УДК 004.056

О. О. Вовк, А. А. Астраханцев
Харківський національний університет радіоелектроніки

РОЗРОБЛЕННЯ МЕТОДИКИ ОЦІНЮВАННЯ ВАЖЛИВОСТІ ХАРАКТЕРИСТИК СТЕГАНОГРАФІЧНИХ АЛГОРИТМІВ

Розв'язана задача оцінювання важливості (ваги) кожної з характеристик алгоритмів стеганографії. Отримані оцінки використовують для аналізу існуючих алгоритмів вбудовування інформації та для багатокритеріального вибору найкращого алгоритму. Методика дає змогу проводити як рівнозважене оцінювання алгоритмів, так і з урахуванням коефіцієнтів важливості характеристик.

Ключові слова: стеганографія, характеристики, методика, вага, алгоритм, стійкість, багатокритеріальний вибір

In this paper the problem of estimating the importance of each of the characteristics of steganographic algorithms is solved. The resulting estimates are used in the analysis of the existing algorithms for information embedding and multiobjective choice of the best algorithm. The technique allows providing an equally weighted algorithms estimation, and also considers the importance of coefficients of characteristics.

Key words: steganography, characteristics, methodic, weight, algorithm, robustness, multiobjective choice

Вступ

З появою глобальних комп'ютерних мереж доступ до інформації став неймовірно легким. Простота і швидкість такого доступу теж значно зросли. Водночас зросли і загрози витоку даних. Стеганографія – один зі способів забезпечення інформаційної безпеки. Це метод передавання, який приховує факт існування секретних повідомлень. Сьогодні стеганографія використовується для захисту інформації від несанкціонованого доступу, у системах моніторингу мережевих ресурсів, а також для захисту авторських прав на деякі види інтелектуальної власності та для автентифікації цифрових об'єктів [1]. Сьогодні у публікаціях [1], [2] запропонована дуже велика кількість різних стеганографічних методів, частина з яких універсальні або призначені для широкого кола завдань. Водночас кожне стеганографічне завдання має різні вимоги до таких характеристик, як стійкість, пропускна здатність, складність вбудовування інформації та інші [3].

У цій роботі розв'язується задача оцінювання важливості (ваги) кожної з характеристик стеганографічних алгоритмів. Отримані оцінки використовують для аналізу алгоритмів вбудовування інформації та для багатокритеріального вибору найкращого алгоритму.

Аналіз останніх досліджень та публікацій

Сьогодні стеганографію використовують для [4] прихованого зв'язку, захисту авторських прав на зображення (автентифікації), відбитків пальців (відстеження порушника), додавання заголовків до зображень, додавання додаткової інформації, такої як субтитри до відео, захисту цілісності зображень (виявлення випадків шахрайства), управління копіюванням при DVD записі та в інтелектуальних браузерах, для автоматичного надання інформації про авторські права. Всі ці області проаналізуємо й оцінимо з використанням набору характеристик, наведених у [3], [4], зокрема:

- Пропускна здатність – кількість бітів прихованого повідомлення, які можуть бути передані за допомогою цього методу в зображенні фіксованого розміру.

- Стійкість – здатність вилучити приховану інформацію після загальних операцій з обробки зображень: лінійні та нелінійні фільтри, стиснення з втратами, регулювання контрастності, перефарбування, передискретизації, масштабування, обертання, додавання шуму, обрізки, друку/копіювання/сканування, переставляння пікселів у малій околиці, квантування кольорів тощо.
- Невидимість – перцепційна прозорість. Це поняття спирається на властивості зорової або слухової систем людини.
- Захищеність – вбудована інформація не може бути видалена цілеспрямованими атаками, основаними на відомому алгоритмі вбудовування та вилучення, і знанні принаймні одного носія з прихованим повідомленням.
- Складність вбудовування і виявлення – кількість стандартних операцій, які будуть виконані для вбудовування і виявлення прихованого повідомлення.

У роботі [4] характеристики оцінено за кольоровою шкалою (рис.1):

Рис. 1. Основні сфери використання та їх вимоги до характеристик

Використовуючи набір характеристик з [4], у цій роботі пропонуємо метод аналізу ієрархій, оснований на порівнянні пар показників для кожного з додатків.

Розрахунок ваг характеристик

Формою представлення попарних порівнянь [5] є зворотно-симетрична матриця (табл. 2), елементи якої W_{ij} є проявами інтенсивності елементів ієрархії *i* відносно ієрархії *j*, що оцінюється за шкалою інтенсивності від 1 до 9, де оцінки мають такі значення:

1 – рівні значення;

3 – помірна перевага одного над іншим;

5 – істотна перевага одного над іншим;

7 – значна перевага одного над іншим;

9 – дуже сильна перевага одного над іншим;

2, 4, 6, 8 – відповідні проміжні значення.

Для отримання матриці парних зіставлень (табл. 2) запропоновано матрицю (табл. 1), що перетворює кольори на коефіцієнти від 1 до 9.

Таблиця 1

Матриця відповідності

	1	1/2	1/3	1/4	1/5	1/6	1/7	1/9
	2	1	1/2	1/3	1/4	1/5	1/6	1/7
	3	2	1	1/2	1/3	1/4	1/5	1/6
	4	3	2	1	1/2	1/3	1/4	1/5
	5	4	3	2	1	1/2	1/3	1/4
	6	5	4	3	2	1	1/2	1/3
	7	6	5	4	3	2	1	1/2
	9	7	6	5	4	3	2	1

Після цього побудовано матриці пріоритетів (табл. 2, табл. 3), що містять: пропускну здатність (*a*), стійкість (*b*), невидимість (*c*), захищеність (*d*), складність вбудовування (*e*) і складність виявлення (*f*).

Таблиця 2

Матриця пріоритетів (для прихованого зв'язку)

W	*a*	*b*	*c*	*d*	*e*	*f*
a		7	1	1	6	6
b	1/7		1/7	1/7	1/2	1/2
c	1	7		1	6	6
d	1	7	1		6	6
e	1/6	2	1/6	1/6		1
f	1/6	2	1/6	1/6	1	

Таблиця 3

Матриця пріоритетів (для захисту цілісності зображення)

W	*a*	*b*	*c*	*d*	*e*	*f*
a		1/5	1/4	1/6	1/6	1
b	5		2	1/2	1/2	5
c	4	1/2		1/3	1/3	4
d	6	2	3		1	6
e	6	2	3	1		6
f	1	1/5	1/4	1/6	1/6	

Заповнюючи матрицю пріоритетів, керуються правилом: якщо у разі порівняння елемента *i* з елементом *j* отримано $W_{ij} = b$, тоді $W_{ij} = 1 / b$.

Після побудови матриці пріоритетів пріоритет кожного об'єкта в ієрархії визначається обчисленням відповідного елемента нормованого головного власного вектора матриці **V**.

Точне визначення основних пріоритетів власного вектора матриці є доволі складним. На практиці запропоновано [5] використовувати один із таких способів:

1. Підсумовуються елементи кожного рядка і нормуються діленням отриманої суми на суму всіх елементів матриці. Перший елемент отриманого вектора буде пріоритетом першого об'єкта, другий другого і т.д.

2. Підсумовують елементи кожного стовпця і знаходять обернені величини цих сум. Їх нормують поділом кожного на обернену величину їх загальної суми, так, що загальна сума нормованих величин дорівнюватиме одиниці.

3. Елементи кожного стовпця діляться на суму елементів цього стовпця (нормується стовпець), потім отримані елементи кожного з рядків підсумовуються і діляться на кількість елементів у рядку.

4. Розраховується середнє геометричне кожного рядка, отримані значення нормуються.

5. Матрицю підносять до як завгодно великого степеня, обчислюється сума елементів рядків і отримані величини нормуються.

Використано четвертий спосіб, згідно з яким компоненти вектора пріоритетів обчислюють так:

$$V_i = \frac{\sqrt[N]{\prod_{j=1}^{N} W_{ij}}}{\sum_{k=1}^{N} \sqrt[N]{\prod_{j=1}^{N} W_{kj}}}, \quad (1)$$

де N – розмірність пріоритетів; W_{ij} – елемент пріоритетів, що відображає результат порівняння елементів i і j.

Усередненням результатів для всіх додатків (2) отримуємо ваги (важливість) кожної з характеристик стеганографічних алгоритмів (табл. 4).

$$R_i = \sum_{i=1}^{7} V_i \,/\, 7 \quad (2)$$

Таблиця 4

Загальні ваги характеристик

Характеристика (i)	Вага (R)
Пропускна здатність	0,084
Стійкість	0,203
Невидимість	0,128
Захищеність	0,299
Складність вбудовування	0,070
Складність виявлення	0,218

Отже, результати оцінки показали, що найважливішими характеристиками стеганографічних алгоритмів є захищеність (вага R = 0,299), складність виявлення (вага R = 0,218) і стійкість (вага R = 0,203).

Огляд стеганографічних алгоритмів

Сьогодні існує велика кількість методів приховування даних у цифрових зображеннях. Найпоширеніші алгоритми використовують просторові та частотні області для приховування інформації. Також існують методи, основані на використанні дискретно-косинусного перетворення (ДКП), дискретного перетворення Фур'є (ДПФ), дискретного вейвлет-перетворення (ДВП), дискретного перетворення Карунена–Лоєва (ДКЛП) та інші. Такі перетворення можна застосувати як до окремих частин зображення, так і для усього зображення. Для досліджень вибрано найпоширеніший метод заміни найменш значущого біта [6], [8], метод Куттера–Джордана–Боссена [6], [9], як один з найкращих у просторовій області, модифікований метод Коха–Жао [8] [10] як один з основних в частотній області, метод Бенгама, що є вдосконаленням попереднього [6], [11], метод, оснований на ДВП [12–14], та методи, основані на розширенні спектра [15–17].

***Метод заміни найменш значущого біта* (*НЗБ*)** найпоширеніший серед методів заміни в просторовій області. Загальний принцип цих методів полягає у заміні надмірності, малозначущої частини зображення бітами секретного повідомлення [6], [8]. Для вилучення повідомлення необхідно знати алгоритм, за яким розміщалась прихована інформація по контейнеру. Популярність цього методу зумовлена його простотою та тим, що він дає змогу приховувати у порівняно невеликих файлах достатньо великі обсяги інформації. Метод НЗБ має низьку стеганографічну стійкість до атак пасивного й активного порушників. Основний його недолік – висока чутливість до найменших виправлень контейнера. Для ослаблення цієї чутливості часто додатково застосовують завадостійке кодування.

Метод Куттера–Джордана–Боссена (метод «хреста»). У цьому алгоритмі запропоновано використовувати канал синього кольору зображення, що має RGB-кодування, для приховування

інформації [6], [9], оскільки ЗСЛ є найменш чутливою до змін яскравості саме синього кольору порівняно з червоним та зеленим. Вбудовування інформації відбувається у такий спосіб – один *i*-й біт m_i повідомлення у один псевдовипадковий піксел контейнера $p = (x, y)$ за такою формулою:

$$B^*_{x,y} = \begin{cases} B_{x,y} + \upsilon \cdot \lambda_{x,y}, \; при \;\; m_i = 0; \\ B_{x,y} - \upsilon \cdot \lambda_{x,y}, \; при \;\; m_i = 1. \end{cases}, \tag{3}$$

де $\lambda_{x,y} = 0.3 \cdot R_{x,y} + 0.59 \cdot G_{x,y} + 0.11 \cdot B_{x,y}$ – яскравість піксела; υ – коефіцієнт, що задає енергію біта даних, що вбудовуються.

Оскільки на приймальній стороні немає зображення – оригіналу, то точно дізнатися, як саме змінилася яскравість синього кольору, ми не можемо. Тому для вилучення прогнозують значення яскравості вихідного синього кольору на основі його сусідів.

Перевагою цього методу є висока пропускна здатність, стійкість до несанкціонованого ознайомлення, до частотного детектування, до руйнування молодшого біта контейнера та до атак стискання. Недоліком є те, що вилучення повідомлення має імовірнісний характер. Для зменшення імовірності помилки використовується завадостійке кодування. Також можна у процесі вбудовування кожен біт повторювати декілька разів (багаторазове вбудовування).

Метод відносної заміни величин коефіцієнтів ДКП (метод Коха і Жао). Один з найпоширеніших сьогодні методів приховування конфіденційної інформації в частотній області зображення полягає у відносній заміні значень коефіцієнтів ДКП [6], [8], [10]. На початковому етапі первинне зображення ділять на блоки розмірністю 8·8 пікселів. ДКП застосовується до кожного блока, внаслідок чого отримують матриці 8·8 коефіцієнтів ДКП. Кожен блок призначений для приховування одного біта даних. Під час організації секретного каналу абоненти повинні завчасно домовитися про два конкретні коефіцієнти ДКП з кожного блока, які використовуватимуться для приховання даних. Вбудовування інформації здійснюється так: для передавання біта «0» прагнуть, щоб різниця абсолютних значень вибраних коефіцієнтів ДКП перевищувала деяку позитивну величину, а для передавання біта «1» ця різниця має бути меншою порівняно з деякою негативною величиною. Отже, первинне зображення спотворюється через внесення змін до коефіцієнтів ДКП, якщо їх відносна величина не відповідає приховуваному біту. Що більше значення P, то стеганосистема, створена на основі цього методу, є стійкішою до компресії, проте якість зображення істотно погіршується. Після відповідного внесення корекцій у значення коефіцієнтів, які повинні задовольняти нерівності, проводиться зворотне ДКП.

Метод Бенгама–Мемона–Ео–Юнга є оптимізованою версією розгляненого вище методу [11], причому оптимізацію проведено за двома напрямами: по-перше, запропоновано для вбудовування використовувати не всі блоки, а лише найпридатніші для цього, по-друге, в частотній області блока для вбудовування вибираються не два, а три коефіцієнти ДКП, що істотно зменшує візуальні спотворення контейнера [10]. Придатними для вбудовування інформації вважаються такі блоки зображення, які одночасно задовольняють такі дві умови:

- блоки не повинні мати різких переходів яскравості;
- блоки не мають бути дуже монотонними.

Вказані особливості виявляються критерієм відбракування непридатних блоків.

Використання трьох коефіцієнтів замість двох і, що найголовніше, відмова від модифікації блоків зображення в разі неприйнятних їх викривлень, зменшують похибки, які вносяться повідомленням. Одержувач завжди може визначити блоки, в які не проводилося вбудовування, просто повторивши аналіз, аналогічний виконаному на передавальній стороні.

Методи на основі дискретного вейвлет-перетворення (ДВП). Вейвлет-перетворення – це локалізований аналітичний метод часових інтервалів із фіксованим розміром вікна й конвертованою формою, що дає змогу добре локалізувати низькочастотні деталі сигналу в частотній області (основні гармоніки), а високочастотні – в часовій [12], [14]. Основна ідея дискретного вейвлет-перетворення у процесі обробки зображення полягає в розкладанні зображення на підзображення різних просторових та частотних областей.

Після ДВП перетворення інформація аналізується в чотирьох частотних областях, одна з яких є низькочастотною (LL) і три – високочастотними (LH, HL, HH) (рис. 2).

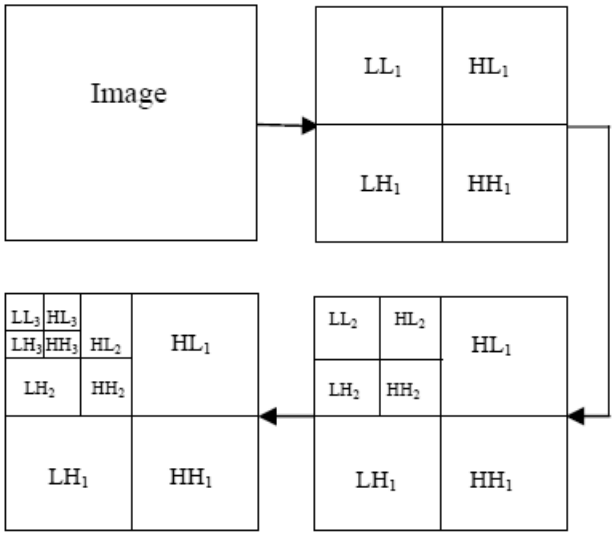

Рис. 2. Трирівневе дискретне вейвлет-розкладання

Як правило, для приховування водяних знаків використовують високочастотні складові, оскільки людське око менш чутливе до змін у цих областях [14]. Але область LL є порівняно стійкішою, бо вона містить переважну більшість енергії зображення. Для того, щоб отримати кращий показник надійності, водяний знак вбудовують саме у це підзображення.

Для дискретного вейвлет-аналізу використовують різні базиси вейвлетів, зокрема вейвлети Хаара, Добеші, симлети, кофлети та ортогональні вейвлети. Наведені базиси відрізняються різними значеннями вейвлет-коефіцієнтів та підходами до формування спектрів.

Методи розширення спектра. Для досліджень вибрано два методи, які вбудовують водяний знак за допомогою модуляції коефіцієнтів ДКП [15], бо у них найвищі показники стійкості серед методів розширення спектра. Перший алгоритм, що описав д-р Руні [16], оснований на модуляції середньої смуги частот окремих блоків зображення за допомогою випадкового гауссівського сигналу. Другий метод згідно з Піва та ін. [17] також модулює коефіцієнти ДКП, але використовує інший частотний діапазон нижчих частот. Стійкість водяного знака надалі корегується згідно з перцепційною маскою.

Використання багатокритеріальної оптимізації для вибору оптимального стеганографічного алгоритму

Подамо порівняльний аналіз характеристик для методів, коротко описаних вище. Використовуючи метод порівняння, описаний в частині 2 та на основі інформації, наведеної в [6–17], створено табл. 5.

Таблиця 5

Порівняння алгоритмів вбудовування

	a	*b*	*c*	*d*	*e*	*f*
A1	8	1	7	1	8	8
A2	6	4	7	4	7	7
A3	2	7	5	7	5	5
A4	1	6	6	7	4	4
A5	4	7	8	6	3	3
A6	3	8	8	8	1	1

де *A1* – метод НЗБ; *A2* – метод Куттера; *A3* – метод Коха–Жао; *A4* – метод Бенгама; *A5* – метод розширення спектра; *A6* – трирівневий ДВП метод; *a* – ємність; *b* – стійкість; *c* – невидимість; *d* – захищеність; *e* – складність вбудовування; *f* – складність виявлення.

У табл. 5 показник "8" є найкращим значенням характеристики, "1" – найгіршим. Для розуміння значень, що описані в табл. 5, нижче наведено розрахунок коефіцієнтів для пропускної здатності.

Для методу НЗБ пропускна здатність залежить від розмірів зображення (h – висота, w – ширина) і розраховується згідно з (4):

$$C_1 = h \cdot w \cdot 3 . \quad (4)$$

Зазвичай тільки один колірний компонент використовується для приховання, але можливість вбудувати інформацію є одразу у всі (три) компоненти.

У методі Куттера один біт інформації може бути вбудований в один піксел зображення, тому пропускна здатність визначається як:

$$C_2 = h \cdot w . \quad (5)$$

Метод Коха–Жао використовує для вбудовування одного біта інформації блок коефіцієнтів ДКП розміром 8 × 8, тому пропускна здатність визначається:

$$C_3 = (h \cdot w)/(8 \cdot 8) . \quad (6)$$

В алгоритмі Бенгама блоки діляться на три класи, і тільки один можна використати для вбудовування, отже, в середньому:

$$C_4 = (h \cdot w)/(8 \cdot 8 \cdot 3) . \quad (7)$$

Для алгоритмів розширення спектра пропускну здатність визначають так:

$$C_5 = \log_2(1 + SNR) , \quad (8)$$

після визначення відношення сигнал / шум (SNR) за рівнянням перетворення (8) можна отримати:

$$C_5 = h \cdot w \cdot 0.264 . \quad (9)$$

Методи, що використовують ДВП перетворення, можуть запропонувати пропускну здатність:

$$C_6 = (h \cdot w)/4 . \quad (10)$$

Після розрахунку середніх значень (4)–(10) визначено коефіцієнти пропускної здатності (перша колонка в табл. 5) порівнянням алгоритмів. Використовуючи метод попарних порівнянь, описаний у розділі 3, можна виконати порівняльний аналіз цих алгоритмів. Для аналізу будуть використані дані з табл. 5. Порівняльний аналіз алгоритмів, оснований на кожній з характеристик, відображений у вигляді матриць в табл. 6 та табл. 7.

Таблиця 6

Матриця порівняння алгоритмів (пропускна здатність)

	A1	*A2*	*A3*	*A4*	*A5*	*A6*
A1		3	7	8	5	6
A2	1/3		5	6	3	4
A3	1/7	1/5		2	1/3	1/2
A4	1/8	1/6	1/2		1/4	1/3
A5	1/5	1/3	3	4		2
A6	1/6	1/4	2	3	1/2	

Таблиця 7

Матриця порівняння алгоритмів (захищеність)

	A1	*A2*	*A3*	*A4*	*A5*	*A6*
A1		1/4	1/7	1/7	1/6	1/8
A2	4		1/4	1/4	1/3	1/5
A3	7	4		1	2	1/2
A4	7	4	1		2	1/2
A5	6	3	1/2	1/2		1/3
A6	8	5	2	2	3	

Отримано порівняльні оцінки методів *A1 – A6* для кожної з характеристик за формулою (1). Підсумовуючи значення всіх параметрів (11) та віднормуючи їх, можна отримати зважену оцінку якості методів, що наведені в табл. 8.

$$WW_a = \frac{\sum_{i=1}^{k=6} V_i}{\sum_{a=1}^{A=6} \sum_{i=1}^{k=6} V_{ia}}, \tag{11}$$

де $\kappa = 6$ – кількість характеристик; A – кількість алгоритмів; V_i – вектор пріоритетів для кожної з характеристик, який розраховується з (1); V_{ia} – вектор пріоритетів для кожної з характеристик для кожного з алгоритмів a. Найбільші значення в табл. 8 та табл. 9 є найліпшими.

Таблиця 8

Порівняння методів, не враховуючи важливість (вагу) характеристик

Метод (*a*)	Значення (*WW*)
A1	0,266
A2	0,181
A3	0,126
A4	0,097
A5	0,137
A6	0,193

Як видно з табл. 8, найвище значення продемонстрував метод НЗБ (*A1*). Але, зважаючи на оцінку важливості характеристик, табл. 8 можна видозмінити до табл. 9, де значення параметрів отримано з виразу (12):

$$WW1_a = \frac{\sum_{i=1}^{k=6} (V_i \cdot R_i)}{\sum_{a=1}^{A=6} \sum_{i=1}^{k=6} V_{ia} \cdot R_i}. \tag{12}$$

Таблиця 9

Порівняння методів, враховуючи важливість (вагу) характеристик

Метод (*a*)	Значення (*WW1*)
A1	0,200
A2	0,149
A3	0,151
A4	0,121
A5	0,139
A6	0,240

Отже, за комплексного порівняння методів вбудовування інформації для прихованого передавання по мережах зв'язку найкращий результат показали інтегровані методи, основані на ДВП (*A6*).

Висновки і перспективи подальших наукових розвідок

У роботі запропоновано методику порівняльного аналізу, що дає змогу об'єктивно визначити важливість (вагу) кожної з якісних характеристик методів приховування інформації за передавання по мережах зв'язку. Враховуючи вимоги, що ставлять найпоширеніші сфери використання принципів стеганографії, згідно з розробленою методикою, визначено найважливіші характе-

ристики стеганографічних алгоритмів для всіх основних напрямів застосування стеганографії. Так, для захисту цілісності зображення найбільшу вагу мають стійкість та безпека, а для прихованого зв'язку одразу три характеристики – пропускна здатність, невидимість та безпека**.** Наукова новизна роботи полягає у визначенні найвпливовіших для всіх сфер застосування стеганографії характеристик, якими виявились захищеність, складність виявлення і стійкість. Також науковою новизною є запропонована методика оцінювання ефективності стеганоалгоритмів, основана на зазначених вище характеристиках. Методика дає змогу проводити як рівнозважене оцінювання алгоритмів, так і з урахуванням коефіцієнтів, отриманих під час оцінювання важливості характеристик. Дослідження показали, що у разі загального оцінювання методів найкращі результати демонструє метод НЗБ (*A1, метрика = 0,266*), тоді як за детальнішого аналізу, враховуючи коефіцієнти важливості різних характеристик, найліпший результат дають інтегровані методи, основані на ДВП (*A6, метрика = 0,240*). На основі проведених досліджень планується розробити власний метод, з високою стійкістю до певних атак, що загалом демонстрував би оцінки, не нижчі за отримані результати для ДВП методів.

1. Cox I., Miller M., Bloom J., Fridrich J., Kalker T. Digital Watermarking and Steganography. Second Edition. (Elsevier, 2008). 2. Watermarking (Vol.1) / Edited by Das Gupta, M. (InTech, Croatia, 2012). 3. Singh P., Chadha R. S. A Survey of Digital Watermarking Techniques // Applications and Attacks. International Journal of Engineering and Innovative Technology, Volume 2, Issue 9, (IJEIT, 2013). 4. Fridrich J. Applications of Data Hiding in Digital Images, 1999. 5. Domarev V. Safety of information technology // Methodology for creating protection systems, (DiaSoft, 2002). 6. Konakhovich G., Puzyrenko A. Computer steganography. Theory and Practice (MK-Press, 2006). 7. Surekha B., Swamy G. N. A Spatial Domain Public Image Watermarking // International Journal of Security and Its Applications Vol. 5 No. 1, (Jan 2011). 8. Jadav Y. Comparison of LSB and Subband // DCT Technique for Image Watermarking. Conference on Advances in Communication and Control Systems 2013, (CAC2S, 2013). 9. Kutter M., Petitcolas F. A fair benchmark for image watermarking systems // Proc. Of Security and Watermarking of Multimedia Contents. – P. 226–239 (Jan 1999). 10. Koch, E., Zhao, J. Toward robust and hidden image copyright labeling // IEE Workshop Nonlinear Signal and Image Processing. (1995). 11. Benham D., Memon N., Yeo B.L., Yeung M. Fast watermarking of DCT-based compressed images // Proc Int Conf Image Science, Systems, and Technology (CISST '97), Las Vegas, NV. – P. 243–253, (June, 1997). 12. Sridevi T., Kumar V. A Robust Watermarking Algorithm Based on Image Normalization and DC Coefficients. IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, (Sept. 2011). 13. Li Z., Xilan Y., Hongsong L., Minrong C. A Dynamic Multiple Watermarking Algorithm Based on DWT and HVS // Int. J. Communications, Network and System Sciences, 5, 490-495. (2012), http://dx.doi.org/10.4236/ijcns.2012.58059. 14. Kashyap N., Sinha G.R. Image Watermarking Using 3-Level Discrete Wavelet Transform (DWT) // I. J. Modern Education and Computer Science, vol.3, 50–56 pp., published online in MECS, (April, 2012). 15. Fridrich J., Goljan M. Comparing robustness of watermarking techniques. Proc. SPIE Vol. 3657, (Security and Watermarking of Multimedia Content), San Jose, (Jan, 1999). 16. Ó Ruanaidh J., Pun T. Rotation, scale and translation invariant digital image watermarking // Proc. of the ICIP'97, vol. 1, pp. 536–539, (California, 1997). 17. Piva A., Barni M., Bartolini F. Threshold Selection for Correlation-Based Watermark Detection // Proceedings of COST 254 Workshop on Intelligent Communications, L'Aquila, Italy, (June, 1998).