УДК 004.056.53 (045)

# УДОСКОНАЛЕННЯ СТЕГАНОГРАФІЧНИХ МЕТОДІВ НА БАЗІ АНАЛІЗУ КОЛІРНИХ МОДЕЛЕЙ ЗОБРАЖЕННЯ

***О. К. Юдін***, д-р техн. наук, проф.; ***Я. А. Симониченко***

Національний авіаційний університет

e-mail: kszi@ukr.net

*У статті проведено дослідження методів підвищення стійкості стеганографічного контейнера до атак під час його передачі каналами зв'язку. Визначено основні характеристики фіксованого контейнера, а саме растрового зображення. Проведено аналіз найпоширеніших колірних моделей зображення. Запропоновано метод округлення значень елементів зображення для модифікації молодшого біту в задачах стеганографічного захисту. Наведено результати дослідження для обґрунтування вибору колірної моделі зображення у разі підвищення стійкості стеганографічної системи.*

**Ключові слова:** стеганографічна система, стеганоконтейнер, растрове зображення, колірна модель.

*In the article has carried out a research methods to improve the stability of steganographic container up to attacks in the time of its transmission of the channels of communication. The main features fixed container was defined, namely a raster image. The analysis of the most common color models images was carried out. A method of rounding meanings elements image for modification low bit was offered. Put the results of the research to justify for the choice of a color model image with increasing stability of steganographic systems.*

**Keywords:** steganographic systems, steganographic container, raster image, color model.

## Вступ

На сучасному етапі розвитку наукоємних технологій інформація є найціннішою як з семантичного погляду, так і з економічного. В сучасному суспільстві все більше виникає необхідність створення нових, більш надійніших методів захисту інформаційних ресурсів. Для розв'язання даної задачі варто використовувати технологію стеганографії. Ці методи дозволяють приховувати не тільки дані, але й факт їх наявності в інформаційних потоках при передачі каналом зв'язку.

Методи стеганографії дають змогу не лише приховано передавати інформацію, але й успішно розв'язувати задачі завадостійкої аутентифікації, захисту інформації від несанкціонованого копіювання, відстеження поширення інформації мережами зв'язку тощо [1].

Реалізація методів стеганографічного захисту призводить до створення спеціальних стеганографічних систем. Під стеганографічною системою слід розуміти об'єднання методів і засобів, які використовуються для створення прихованого каналу передачі інформації. Стеганографічна система виконує вбудовування повідомлення в контейнер, передавання заповненого контейнера стеганоканалом та декодування приховуваного повідомлення.

## Постановка задачі

Одним з основних етапів стеганосистеми є вбудовування повідомлення до контейнера для подальшого передавання по каналах зв'язку. Як контейнер для приховування та передавання повідомлення найчастіше використовуються нерухомі растрові зображення (фіксовані контейнери).

Важливими характеристиками контейнерів для розв'язання задач стеганозахисту є: розмір растру, роздільна здатність, глибина кольору та колірна модель. Зміна цих характеристик впливає на структурні ознаки контейнера. Для підвищення стійкості стеганосистеми необхідно прагнути якнайменше змінювати структурні ознаки базового контейнера [2].

Використання методів стеганографічного захисту інформації сприяло розвитку та застосуванню нового теоретичного напряму — стеганоаналізу. Метою стеганоаналізу є дослідження якісних та кількісних оцінок надійності стеганографічної системи, виявлення контейнера та розкриття тексту. Оптимальніший контейнер визначається рядом показників, що ґрунтуються на відмінностях між контейнером-оригіналом і контейнером-результатом.

Таким чином, **метою даної статті** є підвищення стійкості стеганоконтейнера на базі виявлення базових характеристик та аналізу колірних моделей зображення. На основі проведених досліджень буде визначено оптимальну колірну модель зображення в умовах реалізації процесів стеганозахисту.

## Розв'язання проблеми

Як фіксований контейнер для передавання прихованого повідомлення найчастіше використовуються нерухомі растрові зображення.

Растрове зображення — зображення, що являє собою матрицю пікселів на комп'ютерному моніторі, папері або інших пристроях і матеріалах.

Кожен піксель растрового зображення — об'єкт, що характеризується певним кольором,

яскравістю і, можливо, прозорістю. Один піксель може зберігати інформацію тільки про один колір, який і асоціюється з ним.

Пікселі у растровому зображенні розташовані по рядках і стовпцях.

Чим більше пікселів на одиницю площі містить зображення, тим вище його деталізація. Максимальна деталізація растрового зображення задається при його створенні і не може бути збільшена. Якщо збільшити масштаб зображення, ступінь деталізації при цьому не зростає. Забезпечення плавного переходу між початковими пікселями зумовлено додаванням нових, значення яких обчислюється на підставі значень сусідніх пікселів вихідного зображення [3].

Для опису розміщення пікселів використовують систему цілих координат — номерів пікселів з (0,0) у лівому верхньому куті.

Важливими характеристиками контейнерів є: розмір растру, роздільна здатність, глибина кольору та колірна модель.

**Роздільна здатність зображення.** Роздільна здатність растрового зображення вимірюється в пікселях на дюйм (ppi - pixels per inch). Чіткість зображення залежить від того, скільки пікселів розраховано на один дюйм для відтворення графічної інформації — чим більше пікселів, тим чіткіше зображення.

А роздільна здатність зображень, надрукованих на папері або іншому носії, вимірюється в точках на дюйм (dpi - dot per inch), оскільки найменшою часткою такого зображення є надрукована точка на аркуші паперу. Так, екран монітора здатний відображати 72 (а можливо, 96) пікселі на один дюйм по вертикалі та по горизонталі, тоді як зображення для друкування повинно містити 100 — 300 ppi.

Візьмемо два цифрових зображення із роздільною здатністю 72 та 300 ppi (рис. 1). Фізичний розмір цих зображень буде дорівнювати одному дюйму (2,54 см) по вертикалі та горизонталі. Якщо роздрукувати ці зображення на папері, при однакових фізичних розмірах, якість роздрукованого зображення буде різною.

Краща чіткість буде в зображення 300 ppi і гірша в 72 ppi.

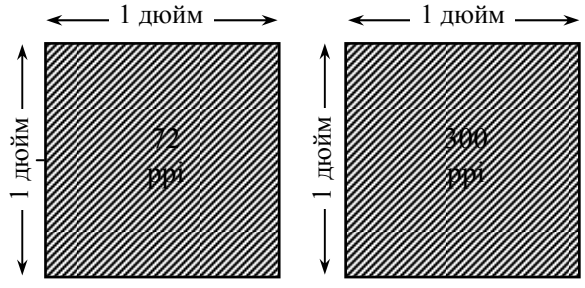


Рис. 1. Роздільна здатність з 72 та 300 ppi

При відтворенні цих зображень на екрані монітора відбудеться помітне збільшення розмірів зображення із 300 ppi (при 100 % масштабуванні). Збільшення відбудеться за рахунок того, що монітор відображає лише 72 пікселя на дюйм. Тобто кожна частина зображення 300 ppi буде збільшена до розміру в один дюйм відносно до екрану монітора.

На рис. 2 пунктирною лінією зображено ділянку в один квадратний дюйм екрану монітора, що відтворює 72 пікселі по горизонталі та по вертикалі. Розміри зображень будуть становити 72 та 300 пікселів по ширині та по висоті, для кожного зображення відповідно. При тому, що фізичний розмір зображень — 1 дюйм із роздільною здатністю в 72 та 300 dpi.

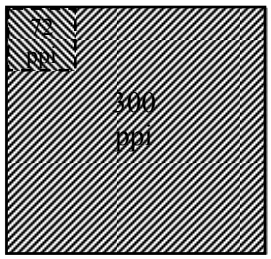


Рис. 2. Відображення 72 та 300 ppi на моніторі

**Розмір растру зображення.** Растр являє собою матрицю N x M пікселів (рис. 3), де N і M — піксельні розміри растру.

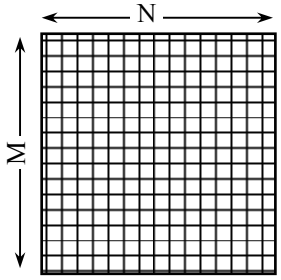


Рис. 3. Растр зображення

Розмір растрового зображення задається у вигляді двох цілих чисел, що визначають розміри зображення в пікселях по горизонталі та вертикалі, наприклад 640x480 (ширина — 640 пікселів, а висота — 480). У результаті зображення складається з 307 200 пікселів. Чим вище роздільна здатність та розмір зображення, тим вища деталізація зображення.

**Глибина кольору зображення.** Однією з важливих характеристик растрового зображення є глибина кольору. Згідно з психофізіологічним дослідженням око людини має здатність розрізнити 350 000 кольорів.

Для кодування кольору пікселя може бути виділено різну кількість біт. Від цього залежить кількість кольорів, що можуть відображатись на екрані одночасно. Чим більше довжина двійкового коду кольору, тим більше кольорів можна використовувати при відтворенні графічного об’єкта.

Глибина кольору — це кількість біт, яку використовують для кодування одного пікселя. Глибина кольору растрового зображення вимірюється в бітах на піксель (bits per pixel, bpp).

Класифікуємо зображення за глибиною кольору таким чином:

– бінарні зображення (бітове) — 1 біт на піксель;

– напівтонові — градації сірого або іншого кольору (1 байт на піксель);

– кольорові зображення. Два байти (16 bpp) дозволяють визначити 65 536 різних кольорів (режим — High Color). Якщо для кодування кольору використовуються 3 байти (24 bpp), можливе відображення 16,7 млн кольорів (режим — True Color).

У комп'ютерних графічних системах використовують і більшу глибину кольору — 32/48 bpp та ін.

Для зберігання і представлення бітового зображення використовується бітова карта, де на кожен піксель відводиться 1 біт інформації. Виділення одного байта (8 біт) дозволяє закодувати 256 різних колірних відтінків. Режим High Color розроблений для представлення відтінків «реального життя», тобто найбільш зручно сприймається людським оком.

32-бітний колір — це дійсний 24-бітний колір із додатковим 8-бітним каналом, який або заповнений нулями, або є Альфа-каналом, який задає прозорість зображення для кожного пікселя. Наприклад, для відображення ефекту напівпрозорих вікон, меню та тіней.

Причиною використання Альфа-каналу є прагнення оптимізувати роботу з відеопам'яттю, яка у більшості сучасних комп'ютерів має 32-бітну адресацію і 32-бітову шину даних.

**Колірні моделі растрового зображення.** Більшість відтінків утворюється шляхом змішування основних кольорів. Спосіб поділу колірного відтінку на складові називається колірною моделлю. Існує багато різних типів колірних моделей. Для розв'язання поставленої задачі, розглянемо такі колірні моделі — RGB, HSV та HLS.

**RGB.** У даній колірній моделі колір пікселя утворюється шляхом змішування трьох основних кольорів RGB-моделі.

Синтез кольору утворюється кодуванням градацій складових трьох каналів (Red, Green, Blue). Змішавши три базові кольори в різних пропорціях, можна отримати все різноманіття відтінків.

Ця модель подається у вигляді тривимірної системи координат.

Кожна координата (канал) відображає внесок складової в результуючий колір, який знаходиться в діапазоні від нуля до максимального значення. Усередині отриманого куба і знаходяться всі кольори, утворюючи колірний простір (рис. 4).

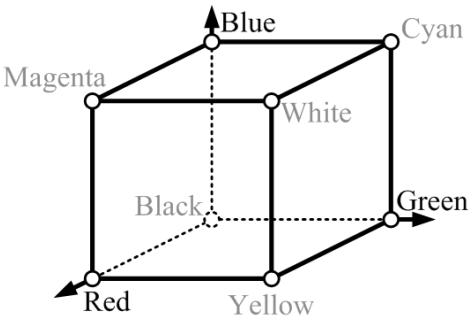


Рис. 4. Колірний простір RGB

Кількість градацій кожного каналу залежить від бітового значення RGB. Зазвичай використовують 24-х бітну модель, у котрій відведено по 8 біт на кожен канал, і тому кількість градацій становить від 0 до 255 (рис. 5).

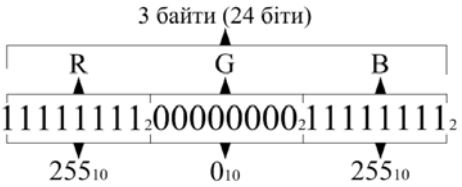


Рис. 5. 24-бітна RGB модель синтезу кольору

У моделі RGB центральна точка з координатами (0,0,0) має чорний колір. Білому кольору відповідають максимальні значення складових (255,255,255). Відповідно червоний — (255,0,0), зелений — (0,0,255) та синій — (0,0,255). Колірна модель RGB призначена відображати зображення в електронних системах, таких як телебачення, комп'ютери, фотографії та ін. [4].

**HSV.** HSV — модель, що описує колірний простір, який заснований на трьох характеристиках кольору: тоні (*Hue*), насиченості (*Saturation*), значенні яскравості (*Value* або *Brightness*). Колірний простір моделі HSV має конусне відображення (рис. 6).

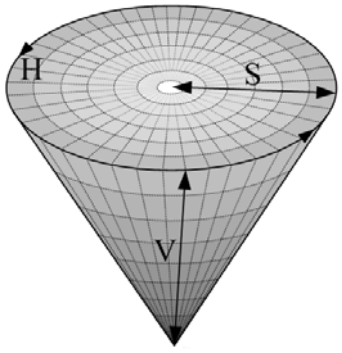


Рис. 6. Колірний простір HSV

Розглянемо більш детально колірний простір:

– тон кольору (спектральний колір) — характеризується позицією H на колірному колі та визначається величиною кута від 0 до 360°;

– насиченість (S) — це параметр, що визначає чистоту кольору. Насиченість змінюється в діапазоні від 0 до 100 %. На границі колірного кола розташовуються максимально насичені кольори (значення насиченості — 100 %). Колір із зменшенням S — освітлюється. При значенні S — 0 %, будь-який колір стає білим;

– яскравість (V або B) — це параметр кольору, який характеризує освітленість. Яскравість змінюється в межах від 0 до 100 %. Зменшення яскравості кольору відбувається шляхом додавання чорного кольору (затемнення кольору).

Колірну модель HSV використовують комп'ютерні художники під час створення зображень у графічних редакторах.

Після створення зображення, його треба перетворити на модель RGB або CMYK.

Перетворення моделі в RGB відбувається для відображення зображення на екрані монітора, а в CMYK — для отримання друкованого зображення.

**HLS.** HLS — це колірна модель, в якій координатами кольору є: *Hue* — тон кольору, *Lightness* — світліть та *Saturation* — насиченість.

У HLS колірний простір зображується у вигляді подвійного конуса (рис. 7), в якій по вертикальній осі відкладається L (світліть), а інші два параметри задаються так само, як і в попередній моделі.

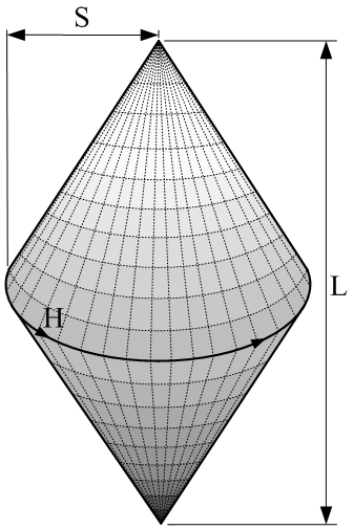


Рис. 7. Колірний простір HLS

Параметр світлості змінюється в межах від 0 до 100 %. Значенню 0 % відповідає вершина нижнього конуса і задає чорний колір.

Білий колір максимальної інтенсивності світла задається вершиною верхнього конуса і відповідає значенню 100 %.

Максимально інтенсивні колірні тони відповідають основам конусів з L = 50 %.

Для знаходження оптимальної колірної моделі при реалізації стеганозахисту, виконаємо порівняння зображень на основі показника коефіцієнта кореляції Пірсона, що визначається за формулою:

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{S_x^2}\sqrt{S_y^2}}, \qquad (1)$$

де $\bar{x}, \bar{y}$ — середні значення вибірки $x$ та $y$; $S$ — середньоквадратичне відхилення.

Під час дослідження колірних моделей зображення було використано 24-бітне зображення. Збереження зображення відбувалося у BMP-форматі, оскільки він є оптимальнішим форматом при виконанні стеганоперетворення [5]. Було використано три колірні моделі, а саме: RGB, HSV, HLS.

Інформація приховувалась методом модифікації молодшого біту елементу зображення. Для виконання дослідження, відбувалося заповнення кожної складової всіх трьох колірних моделей. Ступінь модифікації контейнера становив від 10 до 100 %.

Графічне відображення значень коефіцієнтів кореляції зображено на рис. 8. Як можна побачити, кращою компонентою для приховування даних у моделі RGB є синя компонента.

Коефіцієнт кореляції синьої компоненти залишається найбільшим при різних ступенях модифікації контейнера. Таким чином, синя компонента стійкіша до стеганоперетворення порівняно з іншими компонентами, червоною та зеленою.

Компонента насиченості — S є більш стійкішою до стеганоперетворення при використанні колірної моделі HSV (рис. 9). Оскільки вона має найвищий коефіцієнт кореляції в усіх випадках, порівняно із компонентами H і V. Таким чином, використання компоненти S є більш оптимальнішим при даній колірній моделі.

При дослідженні колірної моделі HLS, оптимальнішим для приховування даних є компонента S. Значення коефіцієнта кореляції, при використанні даної компоненти має найвище значення та становить 0,99999994, що є більш прийнятним для підвищення стійкості стеганосистеми, порівняно з іншими складовими компонентами даної моделі (рис. 10).

Після дослідження всіх трьох колірних моделей растрового зображення слід зазначити, що стійкішою є модель HLS, а саме компонента S, оскільки вона має найвищий коефіцієнт кореляції при різних ступенях заповнення, порівняно з іншими колірними моделями.

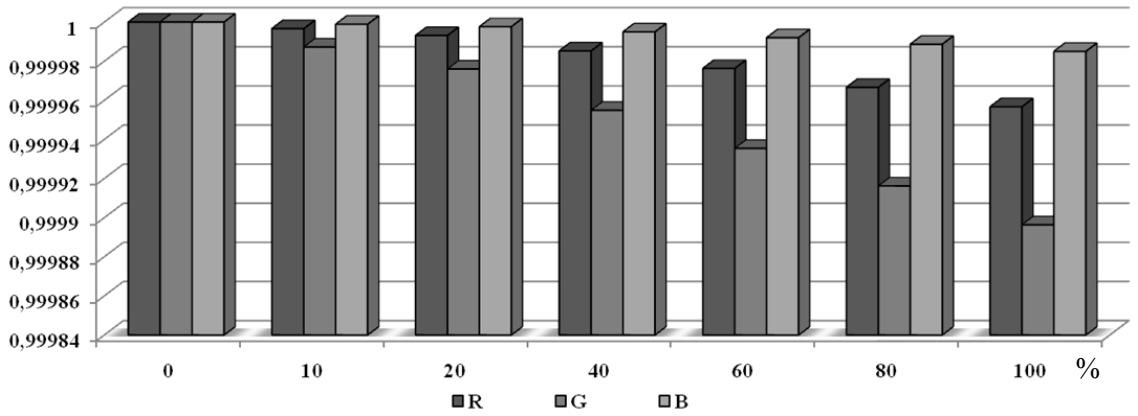


Рис. 8. Значення коефіцієнтів кореляції колірної моделі RGB залежно від ступеня заповнення

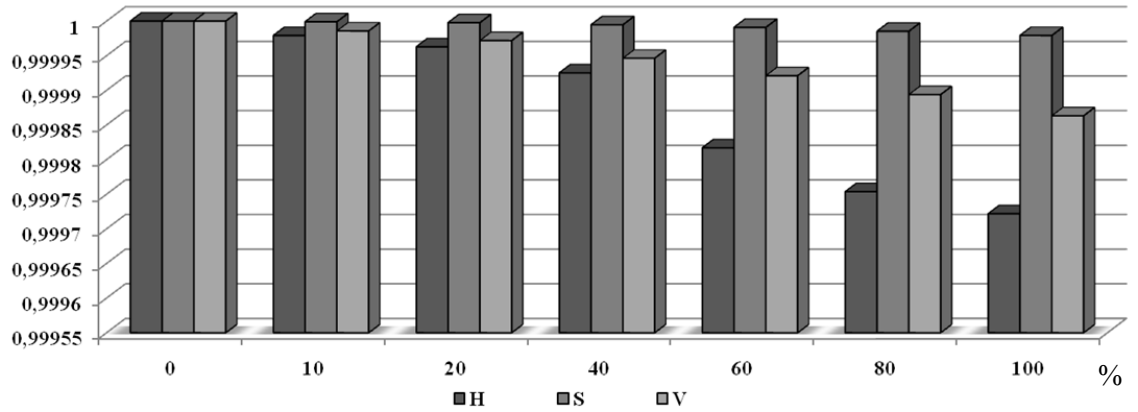


Рис. 9. Значення коефіцієнтів кореляції колірної моделі HSV залежно від ступеня заповнення

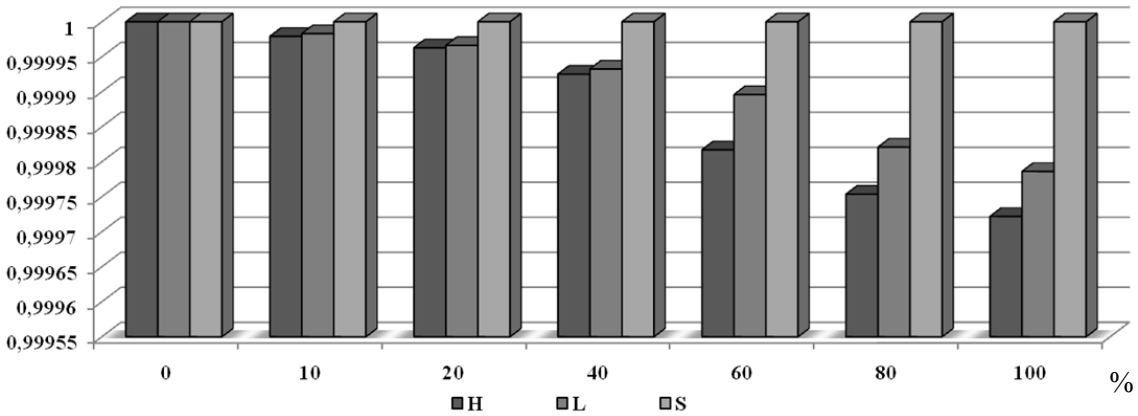


Рис. 10. Значення коефіцієнтів кореляції колірної моделі HLS залежно від ступеня заповнення

Як наслідок, використання даної компоненти підвищує стійкість стеганографічної системи до стеганоаналізу та надійність передачі стеганоповідомлення каналом зв'язку. Компонента насиченості колірної моделі HSV має меншу стійкість до стеганоперетворень, оскільки має менше значення коефіцієнта кореляції.

Компонента синього кольору моделі RGB є менш стійкішою, ніж компонента насиченості. Використання компоненти дещо зменшує стійкість стеганосистеми до стеганоаналізу. Але використання цієї моделі теж доречно під час приховування невеликого повідомлення.

Таким чином, для підвищення стійкості стеганосистеми слід використовувати модель — HLS. При використанні моделі HLS значення елементів компоненти виражено через десятковий дріб (рис. 11).

S =

| | 146 | 147 | 148 |
|---|---|---|---|
| 10 | 61.93 | 61.93 | 61.93 |
| 11 | 61.81 | 61.81 | 61.81 |
| 12 | 61.74 | 61.74 | 61.74 |
| 13 | 61.52 | 61.52 | 61.52 |

Рис. 11. Значення елементів компонентів насиченості

Під час проведення приховування даних кожне значення елементів відповідної компоненти переводиться у двійковий формат для модифікації молодшого біту бітом повідомлення, але перетворення у двійковий формат відбувається тільки цілої частини числа (рис.12, *а*), тому що у двійковому форматі немає дробової частини.

У разі використання двійкової системи кожен біт може набувати значень 0 або 1. Таким чином, чергування молодшого біту двійкових значень числової послідовності при послідовному зростанні відбувається почергово — 0, 1, 0, 1, 0, 1, 0, 1, … (рис.12, *б*)

$61.93_{10} \rightarrow 0011\ 1101_2$ $\quad 10_{10} \rightarrow 1010_2$

$61.81_{10} \rightarrow 0011\ 1101_2$ $\quad 11_{10} \rightarrow 1011_2$

$61.74_{10} \rightarrow 0011\ 1101_2$ $\quad 12_{10} \rightarrow 1100_2$

$61.52_{10} \rightarrow 0011\ 1101_2$ $\quad 13_{10} \rightarrow 1101_2$

*а* *б*

Рис. 12. Двійкове представлення значень:
*а* — компоненти насиченості в HLS моделі;
*б* — числової послідовності

Більш надійнішим буде застосування методу округлення значення елементів зображення в моделі HLS до наступної цілої частини значення цього елементу для зміни молодшого біту. Для порівняльного аналізу методів виконаємо модифікацію молодшого біту елементу зображення при використанні цілої частини. Для цього проведемо перетворення кожного значення елементів компоненти у двійковий вигляд. Після цього виконаємо зміну молодшого біту двійкового значення та зворотне перетворення в десяткове представлення (рис. 13, *а*).

$0011\ 1100_2 \rightarrow 60_{10}$ $\quad 61.93_{10} - 60_{10} = |1.93_{10}|$

$0011\ 1100_2 \rightarrow 60_{10}$ $\quad 61.81_{10} - 60_{10} = |1.81_{10}|$

$0011\ 1100_2 \rightarrow 60_{10}$ $\quad 61.74_{10} - 60_{10} = |1.74_{10}|$

$0011\ 1100_2 \rightarrow 60_{10}$ $\quad 61.52_{10} - 60_{10} = |1.52_{10}|$

*а* *б*

Рис. 13. Знаходження значень:
*а* — зміна молодшого біту та зворотне перетворення;
*б* — сума абсолютних значень різниць
кожних відповідних елементів

Розрахуємо суму абсолютних значень різниць кожних відповідних елементів до стеганоперетворення та після (рис. 13, *б*). Вона становить: 1,93 + 1,81 + 1,74 + 1,52 = 7.

Виконаємо аналогічне перетворення за допомогою методу округлення значень елементів складової компоненти растрового зображення для зміни молодшого біту. Округлення елементів виконаємо до наступної цілої частини (рис. 14, *а*).

Так для зміни молодшого біту числа 61,93 округлимо його значення до 62. Тоді, маємо: $62_{10} = 0011111\mathbf{0}_2$. Після цього отримаємо десяткові значення елементів з модифікованими молодшими бітами. Таким чином, сума абсолютних значень різниць елементів: 0,07 + 0,19 + 0,26 + + 0,48 = 1 (рис. 14, *б*).

$61.93_{10} \sim 62_{10}$ $\quad 61.93_{10} - 62_{10} = |0.07_{10}|$

$61.81_{10} \sim 62_{10}$ $\quad 61.81_{10} - 62_{10} = |0.19_{10}|$

$61.74_{10} \sim 62_{10}$ $\quad 61.74_{10} - 62_{10} = |0.26_{10}|$

$61.52_{10} \sim 62_{10}$ $\quad 61.52_{10} - 62_{10} = |0.48_{10}|$

*а* *б*

Рис. 14. Знаходження значень:
*а* — округлення елементів; *б* — сума абсолютних
значень різниць кожних відповідних елементів

Отже, використання першого методу здійснило зміну значень елементів зображення на сім одиниць, а сума різниць значень елементів після методу округлення значення елементів компоненти, становила 1. Використання методу округлення зменшує різницю значень елементів зображення-оригіналу із зображенням-результатом у даному випадку в сім разів.

**Висновок**

Таким чином, після проведення досліджень растрових зображень та порівняльного аналізу колірних моделей та їх особливостей слід зазначити, що для підвищення надійності стеганосистеми оптимальніше проводити вбудовування повідомлення в компоненту насиченості (S) моделі HLS, а сам процес вбудовування слід виконувати методом округлення значень елементів. Використання округлення дозволяє зменшити спотворення зображення (контейнера) після стеганоперетворення та підвищити стійкість стеганографічної системи до атак.

***ЛІТЕРАТУРА***

1. *Сердюк В.* Информационная безопасность автоматизированных систем предприятий / В. Сердюк // Бухгалтер и компьютер. — 2007. — № 1. — С. 56.

2. *Грибунин В. Г.* Цифровая стеганография. / *В. Г. Грибунин, И. Н. Оков, И. В. Туринцев*. — М. : Солон-Пресс, 2002. — 205 с.

3. *Порев В.* Компьютерная графика: учеб. пособие / В. Порев. — БВХ-Петрбург, 2004. — 432 с.

4. *Ватолин Д.* Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео / Д. Ватолин., А. Ратушняк, М. Смирнов, В. Юкин. — М. : ДИАЛОГ-МИФИ, 2002. — 384 с.

5. *Конахович Г. Ф.* Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. — К. : МК-Пресс, 2006. — 288 с.

Стаття надійшла до редакції 20.11.2011.