УДК 004.[056.54:932.2]

Д. О. Прогонов, С. М. Кущ
Національний технічний університет України
“Київський політехнічний інститут”;
Фізико-технічний інститут,
кафедра фізико-технічних засобів захисту інформації

ВАРІОГРАМНИЙ АНАЛІЗ СТЕГАНОГРАМ, СФОРМОВАНИХ НА ОСНОВІ КОМПЛЕКСНИХ МЕТОДІВ ПРИХОВАННЯ ДАНИХ

Оцінено ефективність використання кореляційного та варіограмного методів для виявлення стеганограм, сформованих при використанні багатоетапної обробки як контейнера, так і стегоданих. Використовуючи варіограмний аналіз, можна виявляти стеганограми навіть за слабкого заповнення контейнера стегоданими. Показано, що застосування кореляційного аналізу для виявлення стеганограм має суттєві обмеження.

Ключові слова: пасивний стегоаналіз, кореляційний аналіз, варіограмний аналіз.

VARIOGRAM ANALYSES OF STEGANOGRAMS SHAPED FOLLOWING INTEGRATED METHODS OF DATA HIDING

The paper is devoted to analysis of effectiveness the applying of correlation and variogram analyses for steganogram detection. The case of usage multistage steganographic methods for data embedding in digital images is considered. Applying of variogram analysis gives opportunity to disclosure the steganograms even in case of low container’s degree of stegodata filling. It is shown that correlation analysis has limited opportunities in mentioned case.

Key words: passive steganalysis, correlation analysis, variogram analysis.

Вступ

Використання сучасних методів цифрової стеганографії для несанкціонованого передавання конфіденційних даних суттєво ускладнює виявлення прихованого повідомлення у контейнері стандартними методами пасивного стегоаналізу (ПС). Це зумовлено тим, що комплексні стеганографічні методи, основані на багатоетапній обробці як контейнера, так і стегоданих, допомагають мінімізувати основні демаскувальні ознаки стеганограм. Тому розроблення ефективних методів виявлення стеганограм, характеристики яких мало відрізняться від характеристик контейнера, є важливою і актуальною задачею.

Переважна більшість існуючих методів ПС основана на застосуванні стегодетекторів (СД) – приладів, в яких на основі правил прийняття рішень, визначених для щільностей умовних ймовірностей характеристик вибраного цифрового зображення (ЦЗ) та, наприклад, чистого контейнера, приймається гіпотеза щодо відсутності (наявності) прихованих даних у досліджуваному зображенні. Кластер характеристик ЦЗ, для яких формується рішення визначення належності ЦЗ до одного з класів – контейнерів, чи стеганограм, вибирають за апріорними даними щодо використаного методу приховання повідомлень у контейнерах або за результатами статистичного аналізу вибраного набору стеганограм. Для виявлення стеганограм, сформованих з використанням поширених методів вбудовування стегоданих (наприклад, JSteg, JPHide, OutGuess, F4/F5 тощо), використовують набір стандартних статистичних параметрів ЦЗ, що дає змогу спростити процедуру налаштування СД без суттєвого зниження точності його роботи.

Для підвищення ефективності роботи СД, у випадку використання багатоетапних та адаптивних методів приховання повідомлень у контейнери, можна застосовувати декілька кластерів характеристик ЦЗ. Недоліком такого підходу є те, що високої ймовірності розпізнавання стеганограм СД можна досягти тільки з використанням значної кількості параметрів ЦЗ (наприклад, кластер для MINMAX-моделі містить 10725 ознак контейнерів [1]), внаслідок чого суттєво зростають як вимоги щодо обсягу тестових вибірок чистих (заповнених) контейнерів, так і складність процедури налаштування СД. Тому представляє інтерес пошук кластерів ознак ЦЗ мінімальної потужності, на основі аналізу яких буде високою ймовірність виявлення стеганограм.

Огляд літературних джерел

Для стеганографічного аналізу ЦЗ широко використовуються методи аналізу стандартних та статистичних параметрів зображень – метрик якості ЦЗ [2], виду гістограми розподілу яскравості пікселів зображень [3] тощо. Недоліком таких методів є те, що під час дослідження ЦЗ слабкі локальні зміни параметрів зображень, зумовлені прихованням повідомлень, усереднюються по всьому контейнеру, що суттєво знижує ефективність роботи СД, особливо у випадку використання комплексних стеганографічних методів.

Методи ПС, основані на загальній теорії марківських випадкових полів (МВП), дають змогу з високою ймовірністю виявляти стеганограми, сформовані з використанням адаптивних методів вбудовування стегоданих [4]. Але через високу обчислювальну складність оцінювання їх параметрів вони широко не застосовуються, і тому при проведенні ПС використовують наближені оцінки параметрів МВП, що отримані аналізом матриць суміжності стеганограм після просторової фільтрації зображень [1]. Ймовірність виявлення стеганограм підвищується з використанням великої кількості просторових фільтрів різного розміру, що суттєво ускладнює процес налаштування СД.

У роботі [5] для проведення ПС запропоновано використовувати методи структурного та спектрального аналізу зображень. Особливістю цих методів є можливість досліджувати ЦЗ у різних просторових областях і діапазонах частот, що підвищує ефективність проведення ПС стеганограм, сформованих з використанням багатоетапних стеганографічних методів. Представляє інтерес порівняння результатів виявлення повідомлень, прихованих в області перетворення ЦЗ, з використанням спеціалізованих методів структурного аналізу зображень, з результатами, одержаними із застосуванням одного з класичних методів обробки ЦЗ – кореляційного аналізу (КА).

Постановка задачі

Метою роботи є оцінювання ефективності використання варіограмного аналізу (ВА) і кореляційного аналізу для виявлення стеганограм, сформованих з використанням багатоетапних методів обробки контейнера та стегоданих для випадку приховання повідомлень в області перетворення ЦЗ.

Приховання повідомлень у цифрових зображеннях

Залежно від способу вбудовування стегоданих в області перетворення зображення-контейнера вирізняють такі класи методів [6]:

1. Адитивні – при формуванні стеганограм розраховується сума коефіцієнтів перетворення зображення-контейнера та взятих із заданим ваговим коефіцієнтом G коефіцієнтів перетворення стегоданих;
2. Квантування – повідомлення приховуються зміною параметрів квантувателя значень яскравості пікселів ЦЗ (наприклад, кроку квантування, порядку слідування векторів кодової книги) за заданим законом;
3. Статистичні – вбудовуються стегодані зміною статистичних параметрів ЦЗ або його окремих частин (наприклад, дисперсії значень яскравості пікселів);
4. Структурні – при формуванні стеганограм проводяться послідовні афінні перетворення (поворот, зсув, масштабування) окремих блоків зображення-контейнера.

Переважна більшість відомих алгоритмів вбудовування повідомлень у ЦЗ належать до класу адитивних методів. Це пояснюється відносною простотою алгоритмів приховання/екстракції, а також можливістю використання різних типів перетворень ЦЗ, що дає змогу підвищити робастність сформованих стеганограм до відомих методів пасивного стегоаналізу.

Узагальнений алгоритм багатоетапного формування стеганограм для випадку вбудовування стегоданих в області перетворення зображення-контейнера наведений на рис. 1.

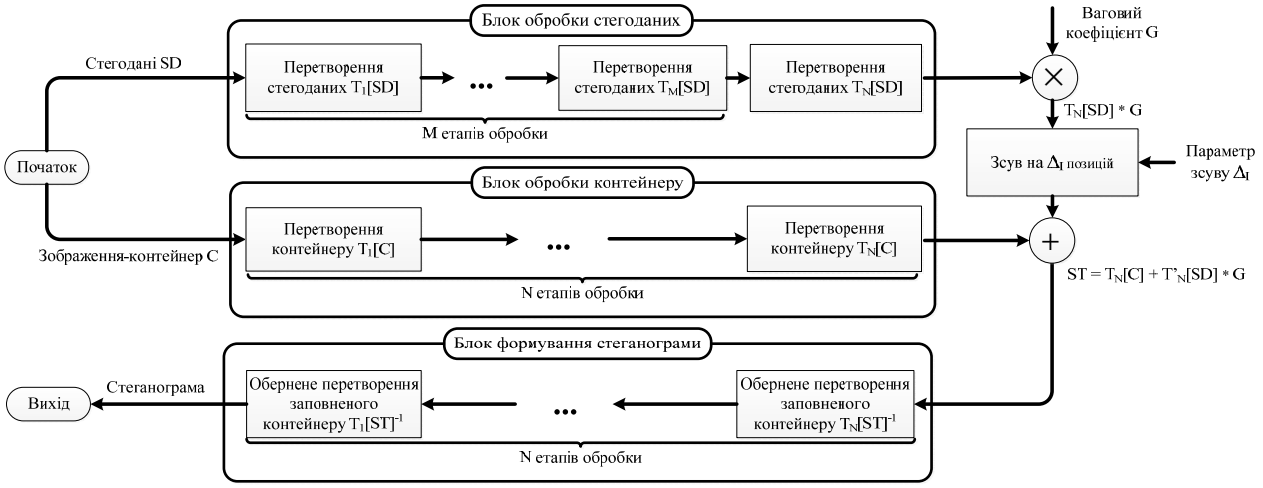

Рис. 1. Узагальнений алгоритм багатоетапного формування стеганограм

У блоках обробки стегоданих та контейнера (рис. 1) проводяться відповідно *M* та *N* етапів перетворень приховуваного повідомлення і ЦЗ. Для попередньої обробки стегоданих широко застосовуються схеми шифрування (наприклад, Triple DES, AES) або методи псевдовипадкової перестановки елементів повідомлення (наприклад, перетворення Арнольда). Для обробки контейнера можна використовувати різні види перетворень: спектральні, наприклад, двовимірне перетворення Фур'є, двовимірне вейвлет-перетворення; матричні, наприклад, сингулярний розклад окремих каналів кольору зображення. Для узгодження форми представлення даних перед формуванням стеганограм на останньому етапі, у кожному блоці обробки (контейнера і стегоданих), до масивів T_N[SD] s T_N[C] застосовується однаковий вид перетворень.

На вхід блоку формування стеганограми (БФС) подається сума коефіцієнтів перетворення контейнера T_N[C] та взятих с заданим ваговим коефіцієнтом G коефіцієнтів перетворення стегоданих T'$_N$[SD], зміщених на Δ_I позицій. Введення вагового коефіцієнта G дає змогу варіювати ступінь візуальних змін контейнера, зумовлених вбудовуванням повідомлень, а зміщення на Δ_I позицій при розрахунках суми коефіцієнтів T_N[C]+T'$_N$[SD]*G підвищує стійкість стеганосистеми до ПС.

При формуванні стеганограми у БФС проводять N обернених перетворень масиву [ST] у порядку, зворотному послідовності проведення перетворень у блоці обробки контейнеру.

Відмітимо, що недоліком багатоетапних методів формування стеганограм є зниження стійкості прихованих повідомлень до методів активного стегоаналізу – незначні зміни стеганограм (наприклад, стиснення чи фільтрація ЦЗ при передачі по каналам зв'язку) можуть призвести до нелінійних спотворень або деструкції вбудованих стегоданих.

У роботі розглянуто такі методи приховання повідомлень в ЦЗ: одноетапний – Дея (Dey) [7] та двоетапний – Елайона (Elahian) [8]. При формуванні стеганограм значення вагового коефіцієнта G для кожного методу змінювалися від мінімального G_{min} (втрата стегоданих в шумах контейнера) до максимального G_{max} (поява візуальних спотворень ЦЗ при вбудовуванні повідомлень) з кроком Δ_G.

Варіограмний аналіз цифрових зображень

У роботі [9] розглянуто ефективний метод аналізу просторово-часових процесів – варіограмний аналіз (ВА). Враховуючи, що при проведенні ВА багатовимірних масивів можливе виявлення областей з аномальними статистичними характеристиками, представляє інтерес його використання для визначення наявності прихованих даних у ЦЗ.

У роботі варіограмний аналіз стеганограм, сформованих за узагальненим адитивним алгоритмом, проведено у декілька етапів.

На першому етапі аналізу розраховано залежність усередненої варіації значень яскравості пікселів рядка/стовпчика ЦЗ $2\gamma(h)$ від величини інтервалу h між ними [9]:

$$2\gamma(h) = \left(1/\left|N(h)\right|\right) \times \sum_{i,\, j \in N(h)} \left(x_i - x_j\right)^2,\ N(h) = \left\{i, j : h = \left|i - j\right|\right\}, \qquad (1)$$

де $N(h)$ – множина всіх інтервалів довжини h у заданому рядку/стовпці ЦЗ.

На другому етапі ВА було проведено апроксимацію $2\gamma(h)$ двома методами: експоненційним та гауссівським. Під час подальших розрахунків використовували результати того методу апроксимації, середнє квадратичне відхилення (СКВ) якого було мінімальним. Вибирали метод з мінімальним СКВ автоматично згідно із розробленим і програмно реалізованим алгоритмом.

На третьому етапі ВА, використовуючи апроксимацію варіограми, визначено такі характеристики розподілу яскравості пікселів рядка/стовпця ЦЗ:

1. Міжелементна варіація (Nugget, N) – характеризує усереднену варіацію значень яскравості сусідніх пікселів;

2. Інтервал кореляції (Range, R) – відповідає інтервалу $h_{\max}$, для якого зберігається кореляція значень яскравості пікселів на рівні Δ_r;

3. Значення S-рівня (Sill, S) – характеризує усереднене значення варіації яскравості пікселів рядка/стовпчика ЦЗ при спрямуванні довжини інтервалу h до нескінченності.

На рис. 2 зображено: профіль яскравості пікселів псевдовипадково обраного рядка каналу зеленого кольору тестового зображення (рис. 2а); варіограму цього профілю, розраховану згідно з (1) та її апроксимацію гауссівським методом (рис. 2б).

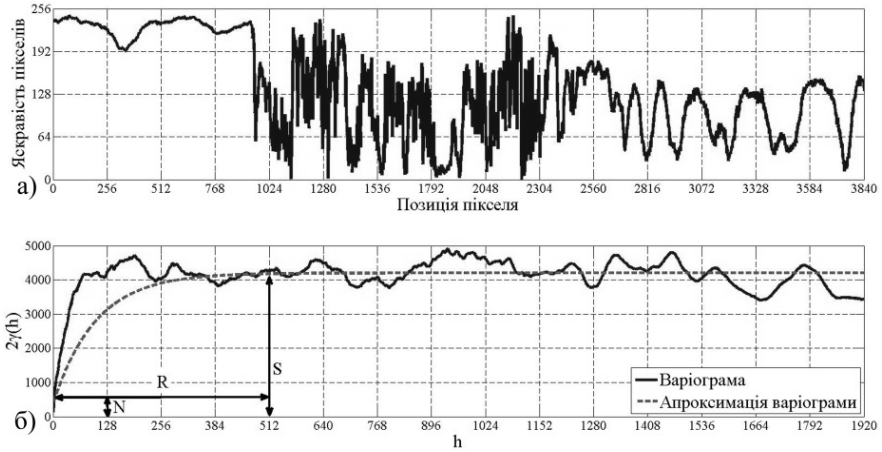

Рис. 2. Результати варіограмного аналізу залежності яскравості пікселів псевдовипадково обраного рядка каналу зеленого кольору тестового зображення від довжини інтервалу h (N=337; R=512; S=4203; Δ_r=0.05)

Оскільки обробка кожного рядка/стовпчика ЦЗ при розрахунках варіограм є обчислювально витратною процедурою, враховуючи значну кореляцію значень яскравості пікселів сусідніх рядків/стовпчиків зображень, ВА проведено для рядків зображення з кроком Δ=1.

Результати досліджень

При формуванні стеганограм був використаний тестовий пакет зі ста зображень-контейнерів з роздільною здатністю UHD-4K (3840x2160 пікселів). Як стегодані було вибрано ЦЗ з різним ступенем деталізації: креслення (567x463 пікселів), карта (800x800 пікселів) та портрет (565x850 пікселів). Ступінь заповнення контейнера варіював у межах від 5% до 25% (з кроком 5%) та від 35 % до 95 % (із кроком 10 %). Вибраний рівень заповнення контейнера забезпечувався масштабуванням зображень-стегоданих.

Формування стеганограм за методом Дея проведено знаходженням суми відповідних коефіцієнтів двовимірного дискретного вейвлет-перетворення (ДДВП) зображення-контейнера та стегоданих, взятих з ваговим коефіцієнтом G (G_{min}=0.02 G_{max}=0.08; Δ_G=0.02). Повідомлення вбудовано в контейнери за методом Елайона у два етапи. На першому етапі проведено: зміну системи кольору зображення-контейнера з RGB на YCbCr; використане перетворення Арнольда [10] для перемішування елементів масиву стегоданих. На другому етапі як до стегоданих, так і Y-каналу (каналу яскравості) зображення-контейнеру було застосовано ДДВП (три рівні декомпозиції), після чого розраховано суму відповідних коефіцієнтів двовимірного дискретного вейвлет-перетворення зображення-контейнера та стегоданих, взятих з ваговим коефіцієнтом G (G_{min}=1; G_{max}=12; Δ_G=4). Які базисні функції ДДВП для обох методів було використано вейвлет Хаара та відповідну йому скейлінг-функцію.

На рис. 3 у вигляді контурних графіків наведено залежності характеристик розподілу значень яскравості пікселів стеганограм (права вісь) при варіації ступеня заповнення контейнера стегоданими (вісь абсцис) та значень вагового коефіцієнта G (вісь ординат):

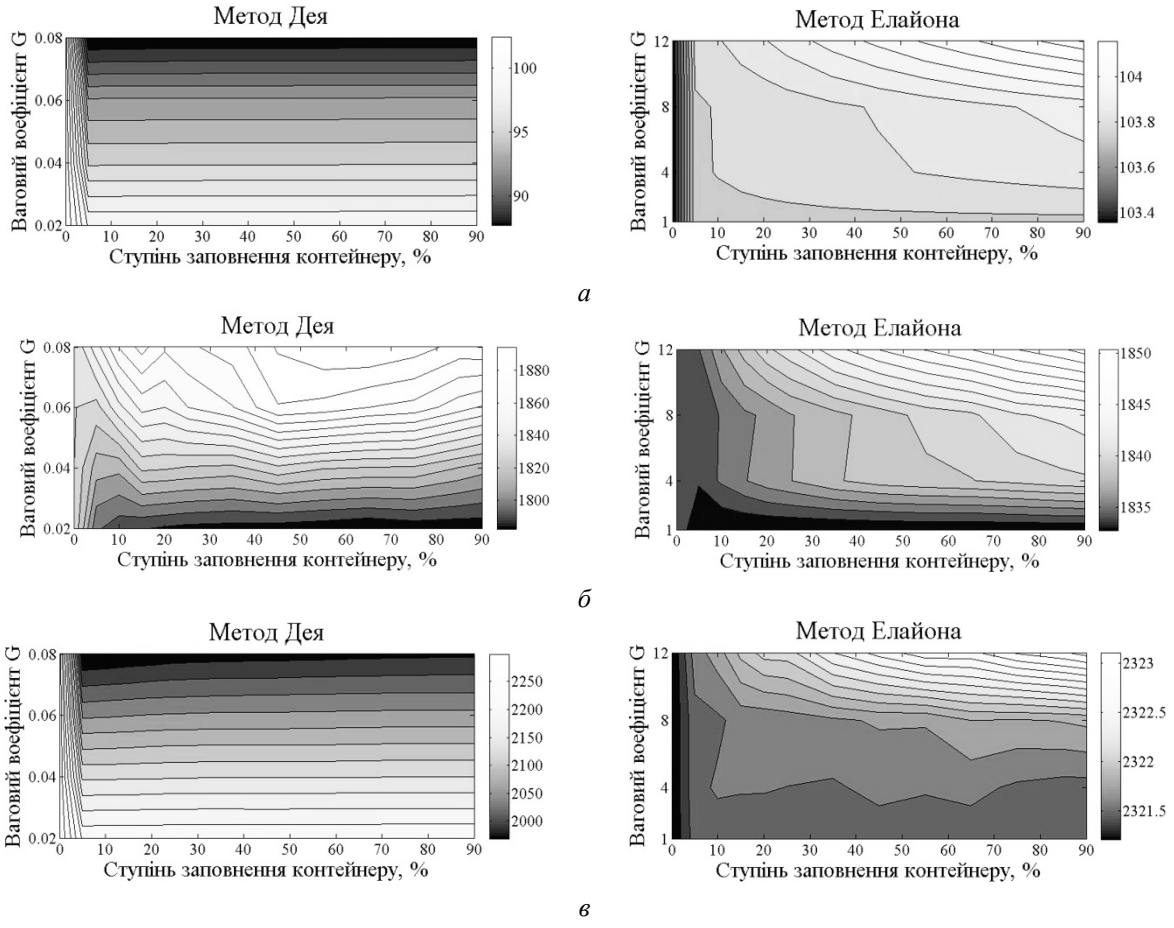

Рис. 3. Залежність характеристик розподілу значень яскравості пікселів у рядках стеганограм (градації сірого кольору) від ступеня заповнення контейнера (вісь абсцис) та вагового коефіцієнта G (вісь ординат): а – міжелементна варіація; б – інтервал кореляції ($\Delta_r = 0.05$); в – S-рівень

Діапазон змін значень досліджуваних характеристик розподілу яскравості пікселів стеганограм (рис. 3) є ширшим для методу Дея (від 20 до 250), ніж для методу Елайона (від 0,1 до 16). Це дає змогу використовувати прості порогові методи обробки результатів ВА стеганограм при налаштуванні СД за методом Дея.

За залежностями характеристик розподілу яскравості пікселів стеганограм (міжелементної варіації та S-рівня) від ступеня заповнення контейнера та значення коефіцієнта G (рис. 3, а, 4), можна визначити, який тип методів (простих чи комплексних) використано для формування стеганограм.

У роботі проведений КА стеганограм та досліджено зміни значень взаємокореляційної функції (ВКФ) сусідніх рядків ЦЗ, що зумовлені вбудовуванням стегоданих. Результати КА для методів Дея (неперервна лінія) та Елайона (штрихова лінія) наведено на рис. 4.

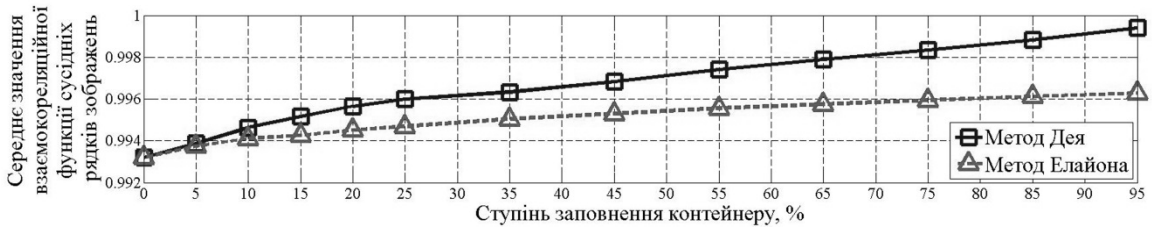

Рис. 4. Усереднені значення взаємокореляційної функції для сусідніх рядків стеганограм

Залежність середніх значень ВКФ яскравості пікселів для сусідніх рядків стеганограм від ступеня заповнення контейнера з використанням обох методів вбудовування стегоданих пояснюється незначним підвищенням середньої яскравості пікселів ЦЗ внаслідок приховання повідомлень. Зміна середніх значень ВКФ при варіації ступеня заповнення контейнера стегоданими від 5 % до 95 % не перевищує 1 %, що суттєво обмежує застосування КА для виявлення стеганограм.

Висновки

У результаті дослідження ефективності використання варіограмного та кореляційного аналізів для виявлення стеганограм встановлено:

1. Аналіз змін характеристик розподілу значень яскравості пікселів стеганограм (міжелементної та S-рівня) дає змогу виявляти приховані повідомлення в ЦЗ навіть за слабкого заповнення контейнера стегоданими (менше 10 %);

2. На основі результатів ВА стеганограм можливе визначення класу методів, використаних для вбудовування стегоданих у контейнер (простих чи багатоетапних), що надалі дає змогу вибрати оптимальний метод деструкції при проведенні активного стегоаналізу;

3. Застосування КА для розпізнавання стеганограм має суттєві обмеження – зміна результатів аналізу є меншою за 1 % при варіації ступеня заповнення контейнера стегоданими в широкому діапазоні значень (від 5 % до 95 %).

1. Fridrich J. Rich Models for Steganalysis of Digital Images / J. Fridrich, J. Kodovsky // IEEE Transactions on Information Forensics and Security. – Vol. 7, No. 3, 2012. – pp. 868–882. 2. Progonov D. O., Kushch S. M. Evaluation of the effectiveness of applying the image quality metrics for acquisition the steganograms. – Proceeding of the 3rd International scientific conference of students and young scientist "Theoretical and applied aspects of cybernetics". – K.: Bukrek, 2013. – pp. 34–42. 3. Голуб В. Комплексный подход для выявления стеганографичсеского скрытия в JPEG-файлах / Голуб В., Дрюченко М. // Инфокоммуникационные технологии. 2009. – Т.7, № 1. – С. 44–50. 4. Ambalavanan A. A Bayesian image steganalysis approach to estimate the embedded secret message / Ambalavanan A., Chandamouli R // Proceeding MM&Sec '05 Proceedings of the 7th workshop on Multimedia and security. – New York, USA, 2005. – pp. 33–38. 5. Прогонов Д. О. Виявлення стеганограм з даними, прихованими в області перетворення цифрових зображень. / Д. О. Прогонов, С. М. Кущ // Вісник НТУУ "КПІ".

Серія – Радіотехніка. Радіоапаратобудування. 2014. – № 57. – С. 128–142. 6. Грибунин В. Цифровая стеганография / В. Грибунин, И. Оков, И. Туринцев, Р. Ковалев, В. Гловачев. – М.: Солон-Пресс, 2002. – 272 с. 7. Dey N. A novel approach of color image hiding using RGB color planes and DWT / Dey N., Roy A.B., Dey S. // International journal of computer application. – Vol. 36, No.5, 2011. – P. 19–24. 8. Elahian A. Improved robust DWT-watermarking in YCbCr color space / Elahian A., Khalili M., Shokouhi S.B. // Global journal of computer application and technology. – Vol. 1, No.3, 2011. – P. 300–304. 9. Cressie N. Statistics for spatio-temporal data / Cressie N., Wikle C. K. – John Wiley & Sons, 2011. – 531 p. 10. Прогонов Д., Кущ С. Варіограмний аналіз стеганограм. – Матеріали III Міжнародної науково-технічної конференції "Захист інформації і безпека інформаційних систем". – Львів: Українська академія друкарства, 2014. – С. 84–85.

УДК 621.3.084.875

В. Я. Пуйда, Н. Т. Мандзевич
Національний університет "Львівська політехніка",
кафедра електронних обчислювальних машин

РОЗРОБЛЕННЕЯ СТРУКТУРНОЇ МОДЕЛІ МІКРОПРОЦЕСОРНОГО ПІД-РЕГУЛЯТОРА

Розглянуто структурне моделювання цифрового мікропроцесорного регулятора температури, що використовує ПІД-алгоритм, за його аналоговим прототипом за допомогою програми сімейства Micro-Cap.

Ключові слова: структурна модель, мікропроцесорний регулятора температури, ПІД-алгоритм, аналоговий прототип, система автоматичного регулювання (САР).

DEVELOPMENT OF STRUCTURAL MODEL FOR MICROPROCESSOR PID-CONTROLLER

The possibility of structural modeling digital microprocessor temperature controller, using PID algorithm in its analog prototype using the family Micro-Cap.

Key words: structural model, microprocessor temperature controller, PID-algorithm, the analogue prototype, system for automatic control (SAC).

Вступ

Метод структурного моделювання має порівняно з методом моделювання за диференціальним рівнянням системи ту перевагу, що дає можливість вводити до складу моделі елементи реальної системи регулювання і легко підбирати параметри кожної ланки моделі, досягаючи бажаного закону регулювання. Крім того, такий метод дає чітке уявлення щодо відповідності параметрів досліджуваної системи та її моделі. Це створює певні зручності як при підборі параметрів самих елементів, так і корегувальних зв'язків. Оскільки параметри кожної ланки моделі однозначно пов'язані з параметрами відповідних ланок реальної системи через постійні масштаби, то результати, одержані при моделюванні, можуть бути пізніше перераховані в параметри ланок реальної системи, за яких досягають необхідного закону керування.