Abstract

In the today’s digital world, the need for powerful steganalysis methods is ever growing because of the vast opportunities for covert communications. There are many robust methods in the literature for quantitative steganalysis of images employing LSB replacement steganography. The error distributions of these methods have fat and lengthy tails owing to extreme outliers. Hence once a steganalist makes estimation, the confidence level he can attach with the result is not very high as he is not sure of which results are accurate and which are inaccurate.

In this thesis we propose the following to make steganalysis of images subjected to LSB replacement steganography more reliable: (i) a new steganalysis method, (ii) a novel image classification method, and (iii) improvements to the two most accurate steganalysis methods in the literature - Sample Pair Method and Least Square Method. All these proposals are based on properties of images which are invariant with embedding. Hence no knowledge about cover image is required for the analysis. Usually steganalysis reveals the flaws in steganographic system and hence leads to better steganography methods. Hence as a consequent result, we also propose, two preprocessing methods for increasing the security of LSB replacement steganography.

The new steganalysis method proposed is more reliable in comparison with the existing methods as it indicates the results it produces are accurate or not. The reliability assessment is done based on certain properties
of images, such as cardinalities and difference in cardinalities of certain pixel groups, which are invariant with embedding. To the best of our knowledge no steganalysis method in the literature gives a confidence interval for the results it produces.

The proposed image classification method for increasing the reliability of steganalysis, classifies images into different classes corresponding to highly accurate, highly inaccurate, and highly probably inaccurate steganalysis results. This helps in attaching a confidence interval to the steganalysis results without the knowledge of cover images.

The proposed suggestions for improving Sample Pair Method and Least Square Method are based on the distribution of cardinalities of certain pixel groups. These suggestions increase the speed and accuracy of the Sample Pair Method. Improved Least Square Method yields almost same accuracy at less computational complexity.

One of the preprocessing methods proposed causes any amount of embedding to be detected as 100% on all images irrespective of the length of embedding which increases confusion in steganalysis and thereby increases security of steganography. The other preprocessing method proposed causes payload upto 50% undetectable. Thus by making use of the second preprocessing method data can be hidden without causing suspicion.

All the proposed methods are evaluated using different image sets downloaded from Internet and another set of 1000 images taken by Nikon Coolpix 8400 camera. The images downloaded include compressed .jpeg
colour images and uncompressed colour images from public image databases. All images are converted to .pnm format and data embedded randomly. All the above proposals are experimentally verified on these different datasets and the results obtained reinforces our findings.