IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

Intelligence System for Data Hiding Behind an Image

Trupti S. Deshmukh[1], Shrutika Siddheshwar Sambharam[2], Aarti Anand Sherla[3], Monika Lingraj Meragu[4], Radha Devidas Vadlakonda[5]
UG Students, Department of Information Technology [1,2,3,4]
Assistant Professor, Department of Information Technology[5]
Shree Siddheshwar Women's College of Engineering, Solapur, Maharashtra, India
tsdeshmukh@sswcoe.edu.in[1], shrutikasambharam@gmail.com[2], sherlaaarti924@gmail.com[3], monikameragu27@gmail.com[4], radhavadlakonda118@gmail.com[5]

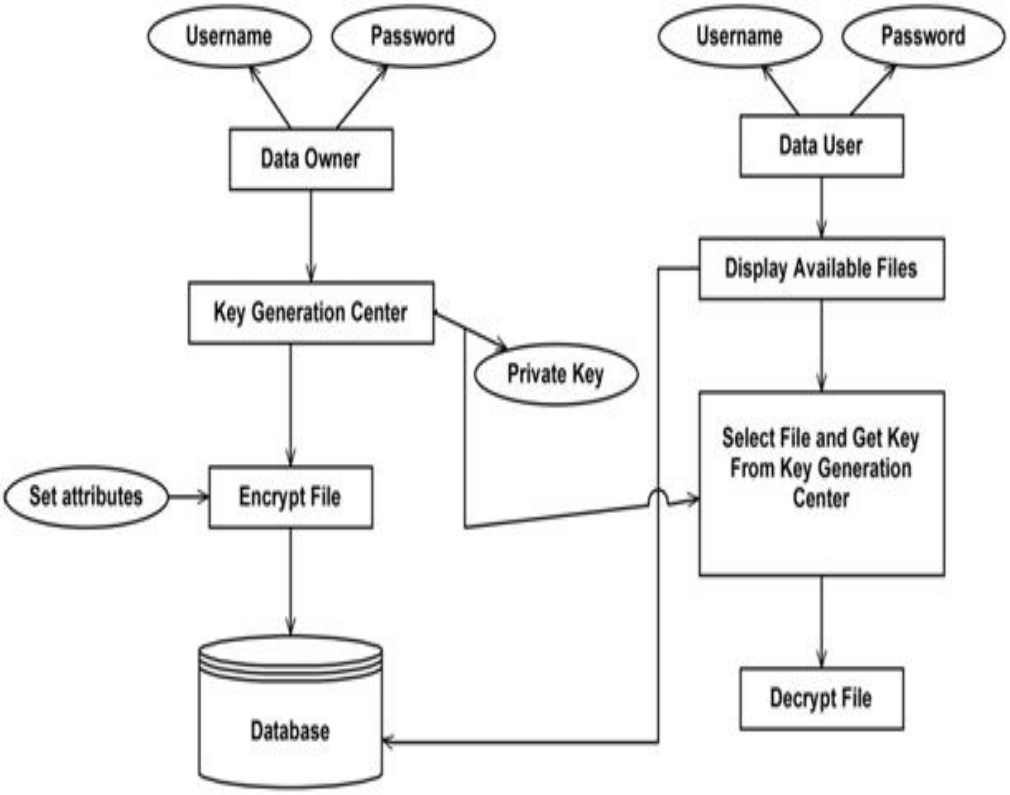
Abstract: *Steganography is the art and science of writing hidden messages in such a way that no one apart from sender and intended recipient even realizes there is a hidden message. There are often cases when it is not possible to send messages openly or in encrypted form. This is where steganography can come into play. While cryptography provides privacy, steganography is intended to provide secrecy. The aim of steganography is to hide the secret messages and also for communication and transferring of data. Steganography is also used in transferring the information of credit card or debit card to e-commerce for purchasing items. So no one apart from the authorized sender and receiver will be aware of the existence of the secret data. This intends to give an overview of image steganography and its uses and hiding the files (text file, audio file etc) by using LSB and AES algorithm where AES used for password protecting system so that if anyone can find the stego image they will not read the message because data still in the encrypt form and LSB is used for hiding the data.*

Keywords: Steganography, Image Steganography, Secret Message Embedding, Stego Image, Cover Image, Message Extraction, User Authentication, Encryption Techniques, Decryption Algorithms, Key Management, Secure Transmission, Data Security

I. INTRODUCTION

The process of Steganography in which we generally embed some secret message into an innocuous looking simple image (called as the cover image) and create a Stego image[1]. The Stego image visually seems to be indifferent from the original cover but hides the secret message inside it and is transmitted to the desired recipients over the communication channels without creating any suspicion in the minds of the intermediately sniffers or/and receivers[2].
When the authorised recipient receives the image, they follow the extraction procedure to retrieve the secret message[3]. To increase the secrecy or security of the hidden message there may some keys involved in this process of embedding and extraction[4]. At the transmission end, during embedding, the message can suitably be encrypted using one or more encryption techniques[5].
These encryption standards can be key based encryptions or non-key based and in key based techniques, they again can be public or private or a mix[6]. Depending upon the encryption method used during the embedding process, the receiver needs to execute certain decryption algorithms to retrieve the correct message[7]. If any of the decryption algorithms or the keys used for the procedure or the sequence is not known to the receiver then the extraction fails and the receiver cannot retrieve the message[8].

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024



II. LITERATURE REVIEW

In Saudi Arabia at the King Abdulaziz City of science and technology, a project was initiated to translate into English some ancient Arabic manuscripts on secret writing which are believed to have been written 1200 years ago. Some of these manuscripts were found in Turkey and Germany [6]. The word Steganography technically means covered or hidden writing. Its ancient origins can be traced back to 440 BC. Although the term steganography was only coined at the end of the 15th century, the use of steganography dates back several millennia[7]. In ancient times, messages were hidden on the back of wax writing tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves[8]. Invisible ink has been in use for centuries for fun by children and students and for serious undercover work by spies and terrorists. The majority of today's steganographic systems uses multimedia objects like image, audio, video etc as cover media because people often transmit digital pictures over email and other Internet communication[9]. Modern steganography uses the opportunity of hiding information into digital multimedia files and also at the network packet level. In the year of 2012 Das, R. and Tuithung, T proposed a novel technique for image steganography based on Huffman Encoding[10]. Two 8 bit gray level image of size M X N and P X Q are used as cover image and secret image respectively. Huffman Encoding is performed over the secret image/message before embedding and each bit of Huffman code of secret image/message is embedded inside the cover image by altering the least significant bit (LSB) of each of the pixel's intensities of cover image[11]. The size of Huffman encoded bit stream and Huffman Table are also embedded inside the cover image, in order that the StegoImage becomes standalone information to the receiver. Results show that the algorithm has a high capacity and a good invisibility[12]. Moreover Peak Signal to Noise Ratio (PSNR) of stego image with cover image shows better result in comparison with other existing steganography approaches. The satisfactory security is maintained in this research[13].

III. FUNCTIONAL REQUIREMENTS

- Admin can See the Users.
- Administrator has privilege to edit user's profile.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

- Users must have valid User ID and password to login thus creating their individual profiles.
- Admin enters his or her user id and password.
- Customer enters his or her user id and password.
- Maintain data.
- Registration required authenticating the user.

IV. NON-FUNCTIONAL REQUIREMENTS

- Secure access of confidential data (user's details).
- 24 X 7 availability
- Better component design to get better performance at peak time.
- Flexible service based architecture will be highly desirable for future extension.

Main Modules Includes:

- ADMIN
- User-Portal

V. ACTUAL RESOURCE USED

Hardware Requirements

- Core i3 or higher,(cache- 3MB or 4MB recommended)
- Memory(RAM): Minimum 2GB; Recommended 4GB or above
- ROM: 500MB or above

Software requirements

- Operating system: Windows 8/10
- Language: POD (5.5.6)
- Server: Xampp (1.8.3)
- Database: MySQL (5.6.14)
- Web Technologies: HTML5, CSS3, JavaScript, Ajax, Query, PHP
- Web Browser: Google Chrome

User Management:

- **View Users**: Admin can view a list of all registered users who are using the steganography system.
- **Edit User Profiles**: Admin can update user information, manage their access permissions, and modify their profiles.
- **Data Security**:
- **Ensure Secure Access**: Admin ensures that all user data, especially confidential data, is securely stored and transmitted.
- **Implement Security Policies**: Admin defines and enforces security policies to protect the system from unauthorized access and data breaches

Encryption Management:

- **Manage Encryption Standards**: Admin can set and manage the encryption standards and keys used for hiding and retrieving data.
- **Data Hiding**:
- **Embed Data**: Users can hide secret messages within cover images using the system's steganography tools.
- **Choose Techniques**: Users may select from different steganography techniques and encryption methods based on their needs.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

Data Retrieval:

- **Extract Data**: Users can retrieve hidden messages from Stego images using the system's tools.
- **Verify Data Integrity**: Users can verify the integrity and accuracy of the retrieved data.

Key Management:

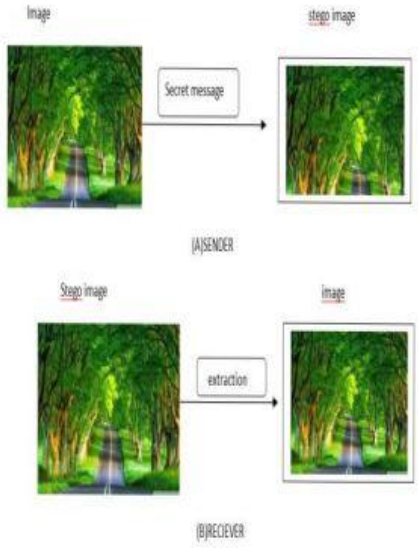
- **Manage Encryption Keys**: Users must securely manage their encryption keys used for hiding and retrieving data.
- **Decrypt Data**: Users must use the correct decryption algorithms and keys to extract the hidden messages successfully

VI. SCOPE AND FUTURE WORK

The scope of the steganography system encompasses secure user management, data hiding and retrieval using various steganography techniques, encryption and decryption methods, system security, monitoring and reporting, performance optimization, and user experience enhancement. Future work will focus on integrating advanced steganography techniques such as machine learning and adaptive methods, implementing enhanced security measures like multi-factor authentication and advanced encryption standards, and expanding support to include video, audio, and text steganography. Additionally, the system will explore secure sharing and collaboration features, integration with blockchain for immutable logs and decentralized storage, automated monitoring and real-time alerts, and user education through tutorials and workshops, ensuring continuous improvement in security, usability, and functionality.

6.1 Proposed System Scope & Objectives

The proposed steganography system aims to provide a secure, efficient, and user-friendly platform for embedding and retrieving secret messages within images. Its scope includes secure user registration and profile management, tools for data hiding and extraction using various steganography techniques, robust encryption and decryption methods, and protection of user data from unauthorized access. The system will maintain activity logs, generate detailed reports, and ensure high performance and availability, even during peak usage times. Objectives include implementing strong security measures, achieving efficient system performance, providing detailed monitoring and reporting, designing a scalable and extensible architecture, and offering educational resources to help users effectively use the steganography tools.



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

VII. METHODOLOGY TO BE USED

DESIGN AND IMPLEMENTATION

This section contains a detailed description of components of software package, components of lowlevel and other sub-components of the projected work. Module design helps for the implementation of the modules. The modules area unit defined in the projected steganography models is initiated by the structure chart. Module's input needs and outputs generated by the modules area unit delineate during this section.

a) Data embedding: This is the method flow sheet for data embedding module to illustrate the initiation of security measures at the side of implementation of IWT and Genetic rule. The main purpose of this application is to point out the flow of information embedding operation involved in the process. The frequency domain illustration of the individual created blocks is calculable by 2 dimensional integer ripple transform in order to accomplish 4 sub bands LL1, HL1, LH1, and HH1. One to sixty four genes area unit generated containing the pixels numbers of each 8x8 blocks because the mapping operates. The bits of message in 4-LSBs IWT coefficients each component consistent with mapping functions area unit embedded. Consistent with fitness analysis, optimal component Adjustment process applied on the Image. At the end, inverse 2nd IWT is computed during this module in order to generate the stego image. The input for this process is largely a canopy image and user text message for embedding purpose.

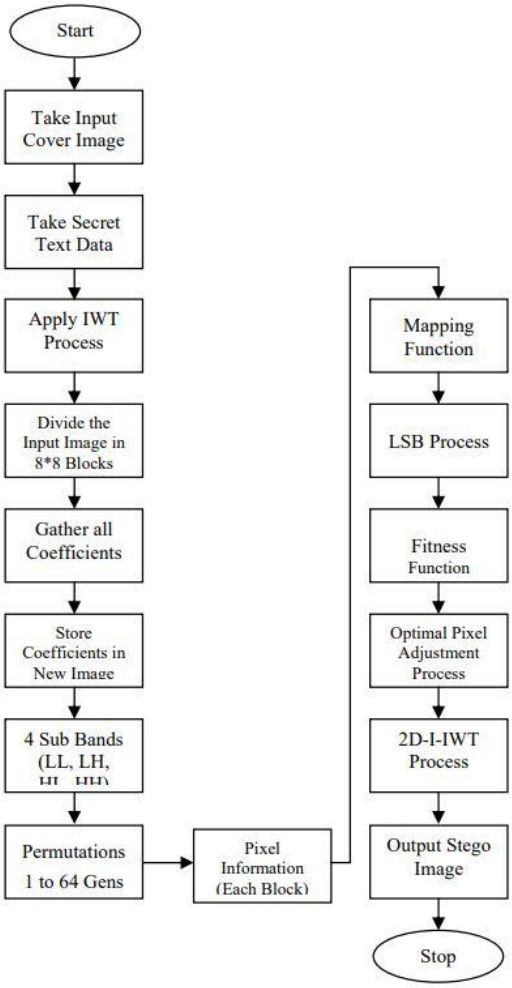


Fig.6 Flow Chart of the Data Embedding process

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

b) Message extraction: This is the method multidimensional language for message extraction module to illustrate the decipherment hidden text within the stego image. The most purpose of this application is to show the flow of message extraction operation involved within the process. This algorithmic rule primarily takes the input of the generated stego image from the embedding process and applies IWT together with decipherment Start Take Input Cover Image Take Secret Text Data Apply IWT Process Divide the Input Image in 8*8 Blocks Gather all Coefficients Store Coefficients in New Image 4 Sub Bands (LL, LH, HL HH) Permutations 1 to 64 Gens Pixel Information (Each Block) Mapping Function LSB Process Fitness Function Optimal Pixel Adjustment Process 2D-I-IWT Process Output Stego Image Stop 31 key to extract the secret text that has been hidden inside the stego image.

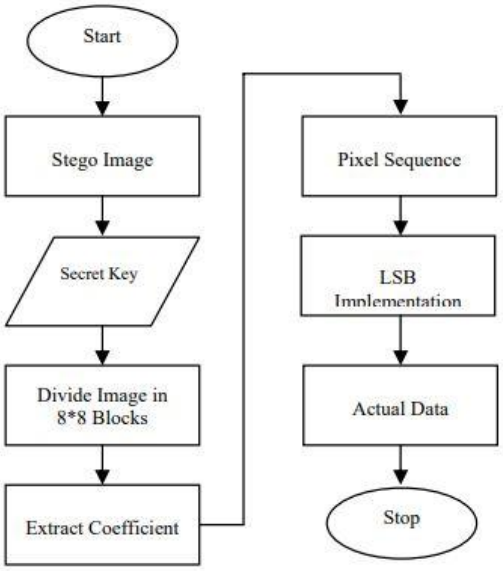


Fig.7 Flow Chart of the Data Extraction process

c) LSB implementation: This method flow chart will show the section wherever LSB is enforced. The most purpose of this method is to indicate LSB implementation. The major operation takes place when the appliance starts getting the size of the cover image and then it creates a tree structure for ease in computation.

VIII. CONCLUSION

A new approach is proposed which gives good quality of the image after encoding the original image by using the LSB technique. Data is encrypted with a password protected system and if third party get the stego image and try to decrypt the stego image, it will not dercrypt and the data will still show in encrypted form. This method helps to enhance the security level of data being embedded. The combination of encryption with steganography further enhances the security level. The image resolution doesn't change much and is negligible when we embed the message into the image and the image is protected with the personal key.

IX. FUTURE WORK

The future work on this project is to improve the compression ratio of the image to the text. Further enhancements can be made to the application, so that the web site functions very attractive and useful manner than the present one.

X. ACKNOWLEDGEMENT

It plunges us in exhilaration taking privilege in expressing our heartfelt gratitude to all those who helped, encouraged and foreseeing successful completion of our project to work under gregarious guidance of Prof T. S. Deshmukh to whom we are extremely indebted for his valuable and timely suggestions. We wish to convey our sincere thanks to

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

Prof. V. V. Shirashyad, for making resources available for completing project work in time, also we would like to give our thanks to all teaching and non-teaching staff members and peons for their excellent support. We would also like to thanks to all those who had directly or indirectly contributed their assistance in finishing out this project successfully. Finally, we wish to thank our parents and friends for being supportive to us, without whom this project could not have seen light of the day.

REFERENCES

[1]. Sneha, B. and Gunjan, B (2014) Data Encryption by Image Steganography. International Journal of Information and Computation Technology, 4, 453-458. http://www.irphouse.c om/ijict.htm

[2].Silman, J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001

[3]. Philip Bateman and Dr. Hans "Image Steganography and Steganalysis", M.S., Department of Computing Faculty of Engineering and Physical Sciences, University of Surrey Guildford Surrey,United Kingdom, 2008.

[4].Hiding data in images by simple LSB substitution by ChiKwong Chan, L.M.Cheng Department of Computer Engineering and Information Technology, City University of Hong Kong, Hong Kong Received 17 May 2002.

[5]. S. Dickman, An Overview of Steganography, Research Report JMU- INFOSEC-TR -2007-002, James Madison University, July, 2007.

[6]. S.B.Sadkhan, Cryptography: Current status and future trends, in: Proceedings of IEEE International Conference on Information & Communication Technologies: From Theory to Applications, Damascus. Syria, April 19-23, 2004, pp. 417-418.

[7]."A Tutorial Review on Steganography" by Samir K Bandyopadhyay, Debnath Bhattacharyya1, Debashis Ganguly1, Swarnendu Mukherjee1 and Poulami Das,Heritage Institute of Technology.

[8]. An overview of image steganography by T. Morkel , J.H.P. Eloff, M.S. Olivier. Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa.

[9]. Prabakaran, G.; Bhavani, R.; Rajeswari, P.S., "Multi secure and robustness for medical image based steganography scheme," Circuits, Power and Computing Technologies (ICCPCT), 2013 International Conference on , vol., no., pp.1188,1193, 20-21 March 2013.

[10]. Akhtar, N.; Johri, P.; Khan, S., "Enhancing the Security and Quality of LSB Based Image Steganography," Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on, vol., no., pp.385, 390, 27-29 Sept. 2013

[11]. Lin Zhang, Jianhua Wu, Nanrun Zhou, "Image Encryption with Discrete Fractional Cosine Transform and Chaos", Fifth International Conference on Information Assurance and Security 2009 IAS '09, pp 61 – 64, 2009.

[12]. The WEPIN Store, "Steganography (Hidden Writing)", 1995, http://www.wepin.com/pgp/stego.html.

[13]. Steganography and Steganalysis by J.R. Krenn January 2004. International Journal of Engineering Science and Computing, April 2017 10624 http://ijesc.org/

[14]. C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, and M. Miller, "Rotation

[15]. Niels Provos, Peter Honeyman,"Hide and Seek: An Introduction to Steganography," IEEE computer society,2003. scale, and translation resilient public watermarking for images," IEEE Trans. Image Process., vol. 10, no. 5, pp. 767-782, May 2001.

[16]. A. Cheddad, J. Condell, K. Curran and P.M. Kevitt. (2010). "Digital image steganography: survey and analysis of current methods." Signal Processing Journal.

[17]. International Journal of Computer Science Engineering Technology (IJC-SET)"Modern Steganographic technique: A Survey" by Pratap Chandra Mandal Asst. Prof., Department of Computer Application B.P.Poddar Institute of Management Technology.

[18]. Data hiding Algorithm for Bitmap Images using Steganography by Mamta Juneja Department of computer science and Engineering, RBIEBT, Sahuran.

[19]. Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav / International Journal of Engineering Research and Applications (IJERA) ISSN: 22489622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, Steganography Using Least Signicant Bit Algorithm.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

[20].Journal of Theoretical and Applied Information Technology 15th February 2012. Vol. 36 No.1. A steganography algorithm for hiding image in Image by improved lsb substitution by minimize Detection by vijay kumar sharma, vishal shrivastava M.Tech. scholar, Arya college of Engineering IT, Jaipur , Rajasthan.
[21] T. Morkel, J.H.P. Eloff, M.S. Olivier, An Overview of Image Steganography, Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa.
[22] Domenico Bloisi and Luca Iocchi, Image based steganography and cryptography, International Journal of Computer Applications, 2010.
[23] V. Lokeswara Reddy, Dr. A. Subramanyam, Dr.P. Chenna Reddy, Implementation of LSB Steganography and its Evaluation for Various File Formats, Int. J. Advanced Networking and Applications, Volume: 02, Issue: 05, Pages: 868-872 (2011).
[24] Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi, A Survey on Image Steganography and Steganalysis, Journal of Information Hiding and Multimedia Signal Processing, Volume 2, Number 2, April 2011.
[25] A. Joseph Raphael, Dr. V. Sundaram, Cryptography and Steganography – A Survey, Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630, ISSN:2229- 6093, 2010.
[26] Amitava Nag, Sushanta Biswas, Debasree Sarkar, Partha Pratim Sarkar, A Novel Technique for Image Steganography Based on DWT and Huffman Encoding, International Journal of Computer Science and Security, (IJCSS), Volume (4): Issue (6), 2011.
[27] H S Manjunatha Reddy, K B Raja, High capacity and security steganography using discrete wavelet transform, International Journal of Computer Science and Security (IJCSS), Volume (3): Issue (6), 2011.
[28] Amin Milani Fard, Mohammad-R. Akbarzadeh, Farshad Varasteh, A New Genetic Algorithm Approach for Secure JPEG Steganography, Engineering of Intelligent Systems, IEEE International Conference, 2006.
[29] Yun Q. Shi, Hyoung Joong Kim, Digital Watermarking, 6th International Workshop, IWDW 2007 Guangzhou, China, December 3-5, 2007, Proceedings Springer, 2008.
[30] Shreelekshmi R, M Wilscy and M Wilscy, Preprocessing Cover Images for More Secure LSB Steganography, International Journal of Computer Theory and Engineering, Vol. 2, No. 4, August, 2010.
[31] Taras Holotyak, Jessica Fridrich, and David Soukal, Stochastic Approach to Secret Message Length Estimation in ±k Embedding Steganography, Communications and Multimedia Security 2005.
[32] El Safy, R.O, Zayed. H. H, El Dessouki. A, "An Adaptive Steganographic Technique Based on Integer Wavelet Transform", IEEE conference, 2009, pp 111- 117.