

УДК 004.056.53

ПСЕВДОГОЛОГРАФИЧЕСКАЯ РАЗВЕРТКА ЦИФРОВЫХ ИЗОБРАЖЕНИЙ КАК СРЕДСТВО ЗАЩИТЫ ИНФОРМАЦИИ ПРИ НЕСАНКЦИОНИРОВАННОМ ДОСТУПЕ К ПЕРЕДАВАЕМЫМ ДАННЫМ

Урывская Д.А.

Самарский государственный аэрокосмический университет имени академика С.П. Королёва (национальный исследовательский университет), г. Самара

Введение

Существует целый ряд методов так называемой «псевдоголографической» развертки цифровых изображений [1-4], согласно которой отсчеты исходного изображения преупорядочиваются, формируя новое изображение - «псевдоголограмму», каждый участок которой, подобно физическому аналогу голограммы, содержит достаточно полную информацию обо всем изображении.

Целью данной работы было изучение возможности приложения псевдоголографической развертки цифрового изображения к задачам защиты информации.

Суть метода [1] заключается в том, что двумерный массив точек изображения разворачивается в одномерную последовательность по определенному правилу, так что каждой паре координат (m, n) – точке в двумерном массиве (изображении), ставится в соответствие некоторое число – k , которое и определяет номер данной точки в последовательности развертки. Связь координат (m, n) и k определяется соотношениями:

$$\begin{cases} n = \sum_{i=0}^{N-1} p^{N-1-i} A_X \left(\left[\frac{k}{p^{2i}} \right] \pmod{p^2} \right), & m = \sum_{i=0}^{N-1} p^{N-1-i} A_Y \left(\left[\frac{k}{p^{2i}} \right] \pmod{p^2} \right), \\ A_X(k) = n, & A_Y(k) = m, \end{cases} \quad (1)$$

где $[\cdot]$ означает целую часть числа.

При строчном сканировании и записи полученной последовательности формируется новое изображение, имеющее шумоподобный вид – «псевдоголограмма» [5].



Рисунок 1. Изображение и его псевдоголограмма

Псевдоголографическая развертка характеризуется параметрами: p , N , и правилом нумерации. Если исходное изображение имеет размер $p^N \times p^N$, то правило нумерации задается некоторой матрицей A , которая определяется выбором нумерации элементарного изображения размера $(p \times p)$.

Восстановление зашифрованного изображения при несанкционированном доступе к передаваемым данным

Пусть требуется восстановить переупорядоченное, согласно методу [1], т.е. зашифрованное цифровое изображение – псевдоголограмму, при отсутствии информации о правиле нумерации – секретном ключе шифрования.

