Advances and Applications in Mathematical Sciences
Volume 20, Issue 11, September 2021, Pages 2775-2780
© 2021 Mili Publications

A STEGANOGRAPHY SYSTEM WITH GAUSIAN MARKOV RANDOM FIELDS AND ERROR DETECTION CODES

B. VENKATA RAMANA REDDY[1], NAGESHBABU DASARI[2] and K. VENKATESWARARAO[3]

[1]Professor, Department of CSE
KSRM College of Engineering
Kadapa, A.P., India
E-mail: drbvrreddy@ksrmce.ac.in

[1,2]Research Scholar, JNTUA
Ananthapuramu, A.P., India
E-mail: dasarinagesh@gmail.com
vrkatevarapu@gmail.com

Abstract

In the current scenario, the usage of digital data is demanded by the users. So, the security should be provided for the digital data. In this regard, the researchers are majorly focusing on the information security mechanisms. Among various mechanisms of information security, multimedia based methods are found to be prominent. For multimedia data, the traditional cryptographic algorithms are failed. Hence, to provide the efficient algorithms for multimedia information security, steganography algorithms are widely used. So, the present paper proposes a novel approach for steganography system by using Gaussian Markov models. The proposed algorithms also use the error detection codes for providing the additional security features. The results of the algorithms indicate the efficiency of the proposed algorithm.

I. Introduction

Presently, the steganography is one of the widely focuses research area due to its importance to the security for the data. It is found that the statistical models [1] are very prominent to detect the regions in the image for providing efficient algorithms. These algorithms uses payload as additional information to be maintained by the input for detection of error. These algorithms use the expressions in closed form [2]. The image

2010 Mathematics Subject Classification: 68Wxx.
Keywords: Parity; Stego Image; Cover Image and Sampling.
Received October 5, 2020; Accepted October 26, 2020

steganography [3] can be performed on the spatial and frequency domains. The spatial domain techniques need to be adopted with hierarchical methods and are not suitable for lossy compressed images where as the frequency domain based methods can be used for lossy compressed images also as efficiently.

During the steganography process, among the given set of input images, ranks will be allocated by using the ranking algorithm. The ranking algorithm [4] uses the matching algorithm which gives the high matching score. The algorithm is well suitable for lossy compressed images. The Genetic Algorithm [5] is well suitable for the optimizing the ranking process by using transform domain techniques. In general, in the transform domain, the crossovers will be used to identify the prominent region of interest in the input image.

The crop operation [6] is also used for decomposing the input image into multiple layers and then the steganography can be performed at selective layers and then the grouping operation will be performed to group all the layers into a single stego image.

The Random Key Matrix [7] will be used for reordering the pixels into a new pattern for performing the steganography process. This will introduce the security at multiple layers identified by the random key matrix. The Data Encryption Standard (DES) [8] is also found to be prominent for the steganography algorithm. The DES algorithm provides high security to the input image at multiple levels. The cryptography can be blended with the steganography to provide security for multiple bits [9] in the input image. With this, the security can be provided for lossless images. The message can be blindly introduced into the input image file with reversible algorithm [10]. The shifting operation and logical XOR operation are found to be prominent for image steganography [11]. The Elliptic Curve Cryptography [12] can be used for double encryption process in the image steganography. The two Least Significant Bits [13] can be used for performing lossy compression based image steganography. The random steganography [14] method includes the partitioning algorithm based on quadtree partitioning. These algorithms are used for developing the lossless steganography algorithms. The maximum flow algorithms [15] are used for solving the linear programming problem of image steganography.

The present paper is organized into five sections. The section 1 gives the introduction to the image steganography, section 2 gives the methodology of the present paper, the section 3 gives the results and discussions and section 4 gives the conclusions of the proposed algorithm.

II. Methodology

The present paper presents an approach for Steganography System with Gausian Markov Random Fields and Error Detection Codes. The steganography algorithm is majorly depends on the selection of the key regions in the input image. The steganography process includes the embedding procedure which will embed the input message into the cover image. After the steganography, the stegao image will be generated which should be identical to the input cover image.

For this, the present paper focuses on the selection of the key regions by using the Gaussian Markov Random Fields. With these models, the steganography systems will be represented with suitable simple expressions.

$$p(I_{ij} \mid I_{k,l}(k, l) \in N_{ij}) = \frac{1}{\sqrt{2 \Pi \sigma^2}} e^{\left[\frac{\left(I_{ij} - \sum_{l=1}^{n} \alpha_l \times S_{kl,j}\right)^2}{2\sigma^2}\right]}. \tag{1}$$

The present paper uses the parity based error detection codes for providing the additional security mechanism to the steganography system. The algorithm of the proposed methodology is

1. Read the input cover image

2. Read the message

3. Append the even parity bits for the message

4. Apply the 3rd neighborhood Gaussian Markov Random Field for identifying the region of interest in the cover image

5. Embed the even parity based message in to the selected ROI of the image in the spatial domain.

III. Results and Discussions

The present algorithm uses the Gaussian Markov Random Fields for selection of the Region of Interest. The Figure 1 shows the result of identified ROIs of the input image.

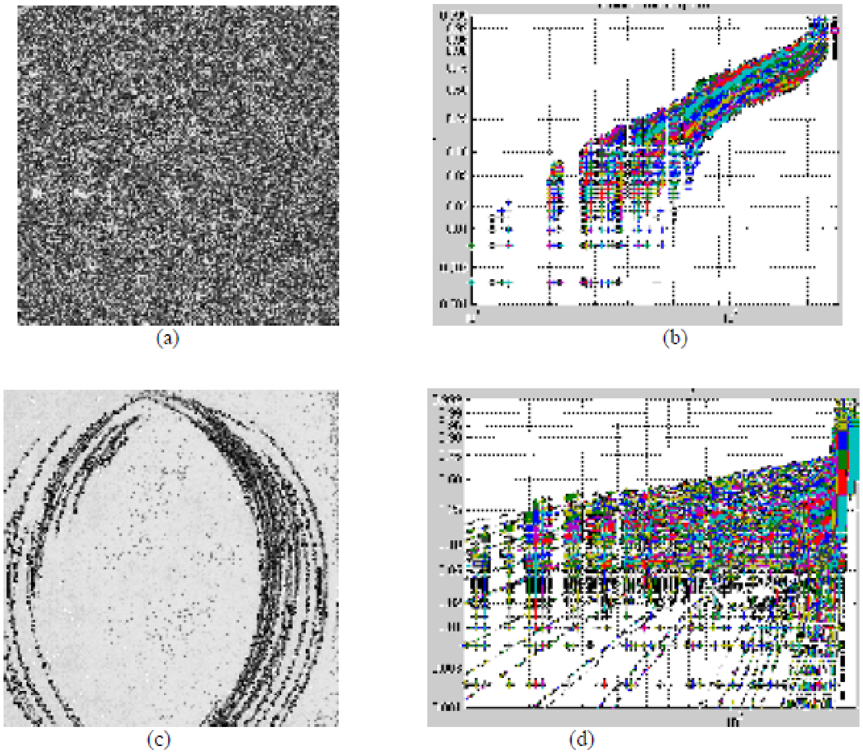

Figure 1. (a) Input Image 1 (b) ROI plot of Image 1 (c) Input Image 2 (d) ROI plot of Image 2.

In the selected ROIs, the secret message along with the even parity bit will be embedded with the Lease Significant Bit (LSB) technique. The results are shown in Figures 2 and 3.

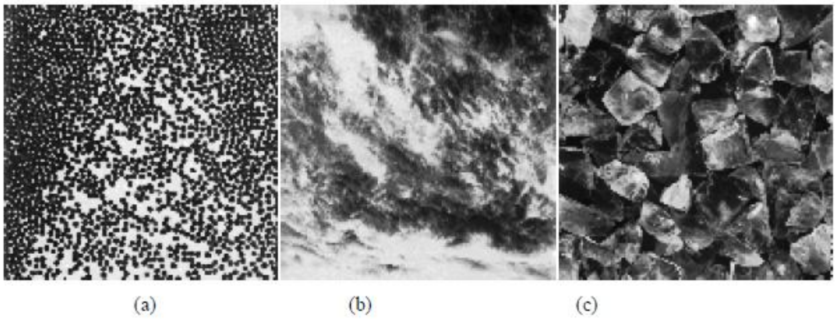

Figure 2. (a) Cover Image 1 (b) Cover Image 2 (c) Cover Image 3.

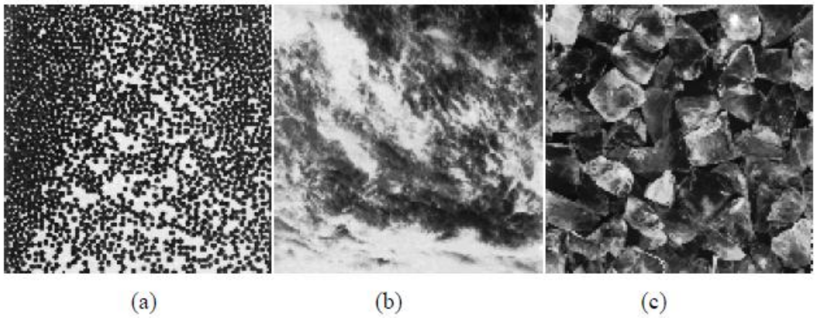

Figure 3. (a) Stego Image 1 (b) Stego Image 2 (c) Stego Image 3.

IV. Conclusions

Steganography is widely used in multimedia information security field. The present paper proposes a novel approach for steganography system by using Gaussian Markov models. The proposed algorithms also use the error detection codes for providing the additional security features. The results of the algorithms indicate the efficiency of the proposed algorithm.

References

[1] M. Sharifzadeh, M. Aloraini and D. Schonfeld, Adaptive Batch Size Image Merging Steganography and Quantized Gaussian Image Steganography, in IEEE Transactions on Information Forensics and Security 15 (2020), 867-879. doi: 10.1109/TIFS.2019.2929441.

[2] K. Alla and R. S. R. Prasad, A New Approach to Hindi Text Steganography Using Matraye, Core Classification and HHK Scheme, 2010 Seventh International Conference on Information Technology: New Generations, Las Vegas, NV, 2010, pp. 1223-1224, doi: 10.1109/ITNG.2010.162.

[3] D. Watni and S. Chawla, A Comparative Evaluation of Jpeg Steganography, 2019 5th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, India, 2019, pp. 36-40, doi: 10.1109/ISPCC48220.2019.8988383.

[4] M. Juneja and P. S. Sandhu, Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption, 2009 International Conference on Advances in Recent Technologies in Communication and Computing, Kottayam, Kerala, 2009, pp. 302-305, doi: 10.1109/ARTCom.2009.228.

[5] J. K. Mandal and A. Khamrui, A Genetic Algorithm based steganography in frequency domain (GASFD), 2011 International Conference on Communication and Industrial Application, Kolkata, West Bengal, 2011, pp. 1-4, doi: 10.1109/ICCIndA.2011.6146670.

[6] K. A. Al-Afandy, O. S. Faragallah, A. Elmhalawy, E. M. El-Rabaie and G. M. El-Banby, High security data hiding using image cropping and LSB least significant bit steganography, 2016 4th IEEE International Colloquium on Information Science and Technology (CiSt), Tangier, 2016, pp. 400-404, doi: 10.1109/CIST.2016.7805079.

[7] Anurag and S. Meena, Color Image Steganography Using Random Key Matrix," 2018 3rd International Conference for Convergence in Technology (I2CT), Pune, 2018, pp. 1-5, doi: 10.1109/I2CT.2018.8529425.

[8] M. K. Ramaiya, N. Hemrajani and A. K. Saxena, Improvisation of Security Aspect in Steganography Applying DES, 2013 International Conference on Communication Systems and Network Technologies, Gwalior, 2013, pp. 431-436, doi: 10.1109/CSNT.2013.96.

[9] R. S. Phadte and R. Dhanaraj, Enhanced blend of image steganography and cryptography, 2017 International Conference on Computing Methodologies and Communication (ICCMC), Erode, 2017, pp. 230-235, doi: 10.1109/ICCMC.2017.8282682.

[10] J. A. R. Kazi, G. N. Kiratkar, S. S. Ghogale and A. R. Kazi, A novel approach to Steganography using pixel-based algorithm in image hiding, 2020 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2020, pp. 1-6, doi: 10.1109/ICCCI48352.2020.9104072.

[11] K. Joshi and R. Yadav, A new LSB-S image steganography method blend with Cryptography for secret communication, 2015 Third International Conference on Image Information Processing (ICIIP), Waknaghat, 2015, pp. 86-90, doi: 10.1109/ICIIP.2015.7414745.

[12] Y. Manjula and K. B. Shivakumar, Enhanced secure image steganography using double encryption algorithms, 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi (2016), 705-708.

[13] O. Khalind and B. Aziz, Single-mismatch 2LSB embedding steganography, IEEE International Symposium on Signal Processing and Information Technology, Athens, 2013, pp. 000283-000286, doi: 10.1109/ISSPIT.2013.6781894.

[14] J. Kumar, A novel approach to image steganography using quadtree partition, 2016 2nd International Conference on Next Generation Computing Technologies (NGCT), Dehradun, 2016, pp. 93-98, doi: 10.1109/NGCT.2016.7877396.

[15] L. Wanqi, N. Che, J. Ren and H. You, Histogram-Preserving Steganography Using Maximum Flow Algorithms, 2011 Second International Conference on Digital Manufacturing & Automation, Zhangjiajie, Hunan, 2011, pp. 590-593, doi: 10.1109/ICDMA.2011.147.