однакові. Немає причини, чому б кількість парних центральних пікселів у множинах п’ятої і шостої груп відрізнялась від кількості непарних пікселів. Проаналізувавши розподіли для зображень без вбудовувань, розглянемо розподіл в них *R*, *S* та *U* типів груп для зображення з вбудовуванням 100% прихованої інформації (табл. 4).

Таблиця 4

Розподіл груп пікселів за множинами для зображення
з вбудовуванням 100% прихованої інформації

	100% $F+$				100% $F–$			
	R	S	U	SUM	R	S	U	SUM
1	1,20	0,00	0,00	1,20	1,20	0,00	0,00	1,20
2	3,65	0,00	4,83	8,48	4,83	0,00	3,65	8,48
3	3,34	0,00	4,58	7,92	4,58	0,00	3,34	7,92
4	0,00	0,00	40,92	40,92	0,00	0,00	40,92	40,92
5	8,33	12,08	0,00	20,42	12,08	8,33	0,00	20,42
6	8,39	12,67	0,00	21,06	12,67	8,39	0,00	21,06
All	24,91	24,76	50,33	100,00	35,38	16,72	47,90	100,00

На перший погляд кількість пікселів у множинах суттєво не змінилась (стовпчики SUM в таб. 3 та таб. 4). Але якщо поглянути на розподіл R, S та U типів всередині множин, можна помітити їх певне перегрупування. Для додатної функції перемикача F_+ спостерігається вирівнювання кількості R та S груп. Для від'ємної маски навпаки відстань між кількістю R та S груп збільшується порівняно із зображеннями без вбудовувань (рядок All в табл. 4). Проаналізувавши дані табл. 4, можна відмітити, що на перерозподіл кількості груп R та S типів впливають п'ята та шоста множина пікселів.

До вбудовування в цих множинах кількість груп із парним центральним пікселем дорівнювала кількості груп із непарним центральним пікселем. Після вбудовування в цих множинах відбулося збільшення кількості груп із парним центральним пікселем і зменшилась кількість груп із непарним центральним пікселем. Більш детальний аналіз наведено на рис. 2. З нього випливає причина перерозподілу R та S груп в п'ятій та шостій множинах.

Пояснимо цю причину на множині п'ятій за умови додатної функції-перемикача. R група початкового зображення розподіляє свій об'єм приблизно порівну між R та S групами зображення із вбудовуванням. Одночас у зображенні із вбудовуванням R група формується лише з R та S початкового зображення. S група початкового зображення розподіляє свій об'єм серед різних множин та груп зображення із вбудовуванням. Одночас S група зображення із вбудовуванням формується з різних множин та груп початкового зображення.

Описаний щойно обмін не є рівноцінним. R група початкового зображення віддає приблизно половину свого об'єму для формування S групи зображення із вбудовуванням. S група початкового зображення віддає суттєво менше за половину свого об'єму для формування R групи кінцевого

зображення. Таким чином, виникає асиметрія, яку можна застосовувати зі стеганоаналітичною метою.

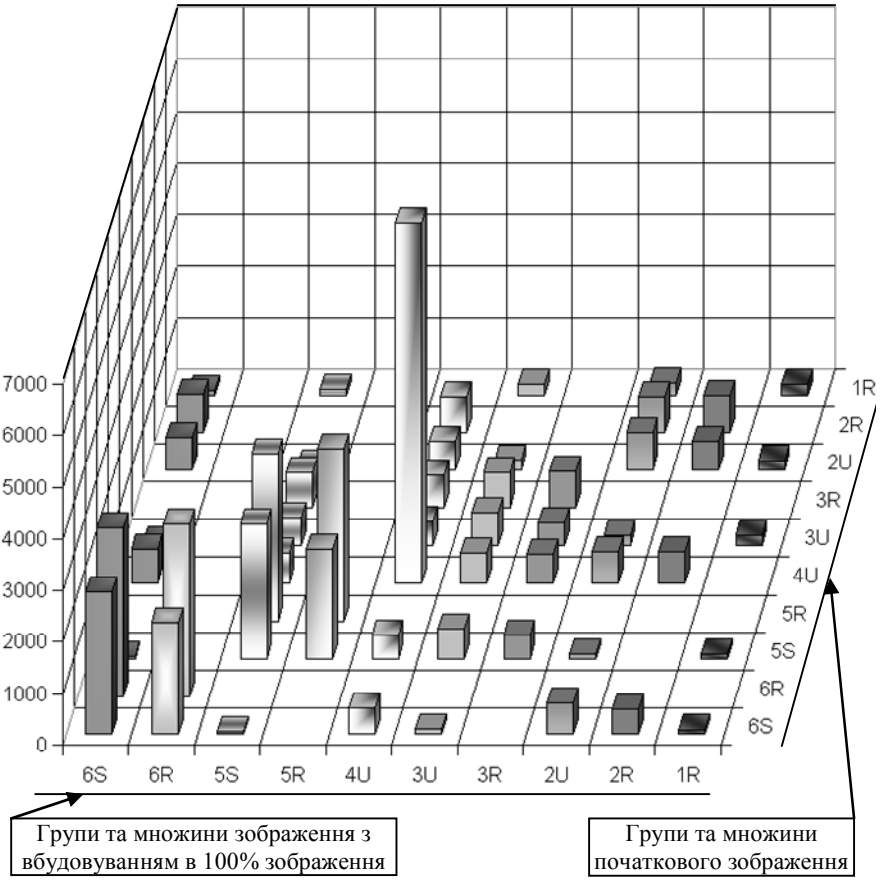

Рис.2. Перехід груп з множин зображення без вбудовування до множин зображення з вбудовуванням прихованого повідомлення максимального розміру (за умови *F*+)

Висновки. Досліджена властивість може застосовуватися при розробці та модифікації методів стеганоаналізу.

Список літератури: **1**. *Генне О.В.* Стеганография: основные положения стеганографии // Конфідент. – 2000. – № 3 (33). – С. 20–41. **2.** *Cachin C.* An information-theoretic model for steganography // Lecture notes on computer science. Springer. – Berlin Heidelberg. – Vol. 1525. – 1998. – P. 306–318. **3.** *Anderson R., Petitcola F.* On the limits of steganography // IEEE Selected Areas Commun, 1998. – P. 474–481. **4.** *Westfeld A.* Detecting low embedding rates // Proc. Information Hiding Workshop. Springer. – 2002. – Vol. 2578. – P. 324–339. **5.** *Гурман В.Е.* Теория вероятностей и

математическая статистика: Учебное пособие для ВУЗов. – М.: Высш. шк., 2003. – 479 с. **6.** *Provos N.* Defending Against Statistical Steganalysis / 10th USENIX Security Symposium. – Washington, DC, 2001. – P. 224–239. **7.** *Westfeld A., Pfitzmann A*. Attack on Steganographic Systems // Lectures Notes in Computer Science. – Berlin: Springer-Verlag, 2000. – P. 61–75. **8.** *Fridrich J., Goljan M.* Practical Steganalysis of Digital Images – State of the Art // Proc. SPIE Photonics California, January, 2002. – Vol. 2554. – P. 1–13.

УДК 651.326

Исследование метода RS-стеганоанализа / Зацеркляний Н.М., Кириченко Г.С. // Вестник НТУ "ХПИ". Тематический выпуск: Информатика и моделирование. – Харьков: НТУ "ХПИ". – 2008. – № 49. – С. 64 – 71.

В статье стеганография рассматривается как инструмент, с помощью которого может нарушаться безопасность информационной системы. Проведено исследование одного из инструментов противодействия определенному классу стеганографичних вложений – метода RS-стеганоанализа. Обстоятельно проанализированы процессы, которые происходят при вложении скрытых данных в типичные изображения. Установлено свойство типичных изображений, которое может быть применено при разработке и модификации методов стеганоанализа. Ил.: 2. Табл.: 4. Библиогр.: 8 назв.

Ключевые слова: стеганография, стеганоанализ, вложение скрытых данных.

UDC 651.326

Research of method of RS-stegananasys / Zacerklyaniy N.M., Kirichenko G.S. // Herald of the National Technical University "KhPI". Subject issue: Information Science and Modelling. – Kharkov: NTU "KhPI". – 2008. – №. 49. – P. 64 – 71.

In this article steganography is examined as an instrument by which can be violated safety of the information system. It is conducted one research of instruments of counteraction the certain class of steganography investments is a method of RS-steganalysis. Processes which take a place at the investment of the hidden information in typical images are thoroughly analysed. Property of typical images, which can be applied at development and modification of methods of steganalysis, is set. Figs: 2. Tabl.: 4. Refs: 8 titles.

Keywords: steganography, stegananalysis, investment of the hidden information

Надійшла до редакції 12.10.2008