Дослідження статистичних закономірностей кольорових каналів зображень за методом RS-стегоаналізу

Корольов В.Ю., Поліновський В.В., Герасименко В.А.

Центр таймерних обчислювальних систем Інституту кібернетики НАН України
dshv937@meta.ua

Abstract

The application of RS-stegoanalysis method for image processing is discussed. The new results for image color channels statistics are presented.

Вступ

Дослідження статистичних характеристик цифрових зображень є основою для розробки нових методів фільтрації шумів, покращення методів інтерполяції, синтезу тримірних моделей віртуальної реальності тощо. Відомо, що багато методів цифрової обробки зображень було запозичено з оптики, кібернетики, спеціальних розділів математики, радіоелектроніки та ґрунтуються на використанні особливості сприйняття візуальних образів людиною.

Постановка задачі

У даній роботі представлено результати досліджень статистичних властивостей кольорових зображень за методом RS-стеганоаналізу, отриманих на великих вибірках зображень різного класу. Подальші дослідження у вказаному напрямку можуть бути використані для побудови нових методів комп'ютерної обробки зображень.

Принцип стеганографічного вбудовування інформації у найменш значимі біти зображення

Введемо терміни, що необхідні для подальшого викладу.

Стеганографія - це область захисту інформації [1-5], предметом якої є засоби та методи, що застосовуються для формування прихованого каналу передачі інформації.

Контейнер - будь-яка форма представлення даних, призначена для приховування таємних повідомлень.

Контейнер з вбудованим секретним повідомленням назвемо *"**стего-образом**"*.

Вбудоване повідомлення - це повідомлення, яке приховане у контейнері.

Стегобіти - це біти даних повідомлення, що підлягають приховуванню стеганографічними методами у контейнері.

НЗБ - найменш значимий біт.

Стеганоаналіз - це процедура виявлення факту вбудовування у контейнер стегобіт і оцінка розміру прихованого повідомлення.

Розглянемо стеганографічне приховування даних у зображеннях за методом заміни найменш значимого біта (НЗБ) на прикладі чорно-білої фотографії (рис. 1). Сучасні комп'ютерні зображення представляють собою масиви натуральних чисел (рис. 2), елементами яких є впорядковані 24-х бітні структури для кольорових зображень або 8-бітні додатні числа для монохромних зображень (рис. 3), що відповідають пікселям зображення.

Рис. 1. Контейнер (тестове зображення) "замок у Іспанії"

На рис. 4 наведено бітове представлення фрагменту рядка зображення і схему стеганографічного приховування інформації за методом заміни найменш значимих бітів (НЗБ) образу бітами текстового рядка. Для цього літери повідомлення замінюють значеннями відповідної кодової таблиці (наприклад, використовують код ASCII - American Standard Code for Information Interchange), а потім його перетворюють у бітову послідовність. Після цього найменш значимі (молодші) біти пікселів для кольорового каналу зображення (чисел, що відповідають яскравості) замінюють бітами вхідного тексту (рис. 4). В результаті, у зображення вбудовується текст без помітної зміни у якості фотографії.

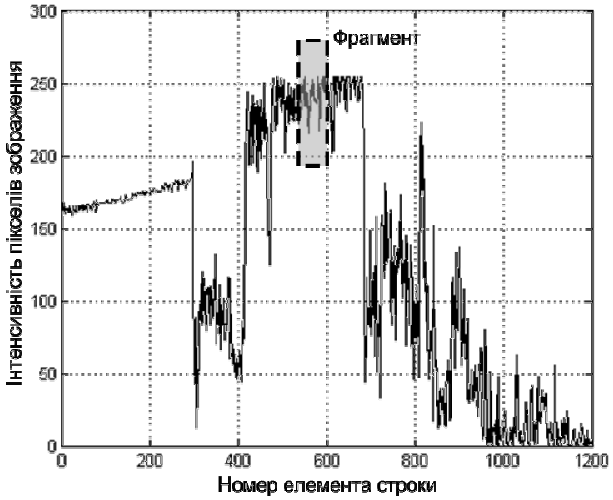

Рис. 2. Рядок контейнера (тестового зображення)

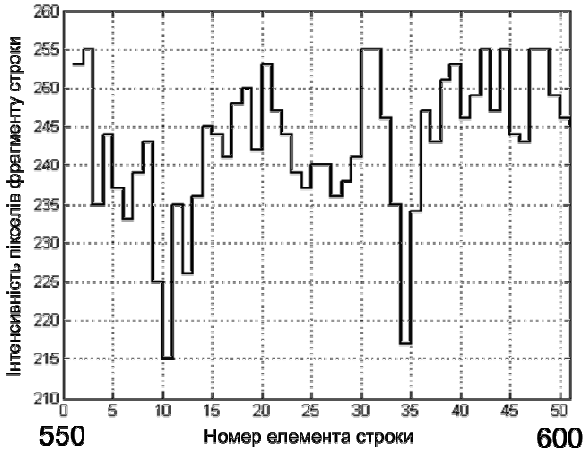

Рис. 3. Фрагмент рядка контейнера (тестового зображення)

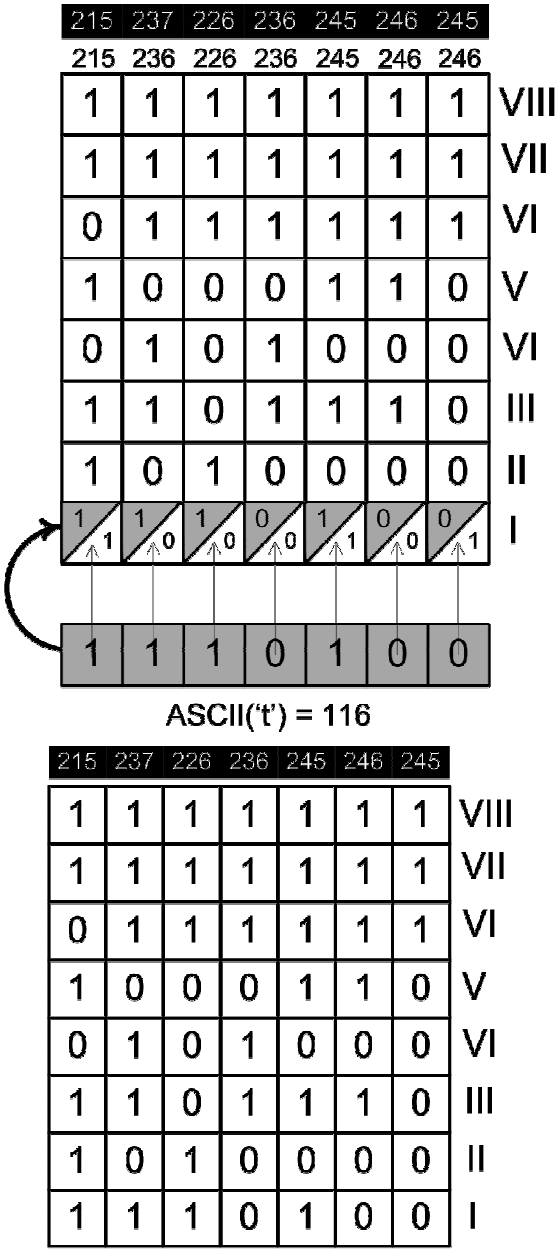

Рис. 4. Ілюстрація принципу стеганографічного приховування інформації у зображеннях

Фактори, що впливають на точність RS-стегоаналізу

Метою стеганоаналізу [1-5] є виявлення даних, прихованих у зображеннях. Випадкові варіації можуть призвести до того, що контейнер, який не містить прихованих повідомлень, буде показувати наявність короткого повідомлення. Метод RS-стегоаналізу [4] більш точний для повідомлень, стего-біти яких випадково розміщені у площині стего-образу, ніж для повідомлень, вбудованих локально. Для того щоб застосувати RS-аналіз у цьому випадку треба перейти до використання методики на базі ковзного вікна.

Іншим фактором, який впливає на точність оцінки довжини вбудованого повідомлення є початкове зміщення [4]. Це початкове не нульове зміщення може мати як позитивний, так і негативний вплив на виявлення стего-бітів та встановлює теоретичні межі точності стеганоаналітичної методики, представленої у винаході [4]. Автори винаходу протестували це початкове зміщення для набору з 331 чорно-білого JPEG зображення, які мають гауссівський розподіл з дисперсією 0,5%. Для менших зображень є тенденція збільшення варіації початкового зміщення, оскільки вони мають меншу кількість RS-груп. Сканування напівтонових і зашумлених зображень показує більш високі варіації зміщення. З іншого боку, зміщення дуже мале для JPEG-зображень, не стиснутих зображень, отриманих з цифрових камер і результатів сканування з високим розрізненням.

Метод RS-стегоаналізу

Нехай контейнер - це зображення розміром MxN пікселів і значеннями пікселів з множини P. Наприклад, для 8-бітного чорно-білого зображення P = {0, 1,…, 255}. Аналіз стего-образу починається з ділення зображення на групи з n суміжних пікселів $(x_1, x_2, \ldots, x_n)$ без перетину елементів. У алгоритмі вибирають групи з n сусідніх пікселів у рядку. Далі визначається дискримінаційна функція f, за якою для кожної групи $G = (x_1, x_2, \ldots, x_n)$ розраховується дійсне число $f(x_1, x_2, \ldots, x_n) \epsilon R$. Значення дискримінаційної функції визначає регулярність (гладкість) групи G пікселів. Чим більше шуму у елементах групи, тим менше значення дискримінаційної функції.

Задамо дискримінаційну функцію f, за якою будемо оцінювати "варіації" групи G:

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

Можна побудувати інші варіанти дискримінаційної функції на базі статистичних моделей або апріорної інформації про контейнер.

Визначимо операцію обернення F на P, яку називають "перевертання". Перевертання - це перестановка рівнів відтінків сірого, яке складається з двох циклів і має властивість таку, що $F(F(x)) = x$, для всіх $x \epsilon P$.

Перестановка F_1: 0<<1, 2<<3, …, 254<<255 відповідає зменшенню НЗБ кожного сірого рівня. Далі ми задаємо зсунуте НЗБ перевертання F_{-1} як 1<<2, 3<<4, …, 253<<254 або $F_{-1}=F_1(x+1)-1$ для всіх x.

Для повноти, ми також визначаємо F_0 як тотожну перестановку $F(x)$ для всіх $x \epsilon P$. Дискримінаційна функція F використовується для виділення трьох груп [4]:

Регулярні групи $G \in R \Leftrightarrow f(F(G)) > f(G)$

Сингулярні групи $G \in S \Leftrightarrow f(F(G)) < f(G)$

Невикористані групи $G \in U \Leftrightarrow f(F(G)) = f(G)$

Позначення $F(G)$ означає, що операція перевертання F застосована до всіх компонент вектора G. Можливі і

інші варіанти перевертання до компонент вектора *G*. Операція перевертання вектора може бути виражена за допомогою маски M, яка називається *n*-кортежем зі значеннями -1, 0 і 1. Перевернута група *F(G)* визначається як $(F_{M(1)}(X_1), F_{M(2)}(X_2),\ldots,F_{M(n)}(X_n))$.

Метою застосування перевертальної функції *F* є збурення малої кількості значень пікселів зворотним способом, чим симулюється дія НЗБ-стеганографічного алгоритму. Для типових зображень додавання невеликої кількості шуму (тобто перевертання малої кількості значень) призведе скоріше до збільшення значення дискримінаційної функції. Тобто загальна кількість регулярних груп (R) буде більшою ніж кількість сингулярних груп (S).

Позначимо кількість регулярних груп для маски M як R_M (у відсотках від всіх груп). Аналогічно, через S_M позначимо відносну кількість сингулярних груп. Маємо $R_M+S_M \le 1$ для позитивної маски і $R_{-M} +S_{-M} \le 1$ для негативної маски. Статистичні гіпотези стеганоаналітичної методики полягають у тому, що в типовому зображенні очікуване значення R_M дорівнює R_{-M} і те саме вірно для S_M і S_{-M}:

$$R_M \approx R_{-M} \text{ і } S_M \approx S_{-M} \qquad (2)$$

Ця гіпотеза може бути перевірена евристично аналізом залежності (1).

Зворотна операція F_{-1}, як і F_1 застосовується до зображення, інтенсивності кольорів якого будуть зсунуті на одиницю. Для типового зображення не існує апріорної причини чому кількість R і S груп повинна суттєво відрізнятись при зсуві кольорів на одиницю.

Автори винаходу [4] переконані, що мають вичерпні експериментальні докази того, що гіпотеза (2) виконується дуже точно для зображень, отриманих з цифрових камер, як для форматів з втратами, так і для форматів без втрат. Це також добре витримується для зображень, оброблених звичайними операціями і для більшості сканованих зображень. Проте відношення (2) порушується, якщо НЗБ-рівень рандомізовано, наприклад, стеганографією НЗБ.

Рандомізація НЗБ-рівня спрямовує різницю між R_M і S_M до нуля, з ростом довжини m повідомлення. Після перевертання НЗБ-рівня 50% пікселів (що буде після вбудовування біта шифрованого повідомлення у кожен піксель) отримаємо $R_M \approx S_M$.

Помічено, що рандомізація НЗБ-рівня має протилежний вплив на R_{-M} і S_{-M}. Їх різниця збільшується зі зростанням довжини m вбудованого повідомлення. Просте пояснення збільшення різниці між R_{-M} і S_{-M} може бути запропоновано для маски M = [0; 1; 1; 0]. Означимо множину $C_i = \{2i, 2i+1\}$, $i = 0,1,\ldots,127$ і множину груп $C_{rst} = \{G|G \in C_r \times C_s \times C_t\}$.

Існує 128^3 замкнутих множин, кожна з яких складається з 8 груп (триплетів). Для цілей аналізу було обрано чотири різних типи множин, ігноруючи ті, що горизонтально і вертикально симетричні. У таблиці нижче представлено ці чотири типи і кількість R, S і U груп після F_1 F_{-1} для кожного типу. З табл.1 видно, що рандомізація НЗБ намагається вирівняти кількість R і S груп в кожній підмножині після F_1, тоді як кількість R груп зростає, кількість S груп спадає після F_{-1}.

Таблиця 1. Кількість R і S груп після перевертання першого і другого етапів

Тип множини	F_1 перевертання	F_{-1} перевертання
r=s=t	2R, 2S, 4U	8R
r=s>t	2R, 2S, 4U	4R, 4U
r<s>t	4R, 4S	4R, 4S
r>s<t	8U	8U

RS стеганоаналітичний метод представлений у винаході [4] обчислює їх перетин за екстраполяцією. Загальна форма чотирьох кривих на RS-діаграмі (рис. 5) змінюється в залежності від контейнера від практично ідеально лінійної до кривої. Експерименти показали, що R_{-M} S_{-M} добре наближуються прямими лініями; внутрішні криві R_M і S_M достатньо добре апроксимуються поліномами другого порядку.

Для стего-образа з повідомленням невідомої довжини p (у процентах від кількості пікселів), яке вбудоване в НЗБ-ти пікселів і випадково розміщене у площині, початкові вимірювання кількості R і S груп відповідають точкам $R_M(p/2)$, $S_M(p/2)$, $R_{-M}(p/2)$ і $S_{-M}(p/2)$. Ділення на два отримуємо з того факту, що для випадкового повідомлення приблизно половина пікселів буде перевернута. Якщо ми перевернемо НЗБ-ти всіх пікселів зображення і порахуємо кількість R і S груп, ми можемо отримати чотири точки $R_M(1-p/2)$, $S_M(1-p/2)$, $R_{-M}(1-p/2)$, $S_{-M}(1-p/2)$.
Через точки можна провести прямі лінії $R_M(p/2)$, $R_{-M}(1-p/2)$ та $S_{-M}(p/2)$, $S_{-M}(1-p/2)$. Точки $R_M(p/2)$, $R_M(1/2)$, $R_M(1-p/2)$ та $S_M(p/2)$, $S_M(1/2)$, $S_M(1-p/2)$ задають дві параболи. Кожна парабола і відповідні лінії перетинаються зліва. Середнє арифметичне від x-координат обох перетинів дозволяє нам оцінити невідому довжину p повідомлення.
Для того щоб уникнути затратного за часом статистичного оцінювання серединних точок $R_M(1/2)$ і $S_M(1/2)$ і, одночасно, зробити оцінку довжини повідомлення більш елегантно, зробимо два додаткових припущення: (А) - точка перетину кривих R_M і R_{-M} має однакову x-координату як і точки перетину кривих S_M і S_{-M}. Це суттєво більш сильне припущення, ніж припущення, зроблене для залежності (2). (Б) - криві R_M і S_M перетинаються при m = 50%, або $R_M(1/2) = S_M(1/2)$.

Автори винаходу [4] перевірили ці припущення експериментально для великої бази даних зображень з не обробленими зображеннями у форматах BMP і JPEG, а також обробленими у форматі BMP. На основі емпіричних даних було отримано просту формулу визначення довжини p секретного повідомлення.

Після зсуву і нормування осі x так, щоб p/2 стало нулем і 100-p/2 стало 1, x-координата точки перетину - це корінь з наступного квадратного рівняння:

$$2(d_1+d_0)x^2 + (d_{-0} - d_1 - 3d_0)\, x + d_0 - d_{-0} = 0,$$

де $d_0 = R_M(p/2) - S_M(p/2)$, $d_1 = R_M(1-p/2) - S_M(1-p/2)$,
$d_{-0} = R_{-M}(p/2) - S_{-M}(p/2)$ $d_{-1} = R_{-M}(1-p/2) - S_{-M}(1-p/2)$.
Довжина прихованого повідомлення p обчислюється з меншого за абсолютним значенням кореня рівняння:

$$p = x/(x-1/2).$$

Прямі лінії визначають кількість R і S груп в p/2 і 1-p/2, а припущення, зроблені при виведенні залежностей (1) і (2), забезпечують достатню кількість обмежень для єдиного завдання парабол і їх перетинів (рис.5).

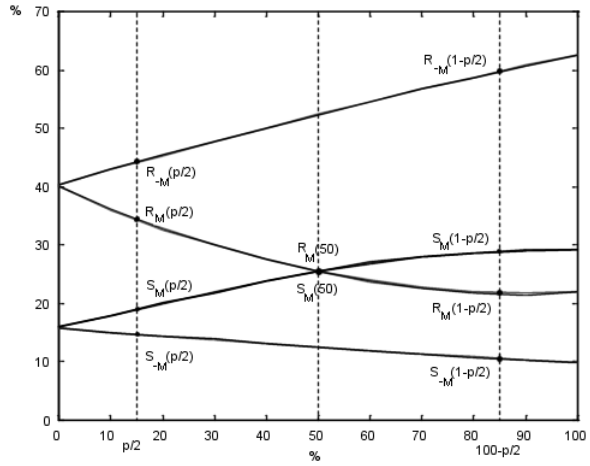

Рис. 5. RS-діаграма

Дослідження закономірностей у каналах кольорових зображень за методом RS-стегоаналізу

В результаті досліджень, проведених співробітниками ЦТОС ІК над 49678 зображеннями (табл. 2) (дві вибірки з 43598 і 6080 файлів), які доступні в Інтернеті, виявилось, що відсоток хибного визначення об'єму прихованого повідомлення для них вищий, ніж вказаний авторами патенту для фотографій з цифрових камер і сканерів.

На думку авторів, це пов'язано з тим, що над такими зображеннями було виконано обробку для підготовки до друку, яка включає високочастотну фільтрацію, підвищення яскравості і контрасту, вирівнювання значень гістограми і т.п. операції, які підвищують візуальну якість зображення. Це супроводжується збільшенням сингулярних груп у контейнері.

Також було помічено нерівномірне співвідношення варіацій значень RS-аналізу по каналам для кольорових зображень. Символами R, G, B позначено значення коефіцієнту, отриманого за RS-аналізом для червоно, зеленого та синього каналу відповідно. В результаті обчислень отримано наступні частоти появи нерівностей у відсотках.

Таблиця 2: Частоти появи нерівностей для двох вибірок

Вибірка 1			Вибірка 2		
	N	%		N	%
R>G>B	5867	13,46	R>G>B	980	16,12
R>B>G	7962	18,26	R>B>G	1152	18,95
G>R>B	3615	8,29	G>R>B	683	11,23
G>B>R	4110	9,43	G>B>R	666	10,95
B>R>G	9589	21,99	B>R>G	1158	19,05
B>G>R	8470	19,43	B>G>R	1032	16,97
R=G>B	448	1,03	R=G>B	52	0,86
B>R=G	1031	2,36	B>R=G	81	1,33
G=B>R	486	1,11	G=B>R	59	0,97
R>G=B	751	1,72	R>G=B	56	0,92
B=R>G	560	1,28	B=R>G	76	1,25
G>B=R	588	1,35	G>B=R	59	0,97
R=G=B	121	0,28	R=G=B	26	0,43

Видно, що нерівності, в яких RS-коефіцієнт більший у червоному або синьому каналі переважають за частотою появи інших.

У таблиці 3 наведено типові значення розмірів виявлених повідомлень у пустих контейнерах для зображень різних типів.

Таблиця 3: Типові відсотки значень розмірів повідомлень, виявлених RS-аналізом

Тип зображення	Відсоток хибних стегобіт у контейнері
Фотографії, скановані зображення	≈ 0-10%
Зображення з Інтернету або підготовлені до друку	≈ 15 ÷ 20 %
Дрібнотекстуровані, високо деталізовані зображення	≈ 30 ÷ 100%

Перелічені фактори суттєво знижують ймовірність виявлення прихованих даних навіть для класичної НЗБ-стеганографії, якщо відповідні програми використовуються підготовленими особами.

Висновки

Для сильно зачушлених і дрібно текстурованих зображень складно розрізнити випадковий процес штучного і фізичного походження. Встановлено, що для кольорових каналів характерне різне значення коефіцієнта, розрахованого за методом RS-стегоаналізу. Більш високі значення для блакитного каналу можна пояснити більш швидким релеєвським розсіюванням (поглинанням) синього спектру повітрям порівняно з іншими кольорами, що відображається як підвищення рівня зашумлення у синьому кольоровому каналі. На думку авторів, високі значення для червоного кольору пояснюються більш високою контрастністю [1] (детальністю), порівняно з іншими кольорами. Ширина спектра для червоного кольору якого є найширшою поміж трьох кольорів, а відносна ступінь поглинання є найменшою, оскільки з червоного починається спектр видимого світла. Найнижче відносне значення зафіксовано для зеленого кольору, який займає проміжне місце у спектрі між червоним і блакитним.

Отримані результати можуть бути використані для розробки нових методів зменшення рівня шумів, перевірки зображень на предмет застосування методів цифрової оброки та вбудовування сторонніх елементів, а також ідентифікації апаратних засобів реєстрації фотографій.

Література

[1] Корольов В.Ю., Поліновський В.В., Герасименко В.А. Стеганографічна персоналізація інформації на базі ПК // Вісті Академії інженерних наук України. - № 2(39). - 2009. - С. 18 - 24.

[2] Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. - К.: "МК-Пресс", 2006.- 288 с., ил.

[3] Digital Watermarking and Steganography / I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, T. Kalker, Morgan Kaufmann Publishers, second edition, 2008.

[4] United States Reissued Patent US RE40,477 E Reliable Detection of LSB Steganography in Color and Grayscale Images. Inventors: Jessica Fridrich, Miroslav Goljan. - Sep. 2, 2008.

[5] Корольов В.Ю., Поліновський В.В., Герасименко В.А. Дослідження стійкості НЗБ-стеганографії до RS-аналізу // Матеріали IV Міжнародної конференції "Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування (СПРТП - 2009)", [Частина 1]. — Вінниця: ВНТУ Мін. Освіти і науки України. — 2009. — С. 53.