дуговой сварке зазора в пластине в режиме тока. // Збірник наукових праць ІПМЕ ім. Г.Є. Пухова НАН України. – 2009.
7. *Евдокимов В.Ф., Жильцов А.В., Максимов С.Ю., Петрушенко Е.И., Прилипко Е.А., Рыбалкин Е. А.* Трехмерная интегральная модель распределения вихревых токов обусловленных внешним синусоидальным электромагнитным воздействием при дуговой сварке зазора в пластине в режиме напряжения // Труды Института электродинамики. – 2009.

Поступила 9.02.2009р.

УДК 682.03

О.Ю.Афанасьєва, Б.В.Дурняк

ЗАГАЛЬНІ ХАРАКТЕРИСТИКИ ЦИФРОВИХ СТЕГАНОГРАФІЧНИХ СИСТЕМ

Стеганографія, як методика укриття інформації, складається з наступних базових єлементів:

- носія укритої інформації, який називається контейнером,
- стеганограми,
- повідомлення, яке передбачається укривати,
- засобів кодування повідомлення,
- засобів синтезу коду повідомлення з носієм інформації,
- ряду допоміжних засобів, що дозволяють реалізувати процес стеганографічного укриття повідомлення.

Носієм інформації може бути довільне цифрове середовище, яке допускає ту чи іншу інтерпретацію, що ділить різні цифрові середовища на наступні типи та види середовищ:

- текстові,
- графічні,
- звукові, або ауді середовища,
- мультимедіальні середовища,
- інформаційні середовища комп'ютерной мережі та інші.

Переважно, в цифровій стеганографії використовується бітове представлення повідомлення. Бінарна форма представлення інформації може бути первинною, або вторинною. В другому випадку, бінарна форма повідомлення представляє собою результат попереднього кодування відповідного представлення інформації, яку передбачається укривати. Найчастіше, таке попереднє кодування ґрунтується на використанні методів криптографічного перетворення цифрового представлення повідомлення [1].

Стеганографічні системи характеризуються наступними параметрами,

які прийнято в сучасних дослідженнях:

- стійкість,
- пропускна здатність,
- невидимість.

Одним з визначальних параметрів, що описує стеганосистему як таку, є параметр невидимості. Він характеризує міру не здатності користувача інформаційної системи, в якій функціонують стеганограми, при неупередженому спостеріганні та використанні фрагментів інформації, які вміщають стеганограми, виявити укриту у відповідних фрагментах інформацію. Методи вимірювання такої невидимості, в основному, ґрунтується на експериментальних дослідженнях окремих стеганосистем та відповідних стеганограм. В загальному, можна стверджувати, що забезпечення невидимості, по суті, може розглядатися, як маскування повідомлення у вибраному середовищі. Таке маскування можна розглядати в двох аспектах: в аспекті, що відображає можливість виділення такого повідомлення з середовища та в аспекті, що відображає невидимість відповідного повідомлення неупередженим споживачем інформації, яка знаходиться у відповідному середовищі.

Перший аспект визначає міру стійкості стеганографічної системи до викриття укритого повідомлення з допомогою технічних засобів стеганоаналізу. Такі технічні засоби можуть представляти собою апаратурні засоби та програмні засоби, які орієнтовані на дослідження та обчислення ймовірності того, що між вибраними учасниками обміну інформацією використовуються стеганографічні методи передачі даних. Можна прийняти, що вбудовану інформацію неможливо викрити, якщо модель стеганограми співпадає, або близька до моделі інформаційного середовища, яке використовується для розміщення укритих даних. Наприклад, якщо метод вбудовування повідомлення в цифрове середовище, яке представляє собою графічний образ, ґрунтується на використанні шуму в образі, то таке вбудовування не повинно приводити до відхилень статистичних параметрів у образі, які перевищували б пороги, що встановлені у відповідних засобах стаганоаналізу. В цьому випадку, відповідний параметр представляє собою статистичний параметр, який відомий для контейнера і вимірюється у стеганограми. Станаоаналіз, в цьому випадку, полягає у порівнянні середніх величин відхилень у стандартних гістограмах.

Параметр, що відповідає другому аспекту і відповідає невидимості, зв'язується з властивостями системи людського зору (SLZ) . В цьому випадку, стеганосистема була би ідеальною, з точки зору цього параметру, якщоб могла в повній мірі використовувати ідеальну психовізуальну модель SLZ . На жаль, сучасні психовізуальні моделі не являються повними, оскільки реальна система SLZ є надзвичайно складною. Тому, на практиці використовуються спрощені психовізуальні моделі. Прикладом такої моделі може служити функція чутливості SLZ до контрасту, яка позначається

скороченням (CSF) [2]. Ця функція описує залежність відносної психофізіологічної чутливості SLZ від оптичної частоти образу, яка описується у вигляді: $CSF = f(\varphi)$, де φ - оптична частота образу. Найчастіше, така функція представляє собою результати експериментальних досліджень і представляється у графічній формі. Не існує точних методів вимірювання величини значень, для цієї функції. Кількість факторів, що впливають на її значення та вигляд не відома. Побудова певної реалізації такої функції тісно зв'язана з конкретним її застосуванням.

Практична перевірка факту, чи засоби впровадження даних в середовище забезпечують необхідний рівень невидимості, полягає у використанні тесту, що відомий, як BLIND TEST. Суть його полягає на тому, що для певних груп людей висвітлюється контейнер і стеганограма. Вимоги до невидимості впровадження даних в контейнер вважаються виконаними, якщо учасники тестування не в стані відрізнити оригінальний образ від образу, який є модифікованим.

Дослідження статистичних параметрів джерел образів є значно простіше ніж моделювання психофізіологічної моделі SLZ. Наприклад, якщо таким джерелом є сканер, то з його допомогою можна отримати велику кількість образів для проведення досліджень їх статистичних параметрів, а фактори, що впливають на параметри образу, переважно, є відомими, наприклад, температура, час і т.д. Значно складніше побудувати психофізіологічну модель SLZ.

Пропускна здатність описує допустимі розміри повідомлення, яке може бути розміщене у контейнері з точки зору забезпечення, як мінімум, її невидимості. Переважно, ця величина вимірюється в кількості бітів повідомлення по відношенню до величини контейнера, яка вимірюється кількістю пік селів. Наприклад, в роботі [3] автори приводять приклад образу, що використовується, як контейнер, який записаний в форматі BMP 768x512 пікселів і палеті 16M кольорів розміром в 1 179 702 В, в якому розміщено образ $JPEG$ 640x480 пікселів і палеті 16M кольорів розміром в 41 254 В.

Стійкість розглядається по відношенню до множини можливих спотворень даних, які виникають в результаті звичайних, або упереджених маніпуляцій з образами. Стеганосистема вважається стійкою, якщо вислане повідомлення може бути виділене з стеганограми незалежно від певних модифікацій стеганограми. Типовими перетвореннями, які можуть приводити до спотворень у образі є – лінійна і нелінійна фільтрація, компресія образу з втратами, зміна контрасту, гамма корекція, конверсія простору кольорів, сканування, малі нелінійні деформації, додавання шумів, обрізання, друкування, копіювання і сканування, цифро-аналогове та аналого-цифрове перетворення і цілий ряд інших перетворень. Відповідні зміни інтерпретуються, як додавання певної кількості того, чи іншого типу шуму. Об'єктивна міра величини шуму вимірюється параметром $PSNR$, який

представляє собою відношення максимального значення амплітуди сигналу до величини шуму. Для растрових образів, для каналів що мають динамічну характеристику в межах 255, це співвідношення описується у вигляді:

$$PSNR = 10\log_{10}(255^2 / MSE),$$

де MSE - величина середньоквадратичної помилки, яка для образі розміру NxN пік селів описується співвідношенням:

$$MSE = (1/N)^2 \sum_{i=1}^{N} \sum_{j=1}^{N} (x_{ij} - \overline{x_{ij}})^2,$$

де x_{ij} - величина значення піксела стеганограми, який не був підданий спотворенню, $\overline{x_{ij}}$ - величина значення піксела, який був підданий критичному спотворенню, але, при цьому, іще існує можливість правильного відтворення впровадженого повідомлення.

В рамках стеганосистем, що орієнтовані на використання цифрових графічних середовищ, широко використовуються процедури перетворення просторів представлення цифрових графічних образів з ціллю досягнення необхідної міри невидимості вбудованих в образ даних.

Один з таких типів перетворень полягає у використанні псевдовипадкової перестановки пікселів графічного образу, яку прийнято називати пер мутацією образу. В перетворений таким чином образ вводиться повідомлення, починаючи з першого піксела у верхньому ряду. Після введення повідомлення в образ, в ньому здійснюється обернена перестановка пік селів образу на основі використання цього самого псевдо випадкового генератора, який визначає відповідні координати пік селів образу в площині їх розміщення. Завдяки цьому, біти повідомлення хаотично розміщаються по всій площині образу. Цей метод забезпечує швидке впровадження даних у образ, але має ряд недоліків. Один з важливих недоліків полягає у тому, що він не дає змоги адаптуватися до семантичного змісту образу. Цей метод не дозволяє враховувати частотні особливості образу, що є досить важливим, при вираховуванні психофізіологічних властивостей SLZ та при забезпеченні стійкості стеганограми проти компресії з втратами.

Початковий, не компресований образ найчастіше записується в форматі BMP з глибиною кольорів в 24 біти на піксел. При цьому, найчастіше використовується модель кольорів RGB. Ця модель найбільше надається для формування зображень на апаратурі, в якій використовується змішування кольорів світла. З точки зору психофізіологічних властивостей SLZ, ця модель є найменш придатна, оскільки, вона взагалі на враховує властивості SLZ. Особливості сприйняття кольорів SLZ полягають у тому, що чутливість людського ока до різних кольорів різна для колбочок та паличок, які являються рецепторами, що реагують на світло і, відповідно, на кольори. З досліджень SLZ відомо, що людське око є найбільш чутливим до відтінків жовто-зелених і найменш чутливим до відтінків фіолетових і червоних. Тому

перетворення простору кольорів до простору, в якому існує можливість враховувати властивості SLZ по сприйняттю кольорів. З точки зору біологічних властивостей людського зору, найбільш придатною, для того, щоб можна було враховувати особливості людського зору, являється модель HSB, відома також як модель HSV. В цій моделі визначається простір кольорів за допомогою трьох складових:

- відтінку кольору (типу кольору, наприклад, зелений, жовтий) в діапазоні від 0 до 3600,
- насичення кольору(чистості кольору) в діапазоні від 0 до 100%,
- вартості, або ясності кольору.

Виходячи з приведеного віще, модель HSV часто використовується художниками, оскільки ця модель близька до моделі сприйняття кольорів людським оком. Моделі RGB, чи $CMYK$ є найбільш придатними для опису технічних методів отримання кольорів. Слід пам'ятати, що модель HSV не можна безпосередньо відобразити на фізичний спектр видимого світла. Тому, не рекомендується реалізовувати безпосереднє перетворення системи координат моделі HSV в спектр видимого світла і навпаки. Якщо необхідно встановити залежності між моделлю кольорів та фізичними властивостями світла, то існує можливість перетворення HSV до координат псевдо фізичних. В термінології психофізіологічної колориметрії можна говорити, що координата H визначає домінанту, або довжину хвилі випромінювання світла в діапазоні від 240 до 360 ступенів. В цьому діапазоні H визначає чистий пурпурний колір. Координата S визначає розмивання частоти променя по відношенню до частоти домінанти. Це можна трактувати, як кількість білого світла, що додається до спектрально чистого кольору. Координата V, з точки зору психології сприйняття кольорів може бути по трактована як параметр, що визначає повну потужність в спектрі. Точніше, він відповідає за потужність головних складників спектру. При кодуванні HSV, необхідно, щоб значення відповідних координат розміщувались в сенсорних границях, переважно в границі від 0 до 255. Складною проблемою, з якою стикаються, при спробі працювати з моделлю є те, що при відповідному кодуванні можна отримати перетворення $HSV \to RGB$, при цьому оберненого перетворення не буде. Крім того, виникає також цілий ряд технічних проблем. При використанні моделі HSV, необхідно її узгоджувати з іншими популярними стандартами, наприклад, з форматом $JPEG$. Досить часто використовується не модель HSV, а модель YUV. Ця модель описується з допомогою трьох складових параметрів: люмінації Y (ясності), хромінації U (величини сірості) та параметра V. Однією з проблем, з якою зустрічаються, при спробах працювати з моделями типу YUV є те, що в моделі RGB всі канали мають однакову динаміку. В моделі YUV найбільшу динаміку має канал Y, інші канали (U, V) мають обмежену динаміку. Крім того, в даній моделі існують не лінійності. В техніці відео необхідно не

лінійність гами барв враховувати. Існують також проблеми з розмірностями, оскільки, канал Y має одну розмірність, а канали U чи V іншу розмірність. Ці проблеми, на сьогоднішній час, розв'язуються, з допомогою сформованих норм для перетворень $RGB \to YUV$ та $YUV \to RGB$. Відповідний стандарт розроблено у зв'язку з потребами телевізійної техніки. В галузі телевізійної техніки використовуються параметри $HDTV$, для яких запропоновано власні перетворення між ними і RGB. Група $JPEG$ визначила формат $JFIF$, для якого запропонувала власне перетворення $RGB \to YUV$ та $YUV \to RGB$. Одним з відомих прикладів таких перетворень може служити наступне перетворення:

$$Y = 0,299R + 0,587G + 0,114B$$

$$U = -0,147R-), 289G + 0,436B,$$

$$V = 0,615R - 0,515G - 0,1B$$

де $C = Y - 16; D = U - 128; e = V - 128$.

$$R = (298C + 409E + 128)/256$$

$$G = (298C - 100D - 208E + 128)/256.$$

$$B = (298C + 516D + 128)/256$$

Опрацьована модель є добрим компромісом. Приймаючи до уваги існуючі стандарти, властивості кінцевих апаратних засобів, вона є стійка до перетворень образу з кольорового на сірий та враховує психофізіологічні властивості зору людини. Остання з них полягає в тому, що SLZ є значно сильніше чутлива до спотворень в каналі Y ніж в інших каналах.

З приведеного вище, видно, що використання інших моделей кольорів, для вбудовування інформації, що укривається, дозволяє підвищити невидимість відповідних модифікацій середовища, якщо використовувати певні канали кольорів та, при цьому, появляється можливість застосовувати такі методи вбудовування окремих елементів повідомлення, які найбільше відповідають цифровому представленню графічних середовищ у масовому медіальному середовищі, яким являється телевізійна система. Збільшення міри невидимості досягається за рахунок того, що модель кольорів типу YUV враховує особливості сприйняття кольорових образів системою людського зору і, тому, появляється можливість адаптувати відповідні методи вбудовування повідомлення до властивостей SLZ.

Найбільш поширеним методом впровадження біті інформації у цифрове середовище є метод, що відомий під назвою «модифікації найменш значущого біта» або метод LSB. Суть цього методу полягає в тому, що для модифікації елемента цифрового середовища, яка полягає у заміні існуючих в середовищі компонент на компоненти, що відповідають впроваджуваній інформації, вибирається найменш значущий біт байту відповідного піксела, або іншої компоненти образу, якщо останній перетворено у той чи інший простір його представлення. Очевидно, що реально, мова не йде виключно

про один біт, а в залежності від ряду факторів, вибирається певна сукупність найменш значущих бітів. Очевидно, що вибір відповідних пік селів можна здійснювати на у відповідності з натуральною послідовністю їх розміщення у просторі образу, а у відповідності з певним алгоритмом вибору чергового пік селу, який може виконувати роль стеганографічного ключа. Більш того, вибір окремих пік селів для подальшої їх модифікації зв'язаної з впровадженням повідомлення, може обумовлюватися умовами забезпечення певного рівня невидимості відповідних модифікацій, з рахунок вибору в образі його фрагментів, що найбільш придатні для розміщення відповідних бітів.

Основним недоліком методу LSB є його вразливість на різного типу фільтрації відповідних цифрових середовищ, які досить часто використовуються, при обробці цифрових образів. Незважаючи на це, метод LSB широко використовується в стеганографії, оскільки він є досить простим в своїй реалізації та забезпечує високу пропускну здатність відповідного стеганографічного каналу. Збільшення пропускної здатності стеганоканалу в цьому методі приводить до підвищення ризику виявлення інформації у відповідному середовищі. Щоб уникнути цього, використовується кодування з мінімальною похибкою підміни (MER). Суть цього методу можна проілюструвати на наступному прикладі. Приймемо, що початкова вартість піксела рівна 1000 у двійковому коді. Тоді, після модифікації трьох останніх бітів піксела вартість піксела стане 1111. Після застосування методики MER, вартість піксела буде рівна 0111. Проста психовізуальна модель, що використовується у цьому методі, може бути представлена наступним співвідношенням:

$$[(P > 191) \to (U = 5)] \& [(P \le 191) \to (U = 4)],$$

де P - вартість піксела в діапазоні [0,255], U - найбільша кількість найменш значущих бітів, які можуть бути модифікованими. Ця модель діє на основі умови, що чим більша ясність піксела, тим більше може бути він модифікованим. Умова локальної варіації говорить про те, що можна модифікувати K бітів, якщо варіація лівого верхнього оточення піксела, що розглядається рівна:

$$V = \max\{A, B, C, D\} - \min\{A, B, C, D\}$$

$$V = [\log_2 V].$$

Відомим методом вбудовування є метод, що називається розподілом спектру. Цей метод укриття повідомлення полягає у розподілі їх в статистиках люмінації пікселів. Суть цього методу полягає у наступному. В ньому вибирається n пар пікселів. Для цього використовується генератор псевдо випадкових чисел. На наступному кроці незначно змінюється їх контраст. Завдяки цьому контраст такої множини виявляється модифікованим без зміни середньої люмінації в образі. При цьому, доведено, що такий алгоритм може бути стійким по відношенню до компресії $JPEG$, якщо прийняти певні значення окремих параметрів алгоритму. Основним

недоліком таких алгоритмів є їх невисока пропускна здатність. Для подолання цього недоліку використовується цей алгоритм для окремих фрагментів образу, на які розбивається весь образ. Техніки спектрального розподілу відомі з області радіо зв'язку, де передача сигналу може бути укрита від сторонніх учасників радіозв'язку на рівні, що є нижчим від атмосферних шумів. Типове, в таких системах, співвідношення сигнал шум має порядок 0,01. Тому, виявлення укритої інформації, при використанні такого способу укриття є неможливим без використання відповідного ключа.

Наступним методом модифікації елементів образу, при вбудовуванні в його середовище повідомлень є метод, в якому використовуються для модифікації коефіцієнти відповідних перетворень образу. Існує багато способів вбудовування елементів повідомлень, що ґрунтуються на використанні цього методу. В першу чергу, кількість таких способів залежить від кількості типів перетворень форми представлення образів в різних просторах. До найбільш поширених, відомих перетворень відносяться наступні перетворення [5]:

- перетворення Фур'є (FFT)
- дискретне косинус не перетворення (DCT),
- дискретне вейвлет перетворення (DWT) та інші.

Використання методів кодування повідомлення в цифровому середовищі типу *LSB* при використанні перетворень форми представлення образу, яку для зручності будемо називати трансформаціями образу, є не можливим. Це обумовлюється тим, що похибки, які виникають в результаті прямого перетворення образу, наприклад з природного простору представлення образу у частотно-часовий простір, що будемо позначати $Q(x,y) \to Q(f,t)$ та $Q(f,t) \to Q(x,y)$, приводять до того, що останні біти можуть бути втрачені. Тому, впровадження кодів повідомлення реалізується шляхом модифікації значень коефіцієнтів перетворень. Коефіцієнти для модифікації вибираються таким чином, щоб модифікації підлягали коефіцієнти, значення яких є найменшими серед значень інших коефіцієнтів. Найпростішим способом модифікації являється збільшення значення коефіцієнта при впровадженні біту рівного одиниці, і зменшенням значення коефіцієнта, при впровадженні біту рівного нулю. Значення коефіцієнтів змінюються на величину, що визначається заданим порогом. Прикладом іншого способу кодування може служити наступний алгоритм модифікації коефіцієнтів. З допомогою псевдо випадкового генератора вибираються два коефіцієнти. Якщо треба закодувати одиницю, то перший коефіцієнт буде мати більшу абсолютну величину по відношенню до другого коефіцієнта. При кодуванні логічного нуля співвідношення вибирається оберненим.

Інший спосіб кодування полягає у використанні окремих трійок вейвлет коефіцієнтів. Модифікації підлягає абсолютна величина середнього коефіцієнта. Інші коефіцієнти повинні попадати в границю, що визначається наступним чином:

$$(c\max - c\min)/2Q,$$

де $c\max$ - найбільший коефіцієнт трійки, $c\min$ - найменший коефіцієнт трійки, Q - ціле число, коефіцієнт який можна змінювати, щоб вибрати необхідне співвідношення між силою кодування та мірою видимості.

По відношенню до всіх способів кодування і кожного типу перетворень існує небезпека виходу величини значення коефіцієнта за границі [0,255]. Це, в свою чергу, приводить до появи ефекту «чорного сонця», що стає видимим.

1. *Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф.* Защита информации в компьютерных системах и сетях. М.: Радио и связь, 1999.
2. *Gregory R.L.* Oko I mozg. PWN, Warszawa, 1971.
3. Mannons J.L., Sakrison D.J., The Effects of a Visual Fidelity Criterion on the Encoding of Images. IEEE Transactions on Information Theory. Pp. 525-535, N4, 1974.
4. *Le Grand Y.* Oczy I widzenie. PWN, Warszawa, 1964.
Nadenau M.J.,Reichle J., Kunt M. Wavelet-based Color Image Compression: exploiting the Contrast Sensitivity Function, IEEE, 2006.

Поступила 26.01.2009р.

УДК 683.03

Б.В.Дурняк, Т.Равецки

ПОДХОДЫ К РЕШЕНИЮ ЗАДАЧ ПРОГНОЗИРОВАНИЯ РАЗВИТИЯ ПРОЦЕССОВ ФУНКЦИОНИРОВАНИЯ ПРЕДПРИЯТИЯ

Задачи прогнозирования являются одними из наиболее востребованных задач во всех областях человеческой деятельности. Это обуславливается целым рядом факторов:

- желанием людей знать о том, что произойдет с ними и их окружением в ближайшем и отдаленном будущем во всех аспектах возможных перемен, что носят естественный и общий характер,
- необходимость в противодействии со стороны людей тем изменениям и тем факторам, которые могут произойти и являются нежелательными и во многих случаях недопустимыми с многих точек зрения,
- необходимость учитывать изменения в ближайшем и отдаленном будущем в текущих действиях или текущих процессах функционирования и т.д.

Приведенные факторы носят в большей степени общий характер. В задачах управления предприятием, техническими объектами или другими искусственными продуктами человеческой деятельности а также процессами, которые создаются людьми в результате их творческой деятельности, задачи