УДК 004.056.55

І.О. РОЗЛОМІЙ
Черкаський державний бізнес-коледж
Г.В. КОСЕНЮК
Черкаський національний університет імені Богдана Хмельницького

ВИЯВЛЕННЯ ПОРУШЕНЬ ЦІЛІСНОСТІ ЕЛЕКТРОННОГО ДОКУМЕНТУ ШЛЯХОМ ПЕРЕХРЕСНОГО ХЕШУВАННЯ

Масове впровадження та використання електронного документообігу спричинило появу такого явища, як підробка електронних документів. Стаття присвячена розробці методу виявлення фальсифікацій в електронних документах для підвищення достовірності інформації. На основі використання методів обчислення хеш-функції електронного документу було побудовано метод перехресного хешування, який дає змогу виявити фальсифікований фрагмент інформації. В статті запропонований новий метод, який дозволяє виявити порушення цілісності електронного документу, вказавши на конкретний інформаційний блок, в якому відбулися зміни. Для цього введено поняття міні хеш-функцій, які спочатку обчислюються послідовно для кожного горизонтального, потім – для кожного вертикального блоку інформації. В разі порушення цілісності електронного документу, невідповідність значень міні хеш-функцій вкаже на перетині якого рядка і стовпця був змінений блок інформації.

Ключові слова: *електронний документ, порушення цілісності, хеш-функція, перехресне хешування, матричні криптографічні перетворення.*

I.O. ROZLOMII
Cherkassy State Business College
G.V. KOSENYUK
Cherkassy Bogdan Khmelnytsky National University

DETECTION OF VIOLATIONS OF ELECTRONIC DOCUMENTS INTEGRITY BY CROSS-HASHING

Mass implementation and using of electronic documents led to the emergence of such the fact as of counterfeiting of electronic documents. The article is devoted to actual issues of developing new and improving existing methods and tools of counteracting falsifications of electronic documents. The method of cross-hashing based on the use of methods for calculating the hash function of an electronic document has been constructed, which enables to detect a fake fragment of information. A new approach that can detect of violations of integrity of the electronic document and it points to specific changed information block was proposed in the article. For this goal, the notion of mini hash functions was introduced that originally calculated for each of horizontal blocks, then – for each of vertical blocks of information. Mini hash functions can be calculated by any hashing method. The model for calculating mini hash functions is based on the use of matrix cryptographic transformation operations has been showed in the article. In case of violation of integrity of the electronic document disparity of values between mini hash functions will point at the intersection whose of row and column has been changed block of information. Thus, an important scientific task of developing a method for detecting falsifications in an electronic document was solved.

Keywords: *electronic document, violations of integrity, a hash function, cross-hashing, cryptographic transformation matrix.*

Вступ. Об’єм цифрової документованої інформації, яку доводиться зберігати, передавати постійно зростає, з’являються системи електронного документування [1]. Сучасні методи накопичення, обробки та передачі електронних документів (ЕД) сприяли появі загроз, пов’язаних з можливістю порушення цілісності інформації. Одним з ефективних способів забезпечення цілісності ЕД є накладання електронного цифрового підпису (ЕЦП), який в найпростішому випадку є результатом обчислення хеш-функції. Тому, очевидною є актуальність розробки алгоритмів хешування. Досить часто виникає необхідність передачі конфіденційних електронних документів. Звичайно, необхідна абсолютна впевненість в тому, що переданий через мережу ЕД повністю ідентичний оригіналу і його основний зміст не був змінений в процесі передачі чи зберігання. Для цього існують засоби ідентифікації цифрової інформації, одним з яких є хешування.

Постановка проблеми. Зважаючи на те, що рівень злочинності в сфері інформаційних технологій постійно зростає, підробка електронних документів набула рис масового явища. Існуючі механізми забезпечення цілісності ЕД, цифровий підпис, зокрема, можуть лише підтвердити чи спростувати факт порушення цілісності інформації. До тепер, ніхто з науковців не займався пошуком методів виявлення підробки в електронних документах. Це питання є досить актуальним, насамперед, тому, що важливо розуміти, який конкретно фрагмент документу був змінений, підроблений. На основі реалізації запропонованого методу виявлення порушень цілісності ЕД, можна робити висновки про мету підробки, визначити круг підозрюваних в здійсненні злочину – фальсифікації документів.

Аналіз останніх досліджень та публікацій. [2–4] показує, що операції прямого та оберненого матричного перетворення є придатними для побудови алгоритмів обчислення хеш-функції, якщо при цьому виконуються всі умови невиродженості матриці. В статті [5] було запропоновано методи обчислення хеш-функції електронного документу, які базуються на матричних криптографічних перетвореннях. Отримані в попередніх дослідженнях результати є основою для створення нового методу виявлення порушень цілісності ЕД шляхом перехресного хешування.

Формулювання цілей статті. Метою роботи є розробка методу виявлення фальсифікацій в ЕД шляхом перехресного хешування.

Виклад основного матеріалу. Як вже говорилося раніше, хешування є одним з основних способів ідентифікації даних. Функція хешування – детермінована функція, на вхід якої подається масив бітів довільного розміру, а на виході отримуємо фіксовану контрольну суму. Контрольна сума – обчислене значення, яке ідентифікує ЕД і є найпростішим способом перевірки цілісності цифрових даних. Обчислення

хеш-функції повністю всього ЕД дає змогу отримати контрольну суму, фіксовану кількість бітів, яка об'єднавшись з документом служитиме найпростішим варіантом ЕЦП. Наявність ЕЦП свідчитиме про автентичність та цілісність інформації при виконанні механізму перевірки підпису. Для перевірки цілісності ЕД отримувач підписаного ЕД обчислює значення хеш-функції і порівнює його з самостійно згенерованим значенням. Тобто в разі порушення цілісності ЕД – навмисних чи випадкових змін в документі, невідповідність значень хеш-функції говоритиме про факт підробки документу.

Завдання захисту ЕД зводиться не тільки до забезпечення цілісності інформації. В багатьох випадках не достатньо знати лише те чи відбулися зміни в ЕД, чи ні. Важливо розуміти, де конкретно в документі відбулися зміни. Тому, вкрай важливим є завдання пошуку способів виявлення фальсифікацій в електронних документах. Для цього, як один з варіантів, можна запропонувати метод, який базується на використанні алгоритмів хешування.

Суть запропонованого методу виявлення фальсифікацій в електронному документі полягає в поблоковому обчисленні хеш-функції електронного документа. Для цього ЕД потрібно розбити на інформаційні блоки однакового розміру, як показано на рис. 1.

A_{11}	A_{12}	A_{13}	A_{14}	….	A_{1n}
A_{21}	A_{22}	A_{23}	A_{24}	….	A_{2n}
A_{31}	A_{32}	A_{33}	A_{34}	…	A_{3n}
A_{41}	A_{42}	A_{43}	A_{44}	…	A_{4n}
…	…	…	…	…	…
A_{n1}	A_{n2}	A_{n3}	A_{n4}	…	A_{nn}

Рис. 1. Поділ електронного документу на фрагменти інформації

З рис. 1 видно, що ЕД розбивається на блоки A_{ij}, де $i \in [1,n], j \in [1,n]$. Далі, необхідно обчислити значення хеш-функції кожного блоку інформації, введемо для них поняття міні хеш-функції.

Обчислення міні хеш-функцій виконуються по аналогії з обчисленням хеш-функції всього електронного документа, як показано в статті [5] і для знаходження міні хеш-функцій може бути використаний будь-який з запропонованих в статті [5] алгоритмів.

Позначимо через послідовність $F_{11}, F_{12}, ..., F_{1n}$ обчислені значення хеш-функцій кожного горизонтального блоку інформації. Значення міні хеш-функцій горизонтальних блоків можна представити у вигляді системи (1).

$$\begin{cases} F_{21} = F(A_{11}) \cup F(A_{21}) \cup ... \cup F(A_{n1}); \\ F_{22} = F(A_{12}) \cup F(A_{22}) \cup ... \cup F(A_{n2}); \\ ..... \\ F_{2n} = F(A_{1n}) \cup F(A_{2n}) \cup ... \cup F(A_{nn}). \end{cases} \quad (1)$$

Аналогічно $F_{21}, F_{22}, ..., F_{2n}$ – міні хеш-функції вертикальних блоків інформації, як показано на рис. 2. Значення міні хеш-функцій вертикальних блоків представлені системою (2).

$$\begin{cases} F_{21} = F(A_{11}) \cup F(A_{21}) \cup ... \cup F(A_{n1}); \\ F_{22} = F(A_{12}) \cup F(A_{22}) \cup ... \cup F(A_{n2}); \\ ..... \\ F_{2n} = F(A_{1n}) \cup F(A_{2n}) \cup ... \cup F(A_{nn}). \end{cases} \quad (2)$$

Для обчислення міні хеш-функцій введемо деякі позначення. Нехай ключова матриця задана виразом (3).

$$A = \begin{pmatrix} a_{11}, a_{12}, ..., a_{1m} \\ a_{21}, a_{22}, ..., a_{2m} \\ . \quad . \quad . \quad . \quad . \\ a_{m1}, a_{m2}, ..., a_{mm} \end{pmatrix}, \quad (3)$$

де $a_{ij} \in [0,1];$ – коефіцієнти ключової матриці, тоді матриця міні хеш-функції, буде задана виразом (4).

$$F_{ij} = \begin{pmatrix} b_{11}, b_{12}, ..., b_{1n} \\ b_{21}, b_{22}, ..., b_{2n} \\ . \quad . \quad . \quad . \quad . \\ b_{n1}, b_{n2}, ..., b_{nn} \end{pmatrix}, \quad (4)$$

де $b_{ij} \in [0;1]$ – коефіцієнти матриці міні хеш-функції.

В найпростішому випадку можна використати алгоритм послідовного додавання до одного рядка матриці іншого рядка, вибраного на основі аналізу фрагменту інформації.

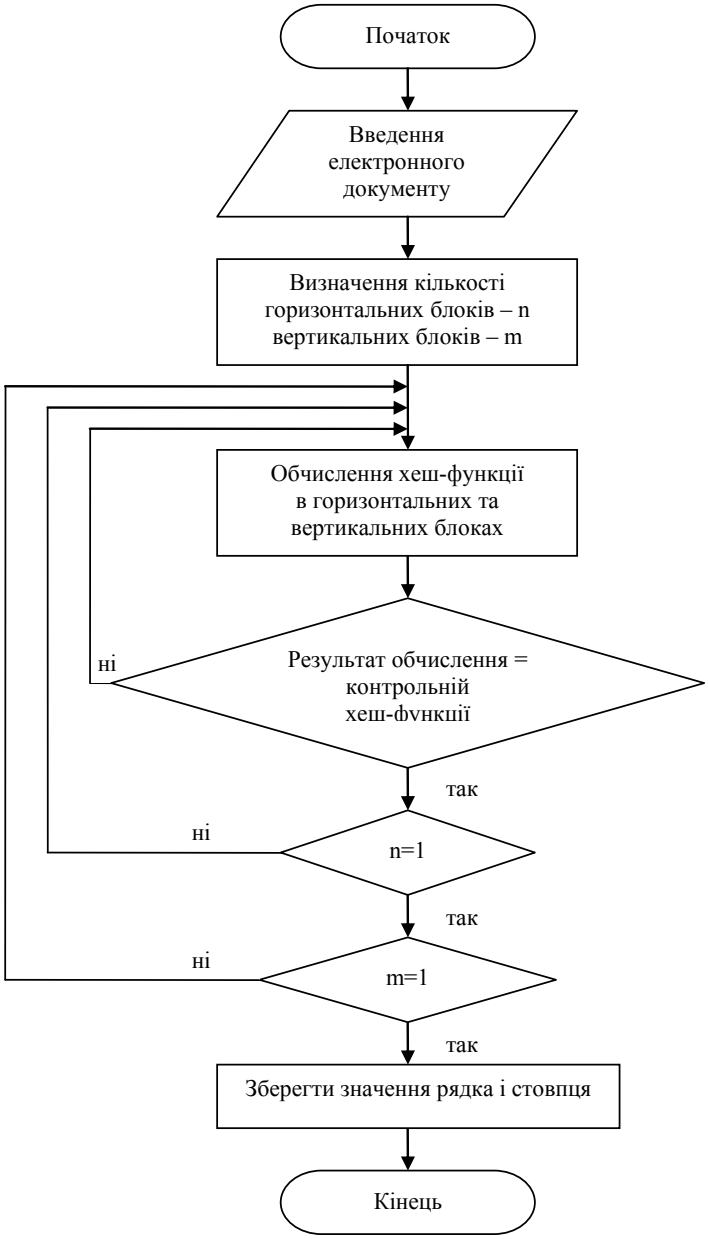

Рис. 3. Алгоритм виявлення фальсифікованого фрагменту електронного документу методом перехресного хешування

Процес обчислення міні хеш-функції з заданої ключової матриці описується моделлю (5).

$$F_{ij} = \begin{pmatrix} b_{11}(a_{11} \oplus a_{21}), b_{12}(a_{12} \oplus a_{22}), \ldots b_{1n}(a_{1n} \oplus a_{2n}) \\ b_{21}(a_{21} \oplus a_{n1}), b_{22}(a_{22} \oplus a_{n2}), \ldots b_{2n}(a_{2n} \oplus a_{nn}) \\ \ldots \\ b_{n1}(a_{n1} \oplus a_{11}), b_{n2}(a_{n2} \oplus a_{12}), \ldots b_{nn}(a_{nn} \oplus a_{1n}) \end{pmatrix} \quad (5)$$

На рис. 3 показана блок-схема алгоритму виявлення фальсифікованого фрагменту електронного документу методом перехресного хешування.

Суть даного алгоритму обчислення міні хеш-функцій можна описати такими кроками:

1) на основі матричних криптографічних перетворень обчислюємо значення міні хеш-функції $F_{11}, F_{12}, \ldots, F_{1n}$, за описаною вище моделлю;

2) далі послідовно потрібно обчислити значення міні хеш-функцій вертикальних блоків інформації $F_{21}, F_{22}, \ldots, F_{2n}$.

В разі здійснення змін, модифікацій в ЕД, звичайно, зміняться і значення міні хеш-функцій. На основі того, які конкретно міні хеш-функції при повторному обчисленні змінили своє значення можна судити в якому саме інформаційному блоці ЕД відбулося порушення цілісності. Тобто горизонтальна міні хеш-функція вкаже на рядок, вертикальна – на стовпець, на перетині яких була змінена інформація, рис. 4.

A_{11}	A_{12}	A_{13}	A_{14}	…	A_{1n}	Обчислення міні хеш-функцій $F(A_{in})$	F_{11}
A_{21}	A_{22}	A_{23}	A_{24}	…	A_{2n}		F_{12}
A_{31}	A_{32}	A_{33}	A_{34}	…	A_{3n}		F_{13}
A_{41}	A_{42}	A_{43}	A_{44}	…	A_{4n}		F_{14}
…	…	…	…	…	…		…
A_{n1}	A_{n2}	A_{n3}	A_{n4}	…	A_{nn}		F_{1n}
Обчислення міні хеш-функцій $F(A_{ij})$							
F_{21}	F_{22}	F_{23}	F_{24}	…	F_{2n}		

Рис. 2. Обчислення міні хеш-функцій

A_{11}	A_{12}	A_{13}	A_{14}	…	A_{1n}	F_{11}
A_{21}	A_{22}	A_{23}	A_{24}	…	A_{2n}	F_{12}
A_{31}	A_{32}	A_{33}	A_{34}	…	A_{3n}	F_{13}
A_{41}	A_{42}	A_{43}	A_{44}	…	A_{4n}	F_{14}
…	…	…	…	…	…	…
A_{n1}	A_{n2}	A_{n3}	A_{n4}	…	A_{nn}	F_{1n}
F_{21}	F_{22}	F_{23}	F_{24}	…	F_{2n}	

Рис. 4. Виявлення фальсифікованого фрагменту інформації

З рис. 3 видно, що при перевірці, міні хеш-функції F_{24} і F_{13} змінили своє значення, це означає, що в інформаційному блоці A_{34} відбулися зміни, тобто даний фрагмент електронного документу був фальсифікований (6).

$$F_{13} \bigcap F_{24} \to A_{34} \tag{6}$$

Висновки. В статті було розкрито питання пошуку шляхів забезпечення цілісності електронних документів. В підсумку було розроблено метод виявлення фальсифікацій в ЕД шляхом перехресного хешування. Запропонований метод базується на знаходженні хеш-функції блоків інформації. У результаті проведених досліджень, можна зробити висновки, що для реалізації даного методу можна використовувати будь-який алгоритм обчислення хеш-функції. Як один з варіантів, показаний алгоритм обчислення міні хеш-функції, на основі послідовного виконання операції додавання за модулем рядків матриці.

Таким чином, запропонований метод дозволить виявляти зміни в електронному документі, на основі яких можна робити припущення про мету підробки та можливих зловмисників.

Література

1. Сабанов А.А. Некоторые аспекты защиты электронного документооборота / А.А. Сабанов // Connect! Мир связи. – 2010. – № 7. – С. 62–64.

2. Рудницький В. М. Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації / В. М. Рудницький, В. Г. Бабенко, С. В. Рудницький // Збірник наукових праць Харківського університету Повітряних Сил. – 2012. – № 4 (33). – С. 198–200.

3. Миронець І.В. Підвищення достовірності процесу матричного криптографічного перетворення / І.В. Миронець // Информационные технологии и системы управления. – 2015. – № 5/6(25). – С. 52–54.

4. Голуб С. В. Метод синтезу операцій криптографічного перетворення на основі додавання за модулем два / С. В. Голуб, В. Г. Бабенко, С. В. Рудницький // Системи обробки інформації : зб. наук. праць. – 2012. – № 3(101). – С. 119–122.

5. Розломій І.О. Методи обчислення хеш-функції електронного документу на основі матричних криптографічних перетворень / І.О. Розломій // Вісник ЧДТУ. Технічні науки. – 2016. – № 4. – С. 88–94.

References

1. Sabanov A.A. (2010) Some Aspects of Electronic Document Work Protection Connect! The world of communication, 7, pp. 62–64.

2. Rudnitsky V.M., Babenko V.G. and Rudnitsky S.V. (2012) The synthesis method of matrix models of cryptographic operations data encoding and decoding. Proceedings of Kharkiv Air Force University, 4, pp. 198–200.

3. Myronets I.V. (2015) Increased process reliability matrix cryptographic transformation. Information Technology and management systems, 5/6 (25), pp. 52–54.

4. Golub S.V., Babenko V.G. and Rudnitsky S.V. (2012) The method of synthesis of the operations cryptographic transformations on the basis of addition modulo two. Information processing systems, 3 (101), pp. 119–122.

5. Rozlomii I.O. (2016) The methods of calculating of hash function of electronic documents on the basis of matrix cryptographic transformation**.** Bulletin of Cherkasy State Technological University. Series: Technical sciences, 4, pp. 88–94.

Рецензія/Peer review : 17.9.2018 р. Надрукована/Printed : 19.9.2018 р.
Рецензент: д.т.н., проф. Рудницький В. М.