Список літератури

1. А.с. 388790 СССР, МКИ B 03 b 11/00. Устройство для автоматического контроля загрузки и стабилизации разжижения пульпы в мельнице / Ф.Н. Дегтярев, А.А. Мерзляков, В.А. Кондратец, В.И. Новохатько, Н.И. Кучма, Т.И. Гуленко (СССР). – 1420849/29-33; заявл. 30.03.70; опубл. 05.07.73, Бюл. № 29.

2. Пат. 7741 Україна, МКВ 7 B 03 B 11/00. Спосіб автоматичного контролю розрідження пульпи в млинах, що подрібнюють піски механічних класифікаторів / Кондратець В.О., Мацуй А.М.; заявник та патентовласник Кіровоградський національний технічний університет. - №20041007979; заявл. 01.10.2004; опубл. 15.07.2005, Бюл.№7.

3. Пат. 87374 С2 Україна, МПК G 01 F 23/00. Спосіб вимірювання рівня рідких середовищ з хвильовими коливаннями / Кондратець В.О., Мацуй А.М.; заявник і патентовласник Кіровоградський національний технічний університет.- №200712196; заявл. 05.11.2007; опубл. 10.07.2009, Бюл. №13.

4. Пат. 62133 Україна, МПК G 01 L 7/00. Спосіб вимірювання тиску рідких середовищ з хвильовими коливаннями / Кондратець В.О., Мацуй А.М.; заявник і патентовласник Кіровоградський національний технічний університет.- №u201101692; заявл. 14.02.2011; опубл. 10.08.2011, Бюл. №15.

5. Кондратець В.О. Ідентифікація співвідношення руда/вода в процесі подрібнення пісків класифікатора / В.О. Кондратець, А.М. Мацуй // Вісник Вінницького політехнічного інституту.- 2009.- №3.- С. 8-12.

ПРИМЕНЕНИЕ МЕТОДОВ СТЕГАНОГРАФИИ ДЛЯ ОРГАНИЗАЦИИ ОБМЕНА ДАННЫМИ В АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫХ СИСТЕМАХ

А.Т. Харь, А.Н. Морозова
(Украина, Днепропетровск, ГВУЗ «Национальный горный университет»)

Вступление. Информация, циркулирующая в каналах передачи данных автоматизированных информационно-измерительных систем (АИИС), во многих случаях носит конфиденциальный характер и, следовательно, выдвигается ряд требований к обеспечению ее целостности, защиты от несанкционированного доступа или сокрытии самого факта ее передачи.

Одним из эффективных методов решения этой задачи является метод стеганографии [1], который предполагает «встраивание» сообщения в поток цифровых данных, как правило, имеющих аналоговую природу – речь, аудиозаписи, изображения, видео и т.п. Также применяется встраивание информации в исполняемые и текстовые файлы программ [1]. Методы стеганографии могут быть эффективно использованы и для передачи измерительной информации в каналах АИИС в различных областях – промышленности, электроэнергетике, медицине, авиации и т.п. Применение данных методов предполагает внесение незначительных модификаций, соответствующих информационному сообщению, в несущий сигнал-контейнер. В АИИС в качестве контейнера могут использоваться сигналы вспомогательных служебных сообщений или информационные сигналы других, менее значимых по важности источников информации.

Состояние проблемы. На сегодняшний день существует ряд программных продуктов, реализующих методы стеганографии, основанные на

перечисленных различных алгоритмах. Данные программные продукты имеют различные возможности, принципы работы, области применения, формат используемых данных и предпочитаемую программную платформу. Однако существует проблема, связанная с плохой переносимостью и узкой специализацией существующих программных продуктов, что делает их не вполне пригодными для эффективного решения задачи применения методов стеганографии в промышленных АИИС.

Постановка задачи. Требуется осуществить выбор и обоснование метода скрытой передачи данных в компьютеризованных системах АИИС и формирование критериев к осуществлению его программной реализации.

Решение задачи. Наиболее подходящей реализацией методов стеганографии в каналах передачи данных АИИС является использование в качестве контейнера отрезков гармонических сигналов. Скрытность передачи должна достигается локальными незначительными модификациями их фазовых характеристик, которые не могут быть определены обычными амплитудными или фазовыми детекторами вследствие их инерционности [2].

Сигналом-контейнером для передачи информационного сообщения может служить отрезок гармонического сигнала вида:

$$u_0(t) = U\sin(2\pi ft), t \in [0, T_H], T_H > 2T, \quad (1)$$

где *U, f, T* – соответственно амплитуда, частота и период сигнала, *t* – текущее время, T_H –интервал времени, на котором наблюдается сигнал-контейнер.

На интервале времени равном *T*с началом в момент $t_H \in [0, T_H]$, фаза сигнала–контейнера модулируется информационным сообщением

$$\varphi(t) = \begin{cases} m\sin 2\pi ft, m < 1, t \in [t_H, t_H + T), \\ 0, t \in [t_H, t_H + T), \end{cases} \quad (2)$$

где *m* – индекс угловой модуляции, *m<1*.

Необходимо реализовать процесс демодуляции сигнала вида:

$$u_0(t) = U\cos(2\pi ft + \varphi(t)), t \in [0, T_H], \quad (3)$$

найти оценку $\tilde{\varphi}(t)$ информационного сообщения и определить ее погрешность.

Идея предложенного метода скрытой передачи данных в каналах ИИС изложена в [3, 4]. Она основывается на определении фазовых характеристик сигнала, полученных с помощью преобразования Гильберта [5]. Методика решения поставленной задачи предполагает выполнение операций [6]:

1. Формирование сигнала-контейнера (3), содержащего информационное сообщение φ(t) (2);

2. Определение гильберт-образа сигнала-контейнера;

3. Определение дробной части фазовой характеристики сигнала-контейнера;

4. Развертывание фазовой характеристики сигнала $u(t)$ на интервале его наблюдения с целью получения оценки развернутой фазовой характеристики;

5. Оценка информационного сообщения как разности фазовой характеристики сигнала и фазы сигнала-контейнера без информсообщения;

6. Определение погрешности оценки.

Теперь возможно сформулировать список требований к разрабатываемому программному продукту:

- устойчивость к статистическому анализу;
- расширяемая архитектура. Программный комплекс должен поддерживать возможность подключения дополнительных модулей, содержащих произвольные реализации методов сокрытия и извлечения информации;
- наглядный и эргономичный интерфейс пользователя. Разрабатываемый комплекс должен изначально поставляться с удобным и простым в использовании пользовательским интерфейсом с достаточным количество подсказок и справочного материала.

Всем вышеперечисленным требованиям удовлетворяет среда разработки Microsoft Visual Studio. Язык C# является строго типизированным объектно-ориентированным языком, а принадлежность его к платформе .NET позволит сделать приложение кроссплатформенным. Это возможно благодаря реализации поддержки данной технологии в UNIX-подобных ОС программным продуктом Mono, включающим компилятор C # и Common Language Runtime.

Выводы. Для обеспечения безопасного информационного обмена в каналах АИИС специального назначения был предложенный метод скрытой передачи информации, основанный на использовании фазовых характеристик сигналов, полученных с помощью преобразования Гильберта. В качестве сигнала-контейнера могут быть использованы сигналы вспомогательных служебных сообщений или информационные сигналы второстепенных источников информации. Для программной реализации данного метода может применяться объектно-ориентированный язык программирования C# совместно с программным продуктом Mono, обеспечивающим необходимую кроссплатформенность.

Список литературы

1. Основи комп’ютерної стеганографії/ В.О. Хорошко, О.Д. Азаров, Ю.Є. Шелест та ін. –Вінниця: ВДТУ, 2003. – 143 с.

2. Куц Ю.В., Щербак Л.М. Задачі модуляції сигналів у системах захисту інформації з використанням дискретного перетворення Гільберта / Защита информации: Сборник научных трудов. – К.: НАУ, 2004. – с.135–144.

3. Патент Украины на корисну модель №51344 спосіб прихованного передавання інформації. Куц Ю.В.. Гопієнко А.В., Монченко О.В. – Опубл. 12.07.2010 бюл. №13, 2010.

4. Куц Ю.В., Щербак А.В., Статистична фазометрія. - Тернопіль: видавництво Тернопільського державного технічного університету імені Івана Пулюя, 2009.-383с.

5. Бендат Дж., Пирсол А. Прикладной анализ случайных данных: Пер. с англ. - М.: Мир,1989.-540 с.

6. Гопиенко А.В., Куц Ю.В., Монченко Е.В. Метод скрытой передачи данных в компьютеризированных измерительно-информационных системах / «Захист інформації», №2, 2011. - с. 5-9.