HIGH CAPACITY IMAGE STEGANOGRAPHY IN THE SPATIAL DOMAIN USING LEHMER CODE

R Sunder[1], P Eswaran[2], A Nagalinga Rajan[3]

[1]*Research Scholar, Manonmaniam Sundaranar University, Tirunelveli, (India)*

[2] *Department of Computer Science and Engineering, Alagappa University, Karaikudi, (India)*

[3] *Research Scholar, Manonmaniam Sundaranar University, Tirunelveli, (India)*

ABSTRACT

Steganography is one of the modern techniques for covert communication through the internet. In addition to providing confidentiality, it also enables the communication of large amounts of data without raising suspicion. This paper presents a novel technique for image steganography using Lehmer code that provides high capacity and better performance. Lehmer code is a way of encoding each possible permutation of a sequence of n numbers. The pixel intensity values are perturbed such that the sorting order of the pixels within a neighbourhood encodes the message digit. If n is the number of pixels in the neighbourhood block then a message digit expressed in base $n!$ could be hidden. This allows high capacity embedding. In order to prevent high distortions of image, only blocks with variance below a set threshold is used for embedding. Experimental results show that the technique promises embedding capacities higher than 2 bits per pixel with minimal distortion. This technique also exhibits significant resistance against common steganalysis methods.

Keywords: *Information hiding, Steganography, Lehmer code, Permutation, Steganalysis*

I. INTRODUCTION

Steganography is the art and science of secret communication where apart from hiding the content of the message, the presence of message itself is hidden. This is useful in cases where suspicious secret messages are monitored and punished by a dictatorial censorship authority. The secret communication is made to look like an exchange of casual harmless information.A typical steganographic message originates from a sender and is transmitted to a receiver via a communication medium. The message is embedded in a cover object. In the digital world, images, audio, video or text in the form of digital objects are used as cover. Once the message is embedded, the cover object becomes the stego-object which is then transmitted through the medium. The intended receiver has the necessary means to extract the original message from the stego object whereas any other observers cannot distinguish between the stego and cover objects either using their senses or through computations. If passive observers are able to detect the presence of hidden messages, then the steganographic exchange is said to be failed. Steganographic exchanges have taken place since the time of ancient Greece [1]. However the prevalence of digital media in the networked world since the advent of the World Wide Web brought steganography to the mainstream. Today large amounts of digital data are exchanged through the Web, which provides for the perfect cover for steganography. The number of multimedia data, especially digital images has skyrocketed in recent years with the popularity of social networking [2]. Thus steganography provides an effective communication tool in the hands of people behind many autocratic censorship regimes

across the world. There is also the danger of terrorist organizations using steganography to plan and implement threats. So the organized study of steganography is an important need.

Digital Images represent the ideal medium for steganographic exchange due to two reasons namely [3]:

- Due to the nature of images and Human visual system, images have a lot of redundancy that provides room for messages.
- Digital Images are transmitted in large amounts in the Internet and is seen as a normal activity that does not raise suspicion. Screening the entire web for stego images is a practically impossible task.

There are many steganographic techniques ranging from the Least Significant Bit (LSB) embedding that hides the message bits in the least significant bits of the image pixel intensity values to more sophisticated approaches like image transforms[4].Steganalysis refers to the statistical methods that attempt to beat the steganography by distinguishing between normal objects from stego objects [5]. The steganographer and the steganalyst are in the constant game of outsmarting each other. Several steganographic techniques have been proposed in the last three decades. However there are many practical impediments in bringing steganography to mainstream applications. The data throughput of steganographic techniques must be high enough to allow the exchange of significant data and the protocols need to be designed to support it. So the improvement of embedding capacity is an important endeavor in steganography design.

Rest of this paper is organized as follows. Section II presents related works and theoretical background. In section III describes the proposed method of embedding multiple bits together similar to Matrix embedding methods using Lehmer code. Section IV proposed method is described in detail with encoding, and decoding procedure step by step. Section V demonstrated the Analysis and validation. Finally conclusions and future are provided in section VI.

II. RELATED WORKS

The simplest and the most computationally efficient steganographic technique is the LSB Replacement. The least significant bits of pixel intensity values are simply replaced by the message bits. The distortion produced at each pixel position is either 0, 1 or -1. Several methods which produce similar distortion profile are termed as ±1 embedding. One effect of replacing the least significant bit is that even values are incremented by one whereas odd values are decremented by one. This asymmetry is utilized by steganalytic techniques that detect the presence of messages in the LSB. A number of steganalysis systems can reliably detect LSB replacement such as RS analysis proposed by Fridrich et al. in [6], Histogram Characteristic Function (HCF) proposed by Harmsen and Pearlman in [7] , Adaptive asymptotically uniformly Most Powerful (AUMP) test [8], [9]. In 2006, Mielikainen proposed an LSB matching Revisited method based on Pixel Pair Matching (PPM) in which two pixels are used as an embedding unit [10]. The first pixel is used to carry a message bit while the second message bit is stored using a binary function that involves both the pixel values. Therefore the modified method allowed the embedding of the same payload as LSB matching but with fewer changes to the cover image. The distortion measured in MSE is reduced from 0.5 for LSB replacement to 0.375 when the embedding capacity is 1 bit per pixel. Specifically the first bit was carried in the LSB of the first pixel and the second bit was carried in the function $LSB\left(\left\lfloor \frac{y_i}{2} \right\rfloor + y_{i+1}\right)$, which is a binary function that allows a selection of addition or subtraction

of the y_i to carry information. In 2006, Zhang and Wang enhanced Mielikainen's method by embedding a 5-ary message digit in a pixel pair by changing atmost one pixel only known as Exploiting Modification Direction (EMD) method [11]. The embedding capacity is increased to 1.161 bpp in EMD. The EMD method proposed a weighing extraction function to embed secret data into a cover image. The extraction function is defined as

$$f(x_1, x_2, \ldots x_n) = \sum_{i=1}^{n} x_i \times i \bmod(2n+1) \quad (1)$$

Where x_i is the i^{th} pixel value, n is the number of pixels of the group. The group of pixels belong to non-overlapping blocks of the image. The best embedding rate is achieved when a 5-ary message digit is embedded in pairs of pixels. The PSNR of the embedding is reported to be 51.9 decibel(dB) in their experiment.

In 2008, Chang et al. proposed a novel image steganographic method Using Tri-way Pixel-Value Differencing (PVD) [12]. The hiding capacity of the PVD method was upgraded using three different directional edges and tri-way pixel-value differencing was designed. In addition, to reduce the quality distortion of stego-image brought from setting larger embedding capacity, an optimal approach of selecting the reference point and adaptive rules were presented. Theoretical estimation and experimental results demonstrated that the proposed scheme provided superior embedding capacity and gave secrecy protection from dual statistical stego-analysis. Besides, the embedded confidential information can be extracted from stego-images without the assistance of original images. In 2009, Chao et al. proposed the Diamond Encoding (DE) method in that increased the embedding capacity [13]. In DE, message digits can be expressed in base of 5, 13, 25 etc and embedding is done by modifying pixel pair values according to a Diamond Characteristic Value (DCV) function of their neighbourhood set. In 2012, DE was subsequently enhanced to use arbitrary base systems and to yield better performance by Hong and Chen in Adaptive Pixel Pair Matching (APPM) [14].

III. LEHMER CODE

Lehmer code is a particular way to encode each possible permutation of a sequence of n numbers. It is an instance of a scheme for numbering permutations and is an example of an inversion table [15]. The Lehmer code makes use of the fact that there are $n!$ permutations of a sequence of n numbers. Let σ denote a particular permutation of a sequence of integers from 0 till $n-1$. A pair of indices (i, j) with $i < j$ and $\sigma_i > \sigma_j$ is called an inversion of σ and the Lehmer code $L(\sigma)_i$ counts the number of inversions with fixed i and varying j. The sum $L(\sigma)_1 + L(\sigma)_2 + \ldots + L(\sigma)_n$ is the total number of inversions of sigma which is also the number of adjacent transpositions that are needed to transform the permutation into the identity permutation [16]. $L(\sigma)$ represents σ and can be used to encode the permutation.

To get the Lehmer code of a particular sequence the following in-place procedure is adopted. For every number of the sequence x starting with the first one, the numbers to the right of x which are greater than x are reduced by 1. The sequence thus obtained is expressed in factorial radix giving the integer encoding of the permutation. For example the permutation $(1,0,3,4,2)$ undergoes the mentioned procedure.

$(1,0,3,4,2)$

$(1,0,2,3,1)$

$(1,0,1,2,0)$

$(1,0,1,1,0)$

$(1,0,1,1,0)$

$L(1,0,3,4,2) = 1*4!+0*3!+1*2!+1*1!+0*0! = 27$

The procedure can be reversed to decode the permutation from the Lehmer code. The proposed method aims to adjust the pixel intensities such that the sorting order is an encoding of the message digits expressed in base of $n!$, where n is the number of pixel intensities in the neighbourhood block.

IV. PROPOSED METHOD

The proposed method perturbs the pixel intensity values in a neighbourhood block of size $b_1 \times b_2$ such that its sorting order gives the message digit as an encoding in Lehmer code. The number of pixels in the block is $n = b_1 b_2$.

4.1 Secret Embedding Algorithm

- Convert the message bits to the base of $n!$ and each message digit expressed as a permutation of sequence of numbers using Lehmer code.
- The image blocks of size $b_1 \times b_2$ are visited in the pseudo random order indexed by a shared key. For every block that satisfies the condition variance< vmax, calculate the mean pixel intensity value as m . vmax is a suitable threshold fixed at 20.
- The values of the pixel intensities are selected from $m - \frac{n}{2}, m - \frac{n}{2} + 1, \ldots m + \frac{n}{2} - 1, m + \frac{n}{2}$ so that their sorting order matches the message digit as the Lehmer code.
- The procedure is repeated for all blocks which satisfy the condition.
  The condition is enforced to prevent distortion in blocks with high variation usually encompassing edges.

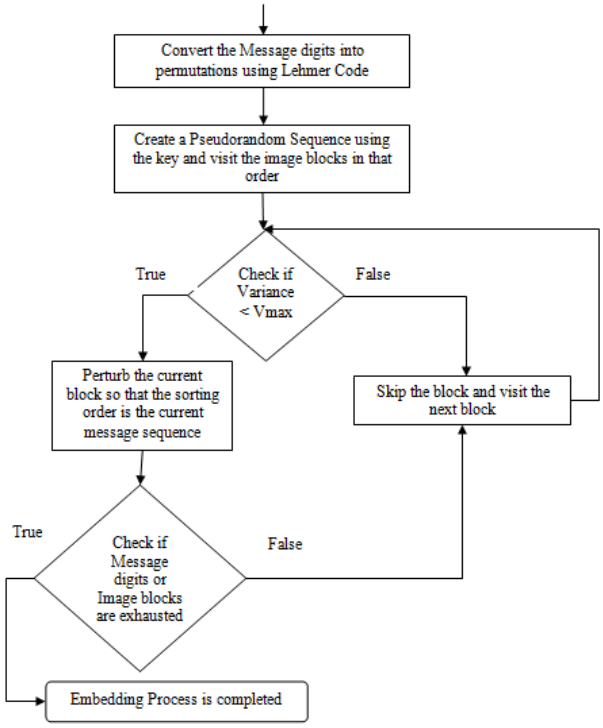

Figure 1 Flow Chart of Embedding

4.2 Secret Extraction Algorithm

The image is divided into blocks of size $b_1 \times b_2$. The image blocks are visited in the same pseudo-random sequence generated using the shared key and the message digits are extracted from the blocks that satisfy the condition on variance.

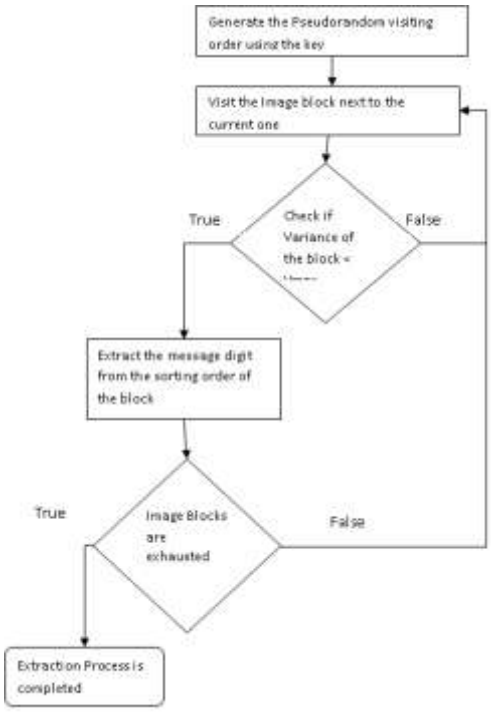

Figure 2 Flow Chart of Extraction

V. ANALYSIS AND VALIDATION

The proposed method is tested in MATLAB 7.9 using the image processing toolbox. Experiments were done on a 100 images chosen from USC-SIPI Image Database as well as miscellaneous test images [17], [18]. All uncompressed images were converted to grayscale images of size 512×512. Pseudorandom binary data is embedded into cover images by using lehmer code method to achieve stego image with different payloads. The peak signal-to-noise ratio (PSNR) was utilized to evaluate the stego-image quality. The PSNR is defined as follows:

The visual distortion of the stego image with respect to the cover image is measured as Mean Square Error (MSE) defined as

$$MSE = \left(\frac{1}{M \times N}\right)\sum_{i=1}^{M}\sum_{j=1}^{N}(s_{i,j} - c_{i,j})^2 \quad (2)$$

and

Peak Signal to Noise Ratio (PSNR) is similarity between two images and expressed in decibels (dB).

$$PSNR = 10 \log_{10}\left(\frac{255^2}{MSE}\right) \quad (3)$$

Here $s_{i,j}$, $c_{i,j}$ is pixel of the cover image and stego-image respectively where the coordinates is (i, j).

$M \times N$ Represent the size of the image, here 255 is the Peak Signal in the image representation. If the PSNR value is higher than 30dB indicates the fact that human vision is discrepancy between cover image and the stego-image is more imperceptible. The maximum capacity for a block size of n pixels is $\frac{\log_2 n!}{n} BPP$ (bits per pixel). The actual capacities are less due to the condition on intensity variation with $v_{max} = 20$.

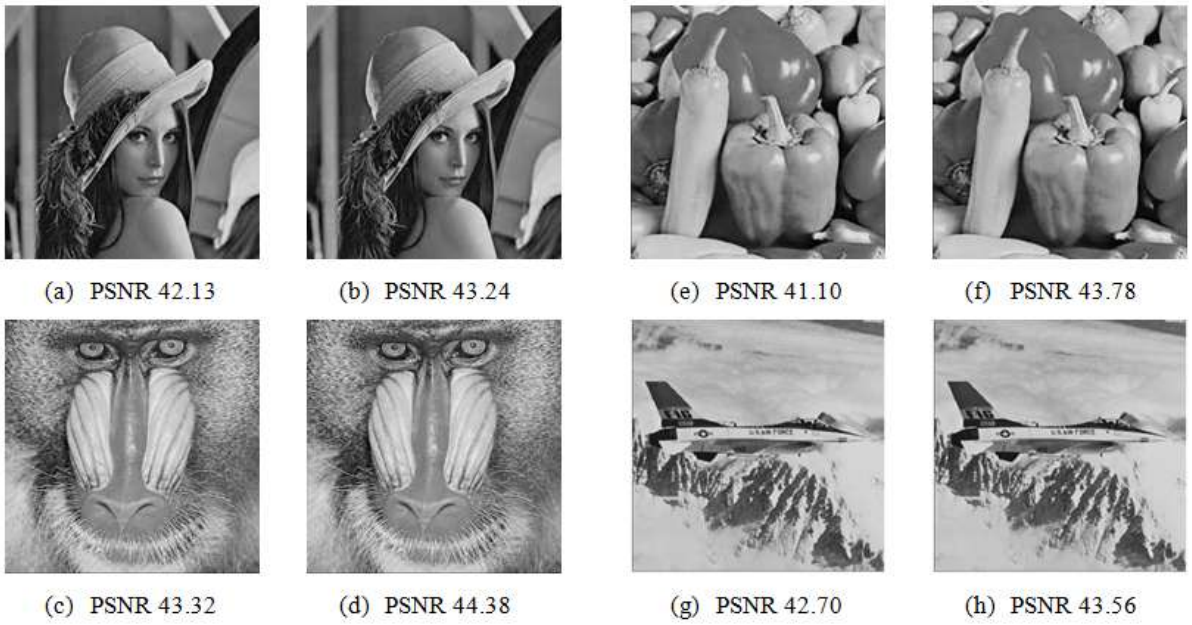

Figure 3. The size of stego-image is 512×512: (a),(c),(e), and(g) are the stego-images produced by LSB replacement technique; (b),(d),(f), and (h) are the stego-images produced by proposed method.

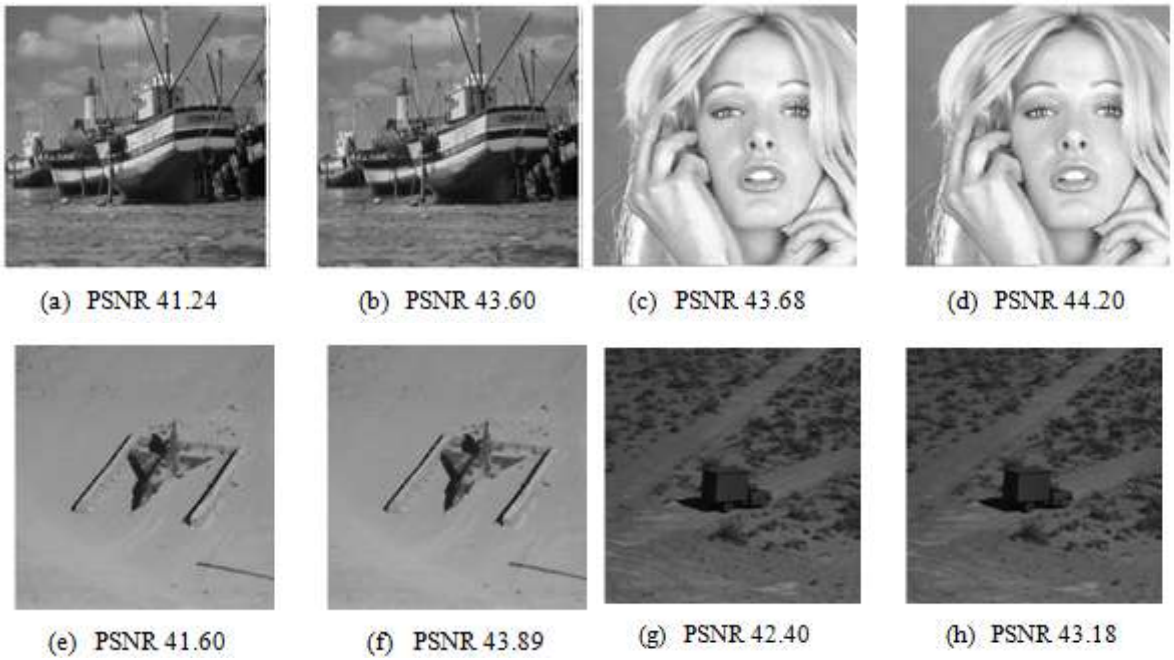

Figure 4. The size of stego-image is 512× 512: (a),(c),(e),and(g) are the stego-images produced by LSB replacement technique; (b),(b),(b),and (h) are the stego-images produced by proposed method.

Table 1 The Results of Embedding the Random Messages by LSB Replacement Technique Including the Proposed Methods

Cover Image (512 × 512)	LSB Replacement (2 bpp)		Proposed Method (4 × 4)	
	Capacity (Bytes)	PSNR (dB)	Capacity (Bytes)	PSNR (dB)
Lena	65536	42.13	75368	43.24
Baboon	65536	43.32	74568	44.38
Peppers	65536	41.10	69980	43.78
Jet	65536	42.70	73290	43.56
Boat	65536	41.24	72450	43.60
Tiffany	65536	43.68	68790	44.20
Airplane	65536	41.60	68910	43.89
Truck	65536	42.40	68210	43.18

The results in fig.3 and fig 4. (a),(c),(e) and(g) are the stego-image produced by LSB replacement technique, and (b),(d),(f) and (h) are the stego-images produced by the proposed method with block size of 4×4. The PSNR values obtained demonstrate that the proposed method is superior to LSB replacement technique as shown in Table 1 with an increase of 0.5 to 2 dB over LSB replacement. It can be inferred that the method delivers high embedding capacities with reasonable distortion.

5.1 Effectiveness Against Steganalysis

The proposed method is tested against Adjacent Histogram Characteristic Function center of Mass (ADJ-HCF-COM) detector and the SPAM Steganalyzer. Ker has proposed ADJ-HCF-COM in [19] which uses calibrated histogram center of mass to detect hidden message embedding. This is calculated from the Image Histogram H by

$$C(H[k]) = \frac{\sum_{i,j=0}^{n} (i+j)\left|H\right|}{\sum_{i,j=0}^{n} \left|H[i,j]\right|} \quad (4)$$

The ratio of ***C*** of an image to that of the calibrated image obtained by down sampling detects the presence of a secret message. The ROC curve for the proposed method with block size of 4×4 is shown in Fig 5. From the ROC curve it is evident that the proposed method can evade detection by ADJ-HCF-COM. The SPAM steganalyzer however, was able to detect the embedding with an equal error rate of 12%.

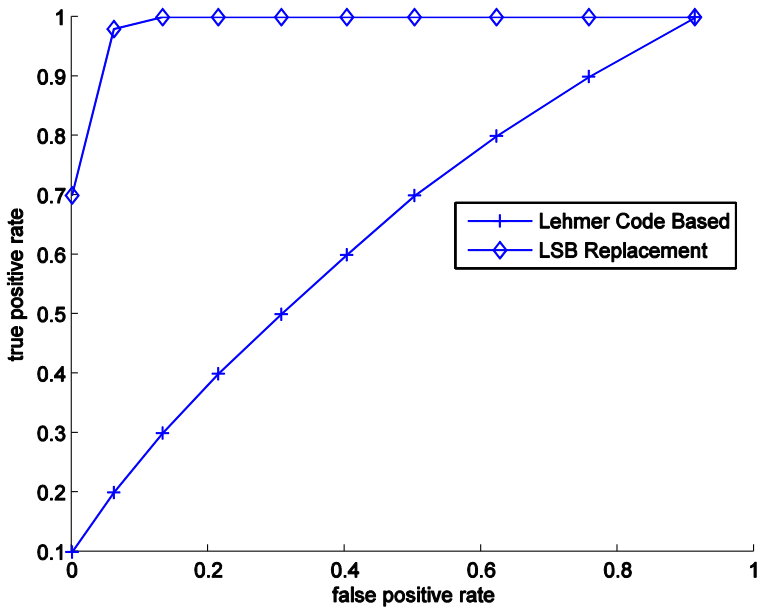

Figure 5 ROC Curves for the Proposed Method and LSB Replacement

VI. CONCLUSION AND FUTURE WORK

In This paper, we presents a high capacity steganographic technique which uses the Lehmer code to encode message digits in the sorting order of image block intensity values. The method offered better performance with higher capacity than existing LSB based methods. It is shown that the proposed method possesses resistance against steganalysis. The visual consistency of the stego images is also shown to be well preserved under the embedding. The proposed method can be effectively used to communicate large amounts of data efficiently.The reordering of values leaves a distinct pattern that can be picked up by pattern based steganalyzers like SPAM. This can be improved by using randomness in the pixel value adjustment and simple reordering with a modified condition on the image blocks. Another improvement could be reordering the gradient values instead of pixel values in order to reduce distortion significantly.

REFERENCES

[1] S.P. Mohanty, "Digital watermarking: A tutorial review", *URL:* http://www. csee. usf. edu/~ smohanty/research/Reports/WMSurvey1999Mohanty. pdf(1999).

[2] B. Parr, Facebook by the Numbers: Inforgraphic, URL: http://mashable.com/2011/10/21/facebook-infographic/

[3] T. Morkel, J. H. P. Eloff and M. S. Olivier, "An overview of image steganography", Proceedings of the Fifth Annual Information Security, Sandton, South Africa, June/July 2005.

[4] S.Y. Frank, "Digital watermarking and steganography: fundamentals and techniques", CRC Press, Inc., 2007.

[5] I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker, "Digital Watermarking and Steganography", second edition, Morgan Kaufmann series in Computer Security.

[6] J. Fridrich,M. Goljan, and R. Du, "Reliable Detection of LSB Steganography in Grayscale and Color Images", Proceedings of ACM, Special Session on Multimedia Security and Watermarking, Ottawa, Canada, October 5, pp.27-30,2001.

[7] J. Harmsen and W. Pearlman, "Steganalysis of additive-noise modelable information hiding", in Proc. SPIE Security Watermarking Multimedia Contents, vol. 5020,pp.131-142, 2003.

[8] L. Fillatre, "Adaptive steganalysis of least significant bit replacement in grayscale natural images", IEEE Transactions on Signal Processing, vol.60, no. 2, pp.556-569,2012.

[9] R. Cogranne and F. Retraint, "An asymptotically uniformly most powerful test for LSB matching detection", IEEE Transactions on Information Forensics and Security, vol.8, no. 3, pp.464-476, 2013.

[10] J. Mielikainen, "LSB matching revisited", IEEE Signal Process. Lett., vol. 13, no. 5,pp.285-287, 2006.

[11] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction", IEEE Communications Letters, vol. 10, no. 11,pp.1-3,2006.

[12] K.C.Chang,C.P. Chang, P.S. Huang, and T.M.Tu, "A novel image steganographic method using tri-way pixel-value differencing", Journal of multimedia vol.3, no. 2 , pp.37-44,2008.

[13] R.M. Chao,H.C Wu, C.C. Lee, and Y.P. Chu, "A novel image data hiding scheme with diamond encoding", EURASIP Journal on Information Security,658047, 2009(1).

[14] W.Hong, and T.S. Chen, "A novel data embedding method using adaptive pixel pair matching". Information Forensics and Security, IEEE Transactions on vol.7,no.1, pp.176-184,2012. .

[15] D.H. Lehmer, "Teaching combinatorial tricks to a computer", Proc. Sympos. Appl. Math. Combinatorial Analysis, Amer. Math. Soc. 10 , pp.179-193,1960.

[16] http://en.wikipedia.org/wiki/Lehmer_code

[17] USC-SIPI Image Database. http//sipi.usc.edu/services/database/Database.html

[18] F.Petticolas, "Public-Domain Test images for home works and projects", URL: http://hompages.cae.wisc.edu/~ece533/images/

[19] A. Ker, "Steganalysis of LSB matching in grayscale images", IEEE Signal Process. Lett., vol. 12, no. 6,pp.441-444,2005.