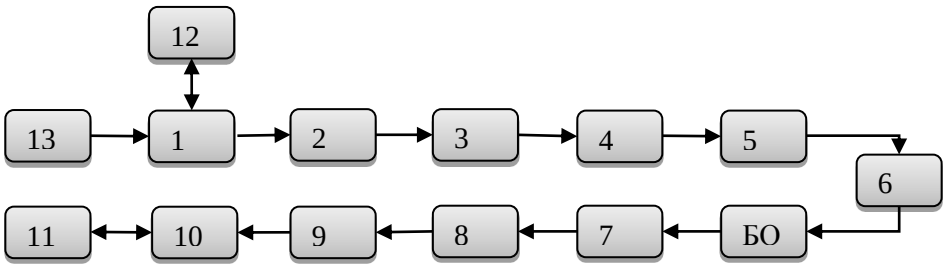

Рис. 2. Апаратна частина приладу кольороінформотерапії. 1 – блок керування, аналізу і обміну інформацією; 2- програмований багатоканальний генератор; 3 - блок управління випромінювачами; 4 - блок випромінювання; 5 - блок просторово-спектрального перетворювання; 6 - блок оптичного транспорту; 7 – блок перетворення сигналу; 8 - блок підсилення та фільтрації сигналу; 9 - блок аналого-цифрового перетворювання; 10 - блок оброблення, керування та збереження інформації; 11 - блок пам'яті даних; 12 - блок зв'язку з комп'ютером; 13 - блок електроживлення.

Схеми підсилення та фільтрації приводять електричні сигнали з перетворювачів до параметрів, необхідних АЦП. АЦП формують цифрову інформацію, яка надходить в блок оброблення, керування і збереження виміряної інформації.

Блок оброблення, керування і збереження виміряної інформації слідкує за потоками і виконує оперативне керування підсилювачами, фільтрами і АЦП, зберігає виміряну інформацію і або передає її в блок керування, аналізу і обміну інформацією. Пам'ять даних призначена для довготривалого збереження отриманої з комп'ютера інформації керування програмованим багатоканальним генератором, виміряної інформації тощо.

Запропонована схема апаратної частини приладу кольороінформотерапії дозволяє виконувати різноманітні та необхідні для фотолікувальних технологій функції:

- Передавання інформації схемою зв'язку до комп'ютера.
- Збереження виміряної інформації в пам'яті комп'ютера та створення бази даних.
- Аналіз інформації для забезпечення режимів програмованого керування параметрами спектрального складу, просторового розподілу фотостимулів за заданою лікувальною програмою.
- Керування програмованим багатоканальним генератором.
- Самодіагностика апаратної частини.

ПЕРЕЛІК ЛІТЕРАТУРИ

1. Коробов А.М. Фототерапевтический апарат Посохова-Коробова «Барва-ЦНС» для профилактики и лечения болезни /Альцгеймера А.М. Коробов, Н.Ф. Посохов, В. Г. Черненков, Е.В. Козырь // Біомедичні оптико-електронні системи та прилади. – 2008. – С. 132-134.
2. Денис Б. Діоди LED завойовують ринок / Б. Денис // Електроінформ. – 2004. – №2. – С. 14-15.
3. Кожухар О. Керування динамікою спектра світлодіодних матриць / О. Кожухар, О. Витичак, А. Зазуляк // Електроінформ – № 3. – 2007. – С.10.

УДК 004.056

ІВАНОВ В.Г., КОШЕВА Н.А., МАЗНІЧЕНКО Н.І.
Національний юридичний університет мені Ярослава Мудрого, Харків (Україна)

ВИКОРИСТАННЯ МЕТОДІВ ТЕКСТОВОЇ СТЕГАНОГРАФІЇ ДЛЯ ЗАХИСТУ АВТОРСЬКИХ ПРАВ В МЕРЕЖІ INTERNET

Анотація. *У роботі розглядаються завдання, які вирішуються в рамках систем захисту інформації, особливе місце серед яких займає задача спеціального кодування інформації у вигляді даних, призначених для прихованої передачі інформації, звана завданням стеганографії. Проведений огляд методів та алгоритмів текстової стеганографії, що застосовуються в сфері захисту авторських прав.*

Постановка проблеми. Бурхливий розвиток інформаційних технологій, який спостерігається в останні роки, призвів до того, що сьогодні величезна кількість інформації, що становить інтелектуальну власність, зберігається і обробляється в комп'ютерних мережах і / або поширюється в цифровій формі.

Найбільш поширеними порушеннями прав інтелектуальної власності сьогодні є піратство, плагіат, підробка інформації, зміна інформації, недобросовісна конкуренція (промислове шпигунство і т. п.).

При цьому найбільша увага приділяється захисту прав інтелектуальної власності мультимедійної інформації, поширюваної на цифрових носіях та в мережі Інтернет, при цьому наголос робиться більше на правове рішення проблеми, технічні питання залишаються на другому плані.

Серед завдань, що вирішуються в рамках систем захисту, особливе місце займає задача спеціального кодування інформації у вигляді даних, призначених для прихованої передачі інформації, звана завданням стеганографії. Побудова стеганографічних методів привертає увагу багатьох фахівців, зайнятих розробкою нових технологій (наприклад, технологій аналізу та фільтрації переданої інформації в мережі), спрямованих на забезпечення високої надійності інформаційних систем. Цифрова стеганографія отримала широке застосування в сфері захисту авторських прав. В об'єкт авторського права може бути впроваджена спеціальна мітка - відбиток пальця (fingerprint), яка ідентифікує законного одержувача. Ще однією вбудовуваною міткою може бути цифровий водяний знак (ЦВЗ), що ідентифікує автора.

У той же час не можна забувати про те, що величезна кількість інформації представлена у звичайному текстовому вигляді: книги, статті, електронне листування, документи, звіти і багато іншого. Причому в сфері електронного документообігу технічні питання захисту інтелектуальної власності не можуть бути повністю вирішені тільки лише стандартними засобами захисту інформації. Стеганографія, що використовує текстові контейнери, називається текстової (text steganography).

Завданням дослідження був аналіз основних вітчизняних і зарубіжних джерел за більш ніж 10 останніх років, присвячених власне методам текстової стеганографії.

Суть дослідження. В даний час існує безліч способів вбудовування прихованої інформації в тестові файли, які можна розділити на наступні групи: синтаксичні методи, лексичні методи та мімікрія.

Синтаксичні методи засновані на використанні особливостей пунктуації, абревіатури та скорочення. До синтаксичним методів відносять також методи, засновані на зміні стилю і структури речення без помітного спотворення вихідного смислового навантаження. При використанні синтаксичних методів в текстових файлах секретна інформація найчастіше кодується шляхом зміни кількості пробілів, використання невидимих символів, регістра букв, шляхом зміни міжрядкових інтервалів, табуляцій і т. д. Синтаксичні конструкції легко вбудовуються в будь-який текст, незалежно від його змісту, призначення та мови. Такі системи легко розробляти і виконуються вони автоматично. Але вони легко зламуються і секретна інформація легко усувається шляхом найпростіших атак. Так само до недоліків представлених методів слід віднести високу ймовірність руйнування прихованого повідомлення при повторному наборі, редагуванні, форматуванні тексту або використанні більш складних текстових редакторів, здатних здійснювати ряд автоматичних операцій над текстом.

Лексичні методи припускають використання семантичних особливостей мови. Даний підхід відрізняється високою ефективністю, обумовленою застосуванням різних методів маніпулювання не другорядними елементами і незначними особливостями текстів, а безпосередньо самими реченнями і словами. Ряд методів, що відносяться до даного напрямку, заснований на використанні синонімів. Принцип роботи базового методу простий: окремі слова в тексті можуть бути замінені іншими словами, які є синонімами вихідних слів. Використання стеганографічного методу, заснованого на заміні синонімів, дозволяє зберегти синтаксичну структуру речення і його смислове навантаження.

Незважаючи на зазначену особливість, такий метод впровадження також не позбавлений недоліків. При заміні деяких слів можливе порушення стилю мови. Також використання деяких слів як синонімів може порушувати авторський стиль написання тексту. На цих фактах базуються багато методів аналізу.

Мімікрія. Методи використання імітуючих функцій (mimic-function). Цей підхід полягає в генерації штучного тексту. Мімікрія генерує осмислений текст, використовуючи синтаксис, описаний в Context Free Grammar (CFG) і вбудовує інформацію, видбираючи з CFG певні фрази і слова. CFG - це один із способів опису мови, який складається з статичних слів, фраз, вузлів, місць, де може бути прийняте рішення, яке слово або фразу далі вставляти в текст. Перевагою методу є те, що результуючий текст не є підозрілим для систем моніторингу. До недоліків можна віднести слабку продуктивність методу, передачу невеликих обсягів інформації і низький ступінь скритності в мережі.

Висновок. Під час аналізу були розглянуті різні методи забезпечення безпеки використання інформаційних технологій за рахунок вбудовування прихованої інформації в тестові файли, кожен з яких має свої переваги і недоліки. Була проведена оцінка ефективності та інформаційної ємності розглянутих методів. На основі запропонованого аналізу кожен окремий користувач може зробити самостійний обґрунтований вибір прийнятного методу в залежності від кола вирішуваних завдань. Запропоновані алгоритми, що базуються на методах цифрової стеганографії, можуть бути використані, наприклад, для захисту авторських прав власників і користувачів текстової інформації, представленої в цифровій формі; для аналізу та фільтрації трафіку, що передається в мережі; з метою припинення витоку комерційної інформації підприємства; побудови систем захисту авторських прав.

ПЕРЕЛІК ЛІТЕРАТУРИ

1. Стеганография, цифровые водяные знаки и стеганоанализ: Монография / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. М.: Вузовская книга, 2009. – 220 с.: ил.

2. В. Текин. Текстовая стеганография // Мир ПК. – 2004. - №11. С. 62-63.

3. Bennett K. Linguistic Steganography: survey, analysis, and robustness concerns for hiding information in text, Center for Education and Research in Information Assurance and Security, CERIAS Tech Report 2004-13. - 30 p.

4. *Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стеганографии.- М.: Горячая линия – Телеком, 2010.-232с.:илл.*

УДК 004.9

КРИВОВА О.А., КОЗАК Л.М.
МННЦ ІТІС НАНУ (УКРАЇНА)

ВИЯВЛЕННЯ ОПТИМАЛЬНОГО НАБОРУ ІНФОРМАТИВНИХ ОЗНАК ДЛЯ КЛАСИФІКАЦІЇ ЕМОЦІЙНИХ РЕАКЦІЙ

Запропоновано методику визначення комплексу інформативних ознак, що базується на поетапному застосуванні багатомірного дисперсійного аналізу, покрокового дискримінатного аналізу з різними стратегіями відбору ознак. Перевірка методу проведена на масиві експериментальних даних: 48 показниках варіабельності ритму серця операторів та результатах самооцінки емоційної реакції при перегляді відео кліпів. Середня точність класифікації 4-х емоційних станів операторів (спокою, перегляд 3-х відео кліпів різної емоційної забарвленості) за комплексом з 10 інформативних показників - 95,6%.

В автоматизованих системах розпізнавання, класифікації, прогнозу має важливе значення моделювання об’єкта на основі системи ознак, що мають максимальну інформативність. Вже на перших етапах розробки інформаційних технологій оцінювання психофізіологічного стану та емоційних реакцій оператора виникає проблема вибору релевантних ознак. За результатами експериментальних досліджень індукованих емоцій відомо, що показники варіабельності ритму серця (ВРС) входять до переліку можливих індикаторів емоційних реакцій. Показано, що досягнена точність розпізнавання основних емоцій залежить як від набору фізіологічних показників так і від методу класифікації і змінюється від 67% до 95% [1].

Метою роботи є розробка методики виявлення набору інформативних ознак для розпізнавання індукованих емоційних реакцій.

Завдання*:* Виділити оптимальний набір показників ВРС для ефективної класифікації реакції оператора на емоційні стимули за допомогою методів дисперсійного та дискримінатного аналізу в