ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 2, Issue 5, May 2013*

# Watermarking of Images in Discrete Cosine transform

Prof. Priya Pise[1], Prof. R M Goudar[2]
Department Of IT Indira College of Engeneering & Management, Pune, India[1]
Department of Computer, MITAOE, Alandi (D), Pune, India[2]

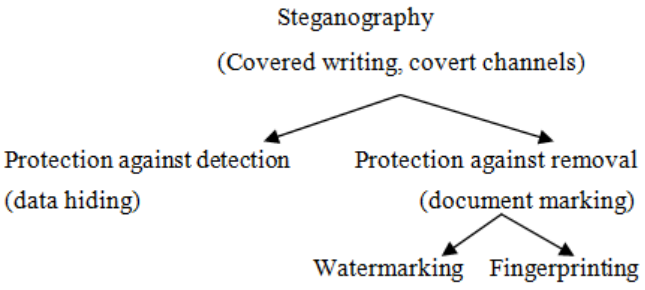
**Abstract:** Data embedding is simplest technique to achieve the secret data sharing information. Now days a color image is a very popular to consider cover image medium used to send the secret data. I have proposed an approach for hiding a secret image in a cover image. In the beginning, the DCT [8] of image is computed that is compress the secret image, and then encrypt cover data by DES. Various authors have proposed many watermarking algorithms. These algorithms are implemented in ether the spatial, frequency or wavelet domains. But which algorithms are better? Is embedding a watermark in one domain better than another? Do combining domains result in a better watermarking algorithm? This report attempts to answer these questions by selecting eight algorithms and analyzing them. Of these eight algorithms 2 embeds the watermark in the spatial domain, 2 in the frequency domain, 2 in the wavelet domain, one in a combination of frequency and spatial domain. Do to the wide variety of algorithms a standard benchmark is also developed, within this report, to analyze the algorithms. In this work, the steganographic paradigm of data hiding in digital images has implemented. Several algorithms based on this approach exist in literature and the strengths and limitations of these algorithms are mentioned. Two existing algorithms which secures a cover image during embedding and DCT [9] algorithm embeds secrete image into a cover image while inherently preserving the first order statistics of the image. Finally, embed the cover image into the middle-frequency domain of DCT [1]. After embedding the secret image, the goal of steganography can be successfully achieved .The proposed algorithms are successful in embedding the image in bit alteration .The purpose of this project is provide n-Bit security.

*Keywords* - Steganography, data hiding, fractal image compression, DCT,BCBS

## I. INTRODUCTION

Steganography is the art of hiding information imperceptibly in a cover medium. The word "Steganography" is of Greek origin and means "covered or hidden writing". The main aim in steganography is to hide the very existence of the message in the cover medium. Steganography and cryptography are counter parts in digital security the obvious advantage of steganography over cryptography is that messages do not attract attention to themselves, to messengers, or to recipients. Also, the last decade has seen an exponential growth in the use of multimedia data over the Internet. These include Digital Images, Audio and Video files. This rise of digital content on the internet has further accelerated the research effort devoted to steganography. The various applications of steganography include secure military communications, multimedia watermarking and fingerprinting applications for authentication purposed to curb the problem of digital piracy. Although these are not perfect applications of steganography, many steganographic algorithms can be employed for these purposes as well.

Here it shows how information hiding can be broken down into different areas. Steganography can be used to hide a message intended for later retrieval by a specific individual or group. In this case the aim is to prevent the message being detected by any other party. The other major area of steganography is copyright marking, where the message to be inserted is used to assert copyright over a document. This can be further divided into watermarking and fingerprinting




## II. REVIEW OF TECHNIQUE USED

**1.DCT (Discrete Cosine Transform) :** A discrete cosine transform (DCT) is a sequence of finitely many data points

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 2, Issue 5, May 2013*

in terms of a sum of cosine functions oscillating at different frequencies. From lossy compression of audio and images to spectral methods for the numerical solution of partial differential equations , it turns out that cosine functions are much more efficient , whereas for differential equations the cosines express a particular choice of boundary conditions.

**2. Data Encryption Standard:** A DES key consists of 64 binary digits ("0"s or "1"s) of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, may be used for error detection. The 8 error detecting bits are set to make the parity of each 8-bit byte of the key odd, i.e., there is an odd number of "1"s in each 8-bit byte 1 . A TDEA key consists of three DES keys, which is also referred to as a key bundle. Authorized users of encrypted computer data must have the key that was used to encipher the data in order to decrypt it. The encryption algorithms specified in this standard are commonly known among those using the standard.

## III. REVIEW OF COMPRESSION ALGORITHMS

**Chin-Chen Chang** discussed [1] that proposed model does the data embedding into the cover image by changing the coefficients of a transform of an image such as discrete cosine transform. The high compression rate is one of the advantages of fractal image compression. Main advantage is the good image quality, after enough iteration for decompression. But the computation time required to encode an image might be very long due to an exhaustive search for the optimal code. And DES encryption is used to provide the security to the data, but it is unable to protect the Stego-Image from subterfuge attack. Which is nothing but , the attacker not only detect a message, but also render it useless or even worse, modify it to the opponent's favor.

**K.B.Raja** [1] has proposed a model which uses LSB ,but LSB provides poor security ,and DCT for converting objects in spatial domain to frequency domain. This model uses only raw Images because of *subterfuge attack*. The JPEG, BMP and GIF image formats, the header contains most of the image information. This leads to the problem of insecurity and therefore the payloads from such images can be easily identified.

**A.Mascher- Kampfer** [3] has found PSNR(Peak Signal To Noise Ratio) to be a good indicator of finger and face recognition matching scores in the case of JPEG2000 and SPIHT. Both wavelet-based algorithms perform exceptionally well in terms of rate-distortion performance and matching scores of all recognition systems considered. While PSNR exactly predicts the poor matching scores of fractal compression the case of fingerprint images, the relatively high PSNR results for face images suggest fractal compression to perform superior to JPEG for this biometric modality. The opposite is true – despite the low PSNR results, JPEG performs quite well in face recognition applications for high and medium bit rate applications with respect to matching results.

**Chin-Chen Chang** [3] He has proposed a scheme to embed an image compressed via fractal image compression into the DCT domain of the cover image. Due to the high compression rate of fractal compression, also it can embed a secret image larger than the cover image itself. Moreover, the more decompression iterations will be done, the better decompressed secret image quality will get. Also, these compression codes of fractal compression must not be lost, or the embedded message cannot be extracted. Thus some modification on the bit streams of the modified coefficients to prevent the information loss caused by discrete cosine transformation. As for security, encrypt the compressed data

**Chaur-Chin Chen** [4] has only reviewed and summarized the characteristics of four up-to-date image coding algorithms based on Wavelet, JPEG/DCT, VQ, and Fractal approaches. Experimental comparisons on four 256×256 commonly used images, Jet, Lenna, Mandrill, Peppers, and one 400×400 fingerprint image suggest a recipe described as follows. Any of the four approaches is satisfactory when the 0.5 bits per pixel (bpp) is requested. Hence for practical applications, he concluded that wavelet based compression algorithms are strongly recommended.
Following are some measurements used to evaluate the performances of lossless algorithms.

**1.Compression Ratio** is the ratio between the size of the compressed file and the size of the source file. Compression Factor is the inverse of the compression ratio. That is the ratio between the size of the source file and the size of the compressed file. Saving Percentage calculates the shrinkage of the source file as a percentage. % size before compression saving percentage size before compression size after compression All the above methods evaluate the effectiveness of compression algorithms using file sizes. There are some other methods to evaluate the performance of compression algorithms. Compression time, computational complexity and probability distribution are also used to measure the effectiveness.

**2.Entropy** This method can be used, if the compression algorithm is based on statistical information of the source file. Self Information is the amount of one's surprise evoked by an event. In another words, there can be two events: first

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 2, Issue 5, May 2013*

one is an event which frequently happens and the other one is an event which rarely happens. If a message says that the second event happens, then it will generate more surprise in receivers mind than the first message.

**3. Error Computation** (i) Bit error rate (BER): Here we compute the BER for two equal size images that is cover image and stego-image. BER is more accurate for error vector quantization may not need great codebook storage having simple encoding and decoding algorithm. Hence high compression ratio can be accomplished by including PVQ
along with MSVQ.

## IV. ACTUAL ALGORITHM USED

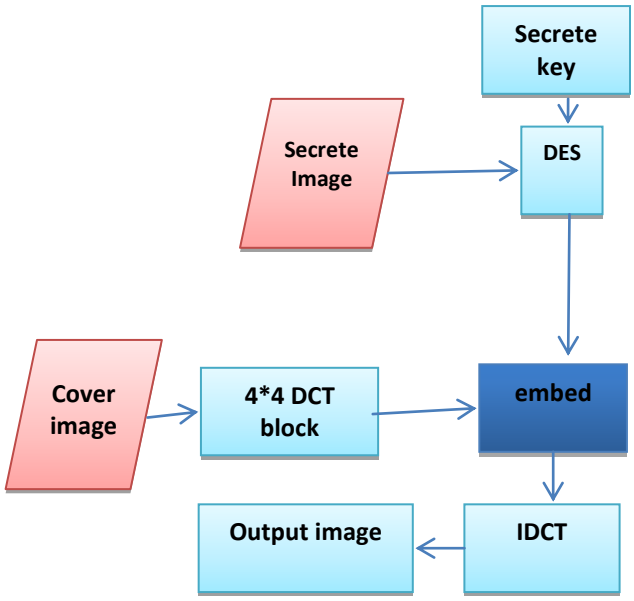



*Figure 1 : System Model*

## V. ALGORITHMIC STEPS

1. For cover image do
2. Apply DES
3. for cover image > secrete image do
4. Apply DCT
5. Apply bit alteration as 1-Bit , 2-Bit ,3-Bit
6. Store it as Stego Image with precise name
7. End for
8. End for
9. Open the stego image
10. Try to apply the same bit alteration method
11. Save the destination image as .bmp or .jpg or .tiff or .gif or .png type.
12. Calculate the quality and PSNR for all extracted and embedded images
13. Calculate the quality and PSNR for various bit altering methods to prove the level of security
14. Make entry in a notepad file about the current PSNR .

## VI. MEASURING COMPRESSION PERFORMANCES

There are different criterion for measuring the performance of the compression also it depends on the nature of the application .When measuring the performance the main concern would be the space efficiency. The time efficiency is another factor. Since the compression behavior depends on the redundancy of symbols in the source file, it is difficulty to measure performance of a compression algorithm in general. The performance depends on the type and the structure of input source. Additionally the compression behavior depends on the category of the compression algorithm: lossy or lossless. If a lossy compression algorithm is used to compress a particular source file, the space efficiency and time efficiency would be higher than that of the lossless compression algorithm. Thus measuring a general performance is difficult and there should be different measurements to evaluate the performances of those compression families.

Following are some measurements used to evaluate the performances of lossless algorithms.

**1.Compression Ratio** is the ratio between the size of the compressed file and the size of the source file. Compression Factor is the inverse of the compression ratio. That is the ratio between the size of the source file and the size of the compressed file. Saving Percentage calculates the shrinkage of the source file as a percentage % size before compression saving percentage size before compression size after compression All the above methods evaluate the effectiveness of compression algorithms using file sizes. There are some other methods to evaluate the performance of compression algorithms. Compression time, computational complexity and probability distribution are also used to measure the effectiveness.

**2.Entropy** This method can be used, if the compression algorithm is based on statistical information of the source file. Self Information is the amount of one's surprise evoked by an event. In another words, there can be two events: first one is an event which frequently happens and the other one is an event which rarely happens. If a message says that the second event happens, then it will generate more surprise in receivers mind than the first message.

**3.Code Efficiency** Average code length is the average number of bits required to represent a single code word. If the source and the lengths of the code words are known, the average code length can be calculated .

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 2, Issue 5, May 2013*

**4. Error Computation** (i) Bit error rate (BER): Here we compute the BER for two equal size images that is cover image and stego-image. BER is more accurate for error analysis when compared to MSE, because in BER we compute the actual number of bit positions which are replaced in the stego image , which is calculated by

$$H(e) = \sum_{i=0}^{m-1} p(e_i)\log_2 p(e_i)$$

**5. Mean square error (MSE)**: The MSE is computed by performing byte by byte comparisons of the two images, since
a pixel is represented by 8 bits and hence 256 levels are available to represent the various gray levels.

## VII. CONCLUSION

In this work, I have studied and implemented the steganographic paradigm of data hiding in digital images. Two approaches prevalent in current steganographic research were studied .Several algorithms based on this approach exist in literature and the strengths and limitations of these algorithms are mentioned .Two existing algorithms which secures a cover image during embedding and DCT algorithm embeds secrete image into a cover image while inherently preserving the first order statistics of the image. Finally, we embed the cover image into the middle-frequency domain of DCT[4]. After embedding the secret image ,the goal of steganography can be successfully achieved .The proposed algorithms are successful in embedding the image in bit alteration .The purpose of this project is provide bitwise security also save memory and provide 2 sided security.

## REFERENCES

[1] K. Munivara Prasad, V.Jyothsna, S.H.K. Raju, S.Indraneel "High Secure Image Steganography in BCBS Using DCT and Fractal Compression" , IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010
[2] Huirong Qi Wesley E. Snydel; William A. Sunder "Blind consistency based steganography for information hiding in digital media", International Conference on Images Steganography May 2010.
[3] Chin-Chen Chang, Chi-Lung Chiang, and Ju-Yuan Hsiao "A DCT-domain System for Hiding Fractal Compressed Images" 19th International Conference on Advanced Information Networking and Applications (AINA'05) 2010
[4] K.B.Raja, C.R.Chowdary, Venugopal K R, L.M.Patnaik "A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images "International conference on Image and Signal Processing ,2009
[5] Neil F. Johnson, Sushil Jajodia, George Mason University "Exploring steganography, seeing the unseen," IEEE Conference , February 2008.
[6] Neils Provos, Peter Honeyman "Hide and Seek: An Introduction to Steganography," IEEE SECURITY & PRIVACY computer society ,2008
[7] Ross J. Anderson and Fabien A. P. Petitcolas " On the Limits of Steganography " IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 16, NO. 4, MAY 2007
[8] A. K. Jain and U. Uludag." Hiding biometric data". IEEE Trans Pattern Analysis and Machine Intelligence, 25(11):1494–1498, 2003
[9] BRASSIL, J.T, LOW, S, MAXLMCHUK, K.F and O'GORMA, "Steganalysis Using Higher-Order Image Statistics". IEEE Transactions on Information Forensiscs and Security,Vol 1,NO.1,USA, 2006.
[10] Nehaluddin Ahmad 'Restrictions on cryptography in India – A case study of encryption and privacy', computer law & security review 25 (2009) 173–180
[11] Anjali A. Shejul, Prof. U.L Kulkarni , 'A DWT based Approach for Steganography Using Biometrics' , IEEE International Conference on Data Storage and Data Engineering 2010
[12] Artech House Compute "Information Hiding Techniques for Steganography and Digital Watermarking", IEEE Trans Pattern Analysis and Machine Intelligence 2001
[13] J. Fridrich, Niels Provos, "Applications of data hiding in digital images," Tutorial for the ISSPA'99 Conference, Brisbane, Australia, , December 2004.
[14]R.Anderson and F. Petitcolas, "Defending against statistical steganalysis", In Proceedings of the 10th USENIX Security Symposium, August 2001.
[15] D.C.Wu and W.H.Tsa" Spatial-domain image hiding using image Differencing" IEEE Proc.-Vcs. hncige Signal Process, 2000.
[16] Bing Zuo , De-Quan Zhou , " Investigation of Robust Digital Watermarking Based on Multi-Level DCT" Industrial Control and Electronics Engineering (ICICEE), 2012
[17] sa, Mohd Rizal , Mohd Aljareh Salem ," Biometric image protection based on discrete cosine trasnsform watermarking technique " Engineering and Technology (ICET), International Conference 2012.
[18].R M Goudar , Priya Pise , "Compression Technique using DCT & Fractal Compression – A Survey" ,IFRSA's International Journal Of Computing|Vol2|issue 1|January 2012
[19].R M Goudar ,Priya Pise, "Study Of Compression technique using DCT & Fractal Compression", International Conference on RECENT TECHNOLOGIES 9th – 11th February 2012
[20].Beenish Mehboob and Rashid Aziz Faruqui "A Stegnography Implementation", Inernational conference on image steganography 2008 IEEE
[21] Information Hiding Techniques for Steganography and Digital Watermarking, Artech House Compute. 2000.
[22] J. Fridrich, "Applications of data hiding in digital images," in Tutorial for the ISSPA'99 Conference, Brisbane, Australia, August 1999, pp. 22-25.
[23] MARVEL, L.M., BONCELET, C.G., Jr., and RETTER, C.T
[24] " Spread Spectrum Image Steganography" IEEE trans. Image Process8(8), Aug 1999, pp.1075-1083
[25] Fast Algorithm of the DCT and IDCT for VLSI Implementation Mong Ying Hou Zhaohuan Institute of Acoustics, Chinese Academy of Sciences
[26] A. K. Jain and U. Uludag. Hiding biometric data. IEEE Trans. Pattern Analysis and Machine Intelligence, 25(11):1494–1498, 2003
[27] N. F. Johnson and S. Katzenbeisser. A survey of steganographic techniques, Information Hiding. Artech House, Norwood
[28] Y. Fisher, Editor, "Fractal Image Compression: Theory and Applications", Springer-Verlag, 1994.
[29] A Review of Image Compression and Comparison of its Algorithms Sachin Dhawan Deptt. of ECE, UIET, Kurukshetra University, Kurukshetra, Haryana, India,May 2011
[30] "On the Selection of Image Compression Algorithms " Chaur-Chin Chen Department of Computer Science National Tsing Hua UniversityHsinchu 300, Taiwan