

*Роман Михайлович Штонда  
Наталія Анатолівна Паламарчук  
Юлія Олександрівна Черниш  
Олексій Володимирович Станович*

*Військовий інститут телекомунікацій та інформатизації Державного університету телекомунікацій, Київ, Україна*

## АНАЛІЗ МОДЕЛЕЙ ТА МЕТОДІВ ВБУДОВУВАННЯ ДАНИХ У ЗОБРАЖЕННЯ

Для покращення показників стеганографічного вбудовування даних в зображення потрібно впроваджувати узагальнені моделі та методи вбудовування даних у зображення з метою подальшої адаптації процесу вбудовування в цілому.

В статті проаналізовані узагальнені методи не адаптивного та адаптивного вбудовування даних у зображення. Наведено структурні моделі процесів вбудовування даних у зображення. Для врахування особливостей процесу вбудовування даних у зображення приведені математичні вирази, що описують процеси вбудовування сукупністю множин та перетворень і, таким чином, дозволяють отримати кращі результати.

Виявлено, що врахування зворотних зв'язків між перетвореннями в методах адаптивного вбудовування дозволяє підвищити характеристики вбудовування даних.

**Ключові слова:** методи не адаптивного та адаптивного вбудовування даних; робастність та таємність; зворотні зв'язки; прями зв'язки.

### Вступ

Задача захисту інформації від несанкціонованого доступу вирішувалася на протязі всього часу існування людства. Ще в старі часи виділилося два основних напрямки рішення цієї задачі, яка існує і на цей час: криптографія та стеганографія. Метою криптографії є захист інформації методом її шифрування. На відміну від цього, при стеганографічному захисті інформації (СЗІ) приховується сам факт існування повідомлення.

**Постановка проблеми.** Методи стеганографії зображень, які ґрунтуються на базисних перетвореннях, є більш стійкими до розповсюджених перетворень обробки зображень, що обумовлює їх широке використання. Але разом з тим, до недоліків даних методів СЗІ в комп'ютерних мережах та системах (КМС) слід віднести занижену таємність вбудовування та меншу пропускну спроможність стегоканалу. Покращення показників стеганографічного вбудовування вимагає впровадження узагальнених моделей та методів вбудовування даних у зображення з метою подальшої адаптації процесу вбудовування в цілому.

**Аналіз останніх досліджень і публікацій.** У розробку узагальнених моделей та методів вбудовування даних у зображення значний внесок зробили В.М.Дубовой [1], Р.Н.Кветний [2], І.В.Кузмін [3], В.В.Лукічок [4] та інші. Внесок зазначених авторів полягає в розробці та вдосконаленні узагальнених моделей та методів вбудовування даних у зображення.

**Метою статті** є аналіз методів не адаптивного та адаптивного вбудовування даних у зображення.

### Методи дослідження

У ході дослідження використовувався такий метод як аналіз теоретичних джерел.

### Виклад основного матеріалу дослідження

Серед важливих факторів, що впливають на характеристики стегозображення є: вибір початкового зображення (наприклад, зображення які розповсюджуються частіше, привертають менше уваги у разі їх стеганографічного використання, деталізовані зображення дозволяють вбудувати більше даних); способи бінарної інтерпретації значень коефіцієнтів, отриманих в результаті базисних перетворень; методи генерації стеганографічних ключів [5]; методи шаблонного вбудовування для забезпечення необхідного співвідношення між таємністю та робастністю.

Комплексне врахування особливостей процесу вбудовування даних у зображення, зокрема, досягається шляхом розробки узагальненої моделі процесу вбудовування [1, 2, 3].

Загальний процес вбудовування даних у зображення можливо представити як послідовність взаємопов'язаних перетворень. З метою опису взаємозв'язків між зазначеними перетвореннями пропонується використати теоретико-множинний підхід.

Розглянемо узагальнені моделі та методи не адаптивного та адаптивного вбудовування даних у зображення [4].

**1. Узагальнені моделі та методи не адаптивного вбудовування даних у зображення**

При врахуванні лише прямих зв'язків між перетвореннями отримуємо модель процесу не адаптивного вбудовування даних у зображення, яку можна описати такою сукупністю множин та перетворень [4]:

$$NE = \{I, D, W, T, Q, B, S, Z, P, \tilde{Q}, \tilde{I}, F_T, F_B, F_S, F_P, F_T^{-1}\}, \quad (1)$$

де  $I = \{I_1, I_2, \dots, I_k, \dots, I_K\}$  – множина зображень;  $K$  – кількість зображень у множині  $I$ ;  $D = \{D_1, D_2, \dots, D_u, \dots, D_U\}$  – множина повідомлень;  $U$  – кількість повідомлень у множині  $D$ ;  $W = \{W_1, W_2, \dots, W_g, \dots, W_G\}$  – множина ключів;  $G$  – кількість ключів у множині  $W$ ;  $T = \{T_1, T_2, \dots, T_n, \dots, T_N\}$  – множина безпечних перетворень;  $N$  – кількість базисних перетворень у множині  $T$ ;  $Q = \{Q_1, Q_2, \dots, Q_y, \dots, Q_Y\}$  – множина результатів базисних перетворень;  $Y = K \times N$  – кількість результатів базисних перетворень у множині  $Q$ ;  $V = \{V_1, V_2, \dots, V_m, \dots, V_M\}$  – множина бінарних представлень;  $M$  – кількість різних бінарних представлень у множині  $V$ ;  $S = \{S_1, S_2, \dots, S_a, \dots, S_A\}$  – множина шаблонних перетворень;  $A$  – кількість різних шаблонних перетворень у множині  $S$ ;  $Z = \{Z_1, Z_2, \dots, Z_l, \dots, Z_L\}$  – множина шаблонів;  $L = U \times G \times A$  – кількість шаблонів у множині  $Z$ ;  $P = \{P_1, P_2, \dots, P_c, \dots, P_C\}$  – множина результатів бінарної інтерпретації елементів  $Q$ ;  $C = Y \times M$  – кількість результатів шаблонних перетворень у множині  $P$ ;  $\tilde{Q} = \{\tilde{Q}_1, \tilde{Q}_2, \dots, \tilde{Q}_h, \dots, \tilde{Q}_H\}$  – множина змінених результатів базисних перетворень;  $H = Y \times M \times L \times C$  – кількість результатів базисних перетворень у множині  $\tilde{Q}$ ;  $\tilde{I} = \{\tilde{I}_1, \tilde{I}_2, \dots, \tilde{I}_r, \dots, \tilde{I}_R\}$  – множини стегозображення;  $R = H \times N$  – кількість стегозображень у множині  $\tilde{I}$ ;  $F_T: I \times T \rightarrow Q$  – функція базисних перетворень;  $F_B: Q \times V \rightarrow P$  – функція бінарної інтерпретації елементів  $Q$ ;  $F_S: D \times W \times S \rightarrow Z$  – функція формування шаблонів;  $F_P: Q \times V \times S \times P \rightarrow \tilde{Q}$  – функція шаблонного вбудовування даних;  $F_T^{-1}: Q \times T \rightarrow \tilde{I}$  – функція зворотного базисного перетворення.

Теоретико-множинній моделі (1) відповідає структурна модель процесів не адаптивного вбудовування даних у зображення, яка показана на рис. 1.

Виходячи з цієї моделі, пропонується такий метод не адаптивного вбудовування даних з використанням функцій базисних перетворень [4]:

1. З множини зображень  $I$  вибрати зображення  $I_k$ .

2. З множини базисних перетворень  $T$  вибрати перетворення  $T_n$ . Виконати базисне перетворення  $F_T$ , з використанням набору параметрів базисного перетворення  $T_n$ , до зображення  $I_k$  отримати результат базисного перетворення  $Q_y$ .

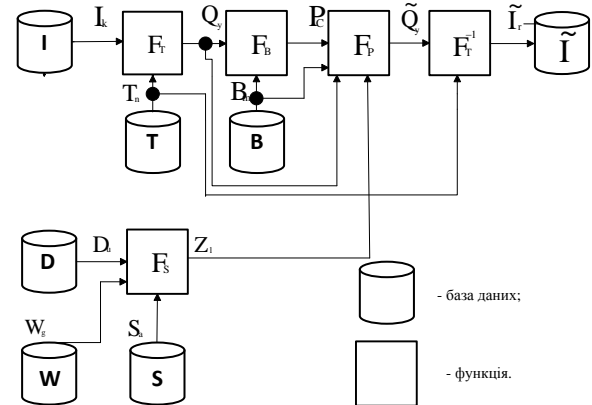
3. З множини бінарних представлень  $V$  вибрати бінарне представлення  $V_m$ . В результаті застосування функції бінарної інтерпретації  $F_B$  до

результату базисного перетворення  $Q_y$  отримати результат бінарної інтерпретації  $P_c$ .

4. З множини повідомлень  $D$  вибрати повідомлення  $D_u$ , з множини ключів  $W$  вибрати ключ  $W_g$  та з множини шаблонних перетворень  $S$  вибрати шаблонне перетворення  $S_a$ . За допомогою функції формування шаблонів  $F_S$  отримати шаблон  $Z_l$ , що належить множині шаблонів  $Z$ .

5. З бінарного представлення  $V_m$ , шаблону  $Z_l$ , результату базисного перетворення  $Q_y$  та результатів бінарної інтерпретації  $P_c$  за допомогою функції шаблонного вбудовування даних  $F_P$  отримати стеганографічно змінений результат базисного перетворення  $\tilde{Q}_h$ .

6. В результаті застосування функції зворотного базисного перетворення  $F_T^{-1}$  з використанням набору параметрів базисного перетворення  $T_n$  до стеганографічно зміненого результату базисного перетворення  $\tilde{Q}_h$  отримати стегозображення  $\tilde{I}_r$ , утворене з  $k$ -го зображення, що належить множині стегозображень  $\tilde{I}$ .



**Рис. 1. Структурна модель процесу не адаптивного вбудовування даних у зображення**

**2. Узагальнені моделі та методи адаптивного вбудовування даних у зображеннях**

Врахування зворотних зв'язків між перетвореннями дозволяє отримати модель процесу адаптивного вбудовування даних у зображення, яку можна описати такою сукупністю множин та перетворень [4]:

$$AE = \{I, D, W, T, Q, B, S, Z, P, \tilde{Q}, \tilde{I}, O, F_T, F_B, F_S, F_P, F_T^{-1}, F_O, F_A, f_B, f_T, f_I, f_S, f_W, f_I\}, \quad (2)$$

де  $F_O: f_{O_1} \times f_{O_2} \times \dots \times f_{O_j} \times \dots \times f_{O_J} \rightarrow O$  – функція комплексного оцінювання стеганографічної таємності;  $f_{O_j}$  – множина комплексних оцінок  $j$ -го параметра;  $\Omega_j: I \times \tilde{I} \rightarrow f_{O_j}$  – функція оцінювання  $j$ -го параметра;  $O = \{O_1, O_2, \dots, O_v, \dots, O_V\}$  – множина значень комплексних оцінок;  $V$  – кількість можливих варіантів комплексних оцінок;  $\tilde{I}_r \in \tilde{I}$  – стегозображення, утворене з  $k$ -го зображення;  $F_A: O \rightarrow x$  – функція адаптації, де  $x = \{1, 2, 3, 4, 5, 6\}$ ;  $f_B(x, m) = \begin{cases} m, & \text{якщо } x \neq 1; \\ m^*, & \text{якщо } x = 1, \end{cases}$  – функція вибору бінарних представлень, де  $m^*$  – номер наступного

бінарного представлення у множині В;  $f_T(x, n) = \begin{cases} n, & \text{якщо } x \neq 2; \\ n^*, & \text{якщо } x = 2, \end{cases}$  – функція вибору базисних перетворень, де  $n^*$  – номер наступного базисного перетворення у множині Т;  $f_I(x, k) = \begin{cases} k, & \text{якщо } x \neq 3; \\ k^*, & \text{якщо } x = 3, \end{cases}$  – функція вибору зображення,  $k^*$  – номер наступного зображення у множині І;  $f_S(x, a) = \begin{cases} a, & \text{якщо } x \neq 4; \\ a^*, & \text{якщо } x = 4, \end{cases}$  – функція вибору шаблонного перетворення, де  $a^*$  – номер наступного шаблонного перетворення у множині S;  $f_W(x, g) = \begin{cases} g, & \text{якщо } x \neq 5; \\ g^*, & \text{якщо } x = 5, \end{cases}$  – функція вибору ключа, де  $g^*$  – номер наступного ключа у множині W;  $f_I(x, r) = \begin{cases} \emptyset, & \text{якщо } x \neq 6; \\ r, & \text{якщо } x = 6, \end{cases}$  – функція вибору стегозображення, де  $\emptyset$  – відсутність зображення.

Моделі, що описується виразом (2), відповідає структурна модель процесів адаптивного вбудовування даних у зображення, яка наведена на рис. 2.

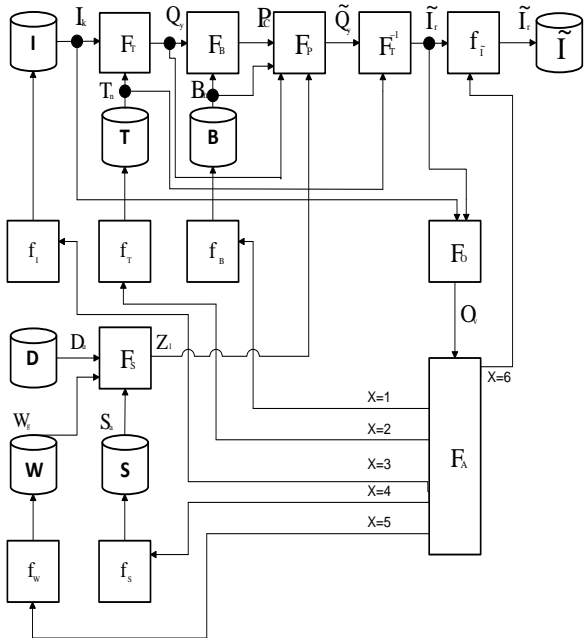


Рис. 2. Структурна модель процесу адаптивного вбудовування даних у зображення

Метод адаптивного вбудовування даних з використанням функцій базисних перетворень можна представити таким чином [4]:

1. З множини зображень І вибрати зображення  $I_k$ .
2. З множини базисних перетворень Т вибрати перетворення  $T_n$ . В результаті застосування функції базисних перетворень  $F_T$ , з використанням набору параметрів базисного перетворення  $T_n$ , до зображення  $I_k$  отримати результат базисного перетворення  $Q_y$ .
3. З множини бінарних представлень В вибрати бінарне представлення  $B_m$ . В результаті

застосування функції бінарної інтерпретації  $F_B$  до результату базисного перетворення  $Q_y$  отримати результат бінарної інтерпретації  $P_c$ .

4. З множини повідомлень D вибрати повідомлення  $D_u$ , з множини ключів W вибрати ключ  $W_g$  та з множини шаблонних перетворень S вибрати шаблонне перетворення  $S_a$ . За допомогою функції формування шаблонів  $F_S$  отримати шаблон  $Z_1$ , що належить множині шаблонів Z.

5. З бінарного представлення  $B_m$ , шаблона  $Z_1$ , результату базисного перетворення  $Q_y$  та результатів бінарної інтерпретації  $P_c$  за допомогою функції шаблонного вбудовування даних  $F_P$  отримати стегографічно змінений результат базисного перетворення  $\tilde{Q}_h$ .

6. В результаті застосування функції зворотного базисного перетворення  $F_T^{-1}$  з використанням набору параметрів базисного перетворення  $T_n$  до стегографічно зміненого результату базисного перетворення  $\tilde{Q}_h$  отримати стегозображення  $\tilde{I}_r$ .

7. В результаті застосування функції комплексного оцінювання стегографічної таємності  $F_O$  до оригінального зображення  $I_k$  та відповідного стегографічно змінено зображення  $\tilde{I}_r$  отримати значення комплексної оцінки  $O_v$ .

8. На основі значення комплексної оцінки  $O_v$  за допомогою функції адаптації  $F_A$  отримати значення змінної x:

якщо  $x=1$ , тоді за допомогою функції  $f_B$  витримати  $m^*$  номер бінарного представлення у множині В та повернутися до пункту 3;

якщо  $x=2$ , тоді за допомогою функції  $f_T$  вибрати  $n^*$  номер базисного перетворення у множині Т та повернутися до пункту 2;

якщо  $x=3$ , тоді за допомогою функції  $f_I$  вибрати  $k^*$  номер зображення у множині І та повернутися до пункту 1;

якщо  $x=4$ , тоді за допомогою функції  $f_S$  вибрати  $a^*$  номер шаблонного перетворення у множині S та повернутися до пункту 4;

якщо  $x=5$ , тоді за допомогою функції  $f_W$  вибрати  $g^*$  номер ключа у множині W та повернутися до пункту 4;

якщо  $x=6$ , тоді за допомогою функції  $f_I$  вибрати  $r$  стегозображення та внести у множини  $\tilde{I}$ .

### Висновки й перспективи подальших досліджень

В статті розглянуто моделі та методи не адаптивного та адаптивного вбудовування даних в зображення. За рахунок врахування зворотних зв'язків між перетвореннями в методах адаптивного вбудовування даних в зображення можливо підвищити характеристики вбудовування та значним чином впливати на таємність і робастність, що в свою чергу призводить лише до незначних спотворень зображення. Загалом, комплексне врахування особливостей процесу вбудовування даних у зображення дає найкращі результати.

*Література*

1. Дубовой В.М. Моделирование систем контролю та керування / Дубовой В.М. – В.: УНІВЕРСУМ, 2005. – 187 с. 2. Кветний Р.Н. Основы моделирования та обчислювальних методів: навч. посіб. / Кветний Р.Н. – В.: ВНТУ, 2007. – 150 с. 3. Кузьмин И.В. Основы моделирования сложных систем / Кузьмин И.В. – К.: ВШ, 2002. – 232 с. 4. Лукічов В.В. Методи та засоби стеганографічного захисту інформації на основі вейвлет-перетворень / Лукічов В.В., Лужецький В.А., Васюра А.С. – В.: ВНТУ, 2014. с. 37-43. 5. Лукічов В.В. Метод виявлення великих простих чисел / Лукічов В.В., Васюра А.С. // Вісник ВПІ – 2003. – № 6. – с.333-339.

**АНАЛИЗ МОДЕЛЕЙ И МЕТОДОВ ВСТРАИВАНИЯ ДАННЫХ В ИЗОБРАЖЕНИЯ**

*Роман Михайлович Штонда  
Наталья Анатольевна Паламарчук  
Юлия Александровна Черныш  
Алексей Владимирович Станович*

*Военный институт телекоммуникаций и информатизации  
Государственного университета телекоммуникаций, Киев, Украина*

*Для улучшения показателей стеганографического встраивания данных в изображение нужно внедрять обобщенные модели и методы встраивания данных в изображения с целью дальнейшей адаптации процесса встраивания в целом.*

*В статье проанализированы обобщенные методы не адаптивного и адаптивного встраивания данных в изображение. Приведены структурные модели процессов встраивания данных в изображение. Для учета особенностей процесса встраивания данных в изображение приведены математические выражения, описывающие процессы встраивания совокупностью множеств и преобразований и, таким образом, позволяют получить лучшие результаты.*

*Выявлено, что учет обратных связей между преобразованиями в методах адаптивного встраивания позволяет повысить характеристики встраивания данных.*

*Ключевые слова:* методы не адаптивного и адаптивного встраивания данных; робастность и секретность; обратные связи; прямые связи.

**MODELS AND METHODS ANALYSIS OF EMBEDDING DATA INTO IMAGES**

*Roman M. Shtonda  
Nataliia A. Palamarchuk  
Yliia O. Chernysh  
Oleksii V. Stanovych*

*Military Institute of Telecommunications and Informatization of State University of Telecommunications, Kyiv, Ukraine*

*For improvement of steganographic embedding data into an image must implement generalized models and methods of embedding data into images to further embedding process adaptation as a whole.*

*In the article the generalized methods of not adaptive and adaptive embedding data into images were analyzed. The structural models of the information embedding processes into image were given. For take into account the peculiarities of the embedding data into images process the mathematical expressions that describe the process of embedding by the aggregate of sets and transformation were presented and thus yield better results.*

*Found that the feedbacks account between transformations in the methods of adaptive embedding may increase the embedding data characteristics.*

*Keywords:* not adaptive and adaptive embedding data methods; robustness and security; feedbacks; direct relationship.

**References**

1. Dubovoy V.M. (2005), Modeling of monitoring and control. [Modeliuvannia system kontroliu ta keruvannia], Universum, Vinnytsia, 187 p. 2. Kvyetnyy R.N. (2007), Fundamentals of modeling and computational methods: teach. guidances. [Osnovy modeliuvannia ta obchysliuvalnykh metodiv]. VNTU, Vinnytsia, 150 p. 3. Kuzmin I.V. (2002), Basics of modeling complex systems. [Osnovy modelirovaniya slozhnykh sistem], HS, Kiev, 232 p. 4. Lukichov V.V., Luzhetskyy V.A., Vasyura A.S. (2014), Methods and tools steganographic information security based on wavelet transformation. [Metody ta zasoby steganohrafichnoho zakhystu informatsii na osnovi veyvlet-peretvoren], VNTU, Vinnytsia, p. 37-43. 5. Lukichov V.V., Vasyura A.S. (2003), Method of identifying large prime numbers. [Metod vyiavlennia velykykh prostykh chysel], Bulletin VPI, Vol. 6, pp. 333–339.

Отримано: 29.01.2015 року