4) певна ізоляція користувача від змін, що відбуваються у структурі інформаційної бази, може розглядатися як один із проявів незалежності інформаційної бази від прикладних засобів автоматизованої обробки інформації, що її використовує користувач;

5) можливість роздільного та фізичного рівні зберігання груп елементів (атомів, молекул), що дозволяє не лише блокувати обхідні шляхи доступу, а й покращує його характеристики. При цьому процедура виділення окремих пристроїв пам'яті для зберігання окремих атомів та молекул БІ повинна завершувати процес проектування фізичної структури БІ. Тут можна одержати додатковий виграш, якщо розподілити згруповані елементи БІ по окремих пристроях пам'яті таким чином, щоб забезпечити пріоритет доступу найбільш часто використовуваною інформацією , або максимізувати степінь близькості розміщення даних, що зберігаються.

Зокрема, якщо прийняти, то до різних елементів, об'єднаних в атоми чи молекули, звертання ймовірно будуть здійснюватися одночасно, то їх групове зберігання в одній і тій же фізичній області сприятиме підвищенню продуктивності системи обробки даних у цілому [4].

Висновки

Описаний метод дозволяє побудувати багаторівневу систему захисту інформації із використанням інформаційної бази та розбиття елементів по молекулах та атомах захисту. Це дозволяє створити модель безпеки інформації більш гнучкою та трансформуватися під конкретний об'єкт.

ЛІТЕРАТУРА

1. Лимов С.В. методы с средства защиты информации в 2х томах./Лимов С.В., Перегудов Д.А., Хорошко В.А.-К.:Арий, 2008.

2. Невойт Я.В. Исследование потоков информации на выходе имитационной модели / Невойт Я.В., Мазуренко А.Н., Хорошко В.А.//збірник наук. праць СНУЯЕтаП,№1(37), 2011.-с.191-196.

3. Сяо Д. Защита ЭВМ./Сяо Д.,Керр Д.,Медтси С.- М.:Мир,1982.-263с.

4. Уелдон Дж.Л. Администрирование и статистика, 1984.-207с.

Надійшла: 29.07.2012 р.

Рецензент: д.т.н., професор Конахович Г.Ф.

УДК 004.43(031):681.3.01(02)

Кущ С.М., Луценко В.М., Прогонов Д.О.

ВИЯВЛЕННЯ ПРИХОВАНИХ ПОВІДОМЛЕНЬ ЯК СКЛАДОВА КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

У статті розглянутою є проблема використання криптографічних методів захисту інформації при проектуванні комплексних систем захисту інформації (КСЗІ). Головна увага приділяється методам виявлення прихованих повідомлень, котрі є вбудованими у 2D-контейнери на основі LSB-методів. Розглядається випадок слабкого заповнення, а процедура виявлення передбачає використання Вейвлет аналіз.

Ключові слова: системи захисту інформації; стеганографія; проект захисту; криптографія; образ.

Постановка проблеми. Забезпечення надійного захисту інформації з обмеженим доступом, що циркулює у системах електронного документообігу об'єкта інформаційної діяльності (ОІД) від витоку до глобальної мережі Інтернет, є особливо актуальною задачею, зважаючи на активність використання глобальної сіті [1-3].

Методи вирішення такої задачі представляють неабиякий інтерес як для приватних організації (захист баз даних клієнтів, конструкторської документації тощо), так і для державних структур (захист інформації, що становить державну таємницю).

Найбільш перспективними напрямками прихованої передачі даних сьогодні є крипто-графічні та стеганографічні методи [4]. Використання лише криптографічних методів має суттєвий недолік.

Такі методи забезпечують приховання від перехоплювача лише змісту повідомлення, але не факту його передачі, що є демаскуючою ознакою каналу зв'язку. Ця ознака практично не враховується при створенні КСЗІ, що зменшує дієздатність захисту.

Тому представляє інтерес дослідження стійкості саме стеганографічних методів (протоколів) передачі інформації до різних типів атак, які проводяться атакуючою стороною з метою виявлення/деструкції прихованого повідомлення (стеганограми).

Метою статті є створення нових методів, котрі підвищують ймовірність виявлення вкладеного повідомлення за умови слабкого заповнення контейнеру (менше 10%), оскільки існуючі пасивні методи виявлення стеганограм є ефективними лише при значному заповненні контейнеру (більше 30%).

Огляд останніх досліджень і публікацій. Переважна частина існуючих стегопротоколів використовує 2D-контейнери (зображення) для передачі інформації, що зумовлено наступними причинами [4]:

1. Відносно великим об'ємом цифрового представлення зображень, що дозволяє приховувати значну кількість інформації, або підвищувати стійкість вкладення (стеганограми) по відношенню до відомих типів атак на стеганографічні протоколи;
2. Наявність в більшості реальних зображень текстурних областей, які мають шумоподібну структуру, тобто найбільш придатні для приховання інформації;
3. Відносно низька чутливість системи людського бачення до незначних змін відтінків кольорів зображення, його яскравості, контрастності.

Існуючі стеганографічні методі приховання інформації в цифрових зображення (ЦЗ) можливо розділити наступним чином [4]:

1. Методи заміни в просторовій області:
   a. Методи заміни найменш значущого біта (англ. Least Significant Bit) – біти інформаційного повідомлення (ІП) приховуються в ЦЗ шляхом зміни значення яскравості $\lambda_{x,y}$ псевдовипадково обраних бітів $p_{x,y}$ згідно визначеного алгоритму;
   b. Методи блочного приховання – ЦЗ розділяється на l_M блоків Δ_i $(1 \le i \le l_M)$, що не перекриваються. Приховання інформації здійснюється шляхом зміни параметрів окремих блоків з можливим ранжуванням всього масиву блоків по заданим критеріям;
   c. Методи зміни палітри – оскільки порядок кольорів у палітрі не є важливим при побудові зображення, тому ІП може біти вбудоване завдяки переставленню кольорів у палітрі згідно деякого алгоритму.
2. Методи приховання у частотній області – використовують особливості представлення ЦЗ у вигляді коефіцієнтів певного перетворення, що застосовується до зображення з метою його стиснення;
3. Статистичні (стохастичні) методи – засновані на зміні статистичних характеристик використовуваного контейнеру або його окремих фрагментів з подальшою перевіркою статистичних гіпотез при детектуванні стеганограми;
4. Структурні методи – суть таких методів полягає у проведенні послідовних перетворень окремих фрагментів заданого зображення, що призводить до формування у ЦЗ стеганограми.

З метою виявлення прихованих повідомлень сьогодні широко використовуються методи стеганоаналізу, які можливо розділити на 2 основних класи [4]:

1. Пасивні методи – спрямовані на виявлення стеганограм в досліджуваних контейнерах, застосовуючи різні підходи:
   a. Статистичний аналіз – дослідження статистичного розподілу значень пікселів ЦЗ, а також оцінка ймовірності появи певного значення пікселю, враховуючи значення сусідніх з ним елементів;
   b. Вейвлет аналіз – виявлення особливостей контейнеру у просторовій та частотній областях;

c. Структурний аналіз – дослідження взаємного розташування окремих фрагментів досліджуваного ЦЗ;

2. Активні методи – метою таких методів є спотворення або знищення прихованих повідомлень:
   a. Компресія контейнеру;
   b. Частотна фільтрація контейнеру;
   c. Геометричні перетворення (поворот, кадрування, масштабування тощо).

Виклад основного матеріалу. Метод Куттера-Джордана-Боссена (МКДБ), що належить до класу LSB-методів, є одним з найпоширеніших методів. Широке використання даного методу пояснюється відносною простотою програмної реалізації алгоритмів вбудовування/детектування ІП. Суть МКДБ полягає у наступному [5]: $i-$тий біт повідомлення S приховується у псевдовипадково обраному пікселі $p_{x,y}$ зображення C, представленого у системі кольорів RGB (англ. Red-Green-Blue), шляхом модифікації яскравості $\lambda_{x,y}$ цього пікселя в каналі синього кольору $B_{x,y}$:

$$\lambda_{x,y} = 0{,}2989 \cdot R_{x,y} + 0{,}5866 \cdot G_{x,y} + 0{,}1145 \cdot B_{x,y},$$

$$\tilde{B}_{x,y} = \begin{cases} B_{x,y} - \upsilon \cdot \lambda_{x,y}, s_i = 0 \\ B_{x,y} + \upsilon \cdot \lambda_{x,y}, s_i = 1 \end{cases} = B_{x,y} + (2 \cdot s_i - 1) \cdot \upsilon \cdot \lambda_{x,y}, \quad (1)$$

де $R_{x,y}$ і $G_{x,y}$ – початкове значення яскравості обраного пікселю $p_{x,y}$ в каналі, відповідно, червоного та зеленого кольору; $s_i - i-$тий біт прихованого повідомлення; $\upsilon-$ константа, що визначає енергію біту, що вбудовується (чим більше значення υ, тим вища стійкість прихованої інформації до можливих спотворень, але й тим вища її візуальна помітність); $B_{x,y}$ і $\tilde{B}_{x,y}$ – початкове та модифіковане значення яскравості обраного пікселю $p_{x,y}$ в каналі синього кольору.

Для детектування прихованого біту s_i використовується передбачення початкового значення пікселя, ґрунтуючись на значеннях сусідніх пікселів. Для розрахунку оцінки первинного значення пікселю авторами методу [5] запропоновано використовувати значення сусідних пікселів, які розташовані у тому ж рядку та стовпці, що і піксель котрий аналізується (у роботі [5] був використаний «хрест» розмірами $n \times n$ при $n = 7$). Оцінка $\tilde{\tilde{B}}^*_{x,y}$ розраховується згідно наступного виразу:

$$\tilde{\tilde{B}}^*_{x,y} = \frac{1}{4 \cdot \sigma} \cdot \left[\sum_{i=(-\sigma)}^{\sigma} B^*_{x+i,y} + \sum_{j=(-\sigma)}^{\sigma} B^*_{x,y+j} - 2 \cdot B^*_{x,y} \right],$$

де $\sigma-$ кількість пікселів знизу/зверху/праворуч/ліворуч від оцінюваного пікселю (у випадку хреста з розмірами 7×7 $\sigma = 3$); $B^*_{x,y}-$ поточне значення інтенсивності досліджуваного пікселя. При детектуванні прихованого біту обчислюється різниця δ між $B^*_{x,y}$ та розрахованою оцінкою $\tilde{\tilde{B}}^*_{x,y}$:

$$\delta = B^*_{x,y} - \tilde{\tilde{B}}^*_{x,y}.$$

Знак отриманої різниці δ буде визначати значення прихованого біту s_i:

$$\begin{cases} \delta < 0, s_i = 1, \\ \delta > 0, s_i = 0. \end{cases}$$

Розглянемо частковий випадок представленого алгоритму: приховання ІП у полутонових зображеннях. Результати, отримані при розгляд такого випадку, можливо поширити і на кольорові ЦЗ, представляючи кожен канал кольору, як полутонове зображення. Ілюстрація роботи МКДБ на прикладі зображення Pict.jpeg при 10% заповненні представлена на рис. 1. Візуально розрізнити «чистий» (рис. 1а) та заповнений (рис. 1в) контейнери практично

неможливо. Об'єм «чистого» контейнеру рівний 511 (кбайт), а об'єм прихованого повідомлення – близько 52 (кбайт). Розміри початкового (Pict.jpeg) та вихідного (PictSteg.jpeg) зображень однакові і рівні 1280×1024 (пікс).

Оскільки пікселі початкового зображення, при прихованні ІП на основі МКДБ, обираються псевдовипадково та рівномірно по всьому зображенню і отримують приріст $\Delta=(2\cdot s_i-1)\cdot\upsilon\cdot\lambda_{x,y}$ згідно (1), тому процедуру приховання даних в загальному випадку можливо трактувати, як додавання до зображення адитивного білого Гаусового шуму (АБГШ) з ненульовим середнім.

Представляє інтерес використання можливостей вейвлет перетворення (ВП) для виявлення прихованих повідомлень, оскільки ВП дає можливість аналізувати особливості ЦЗ як в частотній, так і в просторовій областях, внаслідок використанням масштабованого частотного та рухомого просторового вікон [6].

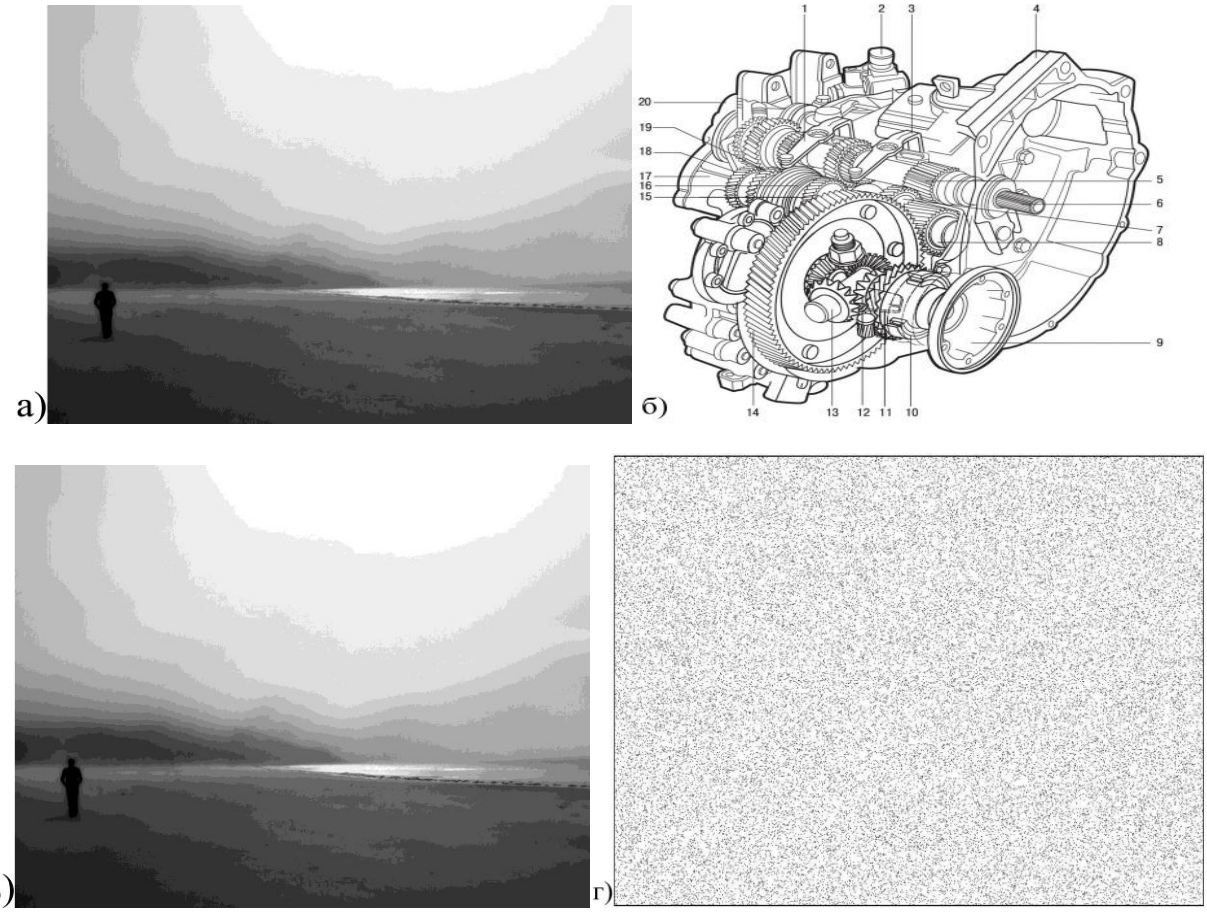

Рис. 1. Ілюстрація роботи методу Куттера-Джордана-Боссена: (а) – початкове зображення Pict.jpeg; (б) – приховане повідомлення (конструктивна схема коробки передач двигуна); (в) – вихідне зображення PictSteg.jpeg після роботи МКДБ; (г) – позиції пікселів, значення яких були змінені при вбудовуванні інформаційного повідомлення

В роботі використано двовимірне дискретне вейвлет перетворення (ДДВП). Коефіцієнти $A_\varphi(m,n)$ (апроксимуючі) та $D_\psi^i(m,n)$ (деталізуючі) ДДВП зображення $f(x,y)$ з розмірами $M\times N$ (пікс) на $j-$тому рівні розкладу (декомпозиції) розраховуються згідно наступних формул [7]:

$$A_\varphi(j,m,n)=\frac{1}{\sqrt{MN}}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)\cdot\varphi_{j,m,n}(x,y),$$

$$D_\psi^i(j,m,n)=\frac{1}{\sqrt{MN}}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)\cdot\psi_{j,m,n}^i(x,y),$$

де $$\varphi_{j,m,n}(x,y)=2^{j/2}\cdot\varphi(2^j x-m,2^j y-n),$$

$$\psi^{i}_{j,m,n}(x,y) = 2^{j/2} \cdot \psi^{i}\left(2^{j}x - m, 2^{j}y - n\right),$$

двовимірні масштабуюча та деталізуюча функції відповідно. У якості базисної функції ДДВП икористаний вейвлет Хаара $\psi(t)$.

Для виявлення ІП, вбудованих в ЦЗ на основі МКДБ, у випадку слабкого заповнення контейнеру розроблений алгоритм, блок-схема якого представлена на рис. 2. Представлений алгоритм заснований на оцінці «зашумленості» заданого зображення. Функція CheckPic розраховує значення середньоквадратичного відхилення (СКВ) по всьому зображенню або його окремим блокам та значення діагональних коефіцієнтів деталізації $D^{D}_{\psi}(m,n)$ на 1-му рівні ДДВП.

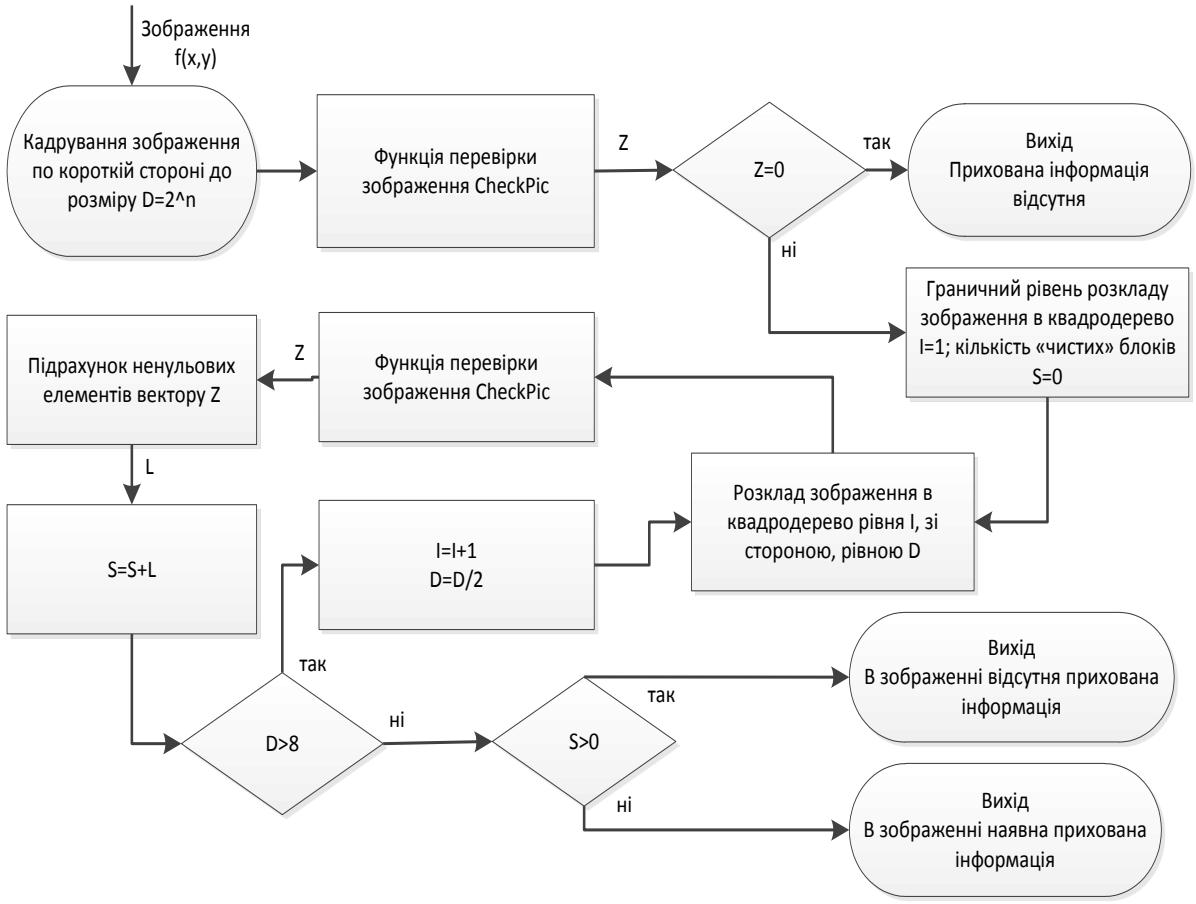

Рис. 2. Блок-схема розробленого алгоритму для виявлення прихованих повідомлень у ЦЗ

У випадку, якщо значення СКВ по ЦЗ є більшим за значення СКВ по ДКД $D^{D}_{\psi}(m,n)$, то досліджуване зображення вважається «чистим», інакше ЦЗ відноситься до підозрілих. Оскільки більшість сучасних цифрових зображень мають високу степінь деталізації, тому можливі ситуації, коли СКВ по значенням ДКД $D^{D}_{\psi}(m,n)$ більше величини СКВ по заданому зображенню $f(x,y)$ (відповідає випадку підозрілого контейнера), хоча в $f(x,y)$ відсутнє ІП.

Для правильної обробки в цьому випадку виконується перетворення зображення в квадродерево з подальшим порівнянням СКВ окремих гілок отриманого квадродерева з відповідними значеннями СКВ по ДКД $D^{D}_{\psi}(m,n)$. Розклад ЦЗ в квадродерево припиняється при досягненні розміру найменшого блоку 8×8 пікселів. «Чисті» блоки квадродерева відповідають частинам зображення з низькою деталізацією. Оскільки ІП, вбудоване на основі МКДБ можливо інтерпретувати як адитивний білий Гаусовий шум (АБГШ), тому кількість «чистих» блоків у випадку «заповненого» контейнера буде рівною нулю. Представлений алгоритм був реалізований програмно у вигляді m-файлу програмного середовища MATLAB. Для його ілюстрації можна розглянути тестові полутонові зображен-

ня з високою та низькою деталізацією у випадку слабкого заповнення контейнеру. Тестові зображення мають рівні розміри 1280×1024 пікселів. Результати аналізу досліджуваних ЦЗ при 5% заповненні контейнеру з використанням розробленого алгоритму ілюструє рис.3.

Розраховані значення СКВ для тестових зображень, а також розрахованих ДКД $D_{\psi}^{D}(m,n)$ ДДВП 1-го рівня декомпозиції у випадку «чистого» і заповненого контейнеру наведені у табл. 1:

Таблиця 1

Значення СКВ для тестових зображень, а також розрахованих ДКД $D_{\psi}^{D}(m,n)$ ДДВП 1-го рівня декомпозиції у випадку «чистого» і заповненого контейнеру

	Тестові зображення	ДКД $D_{\psi}^{D}(m,n)$ ДДВП 1-го рівня декомпозиції	
		«Чистий» контейнер	Заповнений контейнер
Низька деталізація	62,31	56,03	106,2
Висока деталізація	69,63	108,15	112,43

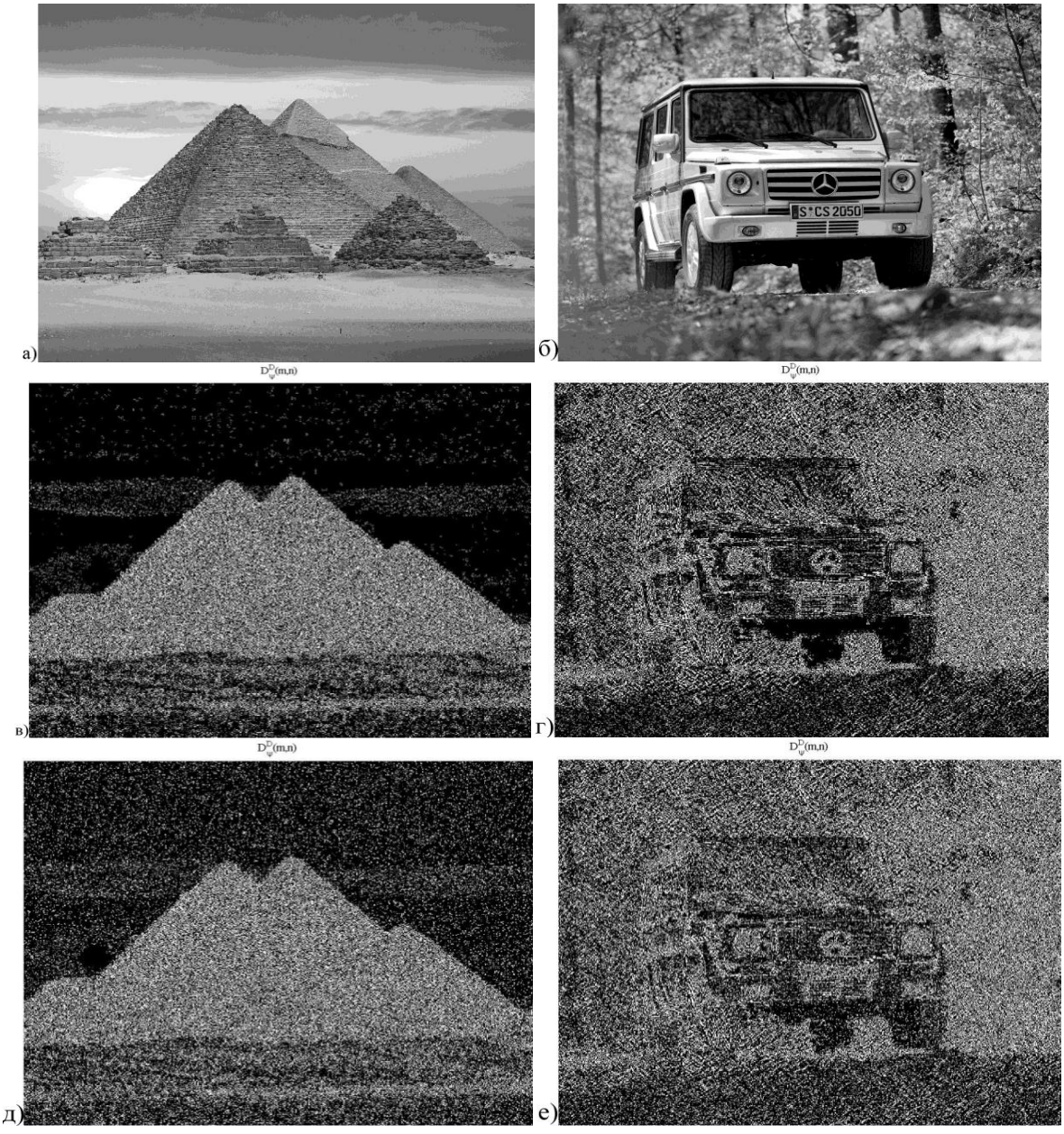

Рис. 3. Ілюстрація роботи розробленого алгоритму. Тестові зображення (5% заповнення): (а) – низька деталізація; (б) – висока деталізація; ДКД $D_{\psi}^{D}(m,n)$ ДДВП 1-го рівня декомпозиції «чистого» контейнеру: (в) – низька деталізація; (г) – висока деталізація; ДКД $D_{\psi}^{D}(m,n)$ ДДВП 1-го рівня декомпозиції заповненого контейнеру: (д) – низька деталізація; (е) – висока деталізація.

Тестове зображення з низькою деталізацією при відсутності стеганограми є «чистим» вже на 1-му рівні ДДВП без розкладу в квадродерево, тоді як для тестового зображення з високою деталізацією необхідний розклад в квадродерево для перевірки наявності прихованого повідомлення. Після роботи алгоритму для зображення з високою деталізацією отримані 4 «чисті» блоки розміром 8×8 пікселів. У випадку заповненого контейнеру обидва тестові ЦЗ є підозрілими згідно критерію СКВ, тому необхідно провести розклад обох зображень в квадродерево.

Після роботи алгоритму отриманий наступний результат: в обох зображеннях відсутні «чисті» блоки, тому зроблений висновок, що в розглянутих ЦЗ присутня стеганограма, вбудована за МКДБ. Для аналізу ефективності розробленого алгоритму розглянуто 2 групи зображень – з високою та низькою деталізацією. Кожна група складалася з 10 високоякісних зображень (наявний АБГШ з дисперсією $\sigma^2 << 10^{-2}$), що мають розмір 1280×1024 (пікс) та досліджувалися при степенях заповнення від 5% до 25%.

За результатами проведеного аналізу зроблений висновок, що розроблений алгоритм дозволяє виявляти приховані на основі МКДБ повідомлення при степені заповнення не менше 10% для зображень з високою деталізацією, та не менше 5% – для ЦЗ з низькою деталізацією.

Висновок

Представлений алгоритм має використовуватися при проектуванні КСЗІ у автоматизованих системах програмного захисту з метою попередження витоку конфіденційної інформації з внутрішньої локальної мережі ОІД до глобальної мережі Інтернет.

ЛІТЕРАТУРА

1. Домарев В.В. Безопасность информационных технологий. Системный подход [Монография]. – К.: ООО ТИД Диа Софт, 2004. – 992 с.

2. Ярочкин В.И. Информационная безопасность [Монография]. – Учебник для студентов вузов. 2-е изд. – М.: Гаудеамус, 2004. – 544 с.

3. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам [Текст]. – Учебное пособие. – М.: Горячая линия-Телеком, 2005. – 416 с.: ил.

4. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика [Текст]. – К.: «МК-Пресс», 2006. – 288 с., ил.

5. M. Kutter, F, Jordan, F, Bossen. Digital signature of color images using amplitude modulation [Text]. – Proc. of the SPIE storage and retrieval for image and video databases Vol. 3022, 1997, – p.518-526.

6. Чарльз К. Чуи. Введение в вейвлеты [Текст]: пер с англ. Я.М. Жилейкина – М.: Мир, 2001. – 412 с.

7. Гонсалес Р., Вудс Р. Цифровая обработка изображений [Текст]. – М.: Техносфера, 2005, - 1072 с.

Надійшла: 30.07.2012 р.

Рецензент: д.т.н., професор Конахович Г.Ф.

УДК 004.056.53

Пасько О.З., Пархоменко І.І., Пономаренко О.В.

БОТ-МЕРЕЖІ ЯК ЗАСІБ ВЕДЕННЯ КІБЕРВІЙН

У даній статті була розглянута проблема захисту інформаційного простору від шкідливого коду ботнет. Суть якої в складності виявлення та нейтралізації інфікованої мережі та центру її керування. Надалі були надані рекомендації щодо вибору організаційних, програмних та апаратних механізмів захисту комп'ютерних мереж від інфікування ботом.

Ключові слова: ботнет, центр управління, файрвол, антивірус, сніфер, спам-фільтр, антируткіт, аналітичний модуль.

Вступ. На тлі проблем розкрадання даних, шпигунства та витоку інформації, комп'ютерних вірусів та хакерських атак, особливу увагу варто приділити кібер війнам, які ведуть державні структури, і які стають серйозною загрозою для національної безпеки. Їхні