Image Steganography In Frequency Domain

Using threshold based Uniqueness of an Image

Kavi Abhishek Venkat (*Author*)

Student-B Tech. Computer Science, Scope

VIT University, Vellore- 632014 [Kaviabhishek.venkat2015@vit.ac.in](mailto:Kaviabhishek.venkat2015@vit.ac.in)

*Abstract*— Steganography is a mode of imperceptible communication, that's done by hiding the particular information in some medium. In image Steganography, the imperceptible communication is achieved by including the info into the original image (original image). The aim of Steganography is to require care of secret communication between a pair of parties. This paper will show however the Steganography within the frequency domain is employed in associate extremely stylish context whereas providing a wise understanding of what Steganography is and also the thanks to accomplish it.

Keywords—Information, image, steganography, information hiding, frequency domain, threshold.

# **Introduction**

Steganography is a word which is created from Greek words Stegans (Originaled), and Graptos (Writing) which accurately refers original writing. Normally, steganography is understood as imperceptible communication. Steganography means that to hide messages subsistence in another medium (audio, video, image, communication). Today’s steganography systems use multimedia system objects like image, audio, video etc as visual media. Individuals typically convey digital pictures over email or share them through diverse web communication application. It's totally different from protecting the particular content of a message. In simple words it might be like concealing data into different data [2].

Steganography isn't to change the structure of the key message, however hides it within a original-object (carrier object). Once concealing method object and stego-object (carrying hidden data object) area similar. So, steganography (hiding information) and cryptography(protecting information) area all totally unlike from each other because of physical property or hidden issue it's hard to reoriginal data while not noted procedure in steganography. Hiding procedure of steganography called Steganalysis.

**2. Basic Image Steganographic Methods**

Image steganography methods are categorised in following domains:

**2.1 Spatial Domain Methods:** There are quite a few versions of spatial steganography, all directly modifying some bits within the image element values which are out of sight information. Least important bit (LSB)-based steganography is one of the methods that hides a secret message within the LSBs of picture element values while not introducing numerous perceptible distortions. Changes within the pixel of the LSB area are not visible to the human. spatial domain methods area generally categorized into [2]:

1. Texture based method

2. Labelling or connectivity method

3. Random pixel embedding method (RPE)

4. Edges based data embedding method (EBE)

5. Histogram shifting methods

6. Pixel value differencing (PVD)

7. Pixel intensity based method

8. Least significant bit (LSB)

9. Mapping pixel to hidden data method

**2.2 Transform Domain Method**: There are seldom a lot of complicated means of concealing data in a picture. Various algorithms and transformations methods are used on the image to original data in it. Frequency domain embedding are seldom termed as a website of embedding methods that variety of algorithms are urged. The method of embedding information within the frequency domain of a symbol is way stronger than embedding principles that operate within the time domain. Most of the robust steganography systems nowadays operate among the Frequency domain methods, have a plus over spatial domain methods as they hide data in areas of the image that are less exposed to compression, cropping, and image processing. Some Frequency domain methods don't appear obsessed with the image format and that they might run lossless and lossy format conversions. Frequency domain methods area in general categorized into [2]:

1. Discrete Fourier transformation method (DFT).

2. Discrete cosine transformation method (DCT).

3. Discrete Wavelet transformation method (DWT).

4. Lossless or reversible method (DCT)

5. Embedding in coefficient bits

**2.3.** **Distortion Methods:** Distortion methods need information of some initial original image throughout the decipherment method wherever the decoder works to visualize for variations between the initial original image and also the distorted original image so as to renew the key note. In this method the encoder append a series of variations to the original image. So, data is represented as stuck by signal distortion [2].

**2.4. Masking and Filtering**: These methods hide data by marking a picture, within the same means on paper watermarks. These methods engraft the data within a lot of important areas than simply concealing it into the background level. The hidden note is a lot further integral to the original image. Watermarking methods are often applied without the worry of image destruction because of lossy compression as they're more embedded into the image [2].

**3. Literature Review**

Hiding secret data within the low important bits (LSB) of image’s pixels could be a casual and extensively used method of steganography. A variety of methods are given within the domain of LSB steganography methods. Every given method has its own pros and cons in terms of embedding capability and signal to noise magnitude relation in paper [5],

**LSB+** is been introduced like the LSB matching, a small message b with value 0 or 1 is inerted by adjusting an integer (such as pixel value or quantized DCT coefficient) but LSB+ matching is done by dynamically determining the embedding operation [5]

This procedure tends to insert more in the low-frequency group, and less in the DC and middle-frequency bands, and smallest in the high-frequency band. The embedding rate is attuned by increasing the value of limit k in matrix encoding (i.e. embedding k bits into 2k 1 bit places). [5]

In paper [1] **Improved MSB using Bit Differencing** is that the planned work, a replacement method is given wherever most important bits (MSB) of pixels’ area taken so as to original secret information bits.

Encoding

i. browse the key data bits

ii. browse the original image

iii. for each picture element of original Image

a. browse bit No. 5 and 6

b. work out the distinction

c. Compare the distinction with secret data bit, if information bit isn't adequate to the distinction then transverse bit No. 5

iv. Write the stego image

Decoding

i. browse the stego image

ii. for each picture element of stego image

a. work out the distinction between fifth and sixth bits: information bit = distinction

iii. write the key information to file

**Snake and Ladder Based Algorithm** [3] is an additional approach in which the formula is introduced within which for encrypting the Stego Key, picture element pixel Differencing is allotted. The most pixel within the PVD matrix is computed and also the Stego key's hold on as associate offset from 255.

D(a,b) = C(a,b+1)-C(a,b) wherever a calculated from i to row of C. To cypher the Stego Key1 of start address D (a, b) =255-maximum [ D (c, d)]. This counterbalances the Stego key of beginning Address. [3]

The size of continuous bits is employed as a 2d Stegno Key wherever the direct right diagonal picture element to the most in PVD matrix is in use as size of continuous bits to be encrypted. D (i,o) =255-D (a+1, b+1)

where m,n is that the location of size of continues bits and p,q is that the location of the beginning column on 1st row of original image. [3]

Through PVD matrix we tend to get the smooth of the original Image and herewith will embed the 2 Stego keys in high frequency area.

The secret writing of 2 stego keys is followed by embedding g the continues bits within the original image by LSB modification method.

The Snake Ladder formula is employed for embedding the info employing Prime - Non Prime Logic. [3]

In paper [6], **(N. 1) Secret Sharing Approach Based on Steganography with grey Digital** pictures is introduced and this method employs the formula Exclusive-OR to every mixture of the N-bit computer code, there exist 2N consequences and it follows the situations shown within the following. Let A(i) be i’th bit of assistant N-bit computer code. Let conjointly Bin2Dec () be a perform to original the given computer code to the equivalent decimal range wherever X is that the result. X are going to be the resulting decimal range once the N bits’ area focused along. [6]

**Data Hiding in Intermediate Significant Bit Planes** [10] is introduced in which the data is to be embedded within the bit planes which has been divided into 3 variable size data vectors of eternally decreasing sizes. The embedding strategy is portrayed.

Embedding Strategy and relationship between size paths: The planned data concealing system, disruptions the info course to be embedded, in smaller extent vectors equal to the amount of ISB planes within which information is to be hidden. The sizes of information vectors are often connected in many ways within the enforced method, the info has been broken into 3 blocks with sizes L1, L2 and L3. This is often as a result of information which is to be embedded in 3 ISBs. The connection among the sizes of information blocks is L1= L/2, L2= 3L/8 and L3=L/8; wherever L is that the total size of information vector to be inserted within the original medium. The info is inserted within the embedder under the management of a private key. [10]

*B. Extraction Strategy:* The engrafting formula uses personal key to embed the info within the ISBs of original image. The resultant image yielded by information embedder is named stego image. At the receiving side the extraction formula uses stego-image together with same key as that used at embedder to extract information from the stego-image. Since original image isn't required for the retrieval of secret data the planned system falls within the class of blind detection. [10]

**Pixel Value Differencing (PVD)**: In PVD method, grey scale image is employed as a original image with an extended bit-stream because of the secret knowledge [4]. It was initially projected to original secret data into 256 grey valued pictures. the tactic relies on the very fact that human eyes will simply observe little changes within the smooth areas, however they cannot monitor comparatively larger changes at the smooth areas within the pictures. PVD uses the similarity between the constituent and its neighbour to see the quantity of inserted bits.

This method is projected to reinforce the embedding capability while not improper visual changes in stego-image. However the disadvantage of This method is projected to reinforce the inserting capability but not inappropriate visual changes in stego-image. However, the disadvantage of the tactic is that the constituent price within the stego-image could exceed the range 0-255 that ends up in improper visual image of the stego image. It's conjointly weak security performance is due of non-adaptive quantisation, inserting some data in swish areas etc.

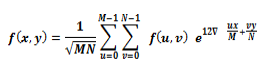
**Histogram Shifting Method:**

Histograms area unit used for graphical illustration of image: It represents the constituent price and density at a selected constituent. It plots the constituent for each and every a part of the image. A bar graph is beneficial to spot constituent distribution, density of colours and tonal spreading. A bar graph provides the best and lowest constituent values in graph. Bar graph shifting is the method that is employed to change or to extract an explicit cluster of pixels from a picture. In bar graph the best price is named maxima and therefore the lowest price is named minima, once the constituent price is changed for inserting method it shouldn't cross the minima and maxima limit. There area unit has many formulas that support bar graph practicality so as to govern the picture. The quantity of the pixels constituting the height within the bar graph of a canopy picture is sufficient the disguise capability as a result of one peak in a very original picture is employed.

In **DFT** all the addition of hidden message is finished within the frequency domain. It's a lot of advanced method of activity message into frequency domain of the picture. The separate Fourier rework of spacial worth f(x,y) for a picture of size M × N is outlined in equation for frequency domain transformation.

.

Equally inverse separate fourier rework (IDFT) is employed to convert frequency element of every px worth to the spacial domain worth and so the equation for transformation from frequency to spacial domain is



When DFT is used it changes the duvet picture from spacial domain to frequency domain and every px in spacial domain is remodeled into 2 parts: real and pure imaginary number. The embedded texts bits square measure inserted in real a part of frequency domain not including 1st px. When inserting, IDFT is performed frequency domain regenerate into spacial domain throughout the removal or cryptography of the message picture from spacial domain is remodeled to frequency domain. When using DFT and removal rule the initial supply picture is retrieved.[9]

The **DCT** converts the picture from spacial to frequency domain and separates the picture into spectral sub-bands with regard to graphic value of the picture, that is low, middle and high frequency elements . Here Sunshine State and FH is employed to denote very cheap frequency elements and better frequency elements severally. FM is employed as inserting region to produce extra resistance to lossy compression methods, whereas avoiding important modification of the duvet picture.

It is utilized in the JPEG compression rule to rework consecutive eight × eight px blocks of the picture into sixty four DCT coefficients every in frequency domain. Every DCT stable F(u,v) of associate degree eight × eight px block of picture pixels f(x,y) is calculated by [10].

1. **Proposed Method**

Steganography has been enforced on pictures in frequency domain so as to original great deal of information with high security, sensible physical property and no loss of secret knowledge. All the operations area unit is administrated in grey scale pictures.

EMBEDING ALGROTHIM:

1. Convert **RGB image to gray scale**
2. Initial threshold is the average of the pixels
3. Average of the pixels below the threshold is the unique key(K)
4. Encrypt the message using **Caesar cipher** and the **unique key**(K)
5. Apply **forward Fourier transform**
6. R=R+K\*EM where R is the real part of image and EM is the encrypted message
7. Apply **inverse Fourier transform** to the entire image (Real +Complex)

EXTRACTION ALGORITHM:

1. Load original and stego image.
2. Convert images into frequency domain.
3. Subtract stego image form original
4. Divide the difference of the image with the original image by K
5. Consider the array obtained as ASCII values of alphabets and obtain the string (alphabets)
6. The array of character is the hidden message

**RGB to grey scale** The lightness method computes the average of the least prominent and the most prominent colors: (min(R, G, B) + max(R, G, B) ) / 2. Whereas the average method merely computes the average of the values: (R + G + B) / 3.

The luminosity method is a better version of the average method. It not only computes the average of the values, but also it forms a weighted average so as to adjust for human perception. For instance, green has a larger weight as our eyes have more sensitivity to green color than other colors. Luminosity can be computed by the formula: 0.21 R + 0.72 G + 0.07 B.

**Uniqueness**- A structured procedure with the concept of mean and threshold has been devised in order to obtain the unique key(K). This is unique for every image and represents where the message is hidden in the image.

1.Get image

2.take average of the pixels

3.remove pixels higher than the average of the image

4.take average again

This new average will be the unique key(K) for the image.

**Caesar cipher** (also known as shift cipher) can be defined as a basic substitution cipher in which every single character of the open text is replaced with a character, which is fixed number of positions below the alphabet. Ci = (Ti+k) (mod m)

Ci - ith character of closed text

Ti – ith character of open text

k - shift

m – total size of alphabet

The decryption process uses reverted procedure:

Ti = (Ci-k) (mod m)

**The** **Fourier Transform** can be considered as a significant image processing tool which can be applied for image decomposition into its sine and cosine elements. The output image of fourier transformation depicts the image in the Frequency or fourier domain, while the input image is equivalent to spatial domain.

The DFT is the sampled Fourier Transform and therefore does not contain all frequencies forming an image, but only a set of samples which is large enough to fully describe the spatial domain image. The number of frequencies corresponds to the number of pixels in the spatial domain image, i.e. the image in the spatial and Fourier domains are of the same size.

For a square image of size N×N, the two-dimensional DFT is given by

We consider the image as R=R+K\*EM where R is the real part of image and EM is the encrypted message.

We can apply inverse Fourier transform to the entire image (REAL+COMPLEX)

To re-transform the fourier image to the spatial domain, we apply the inverse fourier transform by –

1. **APPLICATIONS**

• Originalt communication and sensitive information storing

The benefits of Steganography are that it provides us:

(A) Capability to hide the presence of originalt information

(B) Difficulty to detect hidden information.

(C) Enhancing the encryption of the originalt information.

• Metadata in Media info systems

Metadata refers to aspect info inserted in a picture which will serve several functions. as an instance, a business will infix the online website address for a particular product in an exceedingly image that shows a billboard for that product.

Steganography will solve this drawback as a result of a steganography program unifies 2 types of information into one by manner of inserting operation. So, information will simply be transferred from one system to a different while not hitch.

• The use of watermarking in medical records as a method of correct identification is straight away apparent. With the medical trade migrating additional and additional toward digital records, watermarking becomes a compulsory addition to stop mix-ups in patient records. thanks to the varied protocols and totally different platforms utilized in the pc world, information typically will become corrupted once it's regenerate from one format to a different.

• Modern pc printers use steganography, as well as Hewlett-Packard and Xerox, complete colour optical maser printers. Tiny yellow dots are added by the printer to every page. These almost invisible invisible dots hold encoded time stamps, date and serial numbers of the printer.

• Broadcast monitoring: this is often accustomed monitor if the shrunken range of commercials were broadcasted in an exceedingly given time interval or not. This ensures if the commercials got due air time or not.

• Fingerprinting: this is often accustomed prevents unauthorized duplicates and distribution of information by inserting a definite watermark (or fingerprints) in every copy of the info. E. information binding:

• Originalt communication: To transmit info in secret from transmitter to receiver.

• Access system for distributing digital contents.

In this space inserted information is "hidden", however is "explained" to publicize the content.

Today, digital contents have gotten additional and additional ordinarily distributed over web than before. as an example, music corporations unharness new albums on their Webpage in an exceedingly free or charged manner. However, during this case, all the contents square measure equally distributed to the those who will build access to the page. So, a standard net distribution theme isn't fitted to a "case-by case" and "selective" distribution. after all it's invariably attainable to connect digital contents to e-mail messages and send them to the purchasers. However it'll takes lots of pixel in time and labor.

If you have got some valuable content, that you're thinking that it's distributable if somebody very wants it, and if it's attainable to transfer that content on web in some originalt manner. And if you'll issue a special "access key" to extract the content by selection, you may be terribly happy concerning it. A steganography theme will facilitate understand this kind of system.

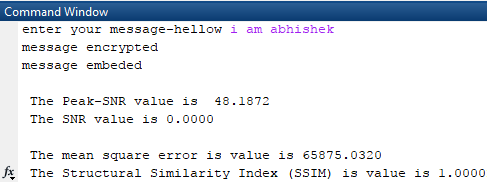
1. **RESULT AND CONCLUSION**:

In this research paper, DFT method is used to hide the message in the image. It concluded that each image has a unique key (K) which is the average of the pixels below the threshold with the help of which along with DFT, image steganography is carried out.

The specifications of the image is : Grey level Lena 512×512×8; and Color Lena 512×512×3.

A long stream of bits is taken as a hidden message. The implementation of the proposition has been carried out via MATLAB tool. Figures below represent the resultant stego images when the proposed algorithm has been implemented.

Embedding



We performed some image quality test using PSNR,

SSIM and MSE the results are as follows-

The Peak-SNR value is 48.1872

The SNR value is 0.0000

The mean square error is value is 65875.0320

The Structural Similarity Index (SSIM) is value is 1.0000

* From the above image quality matrix, we can state that the output stego image is structurally homologous to the original so it is impossible to visually detect any deference
* The mean square error is also in the range of 30-50db which is
* Even though the MSE is high that can be caused due to addition of noise this will not affect the structure and visual appearance of the image

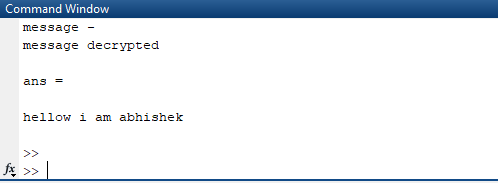
Original image:



Image containing the message:



Extraction-



So this method can be used as a new method for steganography as it is more reliable and advanced than most of the available methods which are generally dependent on spatial data manipulation. By using the frequency domain data manipulation, we have an upper hand in terms of data loss and similarity of the stego image to the original.

1. **REFERENCES**

[1]. Ammad Ul Islam1, Faiza Khalid2, Mohsin Shah2,Zakir Khan2 , Toqeer Mahmood3, Adnan Khan2, Usman Ali2, Muhammad Naeem4: An Improved Image Steganography Method based on MSB using Bit Differencing

[2]. Mehdi Hussain and Mureed Hussain: A Survey of Image Steganography Method

[3]. Jas R Sheth: Snake and Ladder Based Algorithm for Steganographic

[4]. Rupesh Gupta, Dr.Tanu Preet Singh: New Proposed Practice for Secure Image Combing Cryptography Stegnography and Watermarking based on Various Parameters.

[5].Hao-tian Wu, Jiwu Huang: SECURE JPEG STEGANOGRAPHY BY LSB+ MATCHING AND MULTI-BAND EMBEDDING

[6]. Jinsuk Baekl, Cheonshik Kim2, Paul S. Fisherl, and Hongyang Chao: (N. 1) Secret Sharing Approach Based on Steganography with Gray Digital Images

[7]. Xiaozhong Pan, BoTao Yan, Ke Niu: Multiclass Detect of Current Steganographic Methods for JPEG Format Based Re-stegnography

[8]. Beenish Mehboob and Rashid Aziz Faruqui: A Steganography Implementation

[9]. Imran Sarwar Bajwa, Rubata Riasat: A New Perfect Hashing based Approach for Secure Stegnograph

[10]. Shabir A. Parah, Javaid A. Sheikh, G.M. Bhat: Data Hiding in Intermediate Significant Bit Planes, A High Capacity Blind Steganographic Method