УДК 004.056.53
К.В. Защолкін, канд. техн. наук, доц.
Одеський національний політехнічний університет, Україна

КЛАСИФІКАЦІЯ КОНТЕЙНЕРІВ ДЛЯ ВБУДОВУВАННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ

K.V. Zashcholkin, PhD, Assoc. Prof.

CLASSIFICATION OF CONTAINERS FOR EMBEDDING DIGITAL WATERMARKS

Цифровий водяний знак (ЦВЗ) являє собою дані, що вбудовуються в інформаційний об'єкт з метою контролю його використання. Технологія ЦВЗ заснована на застосуванні прийомів цифрової стеганографії, в межах яких приховується факт наявності ЦВЗ в інформаційному об'єкті (контейнері). При цьому ЦВЗ може бути одержаним з контейнера при наявності стего-ключа, що визначає правила доступу до елементів ЦВЗ [1].

В сучасних інформаційних системах ЦВЗ отримали широке розповсюдження в задачах контролю використання мультимедійного контенту: растрових графічних файлів, відеофайлів, цифрового звуку. Очевидно, що необхідність в контролі використання інформаційних об'єктів не обмежується тільки контейнерами даного виду. Така необхідність має місце і для широкого спектра інших інформаційних об'єктів. В даній роботі пропонується класифікація контейнерів для вбудовування цифрових водяних знаків. Класифікація заснована на виділенні характерних ознак контейнерів. Метою даної класифікації є визначення потенційної множини інформаційних об'єктів, які можна контролювати за допомогою ЦВЗ, і виявлення характеристик цих об'єктів, істотних для організації ЦВЗ. Далі пропонується три ознаки класифікації контейнерів, що утворюють класифікаційну систему.

Класифікація контейнера за ознакою активності. Контейнери, що становлять набір даних, який виконує тільки функцію зберігання, будемо називати *пасивними*. Прикладами пасивних контейнерів є класичні контейнери для ЦВЗ: растрові графічний файл, звукові файли, відеофайли.

На противагу пасивним, пропонується називати активними контейнер, що виконують деяку обчислювальну або керуючу функцію. Приклади активних контейнерів: виконувані файли для апаратно-програмних платформ на основі мікропроцесорів [2], файли конфігурації програмованої логічної інтегральної схеми [3].

Класифікація за типом зв'язків між елементарними одиницями контейнера. Традиційні контейнери ЦВЗ складаються з інформаційно автономних елементарних одиниць. Це означає, що дані, які містяться в кожній елементарній одиниці, вичерпно визначають значення цієї одиниці. Тобто для визначення значення однієї одиниці не використовується значення інших одиниць оскільки значення одиниці цілком визначається її інформаційним вмістом. Контейнери такого виду будемо називати контейнерами з *автономними елементарними одиницями*. Разом з тим значення елементарних одиниць для таких контейнерів зазвичай є взаємокорельованими, що лежить в основі багатьох методів злому контейнерів (пасивних атак на ЦВЗ).

На противагу контейнерам з автономними елементарними одиницями визначимо контейнери, для яких дані одних елементарних одиниць або залежать від даних інших елементарних одиниць або перебувають з ними у функціональному зв’язку. Такого роду контейнери будемо називати контейнерами з *неавтономними елементарними одиницями*. Прикладом таких контейнерів може виступати конфігурація програмованої логічної інтегральної схеми, представленої системою пов'язаних між собою блоків LUT (Look Up Table) [4].

Класифікація за способом подання інформації в елементарних одиницях контейнерів. Інформація, що знаходиться в кожній з елементарних одиниць традиційних контейнерів ЦВЗ є наближеною. Варіювання цієї інформації в деякому діапазоні не приводить до спотворення функції контейнера. Так мале змінення значень кольорів пікселів не спотворює зображення, мала зміна значень семплів не чутлива для слуху. Разом з тим можливість варіювання цієї наближеної інформації породжує можливість атаки на приховану в контейнері інформацію (приклад для графіки: стиснення, невеликий поворот, слабке розмиття зображення; приклад для звуку: незначне збільшення амплітуди сигналу). Контейнери такого роду будемо називати контейнерами з *наближеним поданням елементарних одиниць*. На противагу таким контейнерів можна визначити контейнери з *точно поданими елементарними одиницями*. Зміни в значеннях елементарних одиниць контейнерів такого виду не припустимі, оскільки вони приводять до руйнування контейнера (порушення його функціональності).

Було виділено три ознаки класифікації контейнерів ЦВЗ. Можливі комбінації значень цих ознак утворюють класи контейнерів в межах пропонованої класифікації (табл. 1). Наприклад, до класу C_1 відносяться традиційні мультимедійні контейнери, до класу C_8 відносяться контейнери з LUT-орієнтованою архітектурою [4].

Таблиця 1 – Класи контейнерів в пропонованій системі класифікації

Класи контейнерів	За ознакою активності		За типом зв'язків між елементарними одиницями		За способом подання інформації	
	Пасивні	Активні	Автономні	Не автономні	Наближені	Точні
C_1	1		1		1	
C_2	1		1			1
C_3	1			1	1	
C_4	1			1		1
C_5		1	1		1	
C_6		1	1			1
C_7		1		1	1	
C_8		1		1		1

В даній роботі запропоновано класифікацію контейнерів ЦВЗ на основі ознак активності, типу зв'язків між елементарними одиницями контейнера і способом подання інформації в елементарних одиницях. Конкретні значення кожної з ознак запропонованої класифікації визначає особливості методів виконання операцій з ЦВЗ для контейнерів даного класу.

Література

1. Cox I. Digital Watermarking and Steganography / I. Cox, M. Miller, J. Bloom, J. Fridrich. – Burlington: Morgan Kaufmann Publishers, 2008. – 592 p.

2. El-Khalil R. Hydan: Hiding Information in Program Binaries / R. El-Khalil, A. Keromytis // Proceedings of International Conference on Informaton and Communications Security (ICICS 2004). – Malaga, Spain, 2004. – P. 187–199.

3. Защелкин К.В. Метод стеганографического скрытия данных в LUT-ориентированных аппаратных контейнерах / К.В. Защелкин, Е.Н. Иванова // Электротехнические и компьютерные системы. – Киев, 2013. – № 12 (88). – С. 83–90.

4. Защелкин К.В. Метод внедрения цифровых водяных знаков в аппаратные контейнеры с LUT-ориентированной архитектурой / К.В. Защелкин, Е.Н. Иванова // Информатика и математические методы в моделировании. – Одесса. – 2013. – Том. 3, № 4. – С. 369–384.