IMAGE BASED STEGANOGRAPHY TO FACILITATE IMPROVING HIDING CONTENT CAPACITY AND OPTIMIZED SECURITY

Subhash Chandra
M.tech (CSE), Shekhawati Institute of Engineering and Technology, Sikar

Abstract: Steganography is an art of writing for conveying message inside another media in a secret way that can only be detected by its intended recipient. There are security agents who would like to fight these data hiding systems by steganalysis, i.e. discovering covered secret messages and rendering them useless. Steganalysis is the art of detecting the message's existence, message length or place of message where it is to be hidden in covered media and blockading the covert communication. There is currently no more secured steganography system which can resist all steganalysis attacks such as visual attack, statistical attack (active and passive) or structural attack. The most notable steganalysis algorithm is the Reversible Statistical attack which detects the embedded message by the statistical analysis of pixel values. To maintain the security against the Reversible Statistical analysis, the proposed work presents a new steganography model based on Genetic Algorithm using Integer Wavelet Transform. We present a novel approach to resolve such problems of substitution technique of image steganography. Using the proposed Genetic Algorithm and Reversible Statistical analysis Algorithm, the system is more secured against attacks and increases robustness. The robustness would be increased against those attacks which try to reveal the hidden message and also some unintentional attacks like noise addition as well.

In this proposed work, we studied the steganography paradigm of data hiding in standard digital images. In recent literature, some algorithms have been proposed where marginal statistics are preserved for achieving more capacity and more security. Data hiding techniques are divided in two groups: spatial and transform domain. To protect the information from attacks, numbers of data hiding methods have been evolved mostly in spatial and transform domain. The first group embeds message in the least significant bit of the image pixel. In transform domain information concealment techniques, the information is embedded directly on the image plane itself. Data hiding capacity increases through this method but this method is sensitive against attacks such as low pass filtering and compression. In transform domain data hiding techniques, the image is first changed from spatial domain to some other domain and then the secret information is embedded so that the secret information remains more secure from any attack. Information hiding algorithms in time domain or spatial domain have high capacity and relatively lower robustness.

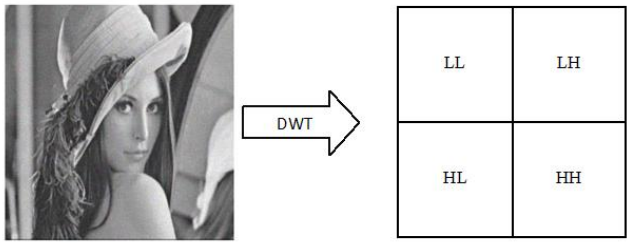
INTRODUCTION

The standard and thought of "What You See Is What You Get (WYSIWYG)" which we have a tendency to encounter typically while printing images or other materials, is no longer precise and would not mislead a stenographer as it does not always hold true. Images are over what we see with our Human Visual System (HVS); therefore, they can convey over 1000 words [1]. Steganography, the art of hiding messages inside other messages, is now gaining more popularity and is being used on various media such as text, images, sound, and signals. However, none of the existing schemes can yet defend against all type of detection attacks. Using GA's that are based on the procedures of natural genetics and the theory of evolution, we can design a general method to guide the steganography process to the best position for data hiding [2].

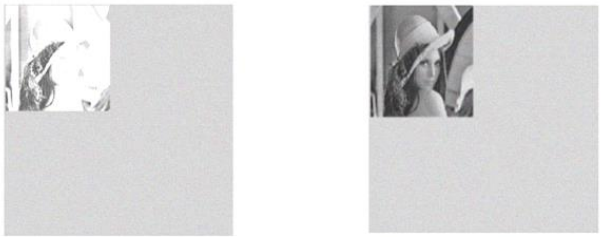
In recent years, many productive steganography strategies have been proposed. Among various strategies, LSB (least significant bit) replacement technique is widely used due to its simplicity and huge capacity. The bulk of LSB steganography algorithms embed messages in spatial domain, such as Bit-Plane Complexity Segmentation (BPCS), Pixel Value Differencing (PVD). Some other method like Jsteg, F5, Outguess, embed messages in discrete cosine transform (DCT) frequency domain (i.e. Joint Photographic Experts Group images) are also in use. In the LSB steganography, secret message is regenerated into binary string. In such cases, the least significant bit-plane is replaced with the binary string. The LSB embedding achieves smart balance between the payload capability and visual quality. However, the LSB substitution method flips one half of the least-significant bits. So the artifacts in the statistics of the image area unit are easy to be detected [2].

1. PROPOSED WORK

1.1 Integer wavelet transform : The proposed algorithm employs the wavelet transform coefficients to embed messages into four subbands of two dimensional wavelet transform. To avoid problems with floating point precision of the wavelet filters, we used Integer Wavelet Transform. The LL subband in the case of IWT appears to be a close copy with smaller scale of the original image while in the case of DWT the resulting LL subband is distorted (figure 1.1) [9]. Thus Integer Wavelet Transform (IWT) is preferred over Discrete Wavelet Transform (DWT).



(a) Lena image and analyze in wavelet domain



(b) One level 2D-DWT in subband LL

(c) One level 2D-IWT in subband LL

Fig. 1.1. Comparison of LL subband for 2D-DWT and 2D-IWT

In 2D IWT transform, first apply one step of the one dimensional transform to all rows and then repeat to whole columns. This decomposition outputs into four classes or band coefficients. The Haar Wavelet Transform is the easiest of all wavelet transform. In this transform, the low frequency wavelet coefficient are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels. The 4 bands produced are (i) Approximate band (LL), (ii) Vertical Band (LH), (iii) Horizontal band (HL), (iv) Diagonal detail band (HH). The approximation band consists of low frequency wavelet coefficients, which have important parts of the spatial domain image. The last band consists of high frequency coefficients, which contain the edge details of the spatial domain image. This IWT decomposition of the signal continues until the desired scale is achieved .Two-dimensional signals, like images, are converted using the 2D IWT. The two-dimensional IWT operates in the same manner, with only minor variations from the one-dimensional transform. Given a two-dimensional array of samples, the rows of the array are processed first with only one level of decomposition. This essentially divides the array into two vertical halves; with the first half taking the average coefficients, while the second vertical half stores the detailed coefficients. This process is again performed with the columns, resulting in 4 sub bands within the array defined by filter output.

In this method, the sender selects and reads an image of size 512x512. The data required to be hidden in the image is converted into bit streams by taking each character of text message and representing their 8 bit binary values from their ASCII code. The data is embedded in the image using LSB embedding technique. The genetic algorithm approach is used to find the best adjustment matrix to protect against RS attack.

Initially, cover image and secret message are read. Secret message is then hidden in the cover image using LSB embedding technique. A stego image is obtained after embedding secret message. The stego image is divided into 8x8 blocks and is labeled by calculating the variations of blocks before flipping and after flipping. During this process, the blocks are categorized into four variables. The variables are based on occurrence of regular group and singular group when positive flipping is used and the occurrence of the regular group and singular group when negative flipping is used. This process is carried out individually for red, green and blue colors. The comparison with the original image shows an increase in certain values of the stego image. The RS attack is therefore able to detect the changes in the values. The genetic algorithm is used to decrease the variation in the value of the variables in order to protect against the RS attack.

2. PROPOSED WORK IMPLEMENTATION

The proposed implementation of RS-analysis using genetic algorithm for the robust security in Steganography application is done on standard 32-bit windows OS with 1.84 GHz processor and 2 GB RAM. The method is applied on 512x512 colored images “Lena” and “Baboon” as shown in Figure 2.1.

a) Lena (JPG, 512x512) b) Baboon (JPG, 512x512)

Fig. 2.1. Input cover images

2.1 Experimental result analysis and discussion

The proposed work is done on 2 set of data image as shown in previous section. Both cover images have utilization of 100% and their respective accomplished results of reversible statistical analysis are as follows:

TABLE 2.1
VARIOUS VALUES FOR LENA IMAGE

For Lena	Initial Value	After Embedding	After OPAP
R_m-R_{-m}	0.0097783	0.0076353	0.0057934
S_m-S_{-m}	0.0029662	0.011807	0.0093702

TABLE 2.2
VARIOUS VALUES FOR BABOON IMAGE

For Baboon	Initial Value	After Embedding	After OPAP
R_m-R_{-m}	0.0059805	0.0076353	0.0056089
S_m-S_{-m}	0.0076634	0.011807	0.0023989

The tables 2.1 and 2.2 have shown the values of |Rm-R-m| and |Sm-S-m| that represent the RS-steganalysis on the regular and singular block. It can be seen that the value of |Rm-R-m| and |Sm-S-m| increases from initial value before embedding and after embedding that exhibits a strong correlation in potential of RS-analysis and the designed module. At initial stage, the values are less, after embedding the message, values increases and finally after applying optimal pixel adjustment process values are decreasing. Human visual system is not able to differentiate the colored images with PSNR more than 36 dB. This proposed work embedded the messages in the k-LSBs, for k=4 and have received PSNR more than 40 which is considered to be a good achievement.

TABLE 2.3
COMPARISON OF HIDING CAPACITY AND PSNR FOR 4-LSBS

Cover Image	Hiding Capacity (bits)	Data Size (KB)	PSNR (dB)
Lena	2137696 (4-LSBs)	260	46.83
Baboon	2137696 (4-LSBs)	260	49.65

Figure 2.2 shows the images after embedding with 4-LSBs. As we compare these embedded images with the input cover images (figure 2.1), we realize that there are no significant changes in images. The embedded images look like the same as cover images. So the attackers cannot realize in between the communication of two parties that secret message is embedded in these images.

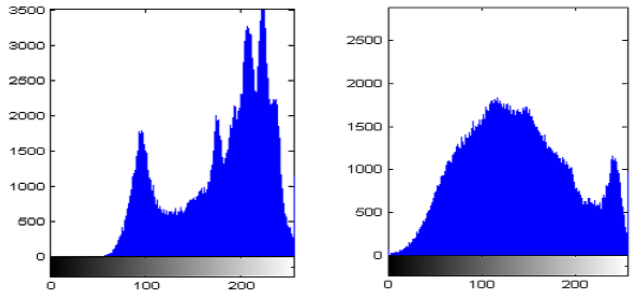
(a) Lena image after embedding with 4-LSBs (b) Baboon image after embedding 4-LSBs

Fig. 2.2. Images after embedding the secret data

TABLE 2.4
MAXIMUM HIDING CAPACITY AND PSNR OBTAINED FROM PROPOSED METHOD AND ITS COMPARISON WITH THE EXISTING METHODS

Cover Image	Method	Max. H. C. (bits)	Max H. C. (%)	PSNR (dB)
Lena	Proposed method	2137696	70%	46.83
	A steganographic method based on IWT and GA [9]	1048576	50%	35.17
	An Adaptive steganography technique based on IWT [5]	986408	47%	31.8
Baboon	Proposed method	2137696	70%	49.65
	A steganography method based on IWT and GA [9]	1048576	50%	36.23
	An Adaptive steganography technique based on IWT [5]	1008593	48%	30.89

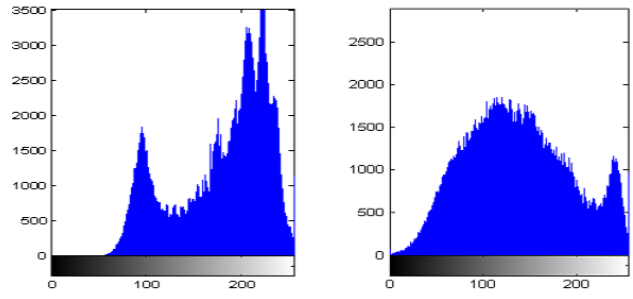
The above Table 2.4 clearly states that the proposed method is much more superior in terms of maximum hiding capacity and in terms of PSNR.



a) Histogram of Lena b) Histogram of Baboon

Fig. 2.3. Input cover images histograms

Figure 2.3 show the histogram of input cover images. Now the various algorithms such as data embedding, RS analysis and genetic are applied on the cover images. The output stego image histogram after embedding the data is represented in Figure 2.4.



a) Lena Histogram b) Baboon Histogram

Fig. 2.4. Output stego images histogram of k=4 after embedding data

Figure 2.4 shows that image for k=4 that there is little significant change in the stego-image histogram for 4-LSBs images, thus it is secured against any statistic attack.

3. CONCLUSIONS

Steganography is a method that provides secret communication between two parties. It is the science of hiding a data, message or information in such a secure way that only the sender and recipient are aware about the presence of the message. The main advantages of this type of secure communication or we can say steganography is that it does not make any attention about the message to attackers or we can say does not attract the attackers. Strongest steganalysis method which is known as RS analysis detects the secret hidden message by using the statistical analysis of pixel values.

The main aim of this work is to develop a steganography model which is highly RS-resistant using Genetic algorithm and Integer Wavelet Transform. This proposed work introduces a novel steganography technique to increase the capacity and the imperceptibility of the image after embedding. This model enables to achieve full utilization of input cover image along with maximum security and maintains image quality. GA employed to obtain an optimal mapping function to lessen the error difference between the cover and the stego image and the use the block mapping method to preserve the local image properties. In this proposed method, the pixel values of the stego image are modified by the genetic algorithm to retain their statistical characteristics. So, it is very difficult for the attacker to detect the existence of the secret message by using the RS analysis technique. We have applied the OPAP to increase the hiding capacity of the algorithm in comparison to other established systems. However, the computational complexity of the new algorithm is high. Further, implementation of this technique improves the visual quality of the stego image which is almost same as the input cover image. But, as we increase the length of the secret message, the chance of detection of secret hidden message by RS analysis also increases. The simulation results show that capacity and imperceptibility of image has increased simultaneity. Also, we can select the best block size to reduce the computation cost and in order to increase the PSNR using optimization algorithms such as GA. However, future works focus upon the improvement in embedding capacity and further improvement in the efficiency of this method.

4. FUTURE SCOPE

This proposed work is restricted to specific functionality only. The proposed work in this dissertation has been experimented on a single computer system and not on any network. Standard input cover image is only used in this steganography module. Proposed method is not applicable on audio, video and other biometrics etc. Large message steganography cannot be performed as the embedding capacity is confine to the data feed.
Future work can be performed on the following:

- Improvement in data embedding capacity and more security against all types of attacks.
- Security design experimented over multiple computers / network.
- The data hiding technique can be applied to video, speech and other biometrics.
- Protection of the system against histogram attack.

REFERENCES

[1] A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, “Digital Image Steganography: Survey and Analysis of Current Methods”, Signal Processing, Volume 90, Issue 3, March 2010, Pages 727-752.

[2] Samir Kumar Bandyopadhyay, Tuhin Utsab Paul and Avishek Raychoudhury, “Genetic Algorithm Based Substitution Technique of Image Steganography”, Journal of Global Research in Computer Science, Volume 1, No. 5, December 2010.

[3] R.J. Anderson and F.A.P. Petitcolas, “On the Limits of Steganography”, J. Selected Areas in Comm., vol. 16, no. 4, 1998, pp. 474–481.

[4] M. F. Tolba, M.A. Ghonemy, I. A. Taha, and A. S. Khalifa, “Using Integer Wavelet Transforms in Colored Image Steganography”, IJICIS, Vol. 4 No. 2, July 2004.

[5] R.O., El.Sofy, H.H.Zayed, “An adaptive Steganographic technique based on the integer wavelet transforms”, 978-1-4244-3778-8/09/$25.00 ©2009 IEEE.

[6] Ali Al- Ataby, and Fawzi Al-Naima, “A Modified High Capacity Image Steganography Technique Based on Wavelet Transform”, The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010.

[7] Souvik Bhattacharya, Avinash Prashad, Gautham Sanyal, “A Novel approach to develop secure image based Steganographic model using Integer wavelet transform”, 2010 International Conference on Recent Trends in Information, Telecommunication and Computing, 978-0-7695-3975-1/10 $25.00 © 2010 IEEE.

[8] H S Manjunatha Reddy, K B Raja, “High capacity and security steganography using discrete wavelet transform”, Dept. of Electronics and Communication, Global Academy of Technology, Bangalore, International Journal of Computer Science and Security (IJCSS), Volume (3): Issue (6).

[9] Elhan Ghasemi, Jamshid & Brahram, “A Steganographic method based on Integer Wavelet Transform & Genetic Algorithm”, Islamic Azad University Science and Research Branch, 978-1-4244-9799- 7/111$26.00 ©20 11 IEEE.

[10] T.C. Manjunath, Usha Eswaran, “Digital Steganography Implementation for colored Images using Wavelet”, International Journal of Communication Engineering Applications-IJCEA-Vol 02, Issue 04; July 2011, ISSN: 2230-8520; e-

ISSN-2230-8539

[11] Amitav Nag, Sushanta Biswas, Debasree Sarkar and Partha Pratim Sarkar, "A novel technique for image steganography based on DWT and Huffman encoding", International Journal of Advances in Image Processing, Vol. 2, Special Issue 1, Part 2,2011.

[12] Yedla dinesh Addanki purna ramesh, "Efficient Capacity Image Steganography by Using Wavelets", Department of Electronics and communications, Sri vasavi engineering college, Tadepalligudem, AP, India.

[13] Saddaf Rubab, M. Younus, "Improved Image Steganography Technique for Colored Images using Wavelet Transform", department of Computer Engineering, College of Electrical & Mechanical Engineering, National University of Sciences & Technology (NUST), Islamabad, Pakistan.

[14] S. Priya and A. Amsaveni, Bonfring, "Edge Adaptive Image Steganography in DWT Domain", International Journal of Advances in Image Processing, Vol. 2, Special Issue 1, Part 2, February 2012.

[15] Rastislav Hovancak, Peter Foris, Dusan Levicky, "Steganography based on DWT transform", Department of Electronics and Multimedia Telecommunications, Technical University of Kosice, Park Komenskeho 13, 041 20 Kosice, Slovak Republic.

[16] A. Yadollahpour and H. M. Naimi, "Attack on LSB Steganography in Color and Grayscale Images Using Autocorrelation Coefficients", European Journal of Scientific Research ISSN 1450-216X Vol.31 No.2 (2009), pp.172-183.

[17] J. Fridrich, M. Goljan, R. Du., "Reliable detection of LSB steganography in grayscale and color images", Proceeding of ACM, Special Session on Multimedia Security and Watermarking, Ottawa, Canada, 2001, pp. 27–30.

[18] Andrew D. Ker, "A General Framework for Structural Steganalysis of LSB Replacement", IH 2005, LNCS 3727, pp. 296–311, 2005, Springer-Verlag Berlin Heidelberg 2005.

[19] Zhang, T., Ping, X., "A new approach to reliable detection of LSB steganography in natural images", Signal Processing 83 (2003) 2085–2093.

[20] J. Fridrich and M. Goljan, "Practical steganalysis of digital images-state of the art", Proc. SPIE, vol. 4675, pp. 1–13, 2002.

[21] X. Kong, T. Zhang, X. You, and D. Yang, "A new steganalysis approach based on both complexity estimate and statistical filter", In Proc. IEEE Pacific-Rim Conf. on Multimedia, vol. LNCS 2532, 2002, pp. 434–441.

[22] R Amirtharajan, S K Behera, M A Swarup, K M Ashfaaq and J B B Rayappan, "Colour Guided Colour Image Steganography", Universal journal of computer science and engineering technology, ISSN 2219-2158, 1(1), 16-23, October 2010.

[23] Dr. M. Umamaheswari, Prof. S. Sivasubramanian, S. Pandiarajan, "Analysis of Different Steganographic Algorithms for Secure Data Hiding", IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.8, August 2010.

[24] Taras Holotyak, Jessica Fridrich, and David Soukal, "Stochastic Approach to Secret Message Length Estimation in ±k Embedding Steganography", Communications and Multimedia Security 2005.

[25] Taras Holotyak, Jessica Fridrich, Sviatoslav Voloshynovskiy, "Blind Statistical Steganalysis of Additive Steganography Using Wavelet Higher Order Statistics", Communications and Multimedia Security 2005.

[26] Sos S. Agaian and Juan P. Perez, "New Pixel Sorting Method for Palette Based Steganography and Color Model Selection", 2004.

[27] Po-Yueh Chen and Hung-Ju Lin, "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering 2006. 4, 3: 275-290.

[28] Kathryn Hempstalk, "Hiding Behind Corners: Using Edges in Images for Better Steganography", 2006.

[29] Ying Wang and Pierre Moulin, "Statistical Modelling and Steganalysis of DFT-Based Image Steganography", Proc. of SPIE Electronic Imaging, 2006.

[30] Youngran Park, Hyunho Kang, Kazuhiko Yamaguchi, and Kingo Kobayashi, "Integrity Verification of Secret Information in Image Steganography", The 29th Symposium on Information Theory and its Applications (SITA2006), Hakodate, Hokkaido, Japan, Nov. 28 (Dec. 1, 2006).

[31] Ms. K. Ramani Dr. E. V. Prasad Dr. S. Varadarajan, "Steganography using BPCS to the integer wavelet transformed image", IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.7, July 2007.

[32] Farhan Khan and Adnan Abdul-Aziz Gutub, "Message Concealment Techniques using Image based Steganography", The 4th IEEE GCC Conference and Exhibition, Gulf International Convention Centre, Manamah, Bahrain, 11-14 November 2007.

[33] Anindya Sarkary, Kaushal Solankiyy and B. S. Manjunathy, "Further Study on YASS: Steganography Based on Randomized Embedding to Resist Blind Steganalysis", Proc. SPIE - Security, Steganography, and Watermarking of Multimedia Contents (X), San Jose, California, Jan. 2008.

[34] Adnan Gutub, Mahmoud Ankeer, Muhammad Abu-Ghalioun, Abdulrahman Shaheen, Aleem Alvi, "Pixel indicator high capacity technique for RGB image based steganography", WoSPA 2008 – 5th IEEE International Workshop on Signal Processing and its Applications, University of Sharjah, Sharjah, U.A.E. 18 – 20 March 2008.

[35] Mohammad Ali Bani Younes and Aman Jantan, "A New Steganography Approach for Image Encryption Exchange by Using the Least Significant Bit Insertion", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.6, June 2008.

[36] Aasma Ghani Memon, Sumbul Khawaja and Asadullah Shah, "STEGANOGRAPHY: A new horizon for safe communication through XML", Journal of Theoretical and Applied Information Technology, 2008.

[37] A.A.Zaidan, Fazidah.Othman, B.B.Zaidan , R.Z.Raji, Ahmed.K.Hasan and A.W.Naji, "Securing Cover-File Without Limitation of Hidden Data Size Using Computation Between Cryptography and Steganography", Proceedings of the World Congress on Engineering 2009 Vol I WCE 2009, July 1 - 3, 2009, London, U.K.

[38] Vinay Kumar, S. K. Muttoo, "Principle of Graph Theoretic Approach to Digital Steganography", Proceedings of the 3rd National Conference; INDIACom-2009.

[39] Shen Wang, Bian Yang and Xiamu Niu, "A Secure Steganography Method based on Genetic Algorithm", Journal of Information Hiding and Multimedia Signal Processing, Volume 1, Number 1, January 2010.

[40] Souvik Bhattacharyya and Gautam Sanyal, "Data Hiding in Images in Discrete Wavelet Domain Using PMM", World Academy of Science, Engineering and Technology 68 2010.

[41] Nadia M. Mohammed, "Multistage Hiding Image Techniques", Raf. J. of Comp. & Math's. , Vol. 7, No. 2, 2010.

[42] Abduljabbar Shaamala, Shahidan M. Abdullah and Azizah A. Manaf, "Study of the effect DCT and DWT domains on the imperceptibility and robustness of Genetic watermarking", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 2011.

[43] K B Shiva Kumar, K B Raja, R K Chhotaray, Sabyasachi Pattnaik, "Performance Comparison of Robust Steganography Based on Multiple Transformation Techniques", Int. J. Comp. Tech. Appl., Vol 2 (4), 1035- 1047, IJCTA | July-August 2011.

[44] Adnan Gutub and Maimoona Al-Ghamdi, "Image based steganography to facilitate improving counting based secret sharing", Springer Link, Article No 6 (2019) 3DR Express.

[45] W. Sweldens, The lifting scheme: A construction of second generation wavelets, SIAM J. Math. Anal., 29:511–546, 1997.

