Int. J. Communications, Network and System Sciences, 2009, 5, 363-370
doi:10.4236/ijcns.2009.25040 Published Online August 2009 (http://www.SciRP.org/journal/ijcns/).

Authentication and Secret Message Transmission Technique Using Discrete Fourier Transformation

Debnath BHATTACHARYYA[1], Jhuma DUTTA[1], Poulami DAS[1], Samir Kumar BANDYOPADHYAY[2], Tai-hoon KIM[3]
[1]*Computer Science and Engineering Department, Heritage Institute of Technology, Kolkata, India*
[2]*Department of Computer Science and Engineering, University of Calcutta, Kolkata, India*
[3]*Hannam University, Daejeon, Korea*
Email: {*debnathb, jhumadutta*81, *dasp*88}*@gmail.com, skb*1*@vsnl.com, taihoonn@empal.com*
Received April 2, 2009; *revised May* 9, 2009; *accepted June* 28, 2009

ABSTRACT

In this paper a novel technique, Authentication and Secret Message Transmission using Discrete Fourier Transformation (ASMTDFT) has been proposed to authenticate an image and also some secret message or image can be transmitted 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 and 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.

Keywords: Data Hiding, Authentication, Frequency Domain, Discrete Fourier Transformation (DFT), Inverse Discrete Fourier Transform (IDFT), S-Tools

1. Introduction

The most popular technique for image authentication or steganographic technique is embedding message or image within the source image, generally termed data hiding. It 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. Although it changes source, 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. 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 in 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 formula of DFT for a function f (x, y) of size M x N is given in Equation 1 for frequency domain transformation.

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

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

$$F(u,v)=\mathrm{Re}\,F(u,v)-\mathrm{Im}\,F(u,v)$$
$$\text{for } u=0,1,\ldots M-1 \quad v=0,1,\ldots N-1 \tag{2}$$

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

$$\mathrm{Re}\,F(u,v)=\frac{1}{\sqrt{MN}}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)\cos\left(\frac{2\pi ux}{M}\right) \tag{3}$$
$$\text{for } u=0,1,\ldots M-1 \quad v=0,1,\ldots N-1$$

$$\mathrm{Im}\,F(u,v)=\frac{1}{\sqrt{MN}}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)\sin\left(\frac{2\pi vy}{N}\right) \tag{4}$$
$$\text{for } u=0,1,\ldots M-1 \quad v=0,1,\ldots N-1$$

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

$$f(x,y)=\frac{1}{\sqrt{MN}}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}F(u,v)\cos\left(\frac{2\pi ux}{M}\right)+F(u,v)\,j\sin\left(\frac{2\pi vy}{N}\right)$$
$$\text{for } x=0,1,\ldots M-1 \quad y=0,1,\ldots N-1 \tag{5}$$

Now consider the real part of the transformed image and embed authenticating message or image bits at the LSB of each component (pixel) of the transformed image. 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.

2. Earlier Works

N. Nameer and E. Eman in April 2007, implemented an algorithm based on hiding a large amount of data (image, audio, text) file into color BMP image. They 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].

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

R. Chandramouli and 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, X. L. Wu and Z. 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].

B. Chen and G. 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].

P. Moulin and J. A. O'Sullivan 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].

P. Moulin and M. K. 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].

C. Y. Lin and S. F. 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].

S. Pavan, G. Sridhar, and V. Sridhar 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, and 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 Steg FD volume [10].

3. Our Work

The presented work is based on information and image protection against unauthorized access in frequency domain. The ASMTDFT 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 scheme is given in Figure 1 and Figure 2 respectively.

3.1. Insertion Technique

Using the proposed scheme embedding is done completely in the frequency domain. DFT is applied on window of size 2 x 2 in sliding window manner to convert from spatial domain to frequency domain. Each pixel (8 bits) in spatial domain is transformed into two parts one is real part and another one is imaginary part. The authenticating bits are inserted at the LSB of the real part (excluding 1st pixel). The process is repeated for the whole image matrix in the same manner. After embedding inverse DFT is performed to convert from frequency domain to spatial domain. The algorithm for insertion is given in Subsection 3.1.1

3.1.1. 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 Discrete Fourier Transformation.

6) Stop.

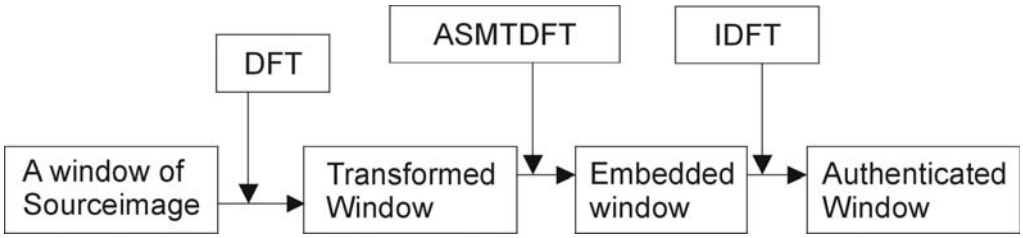


Figure 1. Encoding scheme using ASMTDFT.

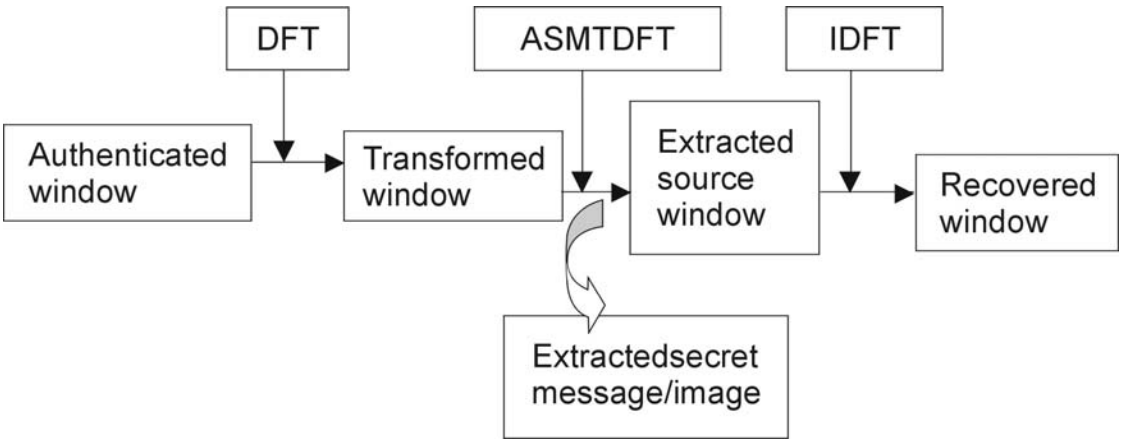


Figure 2. Decoding scheme using ASMTDFT.

3.2. Extraction Technique

During decoding the embedded image has been taken as input in spatial domain. To convert form spatial domain to frequency domain DFT is applied using the same window of size 2 x 2. Apply the extraction algorithm to extract the authenticating message or image from the transformed image. The process is repeated for the whole embedded image matrix in the same manner. Inverse DFT is performed to transform from frequency domain to spatial domain to generate original source image. The algorithm for extraction is given in Section 3.2.1

3.2.1. 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 Discrete Fourier Transformation.
6) Stop.

4. Results and Comparisons

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. Subsection 4.1 illustrates Chi-Square test. Subsection 4.2 deals with histogram analysis.

Figure 3(a) shows source image 'Hill' and Figure 3(b) shows the authenticating image 'Lotus' and Figure 3(c) and Figure 3(d) are embedded image using proposed algorithm and S-Tools respectively. 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.

Figure 4(a) to Figure 4(d) indicate the comparison of visual changes for another source image 'Rasmancha' (Figure 4(a)) embedding with the same Lotus image (Figure 4(b)). The results are embedded image using proposed algorithm (Figure 4(c)) and S-Tools (Figure 4(d)). 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 ASMTDFT.

(a). Hill. **(b). Lotus.** **(c). ASMTDFT.** **(d). S-tools.**

Figure 3. Comparison of visual fidelity in embedding 'Lotus' using ASMTDFT and S-Tools.

(a). Rashmancha. **(b). Lotus.** **(c). ASMTDFT.** **(d). S-tools.**

Figure 4. Comparison of visual fidelity in embedding 'Lotus' using ASMTDFT and S-Tools.

Table 1. Comparison of Chi-Square values in ASMTDFT.

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

(a). Authenticated hill. **(b). Extracted lotus.** **(c). Extracted hill.**

Figure 5. Comparison of visual fidelity in extracting 'Lotus' and source image 'Hill' using ASMTDFT.

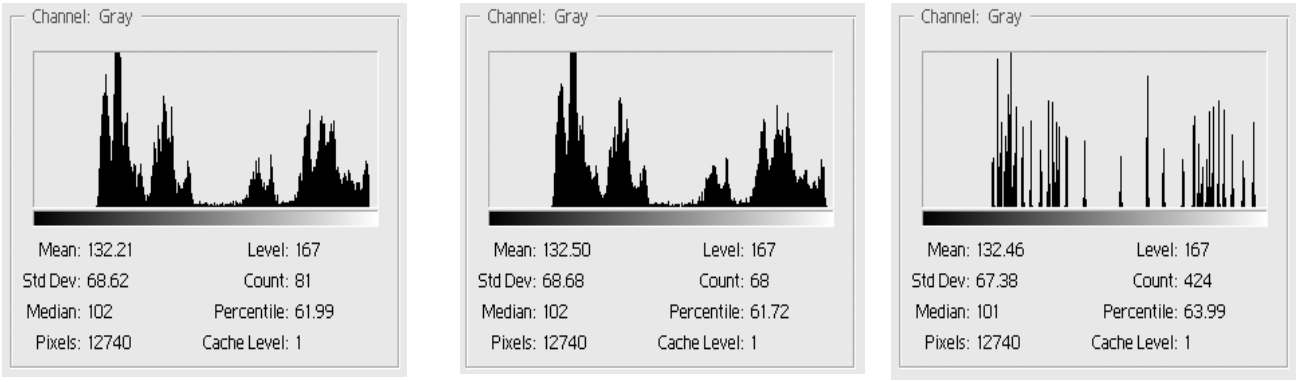
Using ASMTDFT we are also able to separate the Source image and the authenticating image from the authenticated image. Figure 5(a) to Figure 5(c) show this result. Figure 5(a) is the Authenticated Hill image. Now using extraction procedure of ASMTDFT Figure 5(b) is the extracted Lotus image and Figure 5(c) is the Extracted Hill (Source) image. This extraction is not possible by s-tools.

4.1. 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.

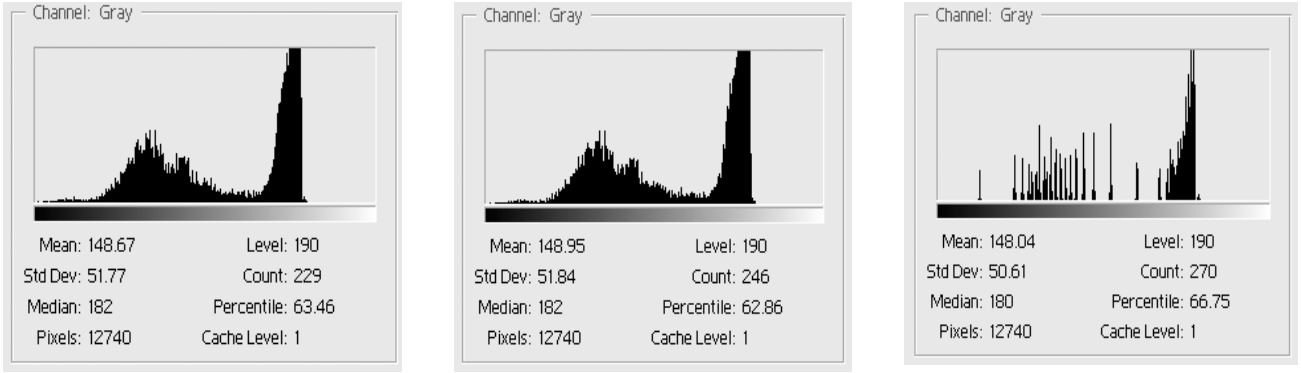
4.2. Histogram Analysis

Histogram analyses have been performed between source image 'Hill' and for the embedded image using 'Lotus' by applying proposed technique and S-Tools and also for the 'Rashmancha' image. 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. Figure 6 shows the visual effect of histograms in embedding source image 'Hill' with proposed technique and S-Tools. The histogram of the source image 'Hill', the histogram of the embedded image by 'Lotus' image using proposed technique and the histogram of the image embedded using 'Lotus' image by applying S-Tools are shown in Figure 6. 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



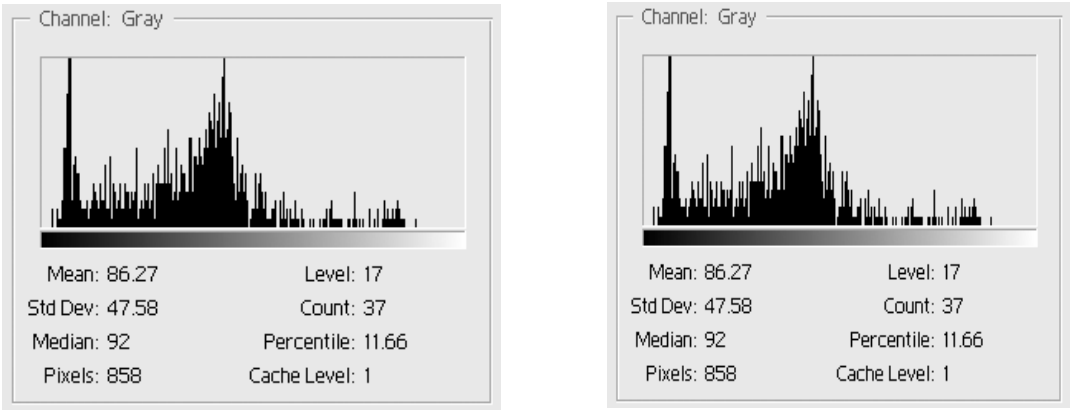
(a). Hill. **(b). ASMTDFT.** **(c). S-Tools.**

Figure 6. Histogram for source image 'Hill', embedded image using.



(a). Rashmancha. **(b). ASMTDFT.** **(c). S-Tools.**

Figure 7. Histogram for source image 'Rashmancha', embedded image using ASMTDFT and S-Tools.



(a). Lotus. **(b). Extracted Lotus.**

Figure 8. Histogram for authenticating image 'Lotus', extracted image 'Lotus' using ASMTDFT.

Table 2. Histogram analysis.

Images	Level	Count	Mean	Std. Dev
Source Hill image	167	81	132.21	68.62
Authenticated Hill image by Lotus using ASMTDFT	167	68	132.50	68.68
Authenticated Hill image by Lotus using S-Tools	167	424	132.46	67.38
Source Rashmancha image	190	229	148.67	51.77
Authenticated Rashmancha image by Lotus using ASMTDFT	190	246	148.95	51.84
Authenticated Rashmancha image by Lotus using S-Tools	190	270	148.04	50.61
Lotus Image	17	37	86.27	47.58
Extracted Lotus Image	17	37	86.27	47.58

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 analyses have also been done for another source image 'Rashmancha', which is depicted in Figure 7(a)−7(c). Figures 8(a), 8(b) show the histogram of the embedding image 'Lotus' and the histogram of the extracted image 'Lotus'. From the histograms we see that there are no differences. So we can conclude that the proposed algorithm gives a very good result for extraction. Table 2 gives a clear idea of the histograms of different images in a tabular form. Here we have considered a particular gray level value for images and check the variances in terms of total no. pixels, Mean, Standard deviation. The comparisons have been done between the source image and authenticated image both for ASMTDFT & S-Tools, and also for the authenticating image and the extracted image which we have got using ASMTDFT.

5. Conclusions

In this paper the proposed technique implemented here for image authentication and secret message transmission. The algorithm used here is the bit level message or image insertion and extraction in the frequency domain. Using ASMTDFT 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 results of Chi-Square test and histogram analysis and comparison with S-Tools the proposed technique may obtain better result.

6. Acknowledgements

This work was supported by the Security Engineering Research Center, granted by the Korea Ministry of Knowledge Economy. And this work has successfully completed by the active support of Prof. Tai-hoon Kim, Hannam University, Republic of Korea and Prof. Samir Kumar Bandyopadhyay, University of Calcutta, India.

7. References

[1] N. Nameer and E. Eman, "Hiding a large amount of data with high security using steganography algorithm," Journal of Computer Sciences, pp. 223−232, April 2007.

[2] P. K. Amin, N. Liu, and K. P. Subbalakshmi, "Statistically secure digital image data hiding," Multimedia Signal Processing, IEEE 7th Workshop, Shanghai, pp. 1−4, October 2005.

[3] R. Chandramouli and N. Memon, "Analysis of LSB based image steganography techniques," International Conference on Image Processing, Thessaloniki, Greece, pp. 1019−1022, 2001.

[4] S. Dumitrescu, X. L. Wu, and Z. Wang, "Detection of LSB steganography via sample pair analysis," IEEE Transactions on Signal Processing, Vol. 51, No. 7, pp. 1995−2007, July 2003.

[5] B. Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," IEEE Transaction on Information Theory, Vol. 47, pp. 1423–1443, 2001.

[6] P. Moulin and J. A. O'Sullivan, "Information-theoretic analysis of information hiding," IEEE International Symposium on Information Theory, Sorrento, Italy, pp. 19, June 2000.

[7] P. Moulin and M. K. Mıhcak, "A framework for evaluating the data-hiding capacity of image sources," IEEE Transaction on Image Processing, Vol. 11, pp. 1029–1042, September 2002.

[8] C. Y. Lin and S. F. Chang, "A robust image authentication method surviving JPEG lossy compression," SPIE, pp. 296–307, 1998.

[9] S. Pavan, G. Sridhar, and V. Sridhar, "Multivariate entropy detector based hybrid image registration," IEEE ICASSP, Vol. 2, pp. 873–876, March 18–23, 2005.

[10] H. H. Pang, K. L. Tan, and X. Zhou, "Steganographic schemes for file system and B-tree," IEEE Transaction on Knowledge and Data Engineering, Vol. 16, No. 6, pp. 701–713, June 2004.

[11] http://www.spychecker.com/download/download_stools.html, visited as on March 28, 2009

