International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Secure and Improvised Edge Based Steganograghy

Ramya N [1], Shamna N V[2]

[1]Department Electronics and Communication Engineering (M. Tech DCN)

[2]Guide/Assistant Professor, Department ECE,PA College of Engineering, Mangalore , India

Abstract: ***In this steganography technique, where edges in the cover image have been used to embed messages. Amount of data to be embedded plays an important role on the selection of edges, i.e., the more the amount of data to be embedded, larger the use of weaker edges for embedding. Experimental results have shown that the proposed technique performs better or at least at par with the state-of-the-art steganography techniques but provides higher embedding capacity.***

Keywords: Steganography; Steganalysis; Information hiding; Edge detection

1. Introduction

Steganography is an art of secure transmission of messages from a sender to a receiver. It should ensure that no one can reliably conclude on the secret communication between the sender and the receiver. To achieve such a secrecy, the message is hidden in some cover media which may not raise any suspicion on the possibility of carrying the secret message to the third party. Embedding introduces distortion in the cover medium. The embedding distortion in visual and statistical properties of the cover mediummay lead steganographic detectability. The objective of any steganographic technique is to preserve these properties while embedding the message in the cover media.

Images are preferred medium for the current steganography techniques. Content adaptability, visual resilience,and smaller size of images make them good carrier to transmit secret messages over the internet. There exists a large number of image steganography techniques which are accompanied by various attacks on the steganography systems. Security of any steganography technique depends on the selection of pixels for embedding. Pixels in noisy and textured area are better choice for embedding because they are difficult to model. Pixels in edges can be seen as noisy pixels because their intensities are either higher or lower than their neighboring pixels due to sudden change in the coefficient gradient. Due to these sharp changes in the visual and statistical properties, edges are difficult to model in comparison to pixels in smoother area. Therefore, edges make a better option to hide secret data than any other region of an image where a small distortion is much more noticeable.

2. Literature Survey

[1]. In an embedding technique, known as pixel value difference technique (PVD) has been proposed. In this technique, the image is divided into non-overlapping blocks of adjacent pixels which are randomly selected, and data is embedded into each of its pixels. The amount of data embedded, i.e., the number of last significant bits used, is directly proportional to the differences in the intensities of adjacent pixels. This uneven embedding in PVD leads to unusual steps in the histogram of pixel difference in the stego image. An improved technique (IPVD), proposed in [22], has exploited this vulnerability.

[2] Adaptive edge LSB technique (AE-LSB) [23] has also removed this uneven pixel difference by introducing a readjusting phase and has provided better capacity. All these techniques are edge adaptive in a way that they can embed more data where pixel difference is high but they have one fundamental limitation. These techniques consider pixel pair at random, rather than selecting on the basis of higher differences. So, they may end up by embedding data at random places in the image and by distorting the texture in LSB plane of the image. Performance of these techniques are found to be poor [4].

[5] In, embedding distortion cost is computed through directional residual obtained using Daubechies wavelet filter bank [6]. The objective is to limit the embedding changes to those parts of the cover image that are difficult to model in multiple directions. Embedding is donein textures or noisy parts and avoiding smooth regions and clean edges of empirical cover images. Distortion function, called as UNIWARD [6],is used to compute delectability map. Syndrome trellis code (STC) [7] and detectability map are used to embed payload while minimizing the embedding distortion. The same distortion design technique can be used for spatial and transform domains.

3. Steganographic System

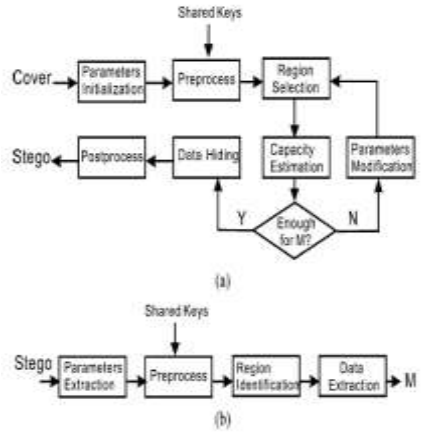

Figure 1: Steganographic System (a) Data Embedding (b) Data Extraction

The flow diagram of our proposed scheme is illustrated in Ftig. 1. In the data embedding stage, the scheme first

initializes some parameters, which are used for subsequent data preprocessing and region selection, and then estimates the capacity of those selected regions. If the regions are large enough for hiding the given secret message, then data hiding is performed on the selected regions. Finally, it does some post-processing to obtain the stego image. Otherwise the scheme needs to revise the parameters, and then repeats region selection and capacity estimation until can be embedded completely. Please note that the parameters may be different for different image content and secret message . We need them as side information to guarantee the validity of data extraction. In practice, such side information (7 bits in our work) can be embedded into a predetermined region of the image.

In data extraction, the scheme first extracts the side information from the stego image. Based on the side information, it then does some preprocessing and identifies the regions that have been used for data hiding. Finally, it obtains the secret message according to the corresponding extraction algorithm. In this we apply such a region adaptive scheme to the spatial LSB domain. We use the absolute difference between two adjacent pixels as the criterion for region selection, and use LSBMR as the data hiding algorithm. The details of the data embedding and data extraction algorithms are as follows.

Two parameters that will be studied in depth and improvised are: Embedding capacity and image quality. Further, a security scheme can be used such as the RC6 or AES to encrypt the data before embedding. Moreover, a verification environment will be written to automatically test the RTL model of the steganographic system. The RTL design and its test bench are shown in Fig. 2.

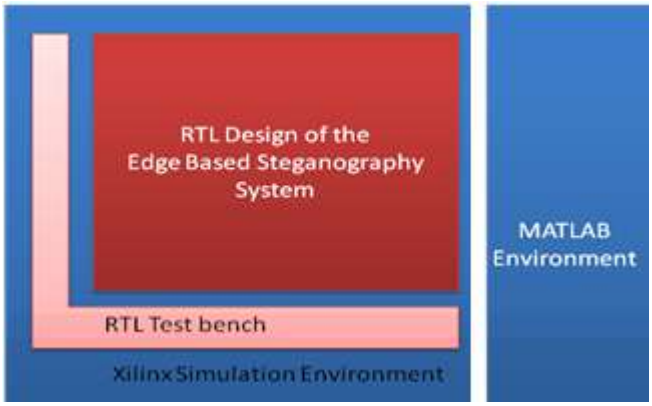

Figure 2: Environment setup for design and analysis of the steganographic system

Advantages

- Data is hidden at the edges of the cover image, and the edges are dynamically selected based on the length of the message
- uses two-bit LSB substitution for embedding.

Disadvantages

- it does not discriminate between smooth areas and the edges in an image causing some distortion in LSB plane of stego image.
- It fails to discriminate between prominent edges and smothered area for a given threshold.

4. Experimental Results

The proposed technique has been tested on BOSS bas database ver. 1.01 and BOWS2 database. Each database contains 10,000 8-bit gray scale images with size of 512 × 512.Images of BOSS base taken from eight different cameras, resized and uncompressed. Secret message is randomly generated by a pseudo random number generator (PRNG) to simulate encryption of the secret message. For experimental purpose, payload is taken to be 10% bits per pixel (bpp) of the cover image to show the effectiveness of the proposed technique.

In both databases, the total number of pixels belonging to edges is found to be less than 10%.Further, the technique is also analyzed for variable payload and for the best threshold and width of the Gaussian filter. It is compared with LSBM, existing edge adaptive techniques HBC and EALMR, and minimizing distortion-based techniques HUGO and S-UNIWARD.The steganographic security is evaluated against visual, structural, and blind steganalysis attacks.Fully implemented steganography system using Verilog in Xilinx Design Suite.

5. Conclusion

In technique for steganography in gray scale images has been proposed.Data is hidden at the edges of the cover image, and the edges are dynamically selected based on the length of the message.The proposed technique can resist visual, structural, and non-structure attacks better than the existing edge-based techniques.HBC is detected by structural detectors due to anomalies created by LSB substitution.

References

[1] D-C Wu, W-H Tsai, A steganographic method for images by pixel-value differencing. Pattern Recogn. Lett.
[2] X Zhang, S Wang, Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. Pattern Recogn. Lett.
[3] C-H Yang, C-Y Weng, S-J Wang, H-M Sun, Adaptive data hiding in edge areas of images with spatial LSB domain systems. IEEE Trans. Inf. Forensics Security
[4] W Luo, F Huang, J Huang, Edge adaptive image steganography based on LSB matching revisited. IEEE Trans. Inf. Forensics Security.
[5] V Holub, J Fridrich, Digital image steganography using universal distortion.Paper presented at the first ACM workshop on information hiding and multimedia security, Montpellier, France
[6] T Filler, J Judas, J Fridrich, Minimizing additive distortion in steganography
[7] S Islam, P Gupta, Revisiting least two significant bits steganography. Paper presented a the 8th international conference on intelligent information processing (ICIIP), Seoul, Republic of Korea

[8] MR Modi, S Islam, P Gupta, ed. by D-S Huang, V Bevilacqua, JC Figueroa,and P Premaratne, Edge based steganography on colored images
[9] C Cortes, V Vapnik, Support-vector networks. Mach. Learn.
[10] T Pevný, JJ Fridrich, AD Ker, From blind to quantitative steganalysis.
[11] K Hempstalk, Hiding behind corners: using edges in images for better steganography. Paper presented at the second computing women congress (CWC), Hamilton, New Zealand S Dumitrescu, X Wu, N Memon, On steganalysis of random LSB embedding in continuous-tone images. Paper presented at the international conference on image processing, Rochester,
[12] AD Ker, R Böhme, Revisiting weighted stego-image steganalysis. Paper presented at the SPIE electronic imaging, security, forensics, steganography, and watermarking of multimedia xontents X, Orlando, FL,
[13] S Tan, B Li, Targeted steganalysis of edge adaptive image steganography based on LSB matching revisited using b-spline fitting. IEEE SignalNProcess.
[14] RO Duda, PE Hart, DG Stork, Pattern Classification,
[15] G Gul, F Kurugollu, ed. by T Filler, T Pevný, S Craver, and A Ker, A new methodology in steganalysis: breaking highly undetectable steganography .

.