

Алі Енверович Бекіров (кандидат технічних наук)¹

Володимир Жоржєвич Яценюк (кандидат технічних наук, доцент)¹

Олександр Станіславович Крейдун²

¹Харківський національний університет Повітряних Сил ім. Івана Кожедуба, Харків, Україна

²Національний університет оборони України імені Івана Черняхівського, Київ, Україна

СТЕГАНОГРАФІЧНИЙ МЕТОД НА ОСНОВІ БЕЗПОСЕРЕДНЬОГО ТА НЕПРЯМОГО ВБУДОВУВАННЯ ДАНИХ ДЛЯ ОБЛАСТЕЙ ЗОБРАЖЕННЯ З РІЗНОЮ НАСИЧЕНІСТЮ

В сучасних умовах обстановки та під час проведення стабілізаційної операції об'єднаних сил Повітряні Сили України є одним з головних носіїв бойового потенціалу Збройних Сил України.

Здійснено аналіз тенденцій впровадження цифрових технологій скритного управління та передачі даних в Збройних Силах Повітряних Сил України під час побудови сучасної системи управління військами. На сьогоднішній день, крім створення нових зразків авіаційної техніки, активно виконується модернізація існуючого бортового радіоелектронного обладнання.

Метою даної статті є розробка стеганографічного методу на основі сумісного використання безпосереднього і непрямого вбудовування даних. В даній статті автори розглядають особливості використання стеганографічних методів для приховування інформації в умовах сучасного збройного протистояння. Сформовано вимоги до стеганографічного методу, які полягають у мінімізації та розподіленні спотворень вихідного зображення-контейнера в результаті вбудовування інформації. Визначено основні вимоги при розробці методу непрямого вбудовування. Розроблений метод непрямого стеганографічного вбудовування, який полягає у модифікації робочих елементів блоку відносно еталонної точки по трьом рівням. Створено систему прямого та зворотного стеганографічного перетворення на основі розробленого методу непрямого вбудовування.

Ключові слова: стеганографічна система, найменш значимий біт, непряме стеганографічне вбудовування

Вступ

Сучасний інформаційний простір характеризується наявністю викликів і загроз. В першу чергу це пов'язано з постійним підвищенням значимості інформації і розширенням областей використання інформаційних систем. Також, на вразливість безпеки інформаційних ресурсів впливає постійне покращення існуючих і створення нових програмних і апаратних засобів для здійснення атак [1, 6].

Постановка проблеми. Найбільш опрацьованими і часто використовуваними на практиці підходами забезпечення інформаційної безпеки є методи гарантованого захисту на основі криптографічних алгоритмів. Однак, такі підходи мають деякі обмеження. Це обумовлено тим, що криптографічно перетворені повідомлення, які передаються по телекомунікаційних мережах, виділяються противником. Іншими словами, противнику стає відомим факт передачі приховуваного повідомлення при відсутності доступу до самої інформації. Перехоплені противником «закриті» повідомлення можуть бути систематизовані і піддаватися аналізу з метою отримання інформації обмеженого доступу [2].

Для усунення наведених обмежень можуть використовуватися стеганографічні підходи для приховування інформації. Такі методи дозволяють непомітно вбудовувати інформацію в нейтральні

контейнери, які не привертають увагу. У якості контейнера можуть використовуватися текстові файли, аудіо та відео дані, а також цифрові зображення. На сьогоднішній день, найбільш поширеними є стеганографічні методи вбудовування на основі використання статичних та динамічних зображень в якості контейнерів [3, 5].

Аналіз останніх досліджень і публікацій. Стеганографічні підходи можна розділити на методи непрямого і безпосереднього вбудовування, які представлені великою кількістю існуючих алгоритмів. Загальними недоліками для них є:

- обмеження за обсягом вбудованих даних;
- внесення значних спотворень в контейнер;
- необхідність наявності ключа для вилучення інформації на приймальній стороні.

Можливим підходом для усунення виявлених недоліків, а саме забезпечення збільшення обсягу вбудованої інформації одночасно з забезпеченням заданого рівня внесених в контейнер спотворень є паралельне використання непрямого і безпосереднього підходу при вбудовуванні додаткової інформації.

Для цього необхідно забезпечити виділення двох груп областей: для непрямого і безпосереднього вбудовування. В якості алгоритму безпосереднього вбудовування

пропонується використовувати метод найменш значущого біту (НЗБ). Даний метод забезпечує приховування 1 біту даних в кожному елементі просторового представлення контейнера, незалежно від його значення. У той же час пропонується розробити непрямий метод вбудовування для областей з незначними змінами елементів [4, 7].

Для цього необхідно забезпечити виділення двох груп областей: для непрямого і безпосереднього вбудовування. В якості алгоритму безпосереднього вбудовування пропонується використовувати метод найменш значущого біту (НЗБ). Даний метод забезпечує приховування 1 біту даних в кожному елементі просторового представлення контейнера, незалежно від його значення. У той же час пропонується розробити непрямий метод вбудовування для областей з незначними змінами елементів [4, 7].

Метою статті є розробка стеганографічного методу на основі сумісного використання безпосереднього і непрямого вбудовування даних.

Виклад основного матеріалу дослідження

Сформулюємо вимоги, яким повинен задовольняти стеганографічний метод непрямого вбудовування:

1. Мінімізація внесених спотворень. Вбудовування не повинно супроводжуватися зміною значень елементів просторово-часового представлення контейнера більш ніж на визначене значення k (коефіцієнт модифікації). Для забезпечення мінімальної візуальної помітності стеганографічного вбудовування, необхідно виконати умову, яке задається наступним виразом $k \rightarrow \min$.

2. Розподіл внесених спотворень між елементами зображення-контейнера, які беруть участь в стеганографічному перетворенні. Дана вимога задається наступним виразом:

$$a^{(\tau)} = a^{(\tau)} + \Delta k, \quad \text{де} \quad \Delta k = \frac{k}{T},$$

де $a^{(\tau)}$ - τ - тий модифікований елемент зображення-контейнера, $\tau = \overline{1, T}$; $a^{(\tau)}$ - елемент $a^{(\tau)}$, модифікований в результаті стеганографічного вбудовування. Виконання даної умови забезпечить «плавну» модифікацію елементів на величину Δk . Графічна інтерпретація даної умови представлена на рис. 1.

Розглянемо масив (блок) A елементів $\{a_{i,j}\}$ зображення контейнера рис.2., де $a_{i,j}$ - елемент i -го рядка j -го стовпця блоку A , $i = \overline{1, n}$; $j = \overline{1, m}$.

Елементи $\{a_{i,j}\}$ просторово-часового представлення блока, характеризуються змінами значень елементів просторового уявлення. Іншими словами динамічний діапазон ψ значень елементів

$\{a_{i,j}\}$ рядків i стовпців в блоці A може набувати різних значень:

$$\psi_i = a_{i,\max} - a_{i,\min} = 0...255;$$

$$\psi_j = a_{j,\max} - a_{j,\min} = 0...255.$$

При цьому ψ_i і ψ_j динамічний діапазон відповідно i - го рядка, j - го стовпчика елементів блоку A ; $a_{i,\max}$ і $a_{i,\min}$ відповідно максимальне та мінімальне значення елементів i - го рядка блоку A ; $a_{\max,j}$ і $a_{\min,j}$ відповідно максимальне і мінімальне значення елементів j -го стовпця блоку A [8, 9].

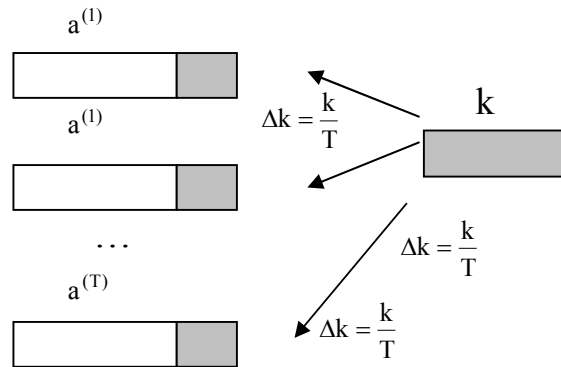


Рис 1. Графічна інтерпретація умови розподілу спотворень.

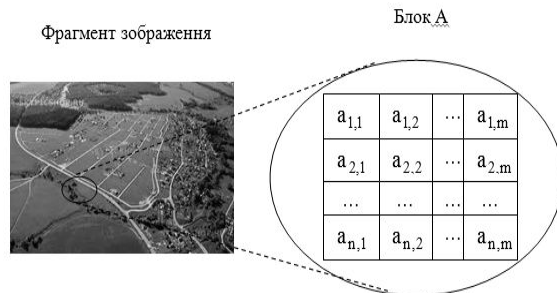


Рис 2. Формування блоку A елементів.

Вимоги до мінімізації спотворень обумовлені наступними аспектами. По-перше, непряме вбудовування передбачає модифікацію одних елементів блоків просторового представлення зображення і залишення без змін інших. По-друге, для забезпечення мінімальних спотворень в результаті вбудовування, необхідно щоб елементи блоків зображення мали мінімальний перепад значень між елементами в блоці. Графічно дану умову можна представити як зображено на рис 3.

Непряме стеганографічне вбудовування буде здійснюватися шляхом створення залежності між елементами $\{a_{i,j}\}$ блоку A . Метод передбачає як модифікацію елементів блоку A , так і взаємного розташування модифікованих елементів. Для створення методу непрямого вбудовування необхідно обґрунтувати правило виділення областей зображення для непрямого і безпосереднього вбудовування.

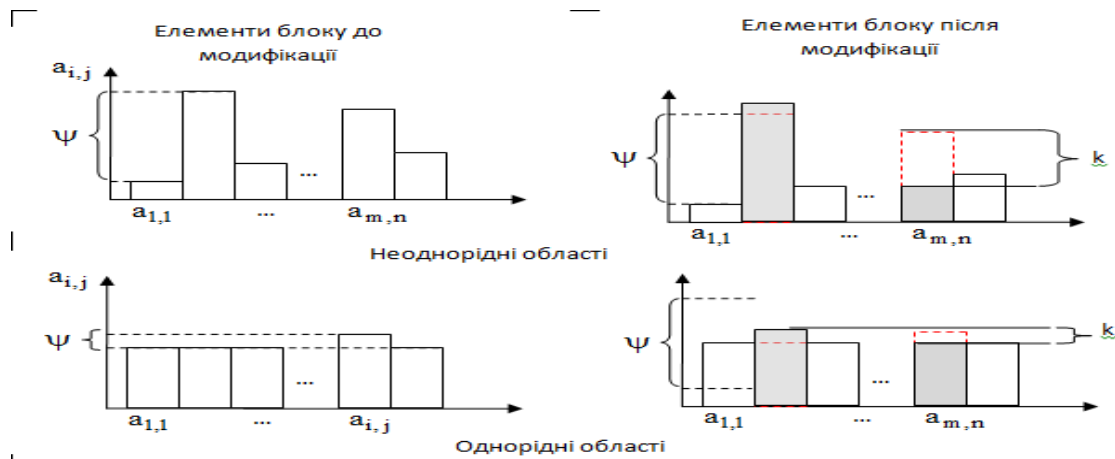


Рис. 3. Графічна інтерпретація модифікації областей з різною насиченістю.

Розробка методу непрямого стеганографічного вбудовування

Для визначення блоку зображення, який потенційно можливо використовувати для стеганографічного вбудовування на основі розробленого методу пропонується **правило**: при розбитті вихідного зображення-контейнера на робочі блоки для кожного блоку пропонується обчислити значення динамічного діапазону його рядків і стовпців. В цьому випадку якщо:

значення динамічних діапазонів рядків ψ_i і стовпців ψ_j блоку А приймає значення від 0 до 2

$$\psi_i = \overline{0, 2} \quad \text{і} \quad \psi_j = \overline{0, 2},$$

то зворотній блок використовується для непрямого стеганографічного вбудовування на основі запропонованого методу;

значення динамічних діапазонів рядків ψ_i і стовпців ψ_j блоку А приймає значення більше чим два

$$\psi_i > 2 \quad \text{і} \quad \psi_j > 2,$$

при цьому розглянутий блок не придатний для непрямого стеганографічного вбудовування і перетворюється на основі методу найменш значущого біту (НЗБ).

Наступний етап передбачає вибір в блоці А еталонного елемента $a_{i,j}^{(\sigma)}$ на основі правила. Даний елемент служить для визначення рівня модифікації інших елементів $\{a_{i,j}^{(\tau)}\}$ (робочих точок). Еталонний елемент $a_{i,j}^{(\sigma)}$ будемо називати еталонною точкою.

Оцінимо кількість інформації, яку можливо вбудувати в блок А розміром $n \times m$ елементів за умови виконання наступних вимог:

1) кількість робочих модифікуємих точок приймає значення $\tau = 1, (n \cdot m) - 1$;

2) рівень k спотворень, який вноситься в результаті модифікації робочих точок $\{a_{i,j}^{(\tau)}\}$, повинен приймати мінімальне значення, а саме:

$$a_{i,j}^{(\tau)} = a_{i,j}^{(\sigma)} \pm k \quad \text{при} \quad k \rightarrow \min.$$

Тоді рівень спотворень буде приймати значення $k \in [-1, 0, 1]$. У цьому випадку кількість варіантів модифікації однієї робочої точки $a_{i,j}^{(\tau)}$ буде дорівнює трьом, а саме:

- 1 варіант $a_{i,j}^{(\tau)} = a_{i,j}^{(\sigma)} - k = a_{i,j}^{(\sigma)} - 1 = a_{i,j}^{(\sigma)} - 1$;

- 2 варіант $a_{i,j}^{(\tau)} = a_{i,j}^{(\sigma)} + k = a_{i,j}^{(\sigma)} + 0 = a_{i,j}^{(\sigma)}$;

- 3 варіант $a_{i,j}^{(\tau)} = a_{i,j}^{(\sigma)} + k = a_{i,j}^{(\sigma)} + 1 = a_{i,j}^{(\sigma)} + 1$.

Для збільшення обсягу вбудованої інформації при одночасному забезпеченні заданого рівня спотворень пропонується підхід варіації позиції робочих точок. Багатопозиційна варіація передбачає зміну позиції робочих точок в блоці зображення відповідно до вбудованого повідомлення В. Розглянемо блок зображення А розміром $n \times m$. Кількість Z елементів блоку А, які можуть бути модифіковані, визначаються на основі виразу:

$$Z = n \cdot m - 1.$$

Цей вираз характеризує загальну кількість елементів в блоці, за винятком еталонного елемента.

Оцінимо кількість інформації, яку можна вбудувати в блок А розміром $n \times m$ на основі багатопозиційної варіації. Якщо корисне повідомлення $B = \{b_1, b_2, \dots, b_\xi, \dots, b_\Xi\}$ поелементно вбудовується в трикутому вигляді, тобто $b_\xi \in [0, 1, 2]$. Тоді кількість елементів $d_{\text{бл}}$, яку можна вбудувати в блок А буде визначатися відповідно формули:

$$d_{\text{бл}} = \log_3 3^{n \cdot m - 1}.$$

Розглянемо блок А розміром 3×3 . Позицію еталонної точки пропонується вибирати на основі наступного правила:

1) позиція компаративної точки $a_{i,j}^{(\sigma)}$ в рядку вибирається на основі виразу:

$$i = \left[\frac{n}{2} + 1 \right];$$

2) позиція j компаративної точки $a_{i,j}^{(\sigma)}$ в стовбці вибирається на основі виразу:

$$j = \left[\frac{m}{2} + 1 \right].$$

У цьому випадку еталонна точка буде мати вигляд $a_{2,2}^{(\sigma)}$. Навпаки, робоча точка може приймати будь-яку позицію за виключенням позиції еталонної точки $a_{2,2}^{(\sigma)}$ (рис 4).

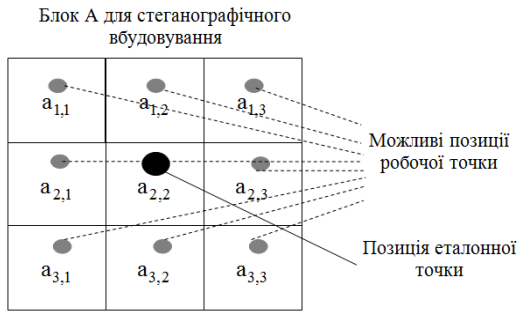


Рис 4. Позиції робочої та еталонної точки в блоці.

Розглянемо етап стеганографічного вбудовування. Даний етап передбачає зміну значення робочої точки $a_{i,j}^{(\tau)}$ відносно значення еталонного елемента $a_{2,2}^{(\sigma)}$ за таким правилом:

$$a_{i,j}^{(\tau)} = \begin{cases} a_{2,2}^{(\sigma)} - 1, & b_{\xi} = 0; \\ a_{2,2}^{(\sigma)}, & b_{\xi} = 1; \\ a_{2,2}^{(\sigma)} + 1, & b_{\xi} = 2, \end{cases}$$

де $a_{i,j}^{(\tau)}$ модифікований елемент $a_{i,j}^{(\tau)}$ вихідного зображення відповідно до правила непрямого вбудовування; b_{ξ} - вбудований елемент. Для забезпечення мінімальних спотворень при непрямому вбудовуванні необхідно щоб значення еталонного елемента дорівнювало значенням інших робочих точок - це ідеальні умови.

Але у реалістичних зображеннях значення деяких елементів мають імпульсну природу. Тому елемент робочого блоку на позиції еталонної точки пропонується піддавати медіанній фільтрації за формулою:

$$a_{2,2}^{(\sigma)} = \left\lfloor \frac{\sum_{i=1}^m \sum_{j=1}^n a_{i,j}^{(\tau)}}{n \cdot m} \right\rfloor.$$

Враховуючи, що сучасні цифрові пристрої працюють виключно в двійковій системі, етап попередньої обробки вбудованого повідомлення передбачатиме перетворення вбудованого двійкового повідомлення у повідомлення трійкового вигляду. У цьому випадку на позиції 8 робочих точок в трійковій системі можна вбудувати 13 біт даних в двійковій системі. На рис. 5 представлена схема розробленого методу прямого та на рис. 6 зворотного стеганографічного перетворення.

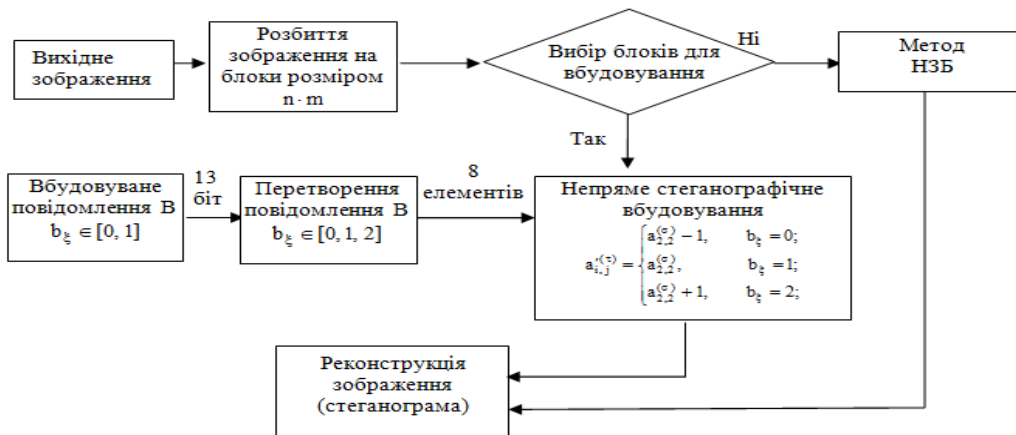


Рис. 5. Схема системи прямого стеганографічного перетворення.

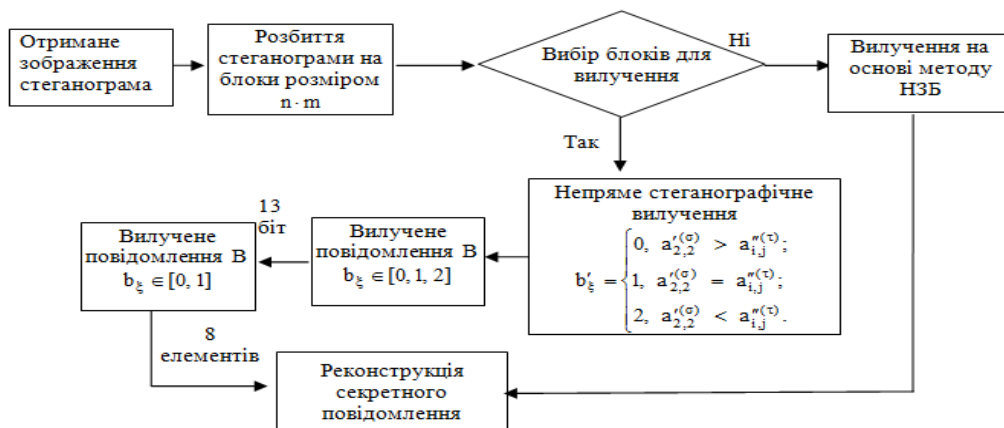


Рис.6. Схема системи зворотного непрямого стеганографічного перетворення.

Використовуючи запропонований метод спільного використання безпосереднього і непрямого підходу, на практиці можливо стеганографічно вбудувати в блок зображення розміром 9×9 елементів наступну кількість інформації:

9 біт на основі методу НЗБ;

13 біт на основі розробленого методу непрямого вбудовування.

Метод зворотного стеганографічного перетворення передбачає непряме вилучення вбудованих даних на основі порівняння еталонної і робочих точок обраних блоків.

Дане порівняння буде здійснюватися за таким правилом:

$$b'_{\xi} = \begin{cases} 0, & a'_{2,2}(\sigma) > a''_{i,j}(\tau); \\ 1, & a'_{2,2}(\sigma) = a''_{i,j}(\tau); \\ 2, & a'_{2,2}(\sigma) < a''_{i,j}(\tau), \end{cases}$$

де b'_{ξ} відновлене значення вбудованого елемента b_{ξ} , $a'_{2,2}(\sigma)$ - значення еталонної точки в блоці стеганограми, $a''_{i,j}(\tau)$ - робоча точка в i -му рядку j -ому стовпці стеганограми.

У випадку неавторизованого доступу у зловмисника відсутня інформація про наявність у стеганограмі прихованого повідомлення. У той же час рівень спотворень, які вносяться в результаті вбудовування є візуально не помітними, що дозволяє використовувати запропонований метод

стеганографічного вбудовування для створення прихованого каналу передачі даних.

Висновки і перспективи подальших досліджень

Проведено аналіз підходів для захисту інформації на основі стеганографії. Виявлені слабкі сторони методів безпосереднього та непрямого стеганографічного вбудовування. Для усунення виявлених недоліків пропонується підхід, який полягає у одночасному використанні непрямого та безпосереднього вбудовування в рамках одного методу із селекцією однорідних та насичених областей зображення.

Сформовано вимоги до методу, які полягають у мінімізації та розподіленні спотворень вихідного зображення-контейнера в результаті вбудовування інформації. Сформульовано правило визначення областей для непрямого стеганографічного вбудовування.

Розроблено метод непрямого стеганографічного вбудовування, який полягає у модифікації робочих елементів блоку відносно еталонної точки на трьох рівнях. Сформульовано правило підбору позиції еталонної точки в блоці.

Створено систему прямого та зворотного стеганографічного перетворення на основі розробленого методу непрямого вбудовування. Відмінною рисою системи є одночасне використання для вбудовування розробленого методу та методу НЗБ для областей з різною насиченістю.

Література

1. Аграновски А.В. Стеганография, цифровые водяные знаки и стегоанализ [Тест]: учеб. пособие для вузов / Аграновски А.В., Балакин А.В., Грибунин В.Г. – М.: Вузовская книга, 2009. – 220 с. **2. Бекіров А.Е.** Метод захисту інформації на основі стеганографічних систем // Озброєння та військова техніка. – 2015. - №1 - С. 29 – 36. **3. Бекиров А.Э.** Пути повышения информационной безопасности ресурсов в системах специального назначения / Баранник В.В., Рябуха Ю.Н., Бекиров А.Е., Комолов Д.И. // Четверга міжнародна науково-практична конференція [«Інформаційні технології та комп'ютерна інженерія»], (Вінниця, 28 - 30 травня 2014 р.) / Вінницький національний технічний університет, Вінниця, 2014. – С. 151. **4. Баранник В.В.** Основы теории структурного стеганографического кодирования / В.В. Баранник, Д.В. Баранник, А.Е. Бекиров – Х.: Издательство «Лидер», 2017. - 256 с. **5. Хорошко В.А.** Методы и

средства защиты информации. / Хорошко В.А., Чекатов А.А. –К.: Юниор, 2003. – 501с. **6. Юдін О.К.** Захист інформації в мережах передачі даних: підручник / Г.Ф. Коначович, О.Г. Корченко, О.К. Юдін. – К.: Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009. – 714с. **7. Bekirov A.** A steganographic method based on the modification of regions of the image with different saturation / Barannik V., Bekirov A., Lekakh A., Barannik D // 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2018 **8. Bekirov A.** Detections of sustainable areas for steganographic embedding / Vladimir Barannik; Andriy Alimpiev; Ali Bekirov; Dmitriy Barannik // 2017 IEEE East-West Design & Test Symposium. **9. Cox I.J.** Bloom, J.A. Fridrick, amd T. Kalkert. (2008), Digital watermarking and steganography, Morgan Kaufman Publishers, USA, pp. 1-591.

СТЕГАНОГРАФИЧЕСКИЙ МЕТОД НА ОСНОВЕ НЕПОСРЕДСТВЕННОГО И КОСВЕННОГО ВСТРАИВАНИЯ ДЛЯ ОБЛАСТЕЙ ИЗОБРАЖЕНИЯ С РАЗЛИЧНОЙ НАСЫЩЕННОСТЬЮ

Али Энверович Бекиров (кандидат технических наук)¹

Владимир Жоржевич Яценко (канд. технических наук, доцент)¹

Александр Станиславович Крейдун²

¹ Харьковський національний університет Воздушних Сил ім. Івана Кожедуба, Харків, Україна

² Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

В современных условиях обстановки и во время проведения стабилизационной операции объединенных сил Воздушные Силы Украины является одним из главных носителей боевого потенциала

ВС України. Осуществлен анализ тенденций внедрения цифровых технологий скрытного управления и передачи данных в ВС Воздушных Сил Украины во время построения современной системы управления войсками. На сегодняшний день, помимо создания новых образцов авиационной техники активно выполняется модернизация существующего бортового радиоэлектронного оборудования.

Целью данной статьи является разработка стеганографического метода на основе совместного использования непосредственного и косвенного встраивания данных. В данной статье рассмотрены особенности использования стеганографического метода для скрытия информации. Сформулированы требования к методу, который заключается в минимизации и распределении искажений исходного изображения-контейнера в результате внедрения информации. Определены основные требования при проектировании метода косвенного встраивания. Разработан метод косвенного стеганографического встраивания на основе модификации рабочих элементов блока относительно эталонной точки по трём уровням. Создана система прямого и обратного стеганографического преобразования на основе разработанного метода косвенного встраивания.

Ключевые слова: стеганографическая система, наименее значимый бит, косвенное стеганографическое встраивание.

STEGANOGRAPHIC METHOD BASED ON THE DIRECT AND INDIRECT DATA EMBEDDING FOR IMAGE AREAS WITH DIFFERENT CONSISTENCY

Ali Bekirov (Candidate of Technical Sciences)¹
Volodymyr Yaschenok (Candidate of Technical Sciences, associate professor)¹
Oleksandr Kreidun²

¹ *Kharkiv National University of Air Force named after Ivan Kozhedub, Kharkiv, Ukraine*

² *National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine*

In today's conditions of the situation and during the stabilization operation of the combined forces, the Air Forces of Ukraine is one of the main carriers of the combat capabilities of the Armed Forces of Ukraine. An analysis of the tendencies of the introduction of digital technologies of secret management and data transmission in the Armed Forces of the Air Forces of Ukraine during the construction of a modern military control system has been carried out. Today, in addition to the development of new models of aviation technology, the modernization of existing on-board electronic equipment is actively being carried out.

The purpose of this article is to develop a steganographic method based on the co-use of direct and indirect data embedding. In this article, the features of using steganographic methods for hiding information are considered. Requirements to the developed method are formed, which consists in minimizing and distributing the distortions of the original container image as a result of embedding information. The main requirements for the design of the indirect embedding method are determined. An estimation of the number of elements that can be embedded in an image block of a certain size is made. A rule for the selection of image regions with different saturation is formulated. A rule for determining the position of the reference and operating points while embedding is formulated. A method of indirect steganographic embedding is developed on the basis of the modification of the working elements of the block relative to the reference point in three levels. It is proposed to use the embedding method based on the modification of the least significant bit. A system of direct and reverse steganographic transformation based on the developed method of indirect embedding is created.

Key words: steganographic system, the least significant bit, indirect steganographic embedding.

References

1. Verba, V., Sydorenko O. (2001). Metodичne napovnennia kursu «Proektnyi analiz» [Methodical content of the course "Project Analysis"]. Sytuatsiina metodyka navchannia: ukrainskyi dosvid. Tsentri innovatsii ta rozvytku, 165-170.
2. Dolgorukov A. Case-study method as modern technology of vocational training. Available at: http://www.vshu.ru/lections.php?Tab_id=3&a=info&id=260.
3. Zhyhylei, Y. M. (2012). Formyrovanye professionalnykh kompetentsiy s pomoshchiu keismetoda v vysshem obrazovanii [Formation of professional competencies using the case-method in higher education]. Prepodavatel KhKhI vek, 29-36.
4. Malysheva M.A. (2011). Sovremennye tekhnologiyi obucheniya y ykh rol v obrazovatel'nom protsesse [Modern technologies of teaching and their role in the educational process]. Sovremennyye tekhnologiyi obucheniya v vuze (opyt NYU VShЭ v Sankt-Peterburhe). – Spb, 6-25.
5. Basics of the case-method. Available at: http://www.pprog.ru/Osnovi_%20keis-metoda.doc.
6. Pohrebelnaia N. Y. (2008). Keis-metod kak usloviye formyrovaniya yssledovatel'skykh sposobnosti studentov vuza [Case-method as a condition for the formation of research abilities of university students]. Nauka y shkola, 73.
7. Surmin Yu. P. (2005). Metod analizu situatsii (Case study) ta yoho navchalni mozhlyvosti. Hlobalizatsiia i Bolonskyi protses: problemy i tekhnologii [Case-study method and its educational capabilities. Globalization and the Bologna process: problems and technologies], 71-82.
8. Surmyn Yu.P.(2002). Sytuatsyonnyi analiz, yly Anatomya Keis-metoda [Situational Analysis, or Case Method Anatomy]. Tsentri innovatsiyi y razvytiya, 41-56.
9. Derevyanchuk. Pidxid do stvorennia y zastosuvannya kejs – metodu pry vyvchenni vijskovo – tekhnichnyh dyscyplin / A. Derevyanchuk // Vijskova osvita. Zbirnyk naukovykh pracz nacional'nogo universytetu obrony Ukrayiny. – K, 2018. – №1(37). – S.92 – 101.