Efficient Hybrid Image Steganography Based on Pattern Matching

Abdul Qadir[1], Mohsin Shah[2], Zakir Khan[3], Toqeer Mahmood[4], Noor Ul Amin[5] ,Abdul Hakeem[6]

Department of Information Technology, Hazara University Mansehra, Pakistan [1,2,3,5,6]

Department of Computer Engineering, University of Engineering and Technology Taxila, Pakistan [4]

Introduction

A new steganographic technique is presented in this paper. This technique is based on the pairs of pixels matched with data bits and hiding the pair number in LSB of the pixel.

Aims and Objectives

The proposed technique improves the hiding capacity over existing techniques with acceptable SNR, RMSE, MSE and UIQI and provides security against statistical attacks.

Proposed Methods

Data Embedding

Secret information bits are divided into chunks of two bits each. Pairs of each pixel are defined as pair number 3 (1, 1), pair number 2 (1, 0), pair number 1 (0, 1), pair number 0 (0, 0). For every pixel, pair 3 represents the bits (7, 6), pair 2 represents the bits (6, 5), pair 1 represent the bits (5, 4) and pair 0 represent the bits (4, 3).

Compare the pairs with data bits and write the pair number into 2-LSB of the pixel.

Data Extraction

The receiver extracts information bits from stego image by separating the 2-LSB of the pixels, and define the pairs accordingly. Data chunk are extracted from the relevant pairs of the respective pixel. Evaluating all the data chunks and obtaining the secret message which is embedded at sender side.

Results

Four standard test images are used for the implementation of this technique. The specifications of these image are: Grey level Lenna & Baboon 512x512; Color Lenna & Baboon 512x512x3.

The resultant stego images for the above four cover images produced are shown in Figure. The changes in stego image are un-detectable. The resultant stego images show that the proposed technique hides a high capacity of information in the cover image with improved signal to noise ratio and the high robustness against the stastical attacks.

Conclusion

Pattern matching LSB based technique is presented in this work. The secret data bits are arranged in pairs of two and similarly bits representing pixels are also arranged in pairs. The technique embeds high payload of information with significant signal to noise ratio.

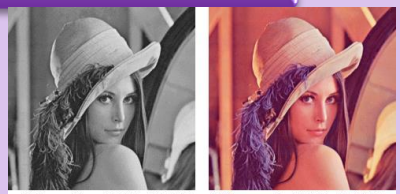
Acknowledgement

The technique presented in this paper was clarified by discussion with Mohsin Shah, Zakir Khan, Muhammad Naeem, Noor Ul Amin and Arif Iqbal. We are thankful to IT Lab of Hazara University Pakistan.

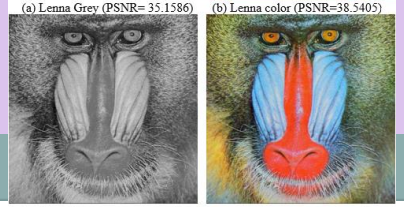
Images	Lenna Grey	Baboon Grey	Lenna Color	Baboon Color
MSE	19.82	21.1	9.09	9.54
RMSE	4.45	4.59	3.01	3.08
UIQI	0.77	0.94	0.84	0.96
SNR	11.09	10.81	14.47	14.26
MAE	2.86	2.99	2.09	2.14
PSNR	35.19	34.92	38.57	38.36
AD	0.3	0.5	0.3	0.4
MD	15	15	15	15
NAE	0.02	0.02	0.01	0.01
Cap	524288	524288	1572864	1572864

Stego Images Results

Stego Images



(a) Lenna Grey (PSNR= 35.1586) (b) Lenna color (PSNR=38.5405)



(c) Baboon Grey (PSNR=34.8879) (d) Baboon color (PSNR=38.3337)