УДК 659.512.011.56.007.52

Восьмая Международная научно-техническая конференция **«Информационные технологии в промышленности» (ITI*2015)** : тезисы докладов (2–3 апреля 2015 года, Минск). – Минск : ОИПИ НАН Беларуси, 2015. – 128 с. – ISBN 978-985-6744-87-0.

Представлены тезисы докладов Восьмой Международной научно-технической конференции «Информационные технологии в промышленности» (2–3 апреля 2015 года, Минск), в которых рассматриваются научно-методические и системные аспекты разработки и внедрения информационных технологий проектирования, производства и управления на предприятиях, в проектно-конструкторских и технологических организациях различных отраслей промышленности, полученные в странах СНГ и дальнего зарубежья за последние годы. В тезисах анализируются вопросы математического моделирования объектов и процессов, анализа и синтеза объектов проектирования, производства и управления, автоматизации проектирования машиностроительных конструкций, микроэлектронных и радиоэлектронных изделий и технологических процессов их изготовления, построения и внедрения CALS/ERP-технологий на промышленных предприятиях, кадрового обеспечения разработки и эксплуатации продуктов и систем информационных технологий, а также модели и методы оптимального планирования и управления производством.

Тезисы одобрены и рекомендованы к публикации программным комитетом конференции, прошли рецензирование и печатаются в виде, доработанном авторами с учетом замечаний рецензентов.

Научные редакторы:

доктор физико-математических наук, профессор М.Я. Ковалев,
доктор технических наук П.Н. Бибило,
кандидат технических наук А.Г. Гривачевский,
кандидат технических наук Н.Н. Гущинский

ISBN 978-985-6744-87-0

ОРГАНИЗАТОРЫ

Национальная академия наук Беларуси

Объединенный институт проблем информатики НАН Беларуси

Министерство промышленности Республики Беларусь

Министерство образования Республики Беларусь

Белорусский национальный технический университет

Белорусский государственный университет

Белорусский государственный университет информатики и радиоэлектроники

ГЕНЕРАЛЬНЫЙ ИНФОРМАЦИОННЫЙ ПАРТНЕР

Научно-практический журнал «Наука и инновации»

УДК 681.32

МОДЕЛИРОВАНИЕ СТЕГАНОГРАФИЧЕСКОЙ СИСТЕМЫ В ЗАДАЧАХ ПО ОХРАНЕ АВТОРСКИХ ПРАВ

Н.П. Шутько, Н.И. Листопад, П.П. Урбанович
Белорусский государственный технологический университет, Минск
e-mail: nadya_ur@rambler.ru

Задача определения и доказательства права собственности на различные документы, относящиеся к области информационных технологий, становится все более актуальной. К основным из упомянутых документов относятся тексты, графические изображения, компьютерные программы и базы данных. Эту задачу можно решить с помощью соединения средств и методов стеганографии и криптографии.

В докладе анализируются особенности математического моделирования таких систем. Основу их функционирования составляет стеганографическое преобразование исходного документа-контейнера с целью осаждения в нем авторской информации [1].

Модель предусматривает использование некоторых важнейших параметров шрифта: размера, или, иначе, кегля (вертикального размера, измеряемого в пунктах; один пункт равняется 0,376 мм), кернинга (избирательного изменения интервала между буквами в зависимости от их формы), апроша (расстояния между соседними буквами или другими шрифтовыми знаками), а также цветовых параметров символов текста.

Предлагаемая модель строится на основе положений, что **M** – это конечное множество сообщений, которые могут быть тайно размещены в документе-контейнере, $\mathbf{M} = \{M_1, M_2, \ldots, M_n\}$; **B** – множество всех допустимых текстовых документов-контейнеров; $\mathbf{B} = \{B_1, B_2, \ldots, B_p\}$, причем $p > n$; **K** – множество всех допустимых ключей, под которыми будем понимать метод (или алгоритм) осаждения стегосообщения в контейнере, $\mathbf{K} = \{K_1, K_2, \ldots, K_z\}$.

Произвольное тайное сообщение M можно скрыть в контейнере B при использовании ключа K: $M \in \mathbf{M}$, $B \in \mathbf{B}$, $K \in \mathbf{K}$. При этом получаем стегосообщение $S \in \mathbf{S} = \{(M_1, B_1, K_1), (M_2, B_2, K_2), \ldots, (M_g, B_g, K_g)\} = \{S_1, S_2, \ldots, S_g\}$.

Функцию F, определенную на $M \times B \times K$ со значениями в S, будем отождествлять с осаждением (или встраиванием) сообщения M в контейнер B на основе использования геометрических и цветовых параметров элементов контейнера B:

$$F: M \times B \times K \rightarrow S,$$

т. е. функция F является отображением $M \times B \times K$ в S.

Имеются в виду такие элементы, информационная составляющая которых может измениться после осаждения определенной части сообще-

ния M. Ключ K является элементом процесса данного типа преобразования, определяющим алгоритм осаждения (например, на основе апроша или иного параметра текста).

Функцию F^{-1}, определенную на $S \times K$ со значениями в M, будем отождествлять с извлечением тайного сообщения M из стегосообщения S:

$$F^{-1}: S \times K \to M.$$

Дополнительным ключом $K_д$ стеганографической системы будем считать конкретное секретное значение набора параметров криптографического алгоритма, используемое для зашифрования ($E_{Kд}$ (M)) и расшифрования ($D_{Kд}(S)$) сообщения (или, например, для помехоустойчивого кодирования-декодирования) об осаждении и извлечении соответственно; $K_д \in \mathbf{K}_д = \{K_{д1}, K_{д2}, \ldots, K_{дг}\}$.

Стеганографической системой будем называть совокупность сообщений, контейнеров, ключей и преобразований, которые их связывают:

$$\sum = (\mathbf{M}, \mathbf{B}, \mathbf{K}, \mathbf{K}_д, \mathbf{S}, F, F^{-1}).$$

Таким образом, последнее выражение формально определяет вид стеганографической системы, которую назовем двухключевой.

Электронный документ-контейнер B будем представлять через дискретную функцию $f(x, y)$, которая определяет координату для каждого пиксела изображения в двухмерном пространстве (или массиве) A, $x = 0, 1, \ldots, w$, $y = 0, 1, \ldots, l$. Пара (x, y) определяет пиксел с координатой по соответствующей оси. Значение функции $f(x, y) \in \{0, 1\}$ – для монохромного, или черно-белого, растрового изображения; $f(x, y) \in \{R, G, B\}$, где R, G, B – 8-битовые бинарные коды, определяющие спектр (цвет) каждого из каналов формирования изображения в так называемой аддитивной цветовой модели. Для формального описания указанной стеганографической системы используем понятие «профиль», которое обозначает проекцию массива A или фрагмента этого массива на одну из осей: x или y [2].

Список литературы

1. Text steganography application for protection and transfer the information / P.P. Urbanovich [et al.] // Przegland Electrotechniczny.– 2010. – № 7. – P. 95–98.

2. Brassil, T.J. Copyright Protection for the Electronic Distribution of Text Documents / T.J. Brassil, S. Low, Ni.F. Maxemchuk // Proc. of the IEEE. – 1999. – Vol. 87, no. 7.– P. 1181–1196.