DFT BASED INDIVIDUAL EXTRACTION OF STEGANOGRAPHIC COMPRESSION OF IMAGES

C. Rengarajaswamy[1]

[1] *Assistant Professor, Department of Electronics and Communication Engineering, M.A.M School of Engineering, Trichy, Tamil Nadu*

Abstract

A Novel scheme of Separable Extraction of concealed data and compressed image is proposed adopting a transform based compression over the encrypted data. Reversible data hiding is branched under Steganography. In this reversible data hiding the art of concealing a secret data over the cover image is practiced. More than that, the main ingredients that play the key role are encryption key and the data hiding key, the compression is performed in between the two processes i.e., encryption and data hiding, to create a spare space to accommodate the secret data. The main aim of this proposed scheme is to limit the distortion and to enhance a wide space for concealing of the secret data i.e., to increase the embedding rate. The compression here classified into lossy and lossless. Lossy compression best suits for image and audio (telephone conversation, etc.) whereas lossless compression needed in the text and videos. Hence to perform the lossless compression over a stegomized image and improve its secrecy, DFT is performed after Encryption.

Keywords: *DFT, Data Embedding, RDH, Separable RDH, Compression*

---***---

1. INTRODUCTION

In the world of communication, security plays a vital role and owns a major regime on its stack. The word communication now a day's does not travel alone, but hand in hand with security aspects. Thus security turns to be the key to unlock a communication box. Coming to security, which is branched into cryptography, information hiding and watermarking etc, provides better role as they take part. As the technology keeps on changing its face with advanced features, there is need to get updated to it in its long run towards the betterment of future. Usually the happening is that when a new algorithm is produced or an existing algorithm is revised, intruders or hackers break the algorithm. So it is a must to develop algorithms more efficient and be stable and unbreakable to most extent. Normally, the network security is branched into cryptography and information hiding. Information hiding contains Steganography and watermarking which may be dated back old compared to cryptography. In cryptography, scramble of data's takes place at the transmitter and unscrambling them gives the exact input at the receiver section. Thus for scrambling and unscrambling denoted technically as encryption and decryption, a key is used. Thus to encrypt and decrypt same key or different keys may be used. Further extending its branches into symmetric (conventional) and asymmetric (public key) encryption. Here in the former encryption, same key is used both at the transmitter and receiver. Bit in the later case, different key is handled. Coming to Steganography, which is art of concealing of data into other. It may be dated past, but again heads to more secure transmission. In order to improve the security level, combination of various techniques is handled. One such try is the Steganography over cryptography. Thus both the techniques provide better authentication and integrity among the users. One such technique chosen under Steganography is RDH (Reversible Data Hiding). In RDH, major ingredients are the cover data and the secret data. Cover data is which the secret data to be hidden, like the letter enclosed in an envelope. The other is secret or additional data. Here the overall data enclosing the cover data and secret data is called the marked cover. In RDH more importance is given to the cover data, such that the user information is inscribed over it. There is a lot application employing RDH mainly in the case of military communication, patient details, in case of emergency over country, etc. The below diagram illustrates the basic block of how RDH is processed through. Thus embedding secret data to the cover data at transmitter and the reverse process explains abut extracting the secret data as well as the cover data without any error, if error data not recovered. The later part of this paper is lapsed as follows. Section II comprises related works describing RDH and its separable extension. Section III describes the proposed work handling stream cipher encryption and DFT compression and embedding. Section IV gives us the exact view of the proposed scheme as the experimental results using Image Processing Tool. Section V summarizes the whole content to a short and sweet manner. Further, in section VI the references are listed.

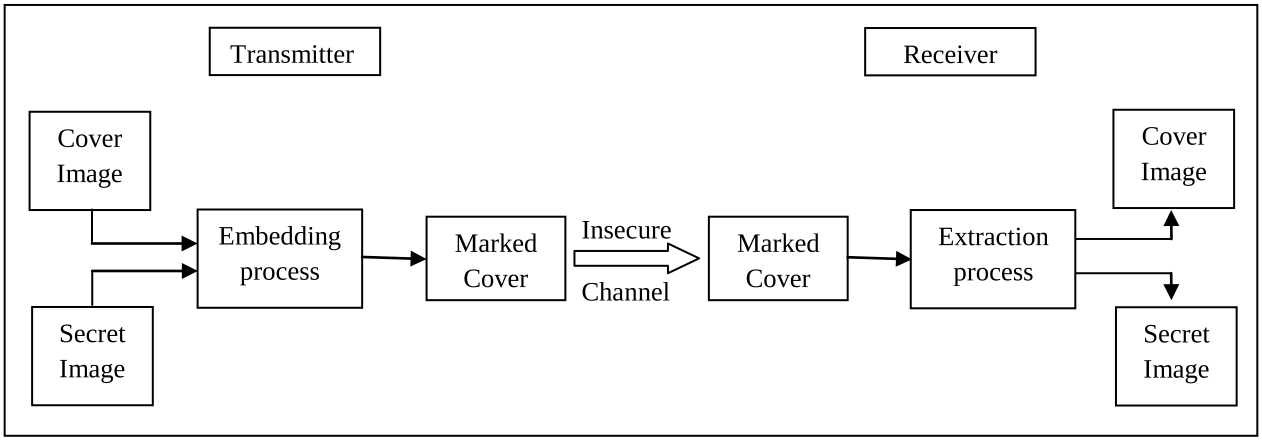


Fig 1 Basic Block diagram of RDH

2. RELATED WORKS

2.1 Embedding in LSB

A digital image is basically divided into pixels. These pixel values may vary for each type of images. For a Binary image, the pixel value is 1, for gray scale and color the range of pixel is 8-bit and 24-bit. So to carry the LSB embedding process, mostly gray scale and color images are preferred. Here in LSB only the least bits of a pixel is altered or cleared to embed the secret or additional data. If any change is made in the MSB bits, they change the whole nature of the Image. Here the Payload Data (secret Data) is embedded in such a way that can be reconstructed only at the receiving end. The common procedure that is carried out to embed a payload data is given by the formula [1],

$$S_i = C_i + C_i \bmod 2^k + m_i$$

Here $S_{i\ -}$ stego image, C_i - the cover image, k - the embedding parameter and m_i - the payload.

Thus LSB is the most basic method and used in common for creating the sparse space. Thus the sparse space created is useful for hiding the additional payload data. This makes the work easier. Hence at the extraction part it is easier to retrieve the original message as well as the secret data with low data loss.

2.2 Reversible Data Hiding

Reversible data hiding (RDH) is a technique which is entirely different from other substitution techniques. In RDH, the main aim is to recover the data without any error. If there is any error either in the cover data or the secret explained as follows. The above diagram shows us how the process is successfully carried out using RDH. The RDH consists of two steps each carried at the transmitter and the receiver end. At the transmitter side the data is embedded into the cover image in the sparse space already created to hide data. Here the additional data hidden in done using the data-hiding key, so that the same key is used at the receiver to recover the secret data. As soon as the compression and embedding process the data is passed to the receiving end along with the data-hiding key. In the receiver end, the extraction process is carried out using the same data-hiding key.

During this process if any change is done in the transmitted data, it causes some error in the transmitted data. Thus if any error occurs either in the cover image r the secret data, the original data cannot be retrieved. This is the special property of using RDH which provides additional authentication and integrity.

2.3 RDH over Encrypted Images

In this section, RDH is performed over an encrypted Image. Thus it carries three steps and two keys which is same for both the transmitter and the receiver. The first is encryption using encryption key and sparse space creation and third is the data embedding using data-hiding key. The receiver is done in an orderly process i.e., decryption using the encryption key to recover the cover image and then applying the data-hiding key to recover the secret data. If any key is applied without the specified manner the cover image and the secret data cannot be recovered, which is a unique property of RDH [2].

2.4 Separable RDH over Encrypted Images

In the earlier method proposed [2], at the receiver end decryption is performed first in order to extract the cover image and then applying the data-hiding key to recover the secret data, which is non-separable in manner. In the case of separable RDH, either of the key can be used irrespective of the other to recover the respective data’s independently [3] was proposed. This proves to be better flexible among the user handling different keys.

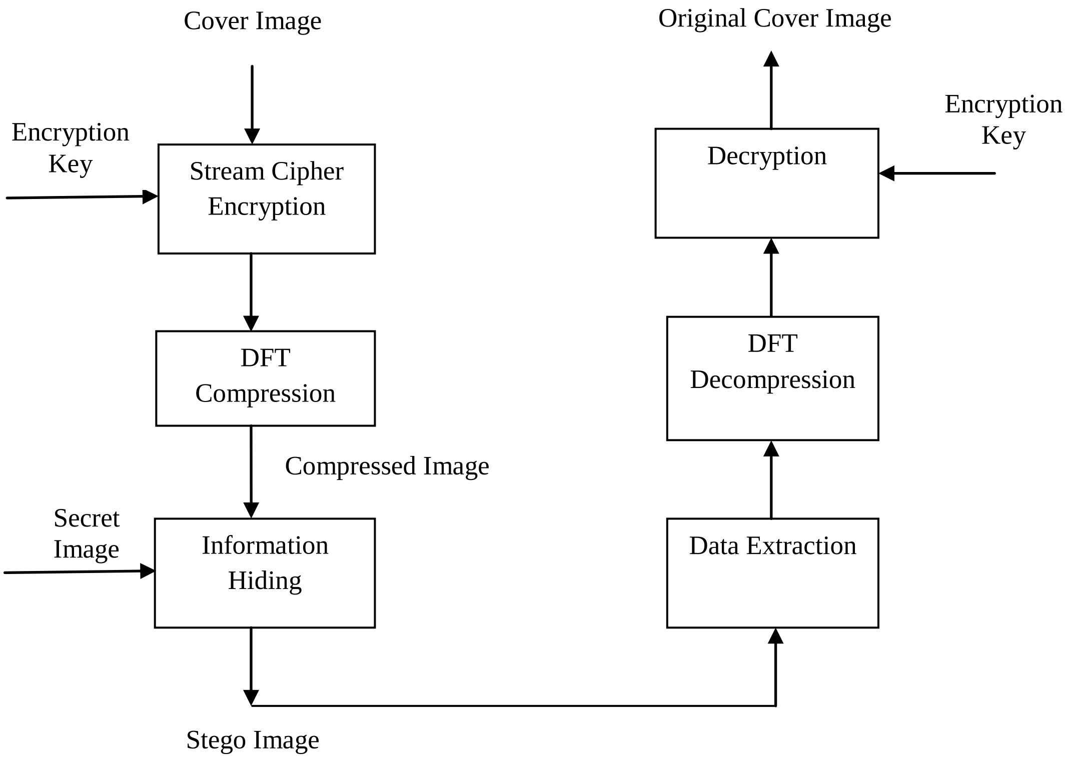


Fig 2 Proposed RDH using DFT

3. PROPOSED SCHEME

3.1 Encryption Using Stream Cipher

In the encryption part, it is a must to choose what type of encryption is adopted and which is best suitable. Stream cipher encryption is chosen despite its high security and flexibility. In stream cipher, the encryption in carried as bit by bit format, whereas in the block cipher, an entire block is subjected to encryption. In stream cipher, a raw data is XOR-ed with the randomly generated key by the pseudorandom generator. The pseudo random generated key is used both at the transmitter and the receiver. Thus the same key is used to decrypt the data at the receiver end, hence the name symmetric key encryption.

$$D_{i,j,u} = d_{i,j,u} \oplus k_{i,j,u}$$

Here i,j represents the row and column of the image and u represents the face value of each bit in the pixel. In this encryption, each bit of the pixel is XOR-ed with the key generated by the pseudorandom generator. As the encryption key is pseudo randomly generated and reproduced only at the receiving end, which cannot be produced by any intruders and is difficult to break or analyze the image. A basic algorithm for stream cipher is RC4 provides better security. Thus each and every bit in the data is encrypted and is highly secured.

3.2 Compression using DFT and Data Embedding

Compression is a technique for reducing the file size making it suitable for data transmission. There are two types of compression, namely lossless and lossy. Image in its 2-D form can be compressed using various techniques. One primary method is to use Discrete Fourier transform (DFT). DFT gives the better approximation of Fourier transform on discrete set of frequencies. The spatial values in such 2-dimension is represented as f(x,y). The transformed image is represented as F(u,v).

$$F(u,v) = \frac{1}{\sqrt{M.N}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) e^{-j2\pi\,(\frac{ux}{M}+\frac{vy}{N})}$$

The inverse Fourier transform is thus given by,

$$f(x,y) = \frac{1}{\sqrt{M.N}} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u,v) e^{j2\pi\,(\frac{ux}{M}+\frac{vy}{N})}$$

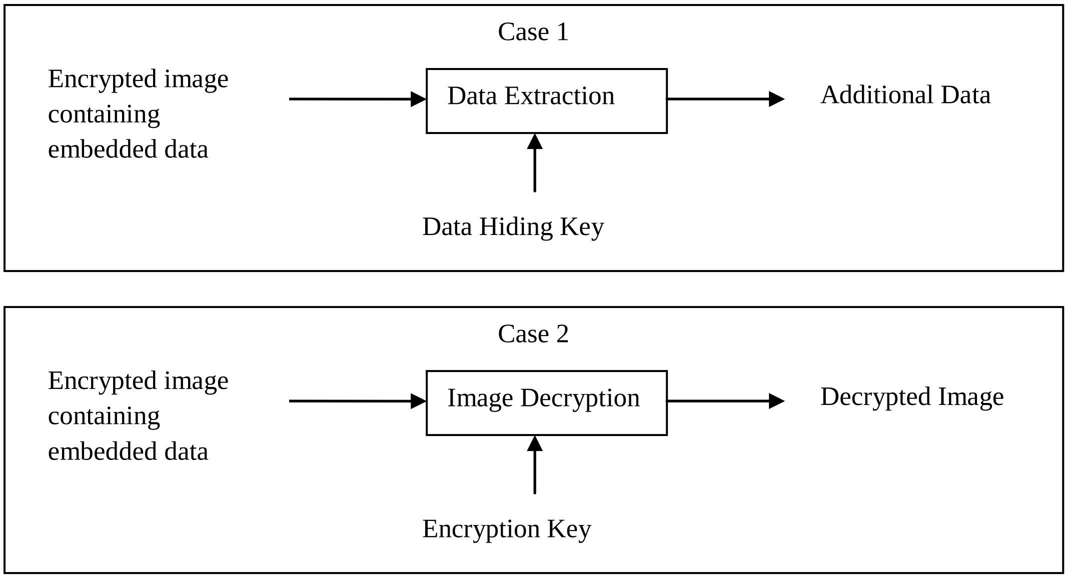


Fig 3 Separable Receiver Section

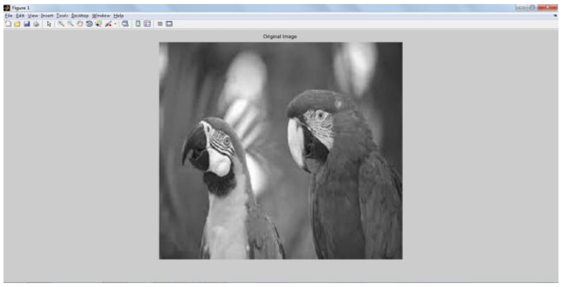
The transform equation suggests that an image of size MxN with spatial values (x,y) is transformed into one with values (u,v) [4].

Fast Fourier Transform (FFT) is the fastest method of DFT. FFT is a high speed and efficient technique. At the reconstruction stage, the image compressed using lossless method will have better image quality than the one that is compressed using lossy method [5].

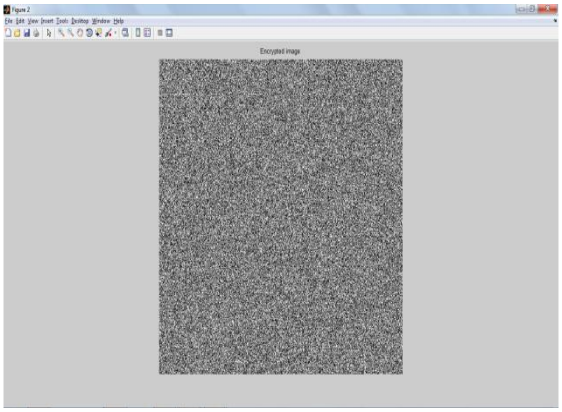
3.3 Decryption and Extraction

In the receiver side, the reverse process is carried out [3]. Here as the data is received they can be separately extracted independently using either the encryption key which is pseudo randomly generated to extract the decrypted image. Here the same pseudo random generated must be provided by the receiver in order to extract the cover image. Then the data-hiding key is applied to the recovered image to extract the secret data. The keys can be used alternatively to recover any one of the data also. Hence offer better flexibility.

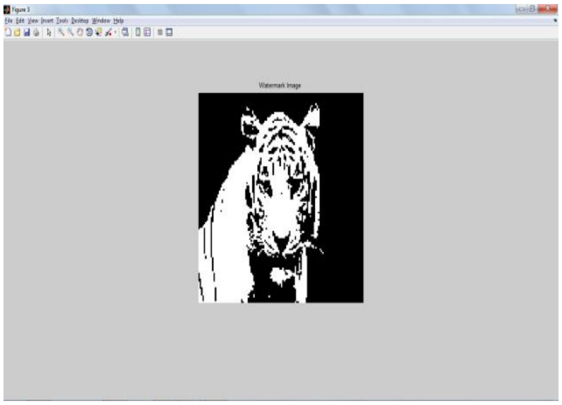
4. EXPERIMENTAL RESULTS



(a) Original Cover Image



(b) Stream Ciphered Image



(c) Secret Image

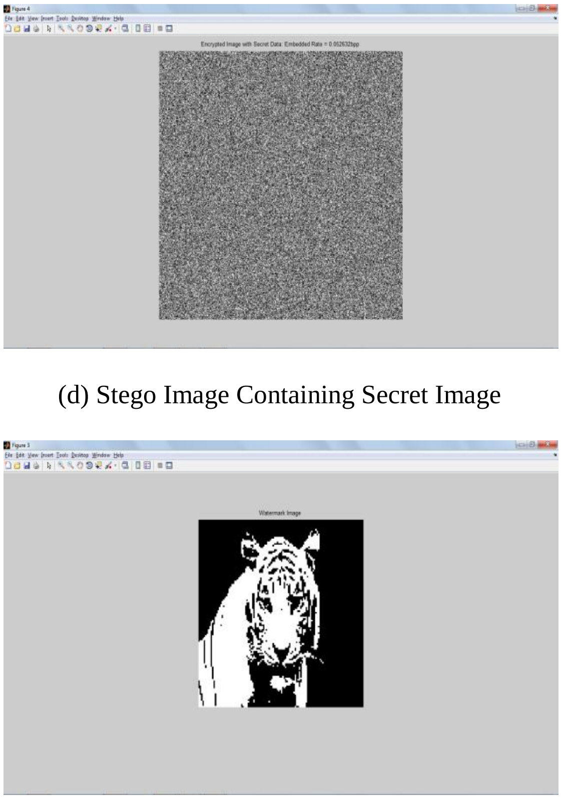


Figure 4
File Edit View Insert Tools Desktop Window Help
Encrypted Image with Secret Data: Embedded Rate = 0.052632bpp
Figure 5
File Edit View Insert Tools Desktop Window Help
Watermark Image

(d) Stego Image Containing Secret Image

(e) Extracted Secret Image

Fig. 4 Implemented Outputs

The figure above shows the results of the proposed system. Initially, an image taken is considered to be a cover image. This image is now given for DFT compression after which the secret image is embedded into the cover. The obtained stego image is then given into a separable receiver for separable extraction of original image and the secret image.

CONCLUSIONS

In this paper we briefly discuss about how to encrypt a data, compress the encrypted data and embed a data to the compressed one. The later part explains about the extraction and decryption. To summarize all this, at the transmitter side an encryption is carried using the encryption. Then the DFT compression is done to the encrypted image to create the space needed to hide the secret image. In the free space provided the additional secret data is embedded using the data-hiding key. DFT thus provides efficient compression in the frequency domain basis. Then at the receiver side, either of the key is used independently to recover the cover image and the secret data separately. Among more other compression techniques DFT operates well in the frequency domain which is best suited for audio and images. Hereby concluding that DFT provided best compression rate and loss is a least part considering.

REFERENCES

[1]. C. K. Chan and L. M. Cheng, “Hiding data in images by simple LSB substitution,” Pattern Recognit., vol. 37, no. 3, pp. 469–474, 2004.

[2]. Manikandan R Asst. Professor, Uma M , MahalakshmiPreethi S M, “Reversible Data Hiding for Encrypted Image”, Journal of Computer Applications ISSN: 0974 – 1925,Volume-5, Issue EICA2012-1, February 10, 2012

[3]. X. Zhang, “Reversible data hiding in encrypted image,” IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.

[4]. Inderjit Singh, Sunil Khullar, Dr. S.C. Laroiya, “DFT Based Image Enhancement and Steganography”, International Journal of Computer Science and Communication Engineering, ISSN : 2319-7080, Vol2, Issue 1, Feb 2013.

[5]. Mridul Kumar Mathur, Gunjan Mathur, “ Image Compression using DFT through Fast Fourier Transform Technique”, International Journal of Emerging Trends and Technology in Computer Science”, ISSN : 2278-6856, Vol 1, Issue 2, July-Aug 2012.