УДК 004.056.5

Гніліцький В.В., к.т.н., доц.
Драч Я.Д., магістр
Житомирський державний технологічний університет

СТАТИСТИЧНІ І НЕЙРОМЕРЕЖЕВІ АЛГОРИТМИ СИНТЕЗУ ТА АНАЛІЗУ СТЕГАНОГРАФІЧНО ПРИХОВАНОЇ ІНФОРМАЦІЇ В АУДІО- ТА ГРАФІЧНИХ ДАНИХ

Звдання стегоаналізу (СА) – виявлення прихованих стеганографічним способом даних, їх вилучення та знешкодження, а також аналіз стійкості існуючих стегоалгоритмів, і розробка нових методів виявлення прихованої інформації. Для ідентифікації та кластеризації, успішно застосовуються штучні нейронні мережі. Нейромережевий підхід відрізняють принципова можливість нелінійної класифікації і можливість побудови процедур класифікації, здатних додатково навчатися, що особливо важливо при використанні стегоаналітичних методів в складі систем, що працюють в реальному масштабі часу. Зазначені перетворення, що описують вбудовування вектора повідомленн $d \in R^m$ в вектор-контейнер $z \in R^n$, $m << n$, і подальше його відновлення мають вигляд: $\tilde{z} = F_1(z,d), \tilde{z} \in \tilde{Z}, \|\tilde{z} - z\| \to \min, \tilde{d} = F_2(\tilde{z}), \tilde{d} \in D, \left\|d - \tilde{d}\right\| \to \min$. (1) Для вбудовування послідовності застосована двошарова лінійна мережа автоасоціативного типу із зменшеним по відношенню до входу і виходу числом нейронів у прихованому шарі $q = n$, що збігається з розмірністю вектора-контейнера (рис. 1, а). Для відновлення інформації доцільно застосовувати лінійну або нелінійну нейронну мережу (НМ) прямого поширення, що реалізує двохальтернативне вирішальне правило при вилученні (відновленні) раніше вбудованої послідовності даних (рис. 1, б).

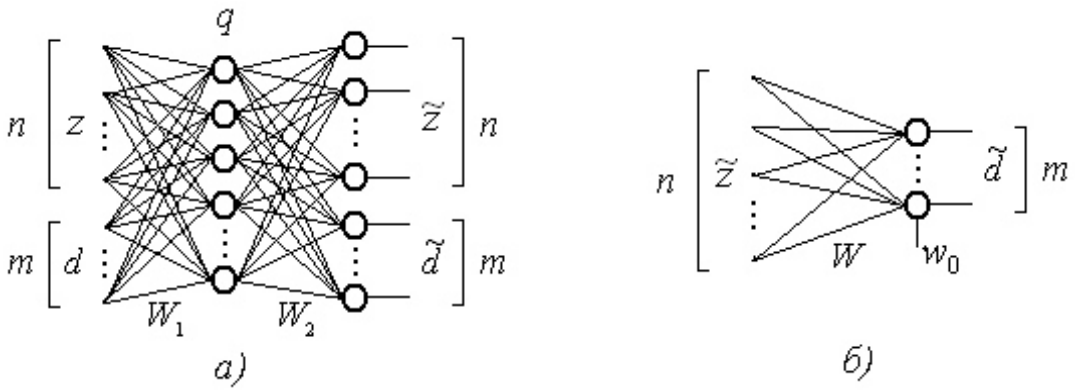

Рис. 1

Сигнал, що подається на входи НМ, яка реалізує стеганографічне приховування інформації (СПІ), може бути представлений як складений вектор $y = (z^T, d^T)^T$ або $y = y_1 + y_2$, де $y_1 = (z_1, z_2, ..., z_n, 0, ..., 0)$, $y_2 = (0, ..., 0, d_1, ..., d_m)^T$, где $d = (d_1, ..., d_m)^T$ – вектор, що містить елемент вбудовуваних даних. При приховуванні цілісного повідомлення, що утворює приховувану послідовність даних $d^{(p)}$, $p = \overline{1,P}$, для кожного її елемента використовується фрагмент контейнера, що описується вектором $z^{(p)}$, $p = \overline{1,P}$. На виході відповідним чином навченої мережі виходить послідовність заповнених фрагментів контейнера $\tilde{z}^{(p)}$, $p = \overline{1,P}$. При навчанні зазначених НМ здійснюється мінімізація середньої квадратичної помилки методом зворотного поширення. Для аналізу закономірностей процесу СПІ в рамках запропонованого підходу була розглянута статистична модель, за якою кожен фрагмент контейнера розглядається як реалізація випадкового вектора z з параметрами $M[z] = 0, M[zz^T] = R_z$. Елементи вбудовуваної послідовності є реалізаціями двійкової випадкової величини d, що не залежить від z і приймає свої значення з однаковими апріорними ймовірностями $P(d = 1) = 0{,}5$ и $P(d = -1) = 0{,}5$, $M[d] = 0$, $M[d^2] = \sigma_d^2 = 1$. Для вбудовування такої послідовності даних доцільно використовувати НМ із зменшеним на одиницю в порівнянні з розмірністю вхідного і вихідного вектора числом нейронів у прихованому шарі (рис. 1, а). Навчання мережі проводиться за сукупністю реалізацій вхідного вектора

$y^{(p)} = \left(z^{(p),T}, d^{(p)}\right)^T$, $p = \overline{1,P}$ так, щоб мінімізувати величину $E = \frac{1}{2}\sum_{p=1}^{P}\left(y^{(p)} - W_2W_1y^{(p)}\right)^T\left(y^{(p)} - W_2W_1y^{(p)}\right)$ (2).

При навчанні і роботі подібної мережі здійснюється стискання вхідних даних з відповідним незначним спотворенням вектора-контейнера і можливим вбудовуванням вектора d в структуру вектора $\tilde{z}$, який є складовою частиною вектора на виході НМ. Для оцінки можливості відновлення даних у процесі СПІ, в роботі пропонується методика аналізу статистичних характеристик вектора $\tilde{z}$ на виході НМ, що реалізує вбудовування інформації. На вхід мережі (рис. 1,а) подаються тестові сигнали $y^+ = (0,0,...,0,1)^T$, $y^- = (0,0,...,0,-1)^T$. На виході отримуються вектори $\tilde{y}^+ = \left(m^+, \tilde{d}\right)^+ = W_2W_1y^+$ і $\tilde{y}^- = \left(m^-, \tilde{d}\right)^+ = W_2W_1y^-$. Компоненти m^+ і m^- розглядаються як математичні очікування корисного сигналу, що відповідають двом різним гіпотезам при вбудовуванні даних в контейнер $\tilde{z}$. Оцінюється матриця коваріації виходу мережі в перших n компонентах, тобто компонентах вектора $\tilde{z}$, при подачі випадкового вектора $y_1 = (z_1, z_2,..., z_n, 0)^T$. Для цього обчислюється матриця $R_{\tilde{y}}^0 = W_1W_2R_y^0W_1^TW_2^T$, і виділяється матриця $R_{\tilde{z}}$, що є блочною в матриці $R_{\tilde{y}}^0$. В результаті сигнал на виході НМ представляється у вигляді $\tilde{z} = W_2^yW_1(y_1 + y_2)$, $\tilde{z} = am^+ + (1-a)m^- + \eta$, $W_2^y = \left\|w_{ij}^{(2)}\right\|$, (3), де $w_{ij}^{(2)}$, $i = \overline{1,n}$, $j = \overline{1,n}$ – елементи матриці W_2, $i = \overline{1,n+1}$, $j = \overline{1,n}$; де $a = 1$, якщо $d = 1$, $a = 0$, якщо $d = -1$; η – вектор флуктуації (перешкоди), в якості якого в даному випадку виступає одержуваний на виході автоасоціативної НМ контейнер з відомою матрицею коваріації. $R_\eta = R_{\tilde{z}}$. Таким чином, для ефективного відновлення прихованих даних необхідно вирішити задачу класифікації спостережуваного вектора $\tilde{z}$ по його приналежності до одного із класів H_1 і H_2, що характеризуються різними математичними очікуваннями m^+ і m^-, в присутності шуму η з відомою матрицею коваріації R_η. Для цього використовується друга НМ, архітектура якої приведена на рис. 1,б. В разі гаусового розподілу вектора шуму η при її навчанні за достатньою кількістю прикладів вона реалізує оптимальне за критерієм максимуму правдоподібності вирішальне правило: $\ln(\tilde{z}) = \tilde{z}^TR_\eta^{-1}\left(m^+ - m^-\right) - 0{,}5\left(m^+ + m^-\right)^TR_\eta^{-1}\left(m^+ - m^-\right) \underset{<}{>} 0$ (4). При цьому ймовірність сумарної помилки в ході відновлення раніше вбудованої двійкової послідовності визначається співвідношенням:

$$P_{ОВ} = \frac{1}{2}P_{12} + \frac{1}{2}P_{21},\ P_{12} = 1 - \Phi(\alpha),\ \alpha = 0{,}5\sqrt{\left(m^+ - m^-\right)^TR_\eta^{-1}\left(m^+ - m^-\right)} \quad (5)$$

де $\Phi(\alpha)$ – інтеграл імовірностей.

Розроблено та досліджено нейромережеві функціональні моделі (НФМ) перетворення інформації для вирішення завдань стеганографічного вбудовування, а також методику для оцінки потенційних можливостей відновлення раніше прихованих даних. Запропоновано та метод СПІ на основі НФМ перетворення даних. Обрано НМ для вбудовування і відновлення раніше прихованої інформації. Запропонована статистична модель стеганографічного вбудовування бітових послідовностей в контейнери. Дані загальні рекомендації та описані підходи до вибору стеганографічних контейнерів для підвищення ефективності функціональної моделі СПІ. Обгрунтувано і доведено збіжності вагових коефіцієнтів нейронних мереж лінійного типу при відновленні регресивних і авторегресивних моделей випадкових процесів і полів за експериментальними даними в умовах прямого і непрямого навчання.

ГНІЛІЦЬКИЙ Віталій Васильович, к.т.н., доц., викладач кафедри автоматики та управління в технічних системах факультету інформаційно-комп'ютерних технологій Житомирського державного технологічного університету (ЖДТУ). Наукові інтереси: цифрова обробка сигналів, інформаційні системи, E-mail: gnil@ztu.edu.ua, тел: (0412) 37-84-82

ДРАЧ Ярослав Дмитрович, магістр групи СІ-64м кафедри автоматики та управління в технічних системах факультету інформаційно-комп'ютерних технологій ЖДТУ. Наукові інтереси: методи та алгоритми стеганографічного приховування інформації, стеганографічний аналіз даних, нейромережеві технології.