Scientific Journal of Impact Factor (SJIF) : 3.134

ISSN (Print) : 2348-6406
ISSN (Online): 2348-4470

International Journal of Advance Engineering and Research Development

A NOVEL DESCENT TECHNIQUE FOR DIGITAL IMAGES STEGANOGRAPHY BASED ON MODIFIED DISCRETE COSINE TRANSFORM & HUFFMAN CODING

Sheetal Kharab [1], Dr. Shelly Garg [2], Mr. Kapil [3]

[1] *Scholar, M.Tech , Indus Institute of Engineering & Technology, Jind (India), sheetalrana89@gmail.com*
[2] *Professor, Dept. of ECE, Indus Institute of Engineering & Technology, Jind (India), S.singla428@gmail.com*
[3] *Assistant Professor, Dept. of ECE, Indus Institute of Engineering & Technology, Jind (India), sachkapil10@gmail.com*

Abstract—*In the recent years image steganography techniques can be divided into two groups: those in the Image Domain and those in the Transform Domain. Image – also known as spatial – domain techniques embed messages in the intensity of the pixels directly, while for transform – also known as frequency – domain, images are first transformed and then the message is embedded in the image.*
Image domain techniques encompass bit-wise methods that apply bit insertion and noise manipulation and are sometimes characterized as "simple systems". The image formats that are most suitable for image domain steganography are lossless and the techniques are typically dependent on the image format.

Keywords: *Paper format, publish, template, sample*

I. INTRODUCTION

With the development of Internet technologies, digital media can be transmitted conveniently over the Internet. However, message transmissions over the Internet still have to face all kinds of security problems. Therefore, how to protect secret messages during transmission becomes an essential issue for the Internet.
Encryption is a well-known procedure for secure data transmission. The commonly used encryption schemes include DES (Data Encryption Standard) , AES (Advanced Encryption Standard) and RSA. These methods scramble the secret message so that it cannot be understood. However, it makes the message suspicious enough to attract eavesdropper's attention. Hence, a new scheme, called "steganography", arises to conceal the secret messages within some other ordinary media (i.e. images, music and video files) so that it cannot be observed. Steganography differs from cryptography in the sense that where Cryptography focuses on concealing the contents of a message, steganography focuses on concealing the existence of a message.

Two other technologies that are closely related to steganography are watermarking and fingerprinting. Watermarking is a protecting technique which protects (claims) the owner's property right for digital media (i.e. images, music, video and software) by some hidden watermarks. Therefore, the goal of steganography is the secret messages while the goal of watermarking is the cover object itself.

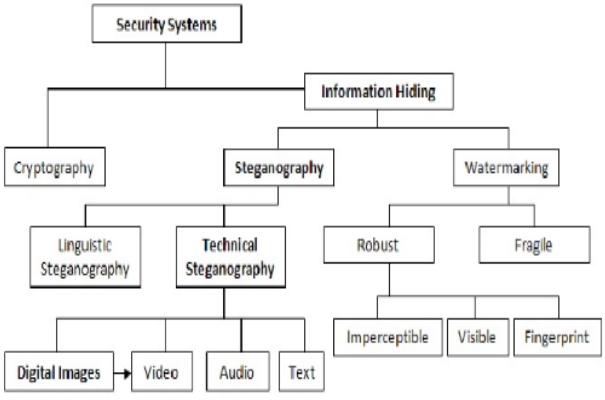

Figure 1 Types of security system

Three techniques are interlinked, steganography, watermarking and cryptography. The first two are quite difficult to tease apart especially for those coming from different disciplines. Drawing a line between these techniques is both arbitrary and confusing. Therefore, it is necessary to discuss briefly these techniques before a thorough review is provided. Figure 2.1 and Table 2.1 may eradicate such confusion.

Table 2.1: Comparison of steganography, watermarking and cryptography

Criterion/*Method*	*Steganography*	*Watermarking*	*Cryptography*
Carrier	any digital media	mostly image/audio files	usually text based, with some extensions to image files
Secret data	payload	watermark	plain text
	no changes to the structure		changes the structure
Key	optional		necessary
Input files	at least two unless in self-embedding		one
Detection	blind	usually informative, i.e., original cover or watermark is needed for recovery	blind
Authentication	full retrieval of data	usually achieved by cross correlation	full retrieval of data
Objective	secrete communication	copyright preserving	data protection
Result	stego-file	watermarked-file	cipher-text
Concern	delectability/ capacity	robustness	robustness
Type of attacks	steganalysis	image processing	cryptanalysis
Visibility	never	sometimes, see Figure 2.2	always
Fails when	it is detected	it is removed/replaced	de-ciphered
Relation to cover	not necessarily related to the cover. The message is more important than the cover.	usually becomes an attribute of the cover image. The cover is more important than the message.	N/A
Flexibility	free to choose any suitable cover	cover choice is restricted	N/A
History	very ancient except its digital version	modern era	modern era

The work presented here revolves around steganography in digital images and does not discuss other types of steganography, such as linguistic or audio. Table2.1

The work is basically about steganography so discussion will be about steganography. Steganography is again divided into different types based on the format . Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display [32]. The redundant bits of an object are those bits that can be altered without the alteration being detected easily

II. RELATED WORK

. The idea and practice of hiding information has a long history. In *Histories* the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave's scalp. When the slave's hair grew back the slave was dispatched with the hidden message [50]. In the Second World War the Microdot technique was developed by the Germans. Information, especially photographs, was reduced in size until it was the size of a typed period. Extremely difficult to detect, a normal cover message was sent over an insecure channel with one of the periods on the paper containing hidden information [51]. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels.

A famous example of steganography is Simmons' .Prisoners' problem ., see [52]. Bob and Alice are in a jail and wish to escape. Their cells are far apart from each other and the only allowed communication is sending messages via prison officer. If warden detects any sign of conspiracy, he will secure their cells even more. Bob and Alice are well aware of these facts . Happily, before they got arrested, they have agreed a stegosystem. Stegosystem describes the way the secret message is embedded into a covertext (seemingly innocent message). According to the standard terminology of information hiding a cover text with hidden information is called stegotext.
Ancient Greeks wrote text on wax-covered tablets. To pass a hidden message, a person would scrape wax off a tablet, write a message on the underlying wood and again cover the tablet with wax to make it appear blank and unused. Another ingenious method was to shave the head of a messenger and tattoo a message or image on the messenger's head. After the hair grew back, the message would be undetected until the head was shaved again. Invisible inks offered a common form of invisible writing. Early in World War II, steganographic technology consisted almost exclusively of these inks.1 With invisible ink, a seemingly innocent letter could contain a very different message written between the

lines.3 Documents themselves can hide information: document text can conceal a hidden message through the use of null ciphers (unencrypted messages), which camouflage the real message in an innocent- sounding missive. Open coded messages, which are plain text passages, "sound" innocent because they purport to be about ordinary occurrences. Because many open-coded messages don't seem to be cause for suspicion, and therefore "sound" normal and innocent, the suspect communications can be detected by mail filters while "innocent" messages are allowed to flow through Document layout may also reveal information. Documents can be marked and identified by modulating the position of lines and words. Message detection improved with the development of new technologies that could pass more information and be even less conspicuous.

III. EXISTING TECHNIQUES

Existing techniques

- A novel technique for image steganography based on Block-DCT and Huffman Encoding
- High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm
- A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images
- Labeling method
- JPEG and particle swarm optimization
- Quantized-frequency Secure Audio Steganography algorithm
- Integer Transform based Secure Audio Steganography algorithm

IV. DESCRIPTION OF FEW TECHNIQUES

Block-DCT and Huffman Encoding

Hiding the secret message/image in the special domain can easily be extracted by unauthorized user [57]. We proposed a frequency domain steganography technique for hiding a large amount of data with high security, a good invisibility and no loss of secret message. The basic idea to hide information in the frequency domain is to alter the magnitude of all of the DCT coefficients of cover image. The 2-D DCT convert the image blocks from spatial domain to frequency domain.

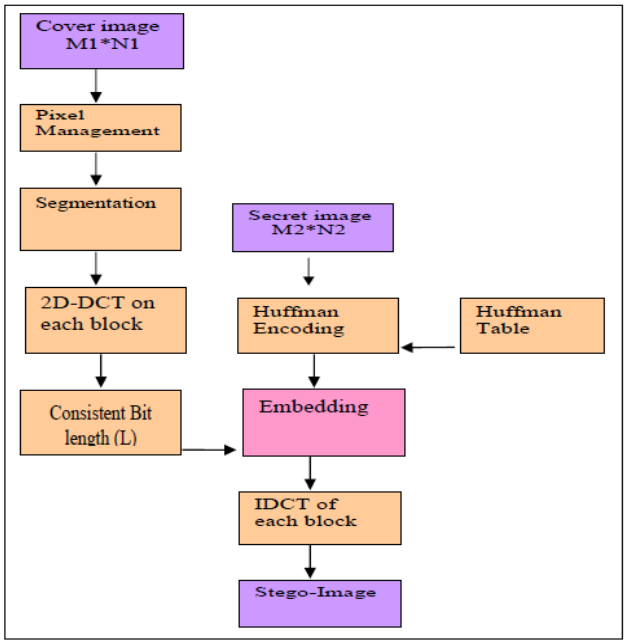

Figure 4.1 Block Diagram of Embedding Technique

The schematic/ block diagram of the whole process is given in figure (a) and (b)

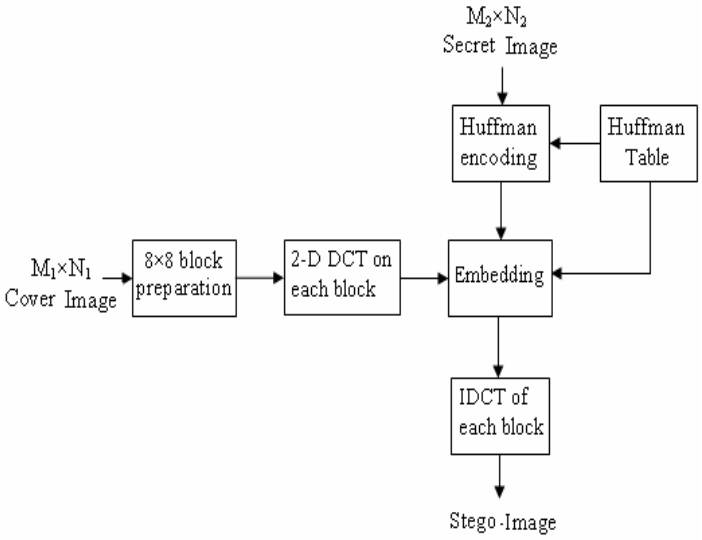

Figure 4.2 (a) Insertion of a Secret image (or message) into a Cover image [58]

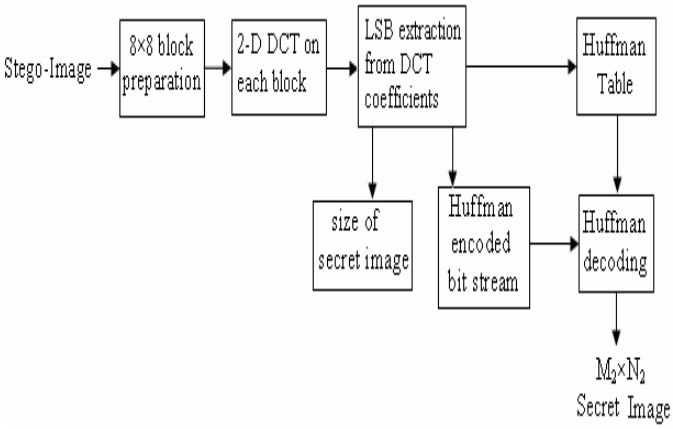

Figure 4.3 (b) Removal of Secret Image (or message)[58]

Advantages

- Improvement in security & image quality
- A good invisibility
- Less distortion after embedding process
- Expected to be practical
- Provides three layers of security

Disadvantages

- Robustness is not achieved
- Can be distorted by unintended users

V. LABELING METHOD IN STEGNOGRAPHY

In this method tried to find binary value of each character of text message and then in the next stage, tried to find dark places of gray image (black) by converting the original image to binary image for labeling each object of image by considering on 8 connectivity. Then these images have been converted to RGB image in order to find dark places. Because in this way each sequence of gray color turns into RGB color and dark level of grey image is found by this way if the Gary image is very light the histogram must be changed manually to find just dark places. In the final stage each 8 pixels of dark places has been considered as a byte and binary value of each character has been put in low bit of each byte that was created manually by dark places pixels for increasing security of the main way of stegnography[syn20].

Advantages

- Applicable for unobtrusive communications
- Easy to implement
- More Effective & efficient
- Reduce manual work load

Disadvantages

- Less secure
- Require skillful & intelligent programmer
- Need an Enhanced technique to make use of Palette and composition of the gif image for better results

Proposed technique

New algorithms keep emerging prompted by the performance of their ancestors (spatial domain methods), by the rapid development of information technology and by the need for an enhanced security system. The discovery of the LSB embedding mechanism is actually a big achievement. Although it is perfect in not deceiving the HVS, its weak resistance to attacks left researchers wondering where to apply it next until they successfully applied it within the frequency domain.

Proposed method in Image steganography using frequency domain is as follows:

Firstly , the image is converted into frequency domain after applying wavelet transform. The cover image is converted from RGB to Grey scale which is more suitable format for data hiding. The secret message or image which is to hide is then processed to know the size of that secret message or image. A key is used to provide secrecy which generates the PN sequence for hiding secret message in cover image. Apply suitable algorithm for hiding the message. The secret message is being hidden at the edges of the cover image. PSNR is calculated by applying mathematical operation.

$$PSNR = 10*\log10 (C^2_{max} / MSE)$$

Where MSE denotes mean square error which is given as:

$$MSE=\frac{1}{M\times N}\sum_{x=1}^{M}\sum_{y=1}^{N}\left(S_{xy}-C_{xy}\right)^2$$

Where x and y are the image coordinates, M and N are the dimensions of the image, S_{xy} is generated stegoimage and C_{xy} is the cover image. Also C^2_{max} holds the maximum value in the ima for example:

$$C^2_{max} \leq \begin{cases} 1, & \text{double precision} \\ 255, & \text{unit 8 bit} \end{cases}$$

Wavelet transform has the capability to offer some information on frequency-time domain simultaneously. In this transform, time domain is passed through low-pass and high-pass filters to extract low and high frequencies respectively. This process is repeated for several times and each time a section of the signal is drawn out. DWT analysis divides signal into two classes (i.e. Approximation and Detail) by signal decomposition for various frequency bands and scales. DWT utilizes two function sets: scaling and wavelet which associate with low and high pass filters orderly. Such a decomposition manner bisects time separability. In other words, only half of the samples in a signal are sufficient to represent the whole signal, doubling the frequency separability.

VI. IMPLEMENTATION

The work is totally worked using MATLAB. The project work is done by this language. The MATLAB high-performance language for technical computing integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation. Using the MATLAB product, you can solve technical computing problems faster than with traditional programming languages, such as C, C++, and Fortran. MATLAB in a wide range of applications, including signal and image processing, communications, control design, test and measurement, financial modeling and analysis, and computational biology. Add-on tool boxes(collections of special-purpose MATLAB functions, available separately) extend the MATLAB environment to solve particular classes of problems in these application areas.

MATLAB provides a number of features for documenting and sharing work. MATLAB code can be integrated with other languages and applications, and distribute your MATLAB algorithms and applications. Features include:

- High-level language for technical computing
- Development environment for managing code, files, and data
- Interactive tools for iterative exploration, design, and problem solving
- Mathematical functions for linear algebra, statistics, Fourier analysis, filtering, optimization, and numerical integration
- 2-D and 3-D graphics functions for visualizing data
- Tools for building custom graphical user interfaces

• Functions for integrating MATLAB based algorithms with external applications and languages, such as C, C++, Fortran, Java™, COM, and Microsoft® Excel® MATLAB can be used in a wide range of applications, including signal and image processing, communications, control design, test and measurement, financial modeling and analysis, and computational biology.

VII. ALGORITHM USED FOR EMBEDDING

Step 1- Read a colored (RGB) image, divide the image into (4 x 4) sub images Gi, (i=1,2,..) ; (each sub image contains 16 pixels).
Step 2- Determine the position in which we will start hiding the data; This is determined by using a random generator function.
Step 3- For each sub image Gi, the following process will be done:

- **Step 3-1**- Convert the least three bits from the blue color byte to decimal for each pixel P(r,c) in Gi, the results will be saved in Bi (4x4) decimal matrix. All elements of Bi are in the range (0…2m -1).
- **Step 3-2** - To hide the following bits
  0101101011100….., convert each three bits to the equivalent decimal number (i.e 010 is converted to D= 2), then find V and the sign S
- **Step 3-3** If the sign S is negative, add the value of V to one of the pixels P(r,c) in the sub image Gi, the values of (r,c)
- **Step 3-4** Otherwise (if S is positive) subtract the value of V from the pixel P(r,c) in the sub image Gi, the values of (r,c) are calculated depending on the values of (i,j) of the point Bi are calculated depending on the values of (i,j) of the point Bi This process will force the value of modulation function to be equal to the embedded data.

This algorithm is used to embed secret image into cover image. The secret message can be any text, image or any other medium.
After embedding process msg is sent to the receiving party. At receiving side the stego image is again applied to reverse embedding process for extracting the original message. The extraction process is as follows :-

VIII. EXTRACTION PROCESS OR STEGANALYSIS PROCESS

Step 1. Read the Stegano image
Step 2. Divide the image into (4 x 4) sub images Gi, (i=1,2,..) ; (each sub image contains 16 pixels).
Step 3. Determine the position in which we will start hiding the data; This is determined by using a random generator function
Step 4. For each sub image Gi, the following process will be done:
(Repeat the following process)

- Read the data area from the sub matrix and retrive as an array of bits
- Reverse the Encoding Process by reperforming the Ex-or operation on data bits.
- 0101101011100….., convert each three bits to number (i.e 010 is converted to D= 2), then find V and the sign S
- If the sign S is negative, add the value of V to one of the pixels P(r,c) in the sub image Gi, the values of (r,c) of (i,j) of the point Bi

- Otherwise (if S is positive) subtract the value of V from the pixel P(r,c) in the sub image Gi, the values of (r,c) are calculated depending on the values of (i,j) of the point Bi the equivalent decimal are calculated depending on the values

Step 5. Convert the data back in Text format
Step 6. Store the data in the form of file

IX. RESULTS AND ANALYSIS

Firstly, image is converted to the frequency domain. The following figures represents How to convert the image into frequency domain.

As we have used here JPEG image, but in embedding we use Bitmap image because the size of the matrices does not match with the JPEG format.
Now embedding is done using bitmap image.

PSNR & MSE values

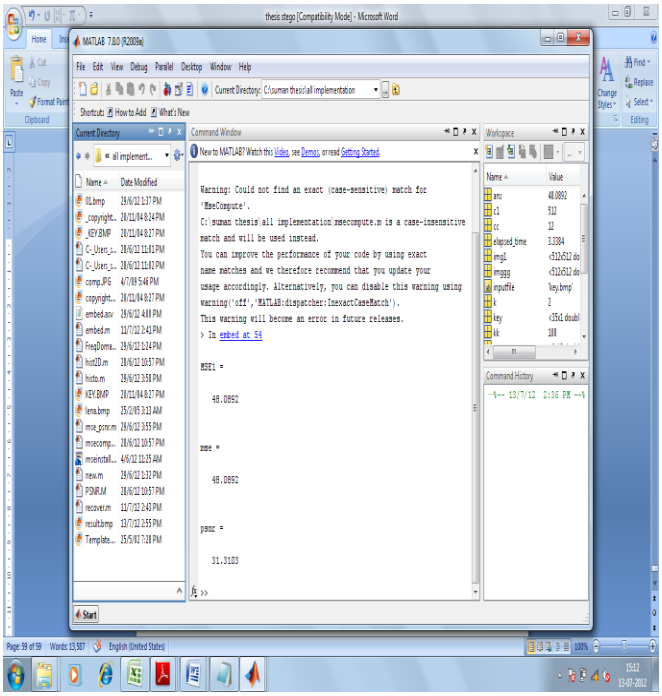

Figure 7.9 Psnr, Mse, Elapsed Time

Output values
MSE = 47.9772
PSNR = 31.3205
Elapsed time = 2.1060

7.2 PSNR values of Different Images

Images	Size	Capacity	PSNR
Lenna	256	299520	31.34
Baboon	256	299520	39.80
Airplane	256	299520	30.56
Boat	256	299520	39.05

Table 7.1 PSNR values

From table, it is observed that for all images, PSNR is near about 40 and the hidden capacity is about 299520 bits. Table below shows that the hiding capacity and PSNR of our proposed algorithm is better than the one in reference [23], except only one case.

REFERENCES

[1] Moerland, T., "Steganography and Steganalysis", *Leiden Institute of Advanced Computing Science*, www.liacs.nl/home/ tmoerl/privtech.pdf
[2] Silman, J., "Steganography and Steganalysis: An Overview", *SANS Institute*, 2001
[3] Jamil, T., "Steganography: The art of hiding information is plain sight", *IEEE Potentials*, 18:01, 1999
[4] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", *Communications of the ACM*, 47:10, October 2004
[5] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", *IEEE Journal of selected Areas in Communications*, May 1998
[6] Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", *IEEE Transactions on image processing*, *8:08*, 1999
[7] Dunbar, B., "Steganographic techniques and their use in an Open-Systems environment", *SANS Institute*, January 2002
[8] Artz, D., "Digital Steganography: Hiding Data within Data", *IEEE Internet Computing Journal*, June 2001

[9] Simmons, G., "The prisoners problem and the subliminal channel", *CRYPTO*, 1983
[10] Chandramouli, R., Kharrazi, M. & Memon, N., "Image steganography and steganalysis: Concepts and Practice", *Proceedings of the 2nd International Workshop on Digital Watermarking*, October 2003
[11] Currie, D.L. & Irvine, C.E., "Surmounting the effects of lossy compression on Steganography", *19th National Information Systems Security Conference*, 1996
[12] Handel, T. & Sandford, M., "Hiding data in the OSI network model", *Proceedings of the 1st International Workshop on Information Hiding*, June 1996
[13] Ahsan, K. & Kundur, D., "Practical Data hiding in TCP/IP", *Proceedings of the Workshop on Multimedia Security at ACM Multimedia*, 2002
[14] Johnson, N.F. & Jajodia, S., "Exploring Steganography: Seeing the Unseen", *Computer Journal*,February 1998
[15] "Reference guide: Graphics Technical Options and Decisions",
http://www.devx.com/projectcool/Article/19997
[16] Owens, M., "A discussion of covert channels and steganography", *SANS Institute*, 2002
[17] Johnson, N.F. & Jajodia, S., "Steganalysis of Images Created Using Current Steganography Software", *Proceedings of the 2nd Information Hiding Workshop*, April 1998
[18] Venkatraman, S., Abraham, A. & Paprzycki, M., "Significance of Steganography on Data Security",*Proceedings of the International Conference on Information Technology: Coding and Computing*, 2004
[19]Krenn,R.,Steganography,andSteganalysis",
http://www.krenn.nl/univ/cry/steg/article.pdf
[20] Lee, Y.K. & Chen, L.H., "High capacity image steganographic model", *Visual Image Signal Processing*, 147:03, June 2000

