ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 23 МАТЕМАТИКИ Выпуск 3
2016

В. А. Федосеев (Самара, Самарский университет, ИСОИ РАН)**. Комплексный анализ систем встраивания информации в цифровые сигналы на основе их формальной модели.**

Системами встраивания информации в цифровые сигналы (СВИ) будем называть стеганографические системы и системы встраивания цифровых водяных знаков (ЦВЗ-системы) в совокупности. Эти два вида систем, хоть и используются для решения разных задач защиты информации, тесно связаны алгоритмически и имеют много общего во внутренних процессах.

Комплексный анализ конкретной СВИ заключается в детальном описании ее структурных элементов, определении присущих ей внешних свойств, изучении вопроса ее применимости для решения конкретных практических задач, а также исследовании стойкости к преднамеренным атакам и непреднамеренным искажениям различного характера.

Все вышеперечисленное должно базироваться на единой формальной модели СВИ, однако таковой до настоящего времени не было предложено, несмотря на то, что известны модели, в той или иной степени описывающие по отдельности стеганографические или ЦВЗ-системы. Так, наиболее проработанная модель ЦВЗ-систем предложена в работе [1] и представляет собой кортеж из 6 элементов. В работе [2] автором предложена унифицированная модель СВИ, обладающая куда большей сложностью.

Данная модель основана на понятии *внутренней информации* (т. е. встраиваемой внутри информационного объекта — контейнера) и трех эквивалентных форм ее представления, используемых на различных этапах функционирования СВИ: двоичная строка длины N_b, а также многомерные матрицы цифрового сигнала $\mathbb{X}_{[]}^{m}$ и признаков $\mathbb{Y}_{[]}^{l}$. Различные формы внутренней информации связаны друг с другом рядом функций (см. рис.). Помимо них, модель дополняется функциями анализа сигнала $\mathcal{A}$, встраивания информации $\mathcal{E}$, извлечения информации $\mathcal{D}$, обнаружения информации $\mathcal{R}$. Важнейшую роль играет составной ключ $k \in K$, являющийся конкатенацией секретного ключа и открытых параметров используемых алгоритмов.

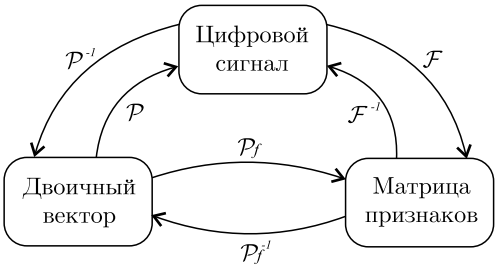

Рис. Связь различных форм представления внутренней информации

При использовании данной модели становится возможным структурный анализ конкретной СВИ и сравнение ее с другими системами. Помимо этого, модель позволяет

четко определить ряд терминов, традиционно используемых для внешнего описания СВИ: детектор, декодер, слепое/неслепое извлечение; слепое, множественное, реверсивное встраивание и др.

Основным индикатором практической применимости СВИ в практических задачах является ее стойкость к конкретным атакам и искажениям. Модель делает возможным введение всех известных видов атак: обнаружения, извлечения, удаления, подмены встроенной информации, отыскания ключа, подделки носителя информации и пр. Далее для каждого вида атак вводится понятие успешности ее применения. На основе полученных определений и формальной модели СВИ становится возможным сформулировать и доказать ряд утверждений, характеризующих достаточные условия успешного применения конкретных атак.

Работа выполнена при поддержке Минобрнауки России в рамках гранта президента РФ МК-4506.2015.9 и государственного задания вузу № 2014/198 (код проекта 2298).

СПИСОК ЛИТЕРАТУРЫ

1. *Nyeem H.*, *Boles W.*, *Boyd C.* Digital image watermarking: its formal model, fundamental properties and possible attacks. — EURASIP J. Advances Signal Process., 2014, v. 2004(1), p. 1–22.
2. *Федосеев В. А.* Унифицированная модель систем встраивания информации в цифровые сигналы. — Компьютерная оптика, 2016, т. 40, № 1, с. 87–98.