

ЗАЩИТА ДАННЫХ С ИСПОЛЬЗОВАНИЕМ КООРДИНАТНОГО ПРЕОБРАЗОВАНИЯ

А.И. Митюхин

*Учреждение образования «Белорусский государственный университет информатики
и радиоэлектроники», Минск, Республика Беларусь*

Предлагается метод защиты информации посредством маскирования с использованием координатного преобразования. Базовым векторным пространством преобразования служат собственные векторы ковариационной матрицы $\text{cov}(C)$ произвольного 2D снимка изображения C [1]. Информационные данные кодируются псевдослучайными последовательностями (ПСП) низкоскоростного помехоустойчивого кода. В основе метода лежит операция гаммирования значений коэффициентов координатного преобразования и поточного шифра (кода) в виде ПСП. Коэффициенты преобразования следует воспринимать как аддитивный помеховый источник, затрудняющий правильное декодирование кода в канале с подслушиванием. Маска в виде сильно коррелированного изображения после преобразования в базисе собственных функций представляется в виде последовательности некоррелированных коэффициентов [2]. Такое свойство позволяет определять коэффициенты как дискретные случайные величины, распределение которых определяется по всему блоку изображения. Это важно для повышения надежности передачи информации по основному каналу и, соответственно, уменьшения до заданного минимального значения пропускной способности канала утечки. Гаммирование кода и коэффициентов преобразования, представленных в двоичной форме после выполнения операции квантования, осуществляется в поле Галуа с характеристикой 2 ($GF(2)$). В качестве кода использовалась конструкция, полученная комбинированием m -последовательностей. В этом случае возможность восстановления структуры неприводимого примитивного над полем $GF(2)$ полинома кода по правильно принятой последовательности $2k$ информационных символов исключается. Не зная закон кодирования (модуляции) и конкретной маски в виде преобразованного изображения, используемой на определенном временном интервале передачи данных, применить в канале подслушивания оптимальные методы (согласованную или корреляционную фильтрацию) становится проблематичным. Экспериментальные исследования в среде МАТЛАБ показали возможность применения метода на практике.

Список литературы

1. Mitsiukhin A. Proceedings 59th IWK. TU Ilmenau, Band 59, 2017, Heft 2.2.02, 6 Seiten.
2. Jahne B. Digital Image Processing. Concepts, Algorithms, and Scientific Applications. E-BOOK, 2013.