A Novel Technique for Image Authentication in Frequency Domain using Discrete Fourier Transformation Technique (IAFDDFTT)

Nabin Ghoshal[1], ***Jyotsna Kumar Mandal***[2]
[1]Dept. of USIC, University of Kalyani, Kalyani, Nadia-741235, West Bengal, India.
E-mail: nabin_ghoshal@yahoo.co.in
[2]Dept. of Computer Science and Engineering, University of Kalyani, Kalyani, Nadia- 741235, India.
E-mail: jkm.cse@gmail.com

ABSTRACT

In this paper a novel technique for Image Authentication in Frequency Domain using Discrete Fourier Transformation Technique (IAFDDFTT) has been proposed to authenticate a gray level PGM, TIFF image by embedding a message/image where 2 x 2 submatrix is taken as source matrix from the image matrix and transform into the frequency domain. Two bits of authenticating message/image are fabricated within the real part of each pixel, excluding the first pixel of each submatrix where the position is chosen using a hash function. The process is repeated for each submatrix on row major order to insert authenticating message/image content and 128 bits Message Digest (MD-5), generated from authenticating message/image. Inverse DFT is performed to transform the embedded image from frequency to spatial domain as final step of encoding. The decoding is done through the reverse procedure. The experimental results against statistical and visual attack has been discussed and compared with the existing steganography algorithm like S-Tools. Histogram analysis, noise analysis, and standard deviation computation of source image with embedded image shows the better results in comparison with existing S-Tools.

Keywords: Steganography, Image Authentication in Frequency Domain using Discrete Fourier Transformation (IAFDDFT), S-Tools, MD-5, Authentication, Discrete Fourier Transformation (DFT), Frequency Domain.

1.0 INTRODUCTION

Steganographic study is a technique to achieve authentication of images and secrete communication between two parties that are inserted in hiding not only the content of secrete message/image but also act as communicating it. To this aim, steganography algorithms embed the secrete information into different types of natural cover data like sound and images. The resulting altered data is referred to as stego-data and it must be perceptually indistinguishable from its natural cover. So, steganography is the art of secrete communication. Security is a big concern in modern day image trafficking across the network. Security can be achieved by hiding data within the image. Data hiding [1] in the image has become an important technique for image authentication and identification. Ownership verification [8] and authentication is the major task for military people, research institute, and scientist. Image authentication is a technique for inserting information into an image for identification and authentication. Image authentication technology is becoming increasingly important due to the proliferation of digital images on the WWW and in e-commerce. So, information security and image authentication has become very important to protect digital image document from unauthorized access [9, 10]. These are tools and techniques used to protect the originality and to ensure the authenticity of the image document.

Data hiding refers to the nearly invisible [2] embedding of information within a host data set as message, image, and video. In steganographic [4] applications, the hidden data may be secrete message or secrete hologram or secrete video whose mere presence within the host data set should be undetectable. The data hiding represents a useful alternative to the construction of a hypermedia document or image, which is very less convenient to manipulate. The goal of steganography is to hide the message/image in the source image by some key techniques as the result observer has no knowledge of the existence of the message/image and it is unlike cryptography where the goal is to secure communications from an eavesdropper by making the data non-understandable. In some situations, sending encrypted information will arouse suspicion while invisible information will not do so. To hide a message inside an image without changing its visible properties [5] the source image may be altered.

Chandramouli et al. [3] developed a useful method for making such alterations by masking, filtering and transformations of the least significant bit (LSB) on the source image. Dumitrescu et al. [4] construct an algorithm for detecting LSB steganography. Pavan et al. [8] used entropy based technique for detecting the suitable areas in the document image where data can be embedded with minimum distortion. S-Tools [11] works by spreading the bit pattern of the file that you want to hide across least significant bits (LSBs) of the color levels in the image to prevent the prediction of potential enemy. Among existing methods discussed, S-tools is a powerful, efficient and well known authentication technique in spatial domain. From potential aspects S-Tool is chosen for comparison with the proposed technique. From recent works [7, 9] it is obvious that digital data can be effectively hidden in an image so as to satisfy the criteria that the degradation to the host image is imperceptible and it should be possible to recover the hidden message/image under a variety of attack.

The presented work emphasizes 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. Once the continuous signal get sampled and quantized they get into a spatial domain where the representation of the image is in discrete form. The most common type of signal entering the Discrete Fourier Transformation (DFT) is composed of samples taken at regular intervals of time. In the sample "real part" means the cosine wave amplitudes while "imaginary part" means the sine wave amplitudes. The DFT of a function (image) f(x , y) of size M x N is given in equation 1 for frequency domain transformation.

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

for u = 0 to M – 1 and v = 0 to N-1

The variables u and v are the frequency variables and x, y are the spatial or image variables. Similarly inverse discrete Fourier transformation, where the frequency domain gets converted to the spatial domain, digital image may be written as in equation 2 for transformation from frequency to spatial domain.

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

for u = 0 to M – 1 and v = 0 to N-1.

This paper presents an algorithm to insert large volume of messages/image data along with MD-5 key generated from authenticating message/image into the source image for image authentication and also to transmit secured message within the image. S-Tools perform authentication process by spreading the bit pattern of the file in spatial domain. The proposed technique implements the authentication process using hash function in frequency domain which has strong potentiality in authentication. Most of the works [1, 7] use bits of source image for embedding in time domain, but the proposed technique embeds bits of authenticating message/image in frequency domain. The scheme uses efficient insertion within a byte, which may conform to proper authentication and identification of the image as well as secret message transmission.

Section 2.0 deals with the proposed technique IAFDDFTT. Experimental results and comparisons are drawn in section 3.0. Conclusions are given in section 4.0 and references are drawn in section 5.0.

2.0 THE TECHNIQUE

The IAFDDFTT provides security by embedding authenticating message/image in frequency domain. Before embedding, the digital image is transformed from time domain to frequency domain representation using DFT technique as given in equation 1. In IAFDDFTT to generate transformed values using DFT a 2 x 2 submatrix has been taken from source image matrix as a window and authenticating message/image bits are embedded within the real part of the transformed data (excluding the 1st pixel in each 2 x 2 submatrix) of the window. One MD-5 key has been generated from authenticating message/image using well known message digest generation method. The size and content of authenticating message/image and MD-5 key is embedded to the transformed source image. After embedding, inverse DFT as given in equation 2 has been performed on the embedded image to transform the embedded image from frequency to spatial domain. The reverse operation is performed at the receiving end, and extracting bits of authenticating message/image and MD-5(R) key for authentication at destination.

Section 2.1 deals with insertion technique and that of section 2.2 with extraction technique. The schematic diagram of the whole process is given in Fig. 1.

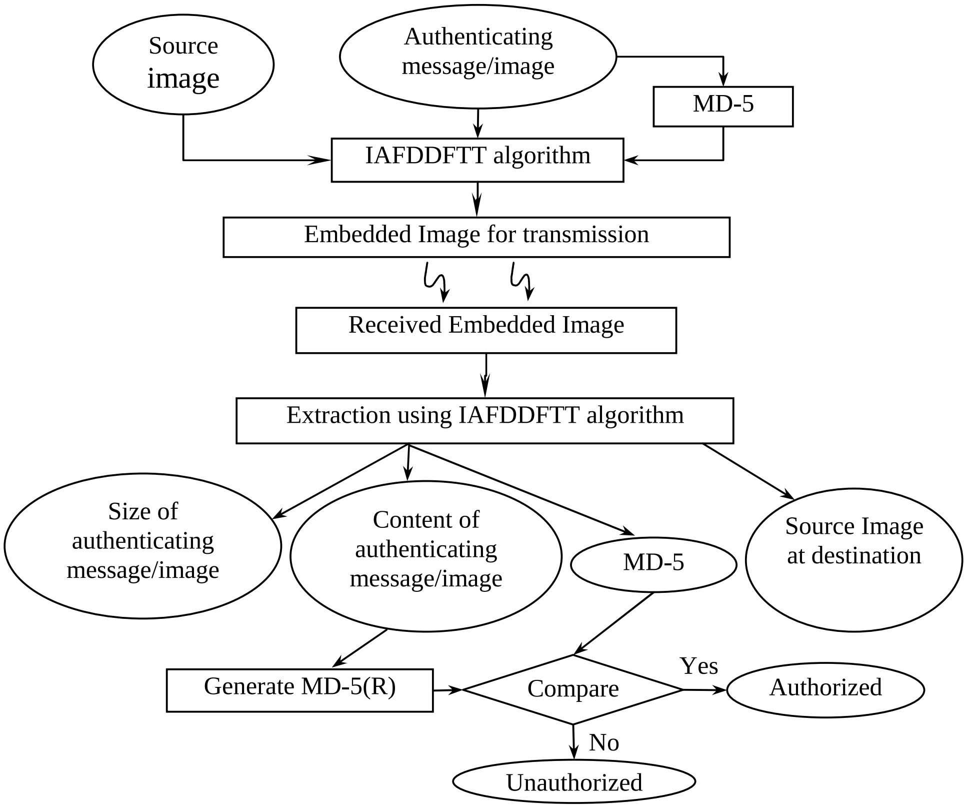
Source image
Authenticating message/image
MD-5
IAFDDFTT algorithm
Embedded Image for transmission
Received Embedded Image
Extraction using IAFDDFTT algorithm
Size of authenticating message/image
Content of authenticating message/image
MD-5
Source Image at destination
Generate MD-5(R)
Compare
Yes
Authorized
No
Unauthorized

Fig. 1: Schematic diagram of IAFDDFTT algorithm.

2.1 The Insertion Technique

Consider an m x n gray scale image. In the spatial domain each pixel may be represented as an 8 bits (i.e.1 byte) integer value. In IAFDDFTT the entire embedding is done in the frequency domain. Taking a window of size 2 x 2 from the source image and generating the DFT values for each pixel values using Discrete Fourier Transform technique. In the frequency domain there are two parts one is real part and another is imaginary part for each pixel values. For each real part of a pixel there are 8 positions where the bits may be inserted. These bit positions are selected using the formula k % s for the first and (k % s) + 1 for the second bit position within a byte, where k varies from 0 to 7 (k represents bit length (1 byte) of each character/pixel of authenticating message/image data) and s=2 …7 which is supplied by user to obtain the string of length s+1, and this s+1 bits from LSB of the byte to be taken as source stream where the bits are altered using IAFDDFTT. Insertion positions are selected and bits from the authenticating message/image are inserted for each byte. After inserting the bits from authenticating message/image, the 128 bits Message Digest (MD-5) is appended using the same rules. After embedding inverse DFT is performed to transform the image representation from frequency domain to spatial domain for transmission. The algorithm is given in section 2.1.1.

2.1.1 Insertion Algorithm

```
Input:   An M x N source image and authenticating message/image.
Output:  An authenticated image.
    1. Calculate size of authenticating message/image in bits (16 bit representation).
    2. Obtain 128 bits MD-5 key of authenticating message/image.
    3. Take a window of size 2 x 2 and apply DFT in sliding manner in row major order of the source image
       matrix till end of the image matrix.
    4. Embed in the real part excluding 1st real part in each window.
    5. Repeat for each bit of authenticating message/image size
         Find two positions in each real part of transformed image
         Insert the size of authenticating message/image.
    6. Repeat for each bit of authenticating message/image
           For each real part of transformed image
           Find the insertion positions
        Insert the authenticating bits.
    7. Repeat for each bit of 128 bits MD-5 key obtained in step 2
         For each real part of transformed image
            Find the insertion positions.
           Insert the key bits.
    8. Apply inverse DFT using identical window size.
    9. Stop.
```

2.2 Extraction Module

The authenticated image is received in spatial domain. DFT is applied using the same window of size 2 x 2 to transform the image representation from spatial domain to frequency domain. Extraction algorithm is applied on each real part of the embedded image in frequency domain. The size of the embedded authenticating message/image and the authenticating message/image is extracted along with the MD-5 key of the authenticating message/image. A new MD-5(R) key is also generated from the extracted authenticating information using the same message digest generation method and compares it with the extracted MD-5 key to verify it for authentication. A very close approximation of the original source image is also obtained by setting the bits at the insertion positions to 0. After extracting all authenticating information from the transformed embedded image inverse DFT is performed to generate original source image. The algorithm for extraction is given in section 2.2.1

2.2.1 Extraction Algorithm

```
Input:   Authenticated image.
Output:  The original image and an authenticating message/image.
    1. Take a window of size 2 x 2 and apply DFT in sliding manner in row major order of the source image
       matrix till end of the image matrix.
    2. Extract from the real part excluding 1st real part in each window.
    3. Repeat for each bit of authenticating message/image size
       Find the insertion positions
       Extract bits for size of authenticating message/image
    4. Repeat for each bit of authenticating message/image
           Find the insertion positions
         Extract data bits.
         If 8 bits are extracted, then
         Insert corresponding value into extracted data storage.
    5. Repeat for each bit of MD(5) key
  Find the insertion positions
         Extract key bits.
         If 128 bits are extracted, then
       Store the corresponding integer value in array1
    6. Generate the MD-5(R) key from extracted authenticating message/image and store it in array2.
```

```
7.  If array1 = array2, then
        Authorized
    Else
        Unauthorized
8.  Apply inverse DFT using same window.
9.  Stop.
```

3.0 DISCUSSION ON RESULTS AND COMPARISONS

In this section a comparative study has been made between IAFDDFTT and S-Tools in terms of visual interpretation, fidelity, histogram analysis, noise analysis, and standard deviation. Section 3.1 illustrates the histogram analysis. Section 3.2 deals with noise analysis and, standard deviation analysis is drawn in section 3.3. For comparison of visual fidelity the ‘Blue-sky’ (Fig. 2a) image of size 250 x 150 is taken as source image. The authenticating image ‘Earth’ (Fig. 2b) of size 80 x 80 has been embedded to ‘Blue-sky’ using IAFDDFTT algorithm and S-Tools algorithm separately (Fig. 2). Fig. 2a shows the source image ‘Blue-sky’ and Fig. 2c and 2d are the embedded images using IAFDDFTT and S-Tools algorithm respectively. Even though there is very little difference in fidelity observed between the source and the embedded image in S-Tools technique, no such difference is found in IAFDDFTT.

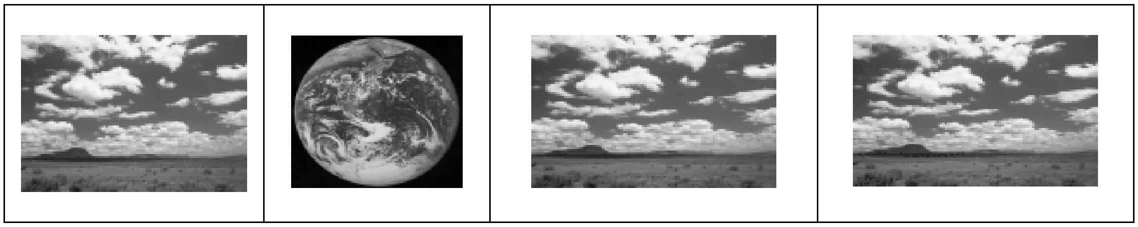

Fig. 2a. Blue-Sky Fig. 2b. Earth Fig. 2c. IAFDDFTT Fig. 2d. S-tools

Fig. 2 : Comparison of visual fidelity in embedding ‘Earth’ using IAFDDFTT and S-Tools

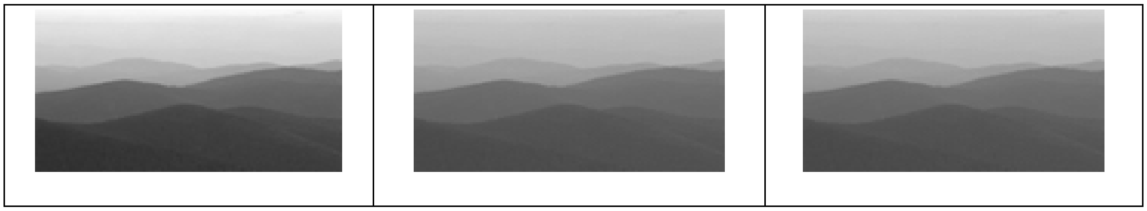

Fig. 3a. Hill Image Fig. 3b. IAFDDFTT Fig. 3c. S-tools

Fig. 3 : Comparison of visual fidelity in embedding ‘Earth’ using IAFDDFTT and S-Tools

Fig. 3 shows the comparison of fidelity in original image ‘Hill’ (Fig. 3a) and those obtained after embedding the image ‘Earth’ (Fig. 2b) using IAFDDFTT and S-Tools algorithm (Fig. 3b and Fig. 3c respectively) which exhibits very small change of fidelity in both implementations. From comparison of results it may be inferred that the fidelity of the embedded image is comparable with the source image. There may be cases where the fidelity in embedding using IAFDDFTT may obtain better results than the authentication technique S-Tools. IAFDDFTT may exceed the capability of S-Tools in terms of the size of the embedding message/image.

3.1 Histogram Analysis

Histogram analysis has been performed between source image 'Blue-sky' and for the image embedded using 'Earth' by applying IAFDDFTT and S-Tools. A noticeable difference is observed in frequency distribution table of pixel values in source image and embedded image using S-Tools algorithm. But very small differences are observed in frequency distribution table of pixel values in source image and embedded image using IAFDDFTT. Fig. 4 shows the visual effect in histogram in embedding source image 'Blue-sky' with IAFDDFTT and S-Tools. Fig. 4a is the histogram of the source image 'Blue-sky', Fig. 4b shows the histogram of the image embedded with 'Earth' image using IAFDDFTT and that of Fig. 4c is the histogram of the image embedded using 'Earth' image by applying S-Tools. It is clear that the IAFDDFTT histogram remains almost identical with the source image even after embedding the image with the 'Earth' image, where as in the case of embedding with S-Tools, there is a noticeable change in the histogram as compared to the histogram of the source image 'Blue-sky'.

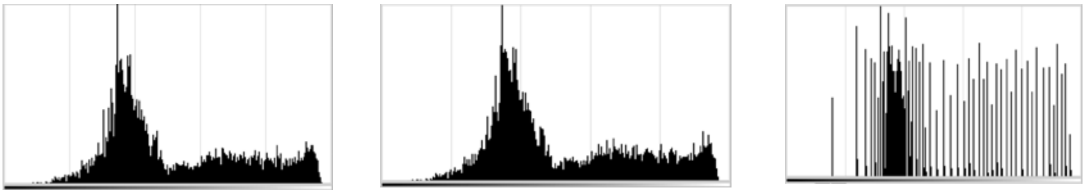

Fig. 4a : 'Blue-sky'   Fig. 4b : IAFDDFTT   Fig. 4c : S-Tools

Fig. 4: Histogram for image 'Blue-sky', embedded 'Earth' using IAFDDFTT and S-Tools

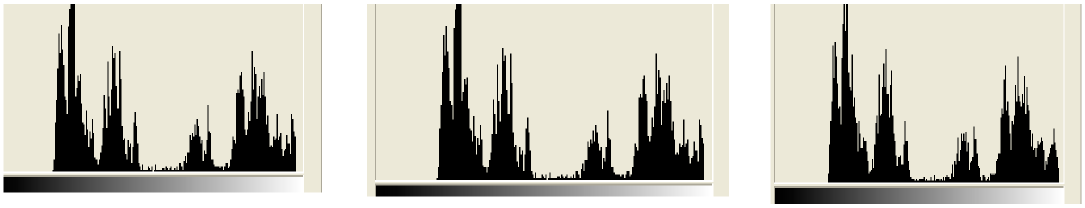

Fig. 5a : 'Hill'   Fig. 5b : IAFDDFTT   Fig. 5c : S-Tools

Fig. 5: Histogram for image 'Hill', embedded 'Earth' using IAFDDFTT and S-Tools

From these observations it may be inferred that the IAFDDFTT may obtain better performance in embedding. Fig. 5a, 5b and 5c shows the histogram of the source image 'Hill', its embedding with 'Earth' using IAFDDFTT and using S-Tools respectively. In this case of embedding the histograms are almost similar.

3.2 Noise Analysis

Noise analysis has also been performed for the embedded 'Blue-Sky' image with IAFDDFTT and S-Tools algorithm. Fig. 6 shows the results of computation of noise. Noise is computed by finding the average of 4 neighbor pixels in the 3x3 pixels (Fig. 7) around the pixel P_i as given in equation (3), where P_i^E and P_i^S are the pixel values of the pixel i in both the embedded image and source image respectively, and (m x n) is a number of pixels in the source image.

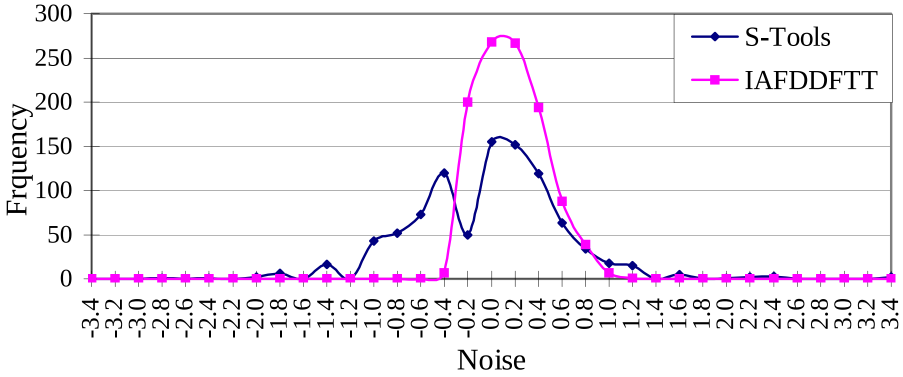

Fig. 6: Noise analysis of the image ‘Blue-Sky’ after embedding

$$Noise_{3\times 3} = \sum_{i=1}^{m\times n}\left(\left|\frac{p_i^E + \sum_{j=1}^{4} p_j^E}{5}\right| - \left|\frac{p_i^S + \sum_{j=1}^{4} p_j^S}{5}\right|\right) \quad \text{……..} \quad (3)$$

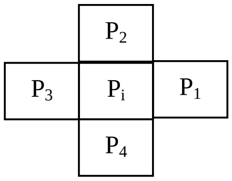

Fig.7: 4 neighbor pixels

It is very much clear from the picture that in the case of embedding with S-Tools frequencies of noise are spread over complete range where as for the IAFDDFTT a central tendency (zero noise intensity values) has been observed. In implementing IAFDDFTT the pixel frequency maximum between the noise ranges from –0.4 to 1 and beyond this region frequency of pixels are almost zero. But in the case of embedding S-Tools pixel frequencies are distributed over a wide range of noise ranges from –2 to 1.8. In the IAFDDFTT implementation a Gaussian nature of distribution has been observed whereas in the case of S-Tools implementation the distribution is not Gaussian in nature and multiple peaks observed in the frequency distribution curve. Therefore it may be concluded that noise integration is minimum for embedding with the IAFDDFTT and embedding/authenticating message/image with the IAFDDFTT may obtain good results.

3.3 Standard Deviation Analysis

Standard deviation has also been calculated for two images ‘Blue-Sky’ and ‘Hill’ embedded with ‘Earth’ and shown in Fig. 8. From Fig. 8, it is clear that the standard deviation is minimum for the source image ‘Blue-sky’, the value of standard deviation is slightly high when embedding with ‘Earth’ through IAFDDTT and the standard deviation is maximum for embedding using S-Tools. In the case of ‘Hill’ image no deviation has been observed in S-Tools algorithm as compared to the IAFDDFTT. This may lead to a conclusion that embedding/authenticating using IAFDDFTT may offer better authentication.

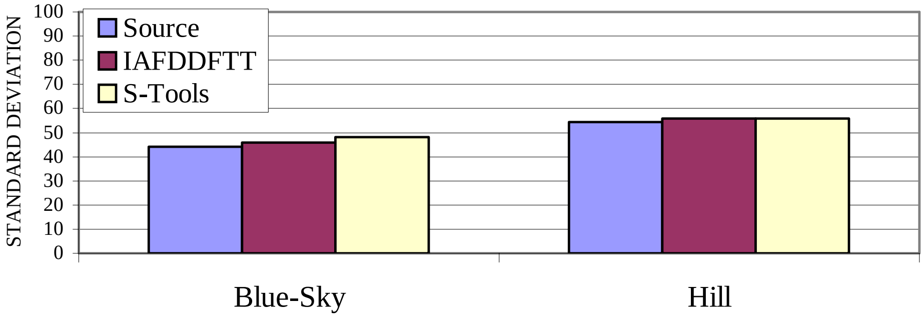

Fig. 8: Comparison results of standard deviation.

4.0 CONCLUSIONS

The proposed technique is an image authentication process in frequency domain to enhance the security compared to the existing algorithms which is done normally in spatial domain. The proposed algorithm provides additional two layers of security by means of transformation. The entire process is hidden under the transformations i.e. DFT and inverse DFT. For DFT 2 x 2 submatrix is selected for image authentication in frequency domain without changing visual property of the authenticated image. As a result the scheme may be more robust against brute force attack. However, the fidelity is persistent and degradation is very small which is based on the window selection. In IAFDDFTT distortion of image and change of fidelity (like sharpness, brightness etc) is negligible. From the analysis of histogram, noise, and standard deviation analysis, and comparison with S-Tools it may be inferred that the IAFDDFTT may obtain better embedded/authenticated image.

Acknowledgement

The authors express deep sense of gratitude to the Dept. of Computer Sc. and Engg. & Dept. of USIC, University of Kalyani, India, where the work has been carried out.

REFERENCES

[1] Amin, P., Lue, N. and Subbalakshmi, K., “Statistically secure digital image data hiding”, in *IEEE Multimedia Signal Processing MMSP05*, China, Oct. 2005, pp. 1-4.

[2] Chen, B. and Wornnel, G.W., “Quantization index modulation: A class of provably good methods for digital watermarking and information embedding”, in *IEEE Trans. On Info. Theory*, May 2001, Vol. 47, No. 4, pp. 1423-1443.

[3] Chandramouli, R. and Memon, N., “Analysis of LSB based image steganography techniques”, in *Proc. of ICIP*, Thissaloniki, Greece, 2001, pp. 1019-1022.

[4] Dumitrescu, S., Xiaolin, W. and Wang, Z., “Detection of LSB steganography via sample pair analysis”, In: *LNCS*, Springer-Verlag, New York, 2003, Vol. 2578, pp: 355-372.

[5] Moulin, P. and O’Sullivan, J.A., “Information-theoretic analysis of information hiding”, in *IEEE Trans. on Info. Theory*, March 2003, Vol. 49, No. 3, pp. 563-593.

[6] Moulin, P. and Mihcak, M. K., “A framework for evaluating the data-hiding capacity of image sources”, in *IEEE Transactions on Image Processing*, Urbana, Illinois, Sept. 2002, Vol. 11, pp. 1029-1042.

[7] Nameer, N. EL-Emam, “Hiding a large amount of data with high security using steganography algorithm”, *Journal of Computer Science ISSN 1549-3636*, Vol. 3, No. 4, 2007, pp: 223-232.

[8] Pavan, S., Gangadharpalli, S. and Sridhar, V.,"Multivariate entropy detector based hybrid image registration algorithm", in *IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, Philadelphia, Pennsylvania, USA, March 2005, pp: 18-23.

[9] Pang, H.H., Tan, K.L. and Zhou, X., "Steganographic schemes for file system and b-tree", in *IEEE Trans. On Knowledge and Data Engineering*, Singapore, June 2004, Vol. 16: pp 701-713.

[10] Rechberger, C., Rijman V. and Sklavos N., "The NIST cryptographic Workshop on Hash Functions", in *IEEE Security & Privacy*, Austria, Jan/Feb 2006, Vol. 4, pp. 54-56.

[11] S-Tools- http://digitalforensics.Champlain.Edu/download/s-tools4.zip. (*accessed in August 2007*).

BIOGRAPHY

Joytsna Kumar Mandal, M.Tech.(Computer Science, University of Calcutta), Ph.D.(Engg., Jadavpur University), Professor in Computer Science and Engineering, University of Kalyani, India. Life Member of Computer Society of India since 1992. 20 years of teaching and research experiences. 3 Scholars awarded Ph.D.; 3 Scholars submitted Ph.D. and 6 scholars are pursuing Ph.D. Total number. of publications 94.

Nabin Ghoshal, M.Tech.(Computer Science & Engineering, University of Kalyani), Scientific Officer, University of Kalyani, India. 7 years teaching experiences. Pursuing research for the degree of Ph.D. Total number of publications are 5.