Steganography: A Juxtaposition between LSB DCT, DWT

Tamanna
(Post Graduate Student)
Guru Kashi University
Talwandi Sabo, Bathinda

Ashwani Sethi
Dy. Director
Guru Kashi University
Talwandi Sabo, Bathinda

ABSTRACT
Steganography is the technique to concealing information to the extent which nobody, except for the transmitter and also the designated receiver, anticipate the presence of the hidden data. Steganography is the craft to concealing important information in such a way that restrict recognition. The Steganography utilized towards transportation important information from just one destination to some other location by using general public network as part of stealth way. Steganography hides the extremely existence of a information to ensure that if worthwhile that it usually appeals to no suspiciousness anyway. Steganography means that concealing a hidden information (the integrated message) inside a more substantial one (source cover) in such a way that an onlooker cannot identify the clear presence of contents of the hidden message [1]. A lot of different service provider file formats can be made use of, however digital images are the most prominent because of the consistency on the Internet. For hiding mysterious important facts in images, there exists a spacious assortment of Steganography strategies some are much more complicated as opposed to others and every one of them have respective robust as well as weak spots. Different programs have actually different specifications for the Steganography approach used. This Particular document promises to provide an introduction to image Steganography, its makes use of as well as strategies. It also initiatives to determine the prerequisites of a good Steganography algorithmic rule as well as quickly demonstrate upon which Steganography strategies tend to be more appropriate which applications.

General Terms
Image Steganography Techniques

Keywords
Steganography, Frequency Domain, Spatial domain, LSB method

1. INTRODUCTION
Mainly because an upswing associated with Internet one of the greatest important aspect in networking is the safety of real information. Steganography may be the art as well as science of undetectable communication. It is completed by hiding critical information some other information, thus hiding the existence of the information. Steganography is originated coming from the Greek terms “stegos” which means “cover” and “grafia” indicating “writing”[1] defining it as “covered writing”. In the image Steganography the important information is actually concealed exclusively in images. The concept and practice of information hiding has a long past. In historical past the Greek historian Herodotus publishes of the Nobleman, Histaeus, who needs to speak along with his son-in-law in Greece, has shaved the head of one of most trustworthy servant and needled on the content on the slave’s head. Whenever slave’s hair grew back, he sends slave with the secret information as soon as slave arrives at to the destination again, he shaved his head and restore the content [2]. During the Second World War the Germans presents brand new information hiding method which is certainly well-known as Microdot approach. In this the important information, like pictures, ended up being minimized in dimensions until eventually it absolutely was the dimensions of a typed time period. It was Extremely complicated to identify a hidden information, a regular encapsulate message was sent over an vulnerable network with one of the periods on the document formulated with invisible information [3]. Nowadays Steganography a brand new used on computers with digital data being the providers as well as networks being the high performance distribution networks. Although associated to cryptography, they are not equivalent. Steganography's objective is to hide the presence of the information, even though cryptography scrambles a message in this sort of a way that it are unable to be recognized [11]. Steganography as well as cryptography tend to be strategies accustomed safeguard facts from undesirable parties but neither of them technologies alone is greatest. Once the existence of hidden insight is actually presented or perhaps suspected, the justification of Steganography is partially defeated. The strength of Steganography enhances by incorporating it with cryptography.

The Steganography has been classified into (i) spatial domain Steganography: It primarily consists of LSB Steganography as well as Bit Plane Complexity Slicing (BPS) algorithm. Spatial domain is continuously utilized as a result of highest capacity for hidden information and simple recognition. (ii) Transform domain Steganography: The secret critical information is integrated in the transform coefficients of the encapsulate image. Illustrations of transform domain Steganography are Discrete Cosine Transform [15], Discrete Fourier Transform and Discrete Wavelet Transform.

Steganography utilized for the wide variety of programs such as for instance defiance organizations for secure movement of secret data, intelligence agencies, in intelligent identity cards where personalized important information tend to be enclosed within the picture by itself for the copyright laws control over materials, medical imaging where patient’s information tend to be stuck within image supplying security of important information as well as shrinking transmission time. The basic model for Steganography is displayed on fig. 1

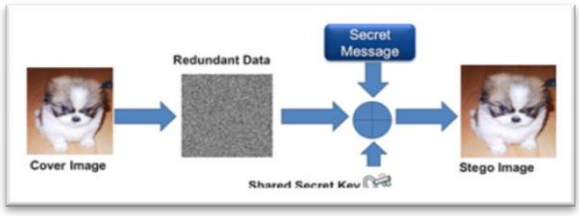

Fig 1 Basic Steganography Model

It demonstrates the fundamental processes involved with Steganography which is composed of Carrier, Information as well as Secret Key. Carrier is also identified as cover-object, in which information is integrated and serves to keep hidden the existence of the content. The information might end up being any sort of information (simple text, cipher text or other image) that the sender needs to stay private. Key is recognized as stego-key, which one helps to ensure that exclusively recipient who understands the key, equivalent decryption key will be able to retrieve the content coming from a cover-object. The cover-object along with the item privately integrated content will then be known as the stego-object [4].

Recouping content coming from a stego-object necessitates the cover-object by itself along with a equivalent decoding key if a object stego-key was actually made use of throughout the important information encoding procedure. The particular document is actually prepared within the adhering to sections: Section 2 identifies stenography basic principle. Section 3 talks about forms of Steganography. section 4 portrays Image Steganography strategies. section 5 describes Evaluation. Subsequently summary introduced within segment 6

2. PRINCIPLE OF STEGANOGRAPHY

The secret information is actually integrated within the encapsulated object in encoded format by making use of the hiding algorithmic rule, therefore delivered to a recipient on a network. The recipient subsequently decrypted the content through the use of the opposite procedure found on the cover information as well as exposes the secret data [4].

Fig 2 The principle of Steganography

Fig. 2 demonstrates the concept of Steganography. Steganography algorithmic rule, attempts to protect the perceptive qualities associated with the authentic image. A appropriate image, referred to as cover/ service provider, is chosen. The secret information will then be embedded straight into the cover making use of the Steganography algorithmic rule, in a manner that cannot modify the unique graphic within a human being significant way. The outcome is completely new image, the stego-image, which is not really appears diverse from authentic image.

3. TYPES OF STEGANOGRAPHY

Steganography can made use of for nearly almost all digital file formats, but the formats all those are along with an excellent degree of repetitiveness are a lot more appropriate. Redundancy can easily be characterized because the bits of an object that incorporate reliability considerably higher than essential for the object's usage as well as display. The redundant bits of an object are those bits which tend to be modified without having the modification currently being recognized effortlessly [4]. Image and audio files specifically abide by this particular requisite, even though studies have additionally uncovered other file formats just that can be utilized for the important information camouflaging. There are certainly four classifications of file formats that can easily be utilized for the Steganography displayed in fig. 3

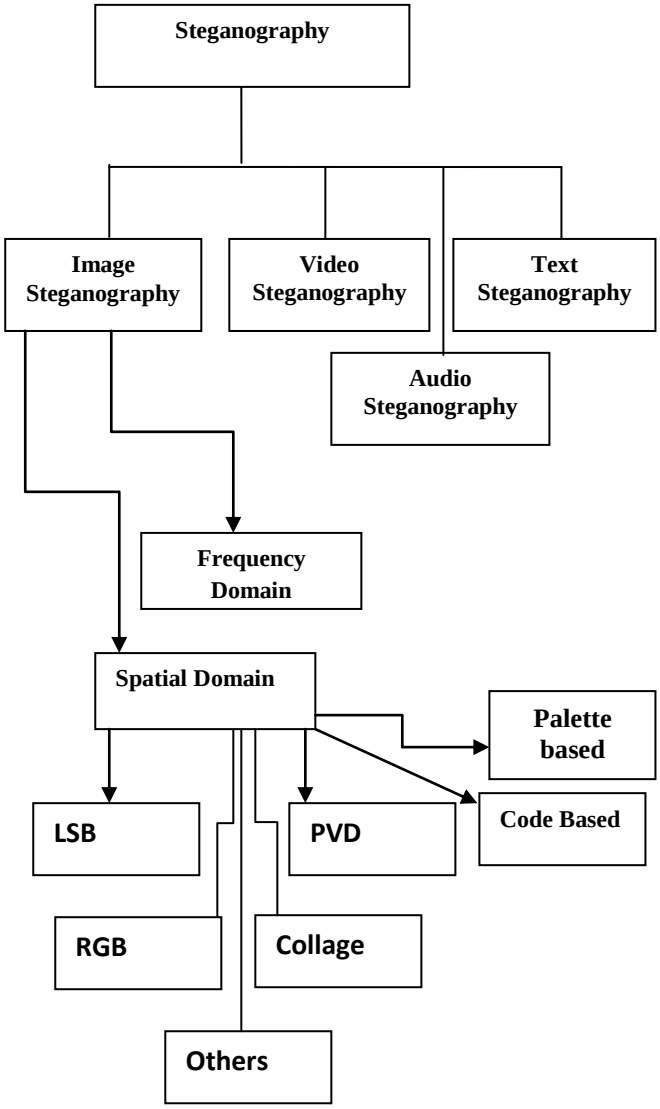

Fig 3 Classification of spatial domain image Steganography method

Since, images are really prominent encapsulate or perhaps service provider objects made use of for the Steganography. Within the domain name of digital images different image file formats can be found, many of them are offered for particular applications.

4. IMAGE STEGANOGRAPHY TECHNIQUES

Steganography in graphics tend to be categorized directly into two classifications: Spatial-domain oriented Steganography and the Transform domain oriented Steganography.

4.1 Spatial Domain Method [12]

These strategies make use of the pixel grey levels and their particular color values immediately for the encoding the content bits. These Types Of methods are among the simplest schemes in terms of embedding and extraction intricacy. The major disadvantage among these techniques is actually level of ingredient noise that creeps in the image which exclusively influences the Peak Signal to Noise Ratio and the analytical properties of the image. Furthermore these types of embedding algorithmic rule tend to be applicable primarily to lossless image-compression techniques such as TIFF images. For lossy compression strategies such as JPEG, a few of the message bits get lost throughout the compression step. The most frequent algorithmic rule belong to this particular class of techniques is the Least Significant Bit (LSB) substitution technique in which in turn the least significant bit of the binary legal representation associated with the pixel gray levels is used to symbolize the message bit. This Particular type of embedding contributes to an addition of a noise of 0:5p on average in the pixels of the image where p is the embedding rate in bits/pixel. This sort of embedding also leads to an asymmetry, plus a grouping in the pixel gray values (0,1);(2,3);. . . (254,255). this asymmetry is taken advantage of within the problems put together .To conquer this particular unfavorable asymmetry, the decision of altering the lowest significant bit is randomized i.e. if the information bit really does not adjust the pixel bit, then pixel bit is sometimes enhanced or perhaps diminished simply by 1. This technique is widely referred to as LSB Matching. It can be observed that even this kind of embedding adds a noise of 0:5p on average. To additional decrease the interference, [17][19] have recommended using a binary function of two encapsulate pixels to implant the information bits. The embedding is carried out working with a set of pixels as a unit, where the LSB of the first pixel brings one particular small amount of information, and a function of the two pixel values carries an additional bit of information.

Least significant bit (LSB) substitution is a very common, straight forward solution to embedding important information in a cover image. The least significant bit (8 bit) of a few or perhaps each of the bytes inside an image is swapped out by having a bit of the hidden message. Whenever working with a 24-bit image, a bit of each of the red, green and blue color can be used, since that they tend to be each represented by a byte. That is one can store 3 bits in each pixel. The image of 800 X 600 pixel ,can thus preserve an overall total amount of 1,440,000 bits or 180,000 bytes of embedded data[10].

For example, 3 pixels grid for of a 24-bit image can be as follows:
(00101101 00011100 11011101)
(10100111 11000101 00001101)
(11010010 10101101 01100011)

When the number 500, which binary representation is 11110100, is embedded into the least significant bits of this part of the image.
the resulting grid is as follows:
(00101101 0001110**1** 11011101)
(10100111 1100010**0** 00001101)
(11010010 1010110**0** 01100011)

Previously Mentioned the amount ended up being embedded straight into the very first 8 bytes of the grid, starting these only the 3 underlined bits recommended to become altered in accordance with the message which is integrated. On the average, exclusively half of the bits in an image will require to be customized to cover up a secret information making use of the maximum cover size. Since generally there can be done intensities of each primary color is 256, By switching the LSB of a pixel results in limited alterations in the strength for the colors[6]. These modifications are unable to be diagnose because of the human eye ,thus the message is successfully hidden in image.

4.2 Transform Domain Method

The transform domain Steganography techniques can be used for the concealing a great deal of data and yields high security, a effective invisibility with no loss of secret message. The objective behind that is to hide important information in frequency domain by transforming order of magnitude almost all of discrete cosine transform (DCT) coefficients of cover image. The 2-D DCT transforms image blocks from spatial domain to frequency domain. The cover image is broken down into non imbrications blocks of size 8×8 and is applicable DCT for each of blocks of cover image making use of forward DCT [7].

4.2.1 The Discrete Cosine Transform (DCT)

The Discrete Fourier Transform (DFT)[12] is mathematical changes transform the pixels in really a manner with regards to provide the effectuation of "distributing" the spot associated with the pixel values over a portion associated with the photograph [5]. The DCT transforms a signal from an photograph depiction right into a frequency representation, by grouping together the pixels into 8 × 8 pixel blocks and remodeling the pixel blocks into 64 DCT. DCT is used in Steganography as- Image is busted into 8×8 blocks of pixels. Working from left to right, top to bottom, the DCT is put on every single block. Almost Every block is pressurized throughout quantization table to degree the DCT coefficients and information is actually integrated in DCT coefficients.

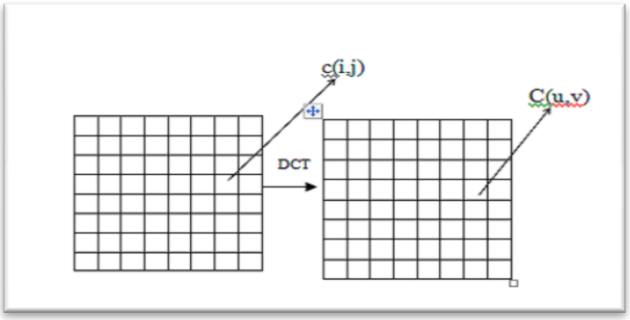

Fig 4 Discrete Cosine Transform of an Image

Although Steganography aims at transferring images without worrying about visual wreckage or perhaps modifications for naked observer, it cannot distribute alongside transforming spatial and transform level specifics in order to embed the data.

DCT coefficients[10][18] are used for JPEG compression[8]. It separates the image into parts of differing importance. It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components.

Image is broken into 8×8 blocks of pixels. Working from left to right, top to bottom, DCT is applied to each block. Each block is compressed through quantization table to scale the DCT coefficients and message is embedded in DCT coefficients.

4.2.2 JPEG Image Steganography Technique [13]

In the beginning it absolutely was thought that Steganography would not be feasible to make use of with JPEG images, since they use lossy compression which outcomes inside components of the image data being modified. One of several secret attributes of Steganography is the fact that important information is actually concealed within the redundant bits of an object and since redundant bits are left out when using JPEG it was dreaded that the hidden message would be destroyed. Even when one could somehow keep the information undamaged it could be challenging to implant the message without worrying about the alterations currently being recognizable as a result of the harsh compression applied. still, characteristics associated with the compression algorithm have been taken advantage of ,in order to formulate a steganographic algorithm for JPEGs[10].

One of these qualities of JPEG is used to really make the modifications towards the image unseen to the human eye. During the DCT transformation phase of the compression algorithm, rounding blunders take place in the coefficient information which are not apparent as well as comprehensible. Even though this property is exactly what categorizes the algorithm as being lossy, this option can also be used to hide messages. It is neither of them feasible nor possible to introduce information in an image that makes use of lossy compression, since the compression would definitely destroy all important information in the process. So, it is significant to identify that the JPEG compression algorithm is definitely separated into lossy as well as lossless stages. The quantization and the DCT phase form part of the lossy stage, on the other hand the Huffman encoding used to further compress the data is lossless. Steganography can take place anywhere between both of these stages. Using equivalent standards of LSB insertion the message can be integrated in to the the very least considerable bits of the coefficients before implementing the Huffman encoding. By embedding the important information at this stage, in the transform domain, it is incredibly difficult to identify, since it is not in the visual domain.

$$C(u) = a(u)\sum_{i=0}^{N-1} x_i \cos\left(\frac{(2i+1)u\pi}{2N}\right)$$

Where u= 0, 1, 2….. N-1

The general equation for a 2D (*N* by *M* image) DCT is defined by the following equation

$$C(u,v) = a(v)\sum_{i=0}^{N-1}[a(u)\sum_{i=0}^{N-1} x_i \cos\left(\frac{(2i+1)u\pi}{2N}\right)] \times \cos\left(\frac{(2i+1)v\pi}{2N}\right)$$

Where u, v = 0,1,2….N-1

Here, the input image is of size N X M. c (i, j) is the intensity of the pixel in row i and column j; C(u,v) is the DCT coefficient in row u and column v of the DCT matrix. DCT is used in Steganography

5. EVALUATION OF IMAGE QUALITY ANALYSIS

For weighing stego image with cover results demands an estimate of image quality, commonly used measures are Mean-Squared Error, Peak Signal-to-Noise Ratio and capability.

5.1 Mean-Squared Error:

The mean-squared error (MSE) in between two graphics I1(m,n) as well as I2(m,n) is:

$$MSE = \frac{\sum_{M,N}[I1(m,n) - I2(M,N)]^2}{M * N}$$

M and N are the numbers associated with rows and columns in the type in graphics, correspondingly.

5.2 Peak Signal-to-Noise Ratio:

Peak Signal-to-Noise Ratio (PSNR)[7][8] eliminates this issue through scaling the MSE in accordance to your image range:

$$PSNR = 10\log_{10}\frac{256^2}{MSE}$$

PSNR is calculated inside decibels (dB). PSNR is an excellent measuring for the researching maintenance outcomes for equivalent graphics.

5.3 Capacity

It is the dimensions associated with the information inside a cover image that can be customized without worrying about weakening their stability of the cover image. The Steganography embedding functioning will have to preserve the analytical qualities for the cover image in addition to its perceptual excellence. Therefore capacity is dependent upon total number of bits per pixel & quantity of bits integrated in each pixel. Potential is actually exemplified through bits per pixel (bpp) and the Maximum Hiding Capacity [14] (MHC) in terms and conditions of proportion.

5.4 Domain Method (DOM):

DOM[16] is sometimes Spatial(S) or perhaps Transform (T). The methods which use transform domain hide important information in considerable aspects of the cover images and may be additional complicated for attackers.

5.5 Normalized Coefficient (NC):

Correlation is one of the best strategies to judge the amount associated with closeness anywhere between the two functions. This measuring can easily be employed to figure out the degree to which the authentic photograph plus stego photograph remain in close proximity to each other, even after embedding the data.

6. CONCLUSION

This analysis presented a foundation of Steganography and a relative review associated with some Steganographic algorithm. Steganography as important information security measures will surely have some useful applications, like other ostensibly associated system (cryptography). The triumph within this analyze is always to determine trustworthy and greatest algorithm readily available in the marketplace for

Steganography. Even Though only a few associated with the leading image Steganography techniques were talked about within paper, one can see that there exists a large selection of approaches to covering up important information in images. In this particular document, evaluation of LSB, DCT & DWT techniques have been effectively executed as well as answers are delivered. The MSE and PSNR of the methods are also discussed and also this paper introduced a back ground conversation as well as inclusion regarding the significant algorithms of Steganography deployed in digital imaging

Features	LSB	DCT	DWT
Invisibility	Low	High	High
Payload Capacity	High	Medium	Low
Robust Against Image Manipulation	Low	Medium	High
PSNR	High	Medium	Low
MSE	Low	Medium	High

Table 1 .Feature Comparison[9]

7. ACKNOWLEDGEMENT

It is our privilege to acknowledge with deep sense of gratitude towards my guide, Prof. Ashwani Sethi, for his valuable suggestions and guidance throughout course of study and timely help given in the completion of my preliminary research work on "image Steganography". It is needed a great moment of immense satisfaction to express out profound gratitude, indebtedness towards our VC Prof Malhi, whose real enthusiasm was a source of inspiration for us. We would also like to thank all other faculty members of Computer Engineering department of Guru Kashi University,Talwandi Sabo who directly or indirectly kept the enthusiasm and momentum required to keep the work towards an effective project work alive in us and guided in their own capacities in all possible**.**

8. REFERENCES

[1] Deshpande Neeta, KamalapurSnehal, Daisy Jacobs, "Implementation of LSB Steganography and Its Evaluation for Various Bits", 2004.

[2] 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", IEEE-0-7803-9588-3/05/$20.00 ©2005.

[3] Vijay KumarSharma, Vishalshrivastava, "A Steganography Algorithm for Hiding Images by improved LSB substitution by minize detection."Journal of Theoretical and Applied Information Technology, Vol. 36 No.1, ISSN: 1992-8645, 15th February 2012.

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

[5] Chen Ming, Zhang Ru, NiuXinxin, Yang Yixian, "Analysis of Current Steganography Tools: Classifications & Features" , International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP'06),IEEE- 0-7695-2745-0/06 $20.00 © 2006.

[6] Aneesh Jain, Indranil Sen. Gupta, "A JPEG Compression Resistant Steganography Scheme for Raster Graphics Images",IEEE-1-4244-1272-2/07/$25.00©2007.

[7] Beenish Mehboob and Rashid Aziz Faruqui, "A Steganography Implementation", IEEE -4244-2427-6/08/$20.00©2008.

[8] Hassan Mathkour, Batool Al-Sadoon, Ameur Touir, "A New Image Steganography Technique", IEEE-978-1-4244-2108-4/08/$25.00 © 2008.

[9] NageswaraRaoThota, Srinivasa Kumar Devireddy, "Image Compression Using Discrete Cosine Transform", Georgian Electronic Scientific Journal: Computer Science and Telecommunications, No.3 (17), 2008.

[10] Mamta Juneja, Parvinder Singh Sandhu, "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption", International Conference on Advances in Recent Technologies in Communication and Computing, 2009.

[11] Dr. EktaWalia, Payal Jain, Navdeep, "An Analysis of LSB & DCT based Steganography", Global Journal of Computer science & technology, Vol. 10 Issue 1 (Ver 1.0), April 2010.

[12] K.B. Shiva Kumar, K.B. Raja, R.K. Chhotaray, Sabyasachi Pattnaik, "Coherent Steganography using Segmentation and DCT", IEEE-978-1-4244-5967-4/10/$26.00 ©2010.

[13] K Suresh Babu, K B Raja, Kiran Kumar K, Manjula Devi T H, Venugopal K R, L M Patnaik, "Authentication of Secret Information in Image Steganography" .

[14] Arvind Kumar, Km. Pooja, "Steganography- A Data Hiding Technique", International Journal of Computer Applications (0975 – 8887), Volume 9– No.7, November 2010.

[15] Atalla I. Hashad, Ahmed S. Madani, "A Robust Steganography Technique Using Discrete Cosine Transform Insertion".

[16] H. C. Wu, N.I. Wu, C.S. Tsai,and M.S Hwang "Image Steganography scheme based on pixel-value differencing and LSB replacement methods", IEEE Proceedings Vision, Image and Signal Processing, vol.152, no.5, pp.611-615, 2005.

[17] X. Wang, "A palette-based image steganographic method using color quantization", in Proceedings of IEEE International Conferenceon Image Processing, vol.2, 2005, pp.1090-1093.

[18] K. Satish, T. Jayakar, C. Tobin, K. Madhavi, and K. Murali, "Chaos based spread spectrum image Steganography", IEEE Transactions on Consumer Electronics, vol.50, no.2, pp.587-590, 2004

[19] R. J. Anderson, and F. A. P. Petitcolas, "On the limits of Steganography", IEEE Journal of Selected Areas in Communications,vol.16, no.4, pp.474-481, 1998.