ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 11, November 2013

Image Steganography Based On DCT Algorithm for Data Hiding

Suchitra. B, Priya. M, Raju.J

Abstract- The main aim of steganography is to conceal a secret memo into a host image in a way that the host should stay as alike as probable in older version. The big benefit of steganography and cryptography is it didn't give more notice to attackers and recipients. In this globe the significant problem of modern communication is launching the communication in public channel that is attain by steganography. In this paper we introduce a new steganography called statistically invisible steganography (SIS) to hide date in jpeg image. And we embed the information in the choosy coefficients of the selective dct block that have high complexity .it is safety and worth able comparing to the existing techniques.

Index Terms-Steganography, Cover image, Security, Discrete cousine transform, Least significant bit

I.INTRODUCTION

Most of the recent researchers concentrates on security i.e keeping our information from the attackers and hackers. Transmitting the information over the communication media in secure way it can be attained by steganography. The advance security is not sustained by the password security but is achieved by hiding the existence of information, which can done by steganography.steganography systems can hide message inside of digital objects such as file that has been hided inside a digital picture, video or audio file. The steganography and cryptography is used to guarantee the security of the secret message.steganography can be accomplished by hiding the existing information within seemingly harmless cover or carriers. The cover can be text, image, video, audio, etc.there are other types of information hiding are there, they are watermaking and cryptography. In watermaking communication is the host signal, with the protected data providing copyright protection. The existence of watermark is often declared as openly. If anyone try to remove or invalidate the protected data's renders the host useless. In cryptography is the most used field to hide the msg from hackers and send the msg from source to destination in secure manner.jpeg steganography with a complementary embedding strategy was presented. By using these we can disable lots of steganalysers such as chi-square family and s family detectors, this are been used to harass j-steg,jphide and f5.[1] in this paper they described about the robust method for image hiding that uses the notion of texture similarity among host and secret images using Gabor filter.[2]in this paper they discussed about the steganalytic method that can simply notice the messages from jpeg images using steganography algorithm yass.[3] in this paper they purpose a high performance jpeg steganographic method .that protects the complementary embedded strategy to avoid the detection of numerous attacks.[4]in this paper they compares the jhrf algorithm with fr algorithm. And establish that jhrf algorithm can find better experimental result then fr. [5] it describes about the coherent steganographic technique using dct and segmentation. Here the cover image is divided into blocks and dct have been applied to each block.

II. STEGANOGRAPHY

Steganography comes from the Greek and literally means "secret writing or covered". Nowadays in this modern globe privacy, safe and secrecy is must for the internet users. The former uses of steganography are for conveying the top secret files and documents among worldwide governments. The mainly used method today is hiding of covert msg into a digital image is steganography.the steganography method take advantage of the weakness of the human visual system. The persons cannot easily find the hidden information in the image. The vital objective of steganography is to hide the data from the attackers view and securely transmit the data over the image from source to destination.

A. JPEG image

Jpeg stands for joint photographic expert group is a compressed file format. Contrasting to the original image jpeg image size will be lesser. Benefits of jpeg are produce a small image size, ideal for most images and uses more colours, drawbacks are high compression loses quality. By using steganography in image it make changes to the image and invisible to the human eye. Some of the jpeg steganographic methods are j-steg, jphide, f5 and outguess. The jpeg file formats have been used in steganography, it is used in the images to hide the information and secure the information between two parties.

III.JPEG STEGANOGRAPHY DESIGN

A. Embedding Design Process

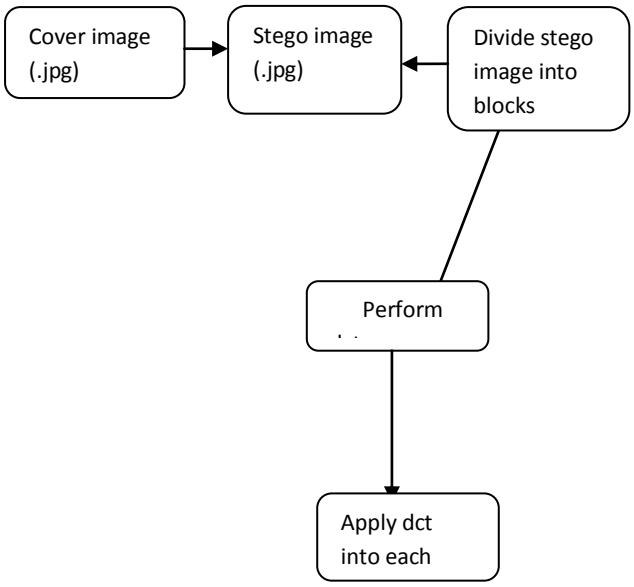

Fig 1.Embedding design process

Cover Image
The cover image is used to hide the information or data in it. It will be more secure, the cover image in modern communication such as text, video, audio, imge.
Stego Image
The stego image is after hiding the data in a cover image we will get the stego image.
Steganalysers
This is the process of finding the secret memo by using different factors in stego image. In this process its major steps to recognize a suspected stego image. Then the steganlysers will verify the stego image holds hidden information and then it will try to recover the records from it. From the optical detection steganalysers technique, an original cover image is matched with the stego image and notes the visible modifies in it. The unique hidden data will be found out by comparing these two images. The other evidence of visual hidden information is cropping or padding. The dissimilarity in file size between stego image and cover image reduces or raises of unique colours in stego image can be used in visual detection steganalysers attack. Some of the steganalysers such as chi-square family detectors and s family detector.

Steganography Harass
The harass here consists of finding, extracting and spoiling the hidden data in stego image.steganography harass is followed by steganalysers.some of the attacks are,

- CARRIER HARASS: the original stego image and cover image both are used for the analysers.
- ONLY STEGANOGRAPHY HARASS: only the stego image is used for analysers.
- MESSAGE HARASS: the hidden information is known in this case.
- STEGANOGRAPHY HARASS: stego media, cover media and steganography tool or algorithm are known

B. Decreation Of Stenography

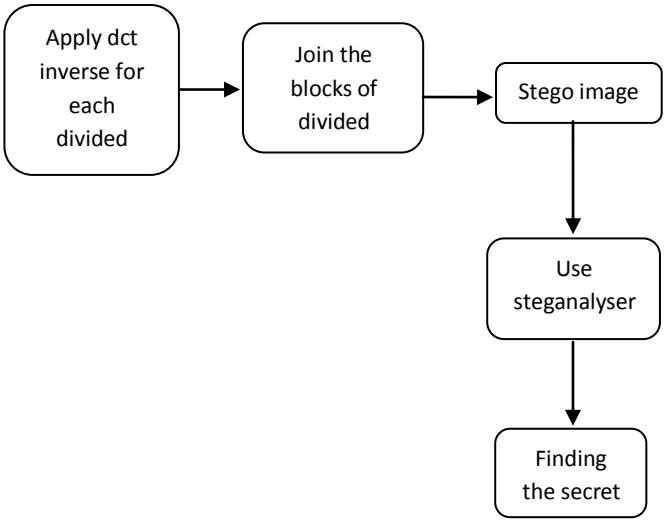

Fig 2.Decreation of Steganography

C.Detailed System Design

LEVEL 0:

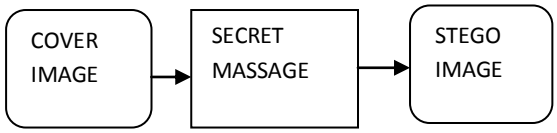

Fig 3.Level 0

LEVEL 1:

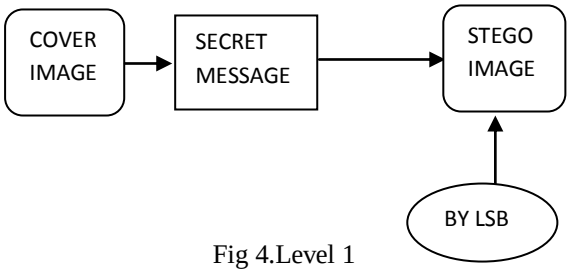

Fig 4.Level 1

LEVEL 2:

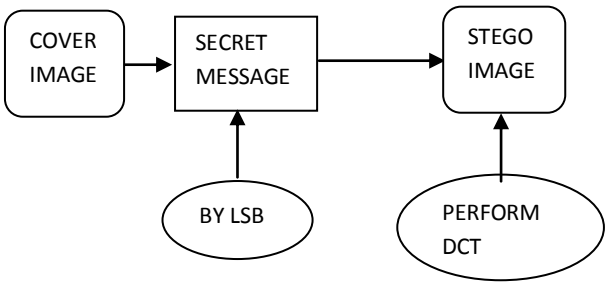

Fig 5.Level 2

LEVEL 3:

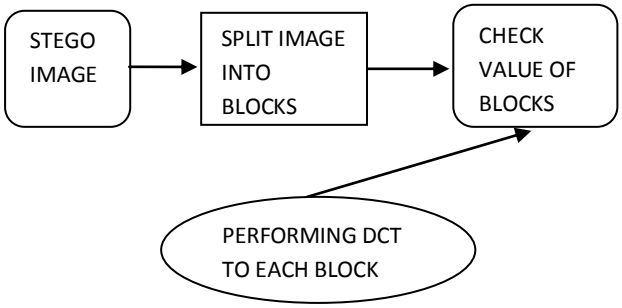

Fig 6.Level 3

In level0 the secret message is send to cover image then the cover image will be converted to block image. In level1 the message is not hidden by attackers by performing the lsb in message. In level2 we must apply the dct for stego image. In level 3 the stego image have been divided into blocks and for each block we apply the dct.the applying of dct for each block avoid the steganalysers attack.

IV.DCT

Divide the stego image into blocks; the image is splitter into 8*8 pixels, labouring from top to bottom, left to right, the dct have been applied to each block. The dct efforts to decorrelate the image data, the dct have been classified into one dimensional dct, two dimensional dct, the quantised discrete cousine transform coefficient and the qdct coefficient histogram will be used for inserting the secret message.

A.Dependencies Of Block

Inter block dependencies-Here it will check the histogram of stego image; it will show the modifications and steganalysers attack of secret message. Here the whole image is taken for the calculation.

Intra block dependencies-Here the stego image will be splitted; the steganalysers cannot find the hidden message .here the operations have been performed by block by block.

B.Least Significant Bit Technique

The LSB have been used to conceal the data in the image. The LSB insertion varies according to the number of bits in an image. For 24-bit image the colours red, green and blue have been changed. For an 8-bit image, the eighth bit of the each image is changed to the bit of secret message.

V.CONCLUSION

Today in this insecure world transmitting of data from source to destination is very important, because the transmitting message can be easily hacked by attackers and hackers, hence the efficient way of transmitting the data over jpeg image can be done by steganography, here the stego image have been divided into blocks so this the advantage of the users, by the steganalysers cannot be able to find the secret msg in the image.

REFERENCES

1. Zahara zahedi kermani and Mansour jamzad,"a robust steganography algorithm based on texture similarity using Gabor filter".

2, Xiaoyi yu and Noboru babaguchi,"breaking the yass algorithm via pixel and dct coefficient analysis".
3. Mohammed ishaque, Dr.Syed abdul sattar,"quality based jpeg steganography using balanced embedding technique".
4. Tang ming-wei ,Wang gaug-wei, Fan ming-yu and Li-wei,"an jpeg information hiding algorithm of resisting Fr".
5.K.b Shivakumar, k.b.Raja, r.k.Choutay and Sabyasachi pattnaik,"coherent steganography using segmentation and dct".
6. Saman Shojae Chaeikar, Azizah Bt Abdul Manaf and Mazdak Zamani. Comparative analysis between Master key and Interpretative Key Management (IKM) Framework to provide utilization guideline for researchers and developers. Cryptography and Security in Computing, ISBN: 978-953-51-0179-6. Publisher online InTech.2012.
7. Mazdak Zamani, Azizah Bt Abdul Manaf, Shahidan M. Abdullah,Saman Shojae Chaeikar. Mazdak Technique for PSNR Estimation in Audio Steganography. 2012 International Conference on Mechanical and Electrical Technology (ICMET 2012). July24-26, 2012, Kuala Lumpur, Malaysi
8. Shahidan M. Abdullah, Azizah A. Manaf, and Mazdak Zamani. Recursive Reversible Image Watermarking Using Enhancement of Difference Expansion Techniques. Journal of Information Security Research. Volume 1 Number 2. June 2010. Pages 64-70.
9. Concerns for Hiding Information in Text" Technical Report, Center for Education and Research in Information Assurance and Security (CERIAS), 2004.
10. J.M. Rodrigues, J.R. Rios and W. Puech." SSB-4 System of Steganography using Bit 4". Proc. 5th International Workshop on Image Analysis for Multimedia Interactive Services, (WIAMIS'04), Lisboa, Portugal, April 2004.
13.R. Chandramouli, M. Kharrazi, N. Memon, "Image Steganography and Steganalysis: Concepts and Practice " , International Workshop on Digital Watermarking, Seoul, October 2004.
14. Westfield, A., and A. Pfitzmann. "Attacks on Steganographic Systems -Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and Stools - and Some Lessons Learned," Lecture Notes in Computer Science,
1768: 61-75 (2000).
15. Fridrich ,J, M. Goljan, and R. Du, "Detecting LSB steganography in color and grayscale images," IEEE Multimedia Special Issue on Security, pp.22–28, October- November 2001.
16. Fridrich, J., M. Goljan, , H. Dorin ,"Steganalysis of JPEG Images: Breaking the F5 Algorithm". Information Hiding 2002, pp. 310-323.
17. Provos, N. and P. Honeyman. "Hide and Seek: An Introduction to Steganography." IEEE Security & Privacy, 2003.
18. OutGuess Web Site ."Steganography Detection with Stegdetect ."URL: http://www.outguess.org/detection.php.Last accessed: 2004
19. Fridrich, J., Goljan, M., and Hogea, D. " Attacking the OutGuess". In:Proceedings of the ACM Workshop on Multimedia and Security 2002,Juan-les-Pins, France, December 2002.
20. Hatim A. Aboalsamh, Sami A. Dokheekh, Hassan I. Mathkour, Ghazy M.Assassa. "Breaking the F5 Algorithm: An Improved Approach", Egyptian Computer Science Journal Vol.29 No 1. January 2007, pp 1-9.

Ms.Suchitra.B is a student of final year MCA in School of Information Technology & Engineering ,VIT University ,Vellore

Prof.Priya.M, working as a Assistant Professor Senior in School of Information Technology & Engineering ,VIT University ,Vellore.She has published so many papers in networks and data mining.

Prof.Raju.J , working as a Assistant Professor Selection Grade in School of electrical and ElectronicsEngineering ,VIT University ,Vellore.He has published so many papers in power electronics.