Устройство представляет собой боек (1), вертикально установленный в жестко закрепленный к основанию корпус (2). Боек свободно перемещается относительно вертикальной оси конструкции, что позволяет установить его на заданную высоту в пределах 20 мм. В качестве регулировки положения бойка выступает зубчатое колесо (3), имеющее свободное вращение. Фиксируется положение зубчатого колеса стопором (4).

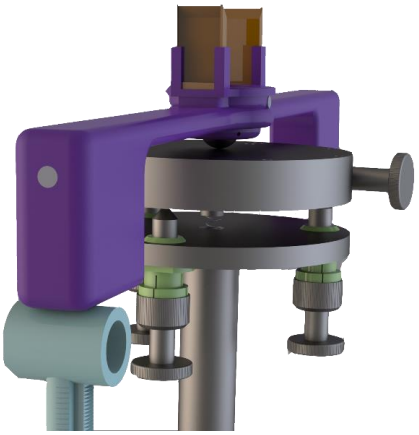

Рис. 1. Расположение устройства в установке

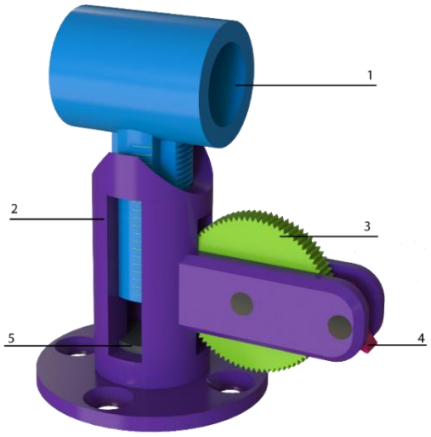

Рис. 2. Устройство запуска маятника

Маятник запускается следующим образом: боек подводится к маятнику до контакта поверхностей, тем самым задается нулевой уровень отсчета угла отклонения маятника, затем поднимается на дополнительное расстояние за счет зубчатого колеса. Положение фиксируется упором. Одновременно с началом измерений, упор отводится от зубчатого колеса и боек под собственным весом опускается в исходное положение. Для минимизации возникших вибраций от удара бойка о дно корпуса, предусмотрен резиновый демпфер (5).

Благодарность: работа выполнена при финансовой поддержке Министерства образования Республики Беларусь, а рамках выполнения гранта студентам на 2022.

Литература

1. Halama, R. Mechanics of Herbert Pendulum Hardness Tester and its Application / R. Halama [et al.] // Key Engineering Materials. – Trans Tech Publications Ltd, 2017. – Vol. 741. – P. 122–127.

2. Джилавдари, И.З. Устройство и методика измерения моментов сил сопротивления качению на пятне контакта / И.З. Джилавдари, С. Мекид, Н.Н. Ризноокая // Приборы и методы измерений. – 2019. – Т. 10. – №. 4.

УДК 621.397.3

ОЦЕНКА ПРИМЕНЕНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

Ст. преподаватель Ковынёв Н.В.
Московский государственный технический университет имени Н.Э. Баумана, Москва, Россия

Задача защиты информации – одна из главных задач, которые решаются с давних времен. Защита информации решает такие задачи как: защита авторских прав, интеллектуальной собственности, подлинности представленной продукции, защита от несанкционированного доступа и т. д. Наиболее остро данная проблема представлена в цифровом виде: фотографии, аудио, видеозаписи. Одним из основных способов защиты информации является стеганография. Стеганография скрывает сам факт существования секретных данных на носители при их передачи. В качестве одного из способов стеганографической защиты информации может выступать способ встраивания цифровых водяных знаков (ЦВЗ) в файлы или документы. Организация стеганографической передачи информации является актуальным направлением для сохранения безопасности информации.

Цифровые водяные знаки изначально предназначены для защиты от копирования или подмены информации, исходя из этого, можно утверждать, что злоумышленник будет знать про

ЦВЗ, но данное знание не является критичным, в отличие от стойкости ЦВЗ. Также, стоит отметить, что более высокий приоритет у задачи достоверности приема бит ЦВЗ, а не у задачи повышения скрытых пропускных способностей каналов передачи информации, так как скрытность встраивания ЦВЗ является определяющим требованием.

В отличие от обычных водяных знаков, цифровые водяные знаки могут быть видимы, но и не видимы, второй вариант наиболее часто используется. Невидимые ЦВЗ анализируются декодером, устанавливающим их корректность. В ЦВЗ может содержаться информация о владельце, какой-либо код, любую управляющую информацию. Рассмотрим стегосистему с декодером.

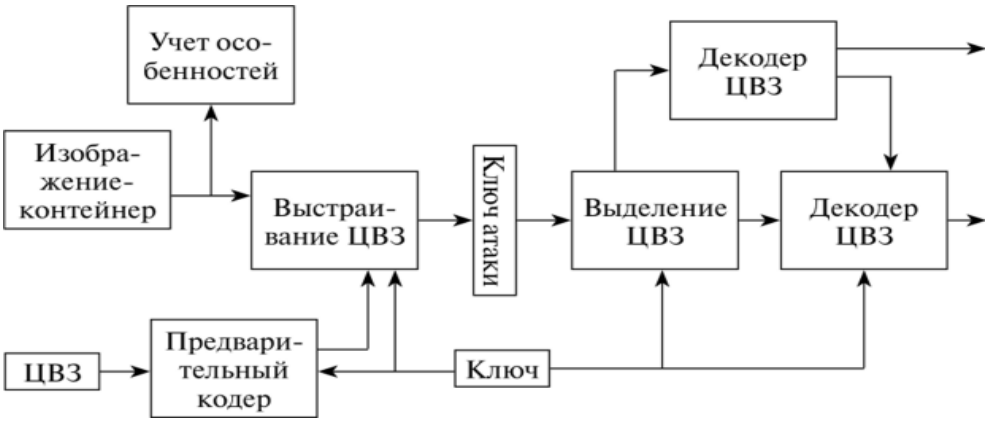

Рис. 1. Структурная схема стегосистемы с ЦВЗ

В данной системе происходят процессы встраивания и выделения ЦВЗ из контейнера. Система состоит из следующих компонентов: предварительный декодер, учет особенностей, устройство встраивания ЦВЗ, устройство выделения ЦВЗ, Декодер ЦВЗ, иногда для проверки наличия ЦВЗ используют детектор ЦВЗ.

Данная система достаточно продуктивна, потому что человек не способен обнаружить ЦВЗ невооруженным взглядом. Стегодетектор (декодер) обнаруживает ЦВЗ в контейнере. Декодеры могут выполнять следующие задачи: обнаружение ЦВЗ и декодирование ЦВЗ. Принятие решения о наличии или отсутствия ЦВЗ в контейнере выносится на основании расстояния по Хэммингу либо на основании взаимной корреляции между данным контейнером и оригиналом или же при помощи статистических методов при отсутствии оригинала.

Исходя из информации, которая требуется декодеру, выделяют три класса стегосистем:

1) закрытые: а) декодеру необходимы исходные контейнер и ЦВЗ для обнаружения наличия или отсутствия ЦВЗ, б) декодеру нужен только исходный контейнер, чтобы получить восстановленный ЦВЗ;

2) полузакрытые: декодер выдает информацию о наличии или отсутствии ЦВЗ по исходному ЦВЗ;

3) открытые: ничего не требуется, выдается восстановленный ЦВЗ.

Наиболее часто применяются открытые стегосистемы, потому что для решения задачи обнаружения им не требуются никакие исходные данные. Стоит отметить, что и сами ЦВЗ бывают разными, а именно:

1) робастные – устойчивые к изменениям: видимые для всех, видимые хотя бы для одной стороны, устойчивые к модификациям и извлечениям контейнера (невидимые ни для кого);

2) хрупкие – чувствительны к любым изменениям и взаимодействиям контейнера, как правило, применяются для проверки целостности контейнера.

3) полухрупкие – чувствительны к определенным воздействия на контейнер, чаще всего применяются для аудиофайлов.

Как показывает практика, актуальность проблемы защиты информации неуклонно возрастает и стимулирует на поиск новых методов и способов защиты информации. Исходя из представленного исследования, можно сделать выводы, что применение цифровых водяных знаков для защиты конфиденциальной информации или интеллектуальной и цифровой собственности дает

гарантии, что злоумышленник не сможет реализовать угрозы конфиденциальности и целостности информации. Однако, стоит отметить, что применение цифровых водяных знаков в изображениях может быть ограничено размерами из-за маленьких размеров исходных изображений, так как при малых разрешениях могут возникать искажения исходных изображений. Не стоит забывать и про помехоустойчивость изображений с ЦВЗ, так как при передачах контейнер может быть подвержен различным воздействиям, из-за которых может нарушиться целостность информации и ЦВЗ.

Литература

1. Грибунин, В.Г. Цифровая стеганография : учебное пособие / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – Москва: СОЛОН-ПРЕСС, 2009. – 264 с.

2. Шелухин, О.И. Основы стеганографии. Часть 1. Скрытие данных в аудио- и текстовых файлах : учебное пособие / О.И. Шелухин, Т.Б.К. Бен Режеб. – Москва: Московский технический университет связи и информатики, 2015. – 129 с.

3. Ганжур, М.А. Особенности цифровой стеганографии как метода обеспечения сокрытия данных / М.А. Ганжур, Я.В. Дзюба, В.А. Панченко // Проблемы современного педагогического образования. – 2018. №59-4. – С. 10 – 14.

4. Алаа Вахаб Методы цифровой стеганографии на основе модификации цветовых параметров изображения / Алаа Вахаб, Д.М. Романенко // Труды БГТУ. Серия 3: Физико-математические науки и информатика. – 2018. – №1 (206). – С. 94–98.

УДК 531.383

КОМПЛЕМЕНТАРНЫЙ ФИЛЬТР ДЛЯ НАВИГАЦИОННЫХ ИЗМЕРЕНИЙ

Студент гр. 120891 Колесникова А.Г.
Д-р техн. наук, профессор Матвеев В.В.
ФГБОУ ВО «Тульский государственный университет», Тула, Россия

Целью любого эксперимента является получение данных и дальнейший их анализ. Однако как понять на сколько точны и правдивы измерения?

К основным погрешностям измерений навигационных элементов относятся нестабильность технических параметров, технологические погрешности в изготовлении, недостаточная чувствительность, несовершенство метода измерения. Также велико влияние внешней среды.

Для анализа и дальнейшей обработки использовались данные, полученные с микромеханического модуля GY-521. Данный модуль подвергался колебаниям математического маятника, и на выходе имел затухающие колебания (рис. 1).

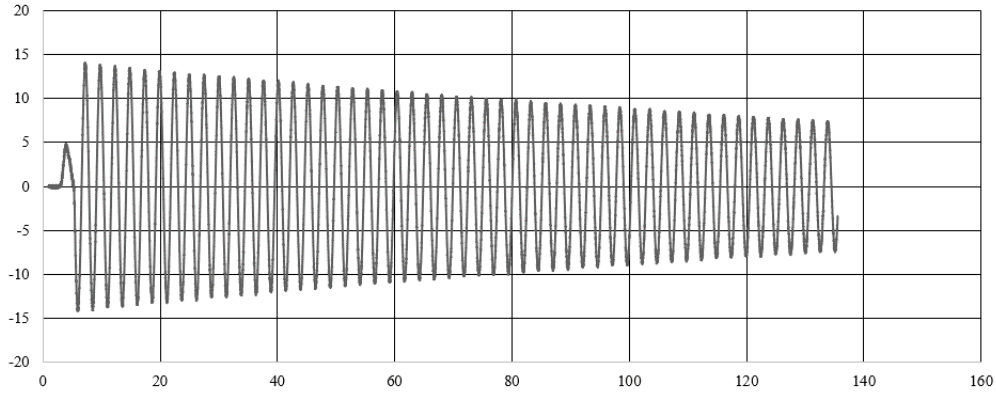

Рис. 1. Исходные данные

Далее стояла задача определить зависимость входных данных W_k и выходных Wf_k

$$Wf_{k+1} := Wf_k(1-\alpha) + \alpha \cdot W_{k+1}. \quad (1)$$

Исследуем наименьший (рис. 2, а) и наибольший (рис. 2, б) коэффициент фильтрации данных.