IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol-6, Special Issue-4, May 2018 E-ISSN: 2347-2693

Lossless Data Hiding Based on Adjacency Pixel Differences

S. Lakshmanan[1], M. Mary Shanthi Rani[2*]

[1,2*] D Department of Computer Science and Applications, The Gandhigram Rural Institute - Deemed to be University, Gandhigram,Dindigul, Tamilnadu - 624 302

[*]*Corresponding Author: m.maryshanthirani@ruraluniv.ac.in, Tel.: 0451- 2452371*

Available online at: www.ijcseonline.org

***Abstract*—** Image steganography has become a vibrant research area due to increase in digital image transmission over untrusted network. Generally, after recovering the hidden data from a stego image, the host image data cannot be reconstructed perfectly. This is a main challenge for applications demanding lossless host image recovery. In this paper, a new lossless reversible data hiding technique is proposed based on differences of adjacent pixels for embedding data and has more hiding capacity compared to existing methods. The number of hiding bits that can be embedded into an image equals the number of pixels related with the peak point. The performance of the algorithm has been evaluated with hiding capacity and peak signal to noise ratio (dB). The experimental results show that the host image and hidden information can be exactly retrieved from the stego image.

***Keywords*—**Reversible data hiding, Lossless reconstruction, Information security

I. Introduction

Information security is the process of protection against the unauthorized use of information. Steganography and Cryptography are two popular techniques in information security. Steganography is that the apply of concealing a file, message, image, or video inside another file, message, image, or video and the Cryptography is a technique of storing and communicating data in a specific form so that only those for whom it is intended can read and process it. Due to information hiding, however, some persistent distortion may occur and hence the original cover medium may not be able to be retrieved exactly after the hidden data have been extracted. Similar to the categorisation of data compression algorithms, this type of data hiding algorithms can be stated to as lossy data hiding. Among three major classes of data hiding algorithms, in the most popularly used spread-spectrum watermarking techniques, either in DCT domain [1] or DCT domain [2], round-off error and/or truncation error may take place during data embedding. As a result, there is no way to reverse the stego-media back to the original or host without distortion. For the least significant bit-plane (LSB) embedding methods, the bits in the LSB are substituted by the data to be embedded and the bit-replacement is not memorized. Consequently, the LSB method is not reversible. With the third group of frequently used watermarking techniques, called quantization index modulation (QIM) [3], quantization error renders lossy data hiding.

On the other hand, reversible data hiding algorithms are able to recover both the hidden data and stego medium without loss. They can be categorized as fragile authentication and semi-fragile authentication. Semi-fragile authentication, allows some minor modification, say, compression within a reasonable extent, while fragile authentication, does not allow any modification to stego-media, with compression. Some reversible data hiding algorithms developed at the initial stage belong to fragile authentication. The embedding capacity of fragile authentication is not large, normally between 1k to 2k bits. As a result, the amount of hidden data is rather limited and may not be suitable for applications such as covert communications and medical data systems. For multimedia, content-based authentication makes more sense than representation based authentication. Hence, research has been triggered towards developing high embedding capacity methods.

II. Related Work

Honsinger et al patent in 2001 [3] explains in detail a reversible data hiding technique used for fragile authentication. The method is carried out in the image spatial domain by using modulo-256 addition which avoids the issue of overflow (grayscale values above its upper bound) and underflow (grayscale values above its lower bound).

Goljan et al [4] developed a reversible technique, known as R-S scheme, which is suitable for the objective of having high data embedding capacity. A difference expansion scheme was proposed by Tian [5], which has the performance of reversible data hiding in terms of data embedding capacity versus PSNR of marked (or) stego images with respect to host images.

M. Mary Shanthi Rani et.al (2016) [6] developed a method for secure communication by combining the concepts of Steganography and QR codes. This method has two stages: (i) Encrypting the data by a QR code encoder and thus generating a QR code (ii) Hiding the QR code inside a colour image.

A novel method has been reported in [7] in which DWT (Discrete Wavelet Transform), DCT (Discrete Cosine Transform) and IWT (Integer Wavelet Transform) are used to hide secret information within a video file.

In 2008, K. A. Navas, et.al presented Electronic Patient Report (EPR) data hiding for telemedicine [8]. This article deals with novel blind and reversible data hiding technique in ROI images using integer wavelet transform and it particularly focused on medical images.

M. Mary Shanthi Rani et.al [9] has developed a new approach for data hiding with compression in medical images. In this method, information is hidden at the border of ROI of the image by applying specific conditions for embedding.

M. Mary Shanthi Rani et al (2017) [10] proposed to hide the data in both Region of Interest (ROI) and Non Region of Interest (NROI) of medical images using LSB technique and recover the data as well. C Nagaraju et.al [12] developed embedding patient information in Electrocardiogram which is further encrypted to ensure better security in spatial domain.

Mohit Gupta et al. (2012) [13] proposed to encode the secret message before embedding in order to increase the capacity of the data hiding system. The main advantage of this method is that at the time of extraction there is no requirement of the original cover image which increases the security of the proposed steganography system.

Mary Shanthi Rani et.al [14] has developed a method for hiding stego images using the Visual Cryptography (VC) shares which are insignificant and robust to Steganalysis tools.

Anupriya Sohal et al. (2015) [16] proposed a new Steganography technique for hiding the information using DWT (Discrete wavelet transform) and back propagation neural network. DWT converts the image into WT (Wavelet transform), from which LSB positions are calculated which are further classified using neural network. Training of different images is done to calculate effective values of LSB.

Divya et.al [17] proposed to apply optimization to hide the secret data messages effectively within cover images to ensure more hiding capacity, good security, distortion less transmission and effective recovery of the hidden messages. The optimization scheme is Particle Swarm Optimization that provides the best pixel positions in the cover image that can be used to embed the secret message bits so that less image distortion occurs.

P.Thiyagarajan et.al [19] proposed design based 3D Image steganography in which they test the various attacks such as cropping, rotation, scaling etc.

Several methods have been proposed which hide data in video frames both in spatial and frequency domain as well [20, 21].

III. METHODOLOGY

The proposed method exploits the inherent property of all images (i.e) high correlation between neighbouring pixels. The pixels are read in spiral order as shown in Figure 1 and the pixel differences (D) between neighbouring pixels are calculated which are very close to zero. The peak point is the pixel difference that has the highest frequency of occurrence among the pixel differences. This frequency determines the data hiding capacity and data is hidden using histogram modification.

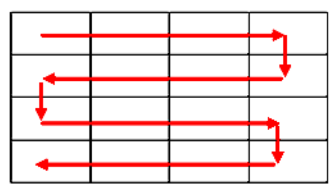

Figure 1. S-Order

The algorithm for histogram modification based on pixel differences is given below.

Algorithm for Embedding Message bits in Grayscale Images

Let us consider grayscale image G with N number of pixels. Let G_i and GG_i denote the grayscale values of i^{th} pixel, before and after modification respectively.

1. Read the image and convert into a vector (G) in S-order as shown in figure 1.
2. Compute the pixel difference D_i between the pixel G_i and G_{i-1} using equation(1)

$$D_i = \begin{cases} G_i & \text{if } i = 0 \\ |G_{i-1} - G_i|, & \text{otherwise} \end{cases} \quad .....(1)$$

3. Determine the peak point P from the pixel differences using equation(2)

$$P = D_i \quad .....(2)$$

For which f(Di) is maximum among all pixel difference. f(Di) is the frequency of occurrence of Di.

4. If Di>P then shift each pixel by 1 using equation(3)

$$GG_i = \begin{cases} G_i & if\ i = 0\ or\ D_i < P \\ G_i + 3,\ if\ D_i > P\ and\ G_i \geq G_{i-1} \\ G_i - 3,\ if\ D_i > P\ and\ G_i < G_{i-1} \end{cases} \quad .....(3)$$

5. If D_i=P, modify the pixel G_i according to the hidden message bits B [0, 1]. In this case, B may take a value from the set {(00),(01),(10),(11)}.

$$GG_i = \begin{cases} G_i + B, if\ D_i = P\ and\ G_i \geq G_{i-1} \\ G_i - B, if\ D_i = P\ and\ G_i < G_{i-1} \end{cases} \quad .....(4)$$

Message bits of B are embedded by adding/subtracting its decimal equivalent to LSB of pixel value. The stego image is thus created by executing the above steps for all the pixels G_i, $1 \leqslant i \leqslant N$.

Recover the hidden data and original medical image

The Stego image is read in the same order as done in the embedding process. The extraction and reconstruction of the original image is done by executing following steps and using equations 5 and 6.

Algorithm for Extraction

1. The message bit B can be extracted from:

$$B = \begin{cases} 0,\ if\ \ |GG_i - G_{i-1}| = P \\ 1,\ if\ \ |GG_i - G_{i-1}| = P + 1 \\ 2,\ if\ \ |GG_i - G_{i-1}| = P + 2 \\ 3,\ if\ \ |GG_i - G_{i-1}| = P + 3 \end{cases} \quad .....(5)$$

2. The Pixel values A_i of the original image can be reconstructed by using equation(5)

$$R_i = \begin{cases} GG_i + 3,\ if\ \ |GG_i - G_{i-1}| > P\ and\ GG_i < G_{i-1} \\ GG_i - 3,\ if\ \ |GG_i - G_{i-1}| > P\ and\ GG_i > G_{i-1} \\ GG_i, \quad otherwise \end{cases} \quad .....(6)$$

An example of embedding and extraction process

Let G be the part of an original image as shown below

$$G = \begin{bmatrix} 200 & 201 & 202 & 204 \\ 206 & 204 & 204 & 205 \\ 206 & 205 & 211 & 208 \\ 206 & 212 & 210 & 209 \end{bmatrix}$$

The S ordered vector (G) is

200	201	202	204	205	204	204	206
206	205	211	208	209	210	212	206

The pixel differences D_i of the adjacent pixels are

1	2	3	4	5	6	7	8
200	1	1	2	1	1	0	2
9	10	11	12	13	14	15	16
0	1	6	3	1	1	2	6

Here the peak point 'P' is 1, as it is the most frequently occurring pixel difference. As the number of occurrences of 1 in the vector is seven, the embedding capacity of the image is fourteen bits. The embedding bits (two bits) are converted to decimal. Let the embedding message (B) be 00111100000010. After embedding the bits using equations 5 and 6, the modified pixels (G_i) are

200	203	202	207	205	204	204	209
206	202	214	205	212	210	215	203

The part of a stego image is shown below

$$GG = \begin{bmatrix} 200 & 203 & 202 & 207 \\ 209 & 204 & 204 & 205 \\ 206 & 202 & 214 & 205 \\ 203 & 215 & 210 & 212 \end{bmatrix}$$

In the extraction process, firstly the stego image is converted into S ordered vector. The S ordered vector of stego image 'GG' is

200	203	202	207	205	204	204	209
206	202	214	205	212	210	215	203

Reconstructed image from S order using equation 6.

$$Reconstructed\ Image(R) = \begin{bmatrix} 200 & 201 & 202 & 204 \\ 206 & 204 & 204 & 205 \\ 206 & 205 & 211 & 208 \\ 206 & 212 & 210 & 209 \end{bmatrix}$$

It is obvious from the above example that the reconstructed image is equal to the original image (i.e) R=G.

PERFORMANCE METRICS

The proposed method is compared with the existing methods based on embedding capacity and the quality of the stego image is considered by measuring the standard metrics, Mean Square Errors (MSE) and the Peak signal-to-noise ratio (PSNR) between the original image and stego image. Bits per pixel (bpp), specifies the number of bits used to represent a pixel.

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [G(i,j) - R(i,j)]^2 \quad .....(7)$$

Where G is the original image and GG is the stego image. The PSNR (in dB) is defined as

$$PSNR = 10\log10(\frac{Max(G)^2}{MSE}) \quad .....(8)$$

$$BPP = \frac{Embedding\ Capacity}{Total\ number\ of\ Pixels} \quad .....(9)$$

IV. RESULTS AND DISCUSSION

Experimental results of the proposed method using natural and medical images are presented in this section. The performance of the proposed method is evaluated in terms of embedding capacity and quality of the reconstructed image. The proposed method, being reversible is able to extract the secret message and the cover image without any loss.

Table 1. Hiding Capacity for 512x512 grayscale Image and Image distortion

Host image (512x512) Grayscale	**Embedding Capacity in bits**			
	Ni et al[22]	***Ramaswamy et al[23]***	***Anushia devi et al[25]***	***Proposed Method***
Lena	2618	40740	59960	113438
Baboon	2759	16465	21532	29270
Cameraman	2905	37885	26214	164066
Barbara	2405	41327	45056	57418
Goldhill	2618	35022	45184	69984

Table 1 presents the performance comparison of the proposed method and similar existing methods. It is evident from Table 1 that the embedding capacity of the proposed method is two to four times higher than existing methods, revealing the superior performance of the proposed method.

Figure 2. (a) Lena cover image 512x512 grayscale (b) Lena Stego image 512x512 grayscale (c) Lena Reconstructed image 512x512 grayscale

Embedding capacity varies with various images. It is also worth noting from Table 1 that the proposed method achieves higher payload capacity. Table 2 shows that the proposed method produces better quality stego images which is revealed by the quality parameters PSNR, MSE and BPP.

Table 2. Comparison of the performance metrics of the proposed and existing methods

Host image (512x512) Grayscale	**Anushia devi et al[25]**		**Proposed Method (2 bits per pixel)**			**Proposed Method (3 bits per pixel)**		
	PSNR	***BPP***	***MSE***	***PSNR***	***BPP***	***MSE***	***PSNR***	***BPP***
Lena	32.11	0.23	6.56	39.96	0.43	35.34	32.65	0.65
Baboon	31.06	0.08	8.40	38.89	0.11	45.68	31.53	0.17
Cameraman	35.15	0.10	5.35	40.84	0.63	28.71	33.55	0.94
Barbara	31.69	0.17	7.64	39.30	0.22	41.42	31.96	0.33
Goldhill	31.64	0.17	7.57	39.33	0.27	41.05	31.98	0.40

Table 2 compares the performance of the proposed method for natural images. It is observed in Table 2 that the existing method achieves PSNR values in between 31 - 32 for 0.1 - 0.22 bpp. On the other hand the proposed method achieves PSNR values in between 38 - 40 for 0.1 – 0.6 bpp.

Performance of the proposed method is graphically represented in Fig. (3), Fig. (4) and Fig. (5).

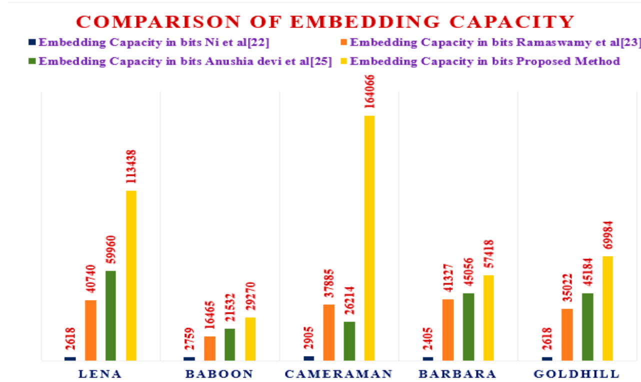

Figure 3. Comparison of embedding capacity of the proposed method and existing method

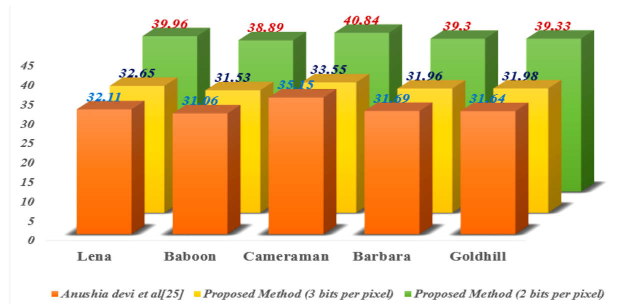

Figure 4. Comparison of PSNR of the proposed method and existing method

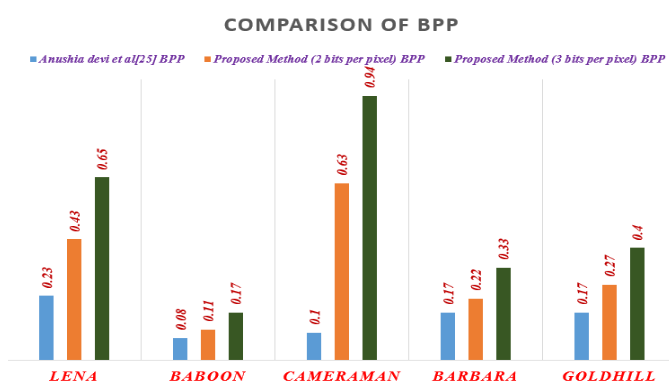

Figure 5. Comparison of BPP of the proposed method and existing method

V. CONCLUSION

In this paper, a novel technique is proposed, it based on differences of adjacent pixels for embedding data. The merits of the proposed method is multifold. 1. Both the secret message and cover image are extracted without any loss. 2. High embedding capacity. 3. Achieves high PSNR thus achieving high imperceptibility one of the important property of any steganography algorithm.

REFERENCES

[1] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," in IEEE Trans. on Image Processing, vol. 6. No. 12, pp. 1673-1687, Dec. 1997.

[2] J. Huang and Y. Q. Shi, "An adaptive image watermarking scheme based on visual masking," IEE Electronic Letters, vol. 34, no. 8, pp. 748-750, April 1998.

[3] C. W. Honsinger, P. Jones, M. Rabbani, and J. C. Stoffel, "Lossless recovery of an original image containing embedded data," US Patent: 6,278,791, 2001.

[4] M. Goljan, J. Fridrich, and R. Du, "Distortion-free data embedding," Proceedings of 4th Information Hiding Workshop, pp. 27-41, Pittsburgh, PA, April, 2001.

[5] Jun Tian, "Reversible data embedding using a difference expansion," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, no. 8, pp. 890-896, Aug. 2003.

[6] M.MaryShanthi Rani and K.Rosemary Euphrasia, "Data Security Through QR Code Encryption and Steganography", Advanced Computing: An International Journal (ACIJ), Vol.7, No.1/2,pp.1-7 March 2016.

[7] M. Mary Shanthi Rani and K.Rosemary Euphrasi, "A Comparative Study On Video Steganography in Spatial and IWT Domain", International Conference on Advances in Computer Applications,2016

[8] K. A. Navas, S. Archana Thampy, and M. Sasikumar "EPR Hiding In Medical Images for Telemedicine" International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering Vol: 2, No: 2, 2008.

[9] M.Maryshanthi Rani, S.Lakshmanan, "An Integrated Method of Data Hiding and Compression of Medical Images" International Journal of Advanced Information Technology (IJAIT) Vol. 6, No. 1, February 2016

[10] M.MaryShanthi Rani and S.Lakshmanan, "Region Based Data Hiding in Medical Images",International Journal of Advanced Research in Computer Science,vol.8 ,No.3 March – April 2017

[11] M.MaryShanthi Rani, G.Germine Mary and K.RosemaryEuphrasia "Multilevel multimedia security by Integrating Visual Cryptography and Stegnography Techniques", Computational intelligence, Cyber Security and Computational Models. Advances in Intelligent Systems and Computing, vol.412, pp.403-412, December, 2015.

[12] C Nagaraju and S S ParthaSarath, "Embedding ECG and patient information in medical images" IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), May 09-11, 2014, Jaipur, India.

[13] Mohit Gupta, Praveen, Kr. Tripathi, "Data Hiding Using Blind Algorithm of Steganography", International Journal for Research in Applied Science & Engineering Technology, Vol. 4, Issue IX, Sep 2016.

[14] M.MaryShanthi Rani and G.Germine Mary, "Compression of VC Shares", International Journal of Computational Science and Information Technology (IJCSITY), Vol.4, Issue.1, pp.57-65, February 2016.

[15] Mary Shanthi Rani, M. Germine Mary, G. and Rosemary Euphrasia,K. "High level Multimedia Security by incorporating Steganography and Visual Cryptography" International Journal of Innovations &Advancement in Computer Science IJIACS - ISSN 2347 – 8616 Volume 4, Special Issue September 2015.

[16] Anupriya Sohaland Dr.Lalita Bhutani, 'Unique Steganography Technique Using Wavelet Transform and Neural Network", International Journal of Latest Trends in Engineering and Technology, vol .5,Issue 1,jan 2015.

[17] E Divya and P Raj Kumar, "Steganographic Data Hiding using Modified APSO", International Journal of Intelligent Systems and Applications (IJISA), Vol.8, Issue.7, pp.37-45, 2016.

[18] M. Mary Shanthi Rani and K.Rosemary Euphrasia, "Dynamic Hiding of message in RGB Domain based on Random Channel Indicator", International Journal of Applied Engineering Research, Vol.10, Issue.76, pp.478-483, 2015.

[19] P.Thiyagarajan, V. Natarajan, G. Aghila, V. PrasannaVenkatesan and R. Anitha, "Pattern Based 3D Image Steganography", 3D Research, Springer, Vol.4, Issue.1, pp.1-8, 2013

[20] M.Mary Shanthi Rani, S.Lakshmanan and P.Saranya, "Video Steganography using Mid-Prime and Discrete Wavelet Technique", International Journal of Computer Engineering and Applications, Vol. 11, Issue 8, pp.180-190, August 17.

[21] M.Mary Shanthi Rani, S.Lakshmanan and G.Deepalakshmi, "Video Steganography using Mid-Point Circle Algorithm and Spatial Domain Technique", International Journal of Engineering and Techniques, Vol. 4 Issue. 1, Jan – Feb 2018.

[22] Z.Ni, Y.-Q.Shi, N. Ansari, W. Su, "Reversible data hiding", IEEE Trans. Circuits Syst. Video Technol. 16 (2006) 354–362.

[23] Rajkumar Ramaswamy and Vasuki Arumugam, "Lossless Data Hiding Based on Histogram Modification", Int. Arab J. Inf. Technol. 9 (2012) 445–451.

[24] M.Mary Shanthi Rani and S.Lakshmanan, "Combination of Reversible Data Hiding and Medical Image Compression", Journal of Global Research in Computer Science, Vol. 9 Issue. 2, Feb 2018.

[25] R.Anushia devi, Padmapriya Praveenkumar, John bosco Balaguru Rayappan and Rengarajan amirtharajan, 'Reversible Secret Data Hiding Based on Adjacency Pixel Difference, Journal if artificial Intelligence, Vol.10 Issue. 1 pp.22-31, 2017.

Authors Profile

Dr. M. Mary Shanthi Rani holds Ph.D in Computer Science and has more than 13 years of teaching experience .She has great passion for teaching and is currently working as Assistant Professor in the Department of Computer Science and Applications, The Gandhigram Rural Institute (Deemed to be University), Gandhigram. She has nearly sixty two publications in International Journals and Conferences .Her research areas of interest are Image Compression, Information Security, Ontology, Biometrics and Computational Biology. She has served in various academic committees in designing the curriculum for B.Sc. and M.C.A courses as well. She has also served as reviewer of Peer-reviewed International Journals and Conferences. She is a Life member of Indian Society for Technical Education. She has the credit of being the Associate Project Director of UGC Indo-US 21st Knowledge Initiative Project.

Mr. S.Lakshmanan is a Research Scholar (Full-time) in the Department of Computer Science and Applications, The Gandhigram Rural Institute – Deemed to be University, Dindigul, India. He received his Bachelor of Science (B.Sc) degree in Computer Science in the year 2012 from Madurai Kamaraj University and Master of Computer Applications (MCA) degree in the year 2015 from Gandhigram Rural Institute - Deemed University. He is currently pursuing Ph.D. degree in Gandhigram Rural Institute- Deemed University. His research focuses on Data hiding in Medical Images.