ВИСНОВКИ

Було розглянуто декілька схем цифрових мультипідписів, що вже існують. Ці схеми дозволяють будь-якому перевіряючому проводити групову перевірку чинності цифрових підписів. Вони дозволяють заощадити багато обчислень ступеня за модулем. Тим не менш, лише схеми BV-DSA та BV-RSA Hwang'a, а також схема Shao є надійними та забезпечують умову неможливості відмови від авторства. Однак ці схеми не мають ефективного методу виявлення підроблених підписів на відміну від схеми Changchien'a. Проблема створення безпечної та ефективної схеми цифрового мультипідпису залишається відкритою та може розглядатися як напрямок подальших досліджень.

СПИСОК ЛІТЕРАТУРИ

1. *Naccache, D.* Can DSA be improved: Complexity trade-os with the digital signature standard / D. Naccache, D. Mraihi, D. Rapheali, S. Vaudenay // Proceedings of Eurocrypt'94. – 1994. – Pp. 85–94.
2. *Lim, C. H.* Security of interactive DSA batch verication / C. H. Lim, P. J. Lee // Electronics Letters. – 1994. – Vol. 30, No. 19. – Pp. 1592–1593.
3. *Harn, L.* Batch verifying multiple DSA-type digital signatures // Electronics Letters. – 1998. – Vol. 34, No. 9. – Pp. 870–871.
4. *Harn, L.* Batch verifying multiple RSA digital signatures // Electronics Letters. – 1998. – Vol. 34, No. 12. – Pp. 1219–1220.
5. *Hwang, M. S.* Cryptanalysis of the batch verifying multiple RSA digital signatures / M. S. Hwang, I. C. Lin, K. F. Hwang // Informatica. – 2000. – Vol. 11, No. 1. – Pp. 15–19.
6. *Hwang, M. S.* Cryptanalysis of the batch verifying multiple DSA-type digital signatures / M. S. Hwang, C. C. Lee, Eric J. L. Lu // Pakistan Journal of Applied Sciences. – 2001. – Vol. 1, No. 3. – Pp. 287–288.
7. *Hwang, M. S.* Two simple batch verifying multiple digital signatures / M. S. Hwang, C. C. Lee, and Y. L. Tang // The Third International Conference on Information and Communication Security (ICICS2001). – Xian, China, 2001. – Pp. 13–16.
8. *Shao, Z.* Batch verifying multiple DSA-type digital signatures // Computer Networks. – 2001. – Vol. 37, No. 3–4. – Pp. 383–389.
9. *Changchien, S. W.* A batch verifying and detecting multiple RSA digital signatures / S. W. Changchien, M. S. Hwang // International Journal of Computational and Numerical Analysis and Applications. – 2002. – Vol. 2, No. 3. – Pp. 303–307.

Надійшла 29.10.2010

Неласая А. В., Дозоренко И. С.

ОБЗОР И СРАВНЕНИЕ СХЕМ ЦИФРОВЫХ МУЛЬТИПОДПИСЕЙ

Рассмотрены известные схемы цифровых мультиподписей с групповой проверкой, использующие только одну вместо нескольких проверок, а также недостатки этих схем. Проведено сравнение свойств схем по нескольким критериям.

Ключевые слова: цифровая подпись, мультиподпись, групповая проверка, RSA, DSA.

Nelasa A. V., Dozorenko I. S.

REVIEW AND COMPARISON OF MULTIPLE DIGITAL SIGNATURES

Several batch verication multiple digital signatures are reviewed in this paper. These schemes use only one verification instead of several verifications. Weakness of these schemes is also pointed out. The schemes were compared by the defined criterions.

Key words: multiple digital signatures, batch verification, RSA, DSA.

УДК 681.142.2; 622.02.658.284; 621.325

Пелешко Д. Д.[1], Кустра Н. О.[2], Шпак З. Я.[1]

[1]Канд. техн. наук, доцент Національного університету «Львівська політехніка»

[2]Канд. техн. наук, старший викладач Національного університету «Львівська політехніка»

СУМІЩЕННЯ ЗОБРАЖЕНЬ НАБОРУ НА ОСНОВІ ВИКОРИСТАННЯ ДИСПЕРСІЇ КОЛЬОРУ ЗОБРАЖЕНЬ

Розроблено швидкий метод суміщення зображень в наборі однотипних зображень на основі розв'язання задачі майже факторизації простору топології зображень з подальшим звуженням цього простору через вирішення задачі пошуку кореляційного максимуму. Задача майже факторизації формулюється через введення напівметрики стосовно дисперсії кольору елементів топології зображення.

Ключові слова: суміщення зображень, фреймове покриття, топологія зображень, дисперсія кольору, кореляційний максимум.

ВСТУП

Традиційно для реалізації процедури знаходження і суміщення зображень використовують кореляційну прив'язку цифрових зображень. Метод кореляційної прив'язки зображень має такі недоліки:

– взаємна кореляційна функція може мати досить розмитий максимум, що ускладнює його знаходження, оскільки не враховує просторову структуру порівнюваних зображень;

– комбінаторна складність – великий перебір ситуацій [1–4].

Основу запропонованого методу складають:

– запропоновані в [4] топологічні представлення та операції, зокрема звуження простору покриття зображення.

– характеристики виділених в [3] класів представлення зображень та наборів.

1. ПОСТАНОВКА ЗАДАЧІ

Метою даної роботи є розробка швидкого методу суміщення зображень в наборі на основі використання дисперсії значень кольору (чи інтенсивності).

Для досягнення цієї мети до розгляду потрібно ввести топологію зображення і визначити на ній задачу майже факторизації топологічного простору.

Основна ідея пропонованого методу суміщення полягає у швидкому формуванні для кожного зображення відповідних наборів «підозрілих» на подібність фреймів (задача звуження простору топологічного покриття зображення через вирішення задачі майже факторизації) з подальшим їх звуженням математичною кореляцією із заданим фрагментом (задача звуження простору топологічного покриття зображення через вирішення задачі пошуку кореляційного максимуму на топологічному покритті зображення).

2. ТОПОЛОГІЇ ДЛЯ ЗАДАЧІ СУМІЩЕННЯ ЗОБРАЖЕНЬ НАБОРУ

Нехай задано набір $\mathbf{P}$ однотипних рисунків з координатною $\Im_{\mathbf{P}} = \Im_{\mathbf{X}^{2,+,d}}$ та колірною топологіями $\mathfrak{O}_{\mathbf{P}}$ [5]. При цьому треба пам'ятати, що $\mathfrak{O}_{\mathbf{P}}$ індукується $\Im_{\mathbf{P}}$. В кожній з цих топологій визначимо скінченні покриття: фреймове $(\chi_{\mathbf{X}^{2,+,d}} | N_\chi) \subseteq \Im_{\mathbf{X}^{2,+,d}}$ та індуковане фрагментне $\vartheta_{\mathbf{P}}$ в $\mathfrak{O}_{\mathbf{P}}$ [6].

Серед зображень набору виберемо довільне зображення, стосовно якого буде здійснюватись операція суміщення. Таке зображення будемо називати *фіксованим*. Для зручності подальшого викладу нехай таке зображення має індекс в наборі, рівний 1. Тобто в наборі $\mathbf{P}$ фіксованим є зображення $P_{\text{фікс}} = P_1$. Тоді через $\mathbf{P}'$ позначимо набір з решти зображень

$$\mathbf{P}' = \mathbf{P} \backslash \{P_1\} = \{P_z\}_{z = 2 \ldots N}. \quad (1)$$

На $(\chi_{\mathbf{X}^{2,+,d}} | N_\chi)$ визначимо фрейм

$$\mathbf{X}^{2,+,d}_{\mathbf{fr}1,\text{ зад}} = \mathbf{X}^{2,+,d}_{\mathbf{fr}1,\text{ зад}}(\Delta_{x\,1,\text{зад}}, \Delta_{y\,1,\text{зад}}, l_{\mathbf{fr}1,\text{ зад}}, h_{\mathbf{fr}1,\text{ зад}}), \quad (2)$$

якому на P_1 відповідає індукований фрагмент зображення $P_{1,\text{ зад}} \in \vartheta_{\mathbf{P}}$.

Проблема вибору початкового фрейму $\mathbf{X}^{2,+,d}_{\mathbf{fr}1,\text{ зад}}$ в даній роботі детально не розглядатиметься. Це питання детально розглядалось в [7]. Приймаємо лише одне припущення – $\mathbf{X}^{2,+,d}_{\mathbf{fr}1,\text{ зад}}$ індукує такий фрагмент зображення P_1, який з достатньою точністю існує на усіх зображеннях набору $\mathbf{P}'$.

Вважатимемо, що фреймове покриття $(\chi_{\mathbf{X}^{2,+,d}} | N_\chi)$ гомеоморфне фрейму $\mathbf{X}^{2,+,d}_{\mathbf{fr}1,\text{ зад}}$ за розмірами. Тут гомеорфізм за розмірами визначає те, що усі елементи $(\chi_{\mathbf{X}^{2,+,d}} | N_\chi)$ мають розміри $l_{\mathbf{fr}1,\text{ зад}}$ і $h_{\mathbf{fr}1,\text{ зад}}$, а відрізняються лише координатами початку.

З $(\chi_{\mathbf{X}^{2,+,d}} | N_\chi)$ при заданій $\Im_{\mathbf{P}}$ сформуємо фреймове покриття набору $\mathbf{P}'$ за правилом

$$\chi_{\mathbf{P}'} = \{\chi_z\}_{z = 2 \ldots N},\ (\chi_z | N_\chi) \in \Im_{\mathbf{P}}, \quad (3)$$

де

$$\forall z, z \in [2 \ldots N]:\ \chi_{z_1} = \chi_{z_2};\ \chi_{z_1}, \chi_{z_1} \in \chi'_{\mathbf{P}}. \quad (4)$$

Формули (3) і (4) означають, що фреймове покриття $\chi_{\mathbf{P}'}$ набору $\mathbf{P}'$ складається з $N-1$ топологічно еквівалентних покриттів $(\mathbf{X}^{2,+,d}, \Im_{\mathbf{X}^{2,+,d}})$, елементи яких ще й рівні за розмірами. При цьому важливо відзначити, що розмірність кожного χ_z рівна N_χ. Тоді має місце

$$\dim \chi_{\mathbf{P}'} = (N-1)N_\chi, \quad (5)$$

і до розгляду треба приймати топологічний простір $(\chi_{\mathbf{P}'} | (N-1)N_\chi)$.

Фреймове покриття (3) засобом неперервного відображення $\mathbf{C}$ [6] індукує фрагментне покриття $\vartheta_{\mathbf{P}'} \subseteq \vartheta_{\mathbf{P}}$, яке належить топології $\mathfrak{O}_{\mathbf{P}'} \subseteq \mathfrak{O}_{\mathbf{P}}$ набору $\mathbf{P}'$, за правилом

$$\begin{gathered} \mathfrak{O}_{\mathbf{P}'} = \mathfrak{O}_{\mathbf{P}} \backslash \{\mathfrak{O}_1\} = \{\mathfrak{O}_z\}_{z = 2 \ldots N}; \\ \vartheta_{\mathbf{P}'} = \vartheta_{\mathbf{P}} \backslash \{\vartheta_1\} = \{\vartheta_z\}_{z = 2 \ldots N}; \\ \vartheta_{\mathbf{P}'} \subseteq \mathfrak{O}'_{\mathbf{P}} \subseteq \mathfrak{O}_{\mathbf{P}} \end{gathered} \quad (6)$$

Фактично $\chi_{\mathbf{P}'}$ і $\vartheta_{\mathbf{P}'}$ виступають звуженнями $\chi_{\mathbf{P}}$ і $\vartheta_{\mathbf{P}}$ відповідно.

Оскільки $\vartheta_{\mathbf{P}}$ є індуковане неперервним відображенням $\mathbf{C}$ [6], то визначений для $(\chi_{\mathbf{X}^{2,+,d}} | N_\chi)$ гомеорфізм (за розмірами) до фрейму $\mathbf{X}^{2,+,d}_{\mathbf{fr}1,\text{ зад}}$ має місце для елементів просторів $\vartheta_{\mathbf{P}}$ і $\vartheta_{\mathbf{P}'}$ до фрагмента $P_{1,\text{ зад}}$. При цьому для елементів $\vartheta_{\mathbf{P}}$ і $\vartheta_{\mathbf{P}'}$ не існує топологічної еквівалентності, подібної до (3). Це означає, що набір $\mathbf{P}'$ можна подати у вигляді скінченного набору фрагментів $P_{z,m}$ з розмірами $l_{\mathbf{fr}1,\text{ зад}}$ і $h_{\mathbf{fr}1,\text{ зад}}$

$$\begin{gathered} \mathbf{P}' = \{P_z\} = \\ = \left\{ \left\{ P_{z,m} | P_{z,m} = C_{z,m}(\mathbf{X}^{2,+,d}_{\mathbf{fr}z,m}) \right\}_{m = 1 \ldots N_\chi} \right\}_{z = 2 \ldots N}; \\ \forall z, m : \mathbf{X}^{2,+,d}_{\mathbf{fr}z,m} \in \chi_z. \end{gathered} \quad (7)$$

Зазначимо, що розмірність кожного ϑ_z складає N_χ, тобто існує простір $(\vartheta_z | N_\chi)$. Тоді розмірність $\vartheta_{\mathbf{P}'}$ за (5) складає

$$\dim \vartheta_{\mathbf{P}'} = (N-1)N_\chi, \tag{8}$$

і до розгляду треба приймати простір $(\vartheta_{\mathbf{P}'} | (N-1)N_\chi)$.

3. СУМІЩЕННЯ ЗОБРАЖЕНЬ НАБОРУ НА ОСНОВІ ВИКОРИСТАННЯ ДИСПЕРСІЇ

3.1. Майже факторизація просторів покриття зображень набору на основі дисперсії

Нехай задано набір **P**, фіксоване зображення $P_{\text{фікс}} = P_1$, фрейм $\mathbf{X}^{2,+,d}_{\mathbf{fr}1,\text{зад}}$ і фрагмент $P_{1,\text{зад}}$, набір $\mathbf{P}'$ (1), топологій $\Im_{\mathbf{P}} = \Im_{\mathbf{X}^{2,+,d}}$ та $\mathfrak{V}_{\mathbf{P}'} \subseteq \mathfrak{V}_{\mathbf{P}}$ [4] і покриття $(\chi_{\mathbf{P}'} | (N-1)N_\chi)$ (3) та $(\vartheta_{\mathbf{P}'} | (N-1)N_\chi)$ (6).

Для кожного фрагмента $P_{z,m}$ визначимо дисперсію $D_{z,m}$ [1] значення кольору (чи інтенсивності) $c^d_{z,m,(i,j)}$ кожного фрагмента. Розрахункова формула має вигляд

$$D_{z,m} = \frac{1}{s_{1,\text{зад}}} \sum_{i = x_{\text{поч}\,z,m}}^{x_{\text{поч}\,z,m} + l_{\mathbf{fr}1,\text{зад}}} \sum_{j = y_{\text{поч}\,z,m}}^{y_{\text{поч}\,z,m} + n_{\mathbf{fr}1,\text{зад}}} \left(c^d_{z,m,(i,j)} - M_{z,m} \right)^2;$$
$$m = 1 \ldots N_\chi;$$
$$z = 2 \ldots N, \tag{9}$$

де $s_{1,\text{зад}} = l_{\mathbf{fr}1,\text{зад}} h_{\mathbf{fr}1,\text{зад}}$ – площа $P_{1,\text{зад}}$: $M_{z,m}$ – математичне сподівання.

Подібно до (9) обчислюється дисперсія $D_{1,\text{зад}}$ для фрагмента $P_{1,\text{зад}}$.

В результаті (9) кожному фрагменту $P_{z,m}$ однозначно поставлена у відповідність характеристика – середнє значення кольорів $D_{z,m}$ відповідного фрагмента зображення P_z

$$P_{z,m} \to D_{z,m}. \tag{10}$$

Це означає, що $(\chi_{\mathbf{P}'} | (N-1)N_\chi)$ засобами (10) через $(\vartheta_{\mathbf{P}'} | (N-1)N_\chi)$ індукує набір характеристик – дисперсій кольору

$$\chi_{\mathbf{P}'} \underset{\mathbf{C}}{\to} \vartheta_{\mathbf{P}'} \underset{M}{\to} \{D_{z,m}\},$$
$$z = 2 \ldots N. \tag{11}$$

Для задачі майже факторизації $(\chi_{\mathbf{P}'} | (N-1)N_\chi)$ введемо напівметрику $d_{D,\mathbf{fr}}(P_{z,m}, P_{1,\text{зад}})$ як відношення еквівалентності фрагменту $P_{1,\text{зад}}$

$$\forall P_{z,m} \in \vartheta_{\mathbf{P}'} : d_{D,\mathbf{fr}}(P_{z,m}, P_{1,\text{зад}}) = \left| D_{z,m} - D_{1,\text{зад}} \right|, \tag{12}$$

Твердження. (12) є напівметрикою.

Доведення.

◁

Оскільки (12) є евклідовою відстанню, то звідси випливають умови метрики.

Відношення еквівалентності як умова напівметрики випливає з того, що для дисперсії (9) як інтегральної характеристики фрагмента можлива ситуація, коли

$$\exists z \in [2 \ldots N],\ m \in [2 \ldots N_\chi] : D_{z,m} = D_{1,\text{зад}}. \tag{13}$$

Це означає, що для $P_{z,m} \neq P_{1,\text{зад}}$ має місце

$$d_{D,\mathbf{fr}}(P_{z,m}, P_{1,\text{зад}}) = 0, \tag{14}$$

що визначає метрику (12) як напівметрику.

▷

Тоді задача майже факторизації простору $(\vartheta_{\mathbf{P}'} | (N-1)N_\chi)$ полягає у побудові $\vartheta_{\left(\vartheta_{\mathbf{P}'} | (N-1)N_\chi\right), d_{D,\mathbf{fr}}} / {}^{\sim\varepsilon}$ за допомогою нерівності

$$\forall P_{z,m} \in \vartheta_{\left(\vartheta_{\mathbf{P}'} | (N-1)N_\chi\right), d_{D,\mathbf{fr}}} / {}^{\sim\varepsilon},$$
$$d_{D,\mathbf{fr}}(P_{z,m}, P_{1,\text{зад}}) \le \varepsilon, \tag{15}$$

де ε – точність суміщення – параметр майже факторизації.

В загальному випадку треба розглядати $\varepsilon = \varepsilon(z)$. Проте на практиці для зручності вибирають точність одну для усіх $N-2$ рисунків набору $\mathbf{P}'$.

Фактично $\vartheta_{\left(\vartheta_{\mathbf{P}'} | (N-1)N_\chi\right), d_{D,\mathbf{fr}}} / {}^{\sim\varepsilon}$ треба розглядати як набір фрагментів набору $\mathbf{P}'$ «підозрілих» на подібність (за 15) фрагменту $P_{1,\text{зад}}$. Оскільки

$$\forall \vartheta_z \in \vartheta_{\left(\vartheta_{\mathbf{P}'} | (N-1)N_\chi\right), d_{D,\mathbf{fr}}} / {}^{\sim\varepsilon} : \dim \vartheta_z \le N_\chi, \tag{16}$$

то має місце оцінка

$$\dim \vartheta_{\left(\vartheta_{\mathbf{P}'} | (N-1)N_\chi\right), d_{D,\mathbf{fr}}} / {}^{\sim\varepsilon} \le$$
$$\le \dim \vartheta_{\mathbf{P}'} = (N-1)N_\chi. \tag{17}$$

Якщо прийняти, що $\vartheta_{\left(\vartheta_{\mathbf{P}'} | (N-1)N_\chi\right), d_{D,\mathbf{fr}}} / {}^{\sim\varepsilon}$ відповідає майже фактор $\chi_{\left(\chi_{\mathbf{P}'} | (N-1)N_\chi\right), d_{D,\mathbf{fr}}} / {}^{\sim\varepsilon}$, такий що

$$\left(\chi_{\left(\chi_{\mathbf{P}'} | (N-1)N_\chi\right), d_{D,\mathbf{fr}}} / {}^{\sim\varepsilon} \middle| \vartheta_{\left(\vartheta_{\mathbf{P}'} | (N-1)N_\chi\right), d_{D,\mathbf{fr}}} / {}^{\sim\varepsilon} \right) \subseteq$$
$$\subseteq (\chi_{\mathbf{P}'} | (N-1)N_\chi), \tag{18}$$

то (17) означає, що через вирішення задачі майже факторизації вдалось звузити простори $(\vartheta_{\mathbf{P}'}|(N-1)N_\chi)$ і $(\chi_{\mathbf{P}'}|(N-1)N_\chi)$ відповідно.

3.2. Задача пошуку кореляційного максимуму на майже фактор просторі зображення

Наступним кроком є звуження просторів $\vartheta_{\left(\vartheta_{\mathbf{P}'}|(N-1)N_\chi\right),\, d_{D,\,\mathbf{fr}}}^{/\sim\varepsilon}$ і $\chi_{\left(\chi_{\mathbf{P}'}|(N-1)N_\chi\right),\, d_{D,\,\mathbf{fr}}}^{/\sim\varepsilon}$ до одного фрейму через вирішення задачі пошуку кореляційного максимуму. Для цього введемо до розгляду метрику

$$\forall P_{z,\,m} \in \vartheta_{\mathbf{P}'} : d_{r_{\max},\,\mathbf{fr}}(P_{z,\,m}, P_{1,\,\text{зад}}) = \\ = r(P_{z,\,m}, P_{1,\,\text{зад}}), \qquad (19)$$

де $r(P_{z,\,m}, P_{1,\,\text{зад}})$ – кореляції [1] між значеннями кольору (чи інтенсивності) фрагменту $P_{z,\,m}$ із заданим $P_{1,\,\text{зад}}$. Розрахункова формула має вигляд

$$r_{z,\,m}(P_{1,\,\text{зад}}, P_{z,\,m}) = \frac{\sum_{i\,=\,x_{\text{поч}\,z,\,m}}^{x_{\text{поч}\,z,\,m}+l_{\mathbf{fr}1,\,\text{зад}}} \sum_{j\,=\,y_{\text{поч}\,z,\,m}}^{y_{\text{поч}\,z,\,m}+h_{\mathbf{fr}1,\,\text{зад}}} (c^d_{1,\,\text{зад},\,(i,\,j)} - M_{1,\,\text{зад}})(c^d_{z,\,m,\,(i,\,j)} - M_{z,\,m})}{\sum_{i\,=\,x_{\text{поч}\,z,\,m}}^{x_{\text{поч}\,z,\,m}+l_{\mathbf{fr}1,\,\text{зад}}} \sum_{j\,=\,y_{\text{поч}\,z,\,m}}^{y_{\text{поч}\,z,\,m}+h_{\mathbf{fr}1,\,\text{зад}}} (c^d_{1,\,\text{зад},\,(i,\,j)} - M_{1,\,\text{зад}})^2 \sum_{i\,=\,x_{\text{поч}\,z,\,m}}^{2x_{\text{поч}\,z,\,m}+l_{\mathbf{fr}1,\,\text{зад}}} \sum_{j\,=\,y_{\text{поч}\,z,\,m}}^{y_{\text{поч}\,z,\,m}+h_{\mathbf{fr}1,\,\text{зад}}} (c^d_{z,\,m,\,(i,\,j)} - M_{z,\,m})^2}; \\ m = 1 \ldots N_{\chi_z};\ z = 2 \ldots N, \qquad (20)$$

де $c^d_{1,\,\text{зад},\,(i,\,j)}$ – значення кольору фрагмента $P_{1,\,\text{зад}}$; N_{χ_z} – розмірність покриттів $\chi_z \in \chi_{\left(\chi_{\mathbf{P}'}|(N-1)N_\chi\right),\, d_{D,\,\mathbf{fr}}}^{/\sim\varepsilon}$ та $\vartheta_z \in \vartheta_{\left(\vartheta_{\mathbf{P}'}|(N-1)N_\chi\right),\, d_{D,\,\mathbf{fr}}}^{/\sim\varepsilon}$.

В результаті (20) для кожного $\chi_{\left(\chi_{\mathbf{P}'}|(N-1)N_\chi\right),\, d_{D,\,\mathbf{fr}}}^{/\sim\varepsilon}$ та $\vartheta_{\left(\vartheta_{\mathbf{P}'}|(N-1)N_\chi\right),\, d_{D,\,\mathbf{fr}}}^{/\sim\varepsilon}$ отримуємо набір значень кореляцій $r_{z,\,m}(P_{1,\,\text{зад}}, P_{z,\,m})$, які є характеристиками фрагментів $P_{z,\,m} \in \vartheta_z$

$$\begin{pmatrix} \chi_z \\ \vartheta_z \end{pmatrix} \to \{r_{z,\,m}(P_{1,\,\text{зад}}, P_{z,\,m})\}_{m\,=\,1 \ldots N_{\chi_z}},\ z = 2 \ldots N; \\ \chi_z \in \chi_{\left(\chi_{\mathbf{P}'}|(N-1)N_\chi\right),\, d_{D,\,\mathbf{fr}}}^{/\sim\varepsilon}; \\ \vartheta_z \in \vartheta_{\left(\vartheta_{\mathbf{P}'}|(N-1)N_\chi\right),\, d_{D,\,\mathbf{fr}}}^{/\sim\varepsilon}. \qquad (21)$$

На наборі $\{r_{z,\,m}(P_{1,\,\text{зад}}, P_{z,\,m})\}$ для кожного z вирішуємо задачу пошуку кореляційного максимуму із заданим $P_{1,\,\text{зад}}$

$$I_{r,\,\max} = \left\{ \max_m (r_{z,\,m}(P_{1,\,\text{зад}}, P_{z,\,m})) \neq 0 \right\}_{z\,=\,2 \ldots N}. \qquad (22)$$

У випадку, якщо ненульового кореляційного максимуму при заданому z не існує, то це зображення видаляється з набору і в подальшому розв'язанні задачі суміщення не розглядається. Надалі вважатимемо, що для будь-якого z ненульова кореляція існує.

За (21) знаходимо відповідний $P_{z,\,m} \in \vartheta_z \in \vartheta_{\left(\vartheta_{\mathbf{P}'}|(N-1)N_\chi\right),\, d_{D,\,\mathbf{fr}}}^{/\sim\varepsilon}$ і формуємо остаточний набір фрагментів

$$\vartheta_{\mathbf{P}'\max r} = \left\{ P_{z,\,m} \middle| (P_{z,\,m} \to \mathbf{I}_{r,\,\max}) \right\}_{z\,=\,2 \ldots N} \qquad (23)$$

і відповідний набір фреймів

$$\chi_{\mathbf{P}'\max r} = \left\{ \mathbf{X}^{2,+,d}_{\mathbf{fr}z,\,m} \middle| P_{z,\,m} = C(\mathbf{X}^{2,+,d}_{\mathbf{fr}z,\,m}),\, P_{z,\,m} \in \vartheta_{\mathbf{P}'\max r} \right\}_{z\,=\,2 \ldots N}. \qquad (24)$$

Оскільки розмірність набору (22) дорівнює $N-2$, то

$$\dim\chi_{\mathbf{P}'\max r} = \dim\vartheta_{\mathbf{P}'\max r} = N-2. \qquad (25)$$

Очевидно, що $\vartheta_{\mathbf{P}'\max r} \subset \vartheta_{\left(\vartheta_{\mathbf{P}'}|(N-1)N_\chi\right),\, d_{D,\,\mathbf{fr}}}^{/\sim\varepsilon} \subseteq \subseteq \vartheta_{\mathbf{P}'} \subseteq \vartheta_{\mathbf{P}}$ належить топологіям $\mathfrak{V}_{\mathbf{P}'}$ та $\mathfrak{V}_{\mathbf{P}}$. Аналогічно для координатної області маємо $\chi_{\mathbf{P}'\max r} \subset \subset \chi_{\left(\chi_{\mathbf{P}'}|(N-1)N_\chi\right),\, d_{D,\,\mathbf{fr}}}^{/\sim\varepsilon} \subseteq \chi_{\mathbf{P}'} \subseteq \chi_{\mathbf{P}}$.

Фрагментний набір $(\vartheta_{\mathbf{P}'\max r}|N-2)$ є результатом двоетапного звуження $\vartheta_{\mathbf{P}'}$ до $N-2$ фрагментів, кожен з який відповідає окремому P_z набору $\mathbf{P}'$.

Подібно до $(\vartheta_{\mathbf{P}'\max r}|N-2)$, фреймовий набір $(\chi_{\mathbf{P}'\max r}|N-2)$ є результатом звуження $\chi_{\mathbf{P}'}$ і містить для кожного z по одному фрейму $\mathbf{X}^{2,+,d}_{\mathbf{fr}z,\,m}$.

За фреймовим набором $(\chi_{\mathbf{P}'\max r}|N-2)$, як зміщення між фрагментами $P_{z,\,m}$ і $P_{1,\,\text{зад}}$, знаходимо зміщення по осях $x - \Delta_{x,\,(1,\,z)}$ та по $y - \Delta_{y,\,(1,\,z)}$ кожного зображення набору $\mathbf{P}'$ відносно P_1,

$$\left\{\begin{matrix}\Delta_{x,\,(1,\,z)} = \Delta_{x,\,z,\,m} - \Delta_{x,\,1,\,\text{зад}} \\ \Delta_{y,\,(1,\,z)} = \Delta_{y,\,z,\,m} - \Delta_{y,\,1,\,\text{зад}}\end{matrix}\right\}_{z\,=\,2\ldots N};$$

$$\mathbf{X}^{2,\,+,\,d}_{\mathbf{fr}z,\,m} \in \chi_{\mathbf{P}'\max r}. \qquad (26)$$

Звертаємо увагу на те, що зміщення $\Delta_{x,\,(1,\,z)}, \Delta_{y,\,(1,\,z)} \in \mathbf{N}$, тобто можуть набувати як додатних, так і від'ємних значень.

4. РЕЗУЛЬТАТИ ПРАКТИЧНИХ ЕКСПЕРИМЕНТІВ СУМІЩЕННЯ ЗОБРАЖЕНЬ НА ОСНОВІ ДИСПЕРСІЇ

На основі викладених вище теоретичних результатів розроблено практичну реалізацію методу суміщення зображень набору на основі дисперсії. Зображення цих наборів є результатами горизонтальних та вертикальних зсувів деякого базового зображення. Надалі такі набори будемо називати наборами штучно-згенерованих зображень (НШЗЗ).

В практичному експерименті для зручності умову (15) замінимо на відносну похибку

$$\frac{d_{D,\,\mathbf{fr}}(P_{z,\,m},\,P_{0,\,\text{зад}})}{\left|D_{z,\,m}\right|} \le \varepsilon. \qquad (27)$$

На рис. 1 наведено результати суміщення зображень НШЗЗ. Характеристики НШЗЗ є такими: розмірність набору – $N = 88$; зображення в градаціях сірого; розмірність кожного зображення – $l = 34 \times h = 54$ пікселів; $P_{\text{фікс}} = P_0$. Параметри заданого фрейму $\mathbf{X}^{2,\,+,\,d}_{\mathbf{fr}z,\,m}$: $\Delta_{x,\,0,\,\text{зад}} = \Delta_{y,\,0,\,\text{зад}} = 10$; $l_{\mathbf{fr}0,\,\text{зад}} = h_{\mathbf{fr}0,\,\text{зад}} = 10$; $\varepsilon = 0{,}001$. Індексування зображень в наборі розпочинається з нуля, тобто $\mathbf{P}' = \{P_1, \ldots, P_{88}\}$. Заданий фрагмент на P_0 виділений червоним кольором.

На рис. 2 наведено результати побудови майже фактор простору $\vartheta^{\,/\,\sim\varepsilon}_{\left(\vartheta_{\mathbf{P}'}\left|(N-1)N_\chi\right.\right),\,d_{D,\,\mathbf{fr}}}$, тобто набори «підозрілих на подібність» фрагментів для кожного зображення набору $\mathbf{P}'$, НШЗЗ, результати суміщення якого наведені на рис. 1. Швидкість формування $\vartheta^{\,/\,\sim\varepsilon}_{\left(\vartheta_{\mathbf{P}'}\left|(N-1)N_\chi\right.\right),\,d_{D,\,\mathbf{fr}}}$ є визначальною для пропонованого алгоритму в порівнянні з відомими методами [7]. Чисельні значення кількості «підозрілих фреймів» для кожного P_z набору $\mathbf{P}'$ можна побачити на рис. 1 в таблиці «Зміщення» → в колонці «значення» → в мітці «підозр. –».

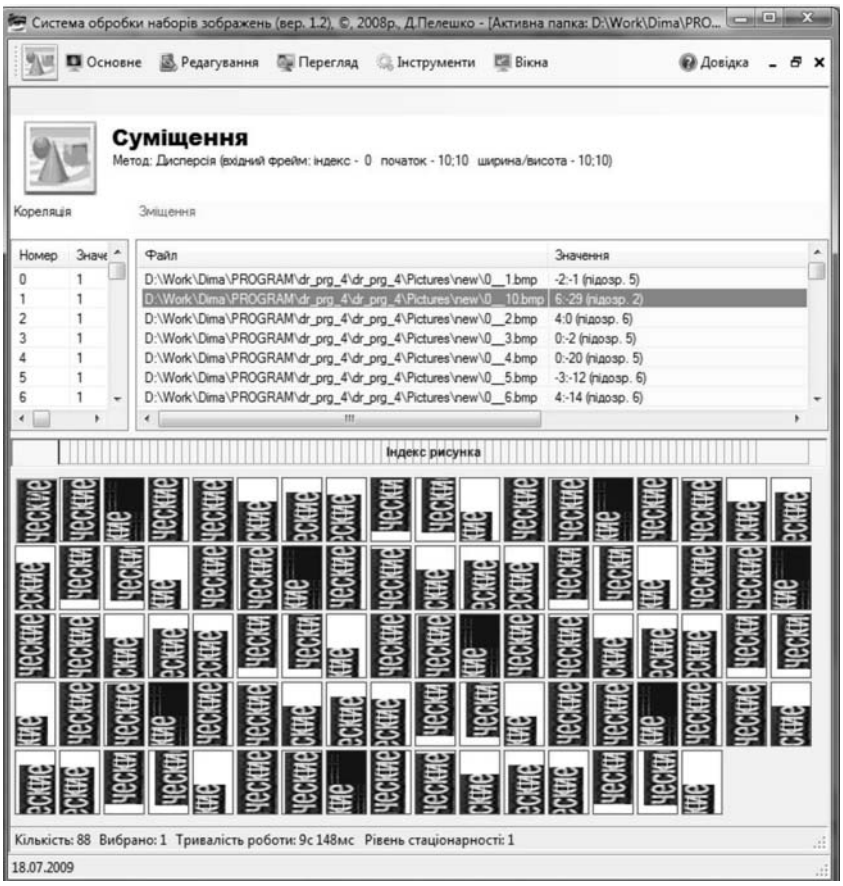

Рис. 1. Зріз екранної форми – результати суміщення на основі дисперсії НШЗЗ

Рис. 2. Зріз екрану – результати формування майже фактор простору $\vartheta_{\left(\vartheta_{\mathbf{P}'}|(N-1)N_{\chi}\right),\, d_{D,\,\mathbf{fr}}}{}^{/\sim\varepsilon}$ при суміщенні методом дисперсії кольору НШЗЗ $\mathbf{P}'$

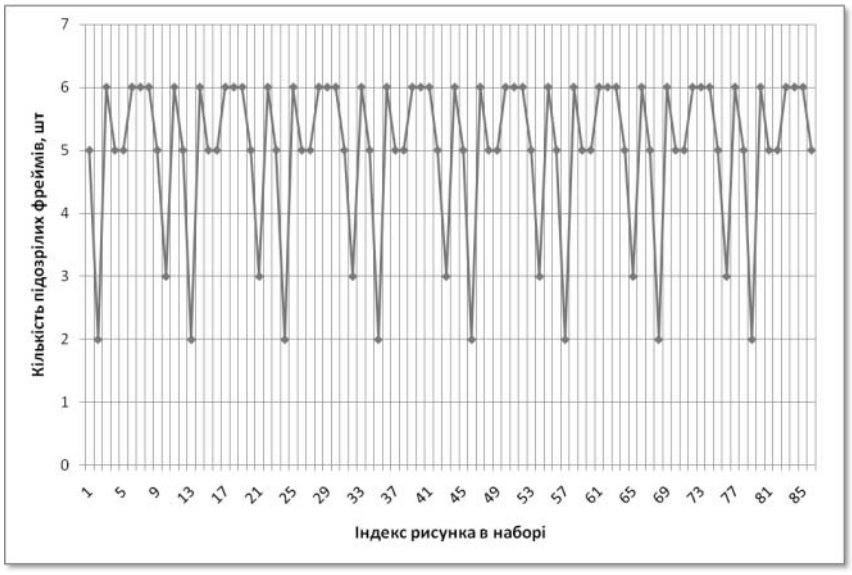

Рис. 3. Розподіл «підозрілих» фрагментів (простору $\vartheta_{\left(\vartheta_{\mathbf{P}'}|(N-1)N_{\chi}\right),\, d_{D,\,\mathbf{fr}}}{}^{/\sim\varepsilon}$) в невпорядкованому НШЗЗ $\mathbf{P}'$ за методом суміщення на основі дисперсії

На рис. 3 наводиться розподіл розмірностей χ_z та ϑ_z, які належать покриттям $\chi_{\left(\chi_{\mathbf{P}'}|(N-1)N_{\chi}\right),\, d_{D,\,\mathbf{fr}}}{}^{/\sim\varepsilon}$ та $\vartheta_{\left(\vartheta_{\mathbf{P}'}|(N-1)N_{\chi}\right),\, d_{D,\,\mathbf{fr}}}{}^{/\sim\varepsilon}$ відповідно. Періодичність розподілу визначається невпорядкованістю набору $\mathbf{P}'$ і штучним генеруванням зображень.

Чисельні значення, тобто $\Delta_{x,\,(1,\,z)}, \Delta_{y,\,(1,\,z)}$, для суміщення на основі дисперсії наведені на рис. 1 в таблиці «Зміщення» → в колонці «значення».

На рис. 4 наведено часові результати (тобто, фактично швидкість) роботи алгоритму суміщення НШЗЗ запропонованим методом залежно від розмірності $\mathbf{P}'$. Характеристики НШЗЗ є такими: розмірність набору – змінна; зображення в градаціях сірого; розмірність кожного зображення – $l = 34 \times h =$ = 54 пікселів; $P_{\text{фікс}} = P_0$. Параметри заданого фрейму $\mathbf{X}^{2,\,+,\,d}_{\mathbf{fr}0,\,\text{зад}}$: $\Delta_{x,\,0,\,\text{зад}} = \Delta_{y,\,0,\,\text{зад}} = 10$; $l_{\mathbf{fr}0,\,\text{зад}} = h_{\mathbf{fr}0,\,\text{зад}} =$ = 10; ε = 0,01.

При суміщенні методом дисперсії результати наведено в табл. 1. При цьому середньоквадратичне відхилення результатів експерименту не перевищувало 20 мс. На основі результатів вибраних експериментів характеристикою швидкості роботи алгоритму виступало середнє значення значень часу усіх експериментів при кожній розмірності набору. Ці значення наведені на графіку рис. 4.

З рис. 4 видно, що час роботи алгоритму зростає із збільшенням розмірності набору. Таке зростання пояснюється різким збільшенням арифметичних операцій.

Таблиця 1. Зведена таблиця експериментальних та характеристичних даних – результатів роботи (в мс) процесу суміщення методом дисперсії при різних розмірностях НШЗЗ

Розмірність набору	Час роботи алгоритму, мс Номер експерименту					Відхилення, мс	Середнє значення, мс
	1	2	3	4	5		
11	1104	1089	1102	1096	1098	5,85	1097,80
22	2272	2248	2263	2247	2238	13,65	2253,60
32	3283	3301	3258	3293	3294	16,81	3285,80
44	4607	4624	4593	4613	4610	11,19	4609,40
88	9148	9145	9112	9107	9112	19,94	9124,80

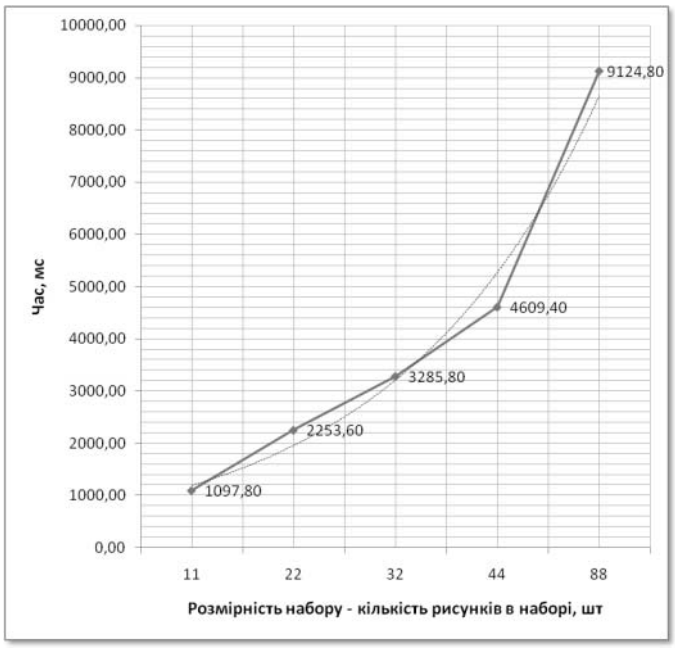

Рис. 4. Часова залежність від розмірності набору $\mathbf{P}'$ роботи алгоритму суміщення НШЗЗ методом дисперсії

Таблиця 2. Порівняльні дані результатів роботи (в мс) процесу суміщення НШЗЗ методом дисперсії при різних розмірах заданого фрейма

Розмір рисунка (пікселі)			
X		Y	
37		54	
Розмір фрейма (пікселі) X	Y	Площа фрейма / площа рисунка	Час
10	10	0,05	1097,80
15	15	0,11	1491,20
20	20	0,20	1772,40
25	25	0,31	1558,20
28	28	0,39	1222,20

В табл. 2 наведено дані залежності швидкості роботи процесу суміщення НШЗЗ від розмірів фрейма $\mathbf{X}_{\mathbf{fr}0,\,\text{зад}}^{2,\,+,\,d}$. Характеристики НШЗЗ є такими, як у випадку з результатами, поданими в табл. 2.

Експерименти проводились подібно до експериментів, результати яких відображені на рис. 4 і в табл. 1. Тобто характеристикою виступало середнє значення результатів п'яти кращих експериментів при різних $s_{0,\,\text{зад}}/s_{P_0}$. При цьому похибка відхилення також не перевищувала 20 мс. Як показали результати експериментів, найгіршим (найдовше працював алгоритм) для даного $\mathbf{P}'$ є співвідношення $s_{0,\,\text{зад}}/s_{P_0} = 0,2$, що відповідає розмірам $l_{\mathbf{fr}0,\,\text{зад}} = h_{\mathbf{fr}0,\,\text{зад}} = 20$.

При більших та менших розмірах заданого фрейма (в даному випадку квадратного) швидкість роботи алгоритму лише зростає.

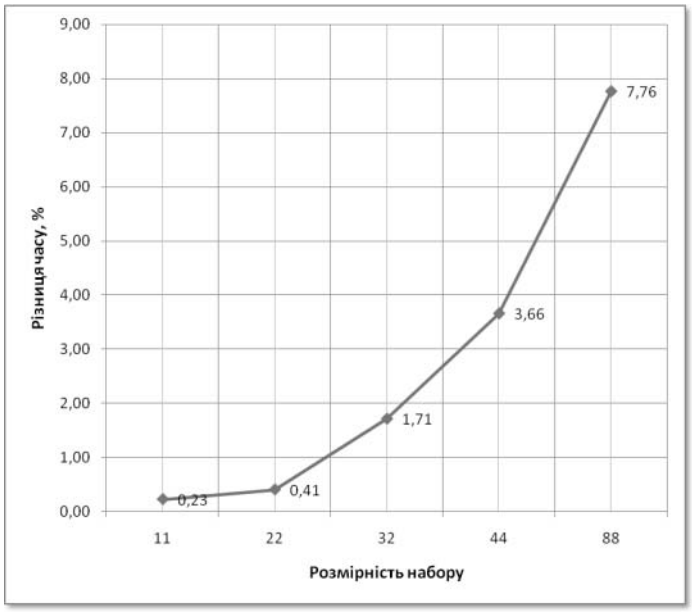

Рис. 5. Порівняння часу роботи алгоритму суміщення НШЗЗ на основі методів кореляційної прив'язки і дисперсії

Наведені результати ілюструють лише характер залежності швидкості роботи алгоритму від розмірів $\mathbf{X}_{\mathbf{fr}0,\,\text{зад}}^{2,+,d}$ (тренд поліномний). Очевидно, що тип і якісний вміст зображення та вибраного фрагмента також будуть впливати на час роботи алгоритму.

Важливим результатом експериментів є існування максимуму – найбільшого часу роботи алгоритму. Відповідно до цього можна зробити висновок, що пришвидшення роботи алгоритму є можливим через вибір за розмірами $\mathbf{X}_{\mathbf{fr}0,\,\text{зад}}^{2,+,d}$. Пошук найменшого значення є достатньо складним, оскільки до розгляду треба приймати двомірний розподіл часу роботи.

На рис. 5 показано порівняння часу роботи різних алгоритмів (у форматі приросту у відсотках пришвидшення роботи запропонованого методу в порівнянні з методом кореляційної прив'язки для суміщення НШЗЗ) суміщення, побудованих на методах кореляційної прив'язки та дисперсії.

ВИСНОВКИ

Як можна побачити з результатів, наведених на рис. 5, метод суміщення, базований на майже факторизації простору $\vartheta_{\mathbf{P}'}$ на основі дисперсії, є суттєво швидшим від методу суміщення на основі кореляційної прив'язки. Зважаючи на дуже малі розміри зображень НШЗЗ, приріст швидкості роботи, наприклад при N = 88 становить 7,76 % і зростає при зростанні розмірності $\mathbf{P}'$.

Запропонований алгоритм може бути застосований для суміщення в горизонтальному та вертикальному напрямках зображень будь-якого типу.

СПИСОК ЛІТЕРАТУРИ

1. *Гусейн-Заде, С. М.* Лекции по дифференциальной геометрии / Гусейн-Заде С. М. – М. : Изд-во МГУ, 2001.– 464 с.
2. *Милнор, Дж.* Дифференциальная топология / Дж. Милнор, А. М. Уоллес. – М. : Мир, 1972. – 279 с.
3. Класифікація моделей представлення зображень та наборів зображень як стохастичних зображень та полів: Матеріали науково-практичної конференції [«Інтелектуальні системи прийняття рішень та проблеми обчислювального інтелекту ISDMCI'2009»], (Євпаторія, 18–22 травня 2009) / Херсонський морський інститут. – Херсон : Видавництво Херсонського морського інституту, 2009. – Т. 2. – С. 401–405.
4. *Пелешко, Д. Д.* Топології зображень та наборів зображень / Д. Пелешко // Науковий вісник НЛТУ України : збірник науково-технічних праць. – 2009. – Вип. 19.4. – С. 236–242.
5. *Александров, П. С.* Введение в теорию множеств и общую топологию / Александров П. С. – М. : Наука, 1977. – 368 с.
6. *Халмош, П.* Конечномерные векторные пространства / Халмош П. – М. : ГИФМЛ, 1963. – 276 с.
7. *Рашкевич, Ю.* Центрування зображень на основі методів кореляційного аналізу / Ю. Рашкевич, Б. Демида, Д. Пелешко, Н. Кустра // Збірник наукових праць Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова. – 2005. – Вип. 29. – С. 121–128.

Надійшла 7.10.2009
Після доробки 30.03.2010

Пелешко Д. Д., Шпак З. Я., Кустра Н. Я.

СОВМЕЩЕНИЕ ИЗОБРАЖЕНИЙ НАБОРА НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ДИСПЕРСИИ ЦВЕТА ИЗОБРАЖЕНИЙ

Разработан ускоренный метод центрирования набора однотипных изображений на основе решения задачи почти

факторизации пространства топологиии изображения с последующим сужением этого пространства с помощью задачи поиска корреляционного максимума. Задача почти факторизации формулируется введением полуметрики относительно дисперсии цвета элементов топологии изображения.

Ключевые слова: совмещение изображений, фреймовое покрытие, топология изображений, дисперсия цвета, корреляционный максимум.

Peleshko D. D., Kustra N. O., Shpak Z. Ya.

COMPOSITION IMAGE REGISTRATION USING PICTURE COLOR DISPERSION

The authors have developed the method of one-type images centering based on solution of the problem of image topology space almost-factorization with further constriction of the space by solving the problem of correlation maximum search. The almost-factorization problem is solved by introduction of semimetrisc relative to image topology elements color dispersion.

Key words: image registration, frame coverage, image topology, color dispersion, correlation maximum.

УДК 629.735

Потий А. В.[1], Комин Д. С.[2]

[1]Д-р техн. наук, доцент, начальник кафедры Харьковского университета Воздушных Сил

[2]Адъюнкт Харьковского университета Воздушных Сил

ОНТОЛОГИЧЕСКОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССА ОЦЕНИВАНИЯ ГАРАНТИЙ В КОНТЕКСТЕ ФУНКЦИОНАЛЬНО-ЛИНГВИСТИЧЕСКОГО ПОДХОДА

Предлагается функционально-лингвистический подход к оцениванию гарантий безопасности. Приводятся методика и результаты онтологического анализа предметной области оценивания гарантий. Обосновывается актуальность применения аппарата онтологического моделирования для задач оценивания безопасности.

Ключевые слова: гарантии, оценивание, онтологическое моделирование, функциональное моделирование, лингвистические переменные.

ВСТУПЛЕНИЕ

Владельцы систем и продуктов информационных технологий (ИТ) хотят быть уверенными в качестве разработки, эффективности функционирования и безопасности приобретенных ИТ-продуктов. Международные [1–4] и национальные [5–7] стандарты в области безопасности информационных технологий определяют функциональные требования безопасности и требования гарантий безопасности, удовлетворение которых позволяет предоставить различные основания для такой уверенности. В ходе активного исследования (оценивания) ИТ-продукта на соответствие требованиям гарантий и формируется уверенность потребителя в корректности реализации функциональных услуг безопасности.

Оценивание ИТ-продуктов проводится аккредитованными испытательными лабораториями на основании программ и методик проведения оценивания. Качественная разработка программы и методики оценивания является важной составляющей при подготовке к проведению оценивания. Сам процесс оценивания подвержен воздействию различных факторов, способных повлиять на итоговый результат оценивания. Поэтому к процессу оценивания выдвигаются требования ширины, глубины и строгости, а к результатам оценивания – требования объективности, повторяемости, беспристрастности, воспроизводимости и сопоставимости.

Обзор научной литературы показал, что моделирование процессов оценивания гарантий безопасности с созданием инструментальных средств для поддержки работы эксперта является актуальной задачей. Однако в основном моделирование направлено на интерактивное представление требований стандарта в виде информационных инструментальных систем. Кроме того, в большинстве работ при моделировании не рассматриваются вышеперечисленные требования.

В работах авторов [8–10] предлагается функционально-лингвистический подход к оцениванию гарантий информационной безопасности, который позволяет разрабатывать программу и методику оценивания и выполнять вышеуказанные требования как к процессу оценивания, так и к результатам оценивания. В данной работе представлены результаты дальнейшего развития функционально-лингвистического подхода и детальное описание первого этапа.