УДК 355. 462.7

А.О. Аносов

Військова частина А1906

СТВОРЕННЯ НА ОСНОВІ ШУМОВИХ ПРОЦЕСІВ СТЕГАНОКОНТЕЙНЕРІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ ПОТРІБНОГО РІВНЯ СТІЙКОСТІ ДО СТЕГАНОАТАК ЗА ВІДСУТНОСТІ ШИФРУВАННЯ КОРИСНОГО ПОВІДОМЛЕННЯ

Запропонований підхід до формування на основі шумових процесів стеганоконтейнерів для забезпечення потрібного рівня стійкість до стеганоатак в умовах відсутності шифрування корисного повідомлення.

Ключеві слова: *захист інформації, шумові процеси, алгоритм, стенографія;моделювання.*

Вступ

Постановка проблеми у загальному вигляді. Дійсний момент часу характеризується активним дослідженням прихованих методів передачі розвідувальних даних по відкритих каналах зв'язку. Одним з можливих шляхів вирішення цього проблемного питання у практиці ведення розвідувальної діяльності є застосування стеганографічних перетворень [1, 2]. При цьому виникає необхідність захистити інформацію що схована у стеганоконтейнер від несанкціонованого доступу та підвищити стійкість контейнеру до стеганоатак не застосовуючи шифрування корисного повідомлення. Одним з напрямків вирішення цього питання є розробка принципово нових методів формування стійких до стеганоатак контейнерів, які дозволяють закладати інформацію не оброблену алгоритмами шифрування. Однак відомі результати не дозволяють вирішити завдання у повному обсязі та вимагають застосовування складних алгоритмів шифрування та дешифрування інформації. Розроблені методи формування стегаконтейнерів не в повній мірі відповідають вимогам стійкості до структурних методів стеганоаналізу.

Вирішити це протиріччя пропонується на основі використання в якості стеганоконтейнерів шумових процесів, що інтегровані у звукові файли. При цьому для захисту корисної інформації від несанкціонованого доступу можуть застосовуватись статистичні характеристики шумів на основі вейвлет - перетворень [3-5].

Тому постає актуальним дослідження шляхів підвищення стійкості контейнерів до стеганоатак за рахунок застосування статистичних характеристик шумів та вейвлет - перетворень для створення захищених стеганоконтейнерів.

Аналіз останніх досліджень і публікацій. Методи стеганографії розглянуті в роботах [2 – 4]. Визначено, що на практиці в якості мультимедійного контейнера для інформації доцільно використовувати широковживаний формат файлів. Розроблені алгоритми вкраплення інформації в контейнер. Однак аналіз відомих результатів показав, що застосування відомих методів та алгоритмів перетворення графічних та звукових форматів не забезпечує потрібної стійкості в умовах здійснення стеганоатак, а для захисту корисного повідомлення необхідно використовувати шифрування. Це не в повній мірі задовольняє сучасні вимоги до прихованої передачі розвідувальної інформації по відкритих каналах зв'язку. Вирішення зазначених проблемних питань можливо із застосуванням статистичних характеристик шумів та вейвлет - перетворень для формування шумових стеганоконтейнерів, в тому числі й для їх подальшого монтування у файли широковживаних форматів.

Формулювання мети статті (постановка завдання). Одним з завдань, що постає при використанні в якості контейнера шумового процесу є захищені впакування та виділення корисного повідомлення з нього. Для вирішення цього завдання пропонується застосувати вейвлет - перетворення.[5 – 7]. При цьому, властивості вейвлетів дозволяють сконструювати базис, за якім опис даних буде виражатися декількома ненульовими коефіцієнтами. Ця властивість вейвлетів може бути використана для впакування даних, у тому числі відео - і аудіо-інформації у шумові сгеганоконтейнери. Тому **мета статті** – розробити порядок застосування статистичних характеристик шумів та вейвлет-перетворень для створення захищених стеганоконтейнерів в умовах відсутності шифрування корисного повідомлення.

Виклад основного матеріалу досліджень

Нехай стеганоконейнер створюється на основі шумового процесу з рівномірним по частоті плоским спектром (характерно для білого шуму). Тоді, задаючи деякий поріг рівня та зрізуючи по ньому

коефіцієнти, що впливають на властивості шумового процесу, можна не тільки зменшувати рівень шумів, але і встановлювати граничні обмеження на декількох рівнях розкладання інформації При цьому виникає можливість врахувати при закладанні інформації конкретні характеристики шумів і сигналів та різних типів вейвлет - перетворень [5-12]. Однак, при цьому необхідно розробити порядок генерації в цифровій формі, сигналу що моделюється сигналу та цифрову схему модуляції.

Для розробки цифрової схеми модуляції можливо застосувати вейвлет - перетворення (DWT) одномірних сигналів вейвлетів Добеші четвертого порядку db4 функціями прямого перетворення:

$$C_{mk} = \int_{-\infty}^{\infty} f(t) + \psi_{\mu\kappa}(t)\, dt, \qquad (1)$$

де f(t) – корисний сигнал; ψ(t) – базис вейвлет - перетворення

$$\psi_{mk}(t) = |a_0|^{m/2}\psi(a^m{}_0 t-k), \qquad (2)$$

де m – параметр масштабу; k – параметр зрушення.

Застосування підходу (1), (2) дозволяє на практиці приховувати інформацію в області високих частот шумового стеганоконтейнерів та уникнути надмірність безперервного переутворення. У випадку, коли a_0 вибирається рівним 2, одержуємо діадне вейвлет - перетворення. Вейвлет Добеши належить до ортогональних вейвлетів і зворотне перетворення при нормованому ортогональному вейвлет-базисі простору можна представити в такий спосіб:

$$s(t) = \sum_{m=-\infty}^{\infty} \sum_{k=-\infty}^{\infty} C_{mk}\, \psi_{mk}(t), \qquad (3)$$

Результати практичного застосування DWT-перетворення цифрової імпульсної послідовності вейвлетом Добеши четвертого порядку, наведені на рис. 1. Аналіз практичних результатів, рис. 1 показав, що кількість відліків в спектрі шумового процесу дорівнює кількості відліків імпульсного сигналу.

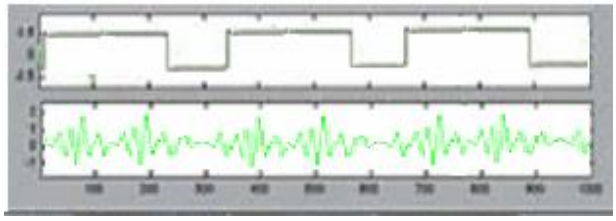

Рис. 1. Діадне вейвлет - перетворення (DWT) цифрової імпульсної послідовності вейвлетом Добеші четвертого порядку

Якщо кількість відліків сигналу не задовольняє умові 2^M, то необхідно або передискретизація сигналу зі зменшенням кроку Δτ, або доповнення інтервалу T.

Модель зашумленного сигналу можливо обрати адитивною з рівномірним кроком за аргументом n

$$s(n) = f(n)+k\cdot e(n), \qquad (4)$$

де f(n) – корисна інформаційна складова; e(n) – шумовий сигнал, наприклад, білий шум визначеного рівня з середнім нульовим значенням.

Результати моделювання застосування (3), (4) для формування стеганоконтейнеру шляхом додавання вейвлет - переутворення з білим шумом наведені на рис. 2.

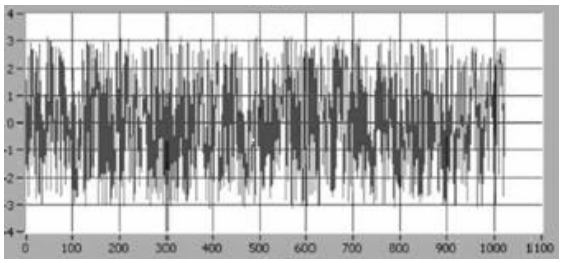

Рис. 2. Результати моделювання формування стеганоконтейнерів шляхом здійснення вейвлет - перетворення над випадковим процесом типу білий шум

У силу диадності перетворення зберігаються всі частотно-часові особливості сигналів та зробити зміни (певну обробку) сигналу на різних рівнях декомпозиції й виконувати зворотне перетворення без втрат інформації.

Виділення корисного сигналу можливо здійснити шляхом вейвлет - розкладання стеганоконтейнерів або його декомпозиції.

Рівень декомпозиції стеганокнтейнеру задається по масштабному коефіцієнту m, при цьому за нульовий рівень (m = 0) ухвалюється рівень максимального тимчасового дозволу сигналу, тобто сам сигнал, а наступні рівні (m > 0) утворюють вейвлет - дерево (від коротких вейвлетів до довгих, або, по середній частоті вейвлетів, від високих частот до низьких). Вейвлет - дерево дозволяє безпосередньо по частотному спектру сформованого шумового сигналу встановити орієнтовну границю шумів і, відповідно рівні декомпозиції, у яких потужність шумів порівнянна й вище потужності сигналу та відповідно зрозуміти порядок формування шумового контейнеру.

Завдання типу й граничних рівнів очищення за відомим даними (дисперсія, стандарт, флуктуації) про характер шумів або за певними критеріями шумів у вхідному сигналі. Граничні рівні очищення можуть бути гнучкими (залежно від номера рівня розкладання) або твердими (глобальними). Модифікації коефіцієнтів деталізації вейвлет - розкладання по заданій кількості нижніх (високочастотних) рівнів «вейвлетного» спектра, і реконструкція сигналу по рівнях, що залишаються, «вейвлетного» спектра.

Порівнянням цих двох реконструйовані складових установлюється оптимальний рівень виділення шумів з «вейвлетного» спектра. Обчислюється гістограма шумових імпульсів і виконується оцінка зв'язку шумів зі значеннями сигналу з можливістю нелінійної регресії статистичних даних.

Результати практичного дослідження можливості виділення корисного сигналу на основі коефіцієнтів апроксимації й модифікованих коефіцієнтів деталізації наведені на рис. 3.

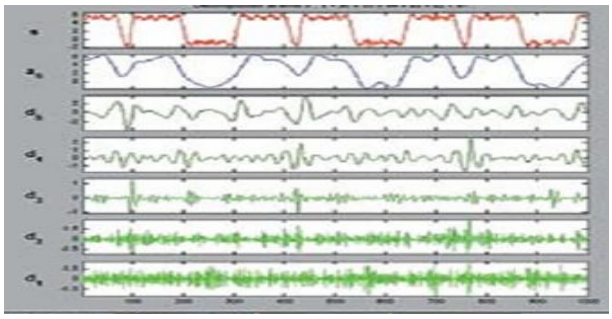

Рис. 3. Результати практичного дослідження можливості виділення корисного сигналу на основі коефіцієнтів апроксимації й модифікованих коефіцієнтів деталізації

На рис. 3 наведено залежність від номера відліку рівнів сигналу і його компонентів. Зроблено важливий з практичної точки зору висновок, що для ортогональних вейвлетів будь-яка точність реставрації сигналу досягається при невеликому (до 6 – 8) числі рівнів L. При обмеженні числа вейвлет - коефіцієнтів можна досягти вейвлет-фільтрації сигналу і його стиску, а вейвлет-фільтрація можлива й для нестаціонарних сигналів і окремих елементів сигналу. Це вказує на те, що у такий спосіб виділення корисного сигналу при правильному виборі порядку базисної функції вся інформація про тонкі особливості сигналу зосереджена у вейвлет-області.

Виходячи з того, що процедура вейвлет відокремлення корисного сигналу від шуму заснована на припущенні, що шум має близький до гауссівського розподілу, тому викид у вейвлет-області розглядається як локальна особливість сигналу і його необхідно виявити й виключити з подальшого розгляду.

Висновок та напрямки подальших досліджень

Розроблений підхід дозволяє створювати на основі шумових процесів стеганоконтейнер на базі аудіо файлів для забезпечення потрібного рівня стійкості до стеганоатак в умовах відсутності шифрування корисного повідомлення.

Напрямком подальших досліджень слід визначити проведення експериментальних досліджень щодо визначення впливу на якість передавання інформації алгоритмів стиску аудіо інформації та порядку монтування шумових контейнерів у графічні файли загальновживаних форматів.

Список літератури

1. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – К.: МК-Пресс, 2006. – 288 с.

2. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: Солон-Пресс, 2002. –272 с.

3. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа / А.Ю. Щеглов. –СПб.: Наука и техника, 2004. – 384 с.

4. Конахович Г.Ф. Компьютерная стеганография. теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – К.: МК-Пресс, 2006. – 288 с.

5. Воробьев В.И. Теория и практика вейвлет-преобразования / В.И. Воробьев, В.Г. Грибунин. – СПб, ВУС, 1999. – 204 с.

6. Вейвлеты и их использование / И.Л. Дремин и др. // Успехи физических наук, – 2001. – Т.1 71, № 5. – С. 465-501.

7. Дьяконов В.П. Вейвлеты. От теории к практике / В.П. Дьяконов. – М.: СОЛОН-Р, 2002. – 448 с.

8. Рогозинский Г.Г. Применение вейвлет-анализа для восстановления зашумленных сигналов / Г.Г. Рогозинский // Материалы НТК студентов и аспирантов институтов и факультетов СПбГУКиТ. СПб.: ГУКиТ, 2005.

9. Рогозинский Г.Г. Применение метода оптимизации вейвлетов в перцепционном кодировании звука / Г.Г. Рогозинский // Радиотехника. – 2010. – № 5. – С. 94 – 98.

10. Рогозинский Г.Г. Биортогональные вейвлеты с улучшенной частотной селективностью / Г.Г. Рогозинский // Материалы НТК студентов и аспирантов институтов и факультетов СПбГУКиТ. СПб.: ГУКиТ, 2010.

11. Переберин А.В. О систематизации вейвлет-преобразований / А.В. Переберин // Вычислительные методы и программирование. – 2001. – Т. 2.

12. Смоленцев Н.К. Основы теории вейвлетов. Вейвлеты в Matlab / Н.К. Смоленцев. – М.: LVR Пресс, 2005. – 304 с.

Надійшла до редколегії 21.10.2013

Рецензент: д-р техн. наук, проф. Е.Т. Скорік, ДП «Центральний НДІ навігації і управління», Київ.

СОЗДАНИЕ НА ОСНОВЕ ШУМОВЫХ ПРОЦЕССОВ СТЕГАНОКОНТЕЙНЕРОВ ДЛЯ ОБЕСПЕЧЕНИЯ НУЖНОГО УРОВНЯ УСТОЙЧИВОСТИ К СТЕГАНОАТАКАМ ПРИ ОТСУТСТВИИ ШИФРОВАНИЯ ПОЛЕЗНОГО СООБЩЕНИЯ

А.А. Аносов

Предложен поход для создания стеганоконтейнеров на основе шумовых процессов для обеспечения нужного уровня устойчивость к стеганоатак при отсутствии шифрования полезного сообщения.

Ключевые слова: *защита информации, шумовые процессы, алгоритм, стенография; моделирование.*

CREATION ON THE BASIS OF NOISE PROCESSES OF STEHANOCONTEYNER FOR SUPPORT OF NECESSARY LEVEL OF FIRMNESS TO STEHANOATTACKS IN THE ABSENCE OF ENCODING OF THE USEFUL MESSAGE

A.A. Anosov

The offered approach to formation on the basis of noise processes of stehanoconteyner for support of the necessary level of firmness to stehanoattacks in the condition of absence of encoding of the useful message.

Keywords: *protection of information; noise processes; algorithm; steganography; modelling.*