

більше підходить для передачі мультимедійного трафіку, наприклад, такого як відео MPEG-4.

1. Тимченко О.В., Кирик М.І., Верхола Б.М., Самі Аскар. Аналіз методів забезпечення якості передачі мультимедійного трафіку // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Вип.50. – К.: 2009. – С. 200-206.
2. R. Braden *et al.*, "Resource Reservation Protocol (RSVP) - Version 1 Functional Specification," RFC 2205, Sept. 1997.
3. L. Andersson *et al.*, "LDP Specification," RFC 3036, Jan. 2001.
4. E. Rosen *et al.*, "Multiprotocol Label Switching Architecture," RFC 3031, Jan. 2001.
5. B. Jamoussi *et al.*, "Constraint-Based LSP Setup Using LDP," RFC 3212, Jan. 2002.
6. A. Ghanwani *et al.*, "Traffic Engineering Standards in IP Networks Using MPLS," IEEE Commun. Mag., vol. 37, no. 12, Dec. 1999, pp. 49-53.
7. M. G. Hluchyj and M. J. Karol, "Queuing in High-Performance Packet Switching," IEEE JSAC, vol. 6, no. 9, Dec 1988, pp. 1587-97.
8. E. Rosen *et al.*, "MPLS Label Stack Encoding," RFC 3032, Jan. 2001.

Поступила 18.01.2010р.

УДК 004.056

Б. В. Дурняк, В.З. Пашкевич

МЕТОДИ ФОРМУВАННЯ ГРАФІЧНИХ ЗАСОБІВ ЗАХИСТУ ДОКУМЕНТІВ

We worked out the formal description of graphic protection means on the basis of graphic introduction and rulers of construction and modification of graphic images in a rectangular coordinate system.

За багатомісячну історію людства документи на паперових носіях стали вагомим інструментом існування державних інститутів, ринкової економіки, носіями важливої інформації та невід'ємними супутниками людини. Внаслідок впливу економічних та соціальних факторів вони стали предметом зацікавленості кримінальних структур до підроблення та фальсифікації [1]. У період розповсюдження систем оперативної поліграфії, копіювальної техніки, настільних видавничих систем і комп'ютерних технологій кількість фальсифікацій документів на паперових носіях значно зростає [2]. На сьогоднішній день поняття документа нерозривно пов'язане з його захистом, оскільки відсутність захищеності документів може завдати значної шкоди і збитків державі та її громадянам.

Розвиток технічних можливостей фальсифікації документів на паперових носіях спричинив різке зростання вимог до їх захисту. Дані вимоги стосуються як організації технологічного процесу виготовлення та використання захищених документів так і створення недорогих і надійних засобів захисту, які задовольняли б реальним потребам захисту технологічних процесів використання документів. Існуючі засоби захисту досить дорогі з точки зору реалізації технологічних процесів їх створення і не забезпечують в повній мірі вище наведених вимог. Вирішення поставленої задачі можливе в межах задач побудови та дослідження нових засобів захисту на основі методів формального опису та методів вимірювання параметрів графічних засобів захисту, які б дозволяли проводити просту і ефективну ідентифікацію документів в системі документообігу.

Графічні засоби захисту, залежно від вибраної базової структури, можуть описуватися параметрами, що мають розподілений характер. В цьому випадку для опису параметрів захисту доцільно використовувати засоби теорії графів, що їх апроксимують [1, 3]. Такі засоби доцільно використовувати ще і тоді, коли зор не має явно вираженого симетричного характеру, а формується згідно з певною стратегією чи програмою, яка на кожному кроці формування узору визначає певний напрямок, що вибирається на основі правил формування узору. В даному випадку, в якості параметра захисту, Використовується визначена алгоритмом формування узору величина його зміни при переході від одного тиражу документів до другого. Тоді параметром захисту є не тільки конфігурація графічного образу, в рамках якої виконуються ті чи інші умови, а і особливості графа, що пов'язаний з образом, і величина тиражу документів, що були видані або надруковані з відповідним рисунком чи ззором.

Задача формування графа з певними зміненими характеристиками зводиться до його генерації. Граф може бути заданим рядом різних методів, що відповідають відомим способам його опису [4]. При модифікації графів доцільно застосовувати інваріантні перетворення графів. Приклад ізоморфного перетворення графів наведений на рис. 1.

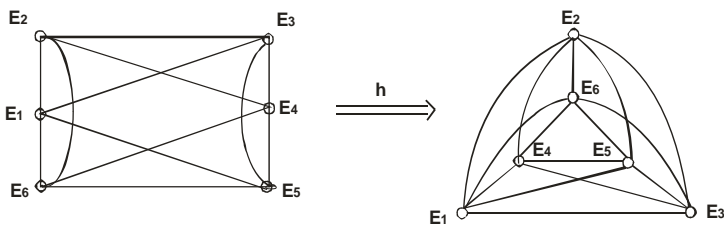


Рис. 1. Приклад ізоморфного перетворення графа G_1 в граф G_2

Якщо граф засобу захисту z , розміщувати на площині документа з визначеною системою координат з відповідним масштабом, то можна

прийняти, що на цій площині задана масштабна сітка, яка визначає величину дискретизації, яка дорівнює $\Delta\xi$ і $\Delta\zeta$.

Введемо поняття про структуру простору або площини, на якій будемо будувати граф G_i . Структура простору визначається функціями, що описують масштаб координат, які прийнято для даного випадку позначати як $E = f_\xi(\xi)$ і $Z = f_\zeta(\zeta)$. Якщо функції f_ξ і f_ζ є лінійними, то структура поверхні є найпростішою і представляє собою прямокутну сітку координат. В цьому випадку $\xi_i = a \cdot \xi$ і $\zeta_i = b \cdot \zeta$. Для спрощення дослідження приймемо, що f_ξ і f_ζ є лінійними. Оскільки існує система координат, то можна говорити про початкові точки побудови графа. Більше того, процес побудови графа G_i можна розглядати як процеси формування деяких траєкторій, що проходять через вершини і можуть перетинатися. Кожну з таких траєкторій позначаємо символом T_i . В цьому випадку граф G_i описується співвідношенням $G_i = U_{i=1}^k \cdot T_i$. Кожна з траєкторій може мати свій початок або починатися з вершини, що вже використовується однією або кількома з попередніх траєкторій T_{i-k} . В цьому випадку до початкових умов з врахуванням яких повинен формуватися граф G_i , крім кількості вершин N , можна додати кількість траєкторій k , які будуть складати граф G_i та початкові точки для кожної з траєкторій $T_i(e_0)$. Очевидно, що початкові точки траєкторій можуть описуватися функціональними співвідношеннями рекурсивного характеру, які обчислюють на основі початкових точок уже сформованих траєкторій T_{i-k} або

$$e_0(T_i) = g[e_0(T_0), h(e_0(T_{i-1}))], \quad (1)$$

де $h(e_0(T_0))$ – функція, що описує спосіб вибору e_0 для T_{i-1} ;

g – функція, що описує залежність між $e_0(T_0)$ початкової точки для першої траєкторії, способу вибору $e_{0(i-1)}$ для траєкторії T_{i-1} та вибором початкової точки $e_{0(i)}$ для текучої траєкторії T_i [5].

Для побудови окремої траєкторії графа T_i необхідно сформулювати умови завершення її побудови, які приведені на (рис.2).

Перша причина припинення формування траєкторії полягає у наступному: правила формування чергового ребра $\mathcal{S}_j \in T_i$ є функціональним описом умов, які визначають спосіб його формування. Змінними в цьому правилі можуть бути ребра, що вже сформовані. При цьому така функція не мусить бути рекурсивною. Кількість змінних $P(e_i)$ або аргументів, що використовується при реалізації функції $L_i(T_i)$, визначають етап побудови T_i , на якому починає використовуватися відповідна функція $L_i(T_i)$.

Оскільки вершини e_i графа G_i розміщуються на структурованій площині, то кожна з них має свої власні координати $e_i = f_e(\xi_i, \zeta_i)$. Функція f_e дозволяє обчислити параметр для вершини e_i на основі значень координат ξ_i, ζ_i . Вибір типу функції f_e залежить від інтерпретації вершин графа G_i , яка приймається в кожному окремому випадку формування засобу захисту окремо. В найпростішому випадку така функція може визначати деяку інтегральну величину, що характеризує віддаль між e_i і e_0 , що можна описати співвідношенням для віддалі між двома точками в Евклідовому просторі [7, 8]:

$$f_e(e_i) = [(\xi_i - \xi_0)^2 + (\zeta_i - \zeta_0)^2]^{1/2}, \quad (2)$$

Розглянемо причину зупинки процесу формування траєкторії T_i , яка полягає у тому, що чергове ребро при своїй реалізації виходить за границі площини, на якій визначено параметри G_i . Суть цього обмеження полягає у наступному. Вся площина чи простір є структурованими. Це також означає, що всі траєкторії, які формуються на площині повинні проходити тільки через вузли структури простору, чи площини. Нехай структура площини є прямокутною ґраткою. Виберемо довільний вузол цієї ґратки $e_{ij}^*(\xi_i, \zeta_i)$ і прийнемо його в якості центрального, або вихідного для подальшого формування траєкторії T_i . Навколо цього вузла існує 8 вузлів, що є безпосередніми сусідами вузла e_{ij}^* . Ці вузли позначимо так:

$$\begin{aligned} & e_{i+1,j}^1(\xi_{i+1}, \zeta_i), e_{i+1,j+1}^2(\xi_{i+1}, \zeta_{i+1}), e_{i,j+1}^3(\xi_i, \zeta_{i+1}), \\ & e_{i-1,i+1}^4(\xi_{i-1}, \zeta_{i+1}), e_{i-1,j}^5(\xi_{i-1}, \zeta_i), e_{i-1,j-1}^6(\xi_{i-1}, \zeta_{i-1}), \\ & e_{i,j-1}^7(\xi_i, \zeta_{i-1}), e_{i+1,j-1}^8(\xi_{i+1}, \zeta_{i-1}) \end{aligned} \quad (3)$$

Всі ці вершини при прямокутній ґратчастій структурі площини є найближчими сусідами вершини e^* і створюють її мінімальне оточення. Якщо на черговому кроці формування ребра $\mathcal{G}_i^*(e_{i,j}^* * e_{i\pm k, j\pm m})$ воно повинно проминути своє найближче оточення, то таке ребро мусить проходити через одну з вершин цього оточення [6].

Суперечність формування чергового ребра \mathcal{G}_i в траєкторії T_i стосовно графа G_i означає порушення умов або властивостей графа заданих у вигляді початкових умов. Наприклад, якщо однією з властивостей графа є задане для нього хроматичне число $\gamma(G_i)$, то формування чергового ребра \mathcal{G}_i з T_i можливе лише за умови його збільшення, тоді процес формування траєкторії графа вважається закінченим і переходимо до формування наступної траєкторії T_{i+1} .

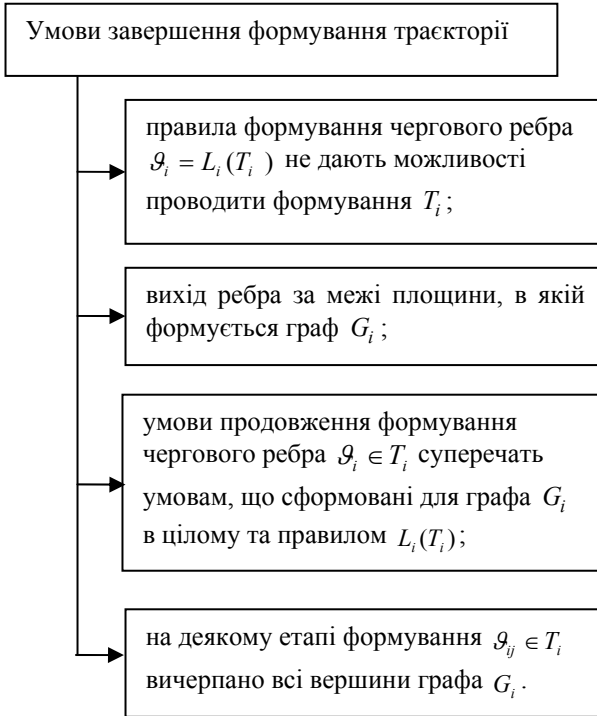


Рис. 2. Умови завершення формування траєкторії графічного засобу захисту

Другий тип правил, що використовується в L_i , складають правила, які описують орієнтацію чергового ребра \mathcal{G}_i . Оскільки всі вершини e_i графа G_i розміщуються у вузлах структури площини і інший спосіб розміщення вершин є недопустимим, то кожна з них описується ідентифікатором, який обчислюється на основі координат відповідної вершини в структурі площини [6]. Тому правила $L_i(T_i)$ для визначення стану вершини можуть використовувати її координати і при цьому не визначати умови досягнення відповідної вершини. В загальному вигляді логічні функції відповідного типу в явній формі записуються таким чином:

$$L_{ij}(T_i) = \left\{ \mathcal{G}_{ik} * \mathcal{G}_{ij} * \left[e_{ij}^g \rightarrow \omega_1(\xi_k, \zeta_r) \rightarrow \dots \rightarrow \omega_g(\xi_m, \zeta_n) \rightarrow e_{i,j+k}^s \right] \right\}, \quad (4)$$

де $\omega_g(\xi_m, \zeta_n)$ – вузол структури площини, який використовується для формування фрагмента t_{ij} траєкторії T_i , і не зайнятий вершиною графа G_i .

Складова умови завершення процесу побудови T_i , яка полягає у тому, що всі вершини G_i вичерпано, не потребує додаткових роз'яснень.

Вище запропонований метод формального опису графічних засобів захисту дозволяє визначати базові параметри, які характеризують стійкість захисту документів, розробити математичну модель в межах якої можна було б досліджувати графічні засоби захисту, оперативно змінювати їх рівень захисту та забезпечити просту і ефективну ідентифікацію документів в системі документообігу.

1. *Киричок П. О.* Захист цінних паперів та документів суворого обліку : монографія / П. О. Киричок, Ю. М. Коростіль, А. В. Шевчук. – К. : НТУУ "КПІ", 2008. – 368 с.
2. *Лазаренко Е. Т.* Захист друкованої продукції : навч. посіб. / Е. Т. Лазаренко, В. З. Майк, А. В. Шевчук, С. В. Жидецький. – Л.: УАД, 2007. – 96 с.
3. *Русин Б. П.* Системи синтезу, обробки та розпізнавання складноструктурованих зображень / Б. П. Русин. – Л. : Вертикаль, 1997. – 264 с.
4. *Зыков А. А.* Основы теории графов / А. А. Зыков. – М. : Наука, 1987. – 384 с.
5. *Сапаров М.* Рекуррентные теоретико-графовые функции и алгоритмы их вычисления / М. Сапаров. – Ашхабад : Ылым, 1987. – 290 с.
6. *Пашкевич В. З.* Опис графічних засобів захисту на основі їх графового представлення / В. З. Пашкевич // Моделювання та інформаційні технології : зб. наук. пр. / НАН України, Ін-т проблем моделювання в енергетиці ім. Г. Є. Пухова. – К., 2005. – Вип. 35. – С. 76–84.
7. *Алексеев В. Б.* Элементы теории графов, схем и автоматов : учеб. пособие / В. Б. Алексеев, С. А. Ложкин. – М. : Изд-во ВМиК МГУ, 2000. – 58 с.
8. *Серебрянников О. Ф.* Эвристические принципы и логические исчисления / О. Ф. Серебрянников. – М. : Наука, 1970. – 282 с.

Поступила 18.01.2010р.

УДК 534.17.171

А. П. Матковский, к.т.н., Е. А. Немкова, к.ф.-м.н.
Институт новейших технологий и управления им.В.Чорновола,
каф. Компьютерных систем и защиты информации, Львов, Украина

ОЦЕНКА ПОГРЕШНОСТИ ОПРЕДЕЛЕНИЯ МЕСТОПОЛОЖЕНИЯ ИЗЛУЧАТЕЛЯ ДАЛЬНОМЕРНЫМИ МЕТОДАМИ

Abstract: The system of equations, depending on parameters which can contain errors, is examined. The method of calculation of maximal and middling quadratic errors of decision of the system at the small errors of parameters is presented.

Рассматривается система уравнений, зависящая от параметров, которые могут содержать погрешности. Предлагается способ вычисления максимальной и среднеквадратичной погрешностей решения системы при малых ошибках параметров. В качестве примера рассматривается задача