Various Steganalytic Techniques Comparison for LSB Embedding

Yambem Jina Chanu
Dept. of CSE, NERIST, Itanagar
jina.yambem@gmail.com

Kh. Manglem Singh
Dept. of CSE, NIT Manipur
manglem@gmail.com

ThemrichonTuithung
Dept. of CSE, NERIST, Itanagar
tth@nerist.ac.in

ABSTRACT
This paper provides the theoretical concepts of Steganography and Steganalytic technique. Various methods developed in this field recently has been compared for least significant bit embedding technique. Steganography refers to the technique of hiding secret messages into media such as text, audio, image and video without any suspicion, while steganalysis is the art and science of unfolding the secret message. It can be deployed for the benefits of the mankind as well as by terrorists and criminals for malicious purposes. Both steganography and steganalysis have received a lot of attention from law enforcement and media.

Keywords
Steganography, Steganalysis, LSB embedding, Universal staganalysis, Transform domain, RS algorithm.

1. INTRODUCTION

Information hiding has been on rise for the past decades and people are obsessed with this phenomenon. Literally it's better to know the components of information hiding. So, important constituents of today's information hiding are cryptography, watermarking and steganography, each of these components has different objectives while deploying. Cryptography is the study of processing digital data by scrambling or encrypting in data bits with a key in such a way that the data is unintelligent to the unauthorized person who does not possess the key to recover or decrypt it. It is very clear in cryptography that the encrypted data stored in the memory or being transmitted takes unreasonable amount of computer processing resources and time during its useful life time to decrypt it. However, message data after decryption may always be distributed in plain form without any restriction, even by the authorized customer. Also encryption clearly marks a message as containing interesting information, and the encrypted message becomes subject to attackers. Watermarking of digital data, on the other hand is the process that enables data called a watermark, digital signature, tag, or label into a multimedia object such as text, audio, image or video in perceptually invisible or inaudible manner without degrading the quality of the object, such that watermark can be detected or extracted later to make an assertion about the object [1-4]. The embedded information can be a serial number or random number sequence, ownership identifiers, copyright messages, control signals, transaction dates, information about the creators of the work, bi-level or gray level images, text or other digital data formats [5]. An important goal of watermarking is to make removal of the inserted watermark bits from the watermarked object impossible without degrading the quality of the object and without additional information such as a key. Second important goal of watermarking is to sense that the object has been tempered by checking that the watermark is being removed or destroyed. Third goal of watermarking is prevention against copying and transmitting music, image, video on CDs and DVDs. Violation of copyrighted materials such as music and video happens frequently [6]. There has been no technique so far developed that meets the expectations of watermarking as desired. Also, it has become a legal to develop, sell or distribute code-cracking commercial software and hardware devices for anti-piracy measures with the advent of Digital Millennium Copyright Act (DMCA) of 1998 [7]. Thus music and video industries no longer depend on watermarking to prove violation of DMCA for copyrighted materials, but they are now rely on other approaches such that, their Internet providers to locate the possible violators. Almost infinite memory size is available for storing digital data in digital devices, more bandwidth is available for sending digital data efficiently in the Internet, and more freeware is available for embedding secret messages inside other media. Steganography is the branch of secret communication which conceals the existence of the message. Various media such as text, audio, digital images and videos which contain perceptually irrelevant or redundant information can be used as covers for hiding messages. The goal is to modify the carrier in an imperceptible way only, so that it reveals nothing neither the embedding of a message nor the embedded message itself. Steganography is not an ordinary means to protect confidentiality.

Digital image and video contain high degree of redundancy in representation, thus appealing for data hiding. Steganography finds applications in copyright control of materials, enhancing robustness of image search engines and smart IDs, where individuals' details are embedded in their photographs, video-audio synchronization, companies' safe circulation of secret data, TV broadcasting, TCP/IP packets and checksum embedding [8-10]. It also finds application in medical imaging systems where a separation is considered between patients' image data or DNA sequences and their captions, e.g., physician, patient's name, address and other particulars. Cyber-crime is believed to benefit from steganography [8] as reported in USA TODAY. Examples are found for hiding data in music files [11], and even in a simpler form such as in Hyper Text Markup Language (HTML), executable files and Extensible Markup Language (XML) [12].

Various techniques have been invented in the embedding process to make the detection hard, but it is still possible to detect the existence of the hidden message. Steganalysis is a technique which tries to discriminate between non-stego objects and cover objects, those objects without the hidden message and stego-objects are those objects that contain a hidden message. Steganography and Steganalysis got lots of attention around the globe, the choice of using these two techniques depends on the purpose of the concern party, as some are interested in securing their communication by hiding the fact that they are exchanging information. On the other hand some are interested in detecting the presence of hidden message may be illegal purpose. Steganalysis is the process of detecting the existence of the steganography in a cover medium and rendering it useless. In addition to detection of embedded message, the main goal of steganalysis are to estimate the length of embedded message, to estimate the stego key used by embedding algorithm, to extract the hidden message etc. Steganalysis finds its uses in cyber forensics, cyber warfare, tracking of criminal activities over the Internet and gathering evidence for investigations in case of anti-social elements [8,13-18]. Steganalysis also finds uses in law enforcement and anti-social significance steganalysis for peaceful applications and consequently improving the security of steganographic tools by evaluating and identifying their weakness. The battle between steganography and steganalysis is not going to end forever. Newer and more sophisticated steganographic techniques for embedding secret message will require more powerful steganalysis methods for detection.

Past decade has been growing interest in researches on image steganography and steganalysis. Existing techniques form a very small part of a very big system that calls for exciting and challenging research for the years to come [19-21].

This paper provides the introduction regarding research background of information hiding and state-of-art LSB detection algorithm. Steganalytic techniques are described for the detection of embedded message bits from stego-images in details. The experiment is designed to compare the performance of the algorithms. Experimental results indicate that RS steganalytic technique outperforms GEFR and histogram difference methods in terms of correct estimation of hidden message from stego-images.

The paper is organized as follows. In Section 2, LSB embedding is explained with the required formulation. Section 3 deals with different steganalytic methods of LSB embedding. Section 4 gives the comparison of different steganalytic techniques for LSB embedding followed by conclusions in Section 5.

2. SPATIAL STEGANOGRAPHY

Spatial steganography deals with changing some bits in the image pixel values while hiding data. Least significance bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without introducing many perceptible distortions [8]. Changes in those values of the LSB are imperceptible to our human eye, thus making it an ideal place for hiding information without any perceptual change in the cover object. Basically two methods exist for embedding secret messages they are done either sequentially or randomly. Embedding operation of LSB steganography may be described by the following equation [22].

$$y_i = 2\left\lfloor \frac{x_i}{2} \right\rfloor + m_i \qquad (1)$$

where m_i, x_i and y_i are the *i*-th message bit, the *i*-th selected pixel value before embedding and that after embedding respectively.

LSB embedding methods hide data in such a way that human does not perceive it, these embeddings often can be easily destroyed by compression, filtering or a less than perfect format or size conversion. Hence, it is

often necessary to employ sophisticated techniques to improve embedding reliability. Steghide, S-tools, Steganos etc. are based on LSB steganographic technique.

3. STEGANALYTIC METHODS

The powerful and popular LSB detection algorithms are Chi-square [23], RS [24], Gradient Energy-Flipping Rate Detection [25] and Histogram difference [26], which are explained in short below.

The first specific statistical steganalytic tool Chi-Square Attack developed for detection of message bits from stego-images embedded by LSB steganographic tool is based on PoV [23]. L-bit color channel can have $P = 2^L$ possible values. Splitting into 2^{L-1}pairs, which differ only in LSBs gives all possible patterns of neighboring bits of LSBs. Each of these pair is called PoV. The distribution of odd and even values of PoV is same as 0/1 distribution of secret bit if all available LSB fields are to be used. The idea of X^2 - analysis is to compare theoretically expected frequency distribution of PoVs with the real observed one, though no expected frequency is available in absence of original image. Let us assume that the pixel values $c_0, c_1, \dots, c_{P-1}$ are already sorted. For $P \leq 256$, there are at the most 128 PoVs. For the i-th pair (c_{2i}, c_{2i+1}), $i = 1,2, \dots, k$, we define $n_i^{'} = 1/2$(number of indices in the set $\{c_{2i}, c_{2i+1}\}$) and n_i= number of indices equal to c_{2i}.The value $n_i^{'}$ is the theoretically expected frequency if a random message has been embedded, and n_i is the actual number of occurrences of pixel value c_{2i}. Chi-square statistics is calculated as

$$X_{k-1}^2 = \sum_{i=1}^{k} \frac{(n_i - n_i^{'})^2}{n_i^{'}} \quad (2)$$

with $k-1$ degree of freedom.

The probability of embedding p can be calculated by

$$p = 1 - \frac{1}{2^{\frac{k-1}{2}} \Gamma\left(\frac{k-1}{2}\right)} \int_0^{X_{k-1}^2} e^{-\frac{x}{2}} x^{\frac{k-1}{1}-1} dx \quad (3)$$

expressing the probability that the distributions $n_2^{'}$ and n_i are equal and Γ is Euler Gamma function.

Chi- square test works well for sequential embedding, and it is less effective for random embedding unless the embedded bits are hidden in majority of the pixels.

Fridrich et al introduce a powerful steganalytic method known as RS analysis that utilizes the spatial correlation in the stego-images [24]. The basic idea is to discover and quantify the weak relationship between the LSB plane and the image itself. The image I to be analyzed is divided into $G(x_1, \dots, x_n)$ disjoint groups of n adjacent pixels. By defining a discrimination function f, which captures the smoothness of G as follow.

$$f(x_1, \dots, x_n) = \sum_{i=1}^{n-1} |x_{i+1} - x_i| \quad (4)$$

With invertible flipping function $F_1: 0 \leftrightarrow 1$, $2 \leftrightarrow 3$, …, $254 \leftrightarrow 255$, shifting function $F_{-1}: -1 \leftrightarrow 0$, $1 \leftrightarrow 2$, …,$255 \leftrightarrow 256$ and identity function $F_0 = F_0(x), \forall x \in P$, and with n- tuple mask M with values in $\{-1, 0, 1\}$ is classified into three types: R_M, S_MandU_M.

- Regular.$G \in R_M \Leftrightarrow f(F_M(G) > f(G)$ (5)
- Singular.$G \in S_M \Leftrightarrow f(F_M(G) < f(G)$
- Unusable. $G \in U_M \Leftrightarrow f(F_M(G) = f(G)$

Similarly, we can classify the groups $R_{-M}, S_{-M}$and U_{-M} for the mask $-M$, where $-M$ is the complement of M. As a matter of fact, it holds that $\frac{R_M + S_M}{T} \leq 1$ and $\frac{R_{-M} + S_{-1M}}{T} \leq 1$,

where T is the total number of G groups.
For typical images, the following hold true.
$R_M \approx R_{-M}$and $S_M \approx S_{-M}$.

The greater the message size, the lower the difference between R_{-M} and S_{-M}, and the greater the difference between R_M and S_M. This behavior is used in detection of hidden message from the stego-image [24].

Zhi et al propose GEFR based on the relation between the length of the embedded message and the gradient energy [25]. Let $I(n)$ be a unidimensional signal. The gradient $r(n)$ before embedding message is

$$r(n) = I(n) - I(n-1) \quad (6)$$

The gradient energy (GE) of the cover $I(n)$ is

$$GE = \sum |I(n) - I(n-1)|^2 = \sum |r(n)|^2 \quad (7)$$

After hiding of a signal $S(n)$ in the original signal, $I(n)$ becomes $I'(n)$ and the gradient is re-written as

$$\begin{aligned} r^{'}(n) &= I^{'}(n) - I^{'}(n-1) \\ &= I(n) + S(n) \\ &\quad - \big(I(n-1) + S(n-1)\big) \\ &= r(n) + S(n) - S(n-1) \end{aligned}$$

The probability distribution function of $S(n)$ is

$$\begin{cases} \rho_{S(n)=0} = \frac{1}{2} \\ \rho_{S(n)=\pm 1} = \frac{1}{4} \end{cases} \quad (8)$$

After embedding, the new gradient energy GE' is

$$GE' = \sum |r(n)|^2 = \sum |r(n) + S(n) - S(n-1)|^2 = \sum |r(n) + \Delta(n)|^2 \quad (9)$$

where $\Delta(n) = S(n) - S(n-1)$.

In order to perform detection we need to know a function known as flipping function. Let us consider a cover image I with $W \times H$ pixels and $p \leq W \times H$ be the size of the hidden message .So after applying the flipping function the following are the results.

- For $= W \times H$, there is $\frac{W \times H}{2}$ pixels with inverted LSB. That means that the embedding rate is 50% and the gradient energy is given by $GE = (\frac{W \times H}{2})$.
- The original image's gradient energy is given by $GE(0)$. After inverting all available LSBs using F, the gradient energy becomes $GE' = W \times H$.
- For $p < W \times H$, there is $\frac{p}{2}$ pixels with inverted LSB. Let $I(\frac{p}{2})$ be the modified image. The resulting gradient energy is $GE = \frac{p/2}{W \times H} = GE(0) + p$. If F is applied over $I(\frac{p}{2})$, the resulting gradient energy is $GE = \frac{W \times H - p/2}{W \times H}$.

Using these above mentioned properties, Zhi et al. proposed the detection procedure [25]:

1. Find the test image's gradient energy $GE = \frac{p/2}{W \times H}$;
2. Apply F over the test image and calculate $GE = \frac{W \times H - p/2}{W \times H}$;
3. Find $GE = \left(\frac{W \times H}{2}\right) = \left[GE = \frac{p/2}{W \times H} + GE = \frac{W \times H - p/2}{W \times H}\right]/2$;
4. $GE(0)$ is based on $GE = \left(\frac{W \times H}{2}\right) = GE(0) + W \times H$;
5. Finally, the estimated size of the hidden message is given by

$$p' = GE = \frac{p/2}{W \times H} - GE(0) \quad (10)$$

Zhang et al introduce the difference image histogram method [26] which deploy the measure of weak correlation between successive bit planes to construct a classifier for which will help to distinguish stego-images and cover images. Here the difference image histogram is used as statistical analysis tool. The difference image is defined as

$$D(i,j) = I(i,j) - I(i,j+1) \quad (11)$$

where $I(i,j)$denotes the value of the image I at the position (i,j).

There exists a difference between the difference image histograms for normal image and the image obtained after flipping operation on the LSB plane. To know this difference image histogram concept in details we need to know some notions first. Let I be the test image with $M \times N$ pixels. The embedding ratio ρ is defined as the percentage of the embedded message length to the maximum capacity. If the difference image histogram of an image is represented by h_i, that of the image after flipping all bits in the LSB plane by f_i and that of the image after setting all bits in the LSB plane to zero by g_i. The following relations exist between three planes as follows:

$$\begin{aligned} h_{2i} &= f_{2i} = a_{2i,2i} g_{2i} \\ h_{2i+1} &= a_{2i,2i+1} g_{2i} + a_{2i+2,2i+3} g_{2i+2} \\ f_{2i+1} &= a_{2i,2i-1} g_{2i} + a_{2i+2,2i+3} g_{2i+2} \end{aligned} \quad (12)$$

$a_{2i,2i+j}$ is defined as the translation coefficient from the histogram $g_i$to h_i, when $j = 0,1,-1$ we have

$$0 < a_{2i,2i+j} < 1$$
Otherwise (13)

$$a_{2i,2i+j} = 0$$

And they satisfy $a_{2i,2i-1} + a_{2i,2i} + a_{2i,2i+1} = 1$ (14)

Combining equation (12) and (13), the following iterative formulae are found.

$$a_{0,1} = a_{0,-1} = \frac{g_0 - h_0}{2g_0}$$

$$a_{2i,2i-1} = \frac{h_{2i}}{g_{21}} \quad (15)$$

$$a_{2i,2i-1} = \frac{h_{2i-1} - a_{2i-2,2i-1} g_{2i-2}}{g_{2i}}, i \geq 1$$

$$a_{2i,2i+1} = 1 - a_{2i,2i} - a_{2i,2i-1}, i \geq 1$$

For $\rho = 100\%$ the LSB plane is independent of the remained bit planes. For such stego images we have$a_{2i,2i-1} \cong 0.25$, $a_{2i,2i} \cong 0.5$, $a_{2i,2i+1} \cong 0.25$.

For a natural image there exists weak correlation between the LSB plane and the remained bit planes. As more and more secret messages are embedded, such that correlation becomes weaker and weaker and finally

the LSB plane becomes independent of the remained bit planes.

From Equation (12) we know that h_{2i+1} consists of two parts: $a_{2i,2i+1}g_{2i}$ and $a_{2i+2,2i+3}g_{2i+2}$ statistical test shows that these two parts contribute equally for natural images *i.e*.

$$a_{2i,2i+1}g_{2i} \cong a_{2i+2,2i+3}g_{2i+2} \quad (16)$$

Let us denote $\alpha_i = a_{2i+2,2i+1}/a_{2i,2i+1,}$ $\beta_i = a_{2i+2,2i+3}/a_{2i,2i-1}$ and $\gamma_i = g_{2i}/g_{2i+2}$ then the statistical hypothesis of the steganalytic method is that for a natural image the following equation should be satisfied.

$\alpha_i \approx \gamma_i$

while for stego-images with the LSB plane fully embedded

$\alpha_i \approx 1$

The quantity α_i can be viewed as the measure of the weak correlation between the LSB plane and its neighboring bit planes. The relationship between α_i and the embedding ratio ρ will be modeled using a quadratic equation $y = ax^2 + bx + c$. By considering four critical points $(P_1 = (0,\gamma_i), P_2 = (p,\alpha_i), P_3 = (1,1), P_4 = (2-p,\beta_i))$ the following equations have been developed

$$\begin{aligned} &c = \gamma_i; \\ &ap^2 + bp + c = \alpha_i; \\ &a + b + c = 1; \\ &a(2-p)^2 + b(2-p) + c = \beta_i; \end{aligned} \quad (17)$$

Assuming $d_1 = 1 - \gamma_i;\ d_2 = \alpha_i - \gamma_i;\ d_3 = \beta_i - \gamma_i$ then the above equation (8) can be simplified as follows

$$2d_1p^2 + (d_3 - 4d_1 - d_2)p + 2d_2 = 0 \quad (18)$$

The embedding ratio ρ can be obtained from the root of the above whose absolute value is smaller if the discriminantis smaller than zero, then $\rho \approx 1$.

4. EXPERIMENTAL RESULTS

RS, GEFR and histogram difference steganalytic methods are compared on 10 different images such as Lena, Pepper, Boat, Terrain, Kodak, Tiffany, House, Splash, Tulips and Airplane for embedding percentage from 0% to 50% for random embedding in increment of 10%. Results on Lena, Pepper, Kodak and Tiffany are shown in Tables 1- 4. It is found from the results that RS outperforms GEFR and Histogram difference in term of correct estimation of hidden message.

Table 1: Comparison on Lena.

% Embedding	RS	GEFR	Histogram
0	-0.0258	0.9668	-0.9603
10	9.9183	9.2351	10.2715
20	21.9932	19.2197	22.2566
30	27.2821	26.7941	29.7445
40	39.3243	35.1227	37.9855
50	51.0441	48.1160	50.7022

Table 2: Comparison on Pepper.

% Embedding	RS	GEFR	Histogram
0	-0.5675	-0.3598	-2.3884
10	10.7508	9.9466	11.0063
20	19.6330	18.9322	23.0959
30	29.7035	26.7574	30.5566
40	49.6960	49.3498	48.3586
50	49.6960	49.3498	48.3586

Table 3: Comparison on Kodak.

% Embedding	RS	GEFR	Histogram
0	-0.8078	1.2822	-4.8214
10	12.1183	6.7513	13.18.38
20	18.3352	16.3050	26.2080
30	31.0766	25.1554	33.2173
40	39.3658	31.1484	38.5263
50	49.9324	46.4819	43.6863

Table 4: Comparison on Tiffany.

% Embedding	RS	GEFR	Histogram
0	-0.3332	-1.9902	-5.9356
10	10.8293	8.9388	16.4187
20	18.1585	19.5168	28.3165
30	29.867	25.0788	33.0158
40	40.5984	40.8258	36.8795
50	50.2198	46.2348	41.3029

5. CONCLUSIONS

This paper describes steganalytic techniques such as Chi-square, RS, Gradient Energy and Histogram Difference attacks etc for the detection of embedded message bits from stego-images in details. Experimental results are included in this paper so that the better performance one method to other methods on different images for random embedding. It is found that RS steganalytic technique outperforms GEFR and histogram difference methods in terms of correct estimation of hidden message from stego-images.

REFERENCES

[1] F. Petticolas, Information hiding techniques for steganography and digital watermarking, StefenKatzenbeisser, Artech house books, ISBN 158053-035-4, Dec. 1999.

[2] F. Hartung and M. Kutter, Multimedia watermarking techniques, Proceedings of the IEEE, vol. 87, no. 7, July 1999.
[3] S. Voloshynovkiy, S. Pereira, T. Pun, J. Eggers and J. Su, Attacks on digital watermarks: classification, estimation-based attacks and benchmarks, IEEE communications Magazine 39, 9 (August) 2001, pp. 118-126.
[4] A. Sequeira and D. Kundur, Communications and information theory in watermarking: A survey, In proc. of SPIE Multimedia systems and application IV, vol. 4518, pp. 216-227.
[5] J.O. Ruanaidh, H. Peterson, A. Herrigel, S. Pereira and T. Pun, Cryptographic copyright protection for digital images based on watermarking techniques, Elsevier Theoretical Computer Science, vol 226, no. 1, pp. 117-142, 1999.
[6] C. Bergman and J. Davidson, Unitary embedding for data hiding with the SVD, Security, Steganography, and Watermarking of Multimedia Contents VII, SPIE, vol. 5681, San Jose, Jan., 2005.
[7] "Digital millennium copyright act ", http://thomas.loc.gov .cgi-bin/query/z?c105:H.R.2281.ENR:
[8] N.F. Johnson and S. Jajodia, Exploring steganography,: seeing the unseen, IEEE Computer, vol. 31, no. 2, pp. 26-34, 1998.
[9] W. Bender, W. Butera, D. Gruhl, R. Hwang, F.J. Paiz, S. Pogreb, Applications of data hiding, IBM Systems Journal vol. 39, no. 3 & 4, pp. 547-568, 2000.
[10] J. Fridrich and M. Golan and R. Du, Detecting LSB steganography in color and gray-scale images, IEEE Multimedia Magazine, Special Issue on Security, pp. 22-28, October-November 2001.
[11] C. Hosmer, Discovering hidden evidence, Journal of Digital Forensic Practice, vol.1, pp. 47-56, 2000.
[12] J.C. Hermandez-Castro, I. Blasco-Lopez, J.M. Estevez-Tapaidor, Steganography in games: A general methodology and its application of the Game of Go, Elsevier Science Computers and Security, pp. 64-71, vol. 25, 2006.
[13] H. Wang and S. Wang, Cyber warfare Steganography vsSteganalysis, ACM Commun. vol. 47, pp. 76-82, October 2004.
[14] A. Nissar and A.H. Mir, Classification of steganalysis techniques: A study, Elsevier Digital Signal Processing, vol. 20, pp. 1758-1770, 2010.
[15] W. Bender, W. Butera, D. Gruhl, R. Hwang, F.J. Paizand and S. Pogreb, Applications for data hiding, IBM Systems Journal, vol. 39, no. ¾, pp. 547-568, 2000.
[16] S. Miaou, C. Hsu, Y. Tsai, and H. Chao, A secure data hiding technique with heterogeous data-combining capability for electronic patient records, Proc. of 22nd IEEE EMBS, pp. 280-283, July 2000.
[17] U.C. Nirinjan, and D. Anand, Watermarking medical images with patient information, Proc. of 20th IEEE International Conference of Biological Society, pp. 703-706, 29 October – 1 November 1998.
[18] Y. Li, C. Li and C. Wei, Protection of mammograms using blind steganography and watermarking, Proc. of IEEE ISIAS, pp. 496-499, 2007.
[19] R. J. Anderson and F.A.P. Pettitcolas, On the limits of steganography, IEEE Journal on Selected Areas in Communication, vol. 16, no. 4, pp. 474-481, 1998.
[20] H. Wang and S. Wang, Cyber warfare: Steganography vs Steganalysis, Communications of ACM, vol. 47, no. 10, pp. 76-82, 2004.
[21] N. Provos and P. Honeyman, Hide and seek: An introduction to steganography, IEEE Security and Privacy, vol. 1, no. 3, pp. 32-44, 2003.
[22] B. Lin, J. He, J. Huang and Y.Q. Shi, A survey on image steganography and steganalysis, Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, pp. 142-172, April 2011.
[23] T.A Hawi, M.A. Qutayari and H. Barada, Steganalysis attacks on stego-images using stego signatures and statistical image properties, in Proc. IEEE TENCON, vol. 2, pp. 104-107, 2004.
[24] J. Fridrich and M. Goljan, Practical steganalysis of digital images – state of the art, Security and Watermarking of Multimedia Contents IV, E.J. Delp III and P.W. Wong, editors, Proc. of SPIE, 4675, pp. 1-13, 2002.
[25] l. Zhi, S.A. Fen and Y. Xian, A LSB steganography detection algorithm, Proc. of IEEE Symposium on Personal Indoor and Mobile Radio Communication, vol. 3, pp. 2780-2783, September 2003.
[26] T.Zhang and X.Ping, Reliable detection of LSB steganography based on the difference image histogram, IEEE International Conference on Acoustics, Speech, and Signal Processing, vol. 3, pp.545-548 April 2003.