УДК 519.15:621

О. Різник, Б. Балич, Д. Скрибайло-Леськів, В. Парубчак
Національний університет “Львівська політехніка”,
кафедра автоматизованих систем управління

АВТОРСЬКИЙ ЗАХИСТ ГРАФІЧНИХ ЗОБРАЖЕНЬ ЗА ДОПОМОГОЮ ЧИСЛОВИХ В’ЯЗАНОК

Розглянуто представлення чисел на основі числових в'язанок для авторського захисту графічних зображень. Розроблена методика побудови кодових комбінацій чисел на основі теорії числових в’язанок, що дає можливість представлення кодових комбінацій чисел у вигляді монолітного коду. Для цих цілей використовується технологія на основі моделі числової лінійки-в'язанки, яка зводиться до заміни певних пікселів в зображенні, що дає змогу створювати ефективні алгоритмів кодування і декодування.

In the article presentations of numbers are examined on the basis of numerical bundles for author defence of graphic images. The developed method of construction of code combinations of numbers is on the basis of theory of numerical bundles, which enables presentation of code combinations of numbers as a monolithic code. For these aims technology is used on the basis of model of numerical line-bundle which is taken to replacement of certain pixels in an image, that allows to create effective algorithms of encoding and decoding.

Вступ

Широке застосування комп’ютерної техніки в різних сферах діяльності, бурхливий розвиток комп’ютерних мереж робить все більш актуальними питання захисту інформації від несанкціонованого доступу, оскільки наслідки цього можуть бути непередбачувані. Незважаючи на те, що захист інформації в комп’ютерних мережах пов’язаний із низкою комплексних заходів – як суто технічних, так і організаційних, без шифрування інформації неможливо побудувати надійну систему її захисту.

Сьогодні гостро стоїть питання збереження конфіденційності та авторського захисту інформації. Існують численні методи захисту інформації. Одним із надійніших є приховування тексту чи будь-якої іншої інформації в зображенні. Наприклад, це необхідно у випадку збереження авторства фотографій різних агентств на комп’ютерах та їх передавання по незахищених мережах. Ідея полягає у зміні відтінку кольору пікселів малюнка так, щоб візуально зміни в малюнку не були помітні. Цей підхід вельми непоганий, тому що визначити технологію приховування тексту досить складно, і він працює не лише з текстовою інформацією, але й із зображеннями. Це означає, що можна без особливих проблем в одне зображення помістити інше.

Технологія використання зображень як контейнера надає набагато ширші можливості, ніж текстові документи. При використанні графічних форматів з'являється можливість захована не лише текстових повідомлень, але й інших зображень і файлів. Єдиною умовою є те, що об'єм захованої інформації не повинен перевищувати розмір зображення-сховища.

Розглянемо новий підхід приховування інформацій у зображенні на основі теорії числових в’язанок.

Постановка проблеми

Зупинимося детальніше на графічних файлах як найпоширеніших сьогодні. Швидкий розвиток алгоритмів компресії зображень привів до зміни уявлень про саму техніку впровадження

секретної інформації. Пропонується вводити інформацію у найменші значущі біти для зменшення помітності для стороннього спостерігача.

Отже, метод найменшого значущого біта (НЗБ), це один з найпростіших методів цифрової стеганографії. Метод використовує утаєння даних із спотворенням контейнера, що засноване на особливостях людського сприйняття. Ідея методу полягає в наступному: якщо узяти картинку у форматі BMP (або, скажімо, як альтернативу 8 і більш - бітовий оцифрований звук), краще всього TrueColor, в 24-бітовому форматі і змінити молодші значущі біти кольору, то візуально це буде непомітно. Чому саме 24 біти? Існує такий важливий чинник, як об'єм контейнера - скільки всього можна втиснути в зображення, поки це не стане явним. Логічно передбачити, що чим більший контейнер, тим більше він може вмістити, а поширені сьогодні 24-бітові файли BMP – найпридатніші. У цьому форматі під кожну точку зображення відводиться три байти (див. рис. 1), в кожному з яких зберігається інформація про червону, зелену і синю складові (разом 3x8=24 біти).

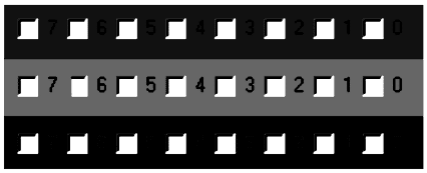


Рис. 1. Складові кольору 24-бітового формату BMP

Секретне повідомлення, наприклад, авторський підпис, додають так:

• беруть повідомлення, заздалегідь шифрують і архівують його. Цим досягається відразу дві мети – зменшення розміру і збільшення стійкості системи.

• беруть контейнер і впроваджують оброблене в першому пункті повідомлення в його байтовий контекст.

Так розкладаємо упаковане повідомлення в бітову послідовність; замінюємо надлишкові біти контейнера бітами повідомлення за деяким алгоритмом. Ось в цьому місці існуючі алгоритми припускає помилки. Надійність подібного впровадження сильно залежить від характеру розподілу змінених бітів у контейнері і в повідомленні. І переважно ці розподіли не є рівномірними за різними бітами. А на картинках, побудованих із застосуванням двійкових кодів, у молодших бітах буде приблизно рівномірний розподіл “0” та “1” і таке впровадження буде помітне навіть на око, якщо відкинути чотири старші біти. Замість оригінального зображення з чотирьох молодших бітів буде зашумлене зображення. Існують спеціальні програми, які аналізують зображення на наявність прихованої інформації. Авторський захист графічних зображень за допомогою комбінаторних моделей типу числової лінійки-в’язанки дозволяє обійти виявлення спеціальними програмами. Тому важливою задачею є вибір розподілу змінених бітів.

Розв’язання задачі

Пропонується застосувати для розподілу змінених бітів комбінаторну модель числової лінійки-в’язанки (ЧЛВ). Числова лінійка-в’язанка (ЧЛВ) з параметрами (S_n, n, r) – це алгебраїчна структура, утворена на послідовності n цілих додатних чисел, значення яких, як і значення сум поруч розміщених між собою чисел, вичерпують числа натурального ряду не більше одного разу $(r=1)$. Елементи ЧЛВ розташовані один біля одного у вигляді ланцюжка, і їх сума дорівнює S_n [2–4].

ЧЛВ являє собою максимальну комбінаторну різноманітність системи цілих чисел $k_1, k_2, ..., k_n$, які підлягають операції арифметичного додавання з обмеженням на правило їх додавання: додавати можна лише поруч розташовані числа. Якщо числа розміщені у вигляді

ланцюжка, розглядаємо ланцюжкову структуру, яка характеризується таким числовим набором елементів (1):

$$\begin{gathered} k_1,\ k_2,\ ...,\ k_n; \\ k_1 + k_3,\ k_2 + k_3,\ ...,\ k_{n-1} + k_n; \\ k_1 + k_2 + k_3,\ k_2 + k_3 + k_4,\ ...,\ k_{n-2} + k_{n-1} + k_n; \\ k_1 + k_2 + ... + k_n. \end{gathered} \tag{1}$$

Розв'язання такої задачі зводиться до пошуку оптимального комбінаторного варіанта ваг розрядів ланцюжка, при якому будь-яке натуральне число можна було б подати єдино можливим способом [2–4].

Числова лінійка-в'язанка порядку N кратності R характеризується: числом N елементів $k_1,k_2,..,k_i,..,k_N$; відповідно до (1) сумою елементів $L_N^R = \sum_{i=1}^{N} k_i$; діапазоном числових значень з початком з числа a; максимальним числом n з діапазону реалізації підряд розміщених значень $1,2,...,n < L_N$ з кратністю R; загальною кількістю способів реалізації сум K на ЧЛВ N-го порядку R-ї кратності [4]

$$K = \frac{N(N+1)}{2}; \tag{2}$$

коефіцієнтом повноти

$$k_p = \frac{n}{K}; \tag{3}$$

коефіцієнтом компактності

$$k_k = \frac{K}{L_N^R}; \tag{4}$$

коефіцієнтом заповнення

$$k_z = \frac{N}{L_N^R}. \tag{5}$$

За допомогою коефіцієнта повноти k_p оцінюють ефективність ЧЛВ з погляду діапазону відтворення найдовшого ряду числових значень сум стосовно ідеальної ЧЛВ. У загальному випадку при $R \geq 1$ коефіцієнт повноти згідно з (2) та (3) визначається формулою

$$k_p = \frac{2n}{N(N+1)}. \tag{6}$$

Коефіцієнт компактності k_k дає можливість оцінити ЧЛВ мінімальної довжини з погляду величини її суми стосовно ідеальної ЧЛВ при заданих N і R. У загальному випадку при $R \geq 1$ коефіцієнт компактності k_k згідно з (4) визначається формулою

$$k_k = \frac{K}{\frac{\frac{N(N+1)}{2} - 1}{R} + 1}. \tag{7}$$

Коефіцієнт заповнення k_z дає змогу оцінити заповнення елементами одно- і багатовимірних ЧЛВ заданих розмірів. Для одновимірних ідеальних ЧЛВ при $R \geq 1$ коефіцієнт заповнення згідно з (5) визначається формулою

$$k_z = \frac{2}{N+1}. \tag{8}$$

Для ідеальних ЧЛВ верхня межа діапазону реалізації послідовно зростаючих значень $n = K$, коефіцієнт повноти $k_p = 1$ і коефіцієнт компактності $k_k = 1$.

Оскільки ми кодуємо таблицю кодів ASCII, яка містить 256 варіантів, а в'язанки з сумою, яка дорівнює 256, не існує, то необхідно використовувати ЧЛВ з більшою сумою, наприклад, ЧЛВ (283, 20, 1) [1, 3, 4].

За вхідними даними складаємо таблицю кодів. Вона складається з масиву, кожен елемент якого має вигляд (0, 0, .., 0, 0) за таким принципом:

• беремо порядковий номер символу заданого алфавіту, якщо цей номер наявний серед елементів в'язанки, то в елемент масиву, в позицію потрібного елементу в'язанки, пишеться “1”;

• якщо заданий порядковий номер в таблиці не знайдений, то “1” пишуть в позиції елементів в'язанки, які в сумі дають потрібний номер (треба пам'ятати, що підсумовування проводиться за правилами, визначеними для ЧЛВ).

Після того проводиться посимвольне зчитування вихідної інформації з файла, потім визначається номер зчитаного символу в заданому алфавіті, визначається код, який відповідає даному номеру і записується в проміжний файл. Код з проміжного файла додають послідовно в наймолодші біти RGB файла BMP.

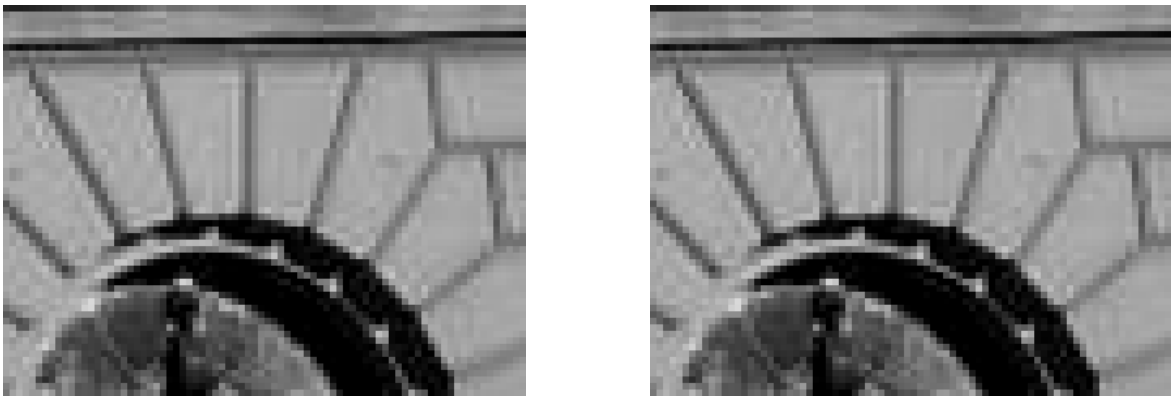
Щоб декодувати таке зображення необхідно з послідовності символів молодших бітів RGB файлу BMP вирахувати оригінальні значення молодших бітів RGB файлу BMP, після того відповідно до порядку n ЧЛВ зчитати послідовності по n символів. Для зчитаних n символів шукаємо в таблиці кодів ЧЛВ який символ ASCII алфавіту був закодований і отримуємо файл результату.

Наведемо приклад авторського захисту інформації. На рис.2 а представлений оригінальний графічний файл формату BMP зображення головного корпусу Національного університету ”Львівська політехніка”, а на рис.2 б – цей самий графічний файл формату BMP з авторським захистом, де в ролі ”ключа” є текст цієї статті.

а *б*

Рис. 2. Графічні файли BMP

На рис.3 а,б представлені відповідно збільшені фрагменти оригінального графічного файла формату BMP та графічного файла формату BMP з авторським захистом, де в ролі ”ключа” є текст цієї статті.



а *б*

Рис. 3. Збільшені фрагменти графічних файлів BMP

Висновки

Отже, представлена можливість авторського захисту графічних зображень за допомогою ЧЛВ моделей, створення ефективних алгоритмів кодування і декодування. Дослідження моделей і методів комбінаторної оптимізації розширює сферу практичних застосувань моделей числових лінійок-в'язанок у задачах інформаційної техніки і проектування надійних систем кодування [5].

1. Дурняк Б.В., Різник О.Я., Різник В.В., Кісь Я.П., Парубчак В.О. Захист даних методом комбінаторної оптимізації // Праці третьої міжнародної наукової конференції ISDMIT'2007, м. Євпаторія. – Т.2. – С.152–153. 2. Різник В.В. Синтез оптимальних комбінаторних систем. - Львів, 1989. 3. Різник О.Я. Завадостійкий спосіб перетворення сигналів // Матеріали Четвертої укр. конф. з автоматичного керування ("Автоматика-97"), Черкаси. – 1997. – С.34. 4. Різник О.Я., Парубчак В.О., Скрибайло-Леськів Д.Ю. Використання числових в'язанок для кодування інформації // Праці міжнародної конференції "Сучасні комп'ютерні системи та мережі: розробка та використання" (ACSN'2007). – С.112–114. 5. Різник О.Я., Парубчак В.О., Скрибайло-Леськів Д.Ю. Кодування інформації за допомогою монолітного коду // Праці 2-ї Міжн. наук.-практ. конф. "Інформаційні технології в наукових дослідженнях і навчальному процесі". – Луганськ, 2007. – Т.2. – С.88–92.