Discrete Fourier Transformation based Image Authentication Technique

Debnath Bhattacharyya, Jhuma Dutta, Poulami Das
Computer Science and Engineering Department, Heritage Institute of Technology, Kolkata, India
E-mail: debnathb@gmail.com, {jhumadutta81,dasp88}@gmail.com

Rathit Bandyopadhyay
Cognizant Technologies, Kolkata, India
E-mail: rathit@rediffmail.com

S.K. Bandyopadhyay
Member, IEEE
University of Calcutta, Kolkata, India
E-mail: skb1@vsnl.com

Tai-hoon Kim
Member, IEEE
Hannam University, Daejeon, Korea
E-mail: taihoonn@empal.com

***Abstract*— In this paper a novel technique, Discrete Fourier Transformation based Image Authentication (DFTIAT) has been proposed to authenticate an image and with its own application one can also transmit secret message or image over the network. Instead of direct embedding a message or image within the source image, choosing a window of size 2 x 2 of the source image in sliding window manner then convert it from spatial domain to frequency domain using Discrete Fourier Transform (DFT). The bits of the authenticating message or image are then embedded at LSB within the real part of the transformed image. Inverse DFT is performed for the transformation from frequency domain to spatial domain as final step of encoding. Decoding is done through the reverse procedure. The experimental results have been discussed and compared with the existing steganography algorithm S-Tools. Histogram analysis and Chi-Square test of source image with embedded image shows the better results in comparison with the S-Tools.**

***Index Terms*— Authentication, Data Hiding, Discrete Fourier Transformation (DFT), Frequency Domain, Inverse Discrete Fourier Transform (IDFT), S-Tools.**

I. INTRODUCTION

THE most popular technique for image authentication or steganographic technique is embedding message or image within the source image, generally termed data hiding which also provides secret message transmission over the communication channel.

Moreover several techniques are available for secret message transmission by hiding a message inside an image without changing its visible properties but the source image may be changed. Instead of direct embedding message or image within the source image, the embedding is done in the frequency domain.

The presented work deals on information and image protection against unauthorized access in frequency domain. The frequency domain is the domain where the analog picture of continuous signal resides. A picture in the spatial domain can be described as a collection of pixel values describing the intensity values. The DFT changes an N point input signal into two point output signals. The input signal contains the N/2 –1 signal being decomposed, while the two output signals contain the amplitudes of the component sine and cosine waves. The input signal is said to be in the time domain. This is because the most common type of signal entering the Discrete Fourier Transformation (DFT) is composed of samples taken at regular intervals of time. Any kind of sampled data can be fed into the DFT, regardless of how it was acquired. The frequency domain signal is represented by a vector F[u,v], and consists of two parts, for each of the samples. These are called the Real part of F[u,v] written as: *ReF*[u,v], and the Imaginary part of F[u,v], written as: *ImF*[u,v]. In the sample "real part" means the cosine wave amplitudes while "imaginary part" means the sine wave amplitudes. The basic formula of DFT for a function f (x, y) of size M x N is given in equation (1) for frequency domain transformation.

For the cause of the proposed algorithm the simpler from of equation (1) is as given in equation (2).

$$F(u,v)=\frac{1}{\sqrt{MN}}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)\cos\left(\frac{2\pi ux}{M}\right)-f(x,y)j\sin\left(\frac{2\pi vy}{N}\right)$$

for u=0,1,... M-1 v=0,1,... N-1 ……..(1)

$$F(u,v)=\mathrm{Re}F(u,v)-\mathrm{Im}F(u,v)$$

for u=0,1,... M-1 v=0,1,... N-1 .... (2)

where the ReF(u ,v) and ImF(u ,v) is given in equation (3) and (4).

$$\mathrm{Re}\,F(u,v)=\frac{1}{\sqrt{MN}}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)\cos\left(\frac{2\pi ux}{M}\right)$$

for u=0,1,... M-1 v=0,1,... N-1 ... ... (3)

$$\mathrm{Im}\,F(u,v) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \sin\left(\frac{2\pi vy}{N}\right)$$

for u=0,1,... M-1 v=0,1,... N-1 ... ... (4)

Similarly inverse discrete Fourier transformation, where the frequency domain gets converted to the spatial domain, digital image may be written as in equation 5.

$$f(x,y) = \frac{1}{\sqrt{MN}} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u,v) \cos\left(\frac{2\pi ux}{M}\right) + F(u,v)\, j \sin\left(\frac{2\pi vy}{N}\right)$$

for x=0,1,... M-1 y=0,1,... N-1 ....(5)

Considering the real parts of the transformed image and embedding authenticating message or image bits at the LSB of each source pixel (exclusive the 1st pixel). After embedding, the embedded image is converted into spatial domain by using IDFT for transmitting over the network. The technique provides more security as embedding the message or image has been done by considering a window of the source image in sliding window manner and then transforming into frequency domain.

II. Earlier Works

Nameer N. EL-Eman in April, 2007, implemented an algorithm based on hiding a large amount of data (image, audio, text) file into color BMP image. They have been used adaptive image filtering and adaptive image segmentation with bits replacement on the appropriate pixels. These pixels are selected randomly rather than sequentially by using new concept defined by main cases with their sub cases for each byte in one pixel [1].

Palak K. Amin, Ning Liu, K. P. Subbalakshmi in 2005, described a discrete cosine transform (DCT) based spread spectrum data-hiding algorithm that provides statistical security [2].

R. Chandramouli, N. Memon in 2001, considered some specific image based steganography techniques and shown that an observer can indeed distinguish between images carrying a hidden message and images which do not carry a message [3].

S. Dumitrescu, Xiaolin Wu and Zhe Wang in 2003 introduced an approach to detecting LSB steganography in digital signals. They shown that the length of hidden messages embedded in the LSB of signal samples can be estimated with relatively high precision. That approach was based on some statistical measures of sample pairs that are highly sensitive to LSB embedding operations [4].

Brian Chen, Gregory W. Wornell in 2001 described the problem of embedding one signal (e.g., a digital watermark), within another "host" signal to form a third, "composite" signal [5].

Moulin, P. O'Sullivan, J.A. in 2000 analyzed Information hiding as a communication game between an information hider and an attacker, in which side information is available to the information hider and to the decoder. They derived several Capacity formulas [6].

Pierre Moulin, M. Kıvanç Mıhçak in 2002 described an information-theoretic model for image watermarking and data hiding. Some recent theoretical results been used to characterize the fundamental capacity limits of image watermarking and data-hiding systems. Capacity was determined by the statistical model used for the host image, by the distortion constraints on the data hider and the attacker, and by the information available to the data hider, to the attacker, and to the decoder. They considered autoregressive, block-DCT and wavelet statistical models for images and compute data hiding capacity for compressed and uncompressed host-image sources [7].

Ching-yung Lin and Shih-fu Chang in 1998 described a different goal from that of image watermarking which embeds into the image a signature surviving most manipulations. They described an effective technique for image authentication which can prevent malicious manipulations but allow JPEG lossy compression. The authentication signature was based on the invariance of the relationship between DCT coefficients of the same position in separate blocks of an image [8].

Pavan, S. Sridhar, G. Sridhar, V. in 2005 proposed a hybrid image registration algorithm to identify the spatial or intensity variations between two color images. The proposed approach extracts salient descriptors from the two images using a multivariate entropy-based detector. The transformation parameters are obtained after establishing the correspondence between the salient descriptors of the two images [9].

H.H. Pang, K.L. Tan, X. Zhou, in 2004 introduced StegFD, a steganographic file driver that securely hides user-selected files in a file system so that, without the corresponding access keys, an attacker would not be able to deduce their existence. They proposed two schemes for implementing steganographic B-trees within a StegFD volume [10].

III. Our Work

The presented work emphasizes on information and image protection against unauthorized access in frequency domain. The DFTIAT uses gray scale image of size (M x N) to be authenticated .The technique inserts authenticating message or image $X_{m,n}$ of size (M/2*N/2*3)-16 bits (maximum) as the first 16 bit holds the dimension of the file. DFT, given in equation-1 is used to transform the image from spatial domain to frequency domain. The encoding and decoding schemes are given in fig. 1 and fig. 2 respectively.

The details algorithm for insertion and extraction are described in the following sections:

A. Insertion Algorithm

1. Take a message file or image whose size is less than or equal to (M/2*N/2*3)-16 bits where M x N is the size of the cover image.
2. Take 2 x 2 window of the cover image in sliding window manner and repeat step 3 and 4 until the ends of the cover image.
3. Apply the Discrete Fourier Transformation.
4. Consider the real part of the frequency component and do the following.
   - Take three frequency component values

but not the first one and do the following.

- Consider the Least Significant Bit position of the DFT component.
  - Replace the bit by one authenticating bit.

5. Apply the Inverse Fourier Transformation.
6. Stop.

B. *Extraction Algorithm*

1. Take the authenticated image as input.
2. Consider 2 x 2 mask of the input image at a time and repeat step 3 and 4 until the ends of the embedded image.
3. Apply the Discrete Fourier Transformation.
4. Consider the real part of the frequency component and do the following.
   - Take three frequency component values but not the first one and do the following.
     - Extract the Least Significant Bit.
     - Replace this bit position by '1' or by '0'.
5. Apply the Inverse Fourier Transformation.
6. Stop.

IV. RESULT

In this section results are analyzed and comparative studies have been made between proposed technique and S-Tools in terms of test for homogeneity i.e. Chi-square test and histogram analysis. Here in our work, Section A illustrates the Chi-Square test and section B deals with histogram analysis.

Fig. 3a shows source image 'Hill' and Fig. 3b shows the authenticating image 'Lotus' and Fig. 3c and Fig. 3d are embedded image using proposed algorithm and S-Tools respectively. In fact, Fig. 3a – 3d shows the visual fidelity in embedding 'Lotus' using DFTIAT and S-Tools. The authenticating image 'Lotus' has been embedded into the source image 'Hill'.

Some differences may be observed between source image and embedded image by S-Tools [11] but no such differences are observed in source image and embedded image by proposed technique.

Fig. 4a – 4d indicates the comparison of visual changes for another source image 'Rasmancha' (Fig. 4a) embedding with the same Lotus image (Fig. 4b). The results are embedded image using proposed algorithm (Fig. 4c) and S-Tools (Fig 4d). Here, may be observed some variations between source image and embedded image by S-Tools but no such differences are observed in source image and embedded image by DFTIAT. Basically, Fig. 4a – 4d shows the comparison of visual fidelity in embedding 'Lotus' using DFTIAT and S-Tools.

A. *Chi-Square Test*

The Chi-Square test has been performed for the source image and authenticated image, and also for the Authenticating Image & Extracted Image. The values of chi-squares are given in Table 1 for different images, which show that the calculated chi-square value is less than the tabulated chi-square value for some level of significance, which indicates the homogeneity of the images. They are more significant for 1% level of uncertainty. For the authenticating and extracted image the Chi-Square value is zero. That is we are able to extract the original image without any noise.

B. *Histogram Analysis*

Histogram analysis has also been performed between source image 'Hill' and for the embedded image using 'Lotus' by applying proposed technique and S-Tools. In both the cases noticeable differences are observed in frequency distribution table of pixel values in source image and embedded image using S-Tools algorithm. But very small variances are observed in frequency distribution table of pixel values in source image and embedded image using proposed technique. Fig. 5a – 5c shows the visual effect in histogram in embedding source image 'Hill' with proposed technique and S-Tools. Fig. 5a is the histogram of the source image 'Hill', Fig. 5b shows the histogram of the image embedded with 'Lotus' image using proposed technique and that of Fig. 5c is the histogram of the image embedded using 'Lotus' image by applying S-Tools. It is seen clearly that in the proposed technique the histogram remains almost identical with the source image even after embedding the image with 'Lotus' image where as in case of embedding with Stools there is a noticeable change in histogram in compare to the histogram of source image 'Hill'. From these observations it may be inferred that the proposed technique may obtain better performance in embedding. Histogram analysis has also been done for another source image 'Rashmancha', which is shown in Fig. 6a – 6c.

V. CONCLUSION

In this paper the proposed technique implemented here for image authentication and secret message transmission scheme. The algorithm used here is the bit level message or image insertion and extraction in the frequency domain. Using DFTIAT we are also able to extract the source image. In this technique 2 x 2 window is selected for better result of authentication. Insertion and extraction is done in frequency domain instead of spatial domain for more security. From the analysis of Chi-Square test and histogram analysis and comparison with S-Tools the proposed technique may obtain better result.

ACKNOWLEDGEMENT

The first three authors would like to thank Prof. Samir Kumar Bandyopadhyay of University of Calcutta, India, and Prof. Tai-hoon Kim of Hannam University, Korea, for their continuous support and inspirations towards completion of this work.

REFERENCES

[1] Nameer, N. EL-Eman, "Hiding a large Amount of data with High Security Using Steganography Algorithm", Journal of Computer sciences, April 2007, pp. 223-232.

[2] Palak K. Amin, Ning Liu, K. P. Subbalakshmi, "Statistically Secure Digital Image Data Hiding", Multimedia Signal Processing, IEEE 7th Workshop, Shanghai, Oct. 2005, pp. 1-4.
[3] R Chandramouli, N. Memon, "Analysis of LSB based image steganography techniques", International Conference on Image Processing, Thessaloniki, Greece, 2001, pp.1019-1022.
[4] S. Dumitrescu, Xiaolin Wu, Zhe Wang, "Detection of LSB steganography via sample pair analysis", IEEE Transactions on Signal Processing, July 2003, Vol. 51, Issue 7, pp. 1995-2007.
[5] Brian Chen, Gregory W. Wornell, "Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding", IEEE Trans. on Information Theory, 2001, volume 47, pp. 1423-1443.
[6] P. Moulin, J.A. O'Sullivan, "Information-theoretic analysis of information hiding", IEEE International Symposium on Information Theory, June 2000, Sorrento, Italy, pp. 19.
[7] Pierre Moulin, M. Kıvanc Mıhcak, "A Framework for Evaluating the Data-Hiding Capacity of Image Sources", IEEE Trans. on Image Processing, Sept. 2002, Vol. 11, pp. 1029-1042.
[8] Ching-yung Lin and Shih-fu Chang, "A robust image authentication method surviving JPEG lossy \ compression", SPIE, 1998, pp.296-307.
[9] Pavan, S. Sridhar, G. Sridhar, V. "Multivariate entropy detector based hybrid image registration", IEEE ICASSP-2005, 18-23 March, 2005, Vol. 2, pp. ii/873- ii/876.
[10] H.H. Pang, K. L. Tan, X. Zhou, "Steganographic schemes for file system and B-tree", IEEE Transaction on Knowledge and Data Engineering, June 2004, Vol. 16, Issue 6, pp. 701- 713.
[11] http://www.spychecker.com/download/download_stools.html visited as on March 28, 2009.

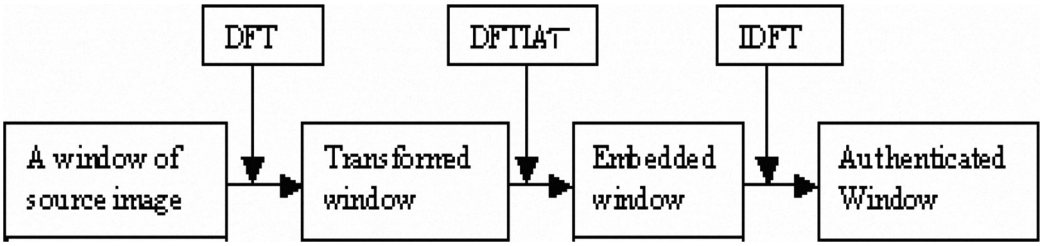

Fig. 1. Encoding scheme using DFTIAT

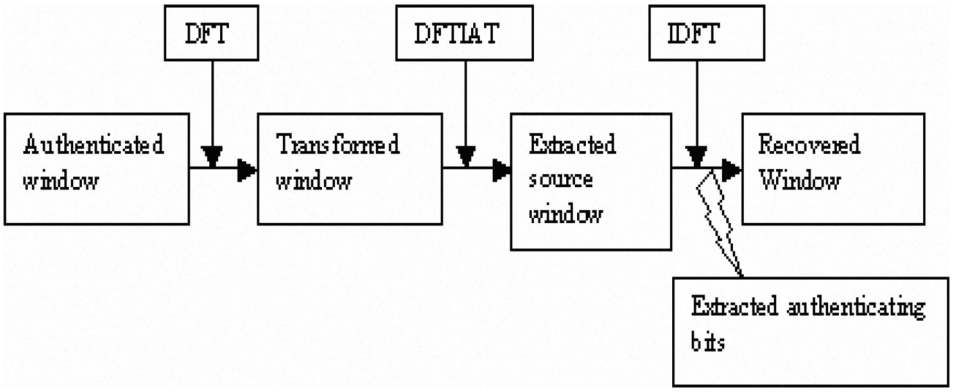

Fig. 2. Decoding scheme using DFTIAT

Fig. 3a. Hill

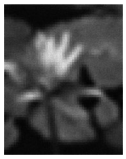

Fig.3b. Lotus

Fig.3c. DFTIAT

Fig. 3d. S-tools

Fig. 4a. Rashmancha

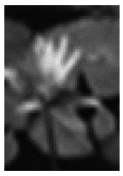

Fig.4b. Lotus

Fig.4c. DFTIAT

Fig. 4d. S-tools

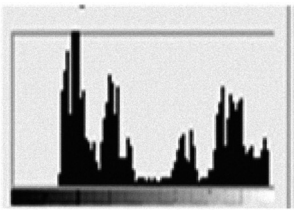

Fig. 5a. Hill

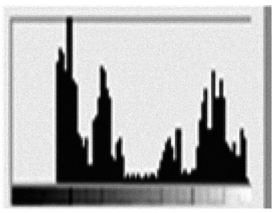

Fig. 5b. DFTIAT

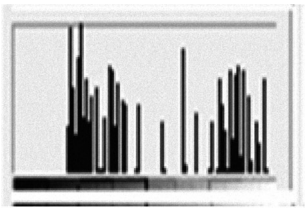

Fig. 5c. S-Tools

Table 1. Comparison of Chi-Square values in DFTIAT

Images	File Size	Uncertainty	Degree of freedom	Calculated Chi-Square	Tabulated Chi-Square
Source and authenticated Hill image by Lotus	98 x 130	0.01	255	264.219	310.457
Authenticated and Extracted Hill Image	98 x 130	0.001	255	315.089	347.650
Source and Authenticated Rashmancha Image	98 x 130	0.01	255	241.284	310.457
Authenticating Image & Extracted Image	33 x 26	0.01	255	0.00	310.457