Image Compression and Steganography

Naveen Kumar[1], Dr. Vikas Siwach[2], Dr. Harkesh Sehrawat
Research Schlor[1], Assistant Professor[2, 3]
University Institute of Engineering & Technology, MDU, Rohtak, India

Abstract

Image compression method is utilized to lessen the quantity of bits required in speaking to image, which diminishes the storage room and transmission cost. In the present research work back proliferation neural system preparing calculation has been utilized. Back engendering neural system calculation builds the execution of the framework and to diminish the union time for the preparation of the neural system. Image compression a technique which is used to reduce the number of bits used for representation. Image compression helps in reducing the size of the image which results in less storage space and less cost of the transmission. The image is as compressed as the quality of the image is retained. A neural system calculation got back to Propagation Neural Network Algorithm is utilized for Image compression. The advantage of utilizing back spread calculation for utilizing Image compression is the huge increment in execution of the framework just as less assembly time for neural system preparing which keep up the nature of the picture as well as diminish the general size of the picture. This neural system technique for Image compression has appeared extremely encouraging outcome in Image compression.

Keywords: Image compression, Steganography, Neural Network etc.

Introduction

Steganography is an art of hiding data. The word steganography combines the Ancient Greek words stegano that means "covered, concealed, or protected" and graphy means "writing". Steganography and cryptography both are used for the protected communication but the mode of functioning is diverse where cryptography encode the message whereas steganography hides the presence of the message. It can hide the information in image, audio, video in all the digital media. Before steganography cryptography was used. Cryptography is also considered for hiding data for countless ages but certain time it fails to provide protected communication .But now a day's steganography is used to communicate. Steganography comprises of two footings that is message and cover image. Message is the stealthy data that desires to hide and cover image is the carrier that hides the message in it.

Fig 1. Steganography Strategy

LSB (the least significant bit) steganography inserts the protected data into the bottom bit plane of a bitmap image because human eyes cannot be sentient of the small variations that LSB bring into the image. LSB replacement rewrites the cover pixels' LSB by the protected bit stream. It is basically to implement but its safety is not so good. [1], [2] and [5] detect LSB replacement through the characters above. LSB matching also amends the cover images' LSBs with undisclosed bit stream. But it does not only overwrite it. Therefore, LSB corresponding removes the inequity statistical characters presented throughout inserting secret messages.

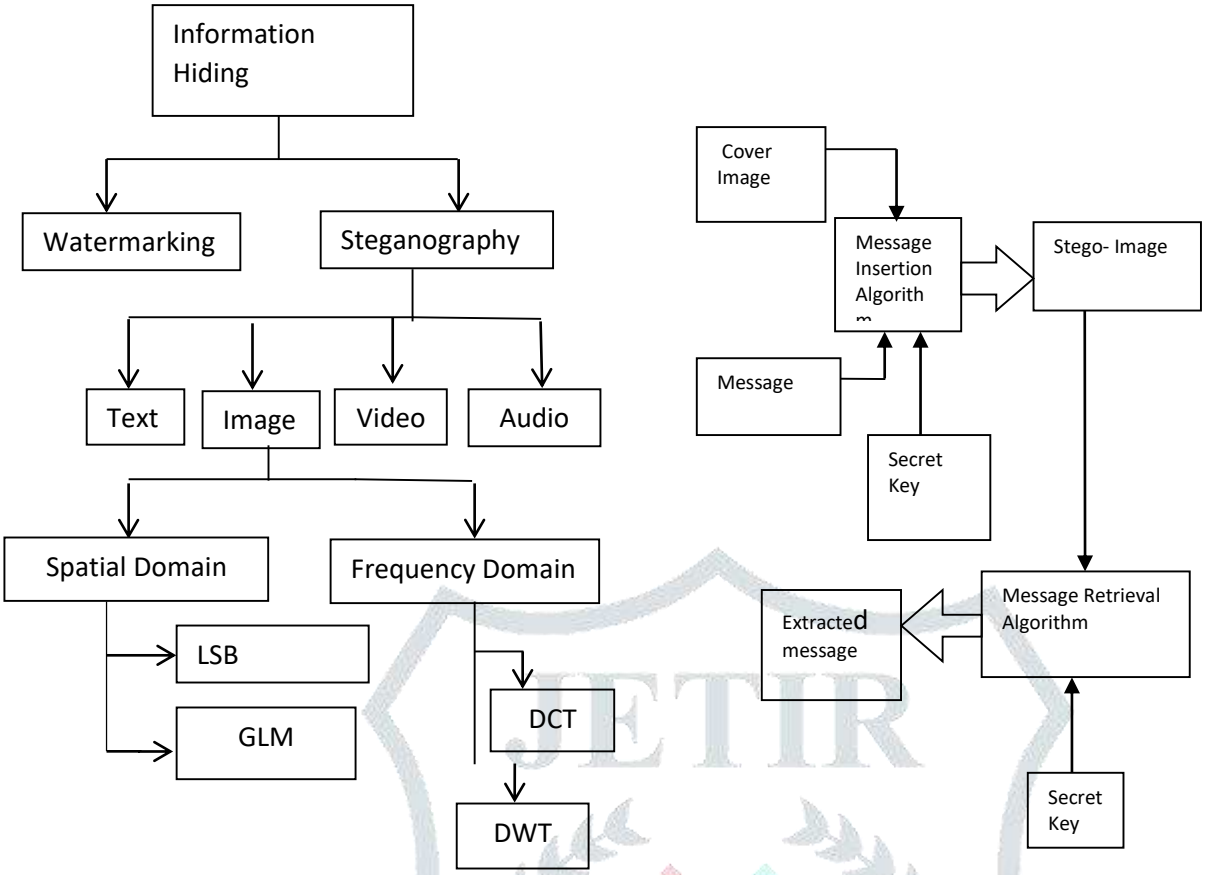

Fig 2 Steganography system and Information Hiding Structure

Literature work

Nowadays, huge numeral of dissimilar steganographic methods are invented, portion of them are unique or planned for an extensive variety of operation. At the similar period, each steganographic task has dissimilar necessities of features such as heftiness, volume, complexity of embedding information and others [6]. In the paper [7], was suggested procedure of examination that allows determining the rank (weight) of each of the qualitative features of the methods for hiding information during broadcast by communiqué networks in impartial mode. In [8] suggested an adaptive LSB replacement grounded data hiding method for image. To attain improved graphic excellence of stego-image it takes care of sound penetrating part for entrenching. Suggested technique discriminates and takes benefit of usual grain and edges area for embedding. This technique analyses the limits, illumination and feel covering of the cover image to calculate the number of k-bit LSB for stealthy data inserting. The value of k is high at non-sensitive image area and over sensitive image area k value remain small to balance overall visual excellence of image. In [3] anthers have projected LSB based image hiding method. Shared design minutes (stego-key) are used to hide data. The LSB's of the pixel are altered depending on the (stego-key) pattern bits and the secret message bits. Pattern bits are grouping of MxN size rows and columns (of a block) and with random key value. In inserting process, each pattern bit is corresponding with message bit, if pleased it modifies the 2nd LSB bits of cover image otherwise leftovers the same.

Image Compression

Image Format

An image is a quadrilateral array of values (pixels). Every pixel signifies the capacity of some property of a scene measured over a limited area. The possessions could be numerous things, but we usually measure either the average brightness (one value) or the brightness's of the image filtered through red, green and blue filters (three values). The values are normally represented by an eight bit integer, giving a range of 256 levels of brightness. A raw image will take up a lot of storage space. Methods have been defined to compress the image by coding redundant data in a more efficient fashion, or by discarding the perceptually less significant

information. MATLAB supports reading all of the common image formats. Image coding is not addressed in this course unit.

Steps of insertion:-

1. Split the image in 6×6 matrix.
2. Now check the location where data is to be insert.

   Alphabet value= (position + (reminder-1) xk^2) + (starting index-1).

   Using this formula.

   Position= location of matrix

   K^2 =size of matrix
3. In proposed technique expect pixels where data is to hide should be mod of 3.

Extraction:-

1. Read the image pixels.
2. Calculate the mod of pixels.
3. Pixels that are non-divisible by 3 having the data.

   Alphabet value= (position+ (reminder-1) xk^2) + (starting index-1).
4. Using same formula data can be retrieved.
5. Use R.S.A to decode data.

Performance Measurement Parameters

PSNR:-

The Peak signal to noise ratio (PSNR) is ratio to determine the image quality of image .It is ratio between possible power and distorted noise that affect the image. If PSNR value is larger than image quality is higher. If value is less than shows more distortion between stego image and cover image.

$$PSNR = 10log_{10}\frac{255^2}{MSE}$$

MSE:-

Means mean square error Given a noise-free $m \times n$ monochrome image I and its noisy approximation K, MSE is defined as:

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(a_{ij} - b_{ij})^2$$

Data Set 1kb of image size 256*256

IMAGENAME	PSNR	MSE	MAXERR	L2RAT	MEAN1	MEAN2	STD1	STD2
CAMERAMAN	45.6572	1.0025	2	1.0133	142.0233	141.2791	23.1241	23.3834
GIRL	45.1517	0.0976	2	1.0139	149.3876	148.3140	21.1122	20.8733
COUPLE	39.0345	1.0021	2	1.0312	26.5736	27.1279	16.8575	19.8368
GIRL2	40.7485	1.0022	2	1.0149	63.0310	64.0116	13.9507	13.8955
GIRL3	45.1801	1.0023	2	1.0038	36.4612	35.4535	14.5976	14.6426

TREE	4.9462	1.0020	2	1.0122	149.9109	149.1047	53.9452	53.8539
HOUSE	45.8193	1.0028	2	1.0133	179.2868	178.3837	24.1748	24.1209
CANDY	43.2001	1.0021	2	1.0089	222.2984	222.3023	14.7379	14.1239

Fig 3 and 4 show the cover image Lena with its stego image.

Fig 3 Original Lena Image Fig 4 Stego Lena Image

Fig 5 and 6 show the cover image Peppers with its stego image

7 Original Peppers Image 8 Stego Peppers Image

Figure 9 and 10 show the cover image Pink Flower with its stego image.

11 Original Pink Flower 12 Stego Pink Flower Image

Conclusion

In the past few years Steganography is interesting topic to make communication more secure. This paper gives an overview about Steganography and its techniques. All techniques of Steganography satisfy all the four properties (robustness, Imperceptibility, embedding capacity, payload capacity).In this paper some main methods of spatial domain have seen. LSB is the first method which was introduced but in this method static attacks are possible. So other methods were introduced. It depends on the user which method user choose. Frequency domain a complex technique but this provides more security than spatial domain. This paper provides an overview, how steganography helps in secure communication. Steganography make communication more secure. In this method combination of both steganography and cryptography is used.

References

[1] Westfeld A., Pfitzmann A., "Attack on steganographic system," in *Lecture Notes in Computer Science* **1768**, pp. 61-75, 2000.
[2] Fridrich J., Goljan M., "Practical steganalysis of digital image – State of the art," in *Security and Watermarking of Multimedia Contents IV*, Delp EJ, Wong PW, ed., *Proc. SPIE* **4675**, pp. 1-13, CA, USA, 2002.
[3] J. Harmsen, W. Pearlman., "Higher-order statistical steganalysis of palette images," in *Security and Watermarking of Multimedia Contents* , *Proc. SPIE* **5020**, pp. 131-142, 2003.
[4] Andrew D. Ker, "Steganalysis of LSB matching in grayscale images," in *IEEE Signal Processing Letters* **12**, pp. 441-444, 2005.
[5] Onkar Dabeer, Kenneth Sullivan, Upamanyu Madhow, "Detection of hiding in the least significant bit," *IEEE Transactions on Signal Processing* **52**, pp. 3046-3058, 2004.
[6] Cox I., Miller M., Bloom J., Fridrich J., Kalker T.: Digital Watermarking and Steganography. 2nd edit. Elsevier 2008. 592 p.
[7] Vovk O.O. and A.A. Astrakhantsev "Rozroblennja metodyky ocinjuvannja vazhlyvosti kharakterystyk steghanoghrafichnykh alghorytmiv [Development of methods of evaluation for importance of steganographic algorithms characteristics]", *Visnyk natsionaljnogho universytetu Ljvivsjka politekhnika*. No 805, pp. 52 – 60, 2014. – In Ukrainian.

[8] Atawneh S. and Sumari P (2013) Hybrid and blind steganography method for digital image based on DWT and chaotic map, J. Commun. 8.11:690–699

[9] Artz , D Digital Steganography: Hiding Data within Data(2001) IEEE Internet Computing Journal A. O. C Efficient Data Hiding System using Cryptography and Steganography (2012) 4.11:6–11

[10] Garg Mukesh and Jangra A.P. Gurudev An Overview of Different Type of Data Hiding Scheme in Image using Steganographic Techniques (2014) International Journal of Advanced Research in Computer Science & Software Engineering 4.1: ISSN: 2277 128X .

[11] Kelley, Jack. (2001) Terror groups hide behind Web encryption USA Today. 19 June 2001. Associated Press. (2001) Bin Laden foils U.S. technology .MSNBC. 20 Sep 2001.

[12] Kahn, D., "The Code breakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet", Macmillan, 1967, ISBN-0-684-83130-9.

[13] Jung K.-H and Yoo K.-Y (2009) Data hiding method using image interpolation Computer Stand. Interfaces 31.2:465–470.

[14] Cheddad A, Condell J, Curran K, and Mc Kevitt P (2010) Digital image steganography: Survey and analysis of current methods Signal processing 90.3:727–752.

[15] Johnson N. F. and Jajodia S (1998) Exploring steganography: Seeing the unseen Computer (Long. Beach. Calif) 31.2.