World Journal of Engineering Research and Technology
WJERT
www.wjert.org

MULTI-BIT LSB STEGANOGRAPHY OF COLOR IMAGE IN DCT DOMAIN

Rajib Biswas[1] and Samir Kumar Bandyopadhyay*[2]

[1]Department of Information Technology, Heritage Institute of Technology, Kolkata, India.

[2]Department of Computer Science and Engineering, Calcutta University, Kolkata, India.

Article Received on 01/12/2015 Article Revised on 20/12/2015 Article Accepted on 12/01/2016

***Correspondence for Author**
Dr. Samir Kumar Bandyopadhyay
Department of Computer Science and Engineering, Calcutta University, Kolkata, India.
skb1@vsnl.com
rajib.biswas.rd@gmail.com

ABSTRACT

We have explored two-dimensional Discrete Cosine Transform (DCT) based steganographic method for hiding the data in a color image (any size) where DCT is used to transform original image (cover image) blocks from spatial domain to frequency domain. Here we propose a novel method for image steganography using key based secret data embedding in frequency domain applying function on it.

KEYWORDS: Steganography, Steganolysis, Discrete Cosine Transform, Sampling, Inverse DCT, LSB Substitution, Encryption, Decryption.

1. INTRODUCTION

Steganography is the art of hiding information in such a way that prevents the detection of hidden information. So, using steganography, you can embed a secret message inside a piece of unsuspicious information and send it without anyone knowing of the existence of the secret message. Secrete message can be hidden inside all types of cover information like text, images, audio, video and more. Here we hide information inside images. The quality of the steganography should only depend on the impossibility of detecting the secret data. Staganalysis methods aim at estimating retrieval of potentially hidden information with little or no knowledge about the steganographic algorithm or its parameters.

2. LITERATURE STUDY

An extensive study of the related papers[1,3,4,5,7] has given shape to this concept. We have meticulously analyzed the possibilities in the sphere of maximizing randomization, minimizing deviations and structuring strong coherence among the working sets. This paper is aimed at further increasing the equalization and reliability of the substitution based 2D-DCT steganography from its referrals.

3. DISCRETE COSINE TRANSFORM

The discrete cosine transform (DCT) [8] is quite closely related to Discrete Fourier Transform (DFT) but offers high energy compaction property in comparison with DFT for natural images. It's a real domain transform which represents an image as coefficients of different frequency of cosine which is basis vector for this transform. The general equation for 2-D (NXM data items) DCT is defined as:

$$F(u,v)=\frac{1}{4}C(u)C(v)\sum_{x=0}^{7}\sum_{y=0}^{7}f(x,y)\cos\left[\frac{\pi(2x+1)u}{16}\right]\cos\left[\frac{\pi(2y+1)}{16}\right]$$

for x=0,..., 7 and y=0,..,7

$$where\ C(k)=\begin{cases}1/\sqrt{2} & for\ k=0\\ 1 & otherwise\end{cases}$$

Similarly the Inverse DCT can be calculated using the following equation, where the signal comes back to spatial domain from Transform domain.

$$f(x,y)=\frac{1}{4}\sum_{u=0}^{7}\sum_{v=0}^{7}C(u)C(v)F(u,v)\cos\left[\frac{\pi(2x+1)u}{16}\right]\cos\left[\frac{\pi(2y+1)v}{16}\right]$$

for $x=0,...,7$ and $y=0,...,7$

4. OUR PROPOSED METHOD

In our method we have mainly three components as sampling, encryption & embedding, decryption. Sampling and functions applied to encrypt the image pixel plays a key role here in our procedure, In the case of Embedding, we first divide the cover image into 8×8 sub blocks and then we transfer it into frequency domain using 2D-DCT.[8] Then we sample mid frequency zone. After that we embed the secret message using a function. Finally we get the stego image applying Inverse 2D-DCT to each modified 8×8 blocks and converting it into cover Image. The decoding process is similar with the encoding process, the stego image is partitioned into 8×8 sub blocks and then we transfer it into frequency domain using 2D-DCT. We take the values from mid frequency zone and apply the inverse function to get the secret message.

Algorithm(sampling and embedding)

I/P: Color original(cover) image

O/P: Color stego image

Begin

Step1: Extract R,G,B value to get three different matrices.

Step2: Convet each matrix into 8x8 blocks.

Step3: Apply 2D-DCT to each block.

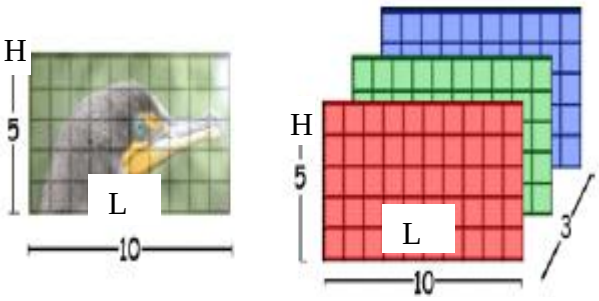
Step4: Value of mid frequency range of DCT matrices are sampled.

Step5: Embed secret Message to sampled frequency value using Password (Key) and function $f_{x1.}$

Step6: Apply The IDCT to each modified 8×8 DCT matrixes.

Step7: Reassemble the modified 8×8 DCT matrices to get stego image.

End



Original Color Image 3 Different Matrix for R,G,B

Fig 1: Extraction of R,G,B color matrix

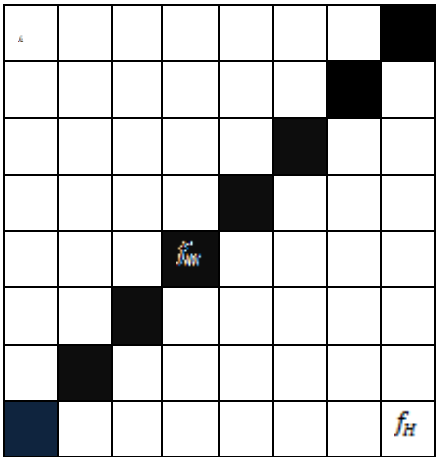


Fig 2: Mid frequency of DCT (8×8)

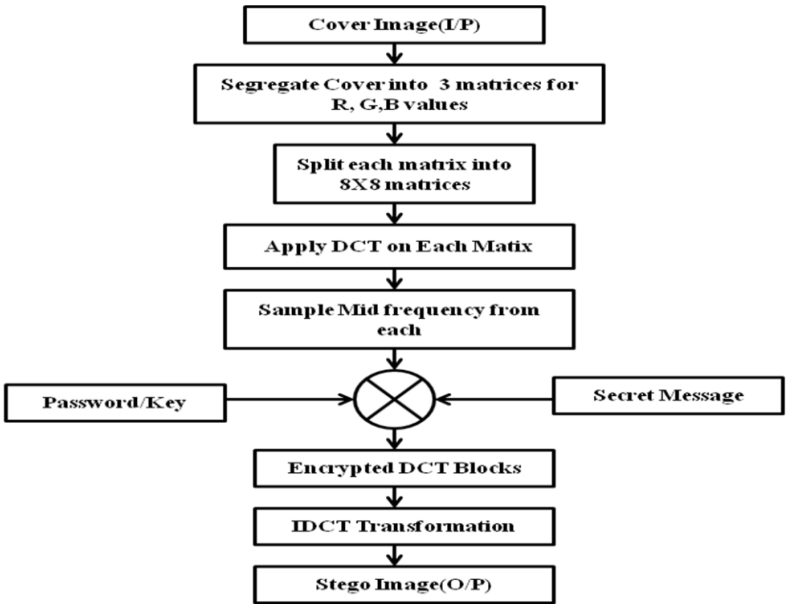


Fig3: Flowchart of sampling, encryption and embedding

Algorithm(Extraction of secret message)

I/P: Color stego image

O/P: embedded secret message

Begin

Step1: Extract three different matrices for R, G, B applying same function as before.

Step2: Convet each matrix into 8x8 blocks.

Step3: Apply 2D-DCT to each block.

Step4: Value of mid frequency range of DCT matrices are sampled.

Step5: Apply the inverse of f_{x2} function (f_{x2}^{-1}) to pick the secret data.

Step6: Put this values and Password into f_{x1}^{-1} function to get the Secret Message.

End

Fig 4: Cover image

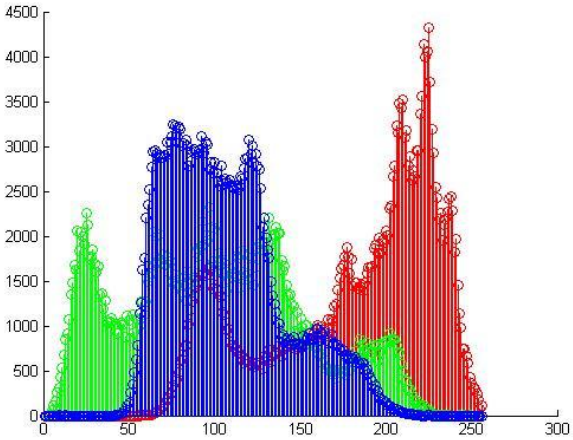


Fig 5: Histogram for Cover image(lena)

Fig 6: Stego image

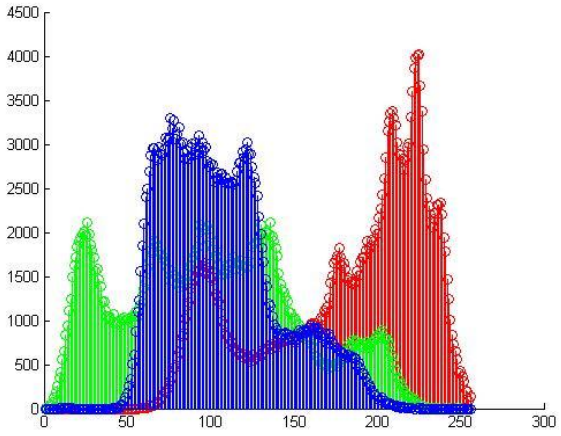


Fig 7: Histogram for stego image (lena)

5. SPLIT AND SEND

To remove the constraint of a fixed size secret message, we intent to put forward an automatic adjustment algorithm.[3] This segment is mainly concerned with ensuring that input secret message size to be embedded bears a fairly reasonable ratio to the cover image size for which the distortion is negligible. The dynamic ratio value is defined depending on the dynamics of the image and the concentration of the color component values across the cross sections of the image. Based on the above concept, our algorithm warn against suspicion and suggests the use of another cover image or the copy of the same cover image, which can be generated automatically. On agreement we split the secret data in the best-proportion and the re-sample it. This process of splitting and re-sampling is a recursive process and terminates once an optimally permitted ratio is reached. We store the necessary values required for decoding in the four corners of a picture.

6. PERFORMANCE ANALYSIS

The Test results and statistical studies further clarify the unnoticeable distortions produced in the stego image after applying the above proposed algorithms. From the table underneath it is noted that the statistical parameters like the mean, variance, Standard Deviation, MSE (Mean square Error) table.1. Change only in their distant decimals thus proving its strong resistance to steganalysis.

MSE (Mean square Error): It is defined as the square of error between original image and the stego image.

$$MSE = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1}(f(x,y) - g(x,y))^2 \Big/ N^2$$

f(x,y)= The intensity of the pixel in the original image;

g(x,y)= The intensity of the pixel in the stego image;

$$\text{MSE} = \sqrt{\frac{\sum_{x=0}^{W-1}\sum_{y=0}^{H-1}\left(f(x,y) - f'(x,y)\right)^2}{WH}}$$

Table 1: Mean, variance, standard deviation, MSE

Image	Statistical Parameters	Original Image	Stego Image
Lena	Mean	128.2284	128.2282
	Variance	3479.1	3479.4
	Standard Deviation	58.9838	58.9860
	MSE	R	0.8289
		G	1.1659
		B	1.2550

StirMark Analysis: Any steganographic algorithm should resist some standard benchmark tests to prove its strength and robustness. We run these tests in StirMark 4.0[11] and our algorithm produced good results. We show a sample of the results in table 3. The negligible gaps between the values corresponding to the cover and the stego image imply that our technique is robust.

Table. 2. StirMark Analysis Results.

Test	Factor	Cover	Stego
SelfSimilarities	1	34.546 dB	36.617 dB
SelfSimilarities	2	31.4939 dB	33.7177 dB
SmallRandomDistortions	1	15.839 dB	14.3582 dB
SmallRandomDistortions	1.05	15.4899 dB	14.2077 dB
MedianCut	3	33.9569 dB	35.9366 dB
MedianCut	5	31.5682 dB	33.2307 dB
PSNR	10	40.315 dB	40.4831 dB
PSNR	30	31.9001 dB	32.0104 dB
AddNoise	20	7.91818 dB	7.87529 dB
AddNoise	40	5.98115 dB	5.92478 dB

Resilience against standard steganalytical tools and tests: To augment our statistical analysis of images, we have realized Stegdetect, an automated analytical tool and Stefan Axelsson's base-rate fallacy to intrusion detection systems where false-positives cast a bearing on system's efficiency. We have calibrated Stegdetect's detection sensitivity against numerous outputs of our algorithm.We can calculate the true-positive rate – the probability that an image detected by Stegdetect really has steganographic content as:

$$P(S|D) = \frac{P(S).P(D|S)}{P(S).P(D|S) + P(\neg S).P(D|\neg S)}$$

Where P(S) is the probability of steganographic content in images, and P(¬ S) is its complement. P(D | ¬ S) is the probability that we'll detect an image that has steganographic content. Conversely, P(¬D | S)=1-P(D | S) is the false positive rate.

We have calibrated Steg detect's detection sensitivity against numerous outputs of our algorithm. The probability of detection is negligible for small messages, but with larger embedded data, the probability is high. In our algorithm, besides the dual cover encryption on the images, we have used a variable split and send algorithm which creates an upper limit on the message size, which is smart barrier against detection.

Dual Statistics Method: This method [9] partitions an image with a total number of pixels P into P/n disjoint groups of n adjacent pixels. For a group of pixels $GP=(x_1, x_{2,\ldots\ldots}, x_n)$. The authors considered discrimination function $gp(x_1, x_{2,\ldots\ldots},x_n)=\sum_{i=1}^{n-1} |x_{i+1} - x_i|$.They define two LSB flipping functions $F_1 = 0\leftrightarrow1, 2\leftrightarrow3,\ldots\ldots,254\leftrightarrow255$ and $F_{-1} = -1\leftrightarrow0, 1\leftrightarrow2,\ldots\ldots,255\leftrightarrow256$, along with an identity flipping function $F_0(x) =x$. The assignment of flipping to a group of n pixels can be captured by a mask $M = (M(1),M(2),\ldots,M(n))$,where $M(i) \varepsilon \{-1,0,+1\}$ denotes which flipping function is applied to which pixel.

The flipped group of a group $GP=(x_1, x_{2,\ldots\ldots},x_n) =(F_{M(1)}(x_1), F_{M(2)}(x_2),\ldots\ldots, F_{M(n)}(x_n))$ They classify the pixel groups as Regular, Singular, or Unchanged, according as $g(F(GP))> g(GP)$, $g(F(GP))< g(GP)$ *or* $g(F(GP))= g(GP)$ respectively. Next, they compute the length of the hidden message from the counts of such groups.

The authors mention that their method does not work well for image that are noisy, or of low quality, or over-compressed, or of small size. Moreover Dumitrescu et al [14] points out that the above schema is based on the following assumptions:

Assumption 1: Suppose X is the set of all pixel pairs (u, v) such that either v is even and u<v, or v is odd and u>v. Suppose Y is the set of all pixel pairs (u, v) such that either v is even and u>v, or v is odd and u<v. The assumption is that statistically we have |X|=|Y|.

Assumption 2: The message bits of LSB steganography are randomly scattered in the image space, independent of image features.

Our method does not make any of the following assumptions. Dumitrescu et al mentions that assumption 1 is valid only for natural images. Our method works on no specified range of images. It works on even cartoon and paint-drawn images. Starting from random sampling, through dual-encryption to embedding, we have used image data attributes vigorously as functional parameters for respective utilities. Hence, it directly violates assumption 2. So, theoretically, our method is not breakable by the dual statistics method.

6.1. Comparative analysis of the state of the art works and resilience against effective steganalysis methods.

The algorithm conceptualizes mid frequency sampling and password based encryption to reduce distortion during embedding. It realizes the shifting from spatial domain to frequency domain technique for improving the quality of image after different operations performed on

it. Due to use of frequency domain technique the brut attach is almost reduced. Our algorithm parallels the strength of grid colorings in steganography[12], based on rainbow coloring graphical analysis employing syndrome coding by perspective based dimensional analysis of the stego image. It considers the signal processing vulnerabilities of substitution technique based spatial steganography [9] and establishes its resilience towards them. It also responses positively to the lagrange's interpolation [11] based steganalysis The algorithm considers the effective steganalysis methods of estimating secret key in sequential embedding methods through low, medium, and high signal-to-noise ratio (SNR) analysis and abrupt change detection based steganalysis.[13] The abrupt change detection using sequential probability ratio test (SPRT) has also been applied against this algorithm as shows inarguably positive statistics. Besides, it recognizes that under repeated embedding, the disruption of the signal characteristics is the highest for the first embedding and decreases subsequently, that is, the marginal distortions due to repeated embeddings decrease monotonically. This decreasing distortion property exploited with Close Color Pair signature is used to construct the classifier that is in turn used to distinguish between stego and cover images. Our algorithm handles the close color pair detection meticulously and shows its resilience against these types of attacks.

7. CONCLUSIONS

In this paper, we propose a steganography process with a color image in discrete cosine transform (DCT) domain to improve security and stego image quality compared to the existing algorithms which are normally done in spatial domain. According to the simulation results the RGB values of stego-images of our method are almost identical to original images and it is very difficult to differentiate between them visually. Our proposed algorithm also provides additional two layers of security by means of transformation (DCT and Inverse DCT) of cover image and it can be applied for any size of an image (not a square image). Hence the proposed method may be more robust against brute force attack. That means secret image keep the secret massage away from stealing, destroying from unintended users.

8. ACKNOWLEDGMENTS

Long term duration hard has given shape to this paper. It is not complete without conveying thanks to all, who have spurred our way to the completion of this endeavour. We express our gratitude to all who has taken part on this work.

9. REFERENCES

1. B. Pfitzmann, "Information hiding terminology," in Information Hiding, First International Workshop (R. Anderson, ed.), vol. 1174 of Lecture Notes in Computer Science, pp. 347–350, Springer,1996.
2. Feature Extraction Methods for Color Image Similarity by R.Venkata Ramana Chary, Dr.D.Rajya Lakshmi, Dr. K.V.N Sunitha. An International Journal (ACIJ), Vol.3, No.2, March 2012.
3. Rajib Biswas, Gaurav Dutta Chowdhury, Samir Kumar Bandhyopadhyay "Perspective Based Variable Key Encryption in LSB Steganography", Springer Verlag, ISSN: 2190-3018, ICACNI, 24-26,June 2014, page(s) 285-293, Print ISBN 978-3-319-07349-1.
4. Biswas, R..; Basak, R.; Bandyopadhyay, S.K. "Generic Function Based Color Image Steganography in 2-D DCT Domain", Elsevier(print) AET-ACS, 13-14, Dec *2013*, NCR, India, page(s) 150-154, ISBN:978-93-5107-193-8.
5. Biswas, R., Mukherjee, S. ; Bandyopadhyay, S.K. "DCT Domain Encryption in LSB Steganography", CICN, 27-29 Sept *2013.*
6. Siddharth Singh and Tanveer J Siddiqui, "A Security Enhanced Robust Steganography Algorithm for Data Hiding", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012.
7. Ekta Walia, Payal Jain, Navdeep, "An Analysys of LSB & DCT based Steganography", Global Journal of Computer Science and Technology, Volume 10, Issue 1(Ver 1.0), April 2010.
8. Discreat Cosine Transform: Algorithms, Advantages, Applications by K.Ramamohan Rao, P.Yip, ISBN-10:012580203X|ISBN=13:978-0125802031, Publication Date: Saptember 11, 1990.
9. A Survey of State of the Art techniques of SteganographyC. Vanmathi , S. PrabuSchool of Information Technology and Engineering School of Computing science and Engineering VIT University, Vellore, Tamilnadu, India.
10. S. Trivedi, Chandramouli, "Secret key estimation in sequential steganography," Signal Processing, IEEE Transactions on, vol.53, no.2, pp.746, 757, Feb. 2005 doi: 10.1109/TSP.2004.839925.
11. ReLACK: A Reliable VoIP Steganography Approach Mohammad Hamdaqa, Ladan Tahvildari Software Technologies Applied Research (STAR) Group Department of Electrical and Computer Engineering University of Waterloo, Waterloo, Canada.

12. Fridrich, J.; Lisonek, P., "Grid Colorings in Steganography," Information Theory, IEEE Transactions on , vol.53, no.4, pp.1547,1549, April 2007, doi: 10.1109/TIT.2007.892768.
13. Fridrich, J., Goljan, M. and Dui, R., \Reliable Detection of LSB Steganography in Color and Grayscale Images," Proceedings of the ACM Workshop on Multimedia and Security, Ottawa, CA, October 5, 2001, pp. 27-30.
14. Dumitrescu S, Wu X, Wang Z (2002) Detection of LSB steganography via sample pair analysis. In: Proc. information hiding workshop, LNCS, vol 2578. Springer, pp 355–372.

Authors

Rajib Biswas received B.E.in IT, M.Tech in Computer Technology currently an Assistant Professor in the Information Technology, Department of Heritage Institute of Technology, Kolkata, India. His research interest includes Ad-hoc Wireless Network, Steganography, Digital Forensic and Software Engineering. He has published 5 international conference papers and 1 international Journal paper.

Prof. Samir Kumar Bandyopadhyay received B.E., M.Tech., Ph. D (Computer Science & Engg.)., C.Engg., D.Engg., FIE, FIETE, currently, Professor of Computer Science & Engineering and Registrar, University of Calcutta, visiting Faculty Dept. of Comp. Sc., Southern Illinois University, USA, MIT, California Institute of Technology, etc. His research interests include Bio-medical Engg, Mobile Computing, Pattern Recognition, Graph Theory, Software Engg.,etc. He has 25 Years of experience at the Post-graduate and undergraduate Teaching & Research experience in the University of Calcutta. He has already got several Academic Distinctions in Degree level/Recognition/Awards from various prestigious Institutes and Organizations. He has published 300 Research papers in International & Indian Journals and 5 leading text books for Computer Science and Engineering. He has visited USA, Finland, Sri Lanka.