International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Improved Steganographic Method for Hiding Secure Data Based on Efficient Keystream Generator

Dr. Ismail K. Ali[1], Salah T. Allawi[2], May M. Abbas[3]

[1]Computer Science Dept. Alma'mon University College

[2]Computer Science Dept. College of Science, AL-Mustansiriyah University

[3]Ministry of Higher Education and Scientific Research, Legal and Administrative Directorate

Abstract: ***Secure transmissions of information become a critical issue in the digital world with the growing importance of the internet. Cryptography and steganography helps in providing this much-needed data confidentiality. This research presented an improved steganographic method for hiding secure data. The proposed system is incorporating of text encryption, steganography and data compression based on an efficient keystream generator. In the first step, the secret data has been encrypted using stream cipher. This cipher text is embedded into BMP image format cover using pseudorandom keystream generator as a private key. Then the image file transmitted is compressed by using discrete cosine transform to obtain the JPEG image format. The experimental results show that the proposed method is provide improved robustness, security due to multi-level security and the use of the efficient keystream generator increases the complexity of the encryption process.***

Keywords: Cryptography, Image Steganography, Data Compression, Keystream Generator

1. Introduction

Information security became an enormous important issue when the Internet provides the basic channel of communication between millions of people, and began to be used increasingly as a tool for the transfer of information. A cryptography algorithm is a mathematical function used to encrypt a number, word or phrase called the plaintext. Cryptography algorithms are classified into two groups one is symmetric key algorithms Fig.1 and another is asymmetric key algorithms, these algorithms work in combination with keys. The security of the encrypted plaintext is entirely dependent on two main factors: the strength of the cryptography algorithm and secrecy of the keys [1].

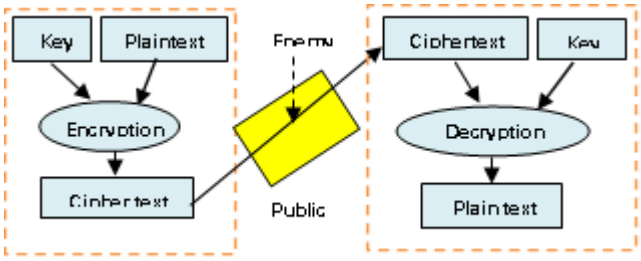

Figure 1: The basic symmetric key cryptography algorithm

Steganography is a process that hides the secret information or message in a multimedia carrier such as, image, audio, video or text without raising any perception of alteration to its data. The embedded message and the original cover object produces a stego-object. Basic hiding data may require a key called a stego-key, which is additional secret dat. Fig.2 illustrates the generic embedding technique takes a cover image and a secret data as inputs to produce a stego-image as output. The recipient receives the stego-image through the channels of communication,and then carry out the extraction process to retrieve the secret data from the stego-image [2].

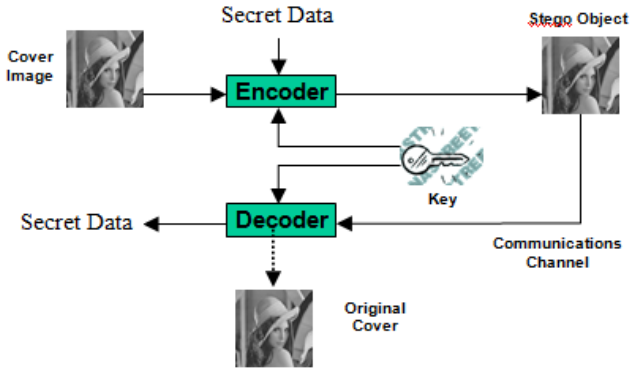

Figure 2: The generic model of image steganography

Cryptography and steganography are closely related. Cryptography converts the plaintext into ciphertext so it cannot be readable, while steganography embed the data so there is no knowledge of the existence of it. In cryptography, the comparison is made between forms of plaintext and forms of ciphertext. With steganography a comparison is made between the cover-media and the stego-media, and possible forms of the data. Ciphertext is the result of cryptography, while stego-media is the result of steganography. The secret data in steganography may or may not be encrypted. Using cryptography and steganography simultaneously provides the best solution as in this case even if the data is detected encryption still keep the confidentiality [3].

The goal of this paper to improve a new system image communication scheme, which uses digital image compressions along with steganography and cryptography for improved security. The rest of the paper is organized as follows: Section 2 presents an overview of the stream cipher.

The underlying principles of image steganography and image compression techniques are presented in sections 3 and 4 respectively. Section 5 describes the system proposed. Experimental results of computational tests to evaluate the performance of the proposed system are reported in section 6.

2. Stream Cipher

In modern occasions technologies, there exists a need for encrypting data streams with high speed, e.g., for satellites, mobile communications or video streams. The main advantages of stream cipher are avoiding the error propagation so in situation of error transmission are highly probable. The stream cipher is easy implementation in hardware and can be up to 5 times faster than Advance Encryption Standard (AES). Keystream generators are used in modern cryptography to produces an output stream of arbitrary length, named the keystream, after it has been initialized with a secret value, called the key Fig.3. The keystream is then combined with the data stream to encrypt it. Many designs of stream ciphers are based on Linear Feedback Shift Registers (LFSRs) and to destroy their inherent linearity they commonly combined by nonlinear memoryless function, which can be constructed in such a way that the output stream has good random statistical, periodical properties and which can be efficiently implemented in hardware[4].

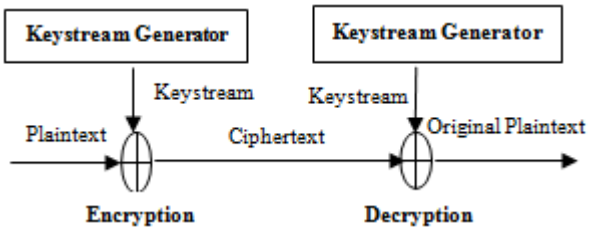

Figure 3: The basic model of stream cipher

3. Image Steganography

Image steganography is a technique that investment the weakness of the Human Visual System (HVS), which cannot detect the variation in luminance of color vectors expressed in terms of 0's and 1's [5],[6]. This technique can be divided into two group's i.e. transform domain and spatial domain techniques. In transform domain technique is a complex way of hiding data in an image where the secret data is embedded in the image after the images are transformed. Transformation of cover image is performed by tweaking the coefficients and inverts the transformation. There are various transformation techniques such as Discrete Cosine Transformation (DCT) [7], Discrete Fourier Transformation (DFT) [8], and Discrete Wavelet Transformation (DWT) [9].

In spatial domain technique, the secret data is embedded in the intensity of the pixels directly in the image. There are various techniques of the spatial domain such as Least Significant Bit (LSB) matching, Least Significant Bit (LSB) replacement, matrix embedding, etc [3].

4. Image Compression Techniques

Image compression is an application of data compression that reduces the size of files. The aim of image compression is to decreasing the redundancy of bits that are not required to represent data and to store or reduce the transmission time. The image compression techniques are widely divided into two type's i.e. lossy and lossless compression. In lossless compression, the original image can be recreated exactly from compressed image, i.e. no data are lost. Only a few applications with strict requirements are used in lossless compression such as in military or medical imaging applications. Lossy compression provide much higher compression ratios than lossless techniques. With lossy compression, the original image cannot be retrieval exactly from compressed image i.e. allows a loss in the actual image data, but it is reasonably close to it. Lossy compression useful for broadcast television, video-conferencing, and facsimile transmission, etc. [10].

5. Proposed System

Instead of using cryptography and steganography directly in this paper, a method introduced to hide a secret message combining cryptography and steganography using a random way to confirm the strength of the method and saves information from the risks of discovery. Fig.4 illustrated the general architecture of the proposed system processes. The entire process is divided into two main parts, which are embedding part and extracting part.

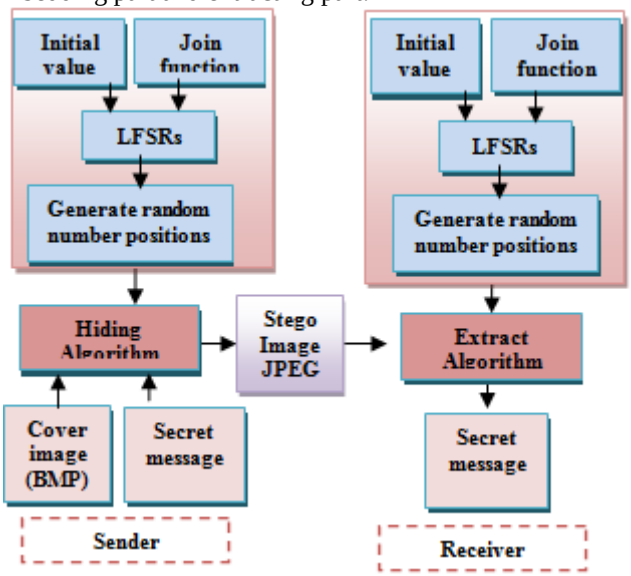

Figure 4: proposed steganographic system

5.1 Embedding Part

This part includes all the actions that implemented to embed and keep the secret message within the cover image object. The sender must use some of processes to encrypt secret data, embeds the bit stream of plaintext data into the image and then compresses the image. Moreover, the secret key is the first situation of the bit stream within the image. The sender and receiver only know this key. The sending process includes of the following phases:

5.1.1 Encryption phase

In the encryption phase, it is necessary to choose what type of encryption method adopted and which is best suitable. Several encryption techniques used to encrypt the data. In stream cipher, the encryption in carried as bit-by-bit format and the raw plaintext data is XOR-ed with the randomly generated key by the pseudorandom generator. The generated key used at both the sender and the receiver, thus, the same key used to decrypt the data at the receiver end, and hence the name is symmetric key encryption. Fig.5 shows the design of pseudorandom generator has been proposed by using on LFSRs with memoryless bits in order to make this steganography system high secure and more flexibility.

These LFSRs used for three purposes: the encryption process, the hiding processes and the extraction phase. The system has prompted user to enter the secret message and then convert it into binary bits. Within the system, user must enter the private key to initialize the registers, and the system will proceed to next step. The output of the LFSR used to encrypt the secret message and generate group of random numbers represent the address of block, which used to embed encrypted secret message bits. By using these LFSRs for embedding part, now the secret message data secured because placed in random places. Even if the cryptanalyst manage to discover that the image contain a secret message, it must be difficult for them to get the message because the already LFSRs scattered the data bits while doing the jumps. In the extraction phase of secret message, these LFSRs being operated again to generate a random numbers in order to get back the ciphertext from the cover image.

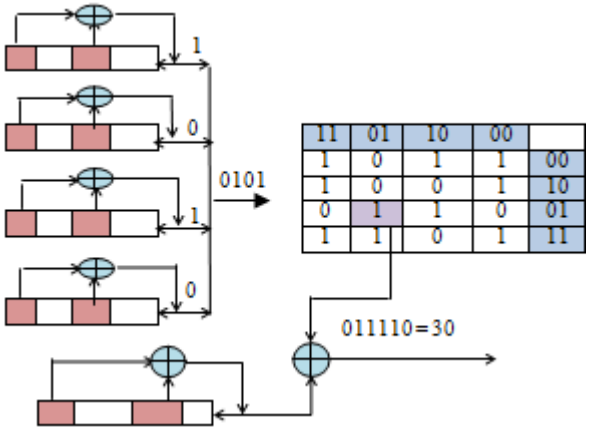

Figure 5: Proposed key stream generator

5.1.2 Embedding phase

Because of large number of redundant bits that are appropriate for data transmission on the Internet, images are the widespread cover object for steganography. The embedding process is the mainly distinguish part of the steganographic methods. In fact, it determines which pixels of the image should be altered and in what order they will be changed with the secret message. The outline of proposed embedding phase is show in Fig.6. The main algorithm for the embedded phase can be listed as follow:

1. Select a suitable cover image (BMP format file) with size (m * n).
2. Open the cover image and read the data in matrix.
3. Input the secret plaintext message that to be hide in the cover image.
4. Generate key K from random keystream generator to encrypted secret message
5. Generate group of random numbers represent address of image blocks.
6. Apply XORed operator on secret plaintext to obtain the ciphertext.
7. Converting a color image mode from (RGB) to (YCbCr) format.
8. Divided each component of the three components (YCbCr) to blocks (8 * 8) pixels.
9. Apply the (DCT) process on each block.
10. Embed encrypted secret message bits in the DC coefficient
11. Apply the quantized process on each block.
12. Apply other process to get stego-image type (JPEG) carries is sent to the receiver.

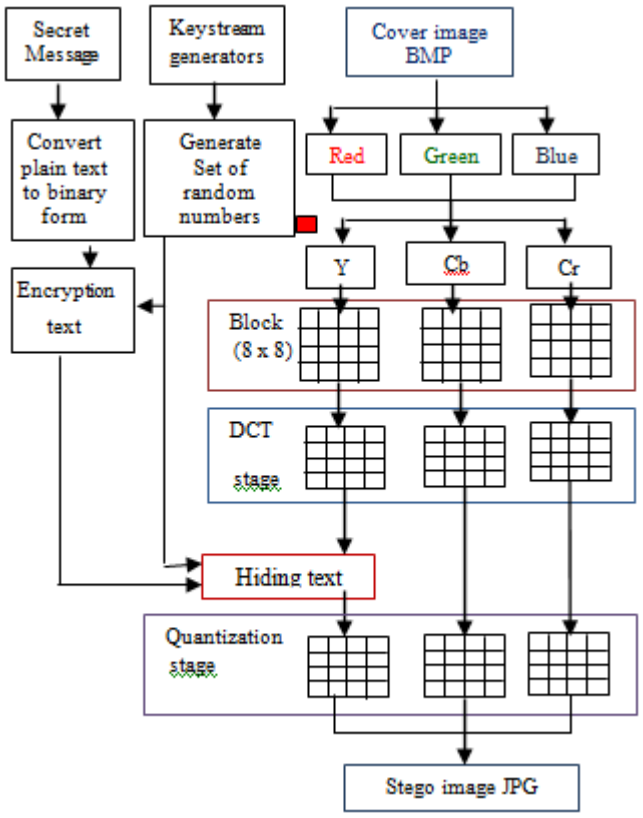

Figure 6: The outline of proposed embedding phase

To compress the BMP cover image format into JPEG image format, the RGB color representations is first converted to a YCbCr representation space and divide each color plane into (8 * 8)blocks of pixels. The next step transforms a signal from an image representation format into a frequency representation by transforming the pixel blocks into DCT coefficients. After compute, DCT on each block obtaining 64 coefficients, first coefficient called DC and other 63 coefficients called AC. The final step is the quantization stage.

The embed process occurs after the DCT process where they are hiding one bit in each block, specifically in the value of the DC coefficient. This value converted to odd or even number depended on the secret message bit, where when the secret bit is equal zero the DC value is even and when the secret bit equal one the DC value is odd. The process of changing the value of DC is done through adds or subtracts one from a certain value of coefficients of each block as

needed. The embedded mechanism of one bit in each block proceeds as follow:

```
QTC1 = round (DC / 16)
  If (QTC1 (even value) and MSB =0) ) or (QTC1 (odd) and
     MSB = 1) )  then
      No is change on the block coefficients
  Else
    If (QTC1 (odd value) and MSB = 0) )
        QTC2 = DC / 16
        DF=QTC2 – QTC1
        AS=0.5 – DF
         NCF=(abs (AS))/0.0078
        If( AS>0)then
             Add one to value of NCF coefficients in the
             block before applying DCT
        If( AS<0)then
            Sub one from value of NCF coefficients in the
           block before applying DCT
        Apply DCT
     Endif
```

Where:
DC is the first coefficient in each block.
QTC1 is the result of dive DC on 16 with round.
QTC21 is the result of dive DC on 16 without round.
DF is the different between QTC1 with QTC2.
AS is the value that must be add or sub to/from DC coefficient.
NCF is the number of pixels must be change (add or sub one to each value).

5.2 Extracting Part

The other hand of the communication channel, the receiver carried out the reverse process. He should be able to realize the secret text within the stego-object. Extracting phase is the process of getting the embedded secret data message out of the stego-image again. The stego image is converted into binary array of 0's and 1's and then the color values of each pixel are studied and the corresponding be extracted. Here as the data is received they can be separately extracted independently using either the encryption key, which is pseudorandom generated to extract the decrypted data. At this time the same pseudo random generated must be provided by the receiver in order to extract the cover image. The resultant image is then decompressed while maintaining the quality of the image. Then the data-hiding key is applied to the recovered the real cover image to extract the secret plaintext. The keys can be used alternatively to recover any one of the data also. Thus, offer better flexibility.

6. Experimental Results

In the proposed system, the secret plaintext message is encrypted to obtain the ciphertext permuted according to the pseudorandom sequence generated through the stream cipher system, and then the ciphertext is embedded within the BMP image file format. The generated stego-image is sending over the communication channels to the receiver. When the receiver receives the stego-image, the ciphertext is extracted from it by reversing the processes that was used to embed it in the first position. The ciphertext is decrypted using M the stream cipher system to retrieve the original plaintext.

In this paper, the results of distortion between two different images were evaluated both quantitatively and qualitatively. Two metrics have been used, to quantify the distortion in the image of sizes (m * n) is defined by Mean Square error (MSE) as equation 1:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left[(f(x,y)-g(x,y)\right]^2 \qquad (1)$$

In addition, to quality the statistical difference between the cover image and stego-image of sizes (m * n) is defined by Peak Signal to Noise Ratio (PSNR) as equation 2:

$$PSNR = 10 \times \log (255^2 / MSE) \qquad (2)$$

Two various BMP images format are used as cover image to implement the proposed system Lena and Baboon with sizes of (352 * 288) and (264 * 280) pixels respectively as shown in Fig.7. Moreover, arbitrary texts with different lengths bits for testing have been used in the embedding phase as secret messages.

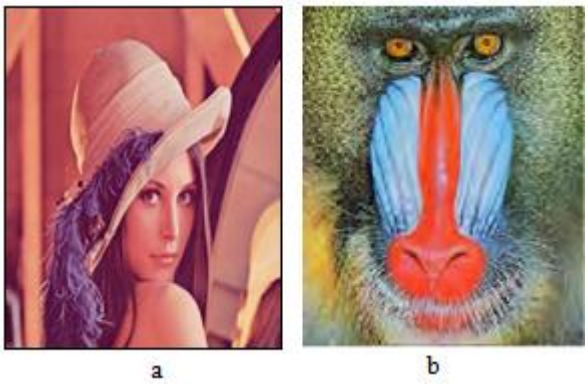

Figure 7: Cover image (a) Lena (b) Baboon

Table 1 shows the results of the proposed method to embed different size of sample picture of Lena and is graphically represented in Figure 8.

Table 1: MSE and PSNR values for the Lena test image

Text length (Bits)	PSNR			MSE		
	Red	Green	Blue	Red	Green	Blue
1038	32.74	32.87	31.58	5.88	5.78	6.71
1362	32.71	32.84	31.55	5.89	5.81	6.74
1500	32.71	32.83	31.54	5.9	5.81	6.75

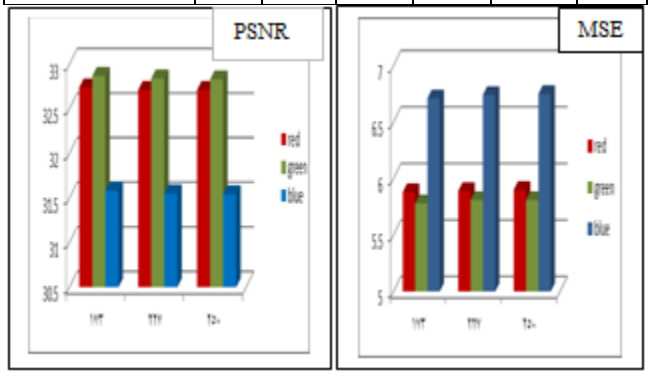

Figure 8: Comparison PSNR and MSE between the cover image and stego image using Lena test image

An addition Table 2 shows the results of the proposed method to embed different size of sample picture of Baboon and is graphically represented in Fig.9.

Table 2: MSE and PSNR values for the Baboon test image

Text length (Bits)	PSNR			MSE		
	Red	Green	Blue	Red	Green	Blue
954	28.89	29.24	28.67	9.16	8.79	9.39
1038	28.88	29.24	28.66	9.16	8.79	9.4
1080	24.88	29.23	28.66	9.16	8.8	9.4

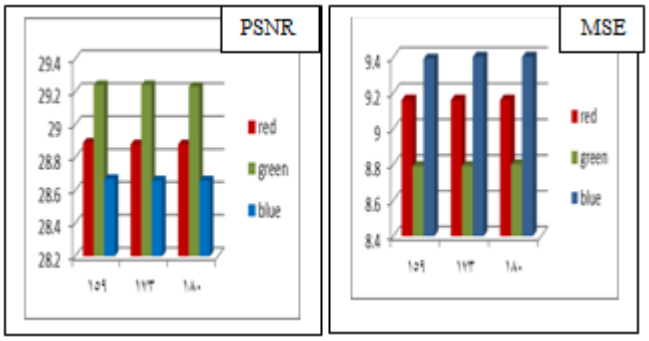

Figure 9: Comparison PSNR and MSE between the cover image and stego image using Baboon test image

The criterion MSE is to quantify the distortion in the image of different sizes and the PSNR determines the stego-image quality and specifies how much the result is similar to the cover-image. A large value measurement for the PSNR quality indicates a lesser degree of distortion for the result image. The values of results indicate that the improvement method produces the MSE and PSNR values in all tested cases. Steganography exploits human perception, as human mind are not trained to look inside an image that has data hidden inside them. In the experiments testing, it is observed that HVS cannot distinguish between the cover-image and stego-image. Fig.10 shows the stego-images obtained using the proposed method. As the figure show, distortions resulted from embedding are invisible to human vision.

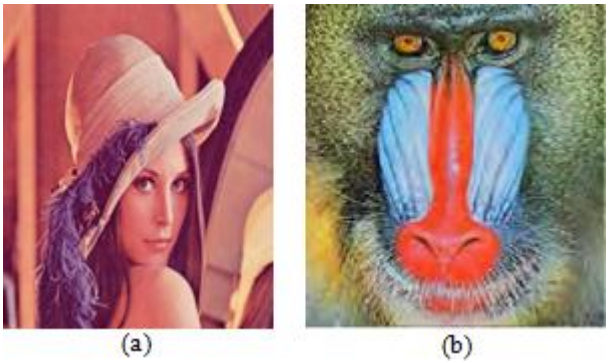

Figure 10: Stego images (a) Lena (b) Baboon

7. Conclusions

This paper concentrated to propose an improved seganographic method has its place in secured of data communication. The proposed system provides three layer of security by incorporating of text encryption, steganography and data compression based on efficient keystream generator. As the results of this work, the effect of the paper is to create a combination of stream cipher based on LFSRs into steganography and compression increased the complexity of the method in terms of security layer and thus has increased its authenticity safely the secret message to the destination place. In order for the intruders to retrieve the message from image, they must generate the same positions of jumps as generated by the LFSRs and even they got it, it still hard for them to decrypt the ciphertext into plaintext itself without knowing the exact key that are used to initialize the registers. In the images of the kind BMP format, data type that can be embedded is large and the image is not distorted because of the ability of this kind of images for carrying lots of data without observe. From the implementation of the proposed system is very rapid in performing extraction process.

References

[1] Gary C. Kessler "An Overview on Cryptography", 21 January 2015.
[2] Guillermito "Analyzing Steganography Software (for the fun of learning about it)", http://www.guillermito2.net/stegano/, A webpage discussing many different steganography programs from 2002-2004 and their various weaknesses.2005.
[3] Hemang A. Prajapati, Dr. Nehal G. Chitaliya, "Secured and Robust Dual Image Steganography", a Survey International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 1, January 2015.
[4] Vorgelegt Von, "Algebraic Attacks on Certain Stream Ciphers", Inaugural dissertation to obtain the academic degree of Doctor of Natural Sciences the University at Mannheim, 2006.
[5] Ronak Dhoshi, Pratik Jain, Lalit Gupta, "Steganography and its Applications in Security", International Journal of Modern Engineering Research (IJMER), Vol.2, pp. 4634- 4638, November 2012.
[6] Pratap Chandra Mandal, "Modern Steganographic Technique: A survey", International Journal of Computer Science & Engineering Technology, Vol.3, pp. 444-448, September 2012.
[7] Dongdong Fu, Yun Shi, Q., Dekun Zou, and Guorong Xuan, "JPEG Steganalysis Using Empirical Transition Matrix in Block DCT Domain", Proceedings of 8th IEEE International workshop on Multimedia Signal Processing, pp.310-313,2006.
[8] Guorong Xuan, Jianjiong Gao, Shi, Y.Q., and Zou, D., "Image Steganalysis Based on Statistical Image Moments of Wavelet Sub band Histograms in DFT Domain", IEEE 7th International Workshop on Multimedia Signal Processing, Shanghai, China, pp.1-4, 2005.
[9] Mehrabi, M.A, Faez, K, and Bayesteh, A.R, "Image Sstegnalysis Based on Statistical Moments of Wavelet Sub band Histograms in Different Frequencies and Support Vector Machine", 3 rd International Conference on Natural Computation, Vol. 1, pp. 587-590, 2007.
[10] Sonal, Dinesh Kumar, "A Study of Various Image Compression Techniques", IEEE Transaction, 2005.