ISSN No. 0976-5697

Volume 2, No. 2, Mar-Apr 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Gray Value based Adaptive Data Hiding for Image Authentication (GVADHIA)

Nabin Ghoshal*
Department of Engineering and Technological Studies
University of Kalyani
Kalyani, Nadia, West Bengal, India
nabin_ghoshal@yahoo.co.in

J. K. Mandal
Department of Computer Science and Engineering
University of Kalyani
Kalyani, Nadia, West Bengal, India
jkm.cse@gmail.com

Abstract: This paper presents a novel adaptive data hiding method in gray images using complement value (CV) of higher order three bits (b_7, b_6 and b_5) of each gray image byte to achieve large embedding capacity and imperceptible stegoimages. The technique exploits the complement value (CV) at each gray image byte to estimate how many bits will be embedded into the image byte. Image byte located in the edge areas are embedded by k-bit LSB substitution technique with a large value of k in deep blackish area than that of the image bytes located in the light gray areas. Any image byte is embedded by the k-bit LSB substitution technique. The value of k is adaptive and is decided by the complement value. In order to keep the fidelity of the embedded image at same level of source image, a re-adjusting phase is used called handle. The experimental results obtained compared with the existing studies of Wu et al's LSB replacement method based on pixel-value differencing (PVD) in gray images, where the proposed GVADHIA is capable to hide large volume of data and gives better image quality than existing techniques. Real life applications of the proposed technique to authenticate legal document has also been discussed.

Keywords: Steganography, Complement Value (CV), gray image, edges, PVD.

I.INTRODAUCTION

Steganography is the art of hiding information into picture or other media in such a way that no one apart from the sender and intended recipient even realizes that there is hidden information. Steganography or secrete writing is the term applied to any number of processes that will hide a message within an object, where the hidden message will not be apparent to an observer. Digital images are transmitted over popular communication channels such as the Internet. For secured communication image authentication techniques have gained more attention due to its importance for a large number of multimedia applications. Therefore, military, medical and quality control images must be protected from alteration as, such manipulations could tamper the decisions based on these images. To protect the authenticity of multimedia images, several approaches have been proposed which include conventional cryptography [16], fragile and semi-fragile watermarking and digital signatures. Digital watermarking is the process of hiding the watermark imperceptibly in the content. This technique was initially used in paper and currency as a measure of authenticity.

Data hiding [7, 12, 15] in the image has become an important technique for image authentication and identification. Ownership verification [8, 9, 17] and authentication is the major task for military people, research institutes, and scientists. Data hiding primarily refers to a digital watermark which is a piece of information hidden in a multimedia content, in such a way that it is imperceptible to a human observer, but easily detected by a computer. The principal advantage is that the watermark is inseparable from the content. Information security and image authentication has become very important to protect digital image document from unauthorized access. In steganographic [1, 2, 3, 4, 5] applications, the hidden data may be secrete message or secrete hologram or secrete video whose mere presence within the host data set should be undetectable. The data hiding represents a useful alternative to construct hypermedia document or image, which is very less convenient to manipulate. Chandramouli et al. [10] developed a useful method for making such alterations by masking, filtering and transformations of the least significant bit (LSB) on the source image. Dumitrescu et al. [11] constructed an algorithm for detecting LSB steganography. H. H. Pang [14] used hash value obtained from a file name, password and position of header of hidden file. Pavan et al. [13] and Nameer N. EL-Emam [6] used entropy based technique for detecting the suitable areas in the image where data can be embedded with minimum distortion. Ker [18] and C. Yang [19] presented general structural steganalysis framework for embedding in two or more LSBs. H. C. Wu [20] and Cheng-Hsing Yang [21] constructed LSB replacement method into the edge areas using pixel value differencing (PVD). These edge detection techniques used pixel value differencing to distinguish between edge and smooth areas. From recent studies [1, 2, 7, 11, 17, 18, 19, 20, 21] it is obvious that digital data can be effectively hidden in an image with the criteria that the degradation to the host image is imperceptible and it is possible to recover the hidden data under a variety of attack. Most of the approaches including PVD based LSB substitution techniques are not tested on colour images. Moreover, some of them did not considered the principle that the deep coloured edge areas are able to tolerate more changes than light coloured edge areas [18, 19, 20, 21].

The aim of this paper is to present an algorithm that would facilitate gray image authentication using data hiding procedure which embeds data adaptively by considering the concept of human vision, with features of high capacity and low distortion. The GVADHIA emphasizes on information and image protection against unauthorized access and to insert large amount of messages/image data in to the source image for image identification and also to transmit secure message within the image. In our technique the tolerance level of deep blackish edge areas, light gray edge areas and smooth gray areas are incorporated and it can embed large volume of secrete data with maintaining the high quality of stegoimages. All image byte is embedded by LSB substitution method with different numbers of secrete bits, but the number of secrete bits is decided by complement value (CV) of higher order three bits of each image byte. The embedding is not a straight way LSB substitution, rather embedding at even and odd positions in each image byte alternatively among lower part of image byte to misguide the eavesdroppers. In order to increase the quality of stegoimages, and to ensure proper decoding a handle is proposed to re-adjust the pixel values.

Section II of the paper deals with the proposed technique. Results, comparison and analysis are given in section III. Section IV of the paper deals with the real life applications. Conclusions are drawn in section V, References are given in section VI.

II. THE TECHNIQUE

The proposed embedding technique is adaptive LSB substitution based on the idea (CV of higher order three bits of each image byte i.e. complement of ($b_7b_6b_5$)) that edge areas may embed large number of authenticating bits than smooth areas. For any image pixel, each image byte is embedded by k-bits LSB substitution, but the value of k decided by CV of each image byte. Usually, the deep blackish edge areas can tolerate more changes than the smooth areas and light gray edge areas. The value of k will be large in deep blackish area than the light gray area because the intensity value of deep black pixel is less than the light black or gray pixel. In case of deep black pixel higher order bits are mostly zeroes, so, CV of higher three bits are tends to 7 i.e. the values of k is high. In GVADHIA the values of k are divided into two levels namely lower and higher levels. Lower level means tolerable level (allowed to change) and is defined as region R_1 with *l-h* values and the higher level means protected levels (not allowed to change) and is defined as region R2 with *l-h* values. Fig. 1 shows the division of ranges, range R_1 = [0, 4] and range R_2 = [5, 7]. The lower division means that image byte with complement values k falling into the region R_1; will be embedded by k bits LSB substitution techniques.

Lower or tolerable levels	Higher or protected levels
R_1 = [0, 4]	R_2 = [5, 8]

Figure 1: Region division in each byte of image

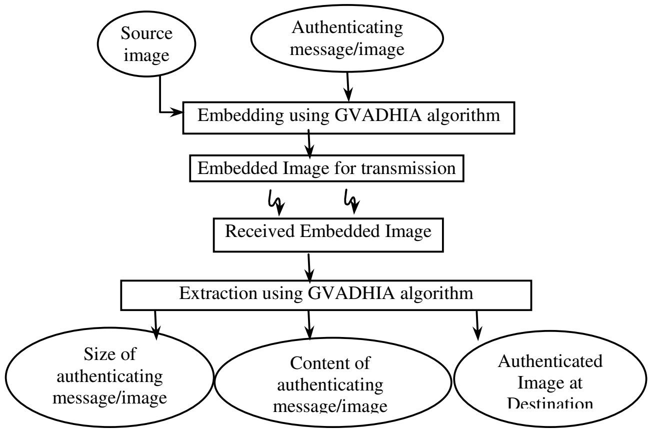
Source image
Authenticating message/image
Embedding using GVADHIA algorithm
Embedded Image for transmission
Received Embedded Image
Extraction using GVADHIA algorithm
Size of authenticating message/image
Content of authenticating message/image
Authenticated Image at Destination

Figure 2: Schematic diagram of GVADHIA algorithm.

The higher division means that image byte with complement values k falling into R_2 then set the value of k = 4 i.e. 4 bits of authenticating message/image can be embedded in each byte of source image. As a result higher order bits are remains unchanged. Here the range of *l-h* values means that CV of an image byte falling in R_1 or in R_2, which indicates that the entire embedding process will be done by *l*-bits to *h*-bits authenticating data i.e. any one cover image byte can be authenticated by any number of secrete bits which is belongs to least value *l* and highest value *h* i.e. $l \le k \le h$. Since the deep gray edge areas can tolerate maximum changes, the proper relation of *l* and *h* in fig. 1 is $l \le h$. In order to improve fidelity of the steogimages, a handle has been applied on embedded image byte. The procedure of this handle is to increase or decrease the most-significant-bit (MSB) part by 1 for reducing the square error between the original pixel and embedded pixel. MSB part i.e. unaltered part, increased or decreased by 1 if the embedded image byte decreased or increased by amount 2^k where k-1 is the highest embedding bit position in each image byte.

A. *Algorithm for Insertion*

Source images represented in 8 bits gray components. The proposed GVADHIA technique embeds authenticating message/image $AI_{p,q}$ along with the size of authenticating message/image (16 bits) for the purpose of authentication of the source image $SI_{m,n}$ of size m x n bytes. The first step in GVADHIA involves reading an image byte in row major order and finds out the complement value (CV) of higher order three bits to find out the ability of embedding of this image byte in terms number of bits. Insert authenticating message/image bits between 1st to 4th positions from LSB of the byte. To enhance the security of authentication process the proposed GVADHIA uses even and odd position embedding strategy alternatively for consecutive image byte in such a way that, if the value of k is 1 then secret bit will be embedded at LSB of an image byte and for the values of k = 2, 3, 4 the secrets bits are embedded within 2-bits, 3-bit, and 4-bits from LSB respectively but embedding will start from even or odd position alternatively and during this process if adequate positions are not available to replace k bits in even or odd positions of LSB part, unaltered bits positions from LSB are used. The detailed embedding steps of GVADHIA are as follows.

Steps:

1. Obtain the size of the authenticating message/image (16 bits representation)
2. For each source image byte do
   - Calculate the complement value CV_i for upper three bits of image byte, say P_i, i.e. CV_i = complement of MSB part of P_i (i.e. CV of ($b_7b_6b_5$)).
   - Find the region where CV_i belong to. Let k = CV_i, if CV_i belongs to R_1 otherwise k = 4 (i.e. highest value of R_1) if CV_i belongs to R_2.
   - Calculate the decimal value of original k bits from LSB of image byte say, K. Embed k bits secrete bits into Pi by k-bit LSB substitution method. Let EP_i be the embedded image byte of P_i. The decimal value of k secrets bits from LSB is K_1, say.
   - Execute handle on EP_i. Calculate the revised complement value CV_i' using same technique i.e. CV_i' = complement of $b_7b_6b_5$. The handle is used as follows.

$$EP_i = \left[\begin{array}{l} \left(EP_i + 2^k\right), \text{ If } CV_i = CV_i' \text{ and if } -(2^k - 1) \le (K_1 - K) \le -2^{k-1} \\ \left(EP_i - 2^k\right), \text{ If } CV_i = CV_i' \text{ and if } (2^k - 1) \ge (K_1 - K) \ge 2^{k-1} \end{array}\right.$$

If the any one above relation is not satisfied the handle is not be executed on EPi.

3. Repeat step 2 for the whole authenticating message/image content and along with the size of the authenticating data.

4. Stop.

For example source image bytes $P_i = 112_{10} = 01110000_2$ and $P_{i+1} = 143_{10} = 10001111_2$ and secrete data $S_d=11010010_2$. First complement values are calculated by CV_i = complement of upper three bits ($b_7b_6b_5$) of P_i = ~ 011=100 = 4 and CV_{i+1} = complement of upper three bits of P_{i+1} = ~ 100 = 011 = 3. As CV_i = 4 and CV_{i+1} = 3 the image bytes P_i and P_{i+1} are embedded by 4 bits and 3 bits LSB substitution in even and odd position alternatively for successive image byte respectively (if the n number of even positions are not available within a image byte, after embedding at even positions of image byte then start embedding at unaltered position from LSB for remaining bits and similar technique is applicable for odd positions in successive image byte) and have results $EP_i = 0111\mathbf{1110}_2 = 126_{10}$ and $EP_{i+1} = 10001\mathbf{010}_2 = 138_{10}$. Here bold bits are embedded bits i.e. 4 bits in EP_i and 3 bits in EP_{i+1}. After applying the handle the stegoimage bytes becomes $EP_i = 01101110_2 = 110_{10}$ and $EP_{i+1} = 10010010_2 = 146_{10}$.

B. .Algorithm for Extraction

During decoding the embedded image has been taken as the input data and the authenticating message/image and the size of secrete data are extracted data from the embedded image. The process of extracting the embedded message/image is the same as the embedding process with the same traversing order of image byte. The detailed steps of data extracting of GVADHIA are as follows.

Steps:

```
1. Read embedded source image byte in row major order
2. For each embedded image byte do
   • Calculate the complement value on embedded image byte $ECV_i$ for upper three bits of each image byte, say $EP_i$, using $ECV_i$ = complement of MSB part of $EP_i$ (i.e. CV of ($b_7b_6b_5$)).
   • Find the region where $ECV_i$ belong to. Let k = $ECV_i$, if $ECV_i$ belongs to $R_1$ otherwise k = 4 (i.e. highest value of $R_1$) if $CV_i$ belongs to $R_2$.
   • Extract the k-bits of authenticating message/image from embedded image byte in even and odd positions alternatively, in the same manner as secrete data were embedded.
   • Replace extracted bit positions in each embedded image byte by '1'.
3. For each 8 (eight) bits of extracting data, construct one alphabet/one image byte.
4. Repeat steps 1 and 2 to complete decoding as per size of the authenticating message/image.
5. Stop.
```

The embedding example shown in the previous subsection is extracted here, for this embedded image $EP_i = 01101110_2$ and $EP_{i+1} = 10010010_2$, the complement value ECV_i = complement of higher order three bits of EP_i = ~ 011 = 100 = 4. Therefore 4 bits embedded in EP_i, thus secrete bits 1101_2 can be extracted from EP_i. And for ECV_{i+1} = complement of higher order three bits of EP_{i+1} = ~ 100 = 011 = 3. Therefore 3 bits embedded in EP_{i+1}, thus secrete bits 001_2 can be extracted from EP_{i+1}.

III.RESULT, COMPARISON AND ANALYSIS

In this section we present some experiments to demonstrate the performance of proposed adaptive data embedding approach. The comparative study has been made on several images using the proposed GVADHIA technique. 50 PPM benchmark [23]

Figure 3a. Source image Peppers

Figure 3b. Source image Airplane

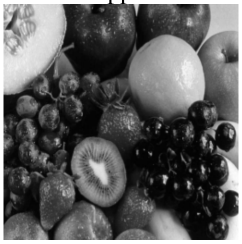
Figure 3c. Source image Fruits

Figure 3d. Source image Lenna

Figure 3e. Authenticating image Earth

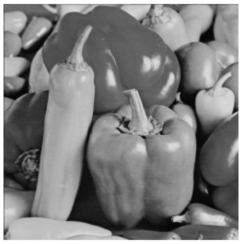
Figure 3f. Embedded image Peppers

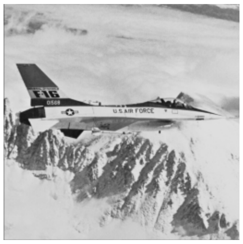
Figure 3g. Embedded image Airplane

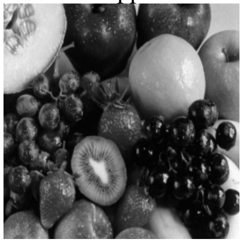
Figure 3h. Embedded image Fruits

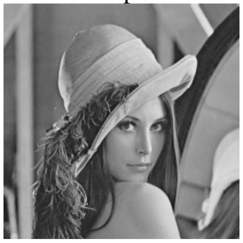
Figure 3i. Embedded image Lenna

Figure 3l. Magnified Embedded image

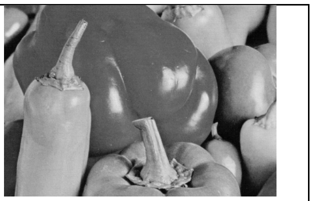

Figure 3m. Magnified Embedded image

Figure 3. Comparison of fidelity in embedded 'Peppers', 'Airplane', 'Fruits' and 'Lenna' images using GVADHIA

Figure 3j. Magnified Embedded image

Figure 3k. Magnified Embedded image

cover gray images with size 512 × 512 are used in the GVADHIA for experiment and four of them Peppers, Airplane, Lenna and Fruits are shown Fig. 3a, 3b, 3c and 3d. Here the gray image 'Earth' shown in Fig. 3e is used to authenticate carrier source images. Authentication is done in 0-4 bits embedding process. The mechanism is defined as l-h (l-least number of bits, h- highest number of bits) process, where k number of bits may be inserted in each image byte and the range of k is defined as l ≤ k ≤ h. Experimental results of stegoimages with 0-4 bits embedding are shown in Fig. 3f, Fig. 3g and Fig. 3h, Fig. 3i respectively. Fig. 3j, Fig. 3k, Fig. 3l, and Fig. 3m are showing the magnified version of different embedded images. From the magnified version of different images it is very difficult to identify the presence of secrete data in the carrier images. To measure the image quality we use peak signal-to-noise ratio (PSNR), Image Fidelity (IF) and Mean Square Error (MSE).

Different experimental results using various l-h ranges are given in Table I. Table I shows that noticeable amount of secrete data embedding is done with higher PSNR values. In 0-4 bits embedding process, the average embedding capacities is 95640 bytes with high PSNR values 38.33 and higher average IF values 0.999829 where average MSE is very minimum which is 3.865820. Table II shows the comparisons between GVADHIA, Wu et al.'s method in which GVADHIA uses a 0-4 bits embedding. Though the change of pixel in flat gray image is more sensitive than the change of pixel in gray image, the GVADHIA embeds more or similar amount secrete data than the existing methods with higher PSNR values. Wu et al.'s methods is developed and experimented on gray images, where GVADHIA method is implemented and experimented also on gray images. The average capacity of Wu et al.'s is 94829 bytes and the average PSNR value is 34.87. From Table II, it is clear that not only the capacity of GVADHIA is more but also it ensures better image fidelity. On average, GVADHIA with 0-4 bits insertion obtains 811 bytes more than Wu et al.'s method. Also PSNR value increases by 3.46 dB on average.

Table I
Capacities and PSNR, IF, and MSE in STHVSDTCI on three bits Embedding

Source images	Capacity (byte), 0-4	PSNR In dB	IF	MSE
Sandiego	96751	39.15	.999890	3.061100
Sailboat	93835	37.01	.999808	3.820600
Woodlad	97751	37.91	.999843	3.750128
Baboon	99187	36.65	.999777	4.270672
Airplane	95961	41.46	.999948	2.838267
Peppers	101699	36.09	.999726	4.549587
Fruits	82329	44.53	.999957	3.823644
Splash	97521	36.27	.999758	4.187430
Oakland	93844	37.68	.999809	4.086103
Lenna	97520	36.56	.999777	4.270672
Average	95640	38.33	0.999829	3.865820

Table II.
Comparisons of results of GVADHIA with WU et al.'s methods

Source Images	Wu et al. 's		**GVADHIA**	
	Capacity	PSNR(dB)	**Capacity**	**PSNR(dB)**
Peppers	96279	35.34	**101699**	**36.09**
Lenna	95754	36.16	**97520**	**36.56**
Baboon	89730	32.63	**99187**	**36.65**
Sailboat	94596	33.62	**93835**	**37.01**
Airplane	97788	36.60	**85961**	**41.46**
Average	94829	34.87	**95640**	**37.55**

IV.REAL LIFE APPLICATIONS OF GVADHIA

Stamp Document	Legal Document
We are Indian. We are proud for our country. We always like to look ahead with positive attitude and giving maximum effort to growth our country. We are so much strong in science and Technology.	We are Indian. We are proud for our country. We always like to look ahead with positive attitude and giving maximum effort to growth our country. We are so much strong in science and Technology.
Nabin Ghoshal	Nabin Ghoshal
Cont.…	Cont.…
Fig. 4a: Signed Document	Fig. 4b: Legal Document

Figure 4: Comparison of fidelity in embedding signature and MD in stamp image using GVADHIA

The proposed technique GVADHIA is applicable in legal document authentication (like passport, agreement copy, title deed etc.). In this aspect, GVADHIA generates message digest MD of length 128 bits from text part of the legal document and embeds it into stamp image as proof of document authenticity. Any change of document the generated message digest MD will differ from the original one which has been generated during the process of authentication, as a result fraud document can be identified. The signature of genuine document holder at the end of the document is also fabricated as an authenticating image using same principle. In the wide range of application of GVADHIA is achieved better robustness and imperceptibility. The strength in embedding is high without changing visible property. Fig. 4 shows the legal document authentication process. Fig. 4a is the stamped signed document. Fig. 4b is the authorized image. Here stamp is considered as a cover image and text part of the document and signature are authenticating data.

V. CONCLUSIONS

The proposed technique is a novel attempt to implement image authentication in spatial domain using adaptive data hiding method to embed secrete data into gray images without making a perceptible distortion. Image bytes located in deep black edge areas are embedded by k-bits LSB substitution method in even and odd positions in each image byte alternatively in successive bytes with a large value of k than that of image bytes located in smooth areas. The CV approach is used to distinguish deep black areas and smooth gray areas. GVADHIA may hide huge amount of data in the form of text message/image. The proposed algorithm shows better results than Wu et al.'s method, which may produce better authenticated images. The l-h bits insertion may yields higher capacity and higher PSNR. The higher image fiedality and low mean square error indicating it is robust and difficult to identify the existance of secrete message/image. For further extension it can be implemented to colour image authentication.

VI. ACKNOWLEDGEMENTS

The author expresses the deep sense of gratitude to the Dept. of Computer Sc. and Engg. & Department of Engineering and Technological studies, University of Kalyani, West Bengal, India, where the work has been carried out.

VII. REFERENCES

[1] N. Ghoshal, J. K. Mandal, A Novel Technique for Image Authentication in Frequency Domain using Discrete Fourier Transformation Technique (IAFDDFTT), Malaysian Journal of Computer Science, ISSN 0127-9094, Vol. 21, No. 1, 2008pp, 24-32.

[2] N. Ghoshal, J. K. Mandal, A Bit Level Image Authentication / Secrete Message Transmission Technique (BLIA/SMTT), Association for the Advancement of Modelling & Simulation Technique in Enterprises (AMSE), AMSE journal of Signal Processing and Pattern Recognition, ISSN 1240-4543, Vol. 51, No. 4, 2008, pp. 1-13.

[3] N. Ghoshal, A. Sarkar, D. Chakraborty, S. Ghosh J. K. Mandal, Masking based Data Hiding and Image Authentication Technique (MDHIAT), Proceedings of 16th International Conference of IEEE on Advanced Computing and Communications ADCOM-2008, ISBN: 978-1-4244-2962-2, December 14-17th, Anna University, Chennai, India, URL:- http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4760437&tag=1, 2008, pp. 119-122.

[4] N. Ghoshal, J. K. Mandal, A. Sarkar, D. Chakraborty, S. Ghosh, Image Authentication by Hiding Large Volume of Data and Secure Message Transmission Technique using Mask (IAHLVDSMTTM), Proceedings of IEEE International Advanced Computing Conference IACC'09, ISBN: 978-981-08-2465-5, March 6-7th, Thapar University, Patiala, India, URL:- http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04809168, 2009, pp. 3177-3188.

[5] R. Radhakrishnan, M. Kharrazi, N. Menon, Data Masking: A new approach for steganography, Journal of VLSI Signal Processing, Springer, Vol. 41, 2005, pp. 293-303.

[6] N. N. EL-Emam, Hiding a large Amount of data with High Security Using Steganography Algorithm, Journal of Computer Science ISSN 1549-3636, vol. 3, no. 4, 2007, pp. 223-232,.

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

[8] B. Chen and G. W. Wornnel, Quantization index modulation: A class of provably good methods for digital watermarking and information embedding, IEEE Trans. On Info. Theory, vol. 47, no. 4, May 2001, pp. 1423-1443.

[9] C.Y. Lin and S. F. Chang, A robust image authentication method surviving JPEG lossy compression, Proc. SPIE, vol. 3312, San Jose, Jan. 1998, pp. 296-307.

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

[11] S. Dumitrescu, W. Xiaolin and Z. Wang, Detection of LSB steganography via sample pair analysis, IEEE Trans. on Signal processing, Vol. 51, no. 7, 2003, pp. 1995-2007.

[12] P. Moulin and J. A. O'Sullivan, Information-theoretic analysis of information Hiding, IEEE Trans. On Info. Theory, vol. 49, no. 3, March 2003, pp. 563-593.

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

[14] H. H. Pang, K. L. Tan and X. Zhou, Steganographic schemes for file system and B-tree, IEEE Trans. On Knowledge and Data Engineering, vol. 16, Singapore June 2004, pp. 701-713.

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

[16] C. Rechberger, V. Rijman and N. Sklavos, The NIST cryptographic Workshop on Hash Functions, IEEE Security & Privacy, vol. 4, Austria, Jan-Feb 2006, pp. 54-56.

[17] A. H. Al-Hamami and S. A. Al-Ani, A New Approach for Authentication Technique, Journal of computer Science, ISSN 1549-3636, Vol. 1, No. 1, 2005, pp. 103-106.

[18] A. Ker, Steganalysis of Embedding in Two Least-Significant Bits, IEEE Transaction on Information Forensics and Security, ISSN 1556-6013, Vol. 2, No. 1, 2008, pp. 46-54.

[19] C. Yang, F. Liu, X. Luo and B. Liu, Steganalysis Frameworks of Embedding in Multiple Least Significant Bits, IEEE Transaction on Information Forensics and Security, ISSN 1556-6013, Vol. 3, No. 4, 2008, pp. 662-672.

[20] H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, Image steganographic scheme based on pixel-value differencing and LSB replacement methods, Proc. Inst. Elect. Eng., Vis. Images Signal Process., Vol. 152, No. 5, 2005, pp. 611-615.

[21] C. H. Yang, C. Y. Weng, S. J. Wang, and H. M. Sun, Adaptive Data Hiding in edge areas of Images With Spatial LSB Domain Systems, IEEE Transaction on Information Forensics and Security, ISSN 1556-6013, Vol. 3, No. 3, 2008, pp 488-497.

[22] M. Kutter and F. A. P. Petitcolas, A fair benchmark for image watermarking systems, Electronic Imaging '99, Security and Watermarking for Multimedia Content, San Josh CA, vol. 3657, 1999, pp. 226-239.

[23] Allan G. Weber, The usc-sipi image database: http://sipi.usc.edu/services/database/Database.html, October 1997, Signal and Image Processing Institute at the University of Southern California.