Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.9854912

IMAGE STEGANOGRAPHY USING FAST DISCRETE CURVELET TRANSFORMATION FOR SECURE COMMUNICATION

Saleem S Tevaramani[1], Ravi J[2]
[1]Research Scholar, Dept. of ECE, Global Academy of Technology Bangalore 560098
[1]Assistant professor, Dept. of ECE, KSIT Bangalore 560109
[2]Professor, Dept. of ECE, Global Academy of Technology Bangalore 560098
Email id: saleemstevaramani@gmail.com

ABSTRACT–The Recent advancements in digital technology have made it possible for us to share a massive volume of files over the internet. However, the security and integrity of such crucial files become the highest concern in the presence of hostile attackers. The security of these files across the internet is ensured through steganography. Steganography is the art of encoding and embedding secret data in cover file in such a manner so as not to be suspicious for eavesdropper. The aim of the paper is to provide security for the communication between two entities. The cover image is preprocessed; Pixel Value Adjustment (PVA) and Bit Plane Slicing (BPS) are applied to choose the average of four Most Significant Bits (MSB) of Cover Image (CI). The secret image is preprocessed, BPS techniques is applied to choose average of four MSB bits and Forward Discrete Curvelet Transformation (FDCT) is applied on it. The approximation curvelet coefficient i.e., magnitude is embedded in Least Significant Bit (LSB) of CI to produce stego image (SI). The histogram of SI and CI is measured to verify the difference between them. The quality result parameters such as Mean Square Error (MSE) and Peak signal to Noise Ratio (PSNR) are measured, which proves the chance of hidden information being detected is reduced.

Keywords: steganography, Bit Plane Slicing, curvelet transformation, PSNR, MSE.

1. INTRODUCTION:

The word steganography is originated from two greek words “stegano” means cover and “graphia” means writing, it is covered writing [1]. Steganography's primary goal is to communicate secret information [2] in a way that makes it undetectable to unauthorized users [3]. Each and every one need internet for digital communication [4] and it is challenging to secure [5] the confidential information [6] over the insecure channel and network [7]. Cryptography protects the information and allows using it only for the intended beneficiary [8]. The information hiding technique, steganography is introduced to safeguard the confidential information [9] within the carrier media such as audio, video and image for various applications. The confidential information is concealed and shared in a secure manner using steganography [10]. The classification of data hiding techniques such as reversible and irreversible is introduced. The information is hidden into an image called cover image (CI) and the image in which confidential information is hidden is called stego-image (SI).

The biometric trait is utilized for the identification of human being. Steganography maintains the anonymity and privacy of the biometric data. The main challenge of designing the steganography system is to provide robustness, high embedding data rate and security.

A. Contribution: In this paper, Fast Discrete Curvelet transformation technique based image steganography using BPS and MSB is proposed.

B. Organization: Section II is Related work; Section III is the proposed steganography technique. Section IV and section V results analysis and conclusion.

2. RELATED WORK:

K.S. Seethalakshmi [11] proposed visual cryptography and neural networks. The data is encrypted using AES algorithm. Neural network and LSB is used to embed. S. Bukhari, M. S. Arif [12] proposed the information protection in wireless channel. The embedding of the data is achieved using LSB; the image is divided into blocks whose size is 8*8. R. Das and I. Das [13] presented an enhanced safe data transfer scheme in smart Internet of Things (IoT) devices such as home server & cloud server. A. Gambhir and S. Khara [14] proposed the data encryption using RSA algorithm. Using LSB the encrypted data is hidden inside audio file.R. Indrayani, H. A. Nugroho [15] proposed the Mp3 file as a cover file. The confidential information is encrypted using AES algorithm and MD5 hash function. N. Patel and S. Meena [16] uses space domain steganography . One image is embedded into another image using a key as a seed pseudo random number. K. Joshi and R. Yadav [17] proposed the encryption of secret message using Vernam cipher and data is embedded using LSB. The authors used grayscale images.V. Shanna and Madhusudan [18] proposed the S-DES algorithm to encrypt the secret message to produce an array. XOR operation is used to embed the data. M. Mukhedkar, P. Powar and P. Gaikwad [19] used blowfish algorithm to encrypt the image to cipher image. Then the encrypted image is embedded using LSB technique in the cover image.

Jing-Ming Guo and Thanh Nam Le [20], measured the quality factor of JPEG images by maintaining quantization tables and performed some permutations along with this scheme to transmit a hidden file.

Kamal deep Joshi and Rajkumar Yadav [21] combined cryptography with steganography by first encrypting a message using Verna cipher and then embedding it with an image using LSB technique with shifting.

Seetha Lakshmi et al. [22] implemented neural networks to identify best locations in the host image to embed the secret data.

Nikhil Patel and Shweta Meena [23] superimposed dynamic cryptography with steganalysis. The LSB of the picture element is modified with the MSB of it and pixel selection is done using pseudo random numbers.

May H [24], proposed the combined image steganography with cryptography. Both encryption and decryption are done using RC4 stream cipher and a hash function along with RGB pixel shuffling are used for steganalysis.

A.A.A. El-Latif, B. Abd El Atty [25] proposed two quantum image hiding strategies. A steganography quantum approach is proposed to hide an image in another image file. Secondly, a quantum watermarking approach is used to hide a water-marked gray image to a carrier image.

Z. Qu, Z. Cheng et al [26] proposed a quantum steganography approach using matrix coding for color images.

2.1 Curvelet Transformation:

Discrete Wavelet Transformation (DWT) is a tool for complex mathematical analysis, but has directionality limitations. Traditional wavelets are not suitable for localizing edge regularities. An anisotropic geometric transform called "ridgelet" was introduced in 1999 by Candes and Donoho [27, 28] for optimal representation of straight-line and surface singularities. However, the real-time problems/applications rarely exhibit straight line singularities rather than curved lines. To analyze a curve or a local line, one way is to split the image into numerous blocks and then use the ridgelet transform. The block based ridgelet transform is called as curvelet transform, which was developed by Candes and Donoho [29].

The Curvelet transforms of the first generation have considerable restrictions due to the blocking effect, since they require subdividing the image into numerous blocks and applying the ridgelet transform to each block. The geometry of ridgelet is ambiguous, as they are not a legitimate ridge function in digital images.

To address these issues, a second generation of the curvelet transform, referred as the Fast Discrete Curvelet Transform (FDCT) was introduced in [30, 31]. This FDCT approach is simple, faster and less redundant than the first-generation curvelet transform.

$$c(j,l,k) = \sum_{0 \le t_1,t_2 < n} f(t_1,t_2)\phi_{j,k,l}(t_1,t_2) \ldots\ldots (1)$$

Where $c(j,l,k)$ are obtained curvelet co-efficient at scale$j$, orientation l and spacing k. $f(t_1,t_2)$ is an input Cartesian array. $\phi_{j,k,l}$ is a digital curvelet transform also called mother curvelet.

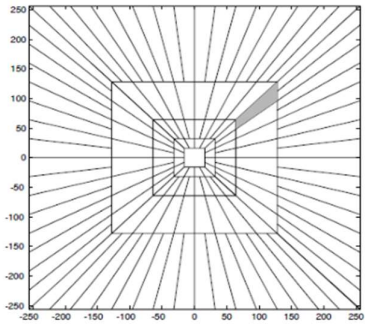

Figure1. Concentric squares tiling into wedges. (Shaded area represents a

3. Proposed Model:

The proposed model of the image steganography is as shown in Figure2. The Model consists of CI, PI and FDCT to generate the stego Image.

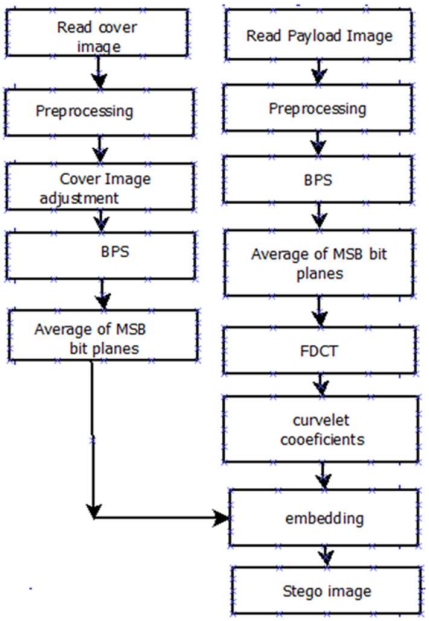

Figure 2: Proposed model of image steganography

3.1 Secure Communication:

Referring to computer-mediated communication, communication is referred as the means of sending and receiving information, specifically from one computer or device to another [32]. In the context of this dissertation, secure communication is defined as sending and receiving information with the certainty that the information remains safe and protected against attacks [33]. The Blocks of Figure 2 is explained as below [34-40].

Cover Image (CI): an image that can hide information.

Payload Image (PI): Actual information that can be concealed in images.

Stego Image (SI): an image with secret information.

Pixel Value Adjustment (PVA): if the pixel value of CI is 255 then subtract it from 15.

Bit Plane slicing (BPS): The image is divided into eight bit planes.

Fast Discrete Curvelet Transformation (FDCT): FDCT is applied on preprocessed payload image to get approximation coefficient to get magnitude.

Embedding: The average of Four MSB bit planes is embedded in the preprocessed CI.

4. **RESULT:** The result analysis is depicted in table1 using the proposed algorithm for secure communication [41-47] and the formula used for Mean Squared Error (MSE) and PSNR [48-52] is shown in equation 2 ,3 and 4 respectively. Images are used for testing [52,53].

$$\mathrm{MSE} = \left[\frac{1}{\mathrm{R}*\mathrm{C}}\right] \sum_{\mathrm{i}=1}^{\mathrm{M}} \sum_{\mathrm{j}=1}^{\mathrm{N}} (\mathrm{SI} - \mathrm{CI})^2 \ldots (2)$$

$$\mathrm{PSNR} = 20\log\left[\frac{(2^{\mathrm{k}}-1)}{\sqrt{\mathrm{MSE}}}\right] \ldots\ldots (3)$$

Where, k is the number of bits required to represent the pixel

for 8-bit grayscale image, PSNR is calculated using equation 4

$$\mathrm{PSNR} = 20\log\left[\frac{255}{\sqrt{\mathrm{MSE}}}\right] \ldots\ldots\ldots (4)$$

Table1. Result analysis.

CI	PI	MSE	PSNR
Horse	Hoverflies	0.2378	60.60
Town Hall Avenue	Tower Bridge	0.2257	61.06
Girl	Fruits	0.1853	62.77
Lena	Airplane	0.186	62.74
Airplane	Lena	0.176	63.19
Cameraman	Barbara	0.1775	63.14
Barbara	Butterfly	0.1611	63.99
Baboon	Zelda	0.1556	64.29
Hoverflies	Horse	0.137	65.36
Arctichare	Goldhill	0.1291	65.90
Mandrill	Lighthouse	0.1218	66.41

Barbara	Goldhill	0.1174	66.73
Cameraman	Cheetah	0.1167	66.79
Circuit	Coins	0.0732	70.83
Lettuce	common ivy	0.0591	72.70
Lena	Kingfisher	0.0402	76.04

Table1. Shows the MSE, PSNR value of color & grayscale CI and color &grayscale PI.

The cover image Horse and the Hoverflies as PI is taken for testing. The PSNR obtained is 60.60; the MSE is 0.23, respectively.

The cover image Lena and the PI as kingfisher is taken for testing. The PSNR obtained is 76.04; the MSE is 0.04, respectively.

Result comparison:

Table2. Result comparison

Authors	**PSNR**
M. A. Hameed et al [33]	36.32
Avi Gupta et al [6]	45.11
Youmin Xu et al [9]	46.71
Kamaldeep Joshi [21]	60.36
Proposed	76.04

V. CONCLUSION:

This paper is providing the information security during the communication. The cover image is preprocessed; PVA and BPS techniques are applied to choose the average of four MSB bits of CI. The secret image is preprocessed, BPS techniques is applied to choose average of four MSB bits and FDCT is applied on it. MSE and PSNR are measured, PSNR achieved from the proposed technique is 76.04.

REFERENCES

1. Mohamad Barakat, ZiadAlqadi, image transformation to increase the security level of lbs method of data steganography, International Journal of Engineering Technology Research & Management, vol. 6, issue 1, pp. 42-53, 2022.
2. Taha, Mustafa Sabah, et al. "High payload image steganography scheme with minimum distortion based on distinction grade value method." Multimedia Tools and Applications pp.1-34, 2022.
3. Mohamad K Abu Zalata, Mohamad T Barakat, Ziad A Alqadi, Carrier Image Rearrangement to Enhance the Security Level of LSB Method of Data Steganography, International Journal of Computer Science and Mobile Computing, vol. 11, issue 1, pp. 182 – 193, 2022.
4. Hadad, Abbas Abd-Alhussein,. "A Robust Color Image Watermarking Scheme Based on Discrete Wavelet Transform Domain and Discrete Slantlet Transform Technique." Journal homepage,pp. 313-319,2022.
5. Hatim Ghazi Zaini and Ziad A. Alqadi Mohammad S. Khrisat, Adnan Manasreh, cover image rearrangement to secure lsb method of data steganography, Journal of Engineering and Applied Sciences, vol. 17, issue 3, pp. 294-302, 2022.

6. Avi. Gupta, H. Shukla, and M. Gupta, "A Secure Image Steganography using X86 Assembly LSB," NEU Journal for Artificial Intelligence and Internet of Things, vol. 1, no. 1, pp. 38-47, 2022.
7. Mohammad S. Khrisat Prof. ZiadAlqadi, Enhancing LSB Method Performance Using Secret Message Segmentation, International Journal of Computer Science and Network Security, vol. 22, issue 7, pp. 1-6, 2022.
8. Ghanavati, Mandana, and Navid Shad Manaman. "An efficient automatic curvelet-contourlet fault detection method using fuzzy entropy." journal of seismic exploration 31, no. 3:pp. 219-238, 2022.
9. Youmin Xu, Chong Mou, Yujie Hu, Jingfen Xie, Jian Zhang, Robust Invertible Image Steganography, Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), pp. 7875-7884,2022.
10. Saleem S Tevaramani, Ravi J, Image steganography performance analysis using discrete wavelet transform and alpha blending for secure communication, Global Transitions Proceedings, Volume 3, Issue 1, ISSN 2666-2857, Pp.208-214,2022.
11. K.S. Seethalakshmi, B Usha and K.N Sangeetha, "Security Enhancement in Image Steganography Using Neural Networks and Visual Cryptography", *IEEE Int. Conf. Computation System and Information Technology for Sustainable Solutions (CSITSS)*, 2016.
12. S. Bukhari, M. S. Arif, M.R. Anjum and S. Dilbar, "Enhancing security of images by Steganography and Cryptography techniques", *IEEE Int. Conf. Innovative Computing Technology (INTECH)*, 2016.
13. R. Das and I. Das, "Secure Data Transfer in IoT environment: adopting both Cryptography and Steganography techniques", *IEEE Int. Conf. on Research in Computational Intelligence and Communication Networks (ICRCICN)*, 2016.
14. A. Gambhir and S. Khara, "Integrating RSA Cryptography & Audio Steganography", *IEEE ICCCA*, 2016.
15. R. Indrayani, H. A. Nugroho, R. Hidayat and I. Pratama, "Increasing the Security of MP3 Steganography Using AES Encryption and MD5 Hash Function", *International Conference on Science and Technology- Computer (ICST)*, 2016.
16. N. Patel and S. Meena, "LSB Based Image Steganography Using Dynamic Key Cryptography", *International Conference on Emerging Trends in Communication Technologies (ETCT)*, 2016.
17. K. Joshi and R. Yadav, "A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication", *IEEE ICIIP*, 2015.
18. V. Shanna and Madhusudan, "Two New Approaches for Image Steganography Using Cryptography", *IEEE Int. Conf. Image Information Processing*, 2015.
19. M. Mukhedkar, P. Powar and P. Gaikwad, "Secure non-real- time image encryption algorithm development using cryptography & Steganography", *IEEEINDICON*, 2015.
20. Jing-Ming Guo and Thanh Nam Le, "Secret Communication using JPEG Double Compression", IEEE Signal Processing Letters, Vol. 17, No. 10, pp. 879-882, 2010.
21. Kamal deep Joshi and Rajkumar Yadav, "A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication", Proceedings of 3rd International Conference on Image Processing, pp. 86-90, 2015.
22. K.S. Seetha Lakshmi, B.A. Usha, and K.N. Sangeetha, "Security Enhancement in Image Steganography using Neural Networks and Visual Cryptography", Proceedings of International Conference on Computational Systems and Information Systems for Sustainable Solutions, pp. 396-403, 2016.

23. Nikhil Patel and Shweta Meena, "LSB Based Image Steganography using Dynamic Key Cryptography", Proceedings of International Conference on Emerging Trends in Communication Technologies, pp. 448-457, 2016.
24. May H, "An Efficient Image Cryptography using Hash-LSB Steganography with RC4 and Pixel Shuffling Encryption Algorithms", Proceedings of Annual Conference on New Trends in Information and Communications Technology Applications, pp. 86-90, 2017.
25. A.A.A. El-Latif, B. Abd El Atty, M.S. Hossain, M.D. A. Rahman, A. Alameri, and B.B. Gupta, "Efficient Quantum Information Hiding for Remote Medical Image Sharing", IEEE Access, Vol. 6, pp. 21075-21083, 2018.
26. Z. Qu, Z. Cheng, and X. Wang, "Matrix Coding-Based Quantum Image Steganography Algorithm", IEEE Access, Vol. 7, pp. 35684-35698, 2019.
27. Emmanuel J. Candès and David L. Donoho, "Ridgelets: A Key to Higher-Dimensional Intermittency," Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, vol. 357, no. 1760, pp. 2495–2509, 1999.
28. Emmanuel J. Candes and David L. Donoho "Curvelets—A Surprisingly Effective Non Adaptive Representation for Objects with Edges," Curves and Surfaces, pp. 1-17, 2000.
29. Emmanuel J. Candes and David L. Donoho, "Continuous Curvelet Transform: II. Discretization and Frames," Applied and Computational Harmonic Analysis, vol. 19, no. 2, pp. 198–222, 2005.
30. Emmanuel J. Candes and David L. Donoho, "New Tight Frames of Curvelets and Optimal Representations of Objects with Piecewise Singularities," Communications on Pure and Applied Mathematics, vol. 57, no. 2, pp. 219–266, 2004.
31. Emmanuel Candes, Laurent Demanet, David Donoho and Lexing Ying, "Fast Discrete Curvelet Transforms," Multiscale Modeling & Simulation, vol. 5, pp. 861–899, 2006.
32. I. Maurya, and S. K. Gupta. "Secure image steganography through preprocessing." In Soft Computing: Theories and Applications, pp. 133- 145. Springer, Singapore, 2019.
33. M. A. Hameed, M. Hassaballah, S. Aly, and A. I. Awad, "An adaptive image steganography method based on histogram of oriented gradient and PVD-LSB techniques," IEEE Access, vol. 7, pp. 185189-185204, 2019.
34. Ramalingam M, Isa NAM, A data-hiding technique using scene-change detection for video steganography. ComputElectrEng 54:pp.423–434, 2016.
35. ZiadAlqadi, Bilal Zahran, QazemJaber, BelalAyyoub, Jamil Al-Azzeh, Enhancing the Capacity of LSB Method by Introducing LSB2Z Method, International Journal of Computer Science and Mobile Computing, vol. 8, issue 3, pp. 76-90, 2019.
36. Rajalakshmi K, Mahesh K, Robust secure video steganography using reversible patch-wise code-based embedding. Multimedia Tools Appl 77(20):27427–27445, 2018.
37. Wu P, Yang Y, Li X, Image-into-image steganography using deep convolutional network. In: Pacific Rim conference on multimedia. Springer, Cham, pp 792–802, 2018.
38. S.A. Parah, J.A. Sheikh, J.A. Akhoon, N. A. Loan, and G.M. Bhat, "Information hiding in edges: A high capacity information hiding technique using hybrid edge detection." Multimedia Tools and Applications. 77(1): pp.185–207, 2018.
39. Duan X, Jia K, Li B, Guo D, Zhang E, Qin C , Reversible image steganography scheme based on a U-Net structure. IEEE Access 7:pp.9314–9323,2019.
40. Sourabh Chandra Etal, "Secure Transmission of Data Using Image Steganography", Ictact Journal on Image and Video Processing, Volume: 10, Issue: 01, August 2019.
41. Mishra A, Kumar S, Nigam A, Islam S, VStegNET: video steganography network using spatio-temporal features and micro-bottleneck. In: BMVC, p 274, 2019.

42. Raja KB, Chowdary CR, Venugopal KR, Patnaik LM, A secure image steganography using LSB, DCT and compression techniques on raw images. In: 2005 3rd international conference on intelligent sensing and information processing. IEEE, pp 170–176,2005.
43. K.B.Shiva Kumar, K.B. Raja, R.K.Chhotaray, Sabyasachi Pattnaik, "Coherent Steganography using Segmentation and DCT", IEEE-978-1-4244-5967-4, 2010.
44. M.Khan, M. Sajjad, I. Mehmood, S. Rho and S. WookBaik, "A Novel Magic LSB Substitution Method (M-LSB-SM) Using Multi-Level Encryption and Achromatic Component of an Image" Multimedia Tools and Applications, Volume 3, Issue 2, 2015.
45. M. Shelke, A. Dongre and P. Soni "Comparison Of Different Techniques For Steganography In Images " International Journal Of Application Or Innovation In Engineering & Management (IJAIEM) ,Volume 3, Issue 2, 2014 .
46. K. S. Babu, K. B. Raja, U. M. Rao, R. K. A, V. K. R, and L. M. Patnaik. Robust and high capacity image steganography using svd. IET UK International Conference on Information and Communication Technology in Electrical Sciences, pages 718--727, 2007.
47. K. S. kumar and K. B. Raja. Khasim T. Dual transform technique for robust steganography. IEEE International Conference on Computational Intelligence and Communication Systems, pages 310--314, 2011.
48. K. B. Raja, C. R. Chowdary, K. R. Venugopal and L. M. Patnaik, "A secure image steganography using LSB, DCT and compression techniques on raw images," In *Proceedings of the 3rd International Conference on Intelligent Sensing and Information Processing* IEEE, Bangalore, India, pp. 171–176,2005.
49. K. B. Raja, S. Sindhu, T. D. Mahalakshmi, S. Akshatha, B. K. Nithin, M. Sarvajith, K. R. Venugopal and L. M. Patnaik, "Robust image adaptive steganography using integer wavelets," in Proc. Int. Conf. Communication Systems, pp. 614–621,2008.
50. Ravi J, Saleem S. Tevaramani and K. B. Raja, "Face recognition using DT-CWT and LBP features," *2012 International Conference on Computing, Communication and Applications*, Dindigul, India, pp. 1-6,2012.
51. H. S. M. Reddy, N. Sathisha, A. Kumari and K. B. Raja, "Secure steganography using hybrid domain technique," 2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT 12), pp. 1-11, 2012.
52. Rafael C. Gonzalez, Richard E.Woods and Steven L. Eddins, "Digital Image Processing Using MATLAB", Gatesmark Publishing, 2009.
53. https://sipi.usc.edu/database/database.php?volume=misc