для отвода тепла и охлаждения, в частности, в ноутбуках. Принцип работы ТТ аналогичен принципу работы термосифона (ТС). Однако ТТ имеет капиллярную структуру, в отличие от ТС. И поэтому работа по охлаждению объекта может происходить в любых положениях ТТ, так как конденсат возвращается в зону поглощения тепла под действием капиллярных сил. К тому же, ТТ имеют ряд преимуществ, таких как: автономность и надежность, столь важные для защиты информации, а также эффективность, бесшумность и компактность. Для увеличения площади контакта ТТ с сервером конструктивно лучше использовать ТТ с квадратным либо прямоугольным сечениями. Все выше перечисленное приводит к концепции расположения сервера на поверхности ТТ. Для проведения исследований изготовлены: экспериментальный ТС и два конструктивно отличающихся друг от друга рабочих радиатора. На основании экспериментальных данных рассчитаны: эффективный коэффициент теплопроводности и термическое сопротивление ТС, что подтверждает правильность выбора ТТ в качестве нового охладительного элемента для оборудования в ЦОД.

ВВЕДЕНИЕ ДИСКРЕТНЫХ ХАОТИЧЕСКИХ ОТОБРАЖЕНИЙ ПРИ ФОРМИРОВАНИИ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ

А.В. Сидоренко, И.В. Шакинко

На современном этапе развития информационных технологий большинство веб-приложений и интернет-ресурсов обеспечивают передачу изображений. Возникает необходимость в решении задач связанных с защитой цифровых изображений из-за невозможности обеспечения требуемых уровней безопасности передаваемой информации в телекоммуникационных каналах [1]. Для этих целей традиционно используется подход, получивший название цифровые водяные знаки (ЦВЗ). Это специальные метки, встроенные в изображение (или другие цифровые данные) для обеспечения контроля его применения [2].

В данной работе приводятся результаты анализа разработанного алгоритма формирования, встраивания и извлечения ЦВЗ. ЦВЗ формируются при использовании следующих хаотических отображений: логистического, тент-отображения и отображения Бернулли.

Установлено, что ЦВЗ, формируемые на основе различных хаотических отображений, при встраивание в изображение практически не меняют его статистические характеристики.

Результаты тестирования предлагаемого алгоритма свидетельствуют о том, что данный алгоритм является стойким к атакам копирования. При использовании алгоритма допустимы потери фрагмента изображений, а также наличие шумов в канале передачи. При этом в последнем случае возможны изменения более 10 % элементов изображения.

Варьируя пороговым значением уровня шума, изменяя размеры блоков изображения становится возможным различать искажения и модификацию областей изображения, произведенных злоумышленником.

Литература

1. Robust Image Watermarking Theories and Techniques: A Review / H. Tao [et al.] // Journal of Applied Research and Technology. 2014. Vol. 12. P. 122–138.

2. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: Солон-Пресс, 2002 . С. 5.

ОБЗОР МЕТОДОВ ДЛЯ ПОИСКА УЯЗВИМОСТЕЙ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ

В.О. Сидорович, А.Е. Варюшина

Провал или успех наших повседневных дел в той или иной степени определяется корректностью функционирования программного обеспечения (ПО), что ставит современное общество в зависимость от уязвимостей в ПО[1].

Уязвимости ПО – критические ошибки, не выявленные в ходе тестирования и не декларированные спецификацией разработчика или заложенные преднамеренно, предоставляющие злоумышленникам исключительные возможности по разглашению