УДК 681.324

О.В. Барабаш, Д.М. Обідін, А.П. Мусієнко

АЛГОРИТМ САМОДІАГНОСТУВАННЯ ТЕХНІЧНОГО СТАНУ ВУЗЛІВ КОМУТАЦІЇ ІНФОРМАЦІЙНИХ СИСТЕМ

В роботі розглядається обробка результатів тестових перевірок системи захисту при виконанні самодіагностування вузлів інформаційної системи за принципом блукаючого діагностичного ядра. По розрахованій ймовірності справного стану кожного вузла приймається рішення про його технічний стан. Пропонується алгоритм аналізу результатів перевірок системи захисту на основі випадкового діагностичного графа. Перевагою запропонованого алгоритму є можливість виконання самодіагностування із достовірністю не нижче заданої, що обумовлено постійним відстеженням структури перевірочних зв'язків і поточного синдрому.

Ключові слова: розподільна інформаційна система, система захисту, самодіагностування, вузол комунікації, блукаюче діагностичне ядро.

Вступ

З появою розподілених інформаційних систем виникла проблема постійного відстеження технічного стану й захищеності їх вузлів комутації та ліній зв’язку. Для вирішення цієї проблеми свого часу було розроблено значну кількість технічних рішень, серед яких перспективною виявилась ідея здійснення самодіагностування окремих вузлів системи іншими. Особливої актуальності ці питання набувають в умовах тривалої автономної роботи інформаційно-керуючих систем, коли звичайні засоби контролю та захисту є недоцільними або неможливими.

Самодіагностуванням називається процес визначення відмовної ситуації в системі шляхом узагальнення результатів взаємних перевірок вузлів комутації. Самодіагностування складається з декількох процедур: виконання перевірок та накопичення діагностичної інформації в кожному вузлі системи, визначення достатності діагностичної інформації, знаходження апостеріорних ймовірностей справного стану вузлів, прийняття рішення про справний чи несправний стан окремих вузлів.

Вперше ідея самодіагностування була запропонована в роботі Ф. Препарата [1]. У подальшому метод само діагностування технічного стану та захисту інформації одержав розвиток у роботах О.А. Машкова [2], О.В. Барабаша [3], Ю.В. Кравченка [4] Г.М. Розорінова [5], В.О. Хорошко [6], О.Г. Корченка [7], С.В. Толюпи [8] та інших. Дослідження проводилися в напрямку розвитку діагностичних моделей та удосконалення методів діагностування та захисту з централізованим і розподіленим діагностичними ядрами, при яких повинен реалізовуватися заданий набір тестових перевірок. У залежності від послідовності виконання перевірок загальний метод поділяється на два види: послідовне і паралельне самодіагностування. Найбільшого поширення набуло паралельне самодіагностування з розподіленим діагностичним ядром [1,2]. В роботі [3] вперше було запропоновано самодіагностування з блукаючим діагностичним ядром при якому перевірки вузлів виконуються випадковим чином.

Актуальність розробки методики самодіагностування з блукаючим діагностичним ядром обумовлена необхідністю підвищення достовірності діагностування і необхідністю виконання фонового діагностування в процесі виконання інформаційною системою основних задач.

Метою даної статті є розробка алгоритму визначення апостеріорних ймовірностей справного стану вузлів комутації інформаційної системи та вдосконаленню її захисту при самодіагностуванні на основі гнучких, випадкових структур перевірочних зв'язків.

Постановка завдання

При виконанні самодіагностування результати перевірок накопичуються в вузлах згідно способу умовної передачі [3]. Вважається, що прийнята система оцінювання Препарата [1], за якою результат перевірки має значення 0 при позитивному результаті, 1 – при негативному та випадковій величині $X \in (0,1)$ з ймовірністю $0{,}5$, якщо перевірку

виконував несправний вузол. Множина результатів перевірок отримала назву синдрому R_ϕ. Необхідно визначити апостеріорні ймовірності справного стану кожного вузла з урахуванням отриманого синдрому R_ϕ для прийняття рішення щодо технічного стану вузлів.

Суть методики визначення апостеріорних ймовірностей розглянемо на простому прикладі.

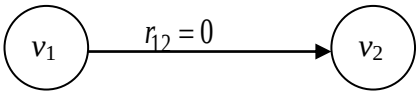

Рис.1. Елементарна перевірка з позитивним результатом

Приклад 1. Припустимо, що система має два вузли комутації ν_1 і ν_2. Відомо, що апріорно з ймовірністю p_1 і p_2, відповідно, вони знаходяться в справному стані, а з ймовірністю $q_i = 1 - p_i$, $i = 1,2$ – в несправному стані. В результаті діагностування виконана одна перевірка t_{12}, результат перевірки $r_{12} = 0$ (рис. 1).

До виконання перевірки в системі можливі такі гіпотези: $H_1 - \nu_1$ і ν_2 справні; $H_2 - \nu_1$ несправний, ν_2 справний; $H_3 - \nu_1$ справний, ν_2 несправний; $H_4 - \nu_1, \nu_2$ несправні.

Ймовірність цих гіпотез має такі значення:

$$P(H_1) = p_1 p_2; \quad P(H_2) = q_1 p_2; \quad P(H_3) = p_1 q_2; \quad P(H_4) = q_1 q_2.$$

Оскільки гіпотези $H_1,...,H_4$ утворюють повну групу подій, то сума їх ймовірностей рівна 1:

$$\sum_{i=1}^{4} P(H_i) = 1.$$

Позначимо через A подію, що полягає в тому, що в системі виконана перевірка t_{12} та її результат $r_{12} = 0$. Виходячи з системи оцінювання Препарату [1], можна визначити умовну ймовірність появи події A за умови прийняття гіпотези H_i, $i = \overline{1,4}$:

$$P(A/H_1) = 1; \quad P(A/H_2) = p_r; \quad P(A/H_3) = 0; \quad P(A/H_4) = p_r,$$

де $p_r = 0,5$ – ймовірність отримання нульового результату перевірки, виконаної несправним вузлом.

За формулою повної ймовірності обчислимо ймовірність події A:

$$P(A) = \sum_{i=1}^{4} P(H_i) \cdot P(A/H_i) = p_1 p_2 + p_r q_1 p_2 + p_r q_1 q_2 = p_1 p_2 + p_r q_1. \qquad (1)$$

На підставі теореми Байєса можна визначити умовну ймовірність прийняття гіпотез H_i за умови виконання події A:

$$P(H_1/A) = \frac{P(H_1) \cdot P(A/H_1)}{P(A)} = \frac{p_1 p_2}{p_1 p_2 + q_1 p_r}; \qquad (2)$$

$$P(H_2/A) = \frac{P(H_2) \cdot P(A/H_2)}{P(A)} = \frac{q_1 p_2 p_r}{p_1 p_2 + q_1 p_r};$$

$$P(H_3/A) = \frac{P(H_3) \cdot P(A/H_3)}{P(A)} = \frac{p_1 q_2 \cdot 0}{p_1 p_2 + q_1 p_r} = 0;$$

$$P(H_4/A) = \frac{P(H_4) \cdot P(A/H_4)}{P(A)} = \frac{q_1 q_2 p_r}{p_1 p_2 + q_1 p_r}.$$

Вузол ν_2 може бути визнаний справним при ухваленні гіпотези H_1 або H_2, які є незалежними, що дає можливість застосування теореми складання ймовірностей. Апостеріорна ймовірність справного стану ν_2, з урахуванням виконання події A:

$$p_2^* = P(H_1/A) + P(H_2/A) = \frac{p_1 p_2 + q_1 p_2 p_r}{p_1 p_2 + q_1 p_r}. \quad (3)$$

Якщо прийняти, що апріорні ймовірності справного стану вузлів ν_1 та ν_2 однакові і дорівнюють $p_1 = p_2 = 0{,}8$, то апостеріорна ймовірність $p_2^* = 0{,}973$. За формулою (3) побудована залежність $p_2^* = f(p_2)$ (рис. 2, крива $Pa(p)$). Аналіз даної залежності показує, що виконання однієї перевірки з результатом 0 підвищує ймовірність справного стану вузлів.

З розрахунків, зведених до таблиці 1, обчислюється апостеріорна ймовірність справного стану ν_2:

$$p^*_2 = p(H_1/A) + p(H_2/A) = \frac{p_1 \cdot p_2 \cdot 0 + q_1 \cdot p_2 \cdot p_r}{q_1 \cdot p_r + p_1 \cdot q_2} = 0{,}308 \quad (4)$$

Таблиця 1

Розрахунок апостеріорної ймовірності справного стану ν_2 при $R_\phi = \{r_{12}\} = 1$ і $p_1 = p_2 = 0{,}8$

$p(H_i)$	$p(A/H_i)$	$p(H_i/A)$
$p(H_1) = p_1 \cdot p_2$	$p(A/H_1) = 0$	$p(H_1/A) = \frac{p_1 \cdot p_2 \cdot 0}{q_1 \cdot p_r + p_1 \cdot q_2} = 0$
$p(H_2) = q_1 \cdot p_2$	$p(A/H_2) = p_r$	$p(H_2/A) = \frac{q_1 \cdot p_2 \cdot p_r}{q_1 \cdot p_r + p_1 \cdot q_2} = 0{,}308$
$p(H_3) = p_1 \cdot q_2$	$p(A/H3) = 1$	$p(H_3/A) = \frac{p_1 \cdot q_2 \cdot 1}{q_1 \cdot p_r + p_1 \cdot q_2} = 0{,}615$
$p(H_4) = q_1 \cdot q_2$	$p(A/H_4) = p_r$	$p(H_4/A) = \frac{q_1 \cdot q_2 \cdot p_r}{q_1 \cdot p_r + p_1 \cdot q_2} = 0{,}077$

Аналіз результатів розрахунків (табл.1) показує, що виконання перевірки з результатом 1 знижує апостеріорну ймовірність. За формулою (4) побудована залежність $p_2^* = f(p_2)$ (рис. 2, крива $Pb(p)$).

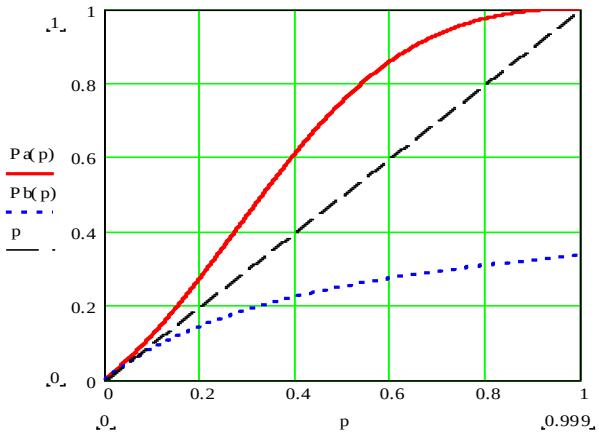

Рис. 2. Залежність апостеріорної ймовірності p_2^* від апріорної ймовірності справного стану p при $r_{ij} = 0$ (крива $P_a(p)$ та при $r_{ij} = 1$ (крива $P_a(p)$

Аналіз даної залежності показує, що виконання однієї перевірки з результатом $r_{ij}=1$ знижує ймовірність справного стану вузлів.

Приклад 2. Припустимо, що на деякий момент часу при діагностуванні системи з $N=6$ вузлів, виконані перевірки, які створили діагностичний граф (рис.3). Результати перевірок виділені кольором ребер на графі. Апріорна ймовірність справного стану вузлів $p_i=p$, $q_i=1-p_i$, $i=\overline{1,6}$. Використовуючи байєсівське оцінювання одержимо апостеріорну ймовірність справного стану вузлів.

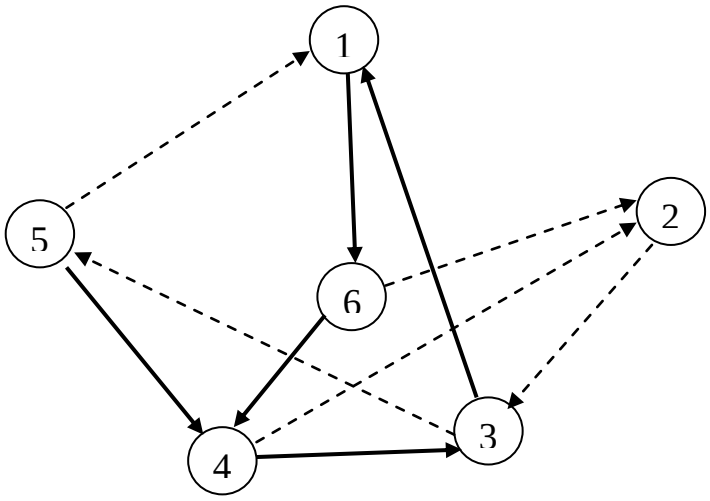

Рис. 3. Поточна структура перевірочних зв'язків:
$\longrightarrow$ $r_{ij}=0$; $\dashrightarrow$ $r_{ij}=1$

Припустимо, що в системі було виконано 10 перевірок і один з вузлів накопичив таку діагностичну інформацію:

$$R_{\phi}=\{r_{16}=0, r_{23}=1, r_{31}=0, r_{35}=1, r_{42}=1, r_{43}=0, r_{51}=1, r_{54}=0, r_{62}=1, r_{64}=0\}$$

Матриця синдрому має вигляд:

$$R_{\Phi}=\begin{pmatrix} - & - & - & - & - & 0 \\ - & - & 1 & - & - & - \\ 0 & - & - & - & 1 & - \\ - & 1 & 0 & - & - & - \\ 1 & - & - & - & 0 & - \\ - & 1 & - & 0 & - & - \end{pmatrix}. \qquad (5)$$

З урахуванням одержаного синдрому R_{ϕ} можливі тільки три гіпотези. Їх апріорна ймовірність $p(H_i)$ та умовні ймовірності $p(A/H_i)$ отримання R_{ϕ} при ухваленні гіпотези H_i:

$$\begin{aligned} p(H_1)&=p_1\cdot q_2\cdot p_3\cdot p_4\cdot q_5\cdot p_6=p^4\cdot q^2; & p(A/H_1)&=p_r{}^3; \\ p(H_2)&=q_1\cdot p_2\cdot q_3\cdot q_4\cdot q_5\cdot q_6=p\cdot q^5; & p(A/H_2)&=p_r{}^9; \\ p(H_3)&=q_1\cdot q_2\cdot q_3\cdot q_4\cdot q_5\cdot q_6=q^6; & p(A/H_3)&=p_r{}^{10}, \end{aligned} \qquad (6)$$

де $p_r=0{,}5-$ ймовірність отримання результату перевірки, виконаної несправним вузлом, згідно системі оцінювання [1]; p_i – ймовірність справного стану вузла v_i.

Оскільки інші (2^6-3) гіпотез, які доповнюють вищевказані до повної групи подій, мають $p(A/H_i)=0$, то їх можна не враховувати. Повна ймовірність події A – отримання $R_ф$:

$$p(A)=\sum_{i=1}^{3} p(H_i)\cdot p(A/H_i)=p^4\cdot q^2\cdot {p_r}^3+p\cdot q^5\cdot {p_r}^9+q^6\cdot {p_r}^{10}. \quad (7)$$

Апостеріорні ймовірності прийняття гіпотез:

$$p(H_1/A)=\frac{p^4\cdot q^2\cdot {p_r}^3}{p(A)};$$

$$p(H_2/A)=\frac{p\cdot q^5\cdot {p_r}^9}{p(A)}; \quad (8)$$

$$p(H_3/A)=\frac{q^6\cdot {p_r}^{10}}{p(A)}.$$

Апостеріорні ймовірності справного стану вузлів:

$$p_1^*=p_3^*=p_4^*=p_6^*=p(H_1/A); \quad (9)$$

$$p_2^*=p(H_2/A); \qquad p_5^*=0.$$

На підставі виразів (6)-(9) побудовані графіки залежностей p_i^* від p для $i=1,2,5$ (рис. 4). Числові значення p_i^* для $p=0{,}8$:

$$p_1^*=p_3^*=p_4^*=p_6^*=0{,}99951; \quad p_2^*=0.00024; \quad p_5^*=0. \; p_5^*=0. \quad (10)$$

Аналіз отриманих значень дозволяє зробити висновок, що справними є вузли ν_1, ν_3,

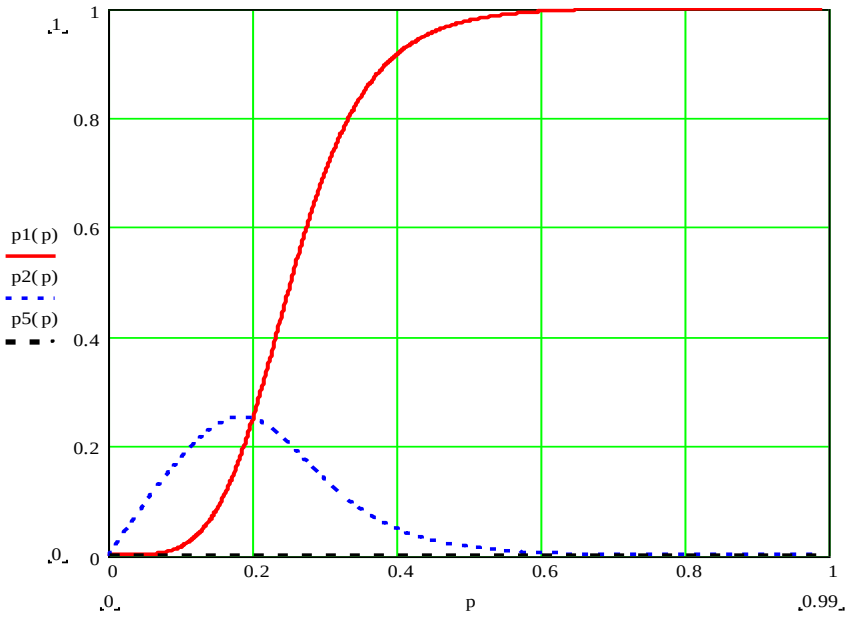

Рис. 4. Графіки залежностей апостеріорних ймовірностей справного стану вузлів для діагностичного графа (рис. 3)

ν_4, ν_6, а несправними ν_2, ν_5. Таким чином, по знайденій апостеріорній ймовірності можна робити висновок про справність або несправність вузлів тієї або іншої підмножини [9]. Слід зазначити, що, взагалі, виконані перевірки не можуть змінити (підвищити або знизити) надійність вузла (ймовірність справного стану). Тому дана ймовірність має сенс достовірності прийняття рішення, за яким можна судити про справність вузла.

Оцінюючи кількісні значення p_i^* можна зробити такі висновки.

1. Чим вища апріорна ймовірність справного стану вузла, тим вища його апостеріорна ймовірність, і навпаки.

2. Найбільш підвищує апостеріорну ймовірність справного стану вузлів циклічна структура, в якій вузли утворюють замкнутий контур з нульовими результатами перевірок. Наявність такого замкнутого контуру в поточній структурі дає можливість з достовірністю $0{,}998$ (при $p = 0{,}8$ і $N = 3$) стверджувати, що всі вузли в замкнутому "нульовому" контурі справні.

3. У структурах з "нульовими" перевірками збільшення числа перевіряючих вузлів приводить до помітного підвищення ймовірності p_i^* справних вузлів. В структурах з "одиничними" перевірками це приводить до пониження значення p_i^* несправних вузлів. Це дозволяє підвищити достовірність прийняття тієї або іншої відмовної ситуації.

4. Розрахунок значень p_i^* по розробленій методиці дає можливість оцінювати достовірність діагностування.

На підставі викладеної методики розроблений алгоритм визначення p_i^* для поточних структур перевірочних зв'язків.

Особливістю даного алгоритму є використання ідеї відсікання невірних гіпотез в процесі визначення ймовірності $p(A/H_i)$ з метою скорочення трудомісткості алгоритму, яка дорівнює $O(2^N)$, де N – число вузлів системи.

Алгоритм визначення апостеріорної ймовірності справного стану вузлів на основі одержаного R_ϕ.

Позначення в алгоритмі: N – число вузлів системи, M – число виконаних перевірок в системі $m = \overline{1, M}$; K – число перспективних гіпотез $k = \overline{1, K}$; $S = \{s_n\}$, $s_n = 0 \vee 1$ – булевий вектор, що позначає поточну гіпотезу: $s_n = 0$ – справний стан ν_n, $s_n = 1$ – несправний стан ν_n; $H = \{H_{kn}\}$ – матриця перспективних гіпотез, для яких $p(A/H_k) = 0$; $p_r = 0{,}5$ – ймовірність правильного результату перевірки, виконаної несправним вузлом.

Крок 0. Згенерувати нульову гіпотезу $S = \{0,0,...,0\}$. Якщо, $\sum_{i,j} r_{ij} = 0$ то всі вузли справні, перейти до кроку 10. Інакше – перейти до кроку 1.

Крок 1. Згенерувати чергову гіпотезу S шляхом інкрементації двійкового числа: $S_{(2)} := S_{(2)} + 1$.

Крок 2. Визначення $p(A/S)$. Привласнити $m := 0$; $p(A/S) := 1$.

Крок 3. Привласнити $m := m + 1$. Проаналізувати m-тий результат перевірки $r_{ij} \in R_\phi$. Поки $m \le M$ для індексів i та j виконати крок 4.

Крок 4. Якщо $(s_i) = 1$, то $p(A/S) := p(A/S) \cdot p_r$ і перейти до кроку 3.

Якщо $[(s_i = 0) \,\&\, (s_j = 0) \,\&\, r_{ij} = 0]$, то $p(A/S) := p(A/S) \cdot 1$ і перейти до кроку 3.

Якщо $[(s_i = 0) \,\&\, (s_j = 1) \,\&\, r_{ij} = 0]$, то перейти до кроку 1.

Якщо $[(s_i = 0) \,\&\, (s_j = 0) \,\&\, r_{ij} = 1]$, то перейти до кроку 1.

Якщо $[(s_i = 0) \,\&\, (s_j = 1) \,\&\, r_{ij} = 1]$, то $p(A/S) := p(A/S) \cdot 1$ і перейти до кроку 3.

Крок 5. Привласнити $k := k + 1$. Запам'ятати перспективну гіпотезу $H(k,n) := S$. Запам'ятати її умовну ймовірність $p(A/H_k) := p(A/S)$. Обчислити $p(H_k) : p(H_k) := 1$. Для $n = \overline{1, N}$ виконати

$$p(H_k) := p(H_k) \cdot p^{(s_n+1) \bmod 2} \cdot q^{s_n}. \quad (11)$$

Крок 6. Якщо $S = \{1,1,...,1\}$, то перейти до кроку 7, інакше – до кроку 1.

Крок 7. Визначення $p(A)$. Привласнити $p(A) := 0$; $K := k$. Для $k = \overline{1,K}$ виконати: $p(A) := p(A) + p(H_k) \cdot p(A/H_k)$.

Крок 8. Визначення $p(H_k/A)$. Для $k = \overline{1,K}$ виконати:

$$p(H_k/A) := p(H_k)p(A/H_k)/p(A).$$

Крок 9. Визначення p_i^*. Для $i = \overline{1,N}$ виконати: $p_i^* := 0$, для $k = \overline{1,K}$ виконати: Якщо $H(k,i) = 0$, то $p_i^* := p_i^* + p(H_k/A)$.

Крок 10. Виведення p_i^*. Кінець алгоритму.

Таким чином, внаслідок виконання алгоритму, визначається апостеріорна ймовірність справного стану кожного вузла системи. Після цього, на підставі знайденої ймовірності, необхідно визначити, яка з підмножин вузлів є підмножиною справних вузлів, а яка – підмножиною несправних.

Висновки

У статті запропоновано алгоритм визначення апостеріорних ймовірностей справного стану вузлів інформаційної системи в процесі виконання самодіагностування на основі випадкового діагностичного графа. Алгоритм заснований на байєсівському оцінюванні, що гарантує його збіжність. Трудомісткість алгоритму складає $O(2^N)$, де N – число вузлів системи. Це накладає обмеження по обчислювальній продуктивності на використання алгоритму. Перевагою запропонованого алгоритму є можливість виконання самодіагностування із достовірністю не нижче заданої, що обумовлено постійним відстеженням структури перевірочних зв'язків і поточного синдрому.

Література

1. Preperata F.P., Metze G., Chien H.T. On the connection assignment problem of diagnosable systems. – IEEE Trans. Elektron. Comput., 1967. EC-16, №12, P.848–854.

2. Машков О.А. Синтез високоточної радіонавігаційної системи на основі метода аналізу ієрархій показників якості / О.А. Машков, Ю.В. Кравченко, В.А. Савченко // Моделювання та інформаційні технології: зб. наук. пр. ІПМЕ НАН України. – 2003. – Вип. 22. – С. 41–48.

3. Барабаш О.В. Построение функционально устойчивых распределенных информационных систем / О.В. Барабаш. – К.: НАОУ, 2004. – 226 с.

4. Кравченко Ю.В. Применение метода последовательного увеличения ранга k-однородного матроида в задаче синтеза структуры псевдоспутниковой радионавигационной системы / Ю. В. Кравченко // Сучасні інформаційні технології у сфері безпеки та оборони. – 2008. – №2(2). – С. 19–22.

5. Брягин О.В. Определение степени независимости отсчетов случайных процессов / О.В. Брягин, А.К. Егоров, Г.Н. Розоринов // Реєстрація, зберігання і обробка даних. – 2004. –Т.6, №4. – С.29-37.

6. Піскун С.Ж. Функціональна ієрархія і алгоритм управління складними технічними системами / С.Ж. Піскун, В.О. Хорошко, Ю.Є. Хохлачова // Захист інформації, – 2013. – №4(15). – С. 327–331.

7. Корченко А.Г. Особенности использования современных квантовых технологий для обеспечения конфиденциальной связи / А.Г. Корченко, В.М. Рудницкий, С.О. Гнатюк // Зб. науч. тр. ХУПС. – 2011. – Вип. 2(28). – С. 80–83.

8. Толюпа С.В. Структура інформаційної мережі та показники її ефективності. / С.В. Толюпа, А.В. Сухін. // Зб. наук. праць КВІУЗ – 2001. – № 3.– С. 68–73.

9. Машков В.А. Организация самоконтроля многомодульных систем на основе оптимальных структур проверочных связей / В.А. Машков, О.В. Барабаш // Электронное моделирование. – 1995. – № 3(17). – С.68–75.

Надійшла 22.05.2014 р. Рецензент: д.т.н., проф. Розорінов Г.М.

УДК 004.056.5

И.И. Бобок, О.В. Костырка

АНАЛИЗ УСТОЙЧИВОСТИ НОВОГО СТЕГАНОГРАФИЧЕСКОГО АЛГОРИТМА К СТЕГАНОАНАЛИТИЧЕСКИМ АТАКАМ

В статье рассмотрена эффективность детектирования нового стеганографического алгоритма, производящего вложение дополнительной информации в пространственной области контейнера-изображения, современными стеганоаналитическими комплексами. Показана устойчивость анализируемого алгоритма к стеганоанализу. Продемонстрирована зависимость эффективности стеганоаналитических программных комплексов от значения показателя качества цифровых изображений. Приведены результаты вычислительных экспериментов.

***Ключевые слова*:** стеганография, стеганоанализ, эффективность детектирования.

Введение

Трагические события 11 сентября 2001 г., повлекшие за собой ограничение, а в некоторых странах, в том числе, и в Украине, запрет шифрования на законодательном уровне, привели к значительной активизации разработок в области стеганографии. В свою очередь, активизация научной деятельности в области стеганографии, публикации новых результатов в открытой печати привели к росту возможностей использования получаемых разработок различными антигосударственными, террористическими структурами. В силу вышесказанного симметричным ответом стало развитие разработок в направлении повышение эффективности стеганоанализа.

На сегодняшний день стеганографический алгоритм может позиционироваться как эффективный только в том случае, если он является устойчивым к стеганоанализу. В силу этого вопрос оценки такой устойчивости является *актуальным* для каждого стеганометода и алгоритма.

Постановка задачи

В [1] авторами был предложен новый стеганографический метод, получивший свою реализацию в виде алгоритма SA, устойчивого к возмущающим воздействиям, осуществляющего погружение дополнительной информации в пространственной области изображения-контейнера, основанного на достаточном условии такой устойчивости, полученном в [2]. Достаточное условие обеспечивается организацией стеганопреобразования путем корректировки яркости пикселей $l \times l$ блоков матрицы цифрового изображения-контейнера. Разбиение на блоки осуществляется стандартным образом. Корректировка на значение $\pm \Delta b$ производится при погружении в очередной блок B очередного бита дополнительной информации, при этом Δb должно удовлетворять следующему условию: $|\Delta b| = \left| \frac{\Delta \sigma_1}{l} \right| > \frac{\left\| \Delta \overline{B} \right\|_2}{l}$, где $\Delta \sigma_1$ - возмущение максимального сингулярного числа блока B при стеганопреобразовании, а $\left\| \Delta \overline{B} \right\|_2$ - спектральная норма матрицы предполагаемого возмущения блока стеганосообщения.

Декодирование дополнительной информации в SA после предварительного разбиения матрицы стеганосообщения и контейнера на $l \times l -$ блоки $\overline{\overline{B}}$ и B соответственно сводится к сравнению количеств положительных и отрицательных элементов в матрице $\Delta B = \overline{\overline{B}} - B$.

С учетом вышесказанного целью настоящей статьи является исследование устойчивости алгоритма SA к стеганоанализу, проводимому современными программными комплексами.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Для всестороннего анализа рассматриваемого алгоритма выделить среди современных стеганоаналитических комплексов такие, которые имеют разные математические основы, используют разные математические инструменты;
2. Определить слабые места в построении и функционировании современных стеганоаналитических комплексов;
3. Провести вычислительный эксперимент и получить числовые характеристики эффективности стеганоанализа для исследуемого стеганографического алгоритма.

Основная часть

Стеганоанализ сегодня развивается в двух основных направлениях: разработка алгоритмов, позволяющих детектировать результаты работы конкретных стеганографических методов, и так называемых, универсальных, или слепых (*blind*), методов, позволяющих путем выявления или констатации отсутствия определенных характерных признаков в анализируемом контенте делать вывод о произведенном внедрении конфиденциальной информации или отсутствии такового, не привязываясь к конкретике использованного стеганографического алгоритма [3].

В процессе достижения поставленной цели первоначально была проведена серия экспериментов с использованием 250 цифровых изображений размером 1000×1000 пикселей (цветовая схема RGB) в формате JPEG из базы изображений NRCS [4], а также фотографий, полученных непрофессиональными фотографами. Погружение дополнительной информации происходило в синюю состаляющую изображения-контейнера. С учетом того, что в работе [5] было показано, что алгоритм *SA* является устойчивым к сжатию, стеганосообщения были сохранены в формате JPEG с различными коэффициентами качества (QF, *quality factor*) – от 50 до 100 с шагом 10, после чего подвергались стеганоанализу.

Использованные стеганоаналитические комплексы представлены следующими продуктами:

1. CANVASS 1.0 (разработка 2009 г.).
2. StegAlyzerSS 3.0 (2007 г.).
3. Stegdetect 0.6.3 (2004 г.).

Данные стеганоаналитические комплексы являются широко используемыми, современными и доступными для свободного (неправительственного) применения, кроме того, как будет показано ниже, они отличаются своими математическими основами.

Результаты эксперимента

Наихудшие результаты показал StegAlyzerSS [6], или Steganography Analyzer Signature Scanner, – данный комплекс не смог осуществить детектирование вложений ни в одной из групп изображений с различным QF.

На первый взгляд, результат кажется фантастическим, однако, если разобраться в принципе работы сканера, то можно понять, что объяснение данного факта лежит на поверхности.

Представленный программный продукт является сигнатурным сканером, а это значит, что принцип его работы базируется на поиске масок и сигнатур различных известных на данный момент стеганографических методов и алгоритмов. Таким образом, любой новый стеганоалгоритм, не внесенный ещё в базы компании-производителя, будет «не замечен» данным программным комплексом.

Этим примером авторы настоящей работы хотели бы обратить внимание научной общественности на бессмысленность дальнейших разработок сигнатурных сканеров для решения задач стеганоанализа. Будущее стеганоанализа может быть связано только со «слепыми» методами, сигнатурные же методы обречены на вечную роль «догоняющего» в гонке с разработчиками стеганографических алгоритмов.

Следующей была проанализирована работа программного комплекса Stegdetect, разработанного в 2000-х гг. Н. Провосом. Данный комплекс способен обнаруживать скрытую информацию в изображениях JPEG-формата, внедренную различными известными алгоритмами стеганографии (например, jsteg, jphide, F5 и т.д.), а также автоматически обнаруживать новые методы стеганографии при помощи линейного дискриминантного анализа [7].

Результаты работы этого комплекса, как и остальных, продемонстрированы в табл. 1. Эффективность детектирования (здесь и далее под эффективностью детектирования будет пониматься процент верно детектированных стеганосообщений от общего числа анализируемых) данного комплекса ни в одной из групп не превысила 13%.

Низкий уровень детектирования данным стеганоаналитическим комплексом, по-видимому, связан с использованием линейного дискриминантного анализа для классификации изображений.

Линейный дискриминантный анализ – методы статистики и машинного обучения, применяемые для нахождения линейных комбинаций признаков, наилучшим образом разделяющих два или более классов объектов или событий. Полученная комбинация может быть использована в качестве линейного классификатора или для сокращения размерности пространства признаков перед последующей классификацией.

Линейный дискриминантный анализ для случая двух классов (а именно это и ставится в задачу стеганоаналитического комплекса – отделить стеганограммы от пустых контейнеров) осуществляется следующим образом: для каждого образца объекта или события с известным классом y рассматривается набор наблюдений x (называемых ещё признаками, переменными или измерениями). Набор таких образцов называется обучающей выборкой. Задачи классификации состоит в том, чтобы построить хороший прогноз класса y для всякого так же распределённого объекта (не обязательно содержащегося в обучающей выборке), имея только наблюдения x [8].

Таким образом, чем больше количество наблюдений, тем вероятно более эффективной будет работа данного стеганоаналитического программного продукта. Данный факт никак не может быть оценен нами как достоинство, это скорее – недостаток.

Следующей была проанализирована работа программного комплекса Canvass, основанного на частично упорядоченных марковских моделях, которые использованы для метода опорных векторов [9]. Эффективность данного комплекса максимальная из всех рассматриваемых в данной работе, однако стоит отметить, что как видно из табл. 1, максимум эффективности достигается при QF от 50 до 70. При высоком качестве стеганограмм данный программный комплекс не особо выделяется на фоне выше рассмотренного stegdetect'a. Эффективность детектирования для группы QF = 75 будет примерно на уровне 50%, что соответствует в бинарном классификаторе случайному отнесению объекта к классу.

Авторы настоящей статьи считают, что использования JPEG с низким QF является неоправданным, ввиду нарушения восприятия даже изображений-контейнеров, а так же излишне привлекающим внимание наличием артефактов особенно на фоновой составляющей.

Таблица 1

Эффективность детектирования нового стеганографического алгоритма современными стеганоаналитическими комплексами

Стеганоаналитический комплекс	Эффективность детектирования, %					
	QF = 50	QF = 60	QF = 70	QF = 80	QF = 90	QF = 100
Canvass	83,6	83,1	72,6	37,2	9,1	1,8
Stegdetect	0	1,6	0,5	13,5	3,1	1
StegAlyzerSS	0					

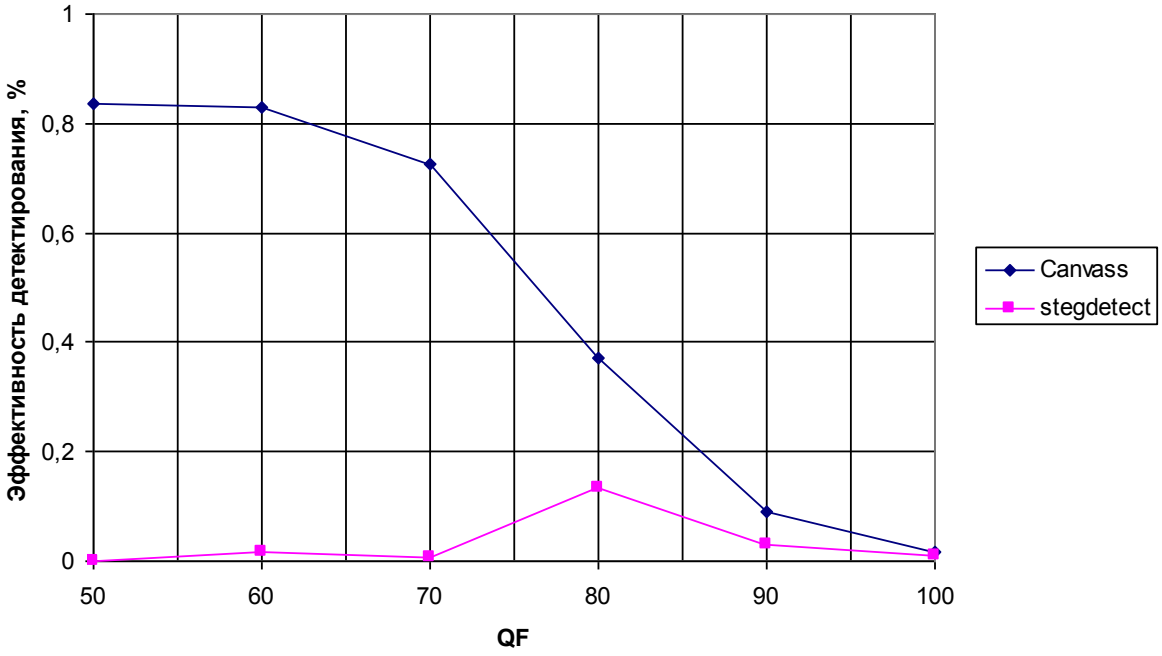

Рис. 1. Зависимость эффективности детектирования нового стеганографического алгоритма от показателя качества JPEG

Выводы

В настоящей статье рассмотрены три стеганоаналитических комплекса, однако недостатки этих программных продуктов могут быть отнесены к работе и других комплексов, ввиду того, что принципы функционирования остаются практически неизменными. Продемонстрирована устойчивость нового стеганографического алгоритма к стеганоаналитическим атакам современными программными комплексами. Полученные результаты свидетельствуют о том, что

1. Разработанный алгоритм не имеет аналогов в базах сигнатур стеганоаналитических комплексов, осуществляющих определение наличия вложения по маске используемого алгоритма;
2. Обучаемость стеганоаналитических комплексов (будь то линейный дискриминантный анализ, или же метод опорных векторов) требует для своей реализации наличия постоянно действующего стеганографического канала, что на практике не только часто не реализуемо, но и является малоэффективным с точки зрения поддержания скрытности и безопасности самого канала;
3. Для высококачественных JPEG изображений с QF выше 90 эффективность детектирования не превышает 10%.

Целью дальнейших исследований может стать исследование зависимости эффективности детектирования от объема вложенной дополнительной информации, что позволит дать ответ на вопрос о максимальной скрытой пропускной способности нового стеганографического алгоритма.

Литература

1. Рудницький, В.М. Стійке стеганоперетворення в просторовій області зображення-контейнера / В.М. Рудницький, О.В. Костирка // Інформатика та математичні методи в моделюванні. – 2013. – Т. 3, № 4. – С. 320-327.

2. Кобозева, А.А. Условия обеспечения устойчивости стеганоалгоритма при организации стеганопреобразования в пространственной области контейнера-изображения / А.А. Кобозева, О.В. Костырка // Інформаційна безпека. – 2013. – №4. – С. 57-65.

3. Бобок, И.И. Метод повышения эффективности детектирования вложения конфиденциальной информации: диссертация … канд. техн. наук – 05.13.21 «Системы защиты информации» / И.И. Бобок. – Одесса, 2013. – 136 с.

4. NRCS Photo Gallery: *[Электронный ресурс]* // United States Department of Agriculture. Washington, USA. Режим доступа: http://photogallery.nrcs.usda.gov (Дата обращения: 26.01.2014).

5. Рудницкий, В.Н. Стеганопреобразование пространственной области изображения-контейнера, устойчивое к сжатию / В.Н. Рудницкий, М.А. Мельник, О.В. Костырка // Сучасна спеціальна техніка. – 2014. – № 1. – С. 38-44.

6. Steganography Analyzer Signature Scanner (StegAlyzerSS): *[Электронный ресурс]* // SARC: Steganography Analysis and Research Center. Fairmont, USA. Режим доступа: http://www.sarc-wv.com/products/stegalyzerss/ (Дата обращения: 26.01.2014).

7. Steganography Detection with Stegdetect : *[Электронный ресурс]* // OutGuess.org by Niels Provos. Режим доступа: http://www.outguess.org/detection.php (Дата обращения: 26.01.2014).

8. Линейный дискриминантный анализ : *[Электронный ресурс]* // MachineLearning.ru - Профессиональный информационно-аналитический ресурс, посвященный машинному обучению, распознаванию образов и интеллектуальному анализу данных. Режим доступа: http://www.machinelearning.ru/wiki/index.php?title=Линейный_дискриминантный_анализ (Дата обращения: 26.01.2014).

9. Jalan, J. Feature selection, statistical modeling and its applications to universal JPEG steganalyzer : *[Электронный ресурс] //* Digital Repository @ Iowa State University. USA. Режим доступа: http://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=2039&context=etd (Дата обращения: 26.01.2014).

Надійшла 22.05.2014 р. Рецензент: д.т.н., проф. Толюпа С.В.