

ШИФРОВАНИЕ КРУГОВЫХ ПАНОРАМНЫХ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ЦИКЛИЧЕСКИХ ПЕРЕСТАНОВОК

О.Дж. Аль-Фурайджи, В.К. Конопелько

Предлагается метод шифрования круговых панорамных изображений на основе циклических перестановок пикселей строк и столбцов. Суть метода состоит в перемешивании пикселей кругового панорамного изображения в результате применения операций циклического сдвига к каждой строке и каждому столбцу кругового панорамного изображения. В качестве ключевых параметров используются номера строк и столбцов, соответствующие им циклические сдвиги по вертикали и горизонтали, а также порядок выборки строк и столбцов. Метод обеспечивает достаточно

высокую криптостойкость за счет применения операций циклически перестановок ко всем пикселям кругового панорамного изображения. При использовании видеокамеры с углом видимости по горизонтали 30° размер панорамного изображения составляет 480×7680 пикселей, что затрудняет применение операции вычисления ключа в результате простого перебора. Особенностью метода является возможность шифрования круговых панорамных изображений как до компрессии, так и после, благодаря сохранению их глобальных статистических свойств в результате циклических перестановок пикселей строк и столбцов.