МЕТОДЫ СТАТИСТИЧЕСКОЙ КЛАССИФИКАЦИИ В ЗАДАЧЕ ОБНАРУЖЕНИЯ ВСТРАИВАНИЯ ИНФОРМАЦИИ

А. М. Капуста

ВВЕДЕНИЕ

Большинство современных стеганографических методов осуществляет встраивание информации в область дискретного косинусного преобразования (ДКП) изображений в формате JPEG, изменяя при этом наименее значимые биты ДКП-коэффициентов [1]. При этом часто выполняется коррекция ДКП-коэффициентов после встраивания информации, чтобы сохранить основные статистические свойства контейнера и затруднить работу стегоаналитика.

Методы стеганоанализа делят на 2 группы: стеганоанализ для конкр-теных алгоритмов встраивания и универсальный стеганоанализ [1; 2]. На практике больше востребованы универсальные методы в силу их гибко-сти и способности быстро приспосабливаться к новым или полностью неизвестным стеганографическим методам [1].

Задача универсального стеганоанализа может быть рассмотрена, как задача распознавания образов с использованием статистических методов классификации с обучением. Наиболее часто применяемыми методами классификации при наличии обучающих выборок являются дискриминантный анализ и метод опорных векторов (SVM) [3; 4].

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ НА ОСНОВЕ ДИСКРИМИНАНТНОГО АНАЛИЗА

Пусть контейнер описывается вектором $x \in R^p$, где p – число признаков классификации. Пусть W_1 – выборка, состоящая из пустых контейнеров (класс Ω_1) с p-мерным гауссовским распределением $N(\mu_1, \Sigma_1)$, W_2 – выборка, состоящая из модифицированных контей-

неров (класс Ω_2) с p-мерным гауссовским распределением $N(\mu_2, \Sigma_2)$, $\mu_1, \mu_2 \in R^p$, $\Sigma_1, \Sigma_2 \in R^{p \times p}$. $W = W_1 \cup W_2$ – обучающая выборка.

В квадратичном дискриминантном анализе для классифицируемого контейнера $x \in R^p$ и для каждого класса Ω_1 и Ω_2 вычисляется дискриминантная функция:

$$d_i = \ln|\Sigma_i| + (x - \mu_i)^T \Sigma_i^{-1} (x - \mu_i), \quad i = 1, 2. \tag{1}$$

Решающее правило состоит в следующем: наблюдение $x \in R^p$ относится к классу Ω_1, если выполняется условие $d_1 < d_2$, иначе наблюдение относится к классу Ω_2.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ НА ОСНОВЕ МЕТОДА ОПОРНЫХ ВЕКТОРОВ

Пусть контейнер описывается вектором $x_i \in R^p$, $1 \le i \le l$, где p – число признаков классификации. Пусть $X = \{x_1, ..., x_l\}$ – обучающая выборка из l контейнеров. Константа $y_i \in \{-1, 1\}$ обозначает класс, к которому принадлежит контейнер x_i. Если $y_i = 1$, то контейнер x_i принадлежит классу Ω_1 пустых контейнеров; если $y_i = -1$, то контейнер x_i принадлежит классу Ω_2 модифицированных контейнеров.

В итоге для обучения используется следующее множество:

$$D = \{(x_1, y_1), ..., (x_l, y_l)\}, \quad x_i \in R^p, \quad y_i \in \{-1, 1\}. \tag{2}$$

Множество (2) является линейно разделимым, если существует вектор w размерности p и скаляр b такие, что для всех элементов множества (2) выполняются следующие неравенства:

$$y_i (w \cdot x_i + b) \ge 1, \quad i = 1, ..., l. \tag{3}$$

Оптимальная разделяющая гиперплоскость $w_0 \cdot x + b_0 = 0$ разделяет обучающую выборку без ошибок и обеспечивает максимальное расстояние между классами. Решающее правило относит наблюдение $x \in R^p$ к классу Ω_1, если $sign(w_0 x + b_0) = 1$, иначе – к классу Ω_2.

Лучшего разделения классов можно добиться при замене скалярного произведения на нелинейную функцию ядра, что эквивалентно поиску оптимальной разделяющей гиперплоскости в пространстве более высокой размерности [4].

ПРИЗНАКИ КЛАССИФИКАЦИИ

Разобьем матрицу ДКП-коэффициентов графического изображения на n_B блоков размером 8×8. Обозначим ДКП-коэффициенты $d_{ij}(k)$, где $k = 1,...,n_B$ определяет номер блока, а $i, j = 1,...,8$ – позицию коэффициента внутри блока.

Глобальная гистограмма $H = (H_L,...,H_R)$, где $L = \min_{i,j,k} d_{ij}(k)$, $R = \max_{i,j,k} d_{ij}(k)$, описывает распределение частот ДКП-коэффициентов по всему изображению. Частные гистограммы h^{ij}, описывают распределение частот ДКП-коэффициентов на заданной позиции внутри блока 8×8.

Для описания межблоковых зависимостей используются следующие показатели [2]:

- вариация ДКП-коэффициентов в соседних блоках;
- меры блочности, описывающие неоднородности на границах;
- матрицы смежности, описывающие распределение частот пар значений соседних ДКП-коэффициентов.

Для описания марковских зависимостей коэффициентов используется следующий набор признаков [5]:

$$M(i,j) = \frac{M_h(i,j) + M_v(i,j) + M_d(i,j) + M_m(i,j)}{4}, \qquad (11)$$

где M_h, M_h, M_h, M_h – матрицы вероятностей переходов по горизонтали, вертикали, диагонали и обратной диагонали соответственно.

РЕЗУЛЬТАТЫ ЭКСПЕРИМЕНТОВ

Анализ эффективности рассмотренных методов стеганоанализа, основанных на моделях дискриминантного анализа и метода опорных векторов проводился на стеганоалгоритме F5, который позволяет встраивать информацию в графические изображения формата JPEG [6].

Обучающая выборка состояла из 2500 пустых контейнеров (фото в формате JPEG) и 2500 модифицированных контейнеров со встроенной с помощью стеганоалгоритма F5 информацией. Экзаменационная выборка состояла из 1250 пустых и 1250 модифицированных контейнеров.

Эффективность построенных решающих правил дискриминантного анализа и метода опорных векторов определялась двумя способами: путем переклассификации обучающей выборки (результаты представлены

в табл. 1) и классификации экзаменационной выборки (результаты представлены в табл. 2) [3].

Таблица 1

Точность классификации обучающей выборки

	Квадратичный дискр. анализ	Ядро SVM		
Контейнеры		Линейное	Полиномиал.	Радиальное
Пустые	0,926	0,988	0,993	0,999
Модифицированные	0,963	0,985	0,992	0,999

Таблица 2

Точность классификации экзаменационной выборки

	Квадратичный дискр. анализ	Ядро SVM		
Контейнеры		Линейное	Полиномиал.	Радиальное
Пустые	0,92	0,92	0,98	0,99
Модифицированные	0,93	0,93	0,97	0,99

ЗАКЛЮЧЕНИЕ

Методы дискриминантного анализа и опорных векторов позволили получить высокую точность классификации. Как следует из результатов, приведенных в таблицах 1-2, более точные результаты стеганоанализа были получены при использовании нелинейного метода опорных векторов с радиальным ядром как для обучающей, так и для экзаменационной выборок. Метод опорных векторов является более эффективным методом классификации в задаче обнаружения встраивания информации в графические изображения, чем линейный дискриминантный анализ.

Литература

1. *Fridrich J., Goljan M.* Practical steganalysis of digital images state of the art. – Proc. SPIE Security and Watermarking of Multimedia Contents IV. 2002, v. 4675. P. 1-13.
2. *Fridrich J., Kodovsky J.* Influence of embedding strategies on security of steganographic methods in the JPEG domain. – Proc. SPIE Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents, 2008.
3. *Duda R.O., Hart P.E., Stork H.G.* Pattern Classification. – 2nd ed. New York: Wiley-Interscience , 2000.
4. *Vapnik V.* The Nature of Statistical Learning Theory. – New York: Springer, 1995.
5. *Shi Y., Chen C., Chen W. A* Markov process based approach to effective attacking JPEG steganography. // Lecture Notes in Computer Science, 2007, v. 4437. P. 249-264.
6. *Westfeld A.* High capacity despite better steganalysis (F5 – a steganographic algorithm). // Lecture Notes in Computer Science, 2002. V. 2137. P. 289-302.