Image Encryption using Bit Plane Complexity Segmentation Algorithm

Arshdeep Singh 19BCB0086

Shivam Singhal 19BCE2112

Kartik Nahta 19BCE2009

ABSTRACT

This project aims to implement a steganographic system that is able to perform the standard steganographic functions using the Bit-Plane Complexity Segmentation approach. The motivation for the same stems from the immense amount of piracy and multimedia in today's world and we think that such a system has wide ranging implications. At the end of this we have developed a python-based project that is able to encode and decode files into images. The default threshold used is 0.45 but the encryption can be done using custom alpha metrics as well.

Keywords: Information hiding, Steganography, Encryption, Bit plane slicing, complexity

Steganography is the science or art of hide the messages into other sources of information like text/documents, audios, videos and images etc. so that it is not visible to unauthorized users The following picture represents different types of steganographic techniques. The internet allows the ease of spreading information over large areas. This is a blessing as well as a curse as your friends all over the world can view your information but everyone else also can view your information.

Encrypting data is the most popular approach to protect information but the protection can be broken with enough computational power. So, an alternate approach to encrypting data would be to hide it by making this information look like something else. This way only friends would be able to realize its true content. In particular, if some important data is hidden inside of an image, then everyone except your friends would view it as an image. At the same time your friends would still be able to retrieve the true information.

We propose to implement a steganographic system that is able to perform all the standard steganographic functions using the Bit Plane Complexity approach. The disadvantage of Least Significant Bit is that it is vulnerable to steganalysis and is not secure at all and thus we don't plan to use this implementation.