



Pixel Steganalysis – A Novel Approach in Image Steganography Using F5 Algorithm

Prabhu Kumar¹, Nikhil Tirpathi², G.Michael³

UG Student, Dept. of CSE, Bharath University, Chennai, India^{1,2}

Assistant professor, Dept. of CSE, Bharath University, Chennai, India³

ABSTRACT: The **Faugère F5 algorithm** first calculates the Gröbner basis of a pair of generator polynomials of the ideal. And it uses to reduce the sizes of initial matrices of created messages which had to be embedded in image steganography. The stenographical systems are weak against statistically and visually weak which offers only a relatively small capacity of stenographic message but the newly developed f5 algorithm help to embedded messages in images large capacity of steganography. It implement matrix encoding and permutation straddling to embedded message with large capacity and reduces the embedded-image.

KEYWORDS: F5 algorithm, Permutation straddling, Matrix encoding, Image steganography, JPEG encoder.

I.INTRODUCTION

Today, the Internet is a key communication infrastructure for inter-connecting individuals across the world with the internet which allowed them to send, receive, and share data even encrypted and decrypted files among each other. As this trend developed into an everyday activity, securing sensitive data became of matter of great concern. The basic need of every growing area in internet world is communication. Everyone wants to keep and share the information inside of work to be secret, safe, secured. We use many insecure pathways in our daily life for transferring and sharing information using internet or telephonically, but at a certain level of internet communication it is not too safe. Steganography and Cryptography are two best methods which could be used to sending, receiving, sharing information in a concealed manner. Steganography includes modification of message in a way which could be in digesting or encrypted form guarded by an encryption key which is known by sender and receiver only and without using encryption key the message could not be accessed from receiver or sender. But in cryptography techniques it's always too clear for any intermediate person in covert channel of communication that the message is in encrypted form, whereas in steganography techniques of embedding messages the secret message is made to hide in image which formed stego-image so that it couldn't be clearer to any intermediate person that whether there is any message which is hidden in the form of information being shared through covert channel. The cover image containing the secret message is then transferred to the recipient. The recipient is has the authority to extract the message with the help of retrieving process of some algorithm and secret key provided by the sender.^[3] It is the art of hiding and transmitting data through apparently carriers in an effort to reveal the existence of the data in another data, the word Steganography which means covered or hiding writing which is literally earned from Greek. Steganography has its place in security for transferring the stego-data. It is not processed for replacing cryptography but supplement it. Hiding a message with Steganography techniques reduces the greater chance of a message being detected. There are lots of algorithms used in image steganography area. However, they have their own weaknesses and strengths. since f5 algorithm is one of the best algorithm which is mainly used for data hiding and embedding message into jpg image which containing the permutation straddling and matrix encoding, encodes message in large capacity of stegano-graphic system and also arrange the message in sense of Huffman coding which mainly increases the security which is not easy to identify and detect in embedding technique which has been used in embedded images.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

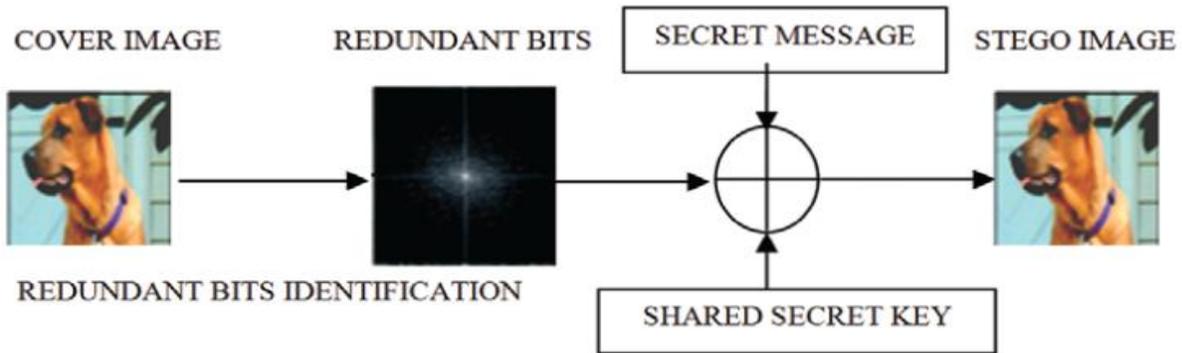


Figure 1. Generic steganography process.

II. LITERATURE SURVEY

There are different types of stegano-graphic algorithm which uses for hiding the data into image. The basic needs for data hiding is cover file related to image which embedded the data file into bit space of image pixels. The F5 technique of data hiding provides the proper protection on transmitting the data. In this paper the newly developed algorithm F5 implemented which provide more security and presumed visual statistical error is almost negligible. The main approach of the paper is consistency of permutation straddling and matrix encoding which is partitioned the image into equal part and encoding through JPEG encoder which encodes more volume of data.



Fig 2: The embedding message into picture



Fig 3: The decoding image from stego-image



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

III. EXISTING SYSTEM

^[2]The main concept which was used in recent project was compared with original file as file weight age and color variations of pixels. The main purpose of Cryptography techniques is latent communication to hide the existence of a message from a third party, but it's too Complex to embedded and Extract the message from stego-data. LSBs of the elements pointed by the determined locations are used for embedding and extraction and it doesn't opposes permutation straddling and matrix encoding which secured not more enough. Before embedding and extraction data, a location finds the method which determines a sequence of locations that point to elements in the cover stego-object. A commonly used strategy for Steganography techniques is to embed the message by slightly distorting the cover-object into the target stego-Object Reducing distortion is a crucial issue.

IV. PROPOSED SYSTEM

The proposed method is driven by an algorithm that works as follows: Every character in the input secret message is encoded using newly generated strong number generator which indexed that points to a random character in the Pangram sentence, and an offset index that denotes the total number of bit character which has to be arrange with an pair of 8bit, 16bit, 24bit index and the first occurrence of the character being encoded in the embedded message. The maximum allowable length of the sentence which is going to be embedded in jpg image is 512 characters. Using hash function the random generated number could be arranged in multiple of bit but if not arranged in sequences of multiple of bit the remaindered number of bit could be added in last arranged bit of generated number which secured more the remained bit which doesn't give space to be statistically and visually attacks.

The primeprogression of the proposed method is that it employs two mediums, instead of one, that complement each other to deliver the secret data, making the covert data so robust against stego-attacks.

V. MODULE DESCRIPTION

1. JPEG file encoding format

^[1]The file format defined by the Joint Photographic Experts Group (JPEG) stores image data in lossy compressed form as quantized frequency coefficients. It expressed losing some quality and reducing the actual frequency of each pixel in order to its easily to identify and convert into BMP which could be recognized by algorithm to be JPEG encoder this algorithm which encodes the image to JPEG after partitioning the images into 8X8 pixel nevertheless, It refers to a standards organization, a secure techniques of file compression, and sometimes a changing the jpeg file format from .gif, .jpg, .etc. First, the JPEG compressor cuts the uncompressed bitmap image into parts of 8 by 8 pixels by blocking the image partition of any extension of image format. The discrete cosine transformation (DCT) which expresses a finite sequences of pixel point in image in terms of sum of cosine function oscillating at different frequency of image position, transfers 8×8 brightness values into 8×8 frequency coefficients (real numbers) and After DCT, the quantization suitably rounds the frequency coefficients to integers in the range $-2048 \dots 2047$. It compressed 8×8 pixel wise and remained pixels of image could return to algorithm procedure of compressing technique through an DCT.

The basic theory about compressing the image in JPEG is "the BMP image which comes across Discrete cosine transform the reason behinds using cosine rather than sine is critical to compress, which generates pixel is in cosine transform which could be arranged through quantization which mapped a large set of pixels input values in smaller sets of values which could be compressed with helps of Huffman coding specializing the character which has been used in pangram sentences.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

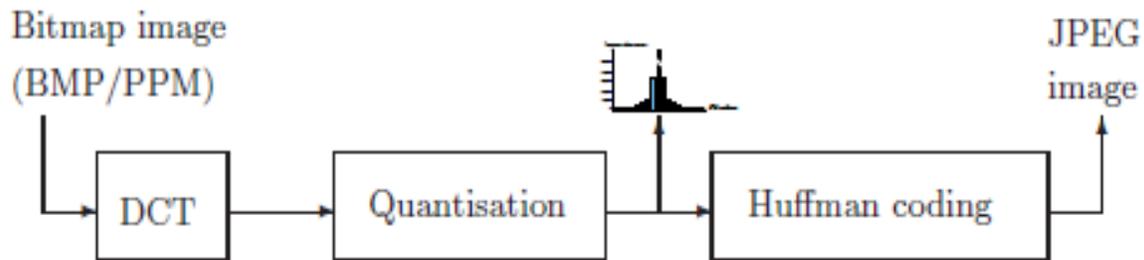


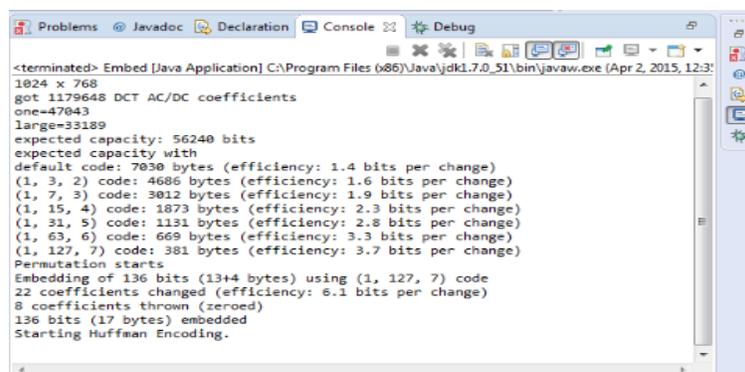
Fig 4: The procedure of jpeg compressor through Huffman coding.

2. Permutation straddling

The straddling mechanism used with F5 shuffles all coefficients using a permutation first. Then, F5 arranged the bits of pixel of image into the permuted sequentially. The shrinkage does not change the number of coefficients. The permutation depends on a key derived from a password. F5 delivers the stegano-graphically changed coefficients in its original sequence to the Huffman coding algorithm. With the correct key, the receiver is capable to repeat the permutation.

VI. RESULT

The stego image could be more secured after the arranging the message in the matrix encoding and permutation straddling which compact in a more secured pangram sentences of message. Steganography can used for almost all digital file formats, but the formats which has a high degree of redundancy are more agreeable. Redundancy can be defined as “the bits of a cover-object which provides more accuracy literally greater than necessary for the object’s manipulation. The redundant bits of a cover-object are those bits that can be modify without the modification being identified easily. Image and audiofiles especially comply with this necessity, while research has also uncovering other file formats that can be used for information hiding.in this paper we got result as the message which we are going to hide will be encoded zigzag technique and every techniques to encode one part of total bit message and remaining will be encode in another technique. It also get update in result about indices shuffled through permutation straddling.



```
<terminated> Embed [Java Application] C:\Program Files (x86)\Java\jdk1.7.0_51\bin\javaw.exe (Apr 2, 2015, 12:3:
1024 x 768
got 1179648 DCT AC/DC coefficients
one=47043
large=33189
expected capacity: 56240 bits
expected capacity with
default code: 7030 bytes (efficiency: 1.4 bits per change)
(1, 3, 2) code: 4686 bytes (efficiency: 1.6 bits per change)
(1, 7, 3) code: 3012 bytes (efficiency: 1.9 bits per change)
(1, 15, 4) code: 1073 bytes (efficiency: 2.3 bits per change)
(1, 31, 5) code: 1131 bytes (efficiency: 2.8 bits per change)
(1, 63, 6) code: 669 bytes (efficiency: 3.3 bits per change)
(1, 127, 7) code: 381 bytes (efficiency: 3.7 bits per change)
Permutation starts
Embedding of 136 bits (13+4 bytes) using (1, 127, 7) code
22 coefficients changed (efficiency: 6.1 bits per change)
8 coefficients thrown (zeroed)
136 bits (17 bytes) embedded
Starting Huffman Encoding.
```

Fig 5: The encoding input of image and message into Stego-image.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

```
<terminated> Extract [Java Application] C:\Program Files (x86)\Java\jdk1.7.0_51\bin\javaw.exe (Apr 2, 2015, 12:36)
Huffman decoding starts
Permutation starts
1179648 indices shuffled
Extraction starts
Length of embedded file: 13 bytes
(1.. 127.. 7) code used
```

Fig 6: The decoding output of stego-image into image and message

VII.CONCLUSION

In this study of F5 algorithm most of the effort is done to get a better imperceptibility, increasing capacity, increasing security without losing stego-image quality and most important concept which has been studied is

like the reducing the embedded image size which does not get lose the image resolution as well as Hash function is used to generate a pattern, which is random selection of edge pixels, for more security and better stego-image quality.

REFERENCES

1. LinjieGuo, Jiangqun Ni “Uniform Embedding for Efficient JPEG Steganography” IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 5, MAY 2014
2. Ravinder Reddy Ch1 RojaRamani A2 “The Process of Encoding and Decoding of Image Steganography using LSB Algorithm” IJCSET Vol 2, Issue 11, November 2012
- 3.Morkel 1, J.H.P. Eloff 2, M.S. Olivier 3 “An overview of image steganography” University of Pretoria, 0002, Pretoria, South Africa
4. Kritika Singla1, and Sumeet Kaur2 “Hash based approach for secure image steganography using canny edge detection method” IJCSC Vol 3. No 1. JAN 2012
5. Jessica Fridrich1, Miroslav Goljan1, Dorin Hoge2 “Steganalysis of JPEG Images: Breaking the F5 Algorithm” NY13902-6000, USA.
- 6.BhagyashriRahangdale , “Hash Based Least Significant Bit Technique For Video Steganography”,IJERA,VOL 4, JAN 2014, INDIA

BIOGRAPHY



Mr. Prabhu Kumar has been with Dept. of CSE, Bharath University, India since 2011.His research interests includes Steganography, Cryptography and Data hiding. He had been with St. Xavier’s college, Ranchi, India whither awarded as best performance in HSC, 2011.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015



G Michael has been with Bharath University, India since 2004. He has more than 10 years of experience in assistance ship. He received the ME degree from Annamalai University, India, BE degree from Rajaa's Engineering college, India and perusing PHD from Bharath university, India. His research interest include digital data hiding, Steganography, Cloud computing, information assurance. He has authored and co-authored more than 22 papers. He awarded as innovative research faculty from the Bharath University, India.



Mr. Nikhil Tirpathi has been with Dept. of CSE Bharath University, India since 2011. His research includes data-hiding, steganography.