International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 4, Number 7 (2014), pp. 777-786

http://www. irphouse.com

Adaptive Edge Steganography for Images

Yambem Jina Chanu[1], Kh. Manglem Singh[2] and Themrichon Tuithung[3]

[1, 3] Dept. of CSE, NERIST, Itanagar,
[2] Dept. of CSE, NIT Manipur,

ABSTRACT

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 detection of the presence of steganography. Steganography can be used for the benefit of the mankind to serve us 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. Newer and more sophisticated steganographic techniques for embedding secret message will require more powerful steganalysis methods for detection. In this paper, an adaptive steganographic technique, which embeds secret message bits in the edges of the image is proposed. The proposed technique has ability to release more edge regions by decreasing pre-defined threshold and some powerful steganalytic techniques fail to detect the hidden message.

Keywords – Steganography; RS technique; Gradient Energy; Histogram Difference; Edge.

1. INTRODUCTION

Steganography refers to the technique of embedding secret messages inside different cover media such as text, audio, image and video without any suspicion. It can be used in many areas. It can be used for the benefit of the mankind to serve us as well as by terrorists and criminals for malicious purposes. The main purpose of steganography is to transmit hidden message embedded in a cover medium in a stealth way that an unauthorized person cannot believe the very presence of the embedded message. 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 [R. Liu et al., March 2002, W. Bender et al., 2000,

J. Fridrich et al., October-November 2001]. 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 [N.F. Johnson et al., 1998] as reported in USA TODAY. Examples are found for hiding data in music files [C. Hosmer, 2000], and even in a simpler form such as in HyperText Markup Language (HTML), executable files and Extensible Markup Language (XML) [J.C. Hermandez-Castro et al., 2006].

The art and science of detection of the existence of embedded message is called steganalysis. In addition to detection of embedded message, the main goal of steganalysis are to estimate the length of embedded message, to estimate the locations of hidden data in the stego data, 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 [N.F. Johnson et al., 1998, H. Wang et al., October 2004, A. Nissar et al., 2010, W. Bender et al., 2000, S. Miaou et al., 2000, U.C. Nirinjan et al., 1998, Y. Li et al., 2007]. 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 never ending. 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 [R. J. Andersonet al., 1998, H. Wang et al., 2004, N. Provos et al., 2003]. This paper proposes a new steganalytic algorithm for LSB image steganography using noncausal linear predictor.

The paper is organized as follows. In Section 2, adaptive steganography is given. Section 3 proposes the new steganaltic algorithm, followed experimental results in Section 4 and conclusions in Section 5.Lastly Section 6 provides the references.

2. ADAPTIVE STEGANOGRAPHY

Spatial steganography, directly change 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 [N.F. Johnson et al., 1998]. To our human eye, changes in the value of the LSB are imperceptible, thus making it an ideal place for hiding information without any perceptual change in the cover object. Embedding of message bits can be done either sequentially or randomly. New algorithms have been emerging in transform domains due to weak resistance in spatial domain, fast development in computing devices and need for better security system. There are many versions of transform steganography. Some popular transform domains are discrete cosine transform (DCT), discrete wavelet transform (DWT) and singular value decomposition (SVD) respectively. JPEG is based on DCT in lossy compression and it is the most common format of images produced by digital cameras, scanners and other photographic capture devices.

Some important requirements of a good steganographic scheme are undetectable, robustness against attacks, embedding capacity and imperceptibility. Adaptive steganography is a special case of the two former techniques and it tries to fulfill at least some or all requirements of a good steganographic scheme.

Manglem et al propose a steganographic technique which embeds message bits in edges of the image, which is found by using Roberts edge detector on every 2×2 non-overlapping block within the cover images [K.S. Manglem et al., 2007]. Some steganalysis tools such as energy gradient steganalysis fail to detect the embedded message in the stego-image.

PVD-based steganographic scheme is another edge adaptive scheme, in which the number of embedded bits is determined by the difference between a pixel and its neighbors [X. Zhang et al., 2004, C.H. Yang et al., 2008]. Larger the difference, the larger the number of message bits that can be embedded.

LSB matching revisited (LSBMR) is another edge adaptive steganography technique, which can release more edge regions for embedding message bits. It can resist some of the steganalytic tools.

The model-based method (MB) generates a stego-image based on a given distribution model, using a generalized Cauchy distribution, which results in minimum distortion. This algorithm can be broken by the first-order difference [R. Bohme et al., 2004].

Chang et al propose an adaptive technique applied to LSB steganographic technique [C.C. Chang et al., 2004]. Their technique exploits the correlation between neighboring pixels to estimate the degree of smoothness.

Raja et al choose to use wavelet transforms that map integers to integers instead of using the conventional wavelet transforms, so as to overcome the difficulty of floating point conversion that occurs after embedding [K.B. Raja et al., 2008]. Their method embeds the message bits in non-overlapping 4×4 blocks of low frequency, where two pixels at a time are chosen, one on either side of the principal axis.

Wu and Shih propose a genetic algorithm (GA) based technique that generates a stego-image to break the detection system by artificially counterfeiting statistical features [Y.T. Wu et al., 2006].

Kong et al propose a content based steganography scheme based on segmenting homogeneous image areas using a watershed method and fuzzy C-means (FCM) [J. Kong et al., 2009]. Four LSBs of each cover image is used to embed secret message bits in the region where entropy is high and two LSBs in low entropy region.

Rakesh et al propose a keyless random steganographic technique that induces enhanced security by incorporating counting out embedding [R. Rakesh et al., 2011]. Their method uses message bits embedded in the current pixel, which acts as a key for the next pixel to which data is to be embedded.

3. PROPOSED TECHNIQUE

The simplest way to hide data on an image is to replace the least significant bits (LSB) of each pixel sequentially in the scan lines across the image in raw image format with the binary data. The portion, where the secret message is hidden is degraded while the rest remain untouched. An attacker can easily recover the hidden message by repeating the process. To add better security, the message may be distributed randomly. This approach may raise suspicion that the image contains the secret message, because the resulting stego-image appears as speckles at the point of message embedding. A better approach is to hide the message in the regions that are least like their neighboring pixels. Such regions contain edges, corners, thin lines, ends of lines, textures etc. with fast varying pixel values. Majority of images contain edges dominantly. An attacker has less suspicion the present of message bits in edges, because pixels in edges appear to be either much brighter or dimmer than their neighbors. Edges from the image can be detected easily by applying the appropriate edge detection filter and many such standard filters are available. For a window of size 2×2 Roberts cross-gradient operator [R. C. Gonzalez et al., 2000] as shown in Fig. 1 has the following form:

$$D = |G_x| + |G_y| \quad (1)$$

where $G_x = x_3 - x_2, G_y = x_1 - x_4$ and x_1, x_2, x_3 and x_4, named as cover bytes are the pixels in the window of size 2×2, scanning from the top left to the bottom right of the image.

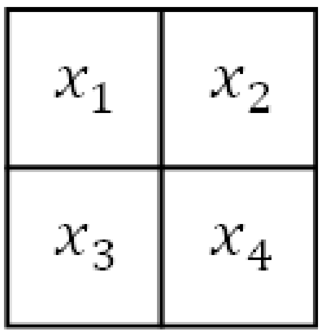

Figure 1. Window of size 2×2 for Roberts edge detection.

A pixel in the window is detected as an edge point if D is bigger than than a pre-defined threshold. For color images, edges should be detected channel-wise. A pixel that is detected as an edge pixel before embedding message bit should be detected as an edge pixel after embedding the message bit and vice versa. The proposed algorithm named as edge steganography (ES) uses LSB embedding algorithm in the edges randomly distributed across the image, depending on the values of $D, G_x, G_y,$ cover bytes x_1, x_2, x_3, x_4 and secret message bit B. The new value of the cover byte after LSB embedding is given by

$$x_1 = \begin{cases} x_1 + 1, & \text{if } D \geq \theta \& G_x \geq 0 \& x_1\%2 = 0 \& B = 1 \\ x_1 - 1, & \text{if } D \geq \theta \& G_x < 0 \& x_1\%2 = 0 \& B = 1 \\ x_1 + 1, & \text{if } D \geq \theta \& G_x \geq 0 \& x_1\%2 = 1 \& B = 0 \\ x_1 - 1, & \text{if } D \geq \theta \& G_x < 0 \& x_1\%2 = 1 \& B = 0 \\ x_1, & \text{Otherwise} \end{cases} \quad (2)$$

where x_1 is the cover byte and θ is a pre-defined threshold. The same equation is used to embed the message bit in x_3 replacing x_1 by x_3 and G_x by G_y. The following equation is used to embed the message bits to the cover bytes x_2 and x_4.

$$x_2 = \begin{cases} x_2 - 1, & \text{if } D \geq \theta \& G_y \geq 0 \& x_2\%2 = 0 \& B = 1 \\ x_2 + 1, & \text{if } D \geq \theta \& G_y < 0 \& x_2\%2 = 0 \& B = 1 \\ x_2 - 1, & \text{if } D \geq \theta \& G_y \geq 0 \& x_2\%2 = 1 \& B = 0 \\ x_2 + 1, & \text{if } D \geq \theta \& G_y < 0 \& x_2\%2 = 1 \& B = 0 \\ x_2, & \text{Otherwise} \end{cases} \quad (3)$$

Truth tables of Eqs. (2) and (3) are shown in Table 1. The value of D remains same for non-edge pixels before embedding and after embedding, but it may increase for edge pixels after embedding the message bit. This is done by either increasing or decreasing the pixel values of edge regions, which ensures to retrieve the message bits correctly from the image at the time of extraction.

Pre-processing is done first before message bits are embedded in the image. The scheme initializes the pre-defined threshold θ, finds the edge regions and checks whether these regions are sufficient to embed the secret message bits. Message bits are embedded if the edge regions are large enough to hold the message bits, otherwise the value of pre-defined threshold is decreased to release more edge regions.

Table 1. Truth table of Equations 2 and 3

	For pixels x_1 and x_3					For pixels x_2 and x_4				
Rule	D	G_x	$x_1\%2$	B	Output x_1	D	G_y	$x_2\%2$	B	Output x_2
1	$D \geq \theta$	$G_x \geq 0$	0	1	$x_1 + 1$	$D \geq \theta$	$G_y \geq 0$	0	1	$x_2 - 1$
2	$D \geq \theta$	$G_x < 0$	0	1	$x_1 - 1$	$D \geq \theta$	$G_y < 0$	0	1	$x_2 + 1$
3	$D \geq \theta$	$G_x \geq 0$	1	0	$x_1 + 1$	$D \geq \theta$	$G_y \geq 0$	1	0	$x_2 - 1$
4	$D \geq \theta$	$G_x < 0$	1	0	$x_1 - 1$	$D \geq \theta$	$G_y < 0$	1	0	$x_2 + 1$

For better security, random edge location is selected to embed message bit by using Arnold cat map [61], which is given below.

$$\begin{bmatrix} X_{i+1} \\ Y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} X_i \\ Y_i \end{bmatrix} \bmod N \quad (4)$$

where (X_{i+1}, Y_{i+1}) is the transformed pixel location of the location (X_i, Y_i), of the image of size $(N \times N)$, a and b are two control parameters, $X_i, Y_i, a, b \in I^+$.

4. EXPERIMENTAL RESULTS

Different color images of such as Lena, Pepper, Kodak, Tiffany, House, Splash, Tulips, Terrain, Airplane and Boat respectively of 512×512 size were used in experimentation. Representative of all images are shown in Figure 2.The proposed algorithm ES shows the ineffectiveness some powerful steganalytic algorithms such RS [J. Fridrich et al., 2002], Gradient Energy (GE) [l. Zhi et al., 2003] and Histogram Difference (HD) [T. Zhang et al., 2003] to extract the hidden message from stego-images.

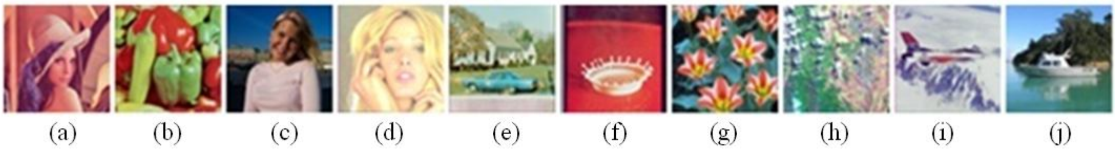

Figure 2. (a) Lena, (b) Pepper, (c) Kodak, (d) Tiffany, (e) House, (f) Splash, (g) Tulips, (h) Terrain, (i) Airplane and (j) Boat.

Table 2. Results of RS algorithm on different images - % Extraction

RS Algorithm										
% Embedding	Lena	Pepper	Kodak	Tiffany	House	Splash	Tulips	Terrain	Airplane	Boat
0	-0.02	-0.56	-0.80	-0.33	-0.19	0.39	-0.00	-2.50	1.52	2.34
10	9.91	10.75	12.11	10.82	10.72	10.51	11.68	12.47	9.08	13.72
20	21.99	19.63	18.33	18.15	19.72	19.35	19.49	19.01	18.49	21.60
30	27.28	29.70	31.07	29.86	30.02	28.23	28.99	30.85	29.73	31.30
40	39.32	40.78	39.36	40.59	39.32	41.31	38.23	37.65	41.12	40.62
50	51.04	49.69	49.93	50.21	50.39	50.19	51.58	48.05	50.02	49.50

Table 3. Results of GE algorithm on different images - % Extraction

GE Algorithm										
% Embedding	Lena	Pepper	Kodak	Tiffany	House	Splash	Tulips	Terrain	Airplane	Boat
0	0.96	-0.35	1.28	-1.99	2.27	-0.92	3.71	21.94	-0.51	2.56
10	9.23	9.94	6.75	8.93	10.88	9.60	13.32	21.23	8.57	6.25
20	19.21	18.93	16.30	19.51	17.12	19.49	18.87	21.58	20.62	21.21
30	26.79	26.75	25.15	25.07	24.88	27.98	27.48	19.99	28.41	28.43
40	35.12	39.81	31.14	40.82	38.16	38.63	37.79	19.87	39.42	46.02
50	48.11	49.34	46.48	46.23	50.80	47.97	45.29	20.95	47.03	41.99

Table 4. Results of HD algorithm on different images - % Extraction

HD Algorithm										
% Embedding	Lena	Pepper	Kodak	Tiffany	House	Splash	Tulips	Terrain	Airplane	Boat
0	-0.96	-2.38	-4.82	-5.93	2.80	--3.69	0.15	-3.71	-2.39	-4.37
10	10.27	11.00	13.18	16.41	11.71	9.68	7.72	11.86	10.99	12.54
20	22.25	23.09	26.20	28.31	21.68	24.82	21.47	25.22	21.49	25.33
30	29.74	30.55	33.21	33.01	29.55	30.98	32.49	31.37	31.04	32.31
40	37.98	39.37	38.52	36.87	38.26	40.67	40.45	38.41	40.01	39.13
50	50.70	48.35	43.68	41.30	45.98	47.53	47.69	46.83	48.84	45.05

Table 5. Results of RS algorithm on different images - % Extraction

RS Algorithm										
% Embedding	Lena	Pepper	Kodak	Tiffany	House	Splash	Tulips	Terrain	Airplane	Boat
0	-0.02	-0.56	-0.80	-0.33	-0.19	0.39	-0.00	-2.50	1.52	2.34
10	1.03	-3.11	-17.94	-0.36	0.59	0.13	-0.66	-1.81	1.96	1.57
20	1.50	-2.82	-17.03	1.29	0.28	0.39	0.46	-1.37	2.16	1.64
30	2.60	-3.03	-16.38	2.26	-0.24	0.17	1.69	-1.62	2.99	1.55
40	2.44	-2.88	-15.68	2.50	-0.36	1.01	2.18	-1.42	3.26	1.67
50	2.35	-1.60	-14.94	2.44	0.09	1.66	2.98	-0.89	4.09	1.53

Table 6. Results of GE algorithm on different images - % Extraction

GE Algorithm										
% Embedding	Lena	Pepper	Kodak	Tiffany	House	Splash	Tulips	Terrain	Airplane	Boat
0	0.96	0.35	0.35	-1.99	2.27	-0.92	3.71	21.94	-0.51	2.56
10	0.69	-8.52	-8.52	-55.42	-18.69	-35.36	-0.95	20.17	-23.78	-35.94
20	1.85	-9.14	-9.14	-47.89	-17.71	-34.73	-0.92	18.16	-21.85	-35.72
30	3.10	-10.65	-10.65	-37.35	-14.57	-33.23	-0.15	17.33	-20.39	-33.83
40	5.05	-12.55	-12.55	-28.85	-15.62	-31.61	0.36	15.79	-20.21	-29.58
50	5.93	-13.49	-13.49	-21.49	-14.45	-30.52	0.30	13.93	-15.66	-33.93

Table 7. Results of HD algorithm on different images - % Extraction

HD Algorithm										
% Embedding	Lena	Pepper	Kodak	Tiffany	House	Splash	Tulips	Terrain	Airplane	Boat
0	-0.96	-2.38	-4.82	-5.93	2.80	--3.69	0.15	-3.71	-2.39	-4.37
10	-0.80	-1.96	-4.64	-6.01	2.20	-3.52	-15.09	-5.77	2.16	-4.70
20	-0.59	-1.87	-5.10	-5.95	2.74	-3.69	-14.68	-8.28	-2.75	-4.51
30	0.43	-1.82	-5.56	-5.86	2.23	-3.69	-16.53	-11.98	-2.4	-4.96
40	0.02	-1.72	-6.02	-5.83	1.44	-3.87	-16.75	-15.08	-1.9	-5.32
50	0.12	-1.62	-6.48	-5.77	1.67	-4.22	-16.17	-18.46	-1.90	-5.50

Tables 2, 3 and 4 show the effectiveness of popular steganalytic algorithms such as RS, GE and HD in extracting hidden message from different stego-images embedded with 10% to 50% in LSB regions of images by using LSB embedding technique. The results show that these steganalytic techniques could extract the hidden message, and among them RS technique could extract with less error in extraction.

Tables 5, 6 and 7 show the ineffectiveness of these steganalytic techniques from the different stego-images embedded with 10% to 50% in edge regions of images by using the proposed techniques. The results show that these steganalytic techniques could not extract the hidden message from the stego-images.

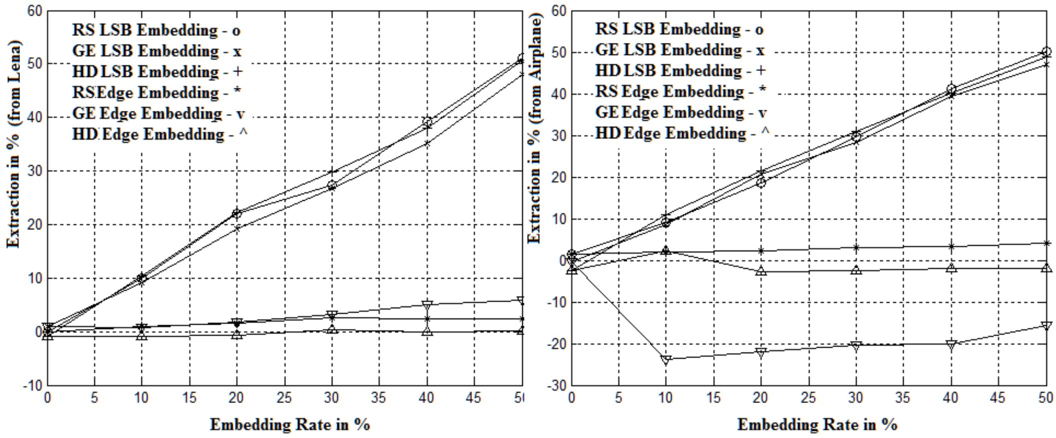

Figure 3. Extraction of hidden message from Lena and Airplane images

Fig. 3 is the graphical plot that shows the inability of RS, GE and HD techniques in extraction of hidden message from stego-images of Lena and Airplane images. It clearly shows that these popular LSB steganalytic techniques, though are powerful to extract hidden message bits accurately from stego-images embedded message bits in LSB positions of images, fail to extract the hidden message bits from the edge regions of stego-images.

5. CONCLUSIONS

The paper proposes a steganographic algorithm, which embeds message bits in the edge pixels of the image that are detected as edge regions by edge detector. It finds impossible for some popular LSB steganalytic algorithms such as RS, GE and HD to detect the presence of message bits in the edge regions. The proposed algorithm has ability to release more edge regions to increase the capacity of embedding algorithm by decreasing the pre-defined threshold.

REFERENCES

[1] A. Nissar and A.H. Mir(2010), Classification of steganalysis techniques: A study, Elsevier Digital Signal Processing, vol. 20, pp. 1758-1770.

[2] C.C. Chang, P. Tsai and M.H. Lin (2004), An adaptive steganography for index-based image using codeword grouping, Advances in Multimedia Information Processing-PCM, Springer, vol. 3333, pp. 731-738.

[3] C. Hosmer(2000), Discovering hidden evidence, Journal of Digital Forensic Practice, vol.1, pp. 47-56.

[4] C.H. Yang, C.Y. Weng, S.J. Wang, H.M. Sun (September 2008), Adaptive data hiding in edge areas of images with spatial LSB domain system, IEEE Transaction Inf. Forensic Security, vo. 3, no. 3, pp. 488- 497.

[5] H. Wang and S. Wang (October 2004), Cyber warfare Steganography vs Steganalysis, ACM Commun. vol. 47, pp. 76-82.

[6] http://mathworld.woffram.com/arnoldsCatMap.html

[7] l. Zhi, S.A. Fen and Y. Xian (September 2003), A LSB steganography detection algorithm, Proc. of IEEE Symposium on Personal Indoor and Mobile Radio Communication, vol. 3, pp. 2780-2783.

[8] J.C. Hermandez-Castro, I. Blasco-Lopez, J.M. Estevez-Tapaidor(2006), Steganography in games: A general methodology and its application of the Game of Go, Elsevier Science Computers and Security, vol. 25, pp. 64-71.

[9] J. Fridrich and M. Golan and R. Du (October-November 2001), Detecting LSB steganography in color and gray-scale images, IEEE Multimedia Magazine, Special Issue on Security, pp. 22-28.

[10] J. Fridrich, M. Goljan and D. Hogeg (2002), Steganalysis of JPEG images breaking the F5 algorithm, Proc. Information Hiding, 5^{th} International Workshop, IH 2002, Noordwijkerhout, The Netherlands, Lecture Notes in Computer Science, October 7-9, 2578/2003, pp. 310-323.

[11] J. Kong, H. Jia, X. Li, Z. Qi (January 2009), A novel content-based information hiding scheme, Proc. On International Conference on Computer Engineering and Technology, vol. 1, pp. 436-440.

[12] K.B. Raja, S. Sindhu, T.D. Mahalakshmi, S. Akshatha, B.K. Nithin, M. Sarvajith, K.R. Venugopal, I.M. Patnaik (6-8 January 2008), Robust image adaptive steganography using integer wavelets, Proc. on 3^{rd} International Conference on Communication Systems Software and Middleware and Workshops, COMSWARE'08, pp. 614-621.

[13] K.S. Manglem, S.S Birendra and L.S. Shyamsundar (April 2007), IJCSNS International Journal of Computer Science and Network Security, vol.7, no.4, pp. 302-307.

[14] N.F. Johnson and S. Jajodia(1998), Exploring steganography, : seeing the unseen, IEEE Computer, vol. 31, no. 2, pp. 26-34.

[15] N. Provos and P. Honeyman (2003), Hide and seek: An introduction to steganography, IEEE Security and Privacy, vol. 1, no. 3, pp. 32-44.

[16] R. Bohme and A. Westfeld (13 September 2004), Breaking Cauchy model-based JPEG steganography with first order statistics, Proc. European

Symposium on Research in Computer Security, Lecture Notes in Computer Science, vol. 3193, pp. 125-140.

[17] R. C. Gonzalez and R. E. Woods (2000), Digital Image Processing, Prentice Hall of India.

[18] R. J. Anderson and F.A.P. Pettitcolas (1998), On the limits of steganography, IEEE Journal on Selected Areas in Communication, vol. 16, no. 4, pp. 474-481.

[19] R. Liu and T. Tan (March 2002), An SVD watermarking scheme for protecting rightful ownership, IEEE Trans. on Multimedia, vol. 4, no. 1, pp. 121-128.

[20] R. Rakesh, S. Devathi, P. Sekhar, C. Sekharan, B. Surendra and K. Tatikonda (June 2011), Message guided adaptive random steganography using counting-out embedding, IJCA, vol. 24, no. 6.

[21] S. Miaou, C. Hsu, Y. Tsai, and H. Chao (July 2000), A secure data hiding technique with heterogeous data-combining capability for electronic patient records, Proc. of 22nd IEEE EMBS, pp. 280-283.

[22] T. Zhang and X.Ping (April 2003), 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.

[23] U.C. Nirinjan, and D. Anand (29 October – 1 November 1998), Watermarking medical images with patient information, Proc. of 20th IEEE International Conference of Biological Society, pp. 703-706.

[24] W. Bender, W. Butera, D. Gruhl, R. Hwang, F.J. Paiz, S. Pogreb (2000), Applications of data hiding, IBM Systems Journal vol. 39, no. 3 & 4, pp. 547-568.

[25] X. Zhang and S. Wang (2004), Vulnerability of pixel value differencing steganography in histogram analysis and modification for enhanced security, Pattern Recognition Letters, vol. 25, pp. 331-339.