Секция 5
ЗАЩИТА ИНФОРМАЦИИ И ТЕХНОЛОГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 004.56+003.26

ИСПОЛЬЗОВАНИЕ ХАРАКТЕРИСТИК РАСТРИРОВАНИЯ WEB-ДОКУМЕНТОВ В СТЕГАНОГРАФИЧЕСКОЙ МОДЕЛИ

М. Г. САВЕЛЬЕВА
(Белорусский государственный технологический университет, г. Минск)

Аннотация. *В современном мире с увеличением объемов цифрового контента и ростом онлайн-пиратства защита авторских прав становится все более актуальной. Стеганография предоставляет возможность встраивания информации об авторстве напрямую в контент, обеспечивая эффективную защиту прав интеллектуальной собственности в онлайн-среде, где распространение и использование контента непрерывно возрастает. Данная работа рассматривает применение характеристик растрирования веб-документов как дополнительного параметра скрытой передачи конфиденциальной информации в стеганографической модели. Предлагается вариант модификации общей стеганографической модели с учетом растрирования векторных элементов документов-контейнеров.*

Ключевые слова: *стеганография, растрирование, алгоритм, математическая модель, цвет, пространственная область, авторское право, изображение.*

В настоящее время цифровая эра привносит значительные изменения в обработку и использование данных. Большинство данных теперь принимают форму цифровых файлов, их хранение, передача и использование становятся неотъемлемой частью нашей повседневной жизни. Однако, с этим также возрастает угроза цифрового пиратства – несанкционированного копирования и распространения данных. Это создает риск нарушения конфиденциальности и безопасности информации, а также экономические потери для компаний и частных лиц [1].

Поэтому современные компании и государства должны активно бороться с цифровым пиратством, разрабатывая и внедряя соответствующие меры защиты данных. Такие меры включают в себя использование шифрования, установку антивирусного программного обеспечения, контроль доступа к конфиденциальным данным и технологии защиты прав интеллектуальной собственности.

Для защиты своего интеллектуального труда авторы активно ищут способы предотвращения незаконного использования своих работ. Одним из таких способов является стеганография, наука о скрытом размещении информации, которая в настоящее время приобретает все большую популярность. С ее помощью авторы могут встраивать свои секретные данные в цифровые документы, обеспечивая тем самым доказательства своих прав на интеллектуальную собственность.

Стеганографическая система, которая не требует предварительного обмена некоторой секретной информацией (например, стеганографическим ключом), относится к так называемой «чистой стеганографии» [2]. Формально процесс встраивания (осаждения) тайных сообщений $\boldsymbol{M}$, с помощью которого, в частности, можно решать упомянутую задачу защиты авторского права на контент, содержащийся в документах из множества $\boldsymbol{C}$, можно описать как отображение $\boldsymbol{E}$:

$$\boldsymbol{E} : \boldsymbol{C} \times \boldsymbol{M} \to \boldsymbol{S}, \tag{1}$$

Процесс извлечения $\boldsymbol{M}$ из стеганоконтейнеров $\boldsymbol{S}$ (документов $\boldsymbol{C}$ с размещенной в нем авторской информацией $\boldsymbol{M}$) описывается функцией, обратной к $\boldsymbol{E}$:

$$\boldsymbol{D} = \boldsymbol{E}^{-1} : \boldsymbol{S} \to \boldsymbol{M}, \mathbf{C}. \tag{2}$$

Стеганографическая система на основе секретного ключа похожа на симметричную криптосистему: отправитель выбирает контейнер C ($C \in \boldsymbol{C}$, $\boldsymbol{C} = \{C_1, C_2, \ldots, C_r\}$) и внедряет секретное сообщение M ($M \in \boldsymbol{M}$, $\boldsymbol{M} = \{M_1, M_2, \ldots, M_n\}$, $r > n$) в C с помощью секретного ключа K ($K \in \boldsymbol{K}$, $\boldsymbol{K} = \{K_1, K_2, \ldots, K_a\}$). Результатом такого преобразования будет стегоконтейнер S, $S \in \boldsymbol{S}$, $\boldsymbol{S} \in \{S_1, S_{2,} \ldots, S_t\}$. Массив из шести множеств:

$$\boldsymbol{\xi} = < \boldsymbol{C}, \boldsymbol{M}, \boldsymbol{K}, \boldsymbol{S}, \boldsymbol{D_K}, \boldsymbol{E_K} >, \tag{3}$$

где

$$\boldsymbol{E_K} : \boldsymbol{C} \times \boldsymbol{M} \times \boldsymbol{K} \to \boldsymbol{S}, \tag{4}$$

$$\boldsymbol{D_K} : \boldsymbol{C} \times \boldsymbol{K} \to \boldsymbol{M} \tag{5}$$

описывает стеганосистему с одним или несколькими стеганографическими ключами [3].

Формулы (4) и (5) справедливы только со свойством [4]:

$$\boldsymbol{D_K}\left(\boldsymbol{E_K}\left(C, M, K\right), K\right) = M; \quad \left(\boldsymbol{D_K}\right)^{-1} = \boldsymbol{E_K}. \tag{6}$$

На рисунке 1 приведена общая структурированная схема стеганографической системы.

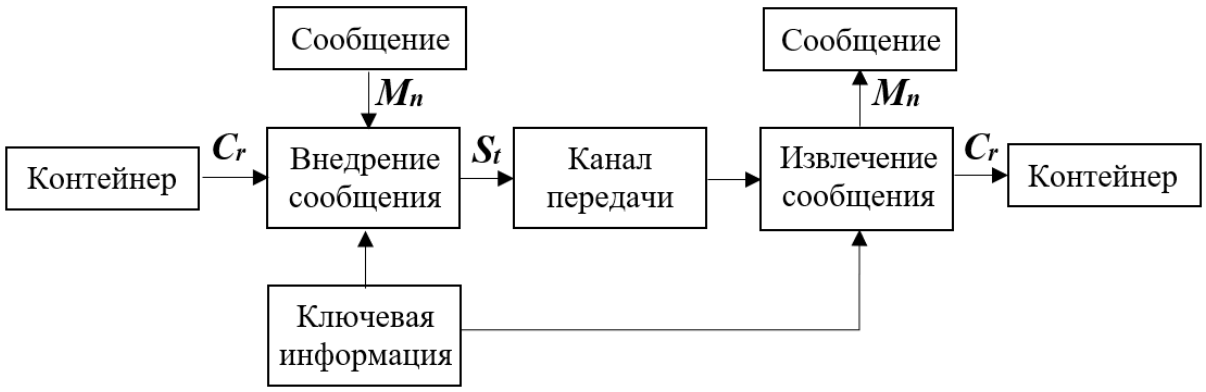

Рисунок 1. – Общая схема стеганографической системы

Электронные текстовые документы подвергаются различным конвертациям и модификациям. В результате такие документы могут рассматриваться как изображения и, соответственно, могут быть частью растровой или векторной графики. В это случае возникает проблема растрирования текста, когда контуры букв становятся размытыми, а цвет по контуру переходит в градиент. Тем не менее, этот факт можно использовать для скрытого внедрения тайной информации, такой как цифровой водяной знак (ЦВЗ), в защищаемое содержимое. Для увеличения пропускной способности такого скрытого канала можно использовать преобладающие оттенки среди переходных оттенков растрированных символов.

Ввиду того, что электронные изображения-контейнеры могут принадлежать растровому типу графики и состоять из пикселей, необходимо учитывать с какими конкретно пикселями будет происходить стеганографическое преобразование или алгоритм их выбора из всего массива пикселей. Так как это может быть реализовано различными методами, использующими различные алгоритмы выбора пикселей для внедрения, необходимо учитывать это при описании модели. Пусть $\boldsymbol{F_E}$ – набор функций, реализующих выбор пикселей для стеганографического преобразования из контейнера $\boldsymbol{C}$ при использовании ключевой информации:

$$\boldsymbol{F_E} : \boldsymbol{C} \times \boldsymbol{K} \to \boldsymbol{Z}, \tag{7}$$

где $\boldsymbol{Z}$ – множество пикселей, используемых непосредственно для стеганографическиого преобразования, $\boldsymbol{Z} = \{Z_1, Z_2, \ldots, Z_q\}$, причем $q \geq n$.

Следовательно, стеганографическая система будет иметь следующий вид:

$$\boldsymbol{\xi} = < \boldsymbol{C}, \boldsymbol{M}, \boldsymbol{K}, \boldsymbol{S}, \boldsymbol{D_K}, \boldsymbol{E_K}, \boldsymbol{F_E} >, \tag{8}$$

при условии использовании одного алгоритма выбора пикселей для внедрения и извлечения, при различных $\boldsymbol{F_D}$ – набор функций, реализующих выбор пикселей

для извлечения секретной информации из контейнера $\boldsymbol{C}$ при использовании ключевой информации:

$$\boldsymbol{F_D} = \boldsymbol{F_E}^{-1} : \boldsymbol{C} \times \boldsymbol{K} \to \boldsymbol{Z}, \tag{9}$$

$$\boldsymbol{\xi} = < \boldsymbol{C}, \boldsymbol{M}, \boldsymbol{K}, \boldsymbol{S}, \boldsymbol{D_K}, \boldsymbol{E_K}, \boldsymbol{F_E}, \boldsymbol{F_D} > . \tag{10}$$

Таким образом, основным отличием описанной математической модели стеганографической системы от известных моделей является использование растрирования текста для скрытой передачи информации. Это позволит в полной мере использовать растрирование векторных символов для увеличения пропускной способности методов внедрения тайной информации.

ЛИТЕРАТУРА

1. Урбанович П. П. Защита информации методами криптографии, стеганографии и обфускации / П. П. Урбанович. – Минск: БГТУ, 2016. – 220 с.
2. Information Hiding Techniques for Steganography and Digital Watermarking / Ed. Stefan Katzenbeisser, Fabien A. P. Petitcolas. – London: Artech House, Inc., 2000. – P. 20–22.
3. Urbanovich, P. Theoretical Model of a Multi-Key Steganography System / P. Urbanovich, N. Shutko // Recent Developments in Mathematics and Informatics. Contemporary Mathematics and Computer Science. – Vol. 2. Chapter 11. – Lublin: KUL, 2016. – P. 181–202.
4. Шутько, Н. П. Защита авторских прав на текстовые документы на основе стеганографической модификации цвета символов текста / Н. П. Шутько, П. П. Урбанович // Информационные технологии: материалы 83-й научно-технической конференции профессорско-преподавательского состава, научных сотрудников и аспирантов (с международным участием), Минск, 4–15 февраля 2019 г. – Минск: БГТУ, 2019. – С. 41–43.