

ОЦЕНКА СТЕГАНОГРАФИЧЕСКИХ КОНТЕЙНЕРОВ НА ОСНОВЕ МАРКОВСКИХ МОДЕЛЕЙ

А.С. ПРОЦКЕВИЧ, Ю.С. ХАРИН

Белорусский государственный университет

Введение

Стеганография скрывает сам факт передачи информации. В настоящее время эта научная область стремительно развивается. Основным свойством, которое характеризует качество стегосистемы, является необнаруживаемость, т.е. невозможность доказательства существования скрытой информации. Свойство необнаруживаемости связано с понятием «качества» контейнера, т.е. оценкой его пригодности для встраивания сообщения. В качестве модели сообщения обычно используется равномерно распределенная случайная последовательность (сжатое зашифрованное сообщение). Одной из оценок «качества» контейнера является стеганографическая ёмкость. Стеганографическая ёмкость — это максимальное число бит, которые могут быть встроены без появления статистически обнаруживаемых модификаций [1]. Актуальными являются задачи оценки свойств контейнера, определения областей контейнера, безопасных для встраивания, а также построения математических моделей, на основании которых производится оценка стеганографической ёмкости контейнера.

В данной работе для решения указанных задач в случае LSB-встраивания сообщения в контейнер применяются математические модели цепи Маркова порядка n Марковского случайного поля, строятся статистические оценки стеганографической ёмкости контейнера, определяются фрагменты контейнера, пригодные для встраивания.

Исследование свойств контейнера на основе двоичных цепей Маркова заданного порядка

Пусть наблюдается контейнер, представляющий собой последовательность n двоичных N -векторов:

$$X_1 = (x_{11}, \dots, x_{1N})^T, \dots, X_n = (x_{n1}, \dots, x_{nN})^T \in V_N = \{0, 1\}^N.$$

Пусть $1 \leq N_0 \leq N$ — число «наименее значимых бит». В методе LSB-встраивания сообщения в контейнер используется последовательность двоичных N_0 — векторов:

$$x_1 = (x_{11}, \dots, x_{1N_0})^T, \dots, x_n = (x_{n1}, \dots, x_{nN_0})^T \in V_{N_0}.$$

Для простоты обозначений в данной работе рассмотрим случай $N_0 = 1$; результаты получены и для $N_0 > 1$. Таким образом, исходные данные представляют собой дискретный временной ряд с пространством состояний $V = \{0, 1\}$:

$$y_t = x_{t1}, t = 1, \dots, n.$$

Зададим число m для $(2m+1)$ -окна скользящего просмотра данных. Если предположить, что y_t есть ОЦМ некоторого заданного порядка с матрицей вероятностей одношаговых переходов [2]

$$P = (p_{i_1, \dots, i_s, j}), p_{i_1, \dots, i_{s+1}} = P(y_t = j | y_{t-1} = i_1, \dots, y_{t-s} = i_s),$$

то находим частоты

$$v_{i_1, \dots, i_s, j} = \sum_{i=t-m+s}^{t+m} I\{y_{t+1} = j, y_t = i_1, \dots, y_{t-s+1} = i_s\}, (i_1, \dots, i_s, j = 0, 1),$$

$$v_{i_1, \dots, i_s} = \sum_{j=0}^1 v_{i_1, \dots, i_s, j},$$

где $I\{\bullet\}$ — индикатор события, указанного в скобках. Используя критерий согласия Пирсона параметрами $(2^s, \alpha)$, где 2^s — число степеней свободы, α — уровень значимости, построим статистический тест проверки гипотезы о виде матрицы вероятностей одношаговых переходов, означающую «чистую случайность» $\{y_t\}$:

$$H_0 = \{p_{i_1, \dots, i_s, j} = 0.5, i_1, \dots, i_s, j = 0, 1\}, H_1 = \overline{H_0}.$$

Этот критерий имеет вид [3]:

$$H_0 \text{ отвергается} \leftrightarrow \{\chi_n^2 > \chi_{1-\alpha, 2^s}^2\},$$

где

$$\chi_n^2 = \sum_{i_1, \dots, i_s, j \in \{0, 1\}} \frac{\left(v_{i_1, \dots, i_s, j} - \frac{1}{2} v_{i_1, \dots, i_s}\right)^2}{\frac{1}{2} v_{i_1, \dots, i_s}},$$

$\chi_{1-\alpha, 2^s}^2$ — квантиль уровня $1 - \alpha$ стандартного хи-квадрат распределения с 2^s степенями свободы.

В случае принятия гипотезы H_0 область контейнера, которая находится в окне скользящего просмотра данных $\{t - m, t - m + 1, \dots, t + m\}$, считается «неопасной» и пригодной для встраивания сообщения.

Исследование свойств контейнера на основе марковских случайных полей

Пусть теперь контейнер представляет собой изображение в градациях серого, представляющее собой $(n_1 \times n_2)$ матрицу $A = (a_{ij})$, $a_{ij} \in V_{256}$. Рассмотрим LSB-матрицу изображения $X = (x_{ij})$, состоящую из наименее значимых бит каждого пикселя, и выберем *шаблон соседства* для элемента x_{ij} этой матрицы следующим образом: $\{x_{i-1, j}, x_{i, j-1}\}$.

Предполагается, что:

$$\mathbb{P}\{x_{ij} | \{x_{kl} : k \leq i, l \leq j\}\} = \mathbb{P}\{x_{ij} | x_{i, j-1}, x_{i-1, j}\},$$

и что X — марковское случайное поле с вероятностями одношаговых переходов:

$$p_{i_1, i_2, i_3} = \{x_{ij} = i_3 | x_{i, j-1} = i_1, x_{i-1, j} = i_2\}, (i_1, i_2, i_3 = 0, 1).$$

Определим гипотезы:

$$H_0 = \left\{ \mathbb{P}(x_{ij} | x_{i,j-1}, x_{i-1,j}) \equiv \frac{1}{2}, i = 2, \dots, n_1, j = 2, \dots, n_2 \right\}; H_1 = \overline{H_0}.$$

Зададим $m_1 \times m_2$ окно просмотра данных и найдём частоты:

$$v_{i_1, i_2, i_3} = \sum_{j=2}^{m_2} I \{ x_{ij} = i_3, x_{i,j-1} = i_1, x_{i-1,j} = i_2 \}, (i_1, i_2, i_3 = 0, 1),$$

$$v_{i_1, i_2} = \sum_{j=2}^{m_2} I \{ x_{i,j-1} = i_1, x_{i-1,j} = i_2 \}, (i_1, i_2 = 0, 1).$$

Для проверки H_0, H_1 используем критерий согласия Пирсона:

$$H_0 \text{ отвергается} \leftrightarrow \{ \chi_n^2 > \chi_{1-\alpha, 4}^2 \},$$

где

$$\chi_n^2 = \sum_{i_1, i_2, i_3 \in \{0, 1\}} \frac{\left(v_{i_1, i_2, i_3} - \frac{1}{2} v_{i_1, i_2} \right)^2}{\frac{1}{2} v_{i_1, i_2}},$$

$\chi_{1-\alpha, 4}^2$ – квантиль уровня $1-\alpha$ стандартного хи-квадрат распределения с 4 степенями свободы.

Если принимается гипотеза H_0 , то фрагмент контейнера $\{t, \dots, t+m_2\}$ с индексом j считается «безопасным» и пригодным для встраивания.

Численные результаты экспериментов

Произведены оценки свойств пяти контейнеров, представляющих собой bmp-изображения размером 512×512 в градациях серого. Получены оценки их относительной стеганографической ёмкости в зависимости от выбранной модели наблюдения, произведена визуализация пригодных и непригодных для встраивания областей контейнера. Относительной стеганографической ёмкостью назовём отношение числа бит, пригодных для встраивания, к числу бит в LSB-матрице изображения. В моделях на основе цепи Маркова заданного порядка, изображение преобразуется в двоичную последовательность построчной развёрткой.

Типы используемых в экспериментах моделей.

1. Модель наблюдения: двоичная цепь Маркова 0-го порядка (т.е. схема независимых испытаний), размер скользящего окна просмотра данных $2m+1=33$ бита.
2. Модель наблюдения: двоичная цепь Маркова 1-го порядка, размер скользящего окна просмотра данных $2m+1=33$ бита.
3. Модель наблюдения: двоичная цепь Маркова 2-го порядка, размер скользящего окна просмотра данных $2m+1=33$ бита.
4. Модель наблюдения: марковское случайное поле с заданным шаблоном, размер окна просмотра данных 2×32 бита ($n_1=2, n_2=32$).

В таблице 1 представлены оценки относительной стеганографической ёмкости в процентах для пяти контейнеров при использовании четырёх указанных выше моделей LSB-контейнеров.



Рис. 1. Контейнеры 1–5

Таблица 1

Оценка относительной стеганографической ёмкости контейнера
в зависимости от параметров испытания

Контейнер	Модель 1	Модель 2	Модель 3	Модель 4
1	84,03	60,77	22,00	20,46
2	76,65	55,25	20,98	16,61
3	74,44	54,62	20,44	17,03
4	83,73	59,82	22,45	23,11
5	71,57	52,37	19,73	19,07

ЛИТЕРАТУРА

1. *Fridrich, J.* Steganography in digital media / J. Fridrich //Cambridge University Press, Cambridge, 2010.
2. Криптология / Ю. С. Харин [и др.]. — Минск: БГУ, 2013.
3. *Медведев, Ивченко.* Введение в математическую статистику. Москва, 2010.

КОНТРОЛЬ ЦЕЛОСТНОСТИ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ И ЕЁ КОНФИГУРАЦИИ

Н. В. МОЗОЛИНА

МФТИ

В тезисах предлагается определение предмета контроля целостности виртуальной инфраструктуры и её конфигурации и способ контроля с помощью представления конфигурации виртуальной инфраструктуры графом специального вида.

Ключевые слова: контроль целостности, виртуальная инфраструктура, конфигурация виртуальной инфраструктуры.

Для защиты среды виртуализации требуется выполнение множества мер [1], в том числе должен выполняться контроль целостности виртуальной инфраструктуры и ее конфигураций. Для обеспечения контроля в первую очередь следует определить, что является предметом контроля и каким способом можно его осуществить.