УДК 004.491.01

І.М. Дронюк, канд. фіз.-мат. наук, доц., Нац. ун-т "Львівська політехніка"

ПІДВИЩЕННЯ РІВНЯ БЕЗПЕКИ ДОКУМЕНТООБІГУ НА ОСНОВІ НОВИХ МЕТОДІВ ЗАХИСТУ ТА ІДЕНТИФІКАЦІЇ ДОКУМЕНТІВ

І.М. Дронюк. **Підвищення рівня безпеки документообігу на основі нових методів захисту та ідентифікації документів.** Розроблено метод захисту та ідентифікації документів на матеріальних носіях на основі узагальнення дискретного перетворення Фур'є з метою підвищення рівня безпеки документообігу. Проведені експериментальні дослідження стійкості методу до ряду атак доводять його ефективність.

Ключові слова: захист документів на матеріальних носіях, ідентифікація документів, Ateb-функції, безпека документообігу.

И.М. Дронюк. **Повышение уровня безопасности документооборота на основе новых методов защиты и идентификации документов**. Разработан метод защиты и идентификации документов на материальных носителях на основании обобщения дискретного преобразования Фурье с целью повышения уровня безопасности документооборота. Проведенные экспериментальные исследования устойчивости метода к ряду атак доказывают его эффективность.

Ключевые слова: защита документов на материальных носителях, идентификация документов, Ateb-функции, безопасность документооборота.

I.M. Dronyuk. Improved security of document workflow based on new methods of protection and identification of documents. The method for the identification and protection of printed documents on the basis of discrete Fourier transform generalization in order to increase the security level of documents is developed. The pilot study of the method's stability to a number of attacks proves its effectiveness.

Keywords: printed document security, identification of documents, Ateb-functions, security of document workflow.

Вступ. Протягом останніх років широко впроваджуються системи електронного документообігу як в приватному секторі, так і в державному. Це створює ряд нових проблем, пов'язаних з інформаційною безпекою, як перед спеціалістами з галузі інформаційних технологій, так і перед спеціалістами в галузі документообігу [1]. Але при цьому важливо розуміти, що інтенсивне впровадження інформаційних технологій у сферу документообігу ставить повністю нові завдання в галузі безпеки традиційного документообігу на матеріальних носіях, що пов'язано як з новими методами утворення, зберігання та розповсюдження інформації на паперових носіях, так і зі зміною самих матеріальних носіїв, а саме введення пластикових носіїв інформації, нових видів паперу та ін. Тому підвищення рівня безпеки документів на матеріальних носіях в умовах інформатизації суспільних процесів є актуальним завданням. Розглядаються нові методи підвищення рівня захищеності друкованих документів, а також методи ідентифікації друкованих документів.

Метою роботи є розроблення методів захисту та ідентифікації документів для підвищення рівня захищеності з метою запобігання порушенню цілісності інформації на матеріальних носіях для забезпечення відповідного рівня безпеки документообігу.

Постановка завдання. Існують загрози, що виникають супроти документообігу як традиційного, так і електронного. До першого виду загроз можна віднести знищення, спотворення документів, несанкціонований доступ до документів, порушення їх цілісності. До другого виду загроз відносяться недотримання норм і законів щодо утворення, зберігання та знищення документів. До третього виду загроз можна віднести різного роду катастрофічні явища, наприклад, пожар або пошкодження водою та інш. [2]. Якщо другий і третій вид загроз можна попередити засобами дотримання загальних норм безпеки життєдіяльності і законодавчих норм, то перший

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

вид загроз існуватиме завжди. Це пов'язане з тим, що при проведенні різних видів діяльності будь-якою організацією чи державою завжди знайдуться зловмисники, які прагнутимуть перешкодити чи видобути інформацію про ці дії.

Загрози, класифіковані до першого виду, їх можна поділити на загрози цілісності та загрози конфіденційності інформації. Можна виділити п'ять основних видів атак на документи на матеріальних носіях: часткова підробка, повна підробка паперового носія, фальсифікація документів, фальсифікація персоніфікованих атрибутів та реквізитів друкованих документів, крадіжка. Завдання засобів захисту — ефективно протидіяти цим загрозам. При сучасному розвитку комп'ютерної техніки підробити можна все. Але є два основні критерії — це витрати часу і грошей, які необхідно затратити, щоб підробити той чи інший документ. Тому методи і засоби захисту повинні розроблятись з врахуванням особливостей кожного конкретного друкованого документа і повинні бути розраховані так, щоб підробка була нерентабельною. Зрозуміло, наприклад, що захист проїзних документів та банківських документів потребує різних рівнів захисту. Запропоновано нові способи захисту, що базуються на векторному форматі, і показано, що графічні методи захисту можуть протидіяти більшості видів атак на документи на матеріальних носіях [3]. Перевагою графічних методів захисту є відносно менша вартість їх реалізації, а також можливість їх утворення за допомогою стандартного устаткування.

Поряд з розробкою нових методів захисту необхідно розробляти нові методи ідентифікації документів. Для підвищення рівня захищеності друкованих документів за методами графічного захисту та ідентифікації запропоновано апарат теорії Ateb-функцій, зокрема Ateb-перетворень. Запропоновано метод ідентифікації документа на основі вбудовування прихованої інформації. Пропонується метод ідентифації документа на основі значень параметрів *m, n* Ateb-функцій $f(m, n, x)$ та введеного аналога дискретних ортогональних перетворень [4]. Перевірка на стійкість реалізована шляхом екпериментальних досліджень.

Результати дослідження. Вводится у розгляд дискретне Ateb-перетворення (ДАП). Нехай документ заданий у вигляді двовимірної дискретної послідовності $\mathbf{S}(p, q)$, де p, q — біжучі пікселі зображення розміром $N \times N$. Введемо у розгляд функції $A(m, n, k, g)$ та $B(m, n, k, g)$ за формулами

$$A(m, n, k, g) = \sum_{p=1}^{N-1} \mathbf{S}(p, q) ca^m \left(m, n, -i\frac{2\Pi pk}{N} \right), \quad k, g = 1, \ldots, N, \tag{1}$$

$$B(n, m, k, g) = \sum_{p=1}^{N-1} \mathbf{S}(p, q) sa^n \left(n, m, -i\frac{2\Pi pk}{N} \right), \quad k, g = 1, \ldots, N, \tag{2}$$

де p, q — номери гармонік;

$ca(m, n, \varpi)$ — функція Ateb-косинуса;

$sa(m, n, \varpi)$ — функція Ateb-синуса;

$\Pi = \Pi(m, n)$ — період Ateb-функції.

Позначивши $i = \sqrt{-1}$, пряме ДАП можна задати формулою

$$X(m, n, k, g) = A(m, n, k, g) - iB(n, m, k, g). \tag{3}$$

Буде отримано вираз для оберненого перетворення у вигляді

$$\begin{aligned} \mathbf{S}(m, n, p, g) = \frac{1}{N} \sum_{k=1}^{N-1} \Bigg\{ & A(m, n, k, q) ca\left(m, n, -i\frac{2\Pi pk}{N}, -i\frac{2\Pi gq}{N} \right) + \\ & + B(n, m, k, q) sa\left(m, n, -i\frac{2\Pi pk}{N}, -i\frac{2\Pi gq}{N} \right) \Bigg\}, \quad p, q = 1, \ldots, N. \end{aligned} \tag{4}$$

Вхідне зображення документа у вигляді матриці $\mathbf{S}(p, q)$ формально при дії прямого та оберненого ДАП трансформується у матрицю $\mathbf{S}(m, n, p, q)$. Параметри *m, n* Ateb-функцій можна використати для персоніфікації документів. Для фіксованих значень параметрів m, n можна відтворити значення пікселя зображення $\mathbf{S}(p, q)$. Таке представлення дозволяє використати запропоновані перетворення для створення прихованих вбудованих повідомлень і персоніфікованого захисту документів.

Для вбудовування прихованого зображення застосовувався адитивний алгоритм з використанням ДАП, заданого формулою (3) з різними значеннями параметрів m і n. Для зчитування

зображення застосовувався алгоритм оберненого перетворення (4). Розроблене додане зображення чи повідомлення є невидимим, оскільки зміни проводяться у невеликій кількості елементів, тому запропонований метод належить до методів приховування даних у частотній області.

За допомогою ДАП переорюється зображення, а далі застосовуються два способи вбудовування прихованого зображення. Перший спосіб: r найбільших значень змінюються за формулою для вбудовування прихованого зображення у вигляді

$$z^{wp} = z^{p} + \alpha w, \tag{5}$$

де z^{wp} — перетворене зображення;

z^{p} — початкове зображення;

w — приховане зображення розміром r;

α — коефіцієнт для регулювання величини вбудовування.

Другий спосіб: замість формули (5) застосовується формула

$$z^{wp} = z^{p} + e^{\alpha w}. \tag{6}$$

Для перевірки ефективності та стійкості запропонованого методу ідентифікації проведені експерименти для значень параметрів m=3, n=1/7. Тестування проводилось для стандартних зображень з тестової бази USC-SIPI [5], зокрема, для одного тестового зображення. Проведена така серія атак:

— зміна розміру файла 10, 25, 50, 75, 150, 200 %;

— поворот 1 ,5, 10, 45, 90, 180°;

— стиснення зображення на 10, 25, 50 %;

— зміна глибини кольору зображення 256→128, 256→64, 256→32, 256→16, 256→8, 256→4, 256→2.

Критерієм присутності прихованого зображення взято кореляцію, що обчислюється за формулою

$$K = \frac{1}{r-1}\sum_{i=1}^{r}\frac{(c_i^w - \overline{c}_i^w)(w_i - \overline{w})}{\sigma_c \sigma_w}, \tag{7}$$

де K — кореляційний критерій;

r — розмір прихованого зображення;

c_i^w — i-й елемент зображення;

$\overline{c}_i^w$ — середнє значення елементів зображення;

w_i — i-й елемент прихованого зображення;

$\overline{w}$ — середнє значення елементів прихованого зображення;

σ_c — стандартне відхилення елементів зображення з прихованим зображенням;

σ_w — стандартне відхилення елементів прихованого зображення.

Якщо обчислене значення K є більшим за задане певне порогове значення $K_{\text{пор}}$, то вважається, що приховане зображення присутнє, а отже документ ідентифіковано.

Результати експериментів ідентифікації документів після проведених атак з різними коефіцієнтами величини вбудованого зображення α за формулами (5) і (6) представлено в таблиці. Знаком "+" позначено виявлення вбудованого зображення, знаком "–" вбудоване не виявлене зображення.

Результати екперименті проведених атак для перевірки ефективності методу на прикладі тестового зображення

Вид атаки	Зміна розміру файла, %							Поворот, градусів						Стиск, рази %			Зміна глибини кольору зображення					
Способи вбудовування	10	25	50	75	150	200	1	5	10	45	90	180	10	25	50	128	64	32	16	8	4	2
Спосіб 1, α=0,1	–	–	–	–	–	–	+	+	+	+	+	+	–	+	+	+	+	+	+	+	+	+
Спосіб 1, α=0,5	–	–	–	–	–	–	+	+	+	+	+	+	–	+	+	+	+	+	+	+	+	+
Спосіб 1, α=0,9	+	+	–	–	–	–	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Спосіб 2, α=0,1	+	+	–	–	–	–	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Спосіб 2, α=0,5	+	+	–	–	–	–	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Спосіб 2, α=0,9	+	+	–	–	–	–	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

Як видно з проведених екпериментів, запропонований метод на основі ДАП є стійким до більшості видів атак. Це доводить ефективність і стійкість запропонованого методу. Метод має ряд переваг перед існуючими за співвідношенням: рівень захищеності — витрати на організацію захисту.

Висновок. Представлені результати експериментальних досліджень застосування опрацьованого методу ідентифікації на основі вбудовування прихованих зображень є ефективними згідно з параметрами стійкості і безпеки. Запропонований метод є новим і належить до методів захисту документів на основі приховування даних у частотній області, полягає у застосуванні ДАП, що базується на Ateb- функціях. Розроблено метод захисту та ідентифікації для підвищення рівня захищеності документів з метою запобігання порушенню цілісності інформації на матеріальних носіях для забезпечення відповідного рівня безпеки документообігу.

Сфера застосування запропонованого методу охоплює документообіг у різних організаціях, де необхіною умовою є захист та ідентифікація документів. Запропонований метод перевірявся на файлах зображень, але може бути використаний для захисту аудіо-, відеофайлів і електронних текстових документів. Це свідчить про актуальність та практичну значимість методу.

Література

1. Кузнецов, С.Л. Современные технологии документационного обеспечения управления: учеб. пособие для вузов / С.Л. Кузнецов; под ред. проф. Т.В. Кузнецовой. — М.: Изд. дом МЭИ, 2010. — 232 с.
2. Коншин, А.А. Защита полиграфической продукции от фальсификации / А.А. Коншин. — М.: Синус, 1999. — 160 с.
3. Назаркевич, М. Методи підвищення ефективності поліграфічного захисту засобами Ateb-функцій: [Моногр.] / М.А. Назаркевич. — Львів: Вид-во Нац. уні-ту "Львів. політехніка", 2011. — 188 с.
4. Сеник, П.М. Обернення неповної Beta-функції / П.М. Сеник. // Укр. мат. журн. — 1969. — № 3. — С. 325 — 333.
5. The USC-SIPI Image Database [Електронний ресурс]. — http://sipi.usc.edu/database/

References

1. Kuznetsov S.L. Sovremennye tekhnologii dokumentatsionnogo obespecheniya upravleniya: uchebnoe posobie dlya vuzov [Modern technologies of document management: a manual for high schools] / edited by prof. T.V. Kuznetsova. — Moscow, 2010. — 232 p.
2. Konshin A.A. Zashchita poligraficheskoy produktsii ot falsifikatsii [Protection of printed products against counterfeiting] / A.A. Konshin. — Moscow, 1999. — 160 p.
3. Nazarkevych, M. Metody pidvyshchennia efektyvnosti polihrafichnoho zakhystu zasobamy Ateb-funktsii: [Monohr.] [Methods of improving the efficiency of printing facilities with Ateb-protection functions] : [monograph] / M.A. Nazarkevych. — Lviv, 2011. — 188 p.
4. Senyk, P.M. Obernennia nepovnoi Beta-funktsii [Inversion of incomplete Beta-function] / P.M. Senyk. // Ukr. mat. zhurn. [Ukrainian Mathematical Journal]. — 1969. — # 3. — pp. 325 — 333.
5. The USC-SIPI Image Database [Electronic resource] : http://sipi.usc.edu/database/

Рецензент д-р техн. наук, проф. Одес. нац. політехн. ун-ту Гогунський В.Д.

Надійшла до редакції 25 жовтня 2013 р.